UNIVERSITAT OBERTA DE CATALUNYA (UOC)

GRADO DE INGENIERÍA INFORMÁTICA

TRABAJO FINAL DE GRADO

ÁREA: SEGURIDAD INFORMÁTICA

Democratización de la ciberinteligencia

Riesgos y oportunidades de la hiperconectividad

Autor: Julián Rafael Cortés Arnau

Tutor: Jorge Miguel Moneo

Profesor: Andreu Pere Isern Deyà

Barcelona, 2 de enero de 2024

Créditos/Copyright

FICHA DEL TRABAJO FINAL

Título del trabajo:	Democratización de la ciberinteligencia
Nombre del autor:	Julián Rafael Cortés Arnau
Nombre del colaborador/a docente:	Jorge Miguel Moneo
Nombre del PRA:	Andreu Pere Isern Deyà
Fecha de entrega (mm/aaaa):	01/2024
Titulación o programa:	Grado de Ingeniería Informática
Área del Trabajo Final:	Seguridad Informática
Idioma del trabajo:	Español
Palabras clave	Ciberinteligencia, OSINT

Cita

Ayudadme a comprender lo que os digo y os lo explicaré mejor.

Antonio Machado

Agradecimientos

En primer lugar, dar gracias a Dios por el don de la vida, por aquellas personas que ha querido que estén a mi lado y, por tantos y tantos bienes que muchas veces pasan desapercibidos y por los que nunca estoy lo bastante agradecido.

También quisiera expresar mi más sincero agradecimiento al tutor Jorge Miguel Moneo por su labor de supervisión durante la realización de este trabajo, así como al profesor Andreu Pere Isern Deyà por su trabajo de coordinación.

Dar las gracias también a mi compañero Eusebio, que fue quien me propuso realizar este TFG sobre ciberinteligencia y me ayudó a dar los primeros pasos. También agradecer a mis padres su apoyo emocional y logístico todos estos años. Vosotros tenéis amor. Por último, –pero no menos importante– solo me queda dar las gracias a mi prometida Isabel. Eres testimonio de superación, esfuerzo y constancia. Sin tus interminables horas de escucha, nunca habría podido comprender tantas y tantas cosas.

Resumen del Trabajo

El propósito del presente Trabajo Final de Grado es el de dar a conocer el concepto de ciberinteligencia desde la perspectiva de la información disponible en Internet de forma abierta (OSINT). Este concepto, desconocido para el gran público, está cobrando una importancia capital en la última década y es un terreno todavía por explotar. Con el auge de la Inteligencia Artificial y la proliferación de ataques de Ingeniería social cada vez más sofisticados, la concienciación y creación de una cultura de ciberseguridad es previsible que cobre una importancia tan grande como la alfabetización. Es por este motivo que, a través de la investigación de fuentes abiertas se van a exponer los riesgos más comunes para posteriormente abordar las mejores prácticas a seguir por parte de los usuarios de internet. Es a través de estas dos fases que se pretende lograr una mayor democratización de la ciberinteligencia, es decir, que aquellas personas cuyos datos están en la red, puedan ser capaces de conocer hasta qué punto su información está siendo vulnerada.

Palabras clave: Ciberinteligencia, OSINT, ciberseguridad, software, herramientas, privacidad, Internet, democratización, ciberalfabetización.

Abstract

The purpose of this work is to publicize the concept of Cyber Intelligence from the perspective of Open Source Information available on the Internet (OSINT). This concept, unknown to the general public, is gaining a capital importance in the last decade and is a field still to be exploited. With the rise of Artificial Intelligence and the proliferation of increasingly sophisticated social engineering attacks, the awareness and creation of a Cybersecurity culture is expected to take on as great importance as literacy. It is for this reason that, through research from Open Sources, the most common risks will be exposed to later address the best practices to be followed by Internet users. It is through these two phases that it is intended to achieve a greater Democratization of Cyberintelligence for those people whose data are on the network may be able to know to what extent their information is being violated.

Keywords: Cyberintelligence, OSINT, cybersecurity, software, tools, privacy, Internet, democratization, cyberliteracy.

Índice general

Índice de figuras

Índice de tablas

Control de cambios

REVISIÓN	FECHA	MOTIVO	CONTENIDO REVISADO
0	27/09/2023	Creación del documento.	Todo
1	10/10/2023	Redacción del capítulo 2, implementación de la bibliografía, modificación del diagrama de Gantt, implementación de notas a pie de página y referencias cruzadas. Realización de los cambios comentados por parte del tutor.	Todo
2	05/11/2023	Ampliación del apartado 2.2.1. añadiendo la infografía sobre los flujos de trabajo y caso concreto de estudio en el TFG.	Todo
3	15/11/2023	Redacción del capítulo 3. Redacción del apéndice A. Traslado de los apartados «Formatos de la información y su representación» y «Las expresiones regulares» al apéndice B. Realización de los cambios comentados por parte del tutor.	Todo
4	29/11/2023	Inicio de la redacción del capítulo 4 y del glosario. Citado del capítulo 3.	Capítulos 3 y 4
5	10/12/2023	Ampliación del capítulo 4 con los resultados obtenidos de los análisis de ciberinteligencia.	Capítulo 4
6	14/12/2023	Inicio de la redacción del capítulo 5 y ampliación del glosario. Redacción de los agradecimientos.	Capítulo 5 y glosario
7	15/12/2023	Cambio de la licencia del documento a una 4.0 Internacional de Creative-Commons siguiendo las recomendaciones de esta organización a causa de que la 3.0 España queda obsoleta	Créditos/Copyright
8	30/12/2023	Ampliación de los casos de estudio del capítulo 4 incluyendo el uso de la herramienta Sherlock. Ampliación del subapartado de trabajos futuros del capítulo 5. Revisión final para presentación.	Capítulos 4 y 5

Tabla 1: Control de cambios

Capítulo 1

Introducción y planificación

1.1. Contexto y justificación del trabajo

En el mundo densamente interconectado de hoy, la cantidad de datos que se generan a diario es, simplemente inimaginable [1], y gran parte de estos son accesibles de forma pública por cualquier persona en cualquier momento y en cualquier parte del mundo. En este aspecto, la inteligencia de fuentes abiertas (OSINT) tiene como beneficio el hecho de que es fácil de recoger, procesar y relacionar para obtener conocimientos [2]. Los últimos avances en inteligencia artificial tales como ChatGPT y otros tipos de sistemas de información para aplicaciones dedicadas a la economía o a la sociedad, pueden ayudar a prevenir las amenazas cibernéticas. Desgraciadamente, la inteligencia de fuentes abiertas es un arma de doble filo que puede utilizarse y, de hecho se utiliza, para la delincuencia.

En los últimos años el perfil del pirata informático ha cambiado radicalmente de ser un lobo solitario, cuyo objetivo era el de piratear algún sistema importante para obtener fama y reconocimiento, a ser el integrante de una organización perfectamente estructurada y con un gran número de componentes. Esto dificulta en gran medida la lucha contra la piratería puesto que, estas organizaciones criminales trabajan de forma coordinada y pueden encontrar debilidades en los sistemas informáticos en las que difícilmente podría reparar una sola persona. El riesgo que esto supone para las empresas y los gobiernos es muy alto puesto que, en el mejor de los casos, los departamentos de ciberseguridad de las empresas cuentan con, a lo sumo decenas de personas mientras que las organizaciones criminales pueden contar con centenares.

Se está viviendo una revolución en la cual los avances tecnológicos crecen a un ritmo al que el ciudadano de a pie no puede permitirse ser ajeno a las últimas tendencias en el uso de los datos accesibles públicamente [3]. Todavía existe cierta precariedad en el conocimiento de los datos que ciertas fuentes poseen de los usuarios y que son de gran importancia [2]. Es un dicho común que algunos portales de internet bien conocidos saben más cosas de los usuarios que ellos mismos; motivo por el cual, se podría estar presenciando en la actualidad el nacimiento de un nuevo concepto que podría llamarse ciberalfabetización.

Lo cierto es, que el ciudadano de a pie debería conocer a la perfección como mínimo las implicaciones básicas que puede tener la exposición de sus datos [4] en la red y, muchas veces esto es extremadamente complicado puesto que, las redes sociales disponen de algoritmos de recolección de datos que no son de código abierto. Si a esto se le suma que es muy difícil entender los acuerdos de usuario propuestos por las empresas a las que se cede los datos, el usuario rehúye totalmente el tratar de comprender los usos básicos de sus datos y termina por confiar en una seguridad intrínseca al servicio que está usando. En este escenario, el conocer o, quizá de forma más poética, democratizar la ciberinteligencia parece ser una salida a un problema que tiene la sociedad. Así pues, tal es la justificación principal de este trabajo: dar a conocer un campo de estudio al que apenas se hace mención en los medios o, al menos no usando explícitamente el término de ciberinteligencia.

La inteligencia de fuentes abiertas u OSINT consiste en la recolección, procesamiento y correlación de información pública de fuentes de datos abiertas tales como: medios de comunicación, redes sociales, foros, blogs, datos públicos de los gobiernos, publicaciones o datos comerciales [5]. A partir de una serie de datos de entrada, con la aplicación de técnicas avanzadas de recolección y análisis, la OSINT está continuamente expandiendo el conocimiento sobre el objetivo; de esta forma la información encontrada alimenta el proceso de búsqueda otra vez para llegar al objetivo final. A día de hoy, la OSINT está ampliamente adoptada por gobiernos y servicios de inteligencia para dirigir sus investigaciones y luchar contra el cibercrimen, sin embargo, no son los únicos como ya se ha dicho más arriba.

1.2. Objetivos del trabajo

El objetivo general de este trabajo es el de dar a conocer las ténicas y procedimientos más habituales en el campo de la ciberinteligencia. Gran parte de la sociedad actual

muchas veces vive totalmente ajena a la enorme cantidad de datos personales que vierte a las redes sociales [6]. Si a esto se suma la información que puede obtenerse indirectamente a partir de otras fuentes tales como redes WiFi inseguras, dispositivos IoT o cámaras conectadas a internet, el cruce de información puede resultar en un perfilado del sujeto extremadamente preciso. Ante tal escenario, se pretende, a través del presente trabajo, realizar una tarea de divulgación, concienciación y democratización de las herramientas de código abierto necesarias para conocer los riesgos a los que se está sometido a diario, convirtiendo estos en una oportunidad para hacer un mejor uso de la tecnología.

1.2.1. Objetivos específicos

1. Concienciar sobre los riesgos de la hiperconectividad en la sociedad actual. Este primer objetivo se pretende lograr mediante una investigación a fondo sobre los riesgos y desafíos asociados con la hiperconectividad, la privacidad en línea, la desinformación y aquellos inherentes a un uso irresponsable de las redes sociales, entre otros.

2. Dar a conocer el impacto que pueden tener sobre las personas y las organizaciones los datos que están disponibles en la red de forma pública, ya sean de forma consciente o inconsciente. A través de ejemplos y estadísticas reales se busca proporcionar formas de reconocer y valorar la calidad de la información que llega al usuario y, si el mensaje que se pretende trasmitir a través de ella tiene intereses ocultos. Resulta de vital importancia el saber discernir la información real de las tan conocidas fake news. A través de diversas técnicas se mostrará al lector cómo identificarlas y, en general ver toda la información con una mirada crítica.

3. Divulgar las diferentes técnicas de ciberinteligencia de fuentes abiertas (OSINT). Aunque no se pretende en este TFG el crear un manual de formación avanzado para analistas de información, sí que se busca el dar a conocer las técnicas básicas para mejorar el autoconocimiento, el pensamiento crítico y la democratización de estas técnicas en aras de la reducción de los ataques de desinformación e ingeniería social. Como decía Sun Tzu en *El arte de la guerra*, «para conocer a tu enemigo, debes convertirte en tu enemigo». Asimismo también se darán a conocer aquellas fuentes en las que va a ser posible estar al día de las novedades sobre amenazas en ciberseguridad y filtraciones de datos.

4. Dar a conocer las herramientas de código abierto disponibles en la red, su funcio-

namiento práctico y crear un conjunto de indispensables de uso gratuito. Existe un gran número de herramientas de auditoría o pentesting, de hecho, tantas que en ocasiones puede ser una ardua tarea el llegar a conocer la más adecuada para el fin que se tenga entre manos. El alto nivel de especificidad de algunas de estas aplicaciones, puede llegar a hacer necesaria una formación previa por parte del usuario; así pues, únicamente se van a elegir aquellas que más se amolden a los objetivos que se persiguen en este TFG y, que además tengan una curva de aprendizaje rápida.

5. Crear un procedimiento para el uso sistemático de las herramientas de OSINT a nivel de usuario, de forma que el mayor número de personas sean capaces de interpretar los resultados obtenidos sin incidir demasiado en detalles técnicos que, en ocasiones pueden ser confusos. Este puede ser quizás el apartado más complicado, porque requiere de llegar a una solución de compromiso entre lo muy técnico y lo intuitivo. Hay que tener en cuenta que, muchas aplicaciones de pentesting y auditorías de seguridad no tienen una interfaz amigable porque están pensadas para usuarios con conocimientos previos de informática y funcionan en entornos de terminal. Lo ideal para el usuario sin estos conocimientos es que estas aplicaciones dispongan de una Interfaz Gráfica de Usuario (o GUI por sus siglas en inglés) por lo que se va a minimizar el uso de las mismas si hay una alternativa con GUI.

6. Realizar un listado de buenas prácticas para aumentar la resiliencia frente a los ciberataques contra personas y organizaciones. Una vez expuesto todo lo anterior, la parte final del trabajo será poner en tela de juicio todo lo aprendido y sintetizarlo para que, de un vistazo sea posible recordar todos los puntos investigados. El objetivo es que, a través de este decálogo sea posible identificar rápidamente la aplicación necesaria y saber en qué punto se está en el proceso. También se expondrá un caso de uso a modo de autoauditoría de seguridad para conocer el nivel de salud de la privacidad del usuario. La idea es que, aunque incluso dando un uso mínimo de este decálogo, sea posible conocer las repercusiones de la información en fuentes abiertas que se pueda encontrar.

1.3. Impacto en sostenibilidad, ético-social y de diversidad

Los puntos que se indican a continuación están basados en los Objetivos de Desarrollo Sostenible (ODS) [7], también conocidos como Objetivos Globales, que fueron adoptados por las Naciones Unidas en 2015 como un llamamiento universal para poner fin a la pobreza, proteger el planeta y garantizar que para el 2030 todas las personas disfruten de paz y prosperidad.

Los 17 ODS están integrados: reconocen que la acción en un área afectará los resultados en otras áreas y que el desarrollo debe equilibrar la sostenibilidad social, económica y ambiental. Los países se han comprometido a priorizar el progreso de los más rezagados.

Los ODS están diseñados para acabar con la pobreza, el hambre, el sida y la discriminación contra mujeres y niñas. La creatividad, el conocimiento, la tecnología y los recursos financieros de toda la sociedad son necesarios para alcanzar los ODS en todos los contextos.

1.3.1. Impacto en sostenibilidad

- **ODS 7 – Energía asequible y limpia.**
  - No tiene ningún impacto, ni positivo ni negativo puesto que las técnicas expuestas en este trabajo no están relacionadas en ningún modo con los procesos de generación eléctrica. En cualquier caso, lo ideal sería que el consumo de los equipos de computación procediera de fuentes limpias.
- **ODS 9 – Industria, innovación e infraestructura.**
  - Las tecnologías que se van a estudiar en el presente TF pueden tener un impacto negativo al hacer uso de aplicaciones de alto consumo computacional. Asimismo, al realizar búsquedas de datos por internet también va a aumentar el consumo computacional de otros equipos conectados a la red.
  - Acciones para potenciar el impacto positivo y minimizar el negativo: Apagar las computadoras cuando no se estén usando, lanzar las consultas indispensables y utilizar dispositivos de alta eficiencia.

- **ODS 11 – Ciudades y comunidades sostenibles.**
  - No tiene ningún impacto ni positivo ni negativo debido a que no está relacionado con la disciplina de la arquitectura o el urbanismo.
- **ODS 12 – Consumo y producción responsables.**
  - Esta tecnología tiene un impacto negativo por la posible contaminación debido a la utilización de elementos electrónicos a partir de los cuales están fabricados los ordenadores y que son potencialmente contaminantes. Por ejemplo, baterías, semiconductores o metales pesados.
  - Acciones para minimizar el impacto negativo: Una vez finalizada la vida útil de los equipos depositarlo en un punto limpio para su reciclaje. Utilizar equipos de calidad para que su vida útil sea prolongada.
- **ODS 13 – Acción climática.**
  - No tiene ningún impacto ni positivo ni negativo puesto que no influye sobre la huella de carbono más allá de lo indicado en el ODS 12.
- **ODS 14 – La vida bajo el agua.**
  - No tiene ningún impacto ni positivo ni negativo ya que no existe una interacción con el medio marino que pueda afectar a este de forma directa.
- **ODS 15 – La vida en la tierra.**
  - No tiene ningún impacto ni positivo ni negativo. No se detectan en principio factores que puedan influir sobre la biodiversidad, puesto que todos los equipos informáticos están siempre aislados de cualquier interacción con la biocenosis.

Las razones para elegir este TF no tienen que ver con la sostenibilidad.

1.3.2. Comportamiento ético y responsabilidad social durante la totalidad del proyecto

- **ODS1 – No pobreza.**
  - No tiene ningún impacto ni positivo ni negativo. Los conocimientos expuestos en este trabajo no proceden de iniciativas solidarias, pero tampoco las

afectan.

- **ODS2 – Cero hambre.**
  - No tiene ningún impacto ni positivo ni negativo. Los conocimientos expuestos no proporcionan técnicas para el incremento de producción de alimentos o la mejor distribución de estos.
- ODS **6 – Agua potable y saneamiento.**
  - No tiene ningún impacto ni positivo ni negativo. En el presente trabajo no se exponen técnicas para la mejora de las redes de distribución de agua potable o de saneamiento debido a que se trata de un campo de estudio diferente.
- **ODS 8 – Trabajo decente y crecimiento económico.**
  - La temática de este TF puede tener un impacto sobre el crecimiento económico al proporcionar herramientas para la adquisición de datos de fuentes abiertas para aumentar la competitividad entre empresas de distintos capitales sociales, incluso entre países con distintos recursos económicos.
- **ODS 16 – Paz, justicia e instituciones sólidas.**
  - El proyecto cumple con los principios éticos y código deontológico de la ingeniera del software. De igual modo, el objetivo del mismo es el de dar mayor visibilidad y, por tanto, democratizar las herramientas de búsqueda de datos de los usuarios de internet. Dichos datos pueden ser sus datos, y poder realizar las reclamaciones pertinentes.

Las razones para elegir este TF no tienen que ver con el comportamiento ético y responsabilidad social durante la totalidad del proyecto.

1.3.3. Impacto sobre la diversidad

- **ODS 5 – Igualdad de género.**
  - La tarea de investigación que se va a llevar a cabo en este trabajo no supone un impacto ni negativo ni positivo en este aspecto. Los conocimientos que se van a exponer pueden ser utilizados indistintamente por cualquier persona debido a que el género no es un factor limitante para su aplicación.

- **ODS 10 – Reducir desigualdades.**
    - Los conocimientos que se van exponer en este trabajo se prevé que ayuden a democratizar el uso de los datos que existen en las fuentes públicas y, por tanto, ayuden a reducir las desigualdades entre los ciudadanos. También se pretende reducir estas desigualdades mediante el uso de un lenguaje sencillo y directo.

Las razones para elegir este TF no tienen que ver con la sostenibilidad. Todos los objetivos de desarrollo (ODS) anteriormente analizados, se tendrán en cuenta a lo largo del desarrollo del proyecto. Son estudiados para reducir el impacto negativo y potenciar el positivo en su fase de estudio, y tenidos en cuenta durante todo el desarrollo del proyecto.

1.4. Estado del arte

En este apartado se hará una exposición general sobre el estado de desarrollo actual del campo de estudio de este trabajo. De esta forma, se podrá tener una idea inicial de lo que se pretende desarrollar antes de entrar en materia en cada uno de los capítulos de que está compuesto este trabajo. La ciberinteligencia es un área en constante evolución que se enfoca en la recopilación, análisis y aplicación de información relacionada con amenazas cibernéticas [8]. Su objetivo principal es identificar y mitigar posibles ataques cibernéticos, así como comprender y prevenir futuras intrusiones. Las tecnologías involucradas en este campo generalmente se considera que son las siguientes:

1. Análisis de datos avanzado. Se trata de una disciplina crucial en la lucha contra las amenazas cibernéticas. La ciberinteligencia se basa en el análisis de grandes volúmenes de datos para identificar patrones y tendencias [9]. Esto incluye el procesamiento de registros de red, registros de actividad del sistema y otros tipos de datos relacionados con la seguridad cibernética. Se utilizan herramientas de análisis de datos avanzadas, como el aprendizaje automático y la inteligencia artificial, para descubrir amenazas ocultas y correlaciones significativas. Si se quiere entrar en mayor detalle, podría dividirse este campo en ocho puntos:

    a) Recopilación de Datos. Se incluyen registros de red, logs de servidores, bases de datos, tráfico de red, contenido web, entre otros. También se pueden incluir feeds de inteligencia, informes de seguridad y bases de datos públicas. Es importante garantizar que la recopilación de datos se realice de manera

legal y ética, cumpliendo con las leyes de privacidad y protección de datos.

b) Procesamiento de Datos. Los datos suelen estar en diferentes formatos y calidades. Es crucial normalizarlos para que sean comparables y limpiarlos de errores o datos irrelevantes. Acto seguido, se debe proteger la privacidad de los individuos cuyos datos están involucrados.

c) Análisis Estadístico y de Machine Learning. Se realizan resúmenes estadísticos para comprender la distribución de los datos y las relaciones entre las variables. También se utilizan algoritmos de machine learning para predecir tendencias futuras o identificar patrones de comportamiento anómalo. Adicionalmente, el aprendizaje no upervisado ayuda a identificar agrupaciones o anomalías sin la necesidad de etiquetas predefinidas.

d) Análisis de Redes. Mediante la creación de grafos de redes se pueden representar las relaciones entre entidades en el ciberespacio como un grafo, lo que facilita la identificación de nodos clave y patrones de comunicación.

e) Análisis de Comportamiento de red. Identificación de patrones de tráfico anómalo que pueden indicar actividades maliciosas.

f) Integración de Inteligencia de Amenazas. Existen feeds de inteligencia que incorporan información de amenazas conocidas para comparar con los datos recopilados y detectar coincidencias. Tambien se utilizan los llamados indicadores de Compromiso (IoCs) cuya función es identificar actividades sospechosas o maliciosas en los sistemas.

g) Visualización de datos, gráficos y diagramas. Ayudan a representar visualmente la información, lo que facilita la identificación de patrones y tendencias. También son de ayuda los dashboards interactivos que permiten a los analistas explorar datos de manera dinámica.

h) Automatización y escalabilidad. Automatización de tareas rutinarias, para lo cual se utilizan scripts y herramientas para tareas repetitivas, liberando tiempo para análisis más complejos. La escalabilidad permite procesar grandes volúmenes de datos, y es especialmente crucial en entornos de alta demanda.

2. Inteligencia de amenazas. La ciberinteligencia se centra en la recopilación y el análisis de inteligencia de amenazas, que incluye información sobre actores ma-

liciosos, sus tácticas, técnicas y procedimientos (TTP) y las vulnerabilidades de software y hardware que explotan [10]. Se utilizan fuentes como feeds de amenazas, informes de seguridad, foros de hacking y la inteligencia de amenazas de código abierto (OSINT) para mantenerse al tanto de las amenazas emergentes.

3. Automatización y orquestación de seguridad. Para hacer frente a la creciente cantidad de amenazas, se ha adoptado la automatización y la orquestación de seguridad [11]. Las soluciones de ciberinteligencia pueden identificar automáticamente amenazas, tomar medidas para mitigarlas y coordinar la respuesta de seguridad en tiempo real. Esto ayuda a reducir el tiempo de detección y respuesta a incidentes.

4. Inteligencia artificial y machine learning. La IA y el aprendizaje automático desempeñan un papel crucial en la identificación de patrones de comportamiento anormal, detección de amenazas y toma de decisiones en ciberseguridad [12]. Estas tecnologías permiten a las organizaciones anticipar amenazas y mejorar la precisión de la detección de intrusiones.

5. Colaboración y compartir información. La ciberinteligencia se beneficia de la colaboración entre organizaciones, gobiernos y la comunidad de seguridad cibernética en general [13]. El intercambio de información sobre amenazas y vulnerabilidades es esencial para una defensa efectiva contra ataques cibernéticos.

6. Trazabilidad y forense digital. La capacidad de rastrear y analizar actividades cibernéticas después de un incidente es fundamental [14]. La forense digital se utiliza para investigar incidentes, determinar su alcance y atribuirlos a actores específicos.

Es importante destacar que el campo de la ciberinteligencia es altamente dinámico, con nuevas amenazas y tecnologías emergiendo constantemente, las cuales serán adecuadamente investigadas, expuestas y aplicadas en los capítulos 2, 3 y 4 respectivamente. Las organizaciones y los profesionales de la ciberseguridad deben mantenerse actualizados con las últimas tendencias y desarrollos para garantizar una defensa efectiva contra las amenazas cibernéticas en evolución constante.

1.5. Enfoque y metodología

La metodología a seguir será la del modelo de desarrollo en cascada [15]. El motivo por el que se elige este método se debe a que, primero es necesario dar a conocer al lector unos conocimientos y una formación básica en el campo de la OSINT. Seguidamente, una vez adquiridos los mismos, se puede pasar a divulgar la relación existente entre los conocimientos básicos y las técnicas que se utilizarán. Finalmente y, únicamente habiendo completado las fases anteriores, será posible poner en práctica lo aprendido para comprobar y verificar que dichos conocimientos se pueden utilizar de forma efectiva. Esta fase final se espera también que llegue a despertar el interés del lector por la disciplina expuesta y fomente una mayor cultura de ciberseguridad. Se estima que, no hacerlo de este modo generaría confusión y desinterés en el lector al no disponer de los conocimientos previos requeridos en cada fase.

Dicho esto, el enfoque que se dará al trabajo será el de investigación inicial para una posterior divulgación y presentación de resultados. Finalmente, se realizará un caso de uso de los recursos, programas y datos que se han investigado.

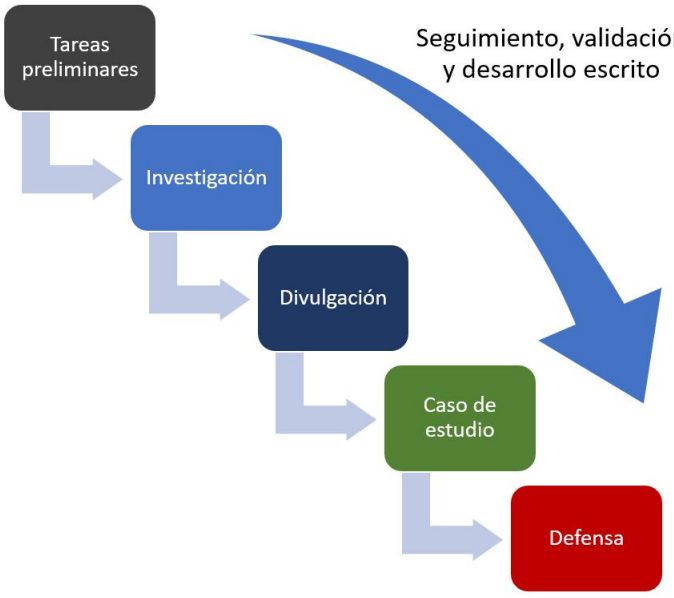

Figura 1.1: Fases de desarrollo del proyecto

Cada fase tiene un conjunto de entregables, que se detallarán en profundidad en el apartado de planificación. En cada una de las fases se redactará la documentación propia de cada fase y, tras las validaciones finales, se analizan y plasman las conclusiones en la documentación.

Cada entregable es valorado por parte del equipo docente. Con esta información, se realizan los cambios necesarios para corregir los aspectos a mejorar, y las soluciones serán implementadas en siguientes entregas o, en último caso, en la entrega final.

A lo largo de todo el proyecto, se mantendrá una comunicación fluida con el personal docente. Dicha comunicación se llevará a cabo principalmente mediante correo electrónico. Es importante destacar que las opiniones del cliente serán consideradas de gran importancia en todo momento, especialmente en caso de que se presenten desviaciones técnicas o temporales a lo largo del proyecto. En estos casos, se trabajará de manera conjunta con el tutor para identificar y abordar cualquier problema que pueda surgir y asegurar así el éxito del proyecto.

1.5.1. Listado de tareas

Seguidamente se establece el plan de trabajo a seguir durante el presente TFG, indicando las fases y las tareas que se van a llevar a cabo en cada una de ellas [16].

- **FASE 1: TAREAS PRELIMINARES**
  - Definición del plan de trabajo y diagrama de Gantt de las tareas según fechas establecidas en el aula para entrega de las PEC.
  - Búsqueda inicial de fuentes de información como puntos de partida. Éstas se irán ampliando si es necesario a medida que el trabajo avance.
  - Revisión del estado del arte y software de OSINT.
- **FASE 2: DESARROLLO DE LA INVESTIGACIÓN (OBJETIVOS 1 Y 2)**
  - Definición detallada de conceptos de ciberinteligencia.
  - Principales riesgos de las redes sociales.
  - Técnicas de recopilación de información.
- **FASE 3: EXPOSICIÓN DE RESULTADOS (OBJETIVOS 3 Y 4)**
  - Recopilación de todos los datos encontrados para su ordenación y exposición en un lenguaje menos técnico que en la fase anterior, de modo que cualquier persona pueda entender el funcionamiento básico de la ciberinteligencia.

- **FASE 4: CASO DE ESTUDIO (OBJETIVOS 5 Y 6)**
  - Utilización de las herramientas, software y otros recursos tecnológicos que se han obtenido en fases anteriores para realizar una prueba real con la propia identidad.
  - Procesamiento y análisis de resultados.
  - Buenas prácticas y lecciones aprendidas. En este punto final, la idea es sacar conclusiones de los resultados obtenidos a lo largo del caso de uso y proporcionar unas pautas básicas para el día a día de las personas y organizaciones que vayan un paso más allá de las que todo el mundo conoce.
- **FASE 5: DESARROLLO ESCRITO**
  - Preparación de la memoria. Si bien esta fase está en curso durante la totalidad de la planificación, es en este punto final donde se realizarán las últimas revisiones, cambios y correcciones en caso de ser necesarias. Puesto que aquí ya se espera que esté realizado gran parte del trabajo, no debería llevar más tiempo que el de la lectura, verificación de párrafos, espaciados, gramática, etc.
  - Desarrollo de la presentación. A partir de la memoria se van a preparar las diapositivas que servirán de síntesis de todo el trabajo realizado.
- **FASE 6: DEFENSA**
  - Grabación del vídeo.
  - Defensa del TFG ante el tribunal.

1.6. Planificación

Se estima una dedicación total de 300 horas, lo que supone una dedicación semanal de 15 horas, que se traducen en alrededor de 2 horas y 10 minutos de trabajo diario. Según lo expuesto en los puntos anteriores, se establecen 6 entregables a lo largo del desarrollo del proyecto, los cuales estarán compuestos por una o varias fases que fueron previamente descritas. Estos entregables se han definido para asegurar que se cumplan los objetivos del proyecto en el plazo establecido y con los recursos disponibles.

Si se distribuye el trabajo de todas las fases entre los distintos entregables, el contenido del proyecto se define como sigue.

- **PEC1: Propuesta y plan de trabajo.**
  Se estima en unas 30 horas distribuidas para lograr los siguientes objetivos.
  1. Determinar en qué consistirá su trabajo final.
  2. Explicar de manera razonada la motivación y justificación del trabajo final escogido.
  3. Definir los objetivos del trabajo.
  4. Ser capaz de realizar una planificación para el desarrollo del trabajo.
  5. Redactar documentos técnicos siguiendo los formalismos establecidos.
- **PEC2: Seguimiento del trabajo y entrega parcial.**
  Se estima en unas 100 horas distribuidas para lograr los siguientes objetivos.
  1. Justificar con evidencias la línea de trabajo escogida.
  2. Buscar bibliografía adecuada para el trabajo a desarrollar.
  3. Refinar los objetivos parciales definidos en la actividad anterior.
  4. Redactar documentos siguiendo los formalismos científicos establecidos.
  5. Organizar la información de manera coherente.
- **PEC3: Seguimiento del trabajo y entrega parcial.**
  Se estima en unas 100 horas distribuidas para lograr los siguientes objetivos.
  1. Realizar las tareas propias para el desarrollo de un proyecto y/o investigación.
  2. Seguir la planificación y la metodología definidos para una investigación concreta
  3. Redactar documentos siguiendo los formalismos científicos establecidos.
- **PEC4: Memoria final y entrega definitiva.**
  Se estima en unas 50 horas distribuidas para lograr los siguientes objetivos.

1. Poner en práctica los conocimientos adquiridos a lo largo de toda la titulación.

2. Adquirir experiencia para afrontar los retos que supone sacar adelante un proyecto completo.

3. Documentar y justificar el desarrollo y el resultado del trabajo.

- **PEC5: Presentación en vídeo.**
  Se estima en unas 10 horas distribuidas para lograr los siguientes objetivos.

  1. Hacer presentaciones de trabajos técnicos.

  2. Hacer vídeos que sinteticen el contenido de un trabajo de gran envergadura.

- **PEC6: Defensa asíncrona del TFG.**
  Se estima en unas 10 horas distribuidas para lograr los siguientes objetivos.

  1. Defender y justificar el desarrollo y el resultado del trabajo realizado durante el TFG.

A continuación, se detallan las fases del proyecto de forma conjunta con las fechas de los entregables mediante el uso de un diagrama de Gantt [17]. Aunque se ha tratado de realizar una planificación equilibrada y acorde con el tiempo disponible, al igual que ocurriría con cualquier proyecto, éste no está libre de que surjan imprevistos, entre los cuales se podrían encontrar:

- Dificultades para obtener información sobre un tema específico. En este caso, habría que reducir su exposición y/o buscar otro tema similar para no consumir el tiempo planificado de la siguiente etapa.

- Baja calidad de la información encontrada. Puesto que el tiempo no es ilimitado y no va a ser posible investigar durante más del disponible, ante todo hay que mantener una calidad homogénea en la información que se vaya a divulgar. Si es necesario, se intentará ampliar contenidos buscando otras disciplinas aparte de la OSINT, pero no se va a divulgar información de dudosa calidad o poco elaborada.

- Dificultades para comprender la información que se va a exponer. En este caso, se contactará con el profesor responsable del seguimiento del TFG para valorar conjuntamente la conveniencia de exponer esa información. Se pedirá asesoramiento

al mismo para encontrar información en fuentes de información recomendadas.

- Pérdida de la información del trabajo. Aunque el trabajo se va a desarrollar en la plataforma Overleaf[1] mediante el sistema de tipografía LaTeX y este sistema está alojado en la nube, no está exento de errores internos o pérdidas de información. Para securizar aún más el trabajo y evitar imprevistos, se van a guardar copias periódicas de información en el OneDrive[2] de la UOC.

- Problemas de compilación del sistema LaTeX. Aunque Overleaf dispone de un excelente manual de intrucciones, en caso de producirse errores de compilación, se dispone también del manual *La Biblia de LaTeX 2ε* de David Santo Orcero [18] como apoyo.

- Problemas de fuerza mayor, tales como enfermedades o problemas familiares. La solución a estos imprevistos –como no puede ser de otro modo– pasará por una solución consensuada con los profesores responsables.

- Problemas técnicos de cualquier tipo. Puesto que la metodología de la UOC es 100 % online, el hecho de que surjan problemas relacionados con los equipos informáticos, es una realidad para la cual hay que tener un plan de contingencia tal como el que sigue:

    - Problemas con la conexión a internet. Disponer de otro lugar en el que conectarse tal como el trabajo, la biblioteca, la casa de un conocido, etc. Lo ideal será tener en preaviso a esta persona el día de la defensa del trabajo y la respuesta a las preguntas del tribunal.

    - Indisponibilidad del ordenador. Lo ideal es disponer de un segundo equipo, lo cual va a ser posible, así como del portátil del trabajo. Este equipo de respaldo deberá tener instaladas también las aplicaciones requeridas para el desarrollo del trabajo.

    - Indisponibilidad de la webcam. Se dispone de webcam incorporada en el portátil que se tendrá preparado como equipo de respaldo.

    - Mal funcionamiento del micrófono. Se dispone de un segundo par de auriculares con micrófono además del que lleva incorporado el PC de respaldo.

[1] https://www.overleaf.com/
[2] https://onedrive.live.com/about/es-es/

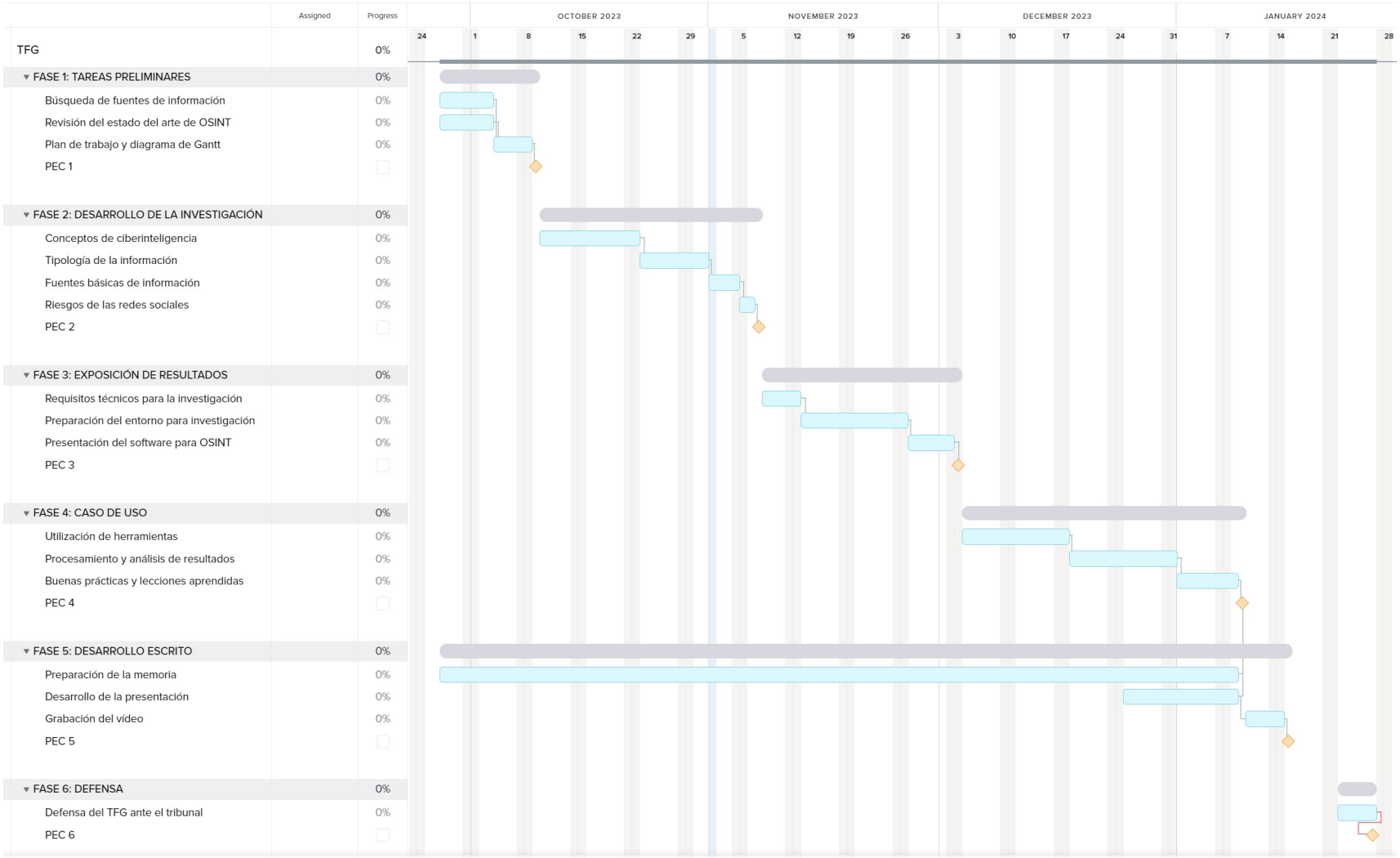

Figura 1.2: Planificación inicial del proyecto

1.7. Breve sumario de productos obtenidos

El resultado del trabajo es un documento de investigación relacionado con la ciberinteligancia y, más concretamente, con la OSINT. Para el desarrolo del mismo se va a hacer uso intensivo de artículos científicos, revistas y libros, los cuales se van a mencionar en la bibliografía. Después de una primera parte de investigación, se va a utilizar todo lo encontrado para crear un manual de buenas prácticas para el día a día, utilizando un lenguaje sencillo y asequible. Asimismo, se va a crear una relación de herramientas de software básico para encontrar información de fuentes públicas y demostrar hasta qué punto existe información propia de un usuario en la red. Mediante esta prueba, se pretende concienciar al usuario estándar de redes sociales u otros servicios comunes sobre la salud de sus datos de su privacidad.

1.8. Breve descripción de los otros capítulos de la memoria

La estructura de este documento se basará en la distribución de los capítulos de acuerdo con las fases de desarrollo del proyecto anteriormente expuestas, que sigue una metodología en cascada. El presente proyecto se estructurará en seis capítulos:

- Capítulo 1: Introducción y planificación.
  Este capítulo consiste en una introducción sobre los objetivos del proyecto y en una presentación de la motivación que conduce a su desarrollo. Se definen los objetivos y se establece la planificación y ejecución del proyecto, incluyendo el cronograma de actividades.

- Capítulo 2: Investigación sobre Ciberinteligencia y OSINT.
  Este capítulo tiene un fundamento puramente teórico. En él se realiza una investigación sobre conceptos básicos de la OSINT para, en el capítulo siguiente, realizar una puesta en común de los mismos y conectarlos con las consecuencias en el uso diario que hacen las personas de internet.

- Capítulo 3: Exposición de resultados.
  A partir de los resultados obtenidos en el capítulo anterior, se va a realizar una exposición y una elección de herramientas de software para realizar el caso de estudio que está previsto en el apartado siguiente.

- Capítulo 4: Casos de estudio sobre OSINT.
  En este capítulo se elegirán sujetos de estudio cuyos datos serán ocultados y se les realizará un estudio de ciberinteligencia a partir de las herramientas halladas en los capítulos anteriores. Se pretende que el procedimiento sea sencillo y realizable por cualquier persona con un mínimo de conocimientos de informática. El objetivo de este apartado es que dicho estudio se lo realice el sujeto a sí mismo para conocer el nivel de salud de sus datos personales en la red.

- Capítulo 5: Conclusiones y trabajos futuros.
  En este capítulo se realizará un análisis de los resultados obtenidos, de las dificultades encontradas durante el desarrollo del proyecto y de los plazos establecidos en la planificación inicial.

- Capítulo 6: Glosario.
  En este capítulo se definirán los diversos términos técnicos a los que se hará referencia a lo largo del trabajo.

- Capítulo 7: Anexos.
  Otra información de interés que se ha utilizado para la realización del presente trabajo y, que por su extensión o su diversidad, no se ha considerado conveniente insertarla en el flujo continuo del trabajo.

- Capítulo 8: Bibliografía.
  Relación de fuentes utilizadas para la redacción del presente trabajo.

Capítulo 2

Investigación sobre ciberinteligencia y OSINT

2.1. Introducción al análisis de inteligencia

En este capítulo se va a tratar de exponer el valor real de la inteligencia en general y la ciberinteligencia en particular, el cual va más allá de la simple tarea de recopilar datos, estructurarlos y redifundirlos. Se trata de un proceso que aporta más que un simple resumen que haya pasado ya por los pasos anteriores y se haya distribuido a la persona adecuada en el momento adecuado para que tome la decisión correcta. Esto es lo mínimo esperable de todo el proceso y, sin embargo, no es ni el fin ni su valor máximo. Se va a tratar de poner esta disciplina en contexto de la mejor manera posible y decir qué es y qué no es. El simple hecho de dar a conocer el concepto ya puede generar interés por parte del lector y justificar este TFG que, en definitiva es de investigación.

Aunque la ciberinteligencia o inteligencia de fuentes abiertas no son términos tan extendidos como podrían ser los ciberataques, el phishing o similares, lo cierto es que, no se trata de un término reciente [19]. De hecho, el glosario de inteligencia editado en 2007 por el Ministerio de Defensa define OSINT como un concepto que trasciende mucho más allá de la tecnología y, como se verá a continuación, se trata del «tipo de inteligencia elaborada a partir de información que se obtiene de fuentes de información de carácter público». A partir de la definición usada por parte del Ejército de Tierra español, en él se define ciberinteligencia como «la inteligencia obtenida del análisis de

la información referente al ciberespacio». Asimismo, también hay que definir tres puntos a los que se dará un uso intensivo durante todo el trabajo y que están íntimamente relacionados con la misma.

- Ciberespacio. Se define como el sistema compuesto por infraestructuras de tecnología de la información, incluyendo internet, redes de telecomunicaciones y sistemas de información.
- Ciberseguridad. Conjunto de actividades dirigidas a proteger el ciberespacio contra el uso malicioso del mismo y en el mismo, y defendiendo la infraestructura tecnológica que lo compone, los servicios que presta y la información que maneja. El Centro Criptológico Nacional la define como la habilidad de proteger y defender las redes de los ciberataques.
- Ciberataque. Acción maliciosa y producida en el ciberespacio para comprometer la disponibilidad, integridad y confidencialidad de la información existente, mediante el acceso no autorizado, la modificación, la degradación o la destrucción de los sistemas de información y telecomunicaciones o las infraestructuras que lo soportan.

Sin embargo, España no es ni mucho menos pionera en este campo [20]. La vecina Francia es toda una referencia a nivel mundial y, según los postulados de Henry Martre (que fue el autor del primer informe sobre inteligencia económica y competitiva en Francia), es «el conjunto coordinado de acciones de búsqueda, tratamiento y distribución con el objetivo de ser utilizada para la toma de decisiones de información útil para los actores económicos». Estas acciones se llevan a cabo con todas las garantías legales y éticas, así como con las máximas garantías de protección y preservación del patrimonio empresarial y en las mejores condiciones de tiempo de entrega y coste de elaboración.

En el día a día no se utiliza el término inteligencia de forma correcta. Tomando como referencia el glosario de inteligencia del Ministerio de Defensa español [21], la definición de inteligencia sería el «producto que resulta de la evaluación, integración, el análisis y la interpretación de la información reunida por un servicio de inteligencia». La elaboración de dicho producto procedería de lo que se conoce como ciclo de inteligencia.

Debido a esto, puede afirmarse que es un error utilizar información como sinónimo de inteligencia ya que, la información sería la materia prima de esta primera. Tampoco

sería correcto utilizar el término espionaje como sustituto de inteligencia ya que este se refiere a todos aquellos medios utilizados para la obtención de información a través de medios clandestinos. Independientemente de la utilización o no de los citados medios, la comparación no es del todo exacta cuando se hace referencia al análisis de la inteligencia.

Habiendo dejado claras las definiciones clásicas de inteligencia, no hay que olvidar que lo realmente importante es el contexto y el momento puesto que, es de suma importancia saber quién necesita el análisis de inteligencia y en qué momento se ha realizado. Aunque no son totalmente imprescindibles de cara al desarrollo del presente trabajo, sí se han considerado necesarias para conocer La diferencia entre los conceptos que se van a utilizar de forma habitual durante todo el desarrollo de este TFG.

2.2. El ciclo de inteligencia clásico

El producto conocido como inteligencia viene de un proceso que se conoce como ciclo de inteligencia clásico el cual fue diseñado por la OTAN y está formado por cuatro fases bien diferenciadas [22], las cuales son: dirección, recolección, procesamiento y difusión.

Figura 2.1: El ciclo de inteligencia clásico [22]

1. La fase de dirección sería la primera parte del ciclo y consistiría en determinar las necesidades de inteligencia, tanto humanas como técnicas, así como planificar las acciones a emprender para conseguirlas. De cara optimizar la planificación de las

acciones, se dividen los requerimientos de inteligencia en generales y específicos. De esta forma, es posible determinar las necesidades reales y las acciones a llevar a cabo para conseguirlas. El plan y los recursos deben revisarse al finalizar cada fase del ciclo en aras de determinar si han surgido nuevas necesidades que deberán tenerse en cuenta a futuro.

2. La segunda fase, conocida como fase de obtención, consistiría en la recolección de datos a través de una variedad de medios y fuentes que van a constituir la base informativa a partir de la cual se generará el nuevo conocimiento. Como ya se ha dicho, el origen de las fuentes de información puede ser muy variado y puede dar lugar a diversos tipos de inteligencia. Tomando como referencia las definiciones del glosario de inteligencia del Ministerio de Defensa, las más conocidas son las siguientes.

   a) Inteligencia de fuentes abiertas (OSINT). Este tipo de inteligencia cobra con el paso de los años una mayor relevancia si procede de información obtenida de fuentes públicas, independientemente de que el contenido sea comercializado, gratuito, o a través de canales restringidos. No necesariamente tiene que tratarse de contenido digital pero, en cualquier caso, debe estar a disposición del público. A tal efecto, las fuentes de información documental abiertas pueden ser enciclopedias, publicaciones científicas y un largo etcétera, así como podcast, fotografías o audiovisuales de cualquier tipo.

   b) Inteligencia de fuentes humanas (HUMINT). Este tipo de inteligencia es elaborada partiendo de información recogida o suministrada directamente por personas, lo cual es muy útil porque no es posible de adquirir por otros medios. Para obtener información a través de estas fuentes, es necesario llevar a cabo dos fases, las cuales son: la captación e infiltración de la fuente y la fase de evaluación de la información adquirida. Esto supone una importante dedicación de recursos para su posterior análisis por parte de analistas especializados en función de la naturaleza de la persona.

   c) Inteligencia de señales (SIGINT). En este caso se trata de inteligencia que implica un mayor número de recursos técnicos y que se elabora partiendo de la obtención y el procesamiento de datos procedentes de la detección, interceptación y descifrado de señales y transmisiones de cualquier tipo. Este tipo de inteligencia usualmente es competencia de un organismo especializado e independiente y no se puede considerar tan accesible como la OSINT

debido a la complicación técnica que lleva implícita. Sin embargo, esto no quita que con el paso del tiempo este tipo de información se desclasifique y pueda ser accedida, con lo cual se convertiría en OSINT. En definitiva, se trata de una capacidad sumamente importante que permite observar la actividad estratégica de un posible enemigo mediante el contenido y el patrón de la señal, brindando información para ser interpretada.

d) Inteligencia de imágenes (IMINT). Si bien existen varias definiciones relativas a la inteligencia de imágenes [23], de forma generalizada podría definirse como la información técnica, geográfica y de inteligencia obtenida a través de la interpretación o análisis de imágenes adquiridas por sensores y de material colateral. Ya sea en un plano político, económico o militar, la obtención de imágenes ha sido y es vital para la toma de decisiones. En definitiva, la necesidad de conocer el entorno, las actividades que se desarrollan en un área concreta y la situación de las partes en un conflicto, ha sido una constante a lo largo de la historia de la humanidad. Sin embargo, en el ámbito de aplicación del presente trabajo, la inteligencia de imágenes cobrará un carácter no tan relacionado con lo político o militar sino más bien en el entorno del individuo.

e) Inteligencia de medición y firma (MASINT). Esta rama técnica de la búsqueda de información es utilizada para detectar, seguir, identificar o describir los rasgos característicos o firmas de objetivos fijos o dinámicos [24]. Esta disciplina incluye habitualmente inteligencia de radar, acústica, nuclear, química o biológica. La MASINT se define como una inteligencia técnica y científica derivada del análisis de los datos obtenidos de instrumentos de detección con el propósito de identificar cualquier característica distintiva asociada con la fuente emisora o receptora para facilitar la identificación y medida por parte de la segunda. Como es de esperar, este tipo de inteligencia suele quedar totalmente fuera del alcance y, al igual que la IMINT está reservada para el uso por parte de gobiernos o entidades de gran relevancia.

f) Inteligencia de la electrónica (ELINT). Este tipo de inteligencia se basa en la adquisición de información por medios electrónicos y, los datos normalmente obtenidos, son los de los sistemas de defensa del rival [25]. Se trata de un tipo de inteligencia muy especifico ya que su objetivo principal es conocer las ubicaciones de sistemas de misiles tierra-aire, aeronaves etc.

g) Inteligencia geoespacial (GEOINT). La inteligencia geoespacial tiene por función la explotación y análisis de imágenes, señales o firmas con información geoespacial [26]. Su fin último es describir y visualizar características geográficas referenciadas en la tierra. También se conoce como inteligencia posicional.

h) Inteligencia estratégica (STRATINT). La inteligencia estratégica [27] se encarga de la recolección, procesamiento, análisis y diseminación de la inteligencia que se requiere para formar planes militares a nivel nacional e internacional. Mucha de esta información procede de la OSINT.

i) Inteligencia financiera (FININT). Este tipo de inteligencia implica el análisis de un gran volumen de datos de transacciones normalmente proporcionados por bancos y otras entidades como parte de requisitos regulatorios. De forma alternativa, las técnicas de minería de datos se pueden utilizar para identificar personas potencialmente implicadas en una actividad concreta. Algunos países industrializados tienen requisitos regulatorios para sus organizaciones financieras. Desde un punto de vista legal puede ser posible para algunas entidades de inteligencia el acceso libre a los datos en bruto.

j) Inteligencia de rumores (RUMINT). Tan importante es conocer lo que es cierto como lo que es falso y, es este tipo de inteligencia la que se encarga de esto. Así pues, en palabras más formales la inteligencia de rumores se encarga de confirmar la veracidad de los datos circulantes.

k) Inteligencia de redes sociales (SOCMINT). Este tipo de inteligencia se refiere a la información que puede encontrarse en las redes sociales. Los recursos disponibles en estos sitios pueden ser públicos –como por ejemplo posts de Facebook– o privados. La información privada no se puede acceder sin los permisos oportunos; por ejemplo, los mensajes privados o los posts compartidos con amigos. Aunque la mayoría de las redes sociales requieren que sus usuarios se registren antes de acceder a la totalidad de sus contenidos, algunas encuestas muestran que los usuarios de las redes sociales esperan tener algún tipo de privacidad sobre sus actividades online aunque las publiquen de forma pública [28]. Sin embargo, los expertos en seguridad generalmente consideran la información compartida en las redes sociales como OSINT directamente porque, en definitiva, se trata de información pública compartida en un dominio público y, por tanto, puede ser explotada para

fines varios.

3. La tercera fase del ciclo inteligencia clásico sería la de procesamiento y explotación intelectual de la información. Para garantizar el éxito de la información que se ha recibido en esta fase, esta debe de haber sido interpretada y evaluada adecuadamente durante la fase anterior. Es en esta fase donde debe establecerse un criterio lógico que permita al analista de inteligencia un desarrollo optimizado de la siguiente fase. Se debe considerar que la información debe ser analizada desde distintas perspectivas y, por regla general, será de carácter muy heterogénea pudiendo estar estructurada o no, y pudiendo estar en formato físico, digital, e incluso estar ordenada cronológicamente, en distintos idiomas y un largo etcétera. Es fundamental que, en esta fase el analista de inteligencia no tenga que dedicar su tiempo rebuscando entre toda la información disponible para poner en conjunto todas las piezas de información que se le han aportado puesto que, el tiempo dedicado a esta labor por parte del mismo es muy valioso.

4. La cuarta y última fase sería la de diseminación en la cual, la información se pone a disposición de aquella persona que debe tomar las decisiones a través de su uso. Normalmente esto se hace a través de un informe de inteligencia. Esta fase no termina simplemente con la comunicación a los usuarios sino que requiere el retorno de las decisiones tomadas a los analistas con la finalidad de que incorporen ese conocimiento adquirido al proceso para su paulatina mejora.

Este proceso no es cerrado, sino cíclico, iterativo y se produce una realimentación a partir de la cual se puede dar lugar a futuras necesidades de información y actualizaciones de informes ya entregados; en definitiva, se trata de un proceso vivo [8].

2.2.1. El plan de inteligencia

Como se ha ido adelantando, todo el método de ciberinteligencia no deja de estar basado en el ciclo de inteligencia, por tanto, su objetivo final es la producción de conocimiento activable orientado para tomar decisiones, sin embargo, se basa en gran medida en un producto mínimo que es el informe de inteligencia. Así pues, la elaboración de estos informes está comprendida por las siguientes fases:

- Definición de las necesidades de información para los usuarios internos, tanto para informar como para actuar.

- Plan de inteligencia.

- Configuración de las herramientas y extracción de la información.
- Análisis de la información para la elaboración de informes o alertas y entrega de estos.
- Utilización y evaluación de los informes.

El hecho de elaborar un plan de inteligencia es fundamental de cara a optimizar los recursos de que se dispone, evitando solapamientos y problemas de carga de trabajo desigual para los analistas. Si se pretende elaborar con éxito un plan de inteligencia, en primer lugar hay que plantearse una serie de cuestiones:

1. ¿Qué es lo que se sabe seguro? Esta pregunta está ligada a la gestión del conocimiento, a los históricos de análisis y a los repositorios existentes. Normalmente se debe de poder responder mediante un documento en el que esté recogido todo aquello que se pueda aportar de forma previa al análisis. No es necesario que sea oficial o explícito; la experiencia previa juega un papel importante de cara a resolver esta cuestión.
2. ¿Qué es lo que no se sabe y se quiere conocer? Se trata de una pregunta muy importante; de hecho, se trata de la razón de ser del proceso mismo de inteligencia.
3. ¿Qué se conoce pero no se ha tenido en cuenta? Para responder a esta cuestión debe hacerse una recopilación de toda aquella información que pueda poseerse y en la que no se había caído que se tenía. El hecho de conocerla de antemano puede reducir el coste de las dos etapas anteriores y agilizar el trabajo. En definitiva, conocer quién puede ser el sabedor de la información que no se conoce.
4. ¿Qué es lo que no se conoce en absoluto? Este es el punto más crítico, porque se pueden dar muchas posibilidades y es posible que no se adopten objetivos previos porque no se conozca que tengan que adoptarse.

Esta exposición teórica del plan de inteligencia está más bien pensada para grandes o no tan grandes organizaciones en las que existe un departamento o, como mínimo, un empleado dedicado a labores de inteligencia. Evidentemente no está tan orientada para el nivel de un usuario particular, ya sea académico o no, pero es importante conocer el fundamento teórico para tener una mínima referencia a la hora de trazar un plan de acción basado en una metodología estandarizada.

En el caso concreto de este TFG, el plan de inteligencia es bastante sencillo, y pue-

de asimilarse a una investigación de recopilación de información en fuentes abiertas sobre personas. Este proceso se simplificará todavía más si cabe, teniendo en cuenta que siempre van a tenerse uno o más datos de partida, puesto que la investigación será realizada sobre el propio usuario. El producto que se quiere obtener es la máxima información que se pueda haber exfiltrado a las redes para tomar las acciones que se consideren oportunas.

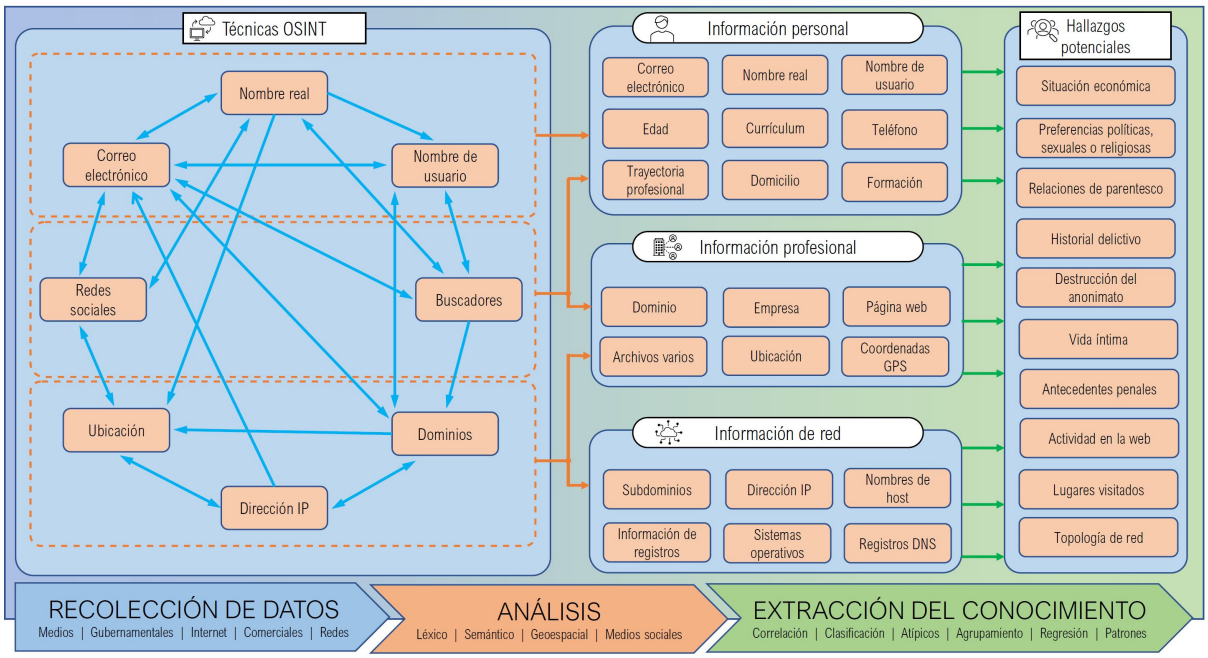

Figura 2.2: Principales flujos de trabajo en ciberinteligencia [5]

En la etapa de recolección de datos se podrán evitar las búsquedas del nombre real, correo electrónico o nombres de usuario puesto que, al ser propios, se conocerán de antemano. Podría darse el caso de que se haya olvidado alguna web en la que se haya estado registrado hace tiempo; esto no va a ser problema, porque en esta situación las técnicas de análisis también las revelarán.

2.2.2. El pensamiento del analista de inteligencia

Un analista debe tener una forma de pensar acorde al valor real de la inteligencia; puesto que éste es quien la produce, su valor estará íntimamente relacionado con ella [20]. Es conocido que el cerebro humano suele funcionar en base a la ley del mínimo esfuerzo o de economía de energía, lo cual significa que ante una situación dada intentará evitar el coste que supone analizarla para centrarse en tareas más importantes. Esto es

algo que el analista de información no puede permitirse y puede conllevar errores de apreciación inherentes a los humanos a la hora de apreciar la pertinencia de una fuente y de analizar su información. Se trata de errores involuntarios, es decir, una suerte de atajos a la hora de procesar la información y son conocidos como sesgos cognitivos. Sin entrar en demasiados detalles, una breve relación de estos sesgos cognitivos [29] seria la siguiente:

- Sesgo de Confirmación. Se trata de una tendencia natural del ser humano a favorecer toda información que confirme sus propias hipótesis sin tener en cuenta la procedencia por el contenido de la misma.
- Sesgo de punto ciego. Sería el opuesto al punto anterior, es decir, la tendencia a no darse cuenta de los propios prejuicios cognitivos o a verse como menos influido por ellos que los demás.
- Efecto del falso consenso. Se trata de un hecho comprobado que la mayoría de las personas juzgan que sus propios hábitos, valores y creencias son más comunes de lo que son en realidad.
- Efecto de percepción ambiental. Factores como el sesgo cultural y de educación producen una gran influencia en el comportamiento de los individuos.
- Efecto de arrastre. Consiste en pensar que algo es correcto porque muchas personas así lo creen.
- Efectos de encuadre. Se trata de una alteración de la percepción en función de cómo se presente la información para tomar la misma decisión. Esto tiene mucho que ver con la decisión que vaya a tomarse dependiendo de si esta está centrada en conceptos positivos o negativos incluso si la información es la misma.
- Sesgo de distinción. Se trata de ver varias opciones como más dispares cuando se las evalúa simultáneamente que cuando se las evalúa de forma individual. Este sesgo es especialmente dañino, ya que si se evalúan dos cosas de forma consecutiva se puede pensar que tienen una relación causal cuando pueden no tenerla.
- Efecto de cesión. Se trata de una tendencia de las personas a dar valor a las cosas o situaciones en cuanto llegan a poseerlas. Es decir, por el mero hecho de haber obtenido cierta información con una mayor o menor dificultad, automáticamente se revaloriza pudiendo llegar a tener un valor superior al real.

- Sesgo de pseudocerteza. Se trata de la tendencia natural a evitar tomar decisiones arriesgadas si los resultados esperados son negativos y, como contrapartida, ser excesivamente confiado a tomar decisiones arriesgadas en caso contrario.

- Heurística de disponibilidad. Este sesgo empuja a utilizar el dato más disponible o reciente como elemento clave de análisis y decisión. Puede llegar a hacer que todo parezca que forma parte de un plan preconcebido y coincidente. De este modo se podría incluso llegar a pensar que ya no es necesario continuar con la búsqueda de nueva información. Como puede verse, puede llegar a tener un impacto muy negativo.

- Relaciones espurias. Es una relación en la cual dos acontecimientos no tienen conexión lógica aunque pueden implicar que la tienen debido a un tercer factor no considerado aún.

Otros aspectos relacionados con los sesgos de la cognición son las falacias [30] o razonamientos incorrectos que parecen ser correctos; también son resultados de sesgos cognitivos. Por mencionar solo unos pocos, se tendrían los siguientes:

- Falacia del centro de atención. Se produce cuando una persona da por sentado que todos los miembros o ejemplos pertenecientes a un mismo grupo, clase o tipología son como una muestra de un grupo mucho mayor.

- Falacia de validación personal. Se da cuando los individuos dan altos índices de acierto a descripciones de algo que les atañe y que supuestamente se adapta específicamente para ellos, pero en realidad son vagas y lo suficientemente genéricas como para aplicarse a una amplia gama de personas.

- Falacia arreglo de bulto. Consiste en asumir como obvio que las personas que han sido agrupadas por tradición o cultura son entendidas de forma que deben seguir siendo tratadas así.

- Falacia del francotirador tejano. Consiste en emitir suposiciones y hacerlas cuadrar con los datos. Esta falacia se llama así porque toma la imagen de un tirador que dispara al azar y luego coloca los impactos en el centro de las dianas.

- Falacia por asociación. Es un tipo de falacia lógica en la que las características de una persona o de algo, lo son también de otra persona o cosa similar simplemente por asociación.

- Probar con el ejemplo. Esta falacia sostiene que una teoría es cierta porque algunos ejemplos la prueban. También se conoce como generalización apresurada.
- Falacia de apelación a la autoridad. Sostiene que un argumento es válido porque lo defiende una autoridad o un experto.
- Falacia ad nauseam. Utiliza la repetición para autoafirmarse; una premisa acaba siendo cierta porque se ha oído en multitud de ocasiones. En esta falacia encuentran soporte los mitos urbanos y la eficacia de algunas publicidades repetitivas.

2.2.3. El perfil del analista

Cuando se habla de este perfil, se hace referencia a personas altamente especializadas, de manera que sus conocimientos estén centrados en labores muy concretas, para así no verse condicionados por otro tipo de información o, lo que podría llamarse ruido de la información. En términos generales, las características que debe tener un analista de inteligencia o ciberinteligencia serían:

- Minuciosidad en ese trabajo concreto y capacidad de analizar con la misma calidad desde la primera hasta la última información obtenida sin tomar atajos.
- Afán de mejora continua y curiosidad por profundizar en las temáticas que va a perseguir.
- Capacidad de análisis y facilidad para poner en contexto toda la información recibida así como poder plasmar ideas complejas de forma sintetizada.
- Capacidad de comprender una problemática dentro de su contexto para poder adecuar el análisis a la necesidad de forma que se pueda dar respuesta únicamente a lo necesario.
- Persona con una gran intuición y con facilidad para contribuir a la toma de requerimientos.
- Conocimiento profundo tanto de los sesgos cognitivos propios como de los ajenos en la medida de lo posible.
- Adaptabilidad y resiliencia a los cambios puesto que, el crecimiento de la web produce nuevas maneras de interactuar con el entorno y estar actualizando los conocimientos de forma continua conforme van naciendo nuevas tecnologías.

2.2.4. La OSINT

Poniendo el foco ahora en el caso concreto de la OSINT, su uso está ampliamente adoptado por gobiernos y servicios de inteligencia [31] para dirigir sus investigaciones y luchar contra el cibercrimen [5]. Por poner varios ejemplos, sería posible obtener mensajes, interacciones y preferencias procedentes de las redes sociales para llevar a cabo análisis de opinión pública. Asimismo, también sería posible analizar datos de fuentes abiertas para la detección y alerta temprana de ataques terroristas, lo cual supone una importante ventaja en la lucha terrorista, sea esta a través de la red o en las calles.

Lamentablemente, estos datos también pueden ser utilizados por parte de los grupos ciberterroristas para llevar a cabo acciones ilegales y, por tanto, hacer uso de los mismos con fines deshonestos. De sobra es conocido a través de los medios que las filtraciones de datos en portales o páginas web cada día más importantes están prácticamente a la orden del día en mayor o menor medida.

También es importante saber que la OSINT puede ser utilizada en otros contextos tales como los ataques de ingeniería social o campañas de marketing que, en ocasiones rozan el límite de lo que se puede considerar de interés para el cliente. Asimismo, prácticas como el ciberacoso o el ciberbullying quedarían englobadas también dentro de lo que puede considerarse un uso malicioso de la información procedente de fuentes abiertas.

2.3. La calidad de la información procedente de fuentes públicas

Como es de suponer, no toda la información procedente de fuentes abiertas es fiable [32]. De hecho, la desinformación es una herramienta de desestabilización según el Centro Criptológico Nacional, el cuál, en su informe CCN-CERT BP/13 [33] sobre desinformación en el ciberespacio, afirma que las noticias falsas y la desinformación han cobrado una importancia capital a la hora de minar la cohesión interna de un estado o grupo de estados considerados como adversarios. Las principales características de estas campañas de desinformación son las siguientes:

1. Alto nivel de efectividad. La revolución tecnológica ha permitido democratizar el acceso a los medios y a la tecnología de producción de mensajes informativos.

De este modo, resulta barato y sencillo producir contenido a través de internet con una elevada calidad técnica y difundirlo de manera directa y eficaz a las audiencias que se consideran más adecuadas para recibirlos. Así pues, con unos recursos objetivamente humildes es posible la difusión masiva de imágenes retocadas o noticias falsas.

2. Dificultad para establecer una atribución directa. Debido a la facilidad para conseguir un anonimato suficiente en las redes sociales, es posible que actores anónimos puedan influir de forma maliciosa en el condicionamiento de la opinión pública. El uso de redes VPN y de herramientas que antaño únicamente estaban al alcance de algunos servicios de inteligencia, hoy están a disposición del gran público. Tan solo es necesaria una –relativamente breve– formación en plataformas de contenido tales como YouTube para obtener unos conocimientos aceptables.

3. Compleja regulación. En contraposición con otras acciones ofensivas como la guerra abierta en un campo de batalla o las acciones terroristas, las acciones de desinformación y de manipulación de opinión pública no son fáciles de combatir desde la perspectiva legal propia de las democracias liberales. Esto se debe a que, la libertad de expresión y de opinión son principios fundamentales en un estado democrático y, en muchos casos no es posible limitar estos derechos. En definitiva, no es un delito crear una cuenta en una red social que difunda información no contrastada. La suma de todos estos factores supone una enorme dificultad para luchar contra estas fuentes si son muy numerosas tal como es el caso hoy en día.

4. Limitación para establecer una relación de causalidad. Si bien las metodologías actuales permiten detectar intentos de desinformación y atribuirlos con menor o mayor grado de certeza, es muy difícil poder probar una relación de causa-efecto como resultado de dichos intentos.

5. Aprovechamiento de vulnerabilidades ya existentes. No sería tanta la efectividad de las campañas de desinformación sí estas tuvieran que iniciarse desde cero. Así pues, el primer paso de las mismas es la detección de vulnerabilidades sociales y políticas ya existentes con el objetivo de aumentar y polarizar ese debate.

6. Infiltración de la desinformación ilegítima en los medios de la comunicación social y política legítimos. En ocasiones las acciones de desinformación ilegítima proceden de actores interesados en influir en la audiencia ciudadana de modo

que estos pueden difundir sitios, mensajes y contenidos. De este modo, pueden darse conversaciones cruzadas con miles de actores en redes sociales sobre temas polémicos de los cuales no son totalmente conocedores.

De dicho informe se desprende también que, la nada despreciable cantidad de más de 20 millones de ciudadanos españoles están en riesgo de ser víctimas de la desinformación. Así pues, queda ya reconocida oficialmente la amenaza que suponen para la seguridad nacional las campañas de desinformación.

Las consecuencias de sufrir un ataque de desinformación son, entre otras, la pérdida de confianza en los medios de comunicación tradicionales así como un aumento creciente de la preocupación por no saber diferenciar entre lo que es cierto y falso en internet. De igual modo, un daño colateral de estos ataques de desinformación sería también la pérdida de confianza en las instituciones públicas la cual está cayendo a mínimos históricos debido a la crisis social actual [34].

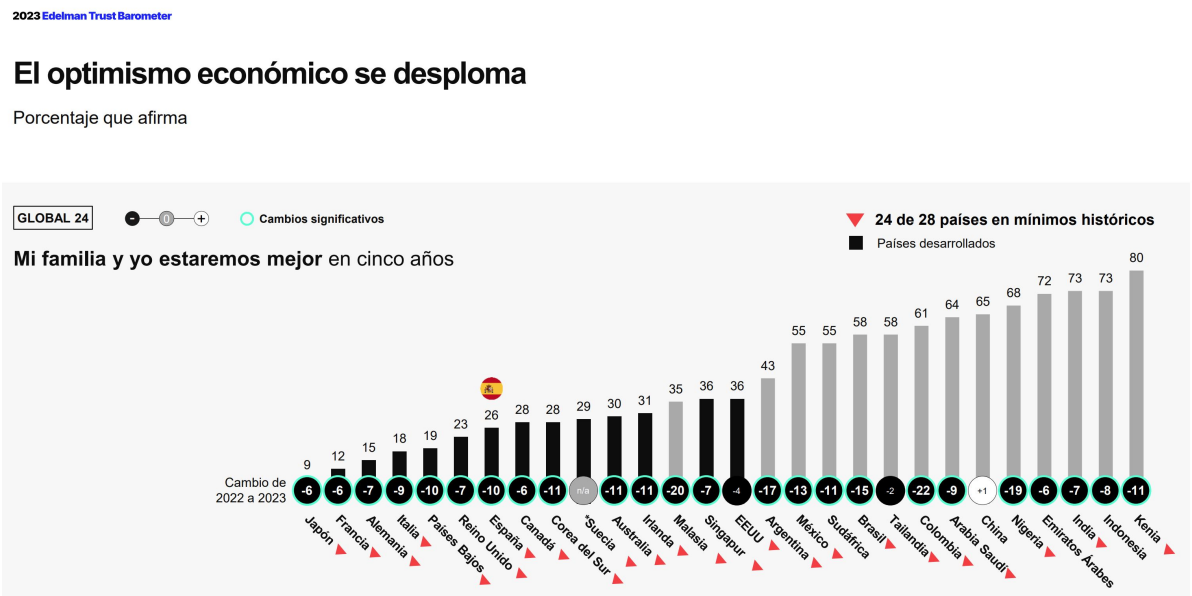

Figura 2.3: Edelman Trust Barometer 2023 [34]

En el caso concreto de las fake news, que son mensajes informativos que se difunden a la opinión pública y que no se corresponden con ningún hecho verdadero o demostrable, científica o históricamente, pueden ser aceptadas como creíbles por un amplio número de ciudadanos y provocar graves crisis políticas y de seguridad en un estado. Su riesgo es tan elevado porque, si bien son falsas, están basadas en elementos

verdaderos, resultan sorprendentes y, al repetirse de forma reiterada se corre el riesgo de que se acepten como ciertas a pesar de que provienen de medios de reciente creación, escasa trazabilidad y no disponen de fuentes fiables o reconocidas.

En definitiva, los ataques de desinformación persiguen minar la confianza del ciudadano en la esencia de la información como elemento de decisión democrática, con lo cual, también se pierde el valor añadido de que el ciudadano mejor informado será capaz de tomar las mejores decisiones para su gobernanza.

2.4. Fiabilidad y evaluación de la información procedente de fuentes públicas

Con todo lo expuesto en el punto anterior, es de prever que no resulta sencillo contrastar y evaluar la fiabilidad de las fuentes a partir de las cuales se van a realizar los estudios de OSINT [35]. Sin embargo existen –para el caso de algunos organismos tales como el Ejército de los Estados Unidos– sistemas de evaluación sobre la fiabilidad de las fuentes de información [36] tal como se explica en el apéndice B del manual FM 2-22.3 de la US Army. A partir de ellos, es posible valorar de la forma más aproximada posible la fiabilidad de la información que se tiene entre manos. Como puede verse, no se trata en absoluto de un método cuantitativo, sino más bien cualitativo y aproximado.

Utilizando las tablas 2.1 y 2.2 y combinando los dos términos, si se realiza la combinación A6, significaría que la fiabilidad de la fuente sería totalmente auténtica con un historial intachable de fiabilidad pero que en ese caso, al estar seguido de un 6 no tendría por qué significar que la información fuera falsa, sino que, al ser nueva no es posible realizar una evaluación de validez.

Algunos procesadores de lenguaje natural basados en la inteligencia artificial tales como ChatGPT han demostrado excelentes capacidades a la hora de establecer la credibilidad de las fuentes de noticias [37], sin embargo, todavía están en fase experimental.

A día de hoy, uno de los portales de internet que goza de mayor prestigio a la hora de calificar la fiabilidad de las fuentes de noticias es MBFC[1]. Dicha organización es independiente y califica para todos los países del mundo la fiabilidad de fuentes de información mediante un método sencillo y directo: en primer lugar, el uso del lenguaje y de los titulares, seguidamente la facilidad para encontrar la fuente de la noticia, en

[1]https://mediabiasfactcheck.com/

A	**Fiable**	**No hay duda** de la autenticidad, confiabilidad o competencia; dispone de un historial de completa fiabilidad
B	**Normalmente fiable**	**Dudas menores** sobre la autenticidad, confiabilidad o competencia; tiene un historial de información válida la mayoría de las veces
C	**Razonablemente fiable**	**Dudas** sobre la autenticidad, confiabilidad o competencia, pero ha proporcionado información válida alguna vez
D	**Habitualmente no fiable**	**Dudas significativas** sobre sobre la autenticidad, confiabilidad o competencia, pero ha proporcionado información válida alguna vez
E	**No fiable**	**Carente** de autenticidad, confiabilidad y competencia; historial de información no válida
F	**Indeterminada**	**No existen pruebas** para evaluar la fiabilidad de la fuente

Tabla 2.1: Evaluación de la fiabilidad de la fuente

1	**Confirmada**	**Confirmada** por otras fuentes independientes; **lógica** en sí misma y **consistente** con otra información sobre la materia
2	**Probablemente verdadera**	No confirmada pero **lógica** en sí misma y **consistente** con otra información sobre la materia
3	**Posiblemente verdadera**	No confirmada pero **razonablemente lógica** en sí misma y **en concordancia con alguna otra información** sobre la materia
4	**Dudosa**	No confirmada; posible pero **ilógica**; **no existe más información** sobre la materia
5	**Improbable**	No confirmada; **ilógica** en sí misma; **entra en contradicción** con otra información sobre la materia
6	**Indeterminada**	**No existen pruebas** para evaluar la validez de la información

Tabla 2.2: Evaluación del contenido de la información

tercer lugar la elección de historias y, por último, la filiación política [38].

2.4.1. El archivo de internet

El archivo de internet es una organización sin ánimo de lucro, la cual engloba gran cantidad de páginas web y otros artefactos como lo haría una biblioteca convencional, de forma que los investigadores, historiadores y estudiantes sin posibilidad de disponer de copias en papel pueden acceder a documentación de todo tipo [39].

Su origen se remonta a 1996 donde se empezó a archivar el propio internet en sí mismo: un medio de comunicación cuyo uso estaba en auge. Al contrario que con los periódicos, el contenido que se publicaba en internet era muy limitado y, además, no estaba siendo archivado. Gracias a Wayback Machine –qué es una especie de hemeroteca digital– se han archivado más de 26 años de historia de la red [40].

De este modo, el archivo de internet puede ser utilizado como una herramienta para determinar la calidad Y la fiabilidad de la información procedente de una página web consultando las diferentes capturas que se han ido realizando a lo largo del tiempo de la misma. Este proceso se llama crawling. Como contrapartida, no es una herramienta tan rápida como pudiera serlo Google u otros buscadores más conocidos, sin embargo, al ofrecer la posibilidad de consultar información que ya no está publicada o vigente, resulta de gran interés si se quiere consultar información que pudiera haber sido eliminada.

2.4.2. Procedimiento básico para detectar una noticia falsa

Como se ha indicado el principio de este punto, para hacer una valoración aproximada sobre la validez de la información, se podrían utilizar las tablas 2.1 y 2.2 aunque este sistema es bastante subjetivo. En la era digital en la que todo está conectado, existen sistemas más modernos tales como los que van a exponerse a continuación. En cualquier caso, no hay que confiar en la información que se publica en las redes sociales solamente; antes de valorar la fiabilidad de una noticia hay que aplicar el sentido común y realizar las siguientes comprobaciones previas:

1. Leer el artículo completo para empezar. No creerlo ciegamente antes de revisar su origen.

2. Revisar la fuente de información y, si es bien conocida y goza de buena reputación, ir a su página web directamente.

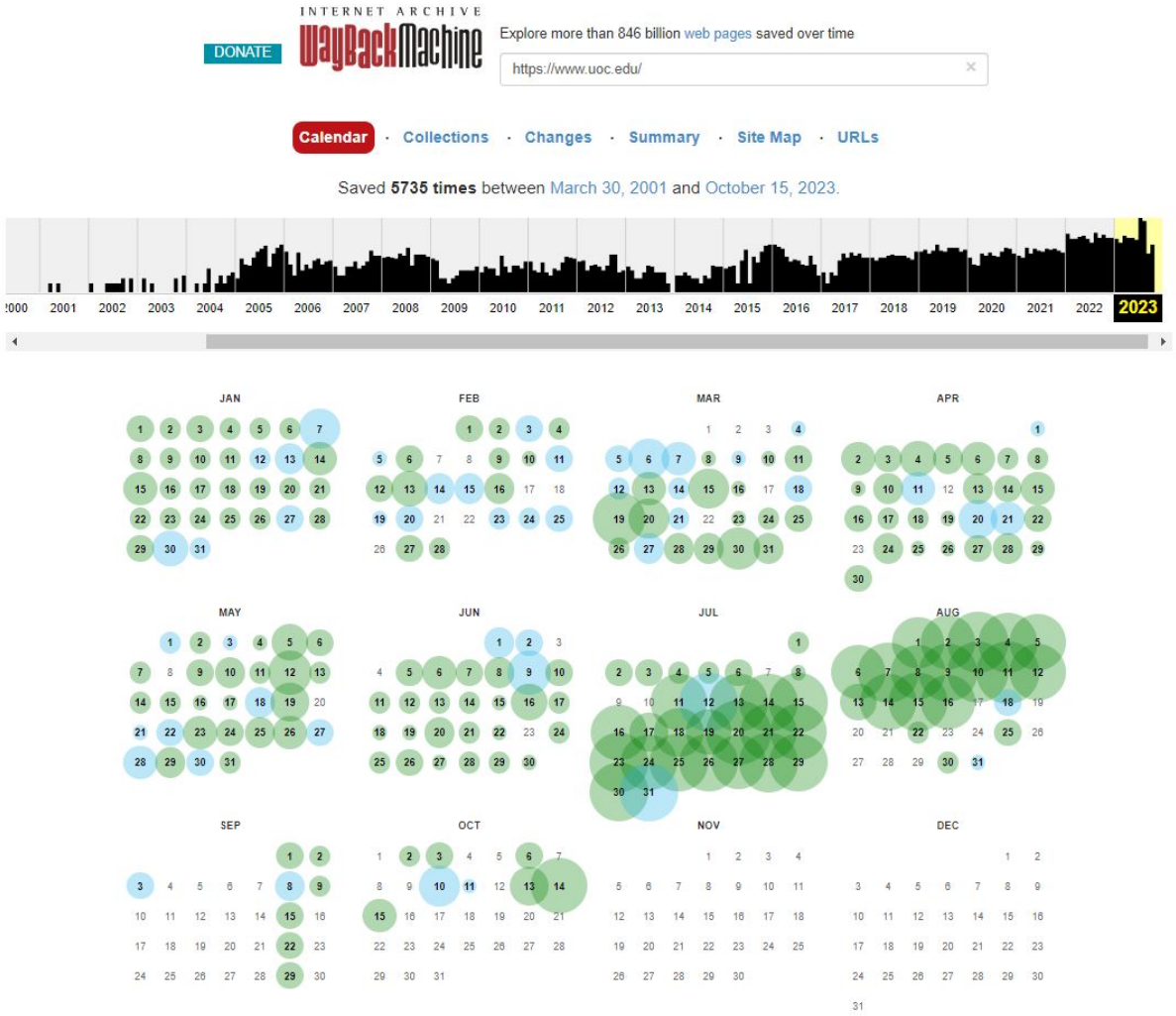

Figura 2.4: Crawling de la web de la UOC

3. Si la fuente de información es poco conocida va a ser necesario dirigir una búsqueda online para ver si alguien más ha publicado las mismas noticias.

4. Si una fuente de información reputada ha publicado la misma noticia, entonces muy probablemente será una historia verdadera.

5. En caso contrario, habrá que seguir investigando más sobre la materia o, directamente, considerarla como falsa.

2.4.3. Sitios para detección de información y noticias falsas

De todo lo que se ha comentado anteriormente, se derivan estos sitios online que ayudarán a detectar si alguna información encontrada en internet es cierta o falsa. A continuación, se incluye una breve lista de los más importantes:

- Snopes[2]. El cual permite descubrir noticias falsas, historias y leyendas urbanas así como investigar y validar rumores para decidir si son verdad.
- Hoaxy[3]. Comprueba la expansión de afirmaciones falsas a través de las redes sociales. Esta web deriva sus resultados a organizaciones reputadas para devolver los resultados más precisos.
- FactCheck[4]. La cual está asociada con Facebook para ayudar a identificar y etiquetar noticias falsas reportadas por sus usuarios. También monitoriza diferentes medios de comunicación en busca de información falsa cubriendo una gran cantidad de temas tales como salud, ciencia y bulos que se extienden a través de correos spam.
- Duke Reporter's Lab[5]. Ofrece un mapa global de sitios de comprobación de hechos.
- TruthorFiction?[6]. Descubre noticias falsas sobre diferentes temáticas tales como política, naturaleza, salud, espacio, crimen, policía, terrorismo, etcétera.
- Verification Handbook[7]. Se trata de la guía definitiva para verificar contenido digital respecto a la cobertura a emergencias y está disponible en diferentes idiomas.
- Verification Junkie[8]. Es un directorio de herramientas para verificar, comprobar hechos y decidir sobre la validez de los informes de testigos y contenido autopublicado por los usuarios en línea.
- Citizen Evidence Lab[9]. Tiene herramientas y tutoriales para enseñar a la gente

[2]https://www.snopes.com/
[3]https://hoaxy.osome.iu.edu/
[4]https://www.factcheck.org/
[5]https://reporterslab.org/
[6]https://www.truthorfiction.com/
[7]https://verificationhandbook.com/
[8]https://verificationjunkie.com/
[9]https://citizenevidence.org/

cómo verificar los contenidos online autogenerados por los usuarios. Está gestionado por Amnistía Internacional.

- InVID Verification Plugin[10]. Se trata de una herramienta que soporta tanto el navegador Mozilla Firefox como el Chrome. Está creada por el proyecto europeo InVID para ayudar a los periodistas a verificar el contenido en las redes sociales.

2.5. Los metadatos

Se podría definir metadatos como los datos que definen otros datos [41], si bien no se trata de una definición única. Su importancia radica en que, gracias a ellos es posible establecer una trazabilidad para conocer la evolución de un archivo o de una web a lo largo del tiempo. Esto, como se ha estudiado con anterioridad, cobra especial interés si se pretende conocer la evolución del contenido de un archivo o de una página web.

2.5.1. Identificación de formatos de archivos

En general se conoce como en el formato de un fichero la extensión que tiene al final, por ejemplo .txt o .jpg sin embargo, detrás de todo esto existe un concepto llamado «número mágico» [42] en el campo de la informática que permite identificar de forma inequívoca el tipo del archivo. La funcionalidad de este número puede ser de gran utilidad en caso de recibir un archivo cuya extensión ha sido modificada intencionadamente; pero aún así sería posible conocer su extensión original y su tipología mediante el uso del siguiente comando.

```
$ hexdump -C logo-uoc.png | head
00000000  89 50 4e 47 0d 0a 1a 0a  00 00 00 0d 49 48 44 52  |.PNG........IHDR|
00000010  00 00 00 f5 00 00 00 b6  08 03 00 00 00 36 a3 3b  |.............6.;|
00000020  95 00 00 00 19 74 45 58  74 53 6f 66 74 77 61 72  |.....tEXtSoftwar|
00000030  65 00 41 64 6f 62 65 20  49 6d 61 67 65 52 65 61  |e.Adobe ImageRea|
00000040  64 79 71 c9 65 3c 00 00  03 22 69 54 58 74 58 4d  |dyq.e<...”iTXtXM|
00000050  4c 3a 63 6f 6d 2e 61 64  6f 62 65 2e 78 6d 70 00  |L:com.adobe.xmp.|
00000060  00 00 00 00 3c 3f 78 70  61 63 6b 65 74 20 62 65  |....<?xpacket be|
00000070  67 69 6e 3d 22 ef bb bf  22 20 69 64 3d 22 57 35  |gin=”...” id=”W5|
00000080  4d 30 4d 70 43 65 68 69  48 7a 72 65 53 7a 4e 54  |M0MpCehiHzreSzNT|
00000090  63 7a 6b 63 39 64 22 3f  3e 20 3c 78 3a 78 6d 70  |czkc9d”?> <x:xmp|
```

Efectivamente, en la primera línea se puede ver que la extensión del archivo es .PNG y, como puede verse a continuación, nada cambiaría aunque se modificara de

[10]https://www.invid-project.eu/tools-and-services/invid-verification-plugin/

forma intencionada su extensión.

```
hexdump -C logo-uoc.jpg | head
00000000  89 50 4e 47 0d 0a 1a 0a  00 00 00 0d 49 48 44 52  |.PNG........IHDR|
00000010  00 00 00 f5 00 00 00 b6  08 03 00 00 00 36 a3 3b  |.............6.;|
00000020  95 00 00 00 19 74 45 58  74 53 6f 66 74 77 61 72  |.....tEXtSoftwar|
00000030  65 00 41 64 6f 62 65 20  49 6d 61 67 65 52 65 61  |e.Adobe ImageRea|
00000040  64 79 71 c9 65 3c 00 00  03 22 69 54 58 74 58 4d  |dyq.e<..."iTXtXM|
00000050  4c 3a 63 6f 6d 2e 61 64  6f 62 65 2e 78 6d 70 00  |L:com.adobe.xmp.|
00000060  00 00 00 00 3c 3f 78 70  61 63 6b 65 74 20 62 65  |....<?xpacket be|
00000070  67 69 6e 3d 22 ef bb bf  22 20 69 64 3d 22 57 35  |gin="..." id="W5|
00000080  4d 30 4d 70 43 65 68 69  48 7a 72 65 53 7a 4e 54  |M0MpCehiHzreSzNT|
00000090  63 7a 6b 63 39 64 22 3f  3e 20 3c 78 3a 78 6d 70  |czkc9d"?> <x:xmp|
```

Para terminar con los ejemplos, a modo de curiosidad puede resultar interesante el conocer que, algunos archivos de texto de uso común en paquetes de procesamiento de texto, tienen extensiones distintas a su formato real. Para el caso concreto del formato .odt tendría, como puede verse, la cabecera de un archivo comprimido que se identifica por .PK y lo mismo ocurre con los ficheros .docx

```
hexdump -C file-sample_1MB.odt | head
00000000  50 4b 03 04 14 00 00 08  00 00 b4 65 10 4b 5e c6  |PK.........e.K^.|
00000010  32 0c 27 00 00 00 27 00  00 00 08 00 00 00 6d 69  |2.'...'.......mi|
00000020  6d 65 74 79 70 65 61 70  70 6c 69 63 61 74 69 6f  |metypeapplicatio|
00000030  6e 2f 76 6e 64 2e 6f 61  73 69 73 2e 6f 70 65 6e  |n/vnd.oasis.open|
00000040  64 6f 63 75 6d 65 6e 74  2e 74 65 78 74 50 4b 03  |document.textPK.|
00000050  04 14 00 00 08 00 00 b4  65 10 4b d7 e4 45 f2 2e  |........e.K..E..|
00000060  88 00 00 2e 88 00 00 18  00 00 00 54 68 75 6d 62  |...........Thumb|
00000070  6e 61 69 6c 73 2f 74 68  75 6d 62 6e 61 69 6c 2e  |nails/thumbnail.|
00000080  70 6e 67 89 50 4e 47 0d  0a 1a 0a 00 00 00 0d 49  |png.PNG........I|
00000090  48 44 52 00 00 00 b5 00  00 01 00 08 02 00 00 00  |HDR.............|
```

Si bien queda fuera del alcance de este trabajo el dar a conocer la totalidad de las firmas iniciales de todos los tipos de archivos, es posible conocerlas consultando en Wikipedia la web que se indica a continuación [43].

2.6. La importancia de la OSINT y sus fuentes

En este punto se tratará de explicar más concretamente cómo puede ayudar la OSINT a combatir los riesgos presentes en la red y utilizarla en beneficio propio, siempre con fines éticamente correctos. Como va a verse, se trata de una herramienta muy potente que, utilizada de forma correcta puede contribuir a la propia protección y, de forma incorrecta, a generar grandes problemas tanto a empresas como a particulares.

Como ya se ha dicho en algunas ocasiones, la OSINT es información de dominio público que puede ser utilizada con fines de inteligencia. Difiere ligeramente de lo que se llamaría OSINF en tanto en cuanto existe un analista detrás que pone la información en contexto [44]. Por ejemplo, si se dispone de una lista de direcciones IP que se ha reportado como parte de un incidente, utilizando la investigación OSINT, el analista puede interrelacionar las direcciones IP a una campaña conocida o actividad. Acto seguido, podrá saberse si se tratará de un ataque sofisticado o cibercrimen de bajo nivel.

Aunque muchas veces se pase por alto, es prácticamente seguro que, en más de una ocasión se han utilizado recursos que se pueden utilizar para investigaciones de OSINT y búsqueda de datos. Sin ir más lejos, Google puede ser uno de ellos, si bien existen plataformas más variadas y complejas tales como SpiderFoot, que serán anlizadas en detalle en el próximo capítulo. Puede resultar bastante desalentador en ocasiones comprender la extensión total de la información que puede encontrarse en internet de forma pública, sin embargo, este tipo de herramientas van a facilitar el trabajo sin ser necesario comprender totalmente su funcionamiento. A continuación, se va a presentar una breve relación de plataformas y medios de donde se pueden adquirir datos de fuentes abiertas para usos de ciberinteligencia.

2.6.1. Buscadores

Los buscadores o tales como Google, Yahoo! o Bing, por citar solo algunos, son herramientas básicas, muy conocidas y utilizadas extensamente en el campo de la OSINT. Su funcionamiento en pocas palabras se resume en que realizan búsquedas en formato texto en internet.

Si se tuviera que definir su uso en una palabra, esta sería sencillez; de hecho, podría afirmarse que, utilizándolos se estaría llevando a cabo la forma más simple de buscar información en fuentes abiertas. Su funcionamiento es bien conocido: estos buscadores disponen de un formulario en el que se introduce una solicitud en formato texto para que proporcionen información al respecto de lo que se está buscando. Los resultados normalmente suelen ser bastante buenos, sin embargo, el elevado número que se obtiene en ocasiones resulta contraproducente para la búsqueda que se está realizando.

Además de esto, hay que tener en cuenta que, los primeros resultados que se obtendrán son normalmente anuncios o posiciones por las que los propietarios de las páginas web han pagado por ocupar. A medida que se avanza en los resultados, pue-

den verse webs cuya popularidad o número de visitas es menor, pero esto no significa que deba ponerse en duda a priori su credibilidad. En el siguiente capítulo se verá el uso avanzado de estos buscadores para limitar los resultados obtenidos a aquellos que realmente interesan.

2.6.2. Plataformas de inteligencia contra amenazas o Threat Feeds

Probablemente el primer lugar al que recurrir para la localización de inteligencia serían las plataformas de inteligencia contra amenazas o Threat Feeds tales como Abuse.ch[11]. En ellas se centraliza una colección de datos de amenazas de numerosas fuentes y formatos proporcionados mediante crowdsourcing. Este tipo de plataformas están diseñadas de tal forma que los datos puedan ser presentados en un solo lugar y tengan formato comprensible y utilizable. Teniendo en cuenta que el volumen de posibles amenazas es enorme, gestionarlas todas por parte de una única entidad puede ser una labor inasumible en costes y personal. Para evitar que muchas de ellas queden ignoradas, se recurre a estas plataformas de uso gratuito y, mediante los datos contenidos en ellas, es posible programar soluciones de inteligencia contra amenazas o TIP (Threat Intelligence Platforms) [45] o SIEM (Security Information and Event Manager).

Como contrapartida, se debe tener en cuenta que existen riesgos de obtener falsos positivos o información incorrecta, puesto que, si bien es lo que se espera, no puede suponerse que toda la información que se haya introducido en estas plataformas sea correcta. Ante todo debe primar el sentido común y el uso crítico de la información que se obtiene así como de los riesgos asociados. También existen plataformas de inteligencia de pago que, en principio dan mejores resultados pero en ningún caso son inmunes a falsos positivos, por supuesto. No obstante, disponen de soporte técnico pero no se pueden considerar como OSINT. En definitiva, este tipo de fuentes pueden ser un buen punto de partida.

2.6.3. Plataformas de investigación

En el punto anterior se ha hablado sobre las TIP y cómo pueden ser utilizadas para la recolección de datos de amenazas desde las fuentes públicas. Algunas plataformas también ofrecen funciones más específicas de investigación contra las amenazas

[11] https://abuse.ch/

cibernéticas; algunas de ellas podrían ser VirusTotal[12], Any.run[13], Hybrid Analysis[14], URLScan[15] o Joe Sandbox[16], entre cuyas funciones están las de investigar archivos, dominios y direcciones IP y páginas web. Todas ellas tienen versiones gratuitas así como suscripciones de pago con funciones mejoradas y mejor compatibilidad. La gran ventaja de las plataformas de investigación es que proporcionan la información contextualizada y facilitan la puesta en común de los datos que, de otro modo, podrían resultar irrelevantes.

2.6.4. Redes sociales

Como se ha comentado al principio de este trabajo, la hiperconectividad es un hecho. Hoy en día existen mayores facilidades para conectarse a la red que nunca y portales como LinkedIn y X (hasta hace poco conocido como Twitter) pueden ser recursos excelentes para identificar riesgos cibernéticos y realizar investigaciones. En el caso particular de X, se trata de un recurso excelente para encontrar nuevas variantes de malware, indicadores de compromiso [46] o TTPs (Tácticas, Técnicas y Procedimientos) [47]. A través de ambos, es posible identificar los modelos de comportamiento individuales o colectivos para prevenir actividades que pudieran tener un riesgo implícito. Aunque actualmente se encuentra en un proceso de cambio de marca, la aplicación TweetDeck resulta muy potente para obtener información de fuentes abiertas. Otras redes sociales tales como Instagram, TikTok o YouTube, están más orientadas a la distribución de contenido de forma más o menos colaborativa y no tanto a la opinión como pudiera ser X.

Otras redes sociales quizá menos conocidas en España tales como Reddit, pueden ser también de interés cuando ocurren ciertos eventos, en especial nuevas vulnerabilidades de importancia o grandes incidentes y pueden ser utilizadas también para la búsqueda de cursos. En definitiva, no se debe subestimar el potencial de las redes sociales como fuente de ciberinteligencia, tanto propia como ajena.

[12] https://www.virustotal.com/gui/home/upload
[13] https://any.run/
[14] https://www.hybrid-analysis.com/Analysis
[15] https://urlscan.io/
[16] https://www.joesandbox.com/

2.6.5. Plataformas de mensajería instantánea

Una de las que más auge ha experimentado en los últimos años es Discord [48] que, si bien en principio estaba pensada para la distribución de contenido relacionado con el mundo de los videojuegos, actualmente alberga un gran número de comunidades de todo tipo. En ella es posible encontrar grupos de mensajería en los cuales se puede intercambiar gran cantidad de información con otros miembros, obtener respuestas así como responder mediante los conocimientos propios de los que se disponga. Participar en estos foros tiene grandes beneficios ya que se puede aprender, encontrar, analizar y obtener conocimientos para entender los datos.

Otra plataforma de mensajería también de gran interés es Telegram que, además de ser totalmente anónima, dispone a su vez de grupos en los que también es posible el intercambio de información sobre OSINT[17]. No obstante, no hay que olvidar que, como todo lo relacionado con la era de internet, las fuentes de datos pueden cambiar grandemente de un año a otro, así que es muy importante también mantenerse conectado en todo momento a través de estas plataformas de mensajería y sus comunidades para expandir conocimientos.

[17] https://t.me/OsinterosSpain

Capítulo 3

Exposición de resultados

En este capítulo se va a llevar a cabo la preparación del equipo para la investigación en fuentes abiertas que se realizará en el capítulo 4. Para este cometido, se expondrán las características que debe poseer un ordenador para poder ejecutar trabajos operativos en entornos de alta tecnología. En primer lugar, se realizarán los preparativos preliminares y aquellas extensiones necesarias para obtener la información buscada, así como dar a conocer las máquinas virtuales que van a ser necesarias para poder trabajar con diversos sistemas operativos en una misma máquina.

Se va a dar a conocer también diversas versiones de imágenes de sistemas operativos especializados y configurados para la investigación en fuentes abiertas así como una breve introducción a la red Tor con el fin de aislar sitios web de programas rastreadores y buscar un anonimato en internet a través de servidores intermediarios. Se ha considerado importante la formación básica sobre Tor browser para navegar de forma anónima o para acceder directamente a la internet profunda –también conocida como Deep Web– con el objetivo de mejorar la privacidad y la seguridad.

Toda esta configuración que se va a realizar no es por capricho; puesto que, a medida que se va realizando una investigación en busca de OSINT se van dejando rastros digitales allá por donde se pasa. El sentido común dice que aquellos actores investigados también van a tener conocimientos sobre ciberinteligencia. De hecho, hasta las organizaciones criminales más pequeñas tienen equipos especializados trabajando en informática para buscar inteligencia online e incluso pueden subcontratar organizaciones para que realicen estas tareas para ellos. Así pues, va a verse cómo salvaguardar la identidad digital y lograr un mayor anonimato en línea. Se aprenderá a intercambiar

datos de forma secreta a través de entornos hostiles como internet y cómo comunicarse de forma privada y anónima.

3.1. El entorno tecnológico de investigación en fuentes abiertas

En primer lugar, para realizar cualquier investigación en fuentes abiertas es fundamental disponer de un ordenador, ya sea de sobremesa o portátil que tenga un sistema operativo instalado. Resulta fundamental que disponga de algún tipo de soporte así como de actualizaciones permanentes con el fin de que dicho sistema operativo no quede obsoleto a futuro.

Aunque se trata de un concepto básico, un sistema operativo consiste en un paquete de software capaz de administrar los componentes, los recursos y las aplicaciones del ordenador. En definitiva, aporta una capa de abstracción tal, que permite que la interacción entre el usuario y la máquina resulte sencilla e intuitiva.

Dependiendo del tipo de sistema operativo, requerirá de una formación más o menos específica para su uso. Para el caso de los sistemas basados en Windows, aunque no son la opción más adecuada –porque Windows no está pensado para ser seguro ni anónimo como va a verse– sí que están orientados a un público más generalista y su usabilidad así como su curva de aprendizaje es más rápida que aquellos que están basados en Linux.

No obstante, para suplir está deficiencia, se hará uso de máquinas virtuales para obtener las mejores características de ambos sistemas; la facilidad de uso de los sistemas basados en Windows y la especificidad de herramientas de qué disponen los sistemas basados en Linux.

Los requisitos mínimos que debe tener un sistema operativo, además de seguro y eficiente podrían resumirse en los 3 siguientes puntos:

- Gestión de los recursos del ordenador. Esto es, asignación de memoria a los procesos que están en funcionamiento en un momento dado.
- Ejecución de servicios y programas activos.
- Ejecución de los mandatos de los usuarios de la forma más sencilla posible, ya que, a medida que han ido evolucionando los sistemas operativos, ha ido des-

apareciendo la necesidad de introducir comandos por línea a favor del uso de las interfaces gráficas de usuario, que resultan más visuales y sencillas.

En cuanto a los requisitos de hardware, es necesario disponer de una cantidad suficiente de memoria RAM (Random Access Memory) ya que, este tipo de memoria de alto rendimiento y velocidad permitirá procesar y almacenar de forma temporal los datos de las aplicaciones y los programas que estén operativos en un momento dado. La principal característica de este tipo de memoria, además de su volatilidad, es su rapidez a la hora de realizar movimientos de datos. El hecho de que se trate de memoria volátil, significa que aquellos datos que estén almacenados en ella serán borrados cuando el equipo se apague o cuando esta se quede sin alimentación eléctrica. Como puede intuirse, el rendimiento de un equipo informático dado, mejorará en función de la cantidad de memoria RAM disponible debido a que podrán gestionarse más aplicaciones de forma simultánea.

Otro componente de gran importancia es la CPU o Central Processing Unit que, en términos simples, vendría a ser como el cerebro de la máquina, puesto que se encarga de coordinar todos los dispositivos de que está compuesto el sistema informático. Actualmente es muy habitual que los procesadores dispongan de varios núcleos para así poder realizar trabajos de forma paralela aportando una mayor velocidad a cualquier proceso. Los procesadores más modernos son incluso capaces de apagar los núcleos inactivos para ahorrar energía. Esta característica cobra especial relevancia en los ordenadores portátiles para mejorar la duración de la batería y en los grandes centros de procesamiento donde puede llegar a generarse una gran cantidad de calor.

3.2. El enfoque holístico de la seguridad en la ciberinteligencia

Tras haber realizado la introducción en el punto anterior, es posible encontrarse con el caso de que el ordenador no tenga ningún sistema operativo instalado. Para este fin, sería necesario instalar un sistema operativo limpio y libre; por ejemplo, Linux o Windows.

En el caso de que ya se disponga un sistema operativo instalado, hay que limpiarlo de virus, software malicioso o spyware que pueda estar contaminándolo y que, en ocasiones procede de sitios varios. No necesariamente puede tratarse de webs cuestionables; la mayoría de veces se trata de cookies de Amazon, Facebook, Google o,

simplemente del historial o de la cola de descargas. En caso de que no se tenga la total certeza de si el ordenador está contaminado o no, lo más recomendable es realizar una limpieza completa. Cuando se habla de una limpieza completa no se trata simplemente de borrar las cookies o el historial de navegación puesto que, algunas webs tales como Amazon disponen de cookies persistentes [49] y permiten saber a otras compañías que el usuario todavía online. Éste es perseguido a las páginas web que visita, tratando de recopilar sus intereses de forma que se presentan anuncios personalizados. Todo esto se traduce en que su huella digital va a estar presente durante cualquier investigación que realice.

Hablando de las cookies [50], existen dos tipos principalmente: las cookies de sesión y las cookies persistentes. Las cookies de sesión se guardan en una ubicación temporal en el explorador del cliente y se eliminan cuando el usuario cierra el navegador o se desconecta de la sesión en uso. Tales cookies se utilizan para guardar la información del carro del comprador o, simplemente, datos entre diferentes páginas. Asimismo, las cookies HTTP se utilizan para guardar las credenciales del usuario. Este tipo de cookies son menos peligrosas que las cookies persistentes y se pueden eliminar de forma segura mediante la forma habitual de borrado de cookies del propio navegador.

En el caso de las cookies persistentes existen dos tipos principalmente: las cookies flash y las evercookies [51], cookies zombies o supercookies. Las cookies persistentes, como su propio nombre indica, son más persistentes en el equipo que las HTTP y contienen información de otras páginas que se usa para seguir la actividad online de un usuario entre distintas páginas. Para el caso de las cookies flash, la cookie se guarda en una carpeta específica del disco duro del cliente; al contrario de lo que ocurre con las cookies HTTP. En otras palabras, esas cookies no se borrarán con el procedimiento estándar de borrar las cookies del explorador.

Por razones de seguridad, es altamente recomendable desactivar este tipo de cookies y borrar las que estén instaladas. Esto se puede realizar yendo al panel de control de Flash Player y seleccionando la opción de «bloquear todas las páginas que guarden la información en nuestro ordenador». A continuación, se pulsará el botón de borrar todas las cookies. De todos modos, antes de realizar esta función, hay que comprobar que, efectivamente el Flash Player está instalado en el ordenador. Esto puede comprobarse en la carpeta de aplicaciones y características del ordenador verificando si está instalado o no. En caso de que no esté instalado no hay que hacer nada.

Para el caso de las evercookies, hay que saber que están basadas en JavaScript e

identifican y reproducen las cookies borradas intencionadamente [51] en el almacenamiento del explorador del cliente. Son un mecanismo que han adoptado algunas webs para identificar usuarios incluso si intentan borrar las cookies guardadas previamente. En principio, la aplicación de limpieza que se va a utilizar más adelante (BleachBit) así como los exploradores y el software antimalware son capaces de detectar y bloquear las evercookies. No obstante, como medida adicional hay que desactivar los plugins de Java o, por lo menos, entrar en el panel de control de Java y seleccionar en la pestaña de seguridad la opción «muy alta». Se puede acceder tecleando «Java» en la barra de búsqueda y seleccionando la opción de «Configurar Java».

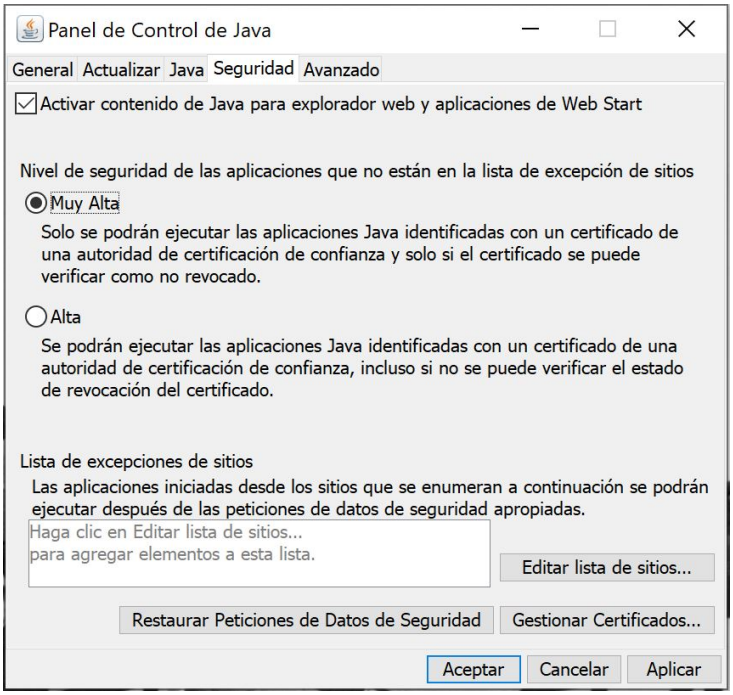

Figura 3.1: Pantalla de desactivación de los plugins de Java

Anteriormente se ha citado a Amazon por poner solamente un ejemplo, pero el caso de otras webs como, por ejemplo Google o Facebook, son mucho peores [49]. El hecho de exponer todos estos datos no está orientado a asustar ni a generar alarma social de ningún tipo, simplemente a concienciar sobre el uso que se hace de los datos de los usuarios. De este modo, si se pretende realizar investigaciones de OSINT, lo ideal es disponer de una máquina dedicada a estos fines y de otra para uso personal. Como ya se ha dicho, no se trata de borrar simplemente los archivos y realizar una limpieza del sistema mediante alguna aplicación de las muchas que hay disponibles en internet. Si se pretende hacer las cosas correctamente, habrá que formatear el disco duro y reinstalar todo el software completamente. Evidentemente esto implica borrar

todos los datos del ordenador.

Este TFG se centrará únicamente en la preparación de un host basado en Windows aunque no habría ningún problema en preparar sistemas basados en Linux o MacOS sin embargo, como el tiempo para la preparación de este trabajo es limitado, se ha elegido Windows debido a que es un sistema muy común y de gran implantación. Más concretamente Windows 10 que, a la fecha de realización del presente trabajo, es la mejor versión disponible [49] y tendrá soporte de actualizaciones hasta octubre de 2025. Llegado ese momento será necesaria la migración obligatoria a Windows 11.

3.2.1. Limpieza completa del sistema y copia de seguridad

Como es lógico, antes de realizar cualquier reposición del sistema a configuración de fábrica, es necesario realizar una copia de seguridad de los datos importantes que se desee salvaguardar. La mayoría de sistemas operativos basados en Windows disponen de una partición oculta para restablecer el sistema. Para restablecer Windows 10 a ajustes de fábrica hay que ir a **Inicio** > **Configuración** > **Actualización y seguridad** > **Recuperación** y pulsar en el botón «Comenzar» tras lo cual se proponen dos opciones:

- Mantener mis archivos
- Quitar todo

Elegir la opción de «quitar todo» y esperar a que se complete el proceso. Después de esto, se dispondrá de un nuevo sistema operativo libre de cualquier contaminación previa. Después de todos los reinicios, hay que renunciar a la propuesta de crear una cuenta de Microsoft y proporcionar únicamente la mínima información necesaria para identificarse en Windows, es decir, un nombre de usuario que nada tenga que ver con el usuario y una contraseña robusta, para lo cual, es necesario que esté formada por al menos 10 caracteres entre los que debe haber mayúsculas, minúsculas, números y algún carácter especial[1]. Otra opción es utilizar un gestor de contraseñas en un dispositivo aparte. En primera instancia no debería realizarse ninguna conexión a internet antes de haber terminado esta configuración preliminar. Seguidamente, se solicitará al usuario elegir entre la configuración rápida o personalizada. Se seleccionará la configuración personalizada y desmarcará todas las opciones disponibles, lo cual ayudará a mantener a salvo la privacidad de las violaciones más intrusivas de Windows como, por ejemplo, recopilar los datos de uso a Microsoft que proceden incluso de las

[1] https://www.incibe.es/ciudadania/formacion/infografias/crea-tu-contrasena-segura

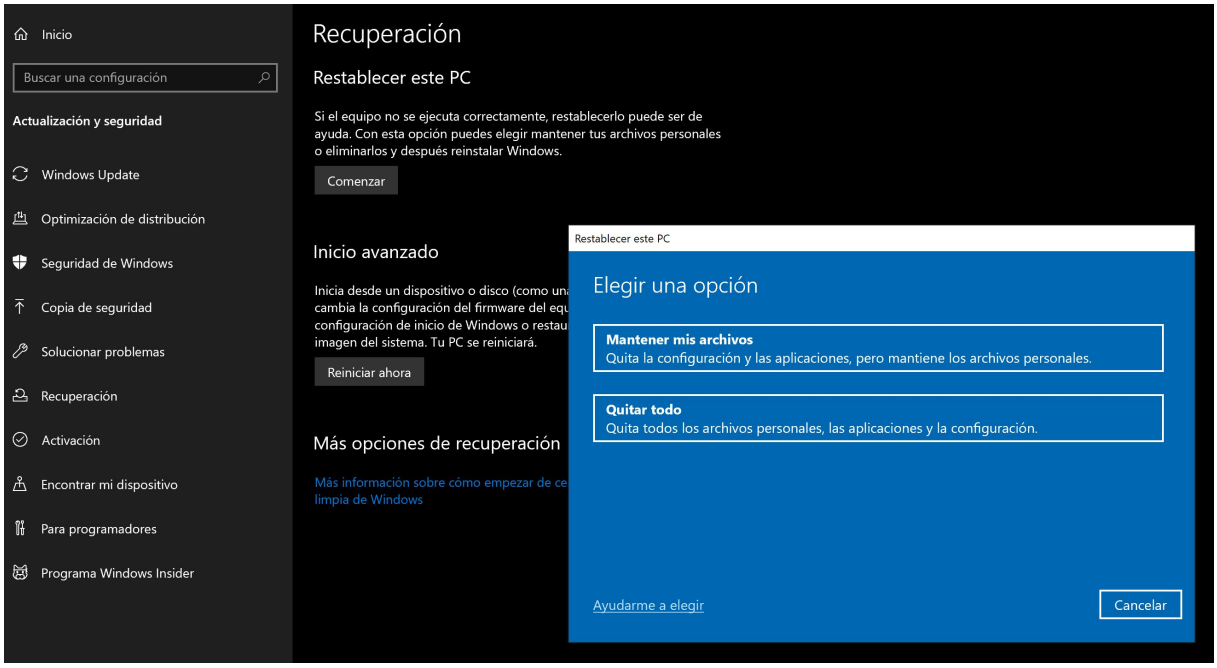

Figura 3.2: Menú de recuperación del PC

pulsaciones del teclado [49].

3.2.2. Configuración del software antivirus y antimalware

Existen varias soluciones gratuitas de antivirus y antimalware Para Windows. Para la mayoría de usuarios de Windows basta con el Windows Defender que va incluido con la instalación. Dos de los más conocidos son Avast[2] y Malwarebytes[3] que son lo suficientemente eficaces contra las amenazas genéricas. Aunque normalmente tienen los escudos activos, es necesario y recomendable realizar una revisión profunda cada 15 días. También es recomendable instalar alguna aplicación para optimizar el sistema operativo como, por ejemplo, CCleaner[4] que es capaz de analizar en profundidad el sistema operativo al completo así como incorporar funciones de escáner para obtener un listado de archivos incorrectos a demanda o de forma automática a través de una línea temporal para permitir que el usuario decida cuáles quiere borrar.

Con todo este software en su versión gratuita se considera que es suficiente para la realización de las pruebas que se van a llevar a cabo en el presente trabajo. Permitirán

[2]https://www.avast.com/
[3]https://www.malwarebytes.com/
[4]https://www.ccleaner.com/es-es

que el ordenador funcione de forma fluida y evitarán la infección de éste por parte de archivos maliciosos. No obstante, hay que remarcar que las investigaciones no se van a realizar desde este host que se está configurando, sino desde una máquina virtual dedicada que se configurará más adelante.

3.2.3. Desactivación de la telemetría en Windows 10

El servicio de telemetría de Microsoft está continuamente recopilando los datos que se indican a continuación [52] así como numerosos detalles adicionales y enviándolos a sus servidores corporativos en Seattle:

- El texto que se teclea.
- Las transmisiones a través del micrófono.
- El índice de todos los archivos de medios en el ordenador.
- Los datos de la webcam.
- El historial de navegación.
- El historial de búsquedas.
- La actividad de localización.
- Los datos de salud recopilados por Microsoft Band y otros buscadores.
- Los ajustes de privacidad a través del ecosistema de aplicaciones de Microsoft.

Con tan solo leer esta lista de puntos resulta muy fácil intuir la sencillez con que el usuario podría ser identificado; especialmente la actividad en línea. A pesar de que Microsoft afirma que estos datos se recopilan solamente para mejorar la experiencia, quizá podría llegar a pensarse que es una práctica demasiado invasiva. Además de esto, pese a haber realizado una configuración personalizada de privacidad durante la instalación, todavía quedan algunos contenidos que Microsoft va a seguir recolectando y que se deberían desactivar. También existen algunas herramientas que pueden ayudar con esto, pero la que se ha elegido para este trabajo por su sencillez es O&O ShutUp10++[5] la cual permitirá realizar ajustes más finos sobre los datos que todavía se siguen enviando a Microsoft. La aplicación es bastante sencilla e intuitiva de utilizar: básicamente todos los indicadores que están marcados en rojo determinan que esa

[5]https://www.oo-software.com/en/shutup10

información está siendo enviada a Microsoft y los que están seleccionados en verde significan que el envío de dicha información está siendo bloqueado.

De cara a la realización de este trabajo, se prefiere la opción de «configuraciones recomendadas y algo recomendadas» porque mantendrán funcionando las actualizaciones y el Windows Defender, que son de vital importancia para la seguridad del equipo. Después de haber realizado todas las selecciones, se cierra el programa y se reinicia Windows. Después de esto, se abre el programa de nuevo y se verifica que todos los ajustes realizados previamente se mantienen. Es recomendable volver a comprobar la configuración de este programa cada vez que se produzca una actualización de Windows por si volviera a ser necesario reajustar la configuración.

Figura 3.3: Configuración del programa O&O ShutUp 10++

3.2.4. Análisis profundo del sistema y limpieza

Aunque anteriormente se ha hablado de CCleaner, otra aplicación muy recomendable es BleachBit[6] que permitirá eliminar restos de todo tipo del historial de navegación en Windows, archivos temporales y cualquier tipo de datos no deseados. Es recomendable ejecutar el programa de forma semanal en cualquier sistema Windows o Linux. Se recomienda marcar todas las opciones excepto la de «espacio libre en disco» porque sobrescribiría todo el espacio libre en el disco duro, resultando en un consumo de tiempo excesivo.

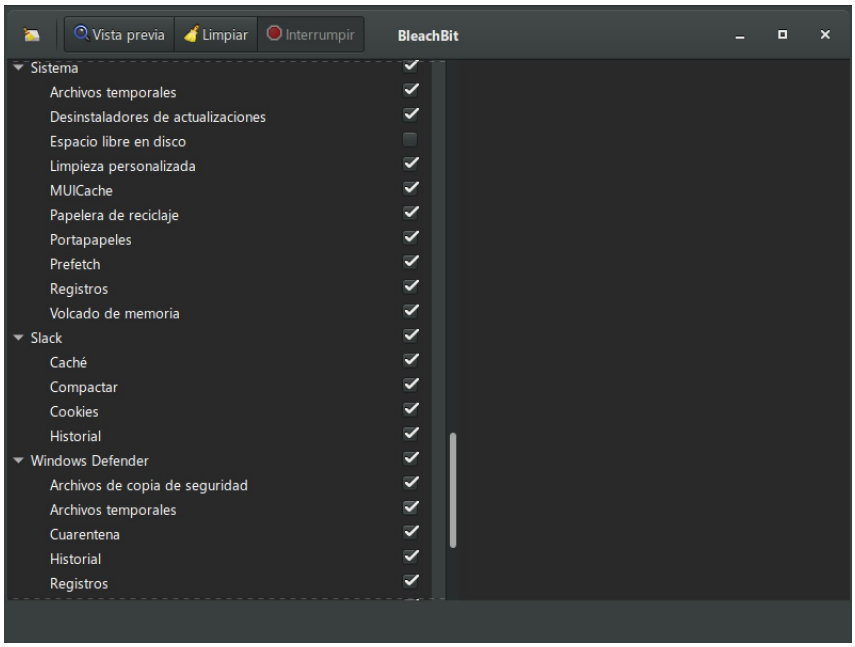

Figura 3.4: Configuración del programa BleachBit

3.2.5. Redes privadas virtuales

Para asegurar una mayor privacidad a la hora de realizar cualquier investigación de OSINT, resulta prácticamente un estándar el disponer de una VPN [49]. A grandes rasgos, una VPN crea una red privada virtual a través de una red pública como puede ser internet. Permite a los usuarios enviar y recibir datos a través de redes públicas beneficiándose de la privacidad y seguridad de una red privada, puesto que los paquetes que circulan por la red viajan encriptados.

De no hacer esto y, simplemente utilizar la conexión a través del proveedor de servicios de internet ISP, en caso de navegar a una página web, esta conocería la dirección

[6]https://www.bleachbit.org

IP, la localización, y el proveedor de internet. Sin embargo, si se navega utilizando la misma conexión, el mismo equipo y mediante una conexión VPN, esta protege, puesto que la conexión se realiza a través de uno de sus servidores. El tráfico que va encriptado no puede ser descifrado por el ISP. De este modo, cuando los datos llegan al servidor VPN, éste los envía y recibe devolviéndo los paquetes. De este modo, la ubicación y la IP frente al servidor que se esté visitando será la del servidor VPN. De este modo no se sabrá la propia localización ni el tipo de conexión a internet que se tenga.

Otra opción podría ser el uso de la red TOR, sin embargo, las conexiones pueden resultar demasiado lentas para un uso constante y algunas páginas web (como por ejemplo entidades financieras) pueden no permitir el acceso a sus servicios a través de proxys TOR y generar alarmas que que, de hecho también pueden aparecer a través de la navegación VPN. La opción selegida para este trabajo es Proton VPN[7] que dispone de una versión gratuita, si bien los servidores elegibles únicamente van a estar ubicados en Estados Unidos, Países Bajos o Japón. La configuración del programa es muy sencilla: simplemente hay que descargarlo, instalarlo, crear un usuario gratuito y, finalmente, pulsar en el botón «conexión rápida», tras lo cual se asignará una ubicación en función de la carga que tengan los servidores. También es posible elegir la ubicación manualmente seleccionando el país que interese.

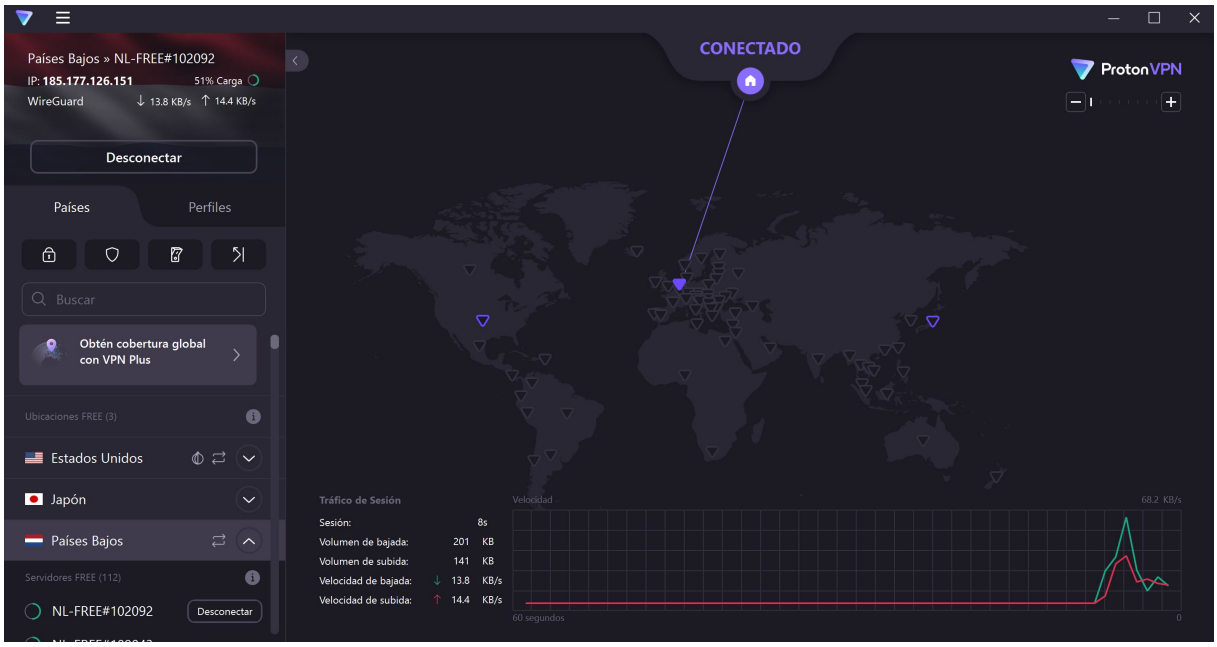

Figura 3.5: Menú principal de Proton VPN

[7]https://protonvpn.com

3.2.6. Gestor de contraseñas

Ya sea realizando una investigación de OSINT o en el día a día, el uso de un gestor de contraseñas es altamente recomendable. Tanto en un ámbito como en el otro, cada día es más habitual la creación y el uso de muchos servicios en los cuales es necesario disponer de nombre de usuario y contraseña. Aunque existen un gran número de aplicaciones e incluso los móviles disponen de su propio gestor de contraseñas integrado, la aplicación KeePassXC[8] es un gestor de contraseñas de código abierto que no sincroniza su contenido a internet. Se descarga e instala siguiendo las siguientes directrices:

1. Ejecutar KeePassXC y seleccionar «nueva base de datos».
2. A continuación, dar nombre a la base de datos y una descripción de la misma si así se desea.
3. En la siguiente pantalla, deslizar la barra de ajustes completamente hacia la derecha para obtener una máxima privacidad.
4. Seguidamente, asignar una contraseña segura a la base de datos que sea fácil de recordar pero que no se esté utilizando en ningún otro sitio.
5. Seleccionar «finalizar» y asignar una localización segura para guardar la base de datos.
6. Cerrar el programa y verificar que es posible abrir la base de datos con la contraseña asignada.

Hay que reseñar que no es posible mostrar capturas de pantalla a lo largo del documento porque, debido a la privacidad del programa, este las tiene deshabilitadas, es decir, no es posible realizar pantallazos ni recortes para mostrar el contenido de lo que la aplicación saca por pantalla.

Habiendo instalado ya este gestor de contraseñas, se utilizará de forma aislada de la máquina virtual que se instalará más adelante y así resultará sencillo realizar cambios en las contraseñas. El trabajar de esta forma aporta una capa adicional de seguridad, puesto que no quedarán credenciales almacenadas en la máquina virtual que se utilice.

Ya que la base de datos de contraseñas quedará almacenada localmente en el ordenador que será el host, es necesario hacer periódicamente una copia de seguridad y almacenarla en un dispositivo externo como un pendrive para que, como en caso

[8] https://keepassxc.org/

de que surja algún problema con el ordenador, no se pierdan todas las contraseñas almacenadas. El dispositivo que se vaya a utilizar para realizar la copia de seguridad debería estar encriptado también.

Así pues, para crear y almacenar una contraseña en KeePassXC se procederá de la siguiente manera:

1. En la pestaña de grupos seleccionar «nuevo grupo», darle nombre y pulsar aceptar.

2. En el menú de la izquierda seleccionar la carpeta nombrada y pulsar el botón de «añadir nuevo apunte», cuyo símbolo es un «+».

3. Cumplimentar el formulario que aparecerá, introduciendo nombre de la cuenta, nombre de usuario, URL y terminar pulsando el botón con forma de dado que está incrustado en el campo contraseña.

4. En la pantalla que se abrirá a continuación, se podrá seleccionar la longitud de la contraseña, que podrá ser de hasta 128 caracteres, sin embargo, con un mínimo de 10 y un máximo de 40, se puede considerar suficientemente segura.

5. Aceptar y grabar la base de datos para que este cambio quede registrado.

Como paso final, habrá que ir entrando en aquellos sitios cuyas contraseñas se quieran cambiar e ir sustituyéndolas por otras más seguras usando esta aplicación. Para aquellos usuarios que no están acostumbrados a utilizar este tipo de aplicaciones para la gestión de contraseñas, todos estos preparativos pueden resultar un poco farragosos, sin embargo, también se persigue a través de esta exposición realizar una labor de concienciación frente a la debilidad de las contraseñas; que muchas veces se reutilizan de unos sitios a otros y que pueden facilitar el acceso a otras cuentas en caso de que se produzca una filtración de datos en alguna de ellas. Trabajando de esta manera se está logrando una seguridad máxima.

3.2.7. Securización del sistema contra ataques de pharming

El Pharming es un tipo de ciberataque que se desarrolló a partir del phishing [53]. El atacante que implementa esta técnica intenta redirigir el tráfico web –especialmente los datos de solicitud– a un sitio web fraudulento. Esto se logra explotando vulnerabilidades de software en los sistemas de nombre de dominio (DNS, por sus siglas en inglés) o en los equipos de los propios usuarios, que permiten a atacantes redirigir un nom-

bre de dominio a otra máquina distinta. De esta forma, un usuario que introduzca un determinado nombre de dominio que haya sido redirigido, accederá en su explorador de internet a la página web que el atacante haya especificado. Para protegerse frente a esta amenaza [28], hay que acceder a la carpeta `C:\Windows\System32\drivers\etc` hacer clic derecho sobre el archivo hosts y seleccionar «propiedades». Finalmente marcar el checkbox de «solo lectura», aplicar cambios y aceptar.

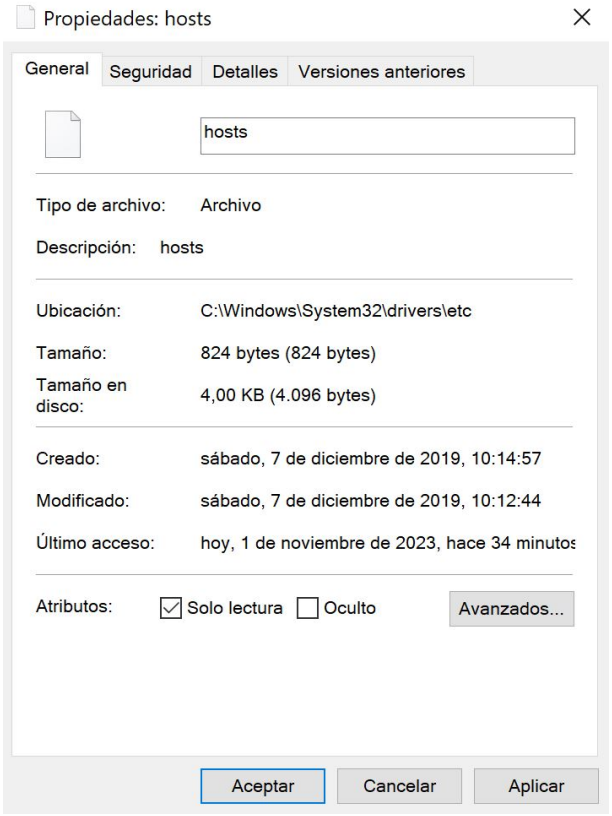

Figura 3.6: Propiedades del archivo hosts para evitar ataques de pharming

3.2.8. Configuración del control de cuentas de usuario

El control de cuentas de usuario monitoriza los cambios que van a realizarse en el ordenador mostrando una ventana emergente en aquellos casos en los que se requiere acceso de administrador como, por ejemplo, instalar o desinstalar programas. Si se selecciona el máximo nivel de notificaciones, cualquier pequeño cambio que se ejecute en el equipo ayudará a detectar si algún malware está haciendo cambios en el ordenador. Para ir hasta allí, simplemente hay que entrar en configuración, teclear «privilegios» en la barra de búsqueda y seleccionar la opción de «cambiar configuración de control de cuentas de usuario».

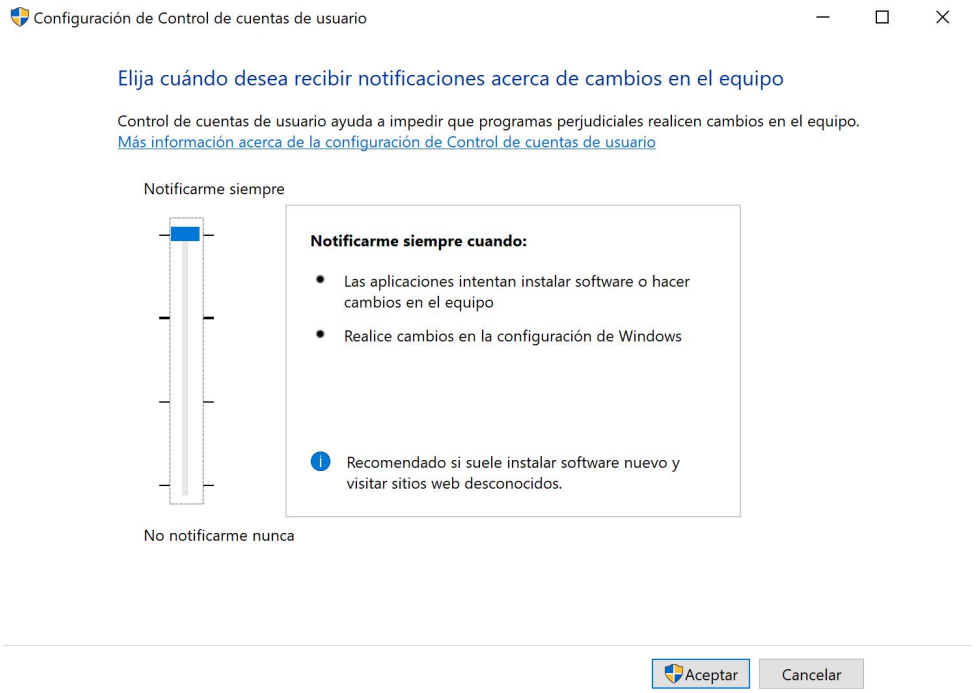

Figura 3.7: Pantalla de control de cuentas de usuario

3.2.9. Desactivación de la asistencia remota

Esta característica permite a un usuario remoto acceder a un equipo a través de una conexión de red. Si no se va a utilizar esta característica, se recomienda desactivarla [28] para evitar que los hackers hagan uso de ella para acceder de forma no autorizada al ordenador. Para desactivarla, simplemente hay que teclear en el buscador la palabra «asistencia remota» y, en la pantalla que aparecerá a continuación, desmarcar el checkbox «permitir conexiones de asistencia remota a este equipo» y, en la parte de abajo de la ventana, marcar la opción «no permitir las conexiones remotas a este equipo».

3.2.10. Hacer visibles los archivos ocultos

Algunos tipos de malware y otros programas maliciosos pueden aparecer ocultos mediante el mismo atributo que utiliza Windows para ocultar los archivos de sistema. Para mostrar los archivos ocultos en Windows 10 hay que teclear en la barra de búsqueda «opciones del explorador de archivos» y, seleccionando la pestaña «ver» seleccionar la opción «mostrar archivos carpetas y unidades ocultos». También hay que verificar que se desmarca la opción «ocultar archivos protegidos del sistema operativo» así como desmarcar también la opción de «ocultar las extensiones de archivo para

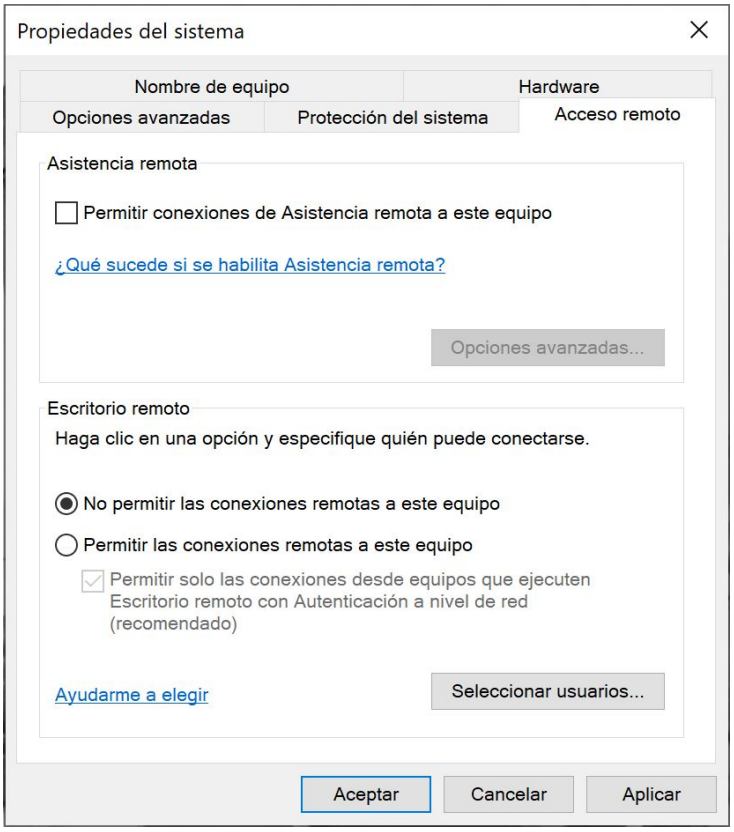

Figura 3.8: Menú de desactivación de la asistencia remota

tipos de archivo conocidos».

3.2.11. Configurar una contraseña para la BIOS/UEFI

Algunos ciberataques contra sistemas operativos y software de encriptación como, por ejemplo el ransomware, se basan en arrancar la máquina de la víctima utilizando un USB o un CD para destruir las llaves de encriptación [28] o para encontrar un una forma de robar los datos sensibles de la víctima. Configurando una contraseña para la para la BIOS/UEFI, cada vez que el usuario arranca la máquina necesita proporcionar algún tipo de credenciales, es decir, una contraseña antes de que el ordenador cargue el sistema operativo.

A través de este procedimiento se podrá evitar que el atacante cambie la configuración de la BIOS/UEFI o dañe el ordenador borrando los datos del sistema operativo. Para realizar esta operación hay que consultar el manual de instrucciones de la placa base porque, dependiendo del fabricante, la forma de acceder y configurarla puede cambiar. Generalmente esta configuración suele estar en un menú que se llama habi-

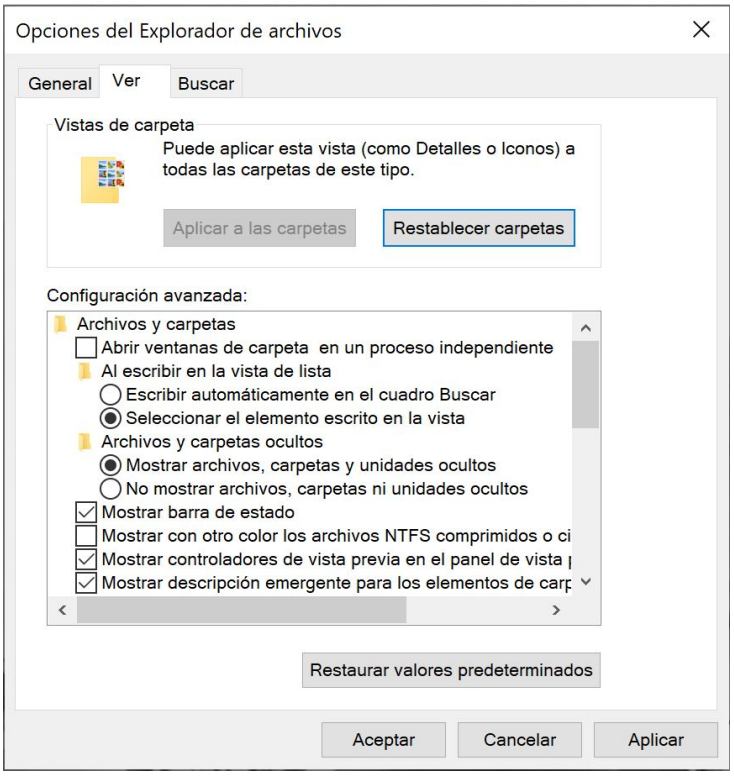

Figura 3.9: Configuración para visualización de archivos ocultos

tualmente «seguridad».

3.2.12. Desactivación de los puertos o los protocolos y servicios que no vayan a utilizarse

Para el caso de los sistemas operativos Linux, la práctica totalidad de los puertos están cerrados por defecto, sin embargo, para el caso de Windows están todos abiertos, lo cual es un riesgo potencial porque se puede ser víctima de un ataque de escaneo de puertos. La tarea de controlar el tráfico que entra y sale de cada puerto es tarea del cortafuegos. Si éste está configurado adecuadamente, deberá evitar que se produzcan este tipo de ataques. En este apartado no se entrará en detalles porque se considera que la máquina virtual estará suficientemente securizada en este aspecto.

3.2.13. Precauciones de sentido común

En este apartado se incluyen una serie de prácticas que, por ser sencillas y en la mayoría de casos no formar parte de la configuración del ordenador, simplemente se van nombrar para general conocimiento:

- Cubrir la webcam. Ya sea con cualquier tipo de cinta o el mecanismo del que disponen las cámaras más modernas, por norma general si no se están utilizando, deberían estar cubiertas, puesto que los hackers y los servicios de inteligencia pueden hacer uso de cámaras y micrófonos cuando están investigando a personas concretas.

- Evitar el software pirata. Cómo es de lógica, un software descargado de internet que ha sido pirateado no puede esperarse de ningún modo que tenga las mismas garantías de seguridad que su contraparte original. Resultaría muy difícil conocer si la persona que ha eliminado las protecciones originales de la aplicación no introdujo un troyano o un keylogger para así conseguir información de cualquier tipo de las personas que muerdan el anzuelo con la excusa de descargarse algún software presuntamente gratuito. Esto cambia para el caso de los programas freeware o de código abierto pero, en cualquier caso, siempre es necesario pasar un antivirus para evitar sorpresas desagradables.

3.2.14. Securización física de los ordenadores

Hasta ahora se ha venido hablando de la securización basada en el software, pero también es fundamental securizar los equipos frente a robos o accesos no autorizados. Para tal fin, las opciones disponibles serían las siguientes:

- Para el caso de un ordenador portátil nunca se debe dejar desatendido en lugares públicos.

- Utilizar un cable antirrobo enganchado al equipo incluso cuando se esté trabajando con él para evitar así en la medida de lo posible los robos con fuerza.

- Desactivar las redes Bluetooth y WiFi si no se están utilizando.

- Colocar un filtro de privacidad en la pantalla de los ordenadores portátiles para evitar el shoulder surfing [54] o, en términos más sencillos, que algun agente malicioso espíe por encima del hombro mientras se trabaja con información sensible.

- Disponer de un registro por escrito de todas las características del ordenador: modelo, número de serie, dirección MAC, y cualquier otro tipo de información de interés que tenga el dispositivo en caso de que sea robado.

3.3. Configuración de la máquina virtual

Como se ha comentado en el apartado anterior, se va a hacer uso de máquinas virtuales para la investigación en fuentes OSINT. A modo introductorio, se define una máquina virtual de forma sencilla como un sistema operativo dentro de otro sistema operativo. Para llevar a cabo esta tarea, es necesario un programa de virtualización que se ejecute en el host. Normalmente, este software permite ejecutar más de una máquina virtual simultáneamente y estas son independientes entre sí y del sistema operativo que actuará como host. El entorno de una máquina virtual no tiene ningún impacto en las demás. De forma sencilla, se puede entender que se dispondrá de diferentes ordenadores en un mismo ordenador. En definitiva, va a ser posible investigar un objetivo concreto en un entorno seguro sin interferencia de otras investigaciones. Asimismo, también será posible clonar una máquina virtual en poco tiempo y no habrá que preocuparse sobre los virus, cookies, etc.

Como se ha dicho, para crear una máquina virtual se necesitará un software de virtualización. Los más comunes son VirtualBox[9] o VMware[10] en su versión gratuita. Teniendo en cuenta siempre que se preparará este entorno de virtualización en un sistema Windows por ser hoy en día el más común y accesible para la mayoría de usuarios. Finalmente, en este apartado hay que decir que también es posible crear máquinas virtuales en entornos de Windows 10 Profesional, Education o Enterprise mediante el uso de su herramienta nativa llamada Hyper-V [55].

3.3.1. Descargando el software de virtualización

Como se ha dicho, el software de virtualización que se va a utilizar será VirtualBox por ser una opción de código abierto, y habrá que hacerlo de su página oficial[11] e instalaro siguiendo las instrucciones indicadas en su manual[12]. Se seleccionará la aplicación para hosts de Windows y la versión más actualizada que, a fecha de realización de este trabajo es la 7.0.12. Con los ajustes por defecto del asistente de instalación será suficiente. También hay que descargar el VirtualBox 7.0.12 Oracle VM VirtualBox Extension Pack e instalarlo también con sus ajustes por defecto.

[9] https://www.virtualbox.org/
[10] https://www.vmware.com/es/products/workstation-player.html
[11] https://www.virtualbox.org/wiki/Downloads
[12] https://download.virtualbox.org/virtualbox/7.0.12/UserManual.pdf

Figura 3.10: Portal de descargas de VirtualBox

3.3.2. Instalación de la máquina virtual

Este punto puede ser el más controvertido para según qué usuarios, puesto que existen varias distribuciones de Linux orientadas hacia el pentesting y, más concretamente hacia la OSINT, tales como Kali Linux[13] o, más específicamente, OSINTUX[14]. También existen otras distribuciones de Linux tales como, DORA OSINT VM[15], HuronOsint[16], Tsurugi Linux[17], CSI Linux[18] o Trace Labs OSINT VM[19] o, la muy reciente máquina virtual OriON[20] de origen español y destinada específicamente a la recopilación de información en fuentes abiertas sobre personas [56].

Sin embargo, el problema de todas estas distribuciones es que suelen ser proyectos muy específicos, de carácter experimental, y la mayoría de ellas caen en un estado de abandono [49] y dejan de recibir actualizaciones. A causa de esto, el usuario que las instaló en su momento recibe errores porque deja de existir el repositorio online. Es por

[13]https://www.kali.org/
[14]https://www.osintux.org/
[15]https://github.com/OSINTResearch/dora-osint-vm/blob/master/README.md
[16]https://github.com/HuronOsint/OsintDistro
[17]https://tsurugi-linux.org/
[18]https://csilinux.com/
[19]https://www.tracelabs.org/initiatives/osint-vm
[20]https://github.com/Cl4r4-5/OriON

este motivo por el que se va a utilizar Kali Linux debido a que es una distribución muy popular, ampliamente utilizada, y que recibe actualizaciones con mucha frecuencia.

Adicionalmente se trata de un sistema muy estable y amigable tanto para usuarios expertos y avanzados como para los usuarios más novatos e inexpertos. A fecha de redacción de este trabajo, la última versión de Kali Linux es la 2023.3 que va a ser la elegida debido a la total disponibilidad de las herramientas de ciberinteligencia que se van a usar. Dicho esto, la opción más sencilla es descargar la máquina virtual preconstruida para VirtualBox[21] e instalarla siguiendo los pasos especificados en el apéndice A.

Figura 3.11: Máquinas virtuales Kali Linux preconstruidas

3.4. Herramientas y técnicas para análisis de ciberinteligencia en el espacio red

En este punto se hará una exposición de todas las herramientas y técnicas más conocidas para llevar a cabo una investigación de ciberinteligencia en fuentes abiertas. Se puede hacer una primera clasificación en base a si estas herramientas son en el

[21] https://www.kali.org/get-kali/#kali-virtual-machines

espacio red o si están alojadas en el ordenador. En el primer caso, se dará a conocer algunas páginas web que van a ser de interés para verificar el nivel de salud o de exfiltración de los datos personales. Los buscadores o motores de búsqueda son las herramientas más sencillas y accesibles a las que todos tiene acceso. Aparte de esto, existen algunas webs de carácter más específico que como se verá más adelante, van a permitir conocer si los datos personales se han visto involucrados en algún tipo de filtración masiva o si las contraseñas en uso son lo suficientemente seguras para que, en caso de que esto haya sucedido se proceda a su cambio inmediato o no.

3.4.1. Buscadores generalistas

Los buscadores más utilizados a día de hoy son Google o Bing [28] y, aunque su uso es bastante sencillo, es conveniente conocer su funcionamiento al detalle así como los comandos que disponen para devolver resultados más refinados. De esta forma, se evitará que el buscador devuelva una cantidad demasiado elevada de respuestas, lo cual resultaría contraproducente. Centrándose en los operadores para refinar las búsquedas de Google o Bing, se verá que son muy similares y, que con poco más de una docena de ellos se va a conseguir un refinamiento muy elevado de los resultados de búsqueda. A esta técnica de búsqueda de datos específicos mediante comandos, se la denomina también Google hacking [57] o Google dorking.

Filtro de Google/Bing	**Operador**	**Ejemplo**
Búsqueda exacta	“”	“universitat oberta de catalunya”
Exclusión de un término o frase	-	universitat -oberta
Buscar X o Y	OR, |	universitat oberta|politecnica
Buscar X e Y (utilizado por defecto)	AND	universitat AND oberta AND catalunya
Comodín	*	universitat de *
Búsqueda de un rango de números	..	premios loteria 2000..2005
Agrupar términos u operadores	()	“universitat oberta de (catalunya|valencia)”
Buscar en un dominio	site:	universitat site:uoc.edu
Buscar un tipo de archivo	filetype:	uoc filetype:pdf
Buscar en los títulos de una página	intitle:	universitat intitle:uoc
Buscar en URLs	inurl:	universitat inurl:uoc
Buscar en el texto de las páginas	intext:	universitat intext:julian
Buscar la versión más reciente de una página	cache:	cache:uoc.edu

Tabla 3.1: Filtros de búsqueda avanzada de Google/Bing

3.4.2. Buscadores específicos

Puesto que, en este trabajo únicamente se harán búsquedas sobre personas, se mencionará únicamente un buscador específico que probablemente es de los más conocidos en el campo de la OSINT y este es Shodan[22]. Se trata de un motor de búsqueda que proporcionará información pública de equipos conectados a internet [20]. Esto incluye servidores, routers, equipos de almacenamiento online, cámaras de vigilancia, webcam, equipos de internet de las cosas [58], o incluso sistemas de telefonía IP.

La recolección de estos datos se hace a través de protocolos como, por ejemplo, HTTP/SSH permitiendo al usuario la búsqueda por direcciones IP, organización, país, o ciudad. El uso que se suele dar a esta herramienta es principalmente con fines de seguridad de red; por ejemplo, para detectar vulnerabilidades en equipos que puedan estar expuestos a la red sin saberlo. También resulta muy interesante su uso de cara a la securización de equipos de internet de las cosas y su aislamiento de la red.

3.4.3. OSINT Framework

OSINT Framework[23] es un catálogo interactivo en línea de herramientas y recursos OSINT. Tiene una lista de 32 elementos de información que son el punto de partida para una búsqueda (por ejemplo, nombre de usuario, dirección de correo electrónico, nombre de dominio, dirección IP, imagen/video/documento y redes sociales). Al hacer clic en «motores de búsqueda de personas», se muestran registros y búsquedas generales de personas. En este catálogo están incluídas la mayoría de las herramientas que se expondrán a continuación.

3.4.4. Servicios de comprobación de emails

Algunos portales ofrecen servicios basados en las direcciones de correo eléctrónico para realizar comprobaciones específicas. Los que se ha considerado que ofrecen información de mayor interés para este trabajo son los siguientes:

- Epieos[24]. Permite validar una dirección de correo y obtener información básica de la misma como, por ejemplo, nombre del usuario, redes sociales a las que está asociada, etc.

[22]https://www.shodan.io/
[23]https://osintframework.com/
[24]https://epieos.com/

- Have I Been Pwned[25]. Se trata de un portal que permite comprobar si una dirección de correo electrónico se ha visto implicada en una filtración de datos. Otra de sus funciones es la de registrar la dirección para recibir futuras actualizaciones en caso de que se produzcan nuevas filtraciones. Con este servicio va a ser posible comprobar en qué webs se ha visto afectada la dirección en cuestión y actuar en consecuencia como, por ejemplo, cambiando la contraseña.

3.5. Software para análisis de ciberinteligencia en el entorno virtualizado

Después de la introducción a estas herramientas de búsqueda en el espacio red, se van a presentar las herramientas específicas que estarán alojadas en la máquina virtual desplegada en el apartado anterior. Únicamente se han seleccionado aquellas que proporcionan una buena cantidad de datos de interés y que disponen de una curva de aprendizaje sencilla para los usuarios con menos experiencia. Las aplicaciones más específicas no es que no resulten de interés, sino que están más orientadas análisis de ciberinteligencia más específicos para analistas más profesionales y no tanto para el usuario inexperto.

3.5.1. The Harvester

The Harvester[26] es una herramienta para la obtención de información en fuentes públicas mediante motores de búsqueda. En concreto, es capaz de generar listas de emails, nombres de host, así como subdominios, direcciones IP y URLs relacionados con el dominio que se quiere analizar. Su funcionamiento es a través de línea de comandos, si bien no son muchos ni excesivamente complicados. En el caso de estudio se verá un análisis sencillo. Viene preinstalado en Kali Linux.

3.5.2. Sherlock

Sherlock[27] va a permitir encontrar en qué redes sociales está registrado un nombre de usuario. Va ser de utilidad para tener una idea aproximada de las redes sociales en las que participa el usuario, conocer aquellas que pudiera haber olvidado estar registrado e incluso saber si hay alguien más con el mismo nombre.

[25]https://haveibeenpwned.com/
[26]https://github.com/laramies/theHarvester
[27]https://github.com/sherlock-project/sherlock

3.5.3. Spiderfoot

Spidefoot[28] es una herramienta de reconocimiento multipropósito que utiliza múltiples fuentes de datos para obtener información. También viene preinstalada en Kali Linux, y su interfaz –que está basada en web– es muy sencilla e intuitiva. En primer lugar, es necesario levantar su servidor mediante el siguiente comando:

```
$ spiderfoot -l 127.0.0.1:80
```

Acto seguido, se realizará la conexión a Spidefoot mediante la interfaz loopback de Linux en el navegador tecleando `http://localhost/` o, simplemente la dirección `http://127.0.0.1:80/`. Mediante los más de 200 módulos disponibles (la mayoría de uso gratuito) en la aplicación [59] para búsqueda en fuentes públicas, se podrá realizar búsquedas por correo electrónico, teléfono, dominio web o nombre, entre otros. Trambién será posible definir los requisitos de búsqueda y los módulos que se quieren activar.

3.5.4. Maltego

Maltego[29] es una aplicación muy conocida que encuentra automáticamente información pública sobre un determinado objetivo dentro de diferentes fuentes (registros DNS, registros Whois, motores de búsqueda, redes sociales, varias API en línea, metadatos, etc.). Las relaciones entre los elementos de interés encontrados están representados en forma de grafo dirigido para su análisis. A diferencia de Spiderfoot, su uso es de pago, aunque su interfaz es más elaborada y compleja. Aunque existe una versión de la comunidad, en principio se va a descartar esta herramienta por su complejidad y su uso menos intuitivo respecto a Spiderfoot.

[28] https://www.spiderfoot.net/
[29] https://www.maltego.com/

Capítulo 4

Casos de estudio sobre OSINT

En este capítulo se van a proponer algunos casos de estudio mediante los cuales se pretende comprobar la funcionalidad de las herramientas que se han presentado en los capítulos anteriores. También se realizará la correspondiente interpretación de los resultados que se obtendrán para un mejor entendimiento de los conceptos que se han venido explicando.

4.1. Exfiltración de contraseña en una dirección de correo electrónico

En este primer caso, se hará uso de la herramienta Have I Been Pwned? y del Archivo de Internet para detectar una exfiltración de contraseña sobre una dirección de correo electrónico que en su día recibió una gran cantidad de spam así como un acceso no autorizado a una cuenta de usuario registrada con ese email.

Como puede verse en la figura 4.1, tras introducir la dirección de correo, se puede ver que ha estado implicada en 11 violaciones de datos y además en un «pegado» lo cual es un síntoma temprano de que, efectivamente la dirección de correo está contenida en alguna violación de datos [60]. En este contexto concreto, un pegado se puede definir como una muestra de datos comprometidos en alguna web que está disponible durante un tiempo breve. En el caso que se está estudiando, la web indicada en Have I Been Pwned? (figura 4.2) ya no está disponible, sin embargo, es posible acceder a ella a través del Archivo de Internet (véase figura 4.3) que pudo hacer una captura de dicha página durante el tiempo que estuvo en línea (figura 4.4).

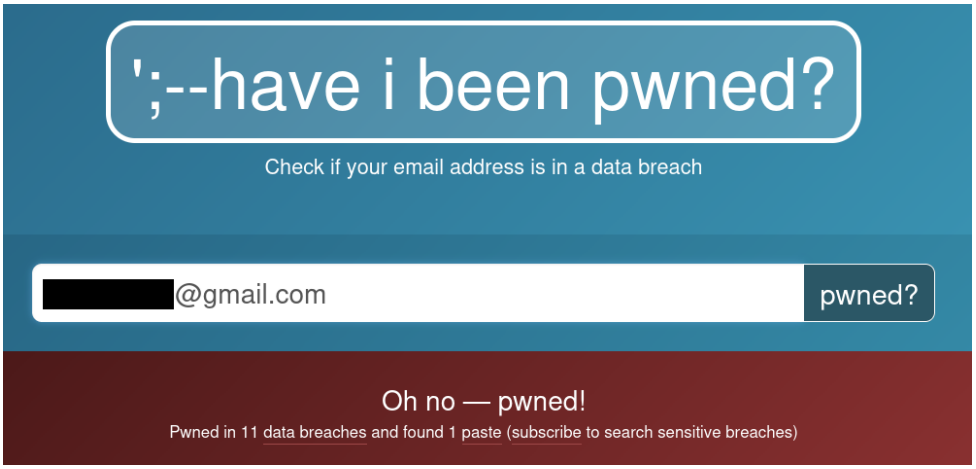

Figura 4.1: Comprobación de una dirección en Have I Been Pwned?

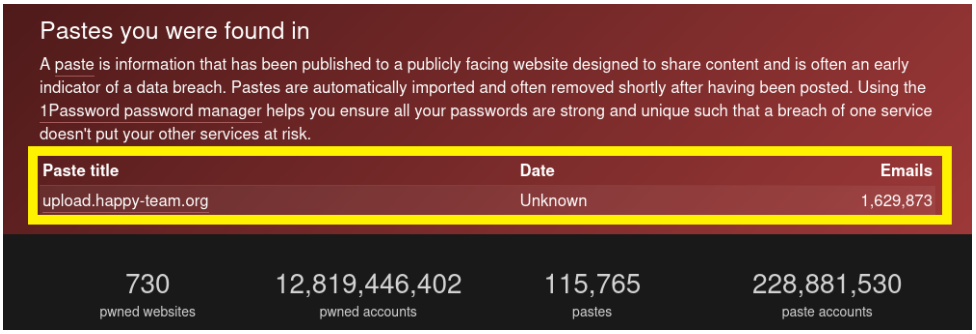

Figura 4.2: Web en la que se detectó el pegado de contraseñas

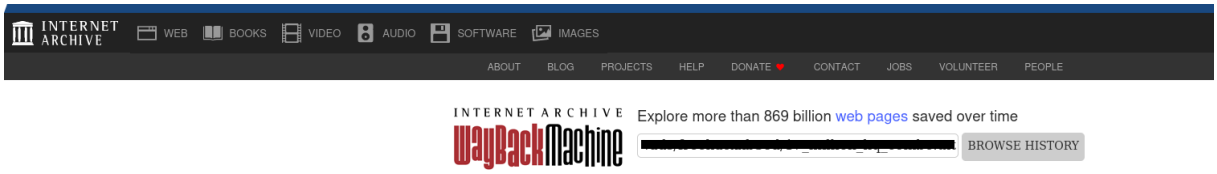

Figura 4.3: Búsqueda en Wayback Machine

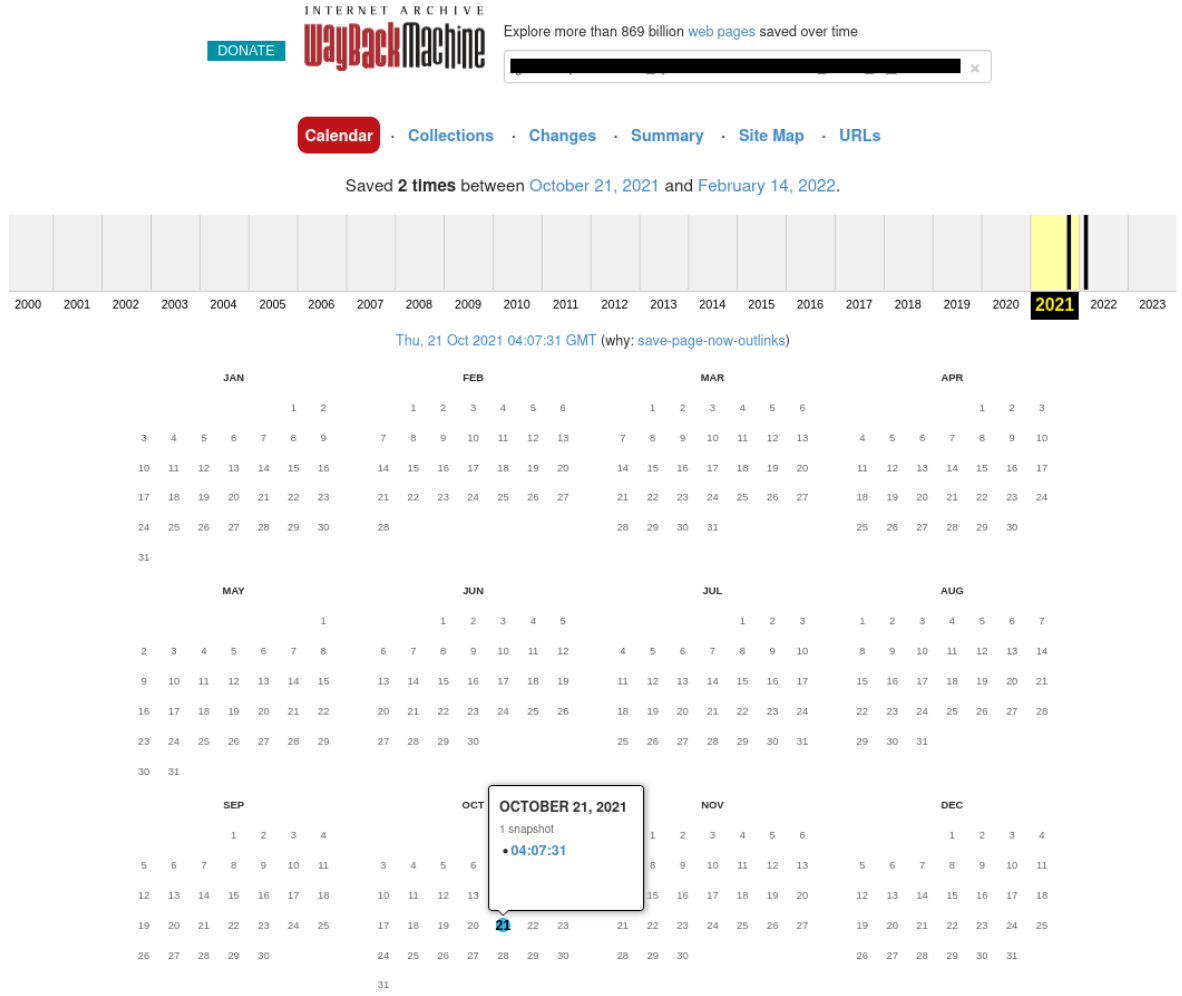

Figura 4.4: Crawlings efectuados en la web de datos exfiltrados

Tal como se muestra en la figura 4.5 y, a través del buscador, puede verse que, efectivamente, la dirección había sido publicada junto con su contraseña. Una contraseña que, a todas luces es poco segura; sin embargo, en caso de producirse un pegado, este aspecto es irrelevante, ya que la contraseña había sido publicada en claro. En este aspecto, poco puede hacerse por parte del usuario, salvo estar atento a las conexiones sospechosas en sus cuentas y cambiar las contraseñas con frecuencia utilizando gestores de contraseñas offline como KeePassXC.

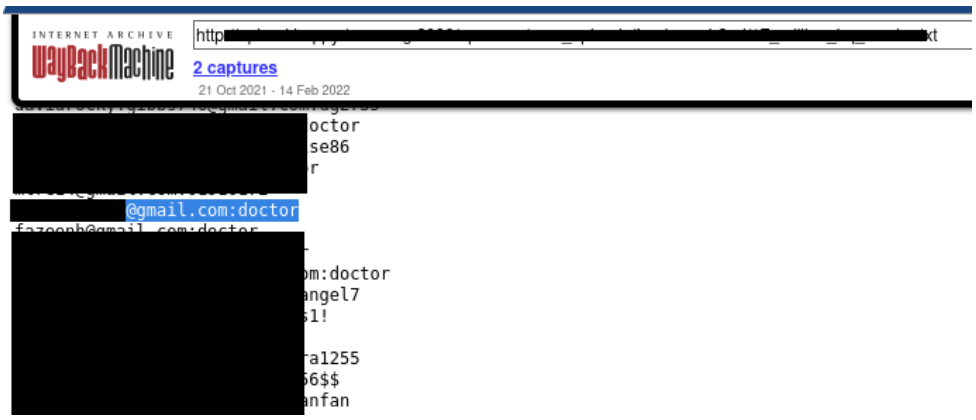

Figura 4.5: Datos de direcciones y sus contraseñas asociadas

4.1.1. Uso de SpiderFoot para localización de datos exfiltrados

Para realizar una búsqueda más intensiva sobre los datos disponibles en la red, se puede hacer uso de la herramienta SpiderFoot sobre la misma dirección de correo que proporcionará datos de otras fuentes. Bastará con introducirla en el formulario de búsqueda, asignarle un nombre y pulsar el botón «Run Scan Now» (figura 4.6). El propio programa identificará que se trata de una dirección de correo electrónico y actuará en consecuencia. Para este caso se ha elegido la opción «Get anything and everything about the target» para activar todos los módulos disponibles en SpiderFoot. Puesto que se trata de una dirección de correo, la búsqueda no llevará demasiado tiempo.

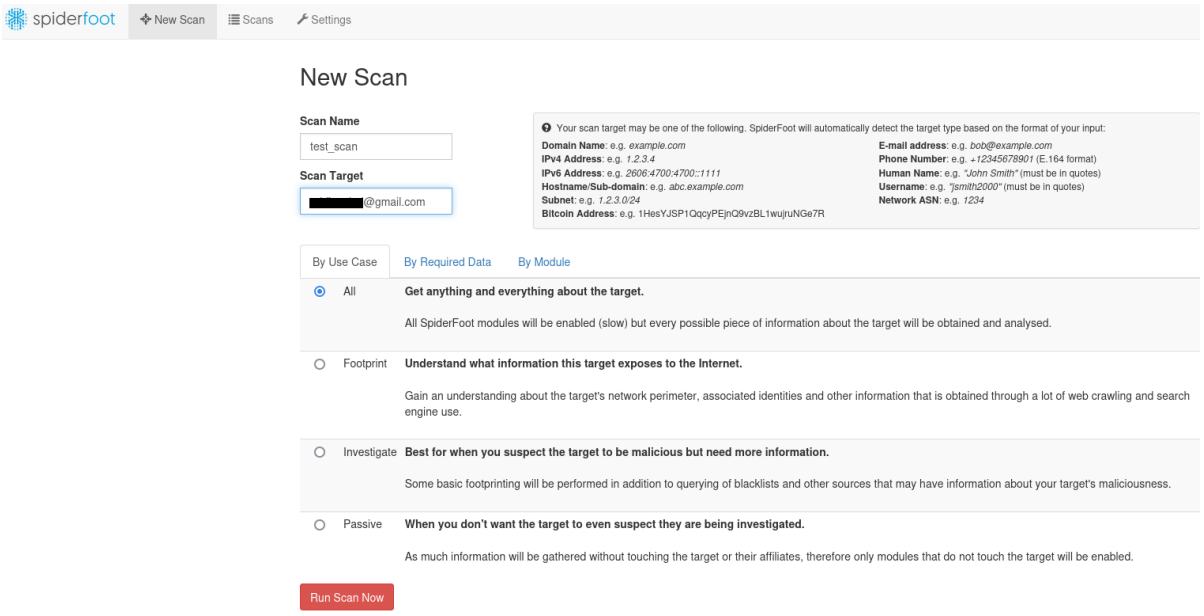

Figura 4.6: Formulario de búsqueda de SpiderFoot

En la pestaña «Settings» (figura 4.7) es posible ver los módulos de uso gratuito y de uso restringido (van identificados con un candado) si bien estos segundos no son todos de pago, sí es necesario registrarse para utilizarlos mediante una API key.

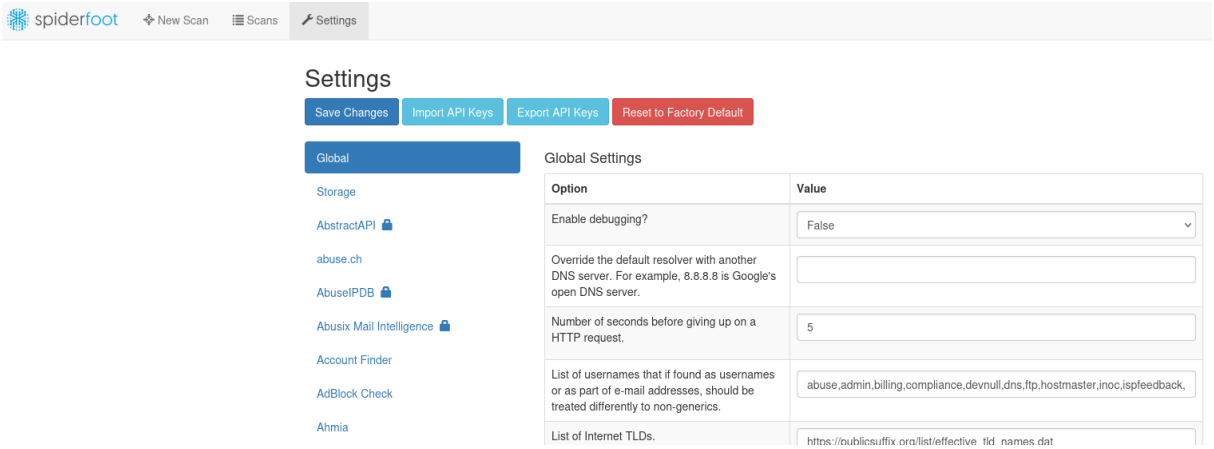

Figura 4.7: Configuración de los módulos de SpiderFoot

Una vez terminado el proceso, se obtiene un gráfico representativo con los porcentajes de datos obtenidos de cada fuente (figura 4.8). Pulsando en el botón «Browse» (figura 4.9) se accederá al menú con la información de todas las tipologías de datos. Pulsando en «Raw Data from RIRs/APIs» se obtienen los datos en crudo [61] de la dirección investigada (figura 4.10), siendo especialmente significativos los del módulo `sfp_emailrep` entre otros:

- Violaciones de datos en las que ha estado implicada.
- Reputación en la red.
- Primera y última vez en ser detectada en una violación de datos.
- Detección reciente (en los últimos 90 días) en una violación de datos.
- Fecha de creación.
- Conducta registrada por la dirección de correo (por ejemplo, envío de mensajes spam) lo cual puede ser un indicativo de que las credenciales están siendo utilizadas y hay que modificarlas cuanto antes.
- El proveedor de correo es gratuito.

- Política de aceptación de correos.
- Posibilidad de ser suplantada (spoofable).
- Perfiles de redes sociales en los que está siendo utilizada.

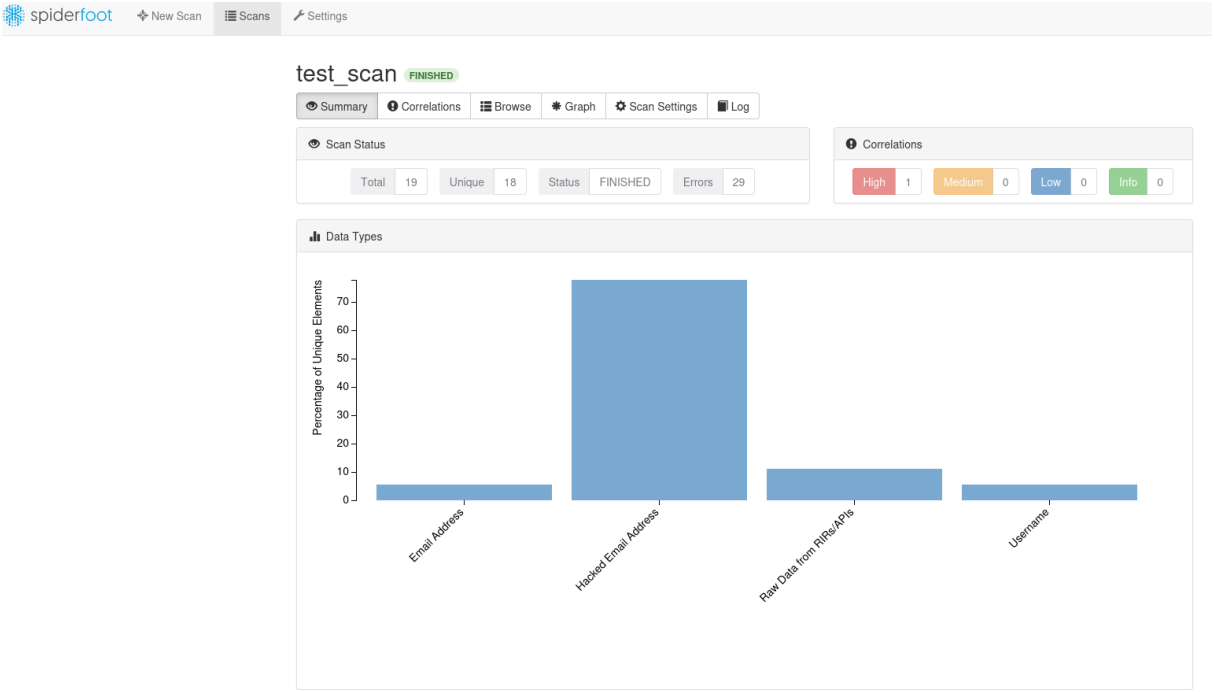

Figura 4.8: Gráfico porcentual de tipos de datos de SpiderFoot

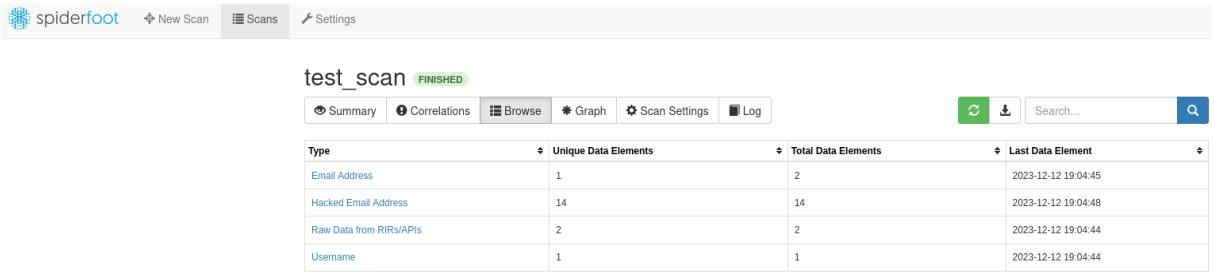

Figura 4.9: Menú browse de SpiderFoot

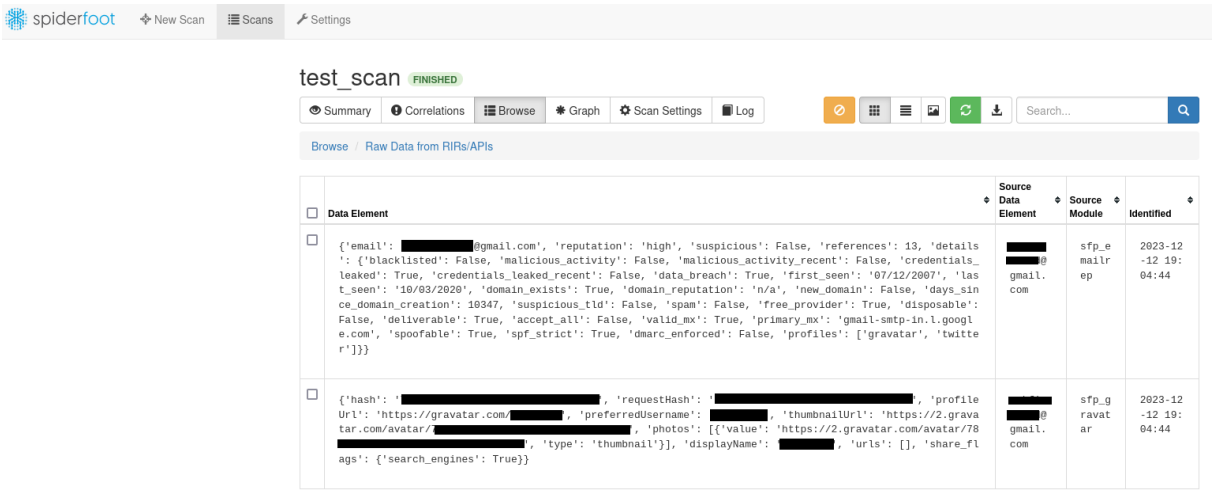

Figura 4.10: Datos en crudo de la dirección de correo investigada

Es de especial interés el módulo `sfp_ahmia` puesto que permite realizar búsquedas en la Dark Web y detectar aquellas webs donde se haya podido estar tratando de comerciar con los datos filtrados. Estos resultados pueden verse pulsando el botón «Log» (figura 4.11) y se muestran a modo informativo. Sería necesaria una investigación en mayor profundidad en la Dark Web, pero este campo queda fuera de los objetivos y la planificación de este trabajo.

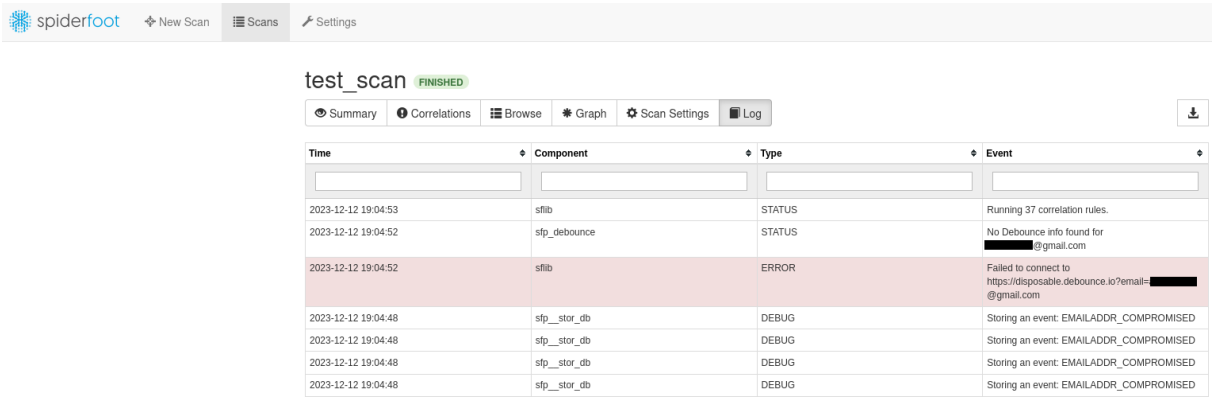

Figura 4.11: Log del análisis realizado por SpiderFoot

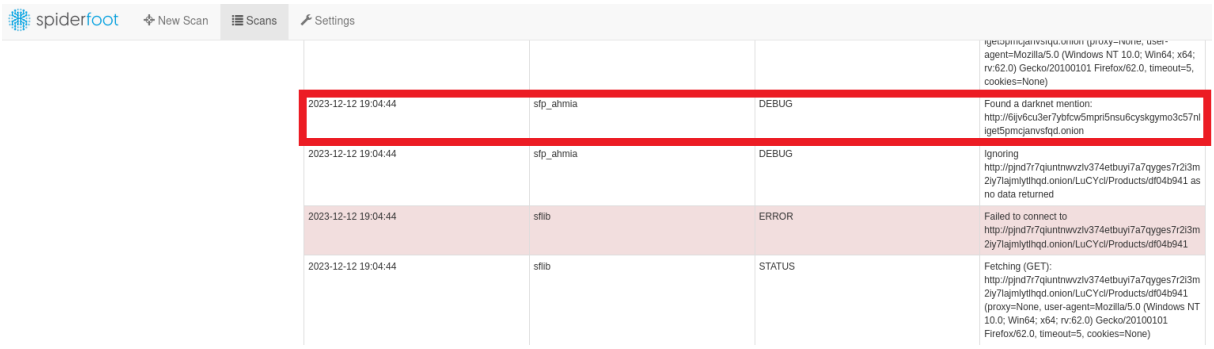

Figura 4.12: Mención encontrada en la Dark Web

4.1.2. Uso de Sherlock para búsqueda de nombres de usuario

Tal como se ha comentado en el subapartado 3.5.2., Sherlock es un herramienta de gran interés a la hora de encontrar nombres de usuario a través de distintas redes sociales que, hasta la fecha son 396 según se indica en la web del proyecto [62]. En este caso de estudio, el objetivo va a ser doble: localizar todas aquellas redes sociales en las que el usuario tenga perfil creado y, además, aquellas en las que dicho usuario pudiera disponer de perfil creado de forma involuntaria por algún agente malicioso para hacerse pasar por él. Esto puede deberse a causa de un ataque de suplantación de identidad. El comando que se introducirá por consola es el siguiente:

```
$ sherlock -v -t --nsfw user
```

Mediante ese comando, el programa devolverá todas aquellas redes sociales en las que el usuario disponga de un perfil con el nombre que le indiquemos (en este caso, user). Además de esto, con los argumentos `-v`, `-t` y `--nsfw` se solicitará al programa que funcione en modo verboso, que realice su búsqueda en la red Tor y que busque también en páginas de contenido para adultos, respectivamente. De este modo, se ampliarán los resultados obtenidos. En la figura 4.13 puede verse el comando introducido, así como el resultado devuelto por Sherlock.

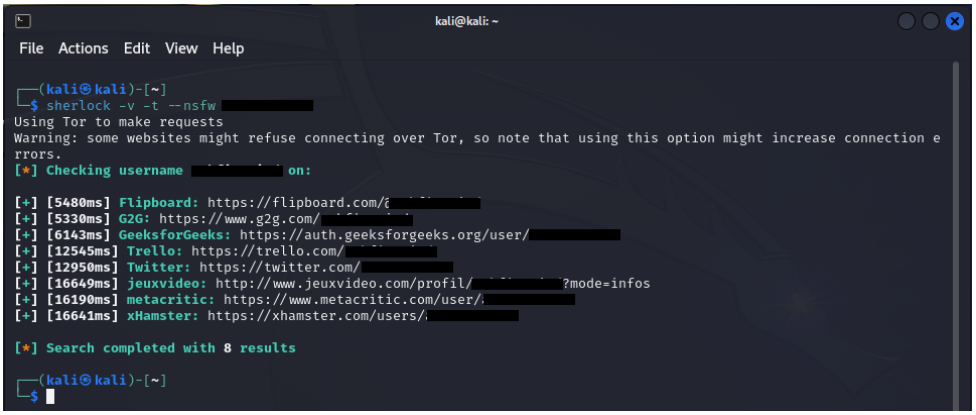

Figura 4.13: Resultados porporcionados por Sherlock

4.2. Obtención de información pública de dominios web

En este caso de estudio, se van a utilizar las aplicaciones theHarvester y Spiderfoot para realizar una búsqueda de información sobre personas. El dominio elegido es la web de la Diputación de Alicante[1] y, tras realizar una primera búsqueda con theHarvester, los resultados obtenidos se detallan en el apéndice C. El comando introducido por consola es:

```
$ theHarvester -d diputacionalicante.es -l 500 -b all -f diputacionalicante.html
```

Con este comando se realizará una búsqueda en todos los módulos preconfigurados por defecto en la aplicación y se guardarán los resultados en un archivo HTML. De dicho análisis se obtienen 40 direcciones de correo electrónico que podrán ser utilizadas para complementar la información que se obtendrá mediante SpiderFoot. En este caso, el funcionamiento es idéntico al de caso anterior; simplemente hay que introducir el dominio sobre el que queremos realizar la búsqueda (diputacionalicante.es) y pulsar en «Run Scan Now». Ahora se seleccionará la configuración «Understand what information this target exposes to the internet» para evaluar la superficie de ataque [63] [64] y la información expuesta del dominio. También se elige esta opción porque el tiempo de análisis es menor, sin embargo, llevó 25 horas y 36 minutos realizarlo (figura 4.14).

[1]https://www.diputacionalicante.es/

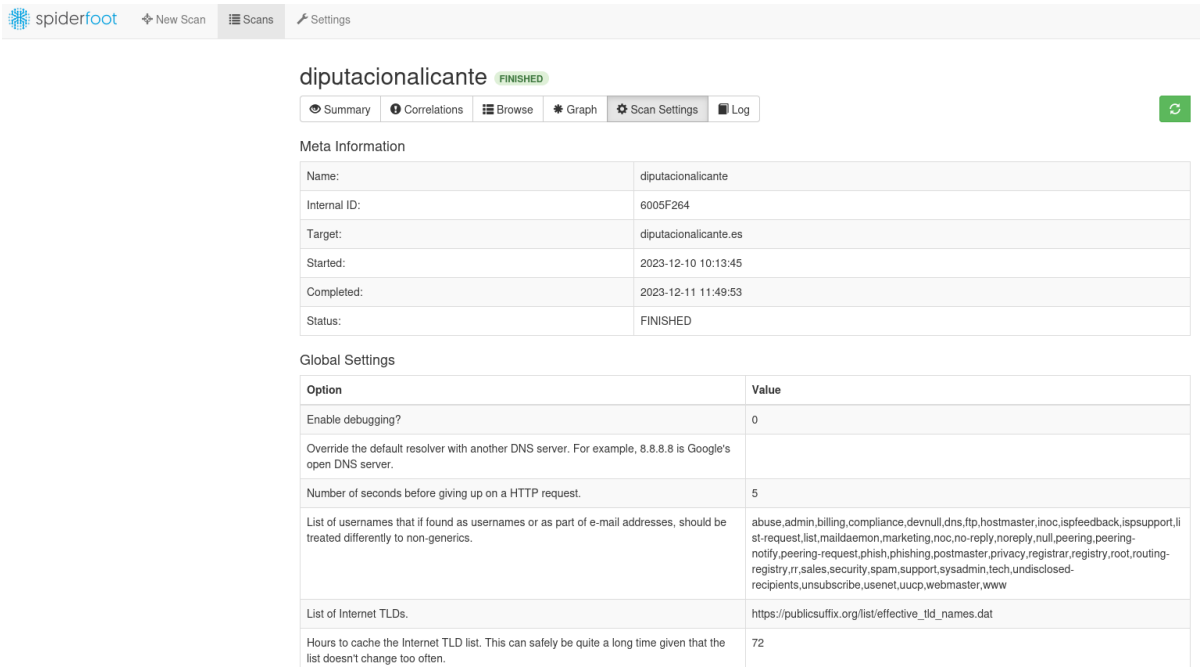

Figura 4.14: Ajustes y tiempo de análisis de la web de la Diputación de Alicante

En este caso, los tres resultados porcentuales más abundantes son los enlaces a las URLs internas, metadatos obtenidos y archivos de interés, en orden descendente.

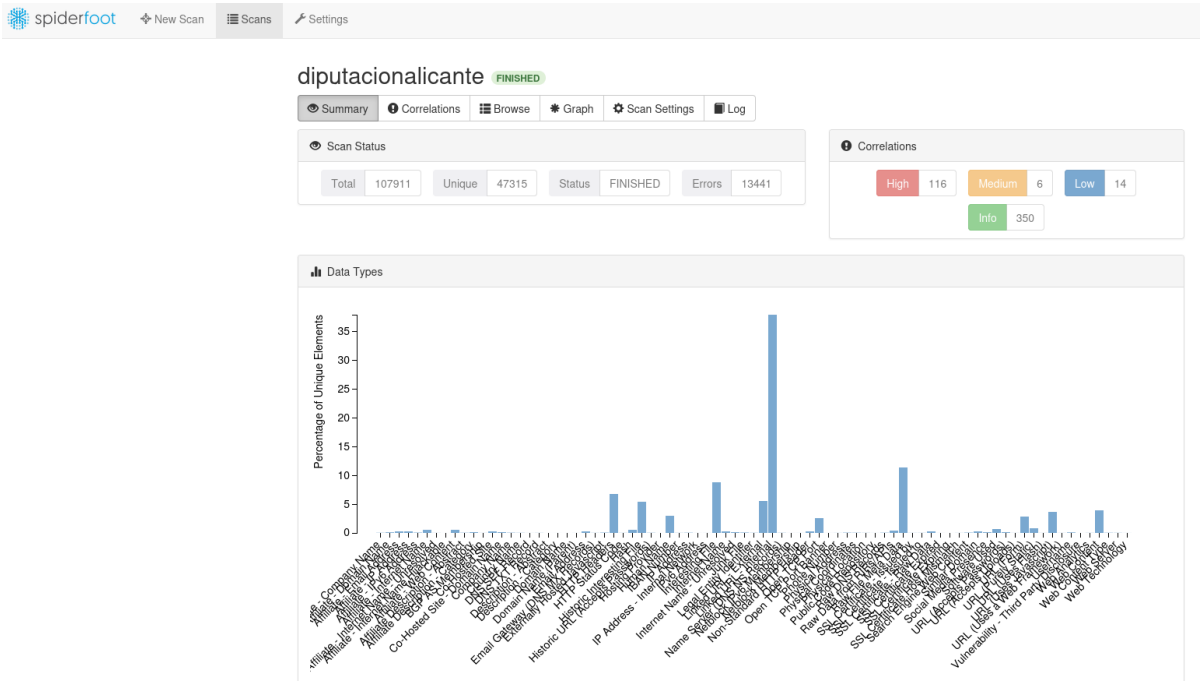

Figura 4.15: Volumen porcentual de datos obtenidos de la web de la Diputación de Alicante

Pulsando en «Correlations» (figura 4.16) pueden verse los resultados de los análisis que cada módulo ha realizado, con información concreta de su significado si se pulsa en el link o en el símbolo de interrogación de cada línea.

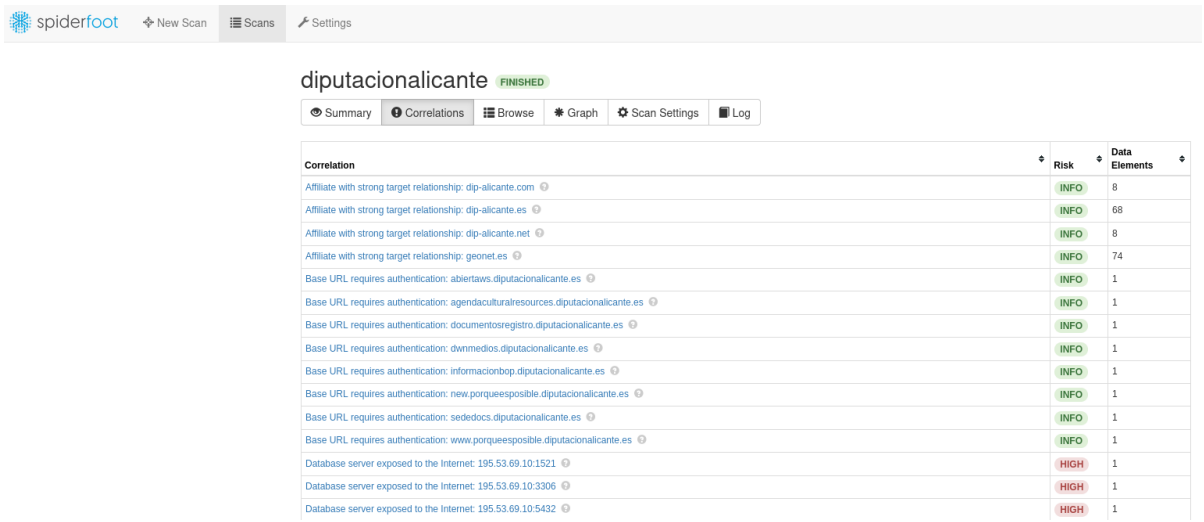

Figura 4.16: Correlaciones de SpiderFoot

En este caso, en el apartado «Browse» se obtiene una gran cantidad de datos de interés, tales como nombres de dominio, servidores de correo, direcciones IP internas y un largo etcétera.

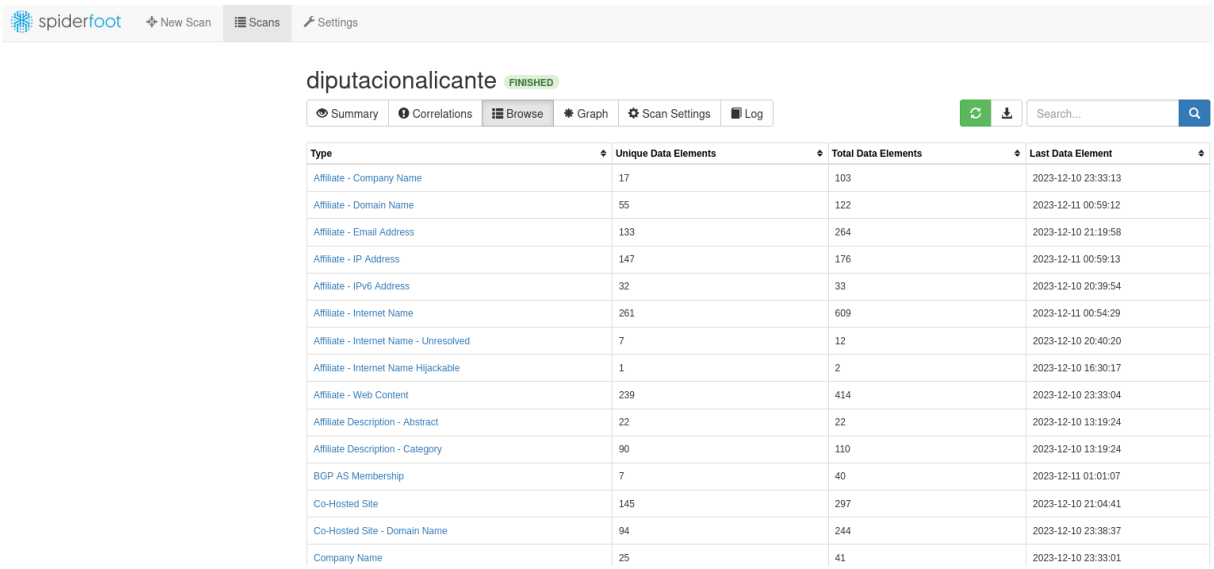

Figura 4.17: Menú de datos obtenidos de la web de la Diputación de Alicante

Para ir concluyendo con este caso, resulta de gran interés –a la par que alarmante– la gran cantidad de direcciones de correo (109 únicas) que están expuestas públicamente; algunas de ellas incluso propias de cargos públicos. No parece esta la mejor política de seguridad, ya que es una puerta de entrada a ataques de ingeniería social y email spoofing entre otros.

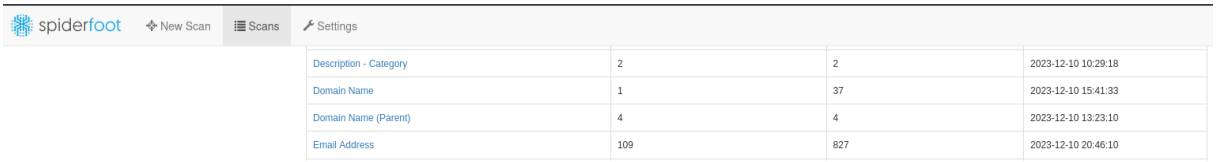

Figura 4.18: Resultados de direcciones de correo expuestas

4.2.1. Datos de personajes públicos en la red

Para concienciar sobre la cantidad de datos expuestos que pueden obtenerse a partir de una dirección de correo, bastaría con seleccionar alguna dirección (figura 4.19) y, mediante un simple ejercicio de Google Dorking (figura 4.20), realizar una búsqueda sistemática sobre los datos del usuario.

Figura 4.19: Dirección elegida al azar de un cargo político

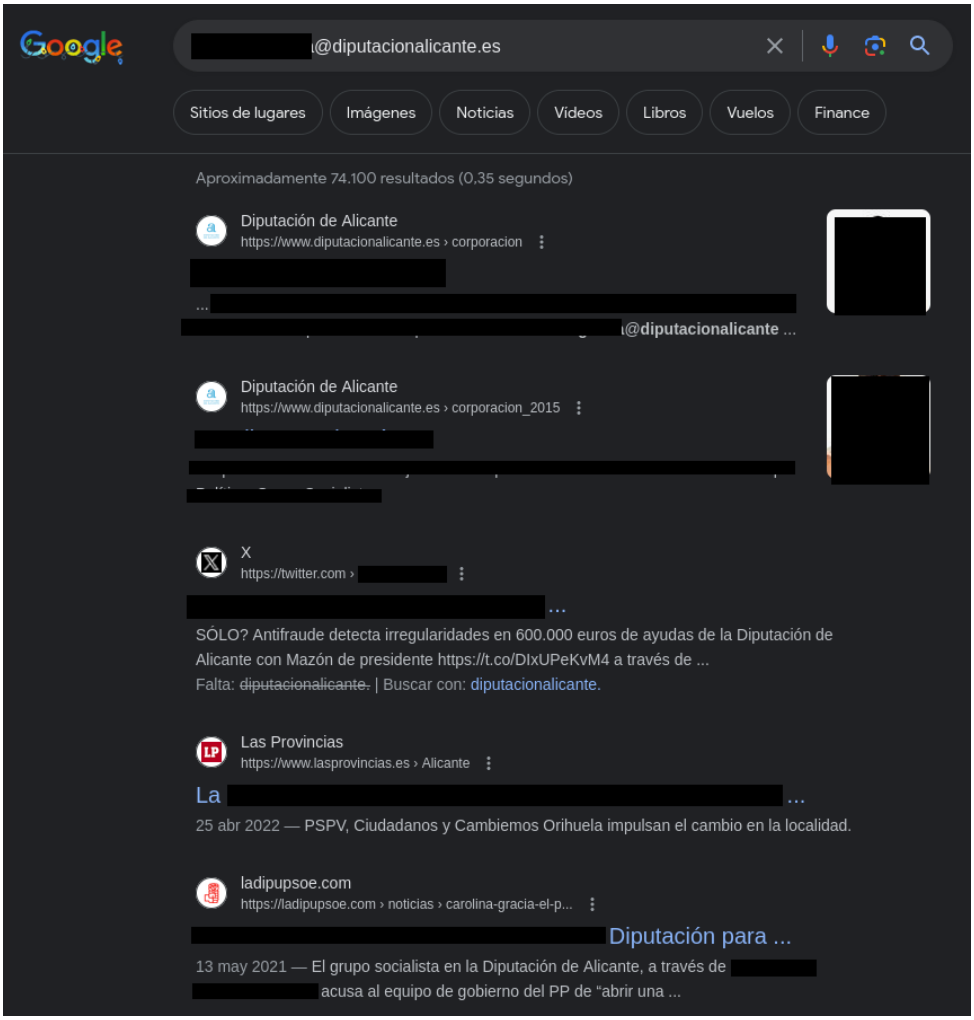

Figura 4.20: Búsqueda en Google de la dirección expuesta

Como ha podido verse, resulta muy sencillo ir accediendo a los diferentes resultados que ofrece el buscador y recopilar información sobre el cargo político (figura 4.21) y no sólo en referencia a su filiación política, sino también a su formación académica, sueldo, y demás datos sensibles. Si bien estos pueden formar parte de la política de transparencia asociada al cargo, esto no quita que puedan ser utilizados por organizaciones delictivas. Siguiendo con la información obtenida de Google, puede verse que el político también dispone de cuenta de Twitter (figura 4.20 tercer resultado) de donde podrá obtenerse información sobre opiniones, rutinas, lugares visitados y otras costumbres o aficiones.

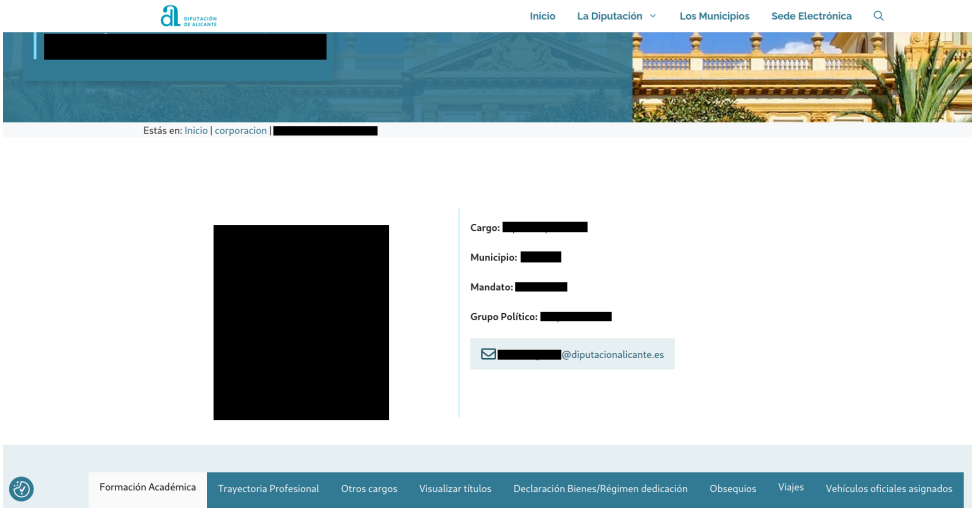

Figura 4.21: Perfil público del político

Como último paso, haciendo uso de la herramienta Sherlock y, habiendo obtenido el nombre de usuario de Twitter de dicho político, podrá hacerse una búsqueda en otras redes sociales para ampliar información, hallando el resultado expuesto en la figura 4.22. Hecho esto, se tendrá la posibilidad de obtener más información según se desee.

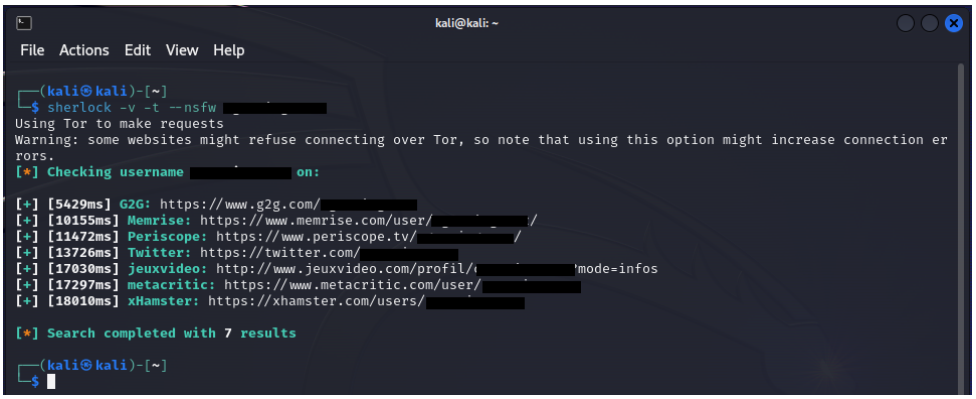

Figura 4.22: Resultados de Sherlock con el usuario de Twitter del cargo político

Finalmente, cabe reseñar tambien que se han detectado 1228 puertos TCP abiertos mediante el módulo `sfp_portscan_tcp` lo cual, al priori no tiene por que ser peligroso siempre y cuando estén supervisados [65]. En caso contrario, pueden ser víctimas potenciales de accesos no autorizados, intrusiones en la red, robos y filtraciones (en los casos de las bases de datos) y ataques de denegación de servicio DDoS.

Capítulo 5

Conclusiones y trabajos futuros

Después de toda la tarea de investigación realizada, puede concluirse que la ciberinteligencia revela la esencia crítica de este campo en el panorama actual. Subestimar su relevancia podría resultar en consecuencias devastadoras. La falta de atención a la OSINT abre la puerta a vulnerabilidades, exponiendo a personas, empresas y gobiernos a amenazas cibernéticas y de seguridad. La omisión de su valor podría significar una pérdida significativa de datos sensibles, el compromiso de la privacidad, el aumento del riesgo de ciberataques y la erosión de la confianza en las plataformas digitales.

Poniendo el foco a nivel de usuario, pese a que los términos ciberinteligencia y OSINT pudieran sonar hollywoodenses, desestimar su importancia puede tener consecuencias directas y graves. Ignorar la ciberinteligencia implica no estar al tanto de posibles amenazas en línea, como estafas, ataques de phishing o robo de identidad. Esto puede resultar en la pérdida de información personal, financiera o sensible. Por otro lado, subestimar la OSINT, como la información disponible públicamente en redes sociales o sitios web, puede exponer a los usuarios a riesgos de privacidad. La sobreexposición de datos personales en línea podría ser aprovechada por ciberdelincuentes para ataques dirigidos o incluso para perjudicar la reputación en línea.

Ya en un contexto más personal, ha resultado inquietante conocer la facilidad con la que se puede obtener información específica de un dominio web mediante herramientas de software libre y con un funcionamiento sencillo. Sumado esto al factor de la creciente ciberdelincuencia actual [66], convierten todavía más la ciberseguridad en una máxima a tener en cuenta ya no sólo por las grandes empresas, sino también por los pequeños negocios, entes públicos y personas.

En resumen, no prestar atención a la ciberinteligencia y a la información disponible públicamente puede dejar a los usuarios vulnerables a diversos riesgos cibernéticos, desde la pérdida de datos hasta la manipulación de la identidad digital, destacando la necesidad crítica de estar informado y tomar medidas proactivas para protegerse en el entorno digital.

5.1. Seguimiento de la planificación inicial

Al finalizar el proyecto se puede considerar que, en líneas generales ha tenido un seguimiento satisfactorio, detectándose únicamente leves desviaciones en la fase de desarrollo de la investigación y en la de los casos de uso.

En primera instancia, la fase de investigación tuvo un desajuste de los hitos debido a que se dedicó demasiado tiempo y esfuerzo al desarrollo de los conceptos de ciberinteligencia y tipología de la información, restando esto tiempo para realizar una identificación más detallada sobre los riesgos de las redes sociales.

En cuanto a la fase de exposición de resultados, se considera que ha tenido un seguimiento adecuado y se ha podido presentar con la calidad y la concreción planificadas. Aunque surgió un imprevisto con el sistema operativo elegido para el despliegue de la máquina virtual, se pudo responder con eficacia aportando una alternativa igualmente funcional. En todo caso se ha tenido presente el plazo de entrega y ha sido posible dedicar el esfuerzo previsto en cuanto a horas.

Finalmente, la fase de casos de uso sufrió también un desajuste en los hitos debido a que la selección y aprendizaje de las herramientas seleccionadas llevó mayor tiempo de lo esperado. A causa de esto, quedó menos tiempo del deseable para realizar un análisis más profundo de los datos obtenidos. También se decidió unir este hito con el de buenas prácticas y lecciones aprendidas, ya que del análisis de los datos se van desprendiendo estas y se va incidiendo en ellas.

5.2. Evaluación de los objetivos alcanzados

Realizando un análisis de los objetivos iniciales del trabajo, puede desprenderse que, el producto obtenido se ajusta a lo planificado. Además de esto se ha podido ampliar el alcance ya que, incluso se ha realizado un análisis de un dominio web, lo cual no estaba planificado inicialmente. No obstante, se ha considerado igualmente

interesante en aras de una mayor divulgación.

También se ha conseguido realizar una configuración suficientemente segura del sistema que se ha utilizado para realizar las investigaciones, siendo este el aspecto en el que más se ha incidido a lo largo del capítulo 3. En todo momento se ha buscado software de uso gratuito y sencillo que esté al alcance de todos los usuarios para poder así ofrecer un enfoque realista, accesible a todos y cercano al lector.

En definitiva, se ha buscado ir más allá de lo planificado tratando de dar al cliente más de lo esperado; si bien teniendo en mente en todo momento que una dedicación excesiva de recursos puede ser también contraproducente en caso de que el presupuesto o los medios sean ajustados. En este caso no se tenía un límite presupuestario, pero sí uno temporal.

5.3. Dificultades encontradas

Durante el desarrollo del presente TFG se han encontrado las siguientes dificultades:

- La variedad de fuentes disponibles en el ámbito de la ciberinteligencia (libros, artículos, trabajos, vídeos o páginas web) ha generado la dificultad de discernir cuál de ellas contiene la información más actualizada, precisa y significativa para el propósito del trabajo. Esta diversidad también amplía el panorama de posibilidades, pero al mismo tiempo, aumenta la complejidad de evaluar la confiabilidad y relevancia de cada fuente, lo que agrega un nivel adicional de dificultad al proceso de selección.

- La rápida evolución del estado del arte de la ciberinteligencia ha supuesto también un importante desafío. La dinámica naturaleza de este campo ha revelado la importancia crítica de la formación continua y la adaptabilidad para poder abordar los desafíos emergentes con eficacia.

- Aunque inicialmente se tenía previsto utilizar un sistema Linux Ubuntu por su mayor soporte a largo plazo, hubo que descartar esta opción a causa de la complejidad encontrada durante la instalación y funcionamiento de algunas herramientas de OSINT. Teniendo siempre en mente la mayor democratización posible, se ha perseguido no complicar demasiado la instalación de dichas herramientas cuando ya se disponía de otro sistema operativo de instalación sencilla

como Kali Linux que ya las tenía instaladas por defecto. Este también es de gran implantación, además de menor consumo de recursos, ampliando así el acceso a un mayor número de usuarios potenciales.

- Dentro del amplio espectro de herramientas de OSINT disponibles, la tarea de seleccionar el software adecuado ha representado un desafío significativo. La dificultad ha radicado en encontrar una solución que no solo proporcione datos relevantes y actualizados, sino que también sea fácil de utilizar, gratuito y, fundamentalmente, evite la redundancia de información proporcionada por las distintas herramientas.

- A pesar de los esfuerzos por condensar y seleccionar la información más relevante y significativa, la amplitud y la riqueza de datos en el campo de la ciberinteligencia han hecho complicada la tarea de mantener el contenido dentro del límite de páginas establecido. Esto resalta la magnitud y complejidad de la ciberinteligencia como disciplina, donde la abundancia de datos valiosos a menudo dificulta la síntesis concisa pero exhaustiva en un espacio limitado.

5.4. Trabajos futuros

Tras la realización de este TFG y, en la búsqueda constante por mejorar las habilidades en seguridad informática, el interés por dominar Kali Linux se ha convertido en una prioridad. Todo este esfuerzo ha servido para reconocer su importancia como una poderosa herramienta para realizar investigaciones y pruebas de todo tipo, ofreciendo un amplio abanico de aplicaciones y comandos específicos que permiten evaluar la seguridad de sistemas y redes. Profundizar en el conocimiento de Kali Linux no solo implicará adquirir destrezas técnicas, sino también entender las vulnerabilidades y cómo proteger activamente contra potenciales amenazas cibernéticas.

Asimismo, la exploración de SpiderFoot como una herramienta especializada en inteligencia de fuentes abiertas representa una vertiente complementaria e igualmente esencial. Su capacidad para recopilar información proveniente de diversas fuentes en la web es invaluable para investigaciones en seguridad y análisis de amenazas. Aprender a utilizarla implica entender la profundidad y riqueza de los datos disponibles públicamente, proporcionando una visión amplia y detallada para evaluar posibles riesgos y fortalecer la postura de seguridad.

Finalmente, como resultado complementario a toda esta investigación, la Dark Web,

como fuente potencial de datos exfiltrados y actividad cibernética clandestina, también ha empezado a despertar un genuino interés en el proceso de aprendizaje. Reconociendo su complejidad y los desafíos inherentes, el deseo de comprender más sobre su funcionamiento y cómo se pueden extraer datos relevantes de manera ética se vuelve un objetivo de investigación fascinante y pertinente en el panorama de la ciberseguridad actual.

Así pues, como se ha perseguido a lo largo de todo este trabajo, la divulgación e investigación sobre la OSINT, Kali Linux y, de forma complementaria la Dark Web, converge en el fomento de la comprensión y el control sobre los aspectos más oscuros y complejos de la tecnología. La exploración de la Dark Web resalta la importancia de entender sus riesgos y potenciales beneficios, mientras que la OSINT proporciona herramientas para recopilar información valiosa en entornos públicos en línea, incluyendo la Dark Web. Kali Linux, como sistema operativo especializado en seguridad, se convierte en una herramienta fundamental para aquellos que buscan comprender y protegerse en estos entornos, permitiendo la experimentación ética y la evaluación de la seguridad en línea. Juntos, estos temas subrayan la necesidad de la educación y el conocimiento en un mundo digital cada vez más complejo y desafiante.

Glosario

- **Amenaza** *f* Toda acción que se aprovecha de una vulnerabilidad.
- **Amenaza cibernética** *f* En el contexto de este trabajo se refiere a todas aquellas técnicas utilizadas para aprovechar las vulnerabilidades externas que se puedan encontrar en el ciberespacio a partir de la información obtenida para llevar a cabo ciberataques.
- **Analista** *m y f* En el contexto de este trabajo, persona especializada en llevar a cabo análisis informáticos y de ciberinteligencia.
- **API** Siglas en inglés de Application Programming Interface o interfaz de programación de aplicaciones. Permite la interacción entre aplicaciones, permitiendo de esta manera consumir o adquirir por medio de instrucciones dadas información de una aplicación.
- **Ciberalfabetización** *f* Término de reciente acuñación que significa tener la capacidad de usar la tecnología informática y comprenderla de una forma correcta.
- **DDoS** Ataque de denegación de servicio distribuido. Es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos.
- **Democratización** *f* Proceso de fortalecimiento de los mecanismos diseñados con el objeto de involucrar a los ciudadanos y organizaciones de la sociedad civil en la formulación, ejecución, control y evaluación de la gestión pública y brindar transparencia al ejercicio de la función administrativa. En este TFG se ha tomado este término con una dimensión orientada hacia el campo de la ciberinteligencia al no existir otro más específico.
- **Hiperconectividad** *f* Término utilizado actualmente para definir la elevada co-

nectividad que existe en el entorno digital y la interacción entre sistemas de información, datos y dispositivos.

- **Internet de las cosas** *m* También conocido como IoT o Internet of Things, es el proceso que permite conectar los elementos físicos cotidianos a Internet: desde los objetos domésticos comunes tales como bombillas, hasta los recursos para la atención de la salud, prendas y accesorios personales inteligentes, e incluso los sistemas de las ciudades.
- **ISP** Proveedor de servicios de internet. Este término es asociado a las organizaciones que prestan servicios de internet.
- **OSINT** Acrónimo utilizado en el documento que se define como Open Source Intelligence o inteligencia de fuentes abiertas.
- **Pirata informático** *m* Definición dada a las personas con grandes habilidades y altos conocimientos en ciberseguridad.
- **Spiderfoot** Herramienta desarrollada para llevar a cabo investigaciones de tipo OSINT.
- **Superficie de ataque** *f* Suma de vulnerabilidades, vías o métodos –a veces llamados vectores de ataque– que los hackers pueden utilizar para obtener acceso no autorizado a la red o a datos confidenciales, o bien para perpetrar un ciberataque.

Apéndice A

Instalación de la máquina virtual Kali Linux en Oracle VM VirtualBox

Una vez instalado VirtualBox y su correspondiente Extension Pack, hay que descomprimir la máquina virtual Kali Linux preconstruida y añadirla pulsando el botón «añadir».

Figura A.1: Pantalla de bienvenida de VirtualBox

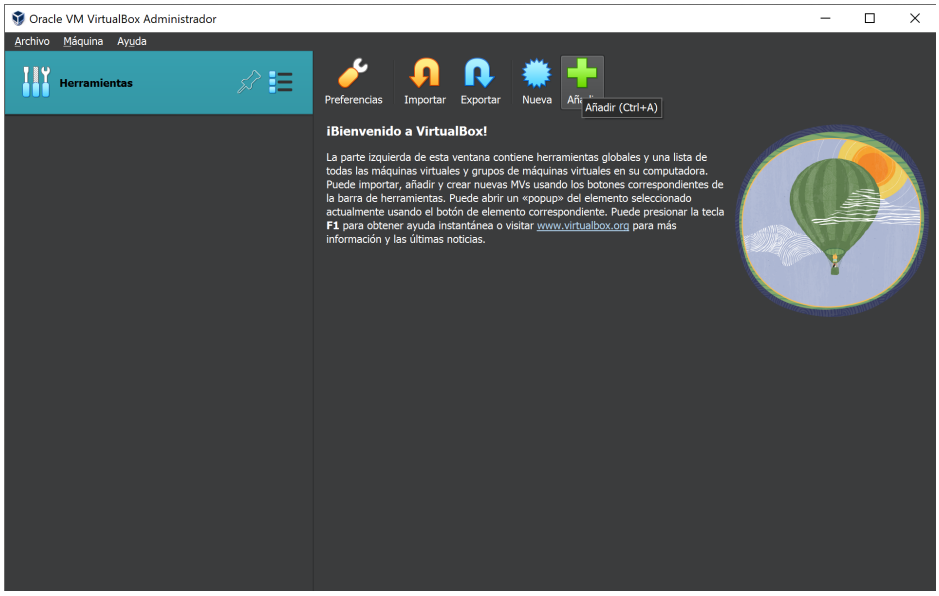

Figura A.2: Ubicación del botón para añadir una nueva máquina virtual

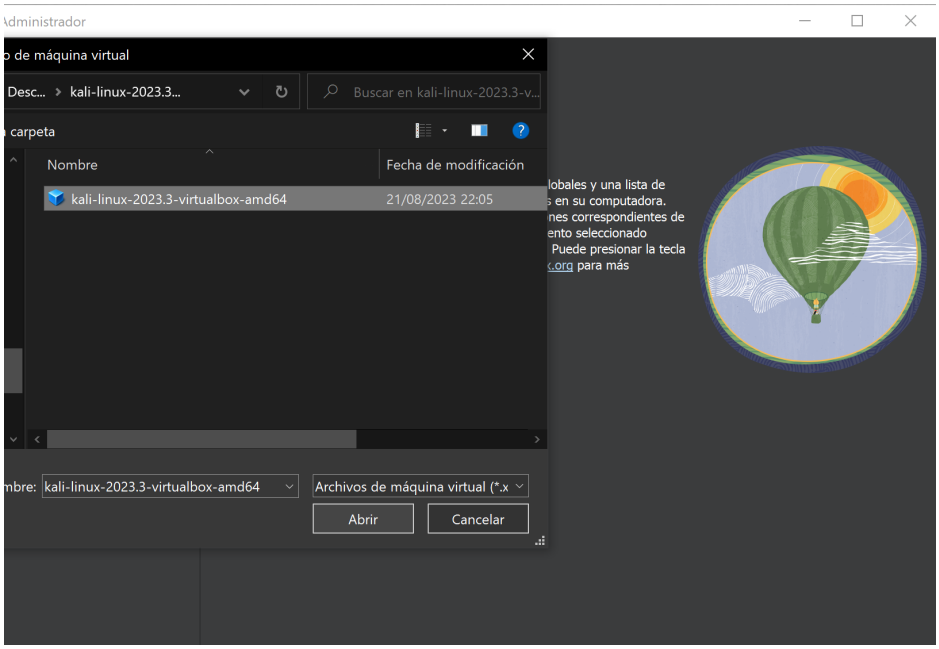

Figura A.3: Selección del archivo de máquina virtual

Una vez aparezca la máquina virtual en la lista de VirtualBox, hay que seleccionarla y pulsar el botón «iniciar».

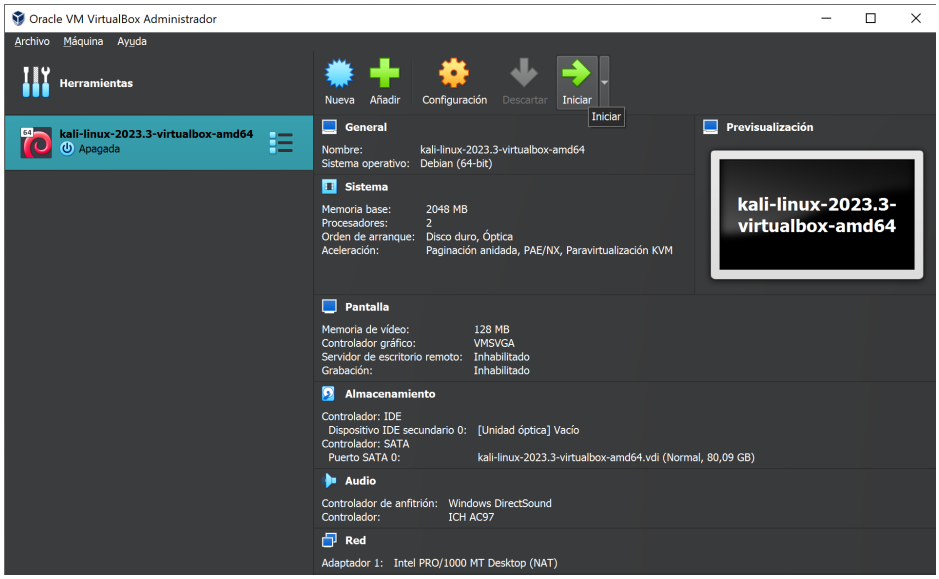

Figura A.4: Seleccion e inicio de la máquina virtual

Después del proceso de inicio, aparecerá la pantalla de login (figura A.5), para lo cual habrá que introducir nombre de usuario y contraseña. Ambos dos serán «kali» sin las comillas.

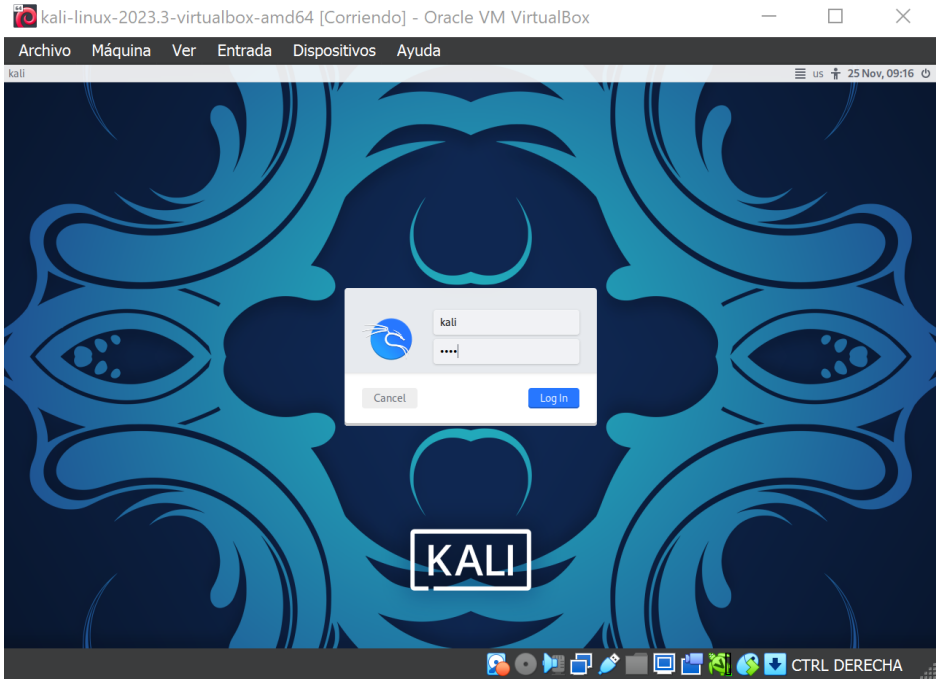

Figura A.5: Pantalla de login de Kali Linux

En caso de que el monitor que se esté utilizando tenga una densidad de píxeles elevada, VirtualBox permite la posibilidad de escalar un 200 % la salida por pantalla para ver el escritorio con mayor tamaño (figura A.6).

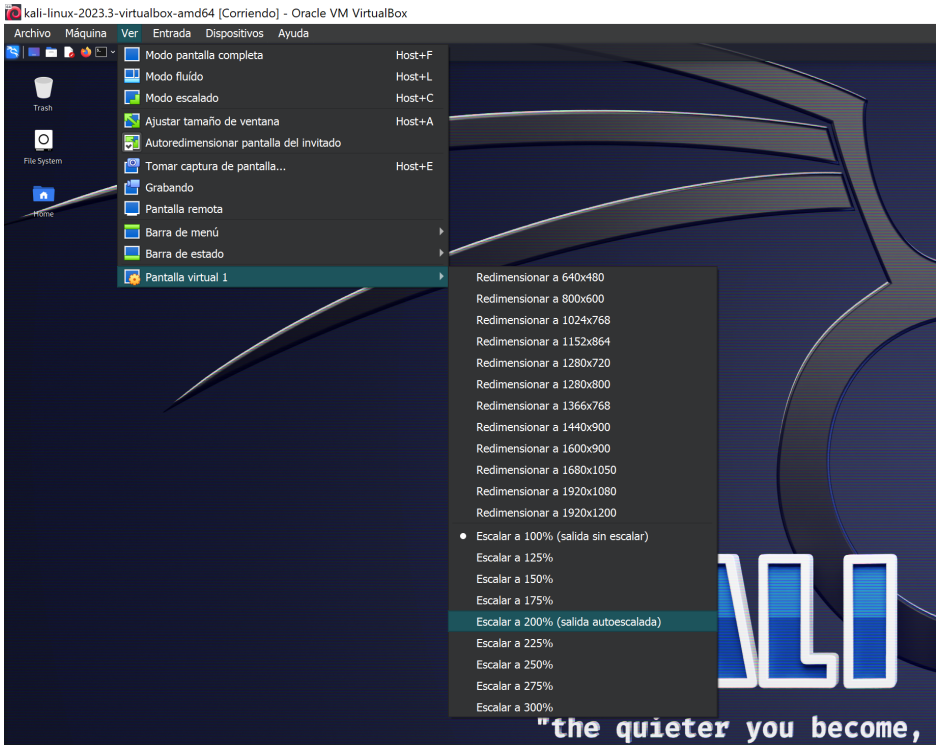

Figura A.6: Escalado de pantalla

Por defecto, la máquina virtual viene configurada con el teclado en inglés, por lo que será necesario configurarlo en español en el menú «settings», deseleccionar los «system defaults», añadir el teclado español pulsando el botón «+» y eliminando el inglés, tal como se muestra en las figuras A.7, A.8 y A.9:

Figura A.7: Búsqueda en el menú de los ajustes del sistema

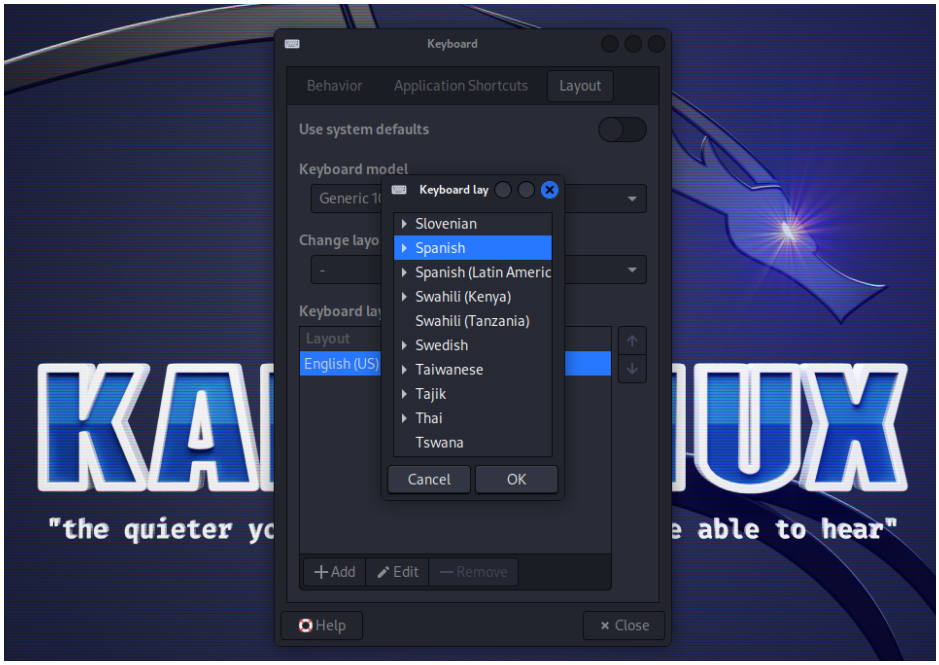

Figura A.8: Desactivación y selección del teclado español

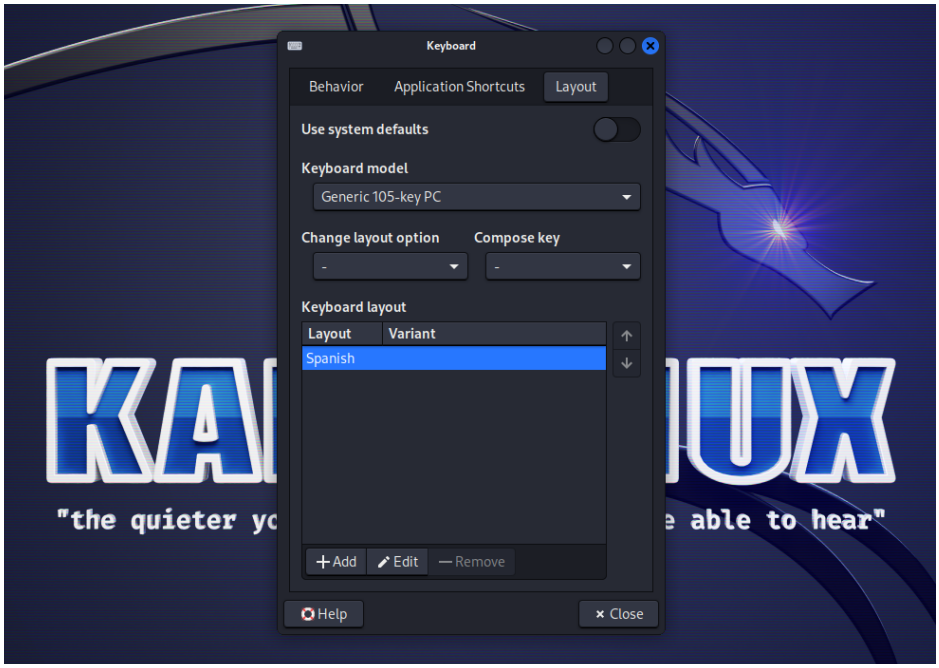

Figura A.9: Ajuste del teclado por defecto del sistema

Una vez realizados todos estos pasos, la máquina virtual estará lista para realizar las investigaciones de ciberinteligencia planificadas en este TFG.

Apéndice B

Conceptos básicos sobre la información

B.1. Formatos de la información y su representación

Como va a verse a continuación, existe gran diversidad de formas de almacenar la información en los equipos informáticos. Esto se determina a través de las extensiones .txt o .zip por poner tan solo dos ejemplos. Resulta difícil de determinar el número exacto de extensiones existentes puesto que cada día aparecen nuevos tipos, sin embargo, se estima que superan ya los 10.000 [67]. Para tratar de normalizar esta situación, la biblioteca del Congreso de los Estados Unidos[1] dispone de una declaración de formatos recomendados para todo tipo de archivos [68], ya sean digitales o analógicos. El objetivo del mismo es maximizar las opciones de supervivencia y accesibilidad continua de ese contenido de cara al futuro. Dicho esto, el presente TFG únicamente se centrará en los formatos de información más comunes y fáciles de acceder, analizar y conseguir.

B.1.1. Formato de texto plano

La extensión de este formato es .txt o .text y, se podría definir como aquel que –a diferencia del formato binario compuesto por unos y ceros– está formado únicamente por caracteres legibles para las personas y, que además carece de cualquier tipo de formato tipográfico tal como negrita, cursiva o tipos de letra [69]. Estos archivos están compuestos de bytes que representan caracteres ordinarios como letras, números y signos de puntuación así como de espacios en blanco. También incluyen algunos carac-

[1] https://www.loc.gov/

teres de control como tabulaciones, saltos de línea y retornos de carro. La codificación de estos archivos puede ser mediante el sistema ASCII, para el cual no sería necesario un identificador explícito en la comunicación digital. En el caso de otros sistemas de codificación de caracteres como los UTF-1, UTF-7, UTF-8 y sucesivos, es necesario que haya al principio de cada fichero de texto una marca de orden de bytes.

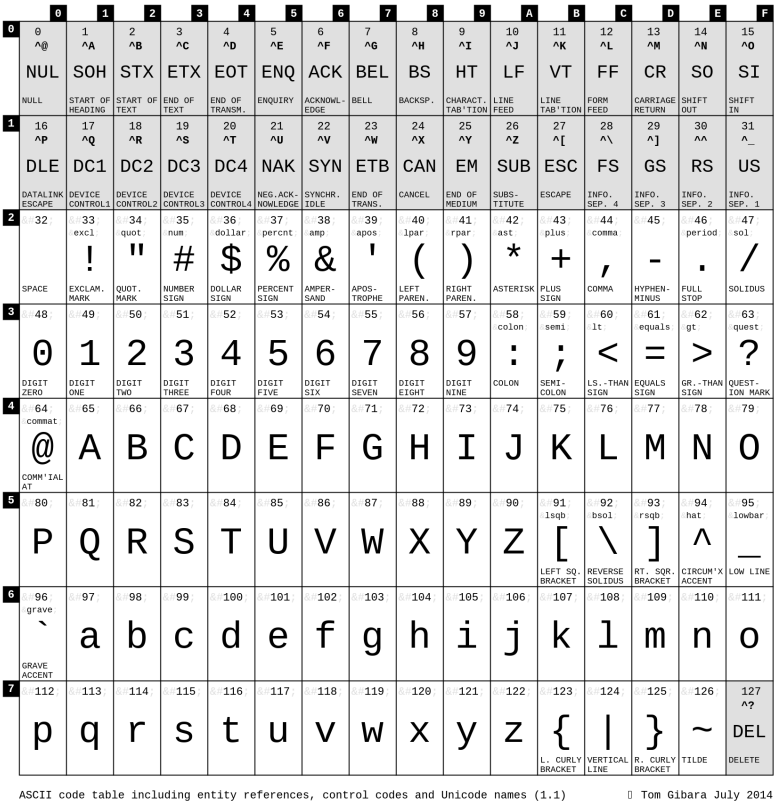

Figura B.1: Código de caracteres ASCII

B.1.2. Código binario

La totalidad de los archivos que se utilizan en los archivos informáticos están codificados en formato binario, puesto que esta es la forma en que se almacenan los datos en los soportes digitales así como la forma de trabajar bajo nivel de los ordenadores [70]. Sin embargo, únicamente se hace mención a este formato de almacenamiento de archivos a título informativo puesto que no se suele trabajar directamente sobre estos archivos al no ser un formato muy amigable para las personas. Debido a eso, se recurre a otros formatos más extendidos como se verá a continuación.

B.1.3. Archivos JSON

El formato JSON (pronunciado yéison) que corresponde con las siglas JavaScript Object Notation, está basado en texto y está ampliamente extendido como herramienta de intercambio de datos entre aplicaciones [71]. Este hecho lo ha convertido en un estándar de facto [19] y, segun la especificación oficial del RFC 7159 [72], un objeto JSON puede obtener atributos con uno de los siguientes tipos de datos:

- Cadenas de texto. Entrecomilladas, utilizando siempre comillas, pudiendo contener cero o más caracteres así como caracteres de escape.
- Booleanos. Que representan un atributo cuyo valor solamente puede ser verdadero indicado como true o falso indicado como false. Dichos valores nunca se ponen entre comillas puesto que, en ese caso equivaldrían a una cadena de texto de 4 y 5 caracteres respectivamente.
- Números. Utilizados para representar cantidades positivas o negativas. También se puede utilizar números decimales separando la parte decimal utilizando un punto.
- Objetos. Que se delimitarán por llaves y que contendrán una secuencia de elementos ordenados por clave-valor. Cada par clave-valor del objeto estará separado por una coma. Los objetos son elementos de cualquier tipo, por ejemplo, nombres y apellidos, direcciones web, coordenadas GPS y un largo etcétera.
- Listas o arrays. Que se utilizan para representar una lista ordenada de cero o más valores los cuales pueden ser de cualquiera de los tipos que se han citado anteriormente. Un array en JSON podría contener de forma combinada números o cadenas de texto de igual manera que los objetos se separan utilizando comas, pero en este caso se utilizan corchetes en vez de llaves.

```
1  Esto es un objeto JSON:
2
3       {
4         "Image": {
5             "Width":  800,
6             "Height": 600,
7             "Title":  "View from 15th Floor",
8             "Thumbnail": {
9                 "Url":    "http://www.example.com/image/481989943",
10                "Height": 125,
11                "Width":  100
12            },
```

```
            "Animated" : false,
            "IDs": [116, 943, 234, 38793]
          }
      }

Esto es un array JSON que contiene dos objetos:

      [
        {
           "precision": "zip",
           "Latitude":  37.7668,
           "Longitude": -122.3959,
           "Address":   "",
           "City":      "SAN FRANCISCO",
           "State":     "CA",
           "Zip":       "94107",
           "Country":   "US"
        },
        {
           "precision": "zip",
           "Latitude":  37.371991,
           "Longitude": -122.026020,
           "Address":   "",
           "City":      "SUNNYVALE",
           "State":     "CA",
           "Zip":       "94085",
           "Country":   "US"
        }
      ]
```

A título informativo, cabe indicar que los espacios, tabulaciones y saltos de línea son descartados por los parseadores de documentos JSON y, sin embargo, es práctica habitual representarlos de forma indentada para facilitar su lectura por las personas.

B.1.4. Archivos XML

El formato XML o .xml (eXtensible Markup Language) que, por sus siglas en inglés se traduciría como lenguaje de marcado extensible, se trata de un metalenguaje que se utiliza comúnmente para dar soporte a las bases de datos [73]. Al igual que el formato JSON permite almacenar los datos de forma legible. No obstante, su manejo es complicado debido a la gran cantidad de atributos y opciones que se pueden configurar. Su gramática es similar a la del lenguaje HTML ya que, cada objeto del fichero está ubicado entre dos marcas, una de comienzo y otra de fin que, además pueden contener atributos adicionales.

Las principales ventajas del XML serían que es extensible, lo cual significa que, después de diseñado es posible extenderlo con la adición de nuevas etiquetas y, como el

analizador es un componente estándar, no sería necesario crear un analizador específico para cada versión del lenguaje. En definitiva, como su formato es legible es sencillo entender su estructura y procesarla por parte de otras personas distintas a aquellas que crearon el documento y transformar dichos datos en información, facilitando así la flexibilidad de su transformación en documentos.

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE Edit_Mensaje SYSTEM "Edit_Mensaje.dtd">

<Edit_Mensaje>
     <Mensaje>
          <Remitente>
               <Nombre>Nombre del remitente</Nombre>
               <Mail> Correo del remitente </Mail>
          </Remitente>
          <Destinatario>
               <Nombre>Nombre del destinatario</Nombre>
               <Mail>Correo del destinatario</Mail>
          </Destinatario>
          <Texto>
               <Asunto>
                    Este es mi documento con una estructura muy sencilla
                    no contiene atributos ni entidades...
               </Asunto>
               <Parrafo>
                    Este es mi documento con una estructura muy sencilla
                    no contiene atributos ni entidades...
               </Parrafo>
          </Texto>
     </Mensaje>
</Edit_Mensaje>
```

Finalmente, como dato de interés, cabe indicar que su desarrollador fue el World Wide Web Consortium[2] (W3C) en el año 1999 [74]. Generalmente su uso en aplicaciones y herramientas ha caído en general en desuso debido a su complejidad y, en lugar de él se utilizan otros formatos como JSON o CSV, el cual se cita a continuación.

B.1.5. Archivos CSV

Los archivos CSV (acrónimo de Comma-Separated Values), están ordenados de forma que las columnas estarán separadas por comas y las filas por saltos de línea [75]. La estructura de estos ficheros de texto está estandarizada en el RFC 4180 [76]. También es posible utilizar comillas dobles para acotar los campos. En el caso de que el campo

[2]https://www.w3.org/

en cuestión contenga saltos de línea, comas o comillas dobles, será necesario utilizar comillas dobles para acotar.

Asimismo, también es habitual en muchos países europeos el uso del punto y coma (puesto que, en ellos es común utilizar la coma decimal) para delimitar los campos así como el símbolo — o tubería. A continuación, se indican algunos ejemplos de formato CSV extraídos del RFC 4180 para su mejor comprensión. El salto de línea Se define como CRLF y en la última línea de la tabla puede aparecer o no. Tal como se ve, el uso de comillas es totalmente opcional siendo incluso posible el utilizarlas o no dentro de la misma tabla. Esto se debe a que el uso del formato CSV no está totalmente estandarizado, si bien su uso está muy extendido.

```
Estos tres ejemplos son equivalentes:

aaa,bbb,ccc CRLF
zzz,yyy,xxx CRLF

aaa,bbb,ccc CRLF
zzz,yyy,xxx

"aaa","bbb","ccc" CRLF
zzz,yyy,xxx
```

B.1.6. Otros formatos para la transferencia de información

Como es de suponer, existen otros formatos de gran importancia y de uso común que, pese a que en muchos casos no son legibles en claro es importante saber de su existencia por su amplia extensión y uso.

- Ficheros de bases de datos. Se utilizan para almacenar los datos de forma estructurada que posteriormente serán utilizados en en las mismas para realizar consultas de forma más eficiente mediante el uso de un lenguaje de consulta diseñado ex profeso. Ejemplos muy conocidos de esto son el SQL, MySQL o Postgres.

- Ficheros de grafos. Se trata de una familia de formatos y de especificaciones diseñadas para representar las relaciones entre diferentes entidades así como los atributos tanto de los nodos como de las aristas del grafo resultante. Ejemplos de ellos serían el .gml [77] o el GraphML que varían en cuanto a su sintaxis y que pueden ser abiertas y exploradas por herramientas como Gephi [78], Graph-tool o Cytoscape.

En el caso concreto de un archivo GraphML, este consistiría en un archivo XML constituido por el elemento de un grafo [79], el cual está formado por una secuencia desordenada de nodos y aristas ya sean estas últimas dirigidas o no. Cada uno de ellos debe estar identificado por un atributo distinto y, para el caso de las aristas deben tener origen y destino. A continuación, un breve ejemplo de un fragmento de código de este lenguaje.

```
<?xml version="1.0" encoding="UTF-8"?>
<graphml xmlns="http://graphml.graphdrawing.org/xmlns"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://graphml.graphdrawing.org/xmlns/1.0/graphml.xsd">
  <graph id="G" edgedefault="undirected">
    <node id="n0"/>
    <node id="n1"/>
    <edge id="e1" source="n0" target="n1"/>
  </graph>
</graphml>
```

B.2. Las expresiones regulares

Se entiende por expresión regular aquel patrón utilizado para encontrar una determinada combinación de caracteres dentro de un archivo de texto [80]. Gracias a esto es posible buscar o reconocer cadenas de texto cuyas variaciones puedan parecerse a la palabra buscada. Las expresiones regulares se construyen normalmente utilizando los operadores unión, concatenación y cláusula de Kleene. Por ejemplo, el grupo formado por las cadenas Handel, Händel y Haendel se describe con el patrón H(a|ä|ae)ndel.

B.2.1. Búsqueda de cadenas de texto

En cuanto a su utilización en un entorno de Linux, uno de los comandos de uso común sería el grep o egrep para realizar búsquedas sobre ficheros de texto [81] tal como se muestra a continuación. El siguiente comando buscaría la cadena de texto «tal» en todos los archivos del directorio actual:

```
$ egrep tal *
```

Con el siguiente comando sería posible encontrar las palabras casa, techo y puerta realizando una búsqueda sobre todos los archivos de tipo .txt en el directorio actual.

```
$ egrep "(casa|techo|puerta)" *txt
```

Puesto que, no es el objeto de este punto la explicación al detalle de todas las funcionalidades de los comandos grep o egrep, en caso de que se quiera ampliar el conocimiento sobre estos, se recomienda la consulta del manual de Linux mediante el comando man grep [82] o man egrep [83].

B.2.2. Búsqueda de entidades mediante el uso de expresiones regulares

En este punto se va a hablar de entidad como aquel tipo de dato bien definido o cuya definición es común, por ejemplo, resultados de funciones hash, tarjetas o cuentas bancarias y direcciones IP. Para el caso de grandes volúmenes de texto, el uso de las expresiones regulares [80] puede ser de mucha utilidad. Dos ejemplos sencillos y bien definidos serían los correos electrónicos o las direcciones IPv4.

En el caso de los correos electrónicos, cuyo uso puede ser común con algunos sistemas de mensajería, recurriendo a la RFC 3696 [84] se hallará cuáles son las formas correctas y las restricciones que aplican al formato de un correo electrónico [85]. La parte local de la dirección de correo puede ir entrecomillada o sin entrecomillar y utilizar cualquiera de los siguientes caracteres ASCII:

- Mayúsculas y minúsculas o cualquier combinación de la A a la Z siempre utilizando caracteres latinos.
- Dígitos desde el 0 hasta el 9.
- Los siguientes caracteres imprimibles: `!#$%&'*+-/=?^_`{|}~`
- Puntos siempre y cuando no sean el primer o último carácter y, siempre y cuando no aparezcan más de una vez de forma consecutiva.

Así pues, si se pretende definir la expresión regular candidata para la búsqueda de un correo electrónico en un archivo de texto, se obtendría la siguiente fórmula:

```
<<[0-9a-zA-Z\-\-]+@[0-9a-zA-Z\-\-]+>>
```

En cuanto al formato de las direcciones IPv4 está definido en el RFC 791 [86]. Como es bien conocido, están formadas por 32 bits repartidos en cuatro octetos separados por puntos, los cuales en decimal pueden ir desde 0 hasta 255 por tanto, si se desea buscar una dirección IP en un documento de texto, la expresión regular candidata que habría que componer sería la siguiente:

```
<<[0-9]{1-3}.[0-9]{1-3}.[0-9]{1-3}.[0-9]{1-3}>>
```

Existen algunas plataformas en internet como RegExr[3] mediante las cuales es posible practicar la eficacia de las expresiones regulares desarrolladas por el usuario y que pueden ser de gran interés si se pretende lograr una formación como analista de información.

[3]https://regexr.com/

Apéndice C

Resultados de la búsqueda con theHarvester

A continuación, se muestra el archivo XML generado por theHarvester:

```
<?xml version="1.0" encoding="UTF-8"?>
<theHarvester>
  <email>bolsa.arpa@diputacionalicante.es</email>
  <email>bolsa.contrabajo@diputacionalicante.es</email>
  <email>bolsa.trombontenor@diputacionalicante.es</email>
  <email>bolsa.trompa@diputacionalicante.es</email>
  <email>bolsa.violin@diputacionalicante.es</email>
  <email>buengobierno@diputacionalicante.es</email>
  <email>ciudadanosextranjeros@diputacionalicante.es</email>
  <email>conserva@diputacionalicante.es</email>
  <email>consorciobomberos@diputacionalicante.es</email>
  <email>consorcioresiduosa2@diputacionalicante.es</email>
  <email>contratacion@diputacionalicante.es</email>
  <email>cultura@diputacionalicante.es</email>
  <email>edictos.bop@diputacionalicante.es</email>
  <email>formacio@diputacionalicante.es</email>
  <email>francisco.cano@diputacionalicante.es</email>
  <email>fruizfe@diputacionalicante.es</email>
  <email>galbert@diputacionalicante.es</email>
  <email>hacienda@diputacionalicante.es</email>
  <email>hogarprovincial@diputacionalicante.es</email>
  <email>iaccursos@diputacionalicante.es</email>
  <email>iberna@diputacionalicante.es</email>
  <email>igualdad@diputacionalicante.es</email>
  <email>imagen.promocion@diputacionalicante.es</email>
  <email>jcacho@diputacionalicante.es</email>
  <email>juanfran.perez@diputacionalicante.es</email>
  <email>juventud@diputacionalicante.es</email>
  <email>lbernabe@diputacionalicante.es</email>
```

```
<email>lsanchez@diputacionalicante.es</email>
<email>lvilapla@diputacionalicante.es</email>
<email>mamartim@diputacionalicante.es</email>
<email>miguel.lopez@diputacionalicante.es</email>
<email>mjrico@diputacionalicante.es</email>
<email>motero@diputacionalicante.es</email>
<email>oficinapd@diputacionalicante.es</email>
<email>plaosa@diputacionalicante.es</email>
<email>preinfraestructuras@diputacionalicante.es</email>
<email>prensa@diputacionalicante.es</email>
<email>presidente@diputacionalicante.es</email>
<email>protocolo.adda@diputacionalicante.es</email>
<email>registro@diputacionalicante.es</email>
<host>datosabiertos.diputacionalicante.es</host>
<host>abierta.diputacionalicante.es</host>
<host>Alicantecocentaina.diputacionalicante.es</host>
<host>gfw.diputacionalicante.es</host>
<host>soportemunicipios.diputacionalicante.es</host>
<host>formacion.diputacionalicante.es</host>
<host>www.archivo.diputacionalicante.es</host>
<host>documentacion.diputacionalicante.es</host>
<host>conductasadictivas.diputacionalicante.es</host>
<host>municipapp.diputacionalicante.es</host>
<host>consorcioresiduosa2.diputacionalicante.es</host>
<host>www.diputacionalicante.es</host>
<host>hemeroteca.diputacionalicante.es</host>
<host>voluntariado.diputacionalicante.es</host>
<host>mico-presupuestariagfw.diputacionalicante.es</host>
<host>sede.diputacionalicante.es</host>
<host>nicasede.diputacionalicante.es</host>
<host>mi.diputacionalicante.es</host>
<host>eiel.diputacionalicante.es</host>
<host>portal.diputacionalicante.es</host>
<host>concejalesayuntamientos.diputacionalicante.es</host>
<host>concursocentrocongresosalicante.diputacionalicante.es</host>
<host>pmh.diputacionalicante.es</host>
<host>*.diputacionalicante.es</host>
<host>datosabiertos.diputacionalicante.es</host>
<host>mail.diputacionalicante.es</host>
<host>repo1.diputacionalicante.es</host>
<host>new.diputacionalicante.es</host>
<host>glpi.diputacionalicante.es</host>
<host>gfw.diputacionalicante.es</host>
<host>abierta-iaf.diputacionalicante.es</host>
<host>congresotransparencia.diputacionalicante.es</host>
<host>municipapp.diputacionalicante.es</host>
<host>www.diputacionalicante.es</host>
<host>expocreativa.diputacionalicante.es</host>
<host>agendacultural.diputacionalicante.es</host>
<host>graylog.diputacionalicante.es</host>
<host>lopd.diputacionalicante.es</host>
<host>voluntariado.diputacionalicante.es</host>
<host>registrypodman.diputacionalicante.es</host>
<host>autodiscover.diputacionalicante.es</host>
<host>registry.diputacionalicante.es</host>
```

```
<host>ftpteleasistencia.diputacionalicante.es</host>
<host>sede.diputacionalicante.es</host>
<host>eiel.diputacionalicante.es</host>
<host>portalproveedor.diputacionalicante.es</host>
<host>planmoderniza.diputacionalicante.es</host>
<host>moderniza.diputacionalicante.es</host>
<host>portal.diputacionalicante.es</host>
<host>cajacredito.diputacionalicante.es</host>
<host>eformacion.diputacionalicante.es</host>
<host>abiertaws.diputacionalicante.es</host>
<host>tramites.diputacionalicante.es</host>
<host>pmh.diputacionalicante.es</host>
<host>
  <ip>195.53.69.179</ip>
  <hostname>hemeroteca.diputacionalicante.es</hostname>
</host>
<host>
  <ip>195.53.69.160</ip>
  <hostname>agenda21.diputacionalicante.es</hostname>
</host>
<host>
  <ip>195.53.69.160</ip>
  <hostname>dwnmedios.diputacionalicante.es</hostname>
</host>
<host>
  <ip>195.53.69.184</ip>
  <hostname>www.torneodegolf.diputacionalicante.es</hostname>
</host>
<host>
  <ip>195.53.69.162</ip>
  <hostname>scpi.diputacionalicante.es</hostname>
</host>
<host>
  <ip>195.53.69.162</ip>
  <hostname>planmoderniza.diputacionalicante.es</hostname>
</host>
<host>
  <ip>195.53.69.160</ip>
  <hostname>formacion2.diputacionalicante.es</hostname>
</host>
<host>
  <ip>195.53.69.146</ip>
  <hostname>presistemas.diputacionalicante.es</hostname>
</host>
<host>
  <ip>195.53.69.184</ip>
  <hostname>3edicion.semcompol.diputacionalicante.es</hostname>
</host>
<host>
  <ip>195.53.69.184</ip>
  <hostname>datosabiertos.diputacionalicante.es</hostname>
</host>
<host>
  <ip>195.53.69.179</ip>
  <hostname>cajacreditonew.diputacionalicante.es</hostname>
```

```
140     </host>
141     <host>
142       <ip>195.53.69.141</ip>
143       <hostname>webservice.diputacionalicante.es</hostname>
144     </host>
145     <host>
146       <ip>195.53.69.184</ip>
147       <hostname>cuesprev.diputacionalicante.es</hostname>
148     </host>
149     <host>
150       <ip>95.61.88.71</ip>
151       <hostname>eformacion.diputacionalicante.es</hostname>
152     </host>
153     <host>
154       <ip>195.53.69.184</ip>
155       <hostname>semcompol.diputacionalicante.es</hostname>
156     </host>
157     <host>
158       <ip>195.53.69.184</ip>
159       <hostname>conductasadictivas.diputacionalicante.es</hostname>
160     </host>
161     <host>
162       <ip>195.53.69.160</ip>
163       <hostname>documentacion.diputacionalicante.es</hostname>
164     </host>
165     <host>
166       <ip>195.53.69.184</ip>
167       <hostname>glpi.diputacionalicante.es</hostname>
168     </host>
169     <host>
170       <ip>195.53.69.184</ip>
171       <hostname>jornadamoderniza.diputacionalicante.es</hostname>
172     </host>
173     <host>
174       <ip>195.53.69.184</ip>
175       <hostname>promyadmin.diputacionalicante.es</hostname>
176     </host>
177     <host>
178       <ip>195.53.69.179</ip>
179       <hostname>registry.diputacionalicante.es</hostname>
180     </host>
181     <host>
182       <ip>195.53.69.157</ip>
183       <hostname>agendaculturalresources.diputacionalicante.es</hostname>
184     </host>
185     <host>
186       <ip>195.53.69.179</ip>
187       <hostname>planmodernizanew.diputacionalicante.es</hostname>
188     </host>
189     <host>
190       <ip>195.53.69.179</ip>
191       <hostname>grupopopular.diputacionalicante.es</hostname>
192     </host>
193     <host>
194       <ip>195.53.69.184</ip>
```

```
    <hostname>1edicion.semcompol.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.146</ip>
    <hostname>phplist.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.179</ip>
    <hostname>documentosregistro.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.179</ip>
    <hostname>consorcioresiduosa2.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.179</ip>
    <hostname>iter-iaf.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.179</ip>
    <hostname>eurojuv.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.158</ip>
    <hostname>abierta.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.179</ip>
    <hostname>agendacultural.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.184</ip>
    <hostname>abiertaws.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.184</ip>
    <hostname>aulavirtual-iafalicante.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.30</ip>
    <hostname>acceso.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.155</ip>
    <hostname>smtp.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.152</ip>
    <hostname>new.porqueesposible.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.179</ip>
    <hostname>premioazorin2020.diputacionalicante.es</hostname>
  </host>
  <host>
```

```
    <ip>195.53.69.179</ip>
    <hostname>participando.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.184</ip>
    <hostname>voluntariado.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.162</ip>
    <hostname>abierta-iaf.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.184</ip>
    <hostname>2edicion.semcompol.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.179</ip>
    <hostname>newdipu.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.149</ip>
    <hostname>premiosalbi.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.179</ip>
    <hostname>accionvip-iaf.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.179</ip>
    <hostname>myadmin.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.179</ip>
    <hostname>hipokrates1-iaf.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.179</ip>
    <hostname>wifi4eulosmontesinos.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.184</ip>
    <hostname>podcastgilalbert.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.184</ip>
    <hostname>corporatepro.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.184</ip>
    <hostname>amigos.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.179</ip>
    <hostname>gruposocialista.diputacionalicante.es</hostname>
  </host>
```

```
<host>
  <ip>195.53.69.162</ip>
  <hostname>clvpruebasdes.diputacionalicante.es</hostname>
</host>
<host>
  <ip>195.53.69.184</ip>
  <hostname>cajacredito.diputacionalicante.es</hostname>
</host>
<host>
  <ip>195.53.69.160</ip>
  <hostname>jornadaprocedimientoadministrativo.diputacionalicante.es</hostname>
</host>
<host>
  <ip>195.53.69.14</ip>
  <hostname>pmh.diputacionalicante.es</hostname>
</host>
<host>
  <ip>195.53.69.184</ip>
  <hostname>procesosparticipativos.diputacionalicante.es</hostname>
</host>
<host>
  <ip>195.53.69.151</ip>
  <hostname>sededocs.diputacionalicante.es</hostname>
</host>
<host>
  <ip>195.53.69.184</ip>
  <hostname>abierta-iaf.diputacionalicante.es</hostname>
</host>
<host>
  <ip>195.53.69.179</ip>
  <hostname>concursocentrocongresosalicante.diputacionalicante.es</hostname>
</host>
<host>
  <ip>195.53.69.157</ip>
  <hostname>aytosapp.diputacionalicante.es</hostname>
</host>
<host>
  <ip>195.53.69.1</ip>
  <hostname>vpn.diputacionalicante.es</hostname>
</host>
<host>
  <ip>195.53.69.160</ip>
  <hostname>ftpvideoactas.diputacionalicante.es</hostname>
</host>
<host>
  <ip>195.53.69.179</ip>
  <hostname>soportemunicipios.diputacionalicante.es</hostname>
</host>
<host>
  <ip>195.53.69.184</ip>
  <hostname>encuestasua.diputacionalicante.es</hostname>
</host>
<host>
  <ip>195.53.69.179</ip>
  <hostname>portalpre.diputacionalicante.es.diputacionalicante.es</hostname>
```

```
  </host>
  <host>
    <ip>195.53.69.162</ip>
    <hostname>abiertaws.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.179</ip>
    <hostname>jornadadeasistenciamunicipios.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.160</ip>
    <hostname>ftpcoronavirus.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.184</ip>
    <hostname>jornadarelacionesafectivas.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.179</ip>
    <hostname>grupociudadanos.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.179</ip>
    <hostname>www.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.179</ip>
    <hostname>parajesnaturales.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>172.16.14.151</ip>
    <hostname>registrypodman.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.151</ip>
    <hostname>gfwpreproductivo.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.160</ip>
    <hostname>formacion.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.184</ip>
    <hostname>torneodegolf.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.179</ip>
    <hostname>participandonew.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.151</ip>
    <hostname>gfw.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.162</ip>
```

```
    <hostname>portal.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.179</ip>
    <hostname>clvpruebasdes.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.162</ip>
    <hostname>newdatos.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.184</ip>
    <hostname>expocreativa.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.179</ip>
    <hostname>grupocompromis.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.146</ip>
    <hostname>espublicofiles.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.179</ip>
    <hostname>sede.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.179</ip>
    <hostname>hipokrates2-iaf.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.179</ip>
    <hostname>municipapp.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.149</ip>
    <hostname>nueva.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.142</ip>
    <hostname>tramites.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.184</ip>
    <hostname>jornadaeuropea.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.10</ip>
    <hostname>moderniza.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.184</ip>
    <hostname>planmoderniza.diputacionalicante.es</hostname>
  </host>
  <host>
```

```
    <ip>195.53.69.146</ip>
    <hostname>predipupressres.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.179</ip>
    <hostname>preglpi.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>82.98.148.168</ip>
    <hostname>lopd.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.160</ip>
    <hostname>indicadoresinf.diputacionalicante.es</hostname>
  </host>
  <host>presistemas.diputacionalicante.es</host>
  <host>grupociudadanos.diputacionalicante.es</host>
  <host>myadmin.diputacionalicante.es</host>
  <host>documentosregistro.diputacionalicante.es</host>
  <host>nueva.diputacionalicante.es</host>
  <host>premiosalbi.diputacionalicante.es</host>
  <host>municipapp.diputacionalicante.es</host>
  <host>amigos.diputacionalicante.es</host>
  <host>espublicofiles.diputacionalicante.es</host>
  <host>wifi4eulosmontesinos.diputacionalicante.es</host>
  <host>acceso.diputacionalicante.es</host>
  <host>predipupressres.diputacionalicante.es</host>
  <host>sede.diputacionalicante.es</host>
  <host>jornadarelacionesafectivas.diputacionalicante.es</host>
  <host>moderniza.diputacionalicante.es</host>
  <host>portal.diputacionalicante.es</host>
  <host>agenda21.diputacionalicante.es</host>
  <host>2edicion.semcompol.diputacionalicante.es</host>
  <host>eformacion.diputacionalicante.es</host>
  <host>abiertaws.diputacionalicante.es</host>
  <host>tramites.diputacionalicante.es</host>
  <host>concursocentrocongresosalicante.diputacionalicante.es</host>
  <host>podcastgilalbert.diputacionalicante.es</host>
  <host>abierta.diputacionalicante.es</host>
  <host>encuestasua.diputacionalicante.es</host>
  <host>glpi.diputacionalicante.es</host>
  <host>gfw.diputacionalicante.es</host>
  <host>soportemunicipios.diputacionalicante.es</host>
  <host>formacion.diputacionalicante.es</host>
  <host>dwnmedios.diputacionalicante.es</host>
  <host>participando.diputacionalicante.es</host>
  <host>documentacion.diputacionalicante.es</host>
  <host>conductasadictivas.diputacionalicante.es</host>
  <host>eurojuv.diputacionalicante.es</host>
  <host>hipokrates1-iaf.diputacionalicante.es</host>
  <host>ftpcoronavirus.diputacionalicante.es</host>
  <host>agendacultural.diputacionalicante.es</host>
  <host>semcompol.diputacionalicante.es</host>
  <host>registry.diputacionalicante.es</host>
  <host>promyadmin.diputacionalicante.es</host>
```

```
525   <host>jornadadeasistenciamunicipios.diputacionalicante.es</host>
526   <host>gfwpreproductivo.diputacionalicante.es</host>
527   <host>new.porqueesposible.diputacionalicante.es</host>
528   <host>webservice.diputacionalicante.es</host>
529   <host>1edicion.semcompol.diputacionalicante.es</host>
530   <host>newdatos.diputacionalicante.es</host>
531   <host>datosabiertos.diputacionalicante.es</host>
532   <host>hipokrates2-iaf.diputacionalicante.es</host>
533   <host>aytosapp.diputacionalicante.es</host>
534   <host>jornadaprocedimientoadministrativo.diputacionalicante.es</host>
535   <host>parajesnaturales.diputacionalicante.es</host>
536   <host>abierta-iaf.diputacionalicante.es</host>
537   <host>cajacreditonew.diputacionalicante.es</host>
538   <host>grupocompromis.diputacionalicante.es</host>
539   <host>iter-iaf.diputacionalicante.es</host>
540   <host>consorcioresiduosa2.diputacionalicante.es</host>
541   <host>www.diputacionalicante.es</host>
542   <host>sededocs.diputacionalicante.es</host>
543   <host>hemeroteca.diputacionalicante.es</host>
544   <host>expocreativa.diputacionalicante.es</host>
545   <host>jornadaeuropea.diputacionalicante.es</host>
546   <host>lopd.diputacionalicante.es</host>
547   <host>gruposocialista.diputacionalicante.es</host>
548   <host>agendaculturalresources.diputacionalicante.es</host>
549   <host>voluntariado.diputacionalicante.es</host>
550   <host>corporatepro.diputacionalicante.es</host>
551   <host>preglpi.diputacionalicante.es</host>
552   <host>ftpvideoactas.diputacionalicante.es</host>
553   <host>procesosparticipativos.diputacionalicante.es</host>
554   <host>formacion2.diputacionalicante.es</host>
555   <host>cajacredito.diputacionalicante.es</host>
556   <host>planmodernizanew.diputacionalicante.es</host>
557   <host>3edicion.semcompol.diputacionalicante.es</host>
558   <host>accionvip-iaf.diputacionalicante.es</host>
559   <host>clvpruebasdes.diputacionalicante.es</host>
560   <host>grupopopular.diputacionalicante.es</host>
561   <host>smtp.diputacionalicante.es</host>
562   <host>indicadoresinf.diputacionalicante.es</host>
563   <host>participandonew.diputacionalicante.es</host>
564   <host>registrypodman.diputacionalicante.es</host>
565   <host>jornadamoderniza.diputacionalicante.es</host>
566   <host>planmoderniza.diputacionalicante.es</host>
567   <host>aulavirtual-iafalicante.diputacionalicante.es</host>
568   <host>cuesprev.diputacionalicante.es</host>
569   <host>phplist.diputacionalicante.es</host>
570   <host>newdipu.diputacionalicante.es</host>
571   <host>premioazorin2020.diputacionalicante.es</host>
572   <host>
573     <ip>195.53.69.179</ip>
574     <hostname>hemeroteca.diputacionalicante.es</hostname>
575   </host>
576   <host>
577     <ip>195.53.69.160</ip>
578     <hostname>www.topcreation.diputacionalicante.es</hostname>
579   </host>
```

```
  <host>
    <ip>195.53.69.160</ip>
    <hostname>agenda21.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>ghs.google.com</ip>
    <hostname>blog.formacion.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.160</ip>
    <hostname>sededocsftp.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.184</ip>
    <hostname>planes.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.160</ip>
    <hostname>dwnmedios.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.13</ip>
    <hostname>tasasmunicipales.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.184</ip>
    <hostname>www.torneodegolf.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.179</ip>
    <hostname>busot.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.179</ip>
    <hostname>portalpre.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>mail.diputacionalicante.es.</ip>
    <hostname>autodiscover.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.188</ip>
    <hostname>wpfordes.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.160</ip>
    <hostname>formacion2.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.184</ip>
    <hostname>azorinsv.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.146</ip>
    <hostname>presistemas.diputacionalicante.es</hostname>
```

```
635   </host>
636   <host>
637     <ip>195.53.69.184</ip>
638     <hostname>3edicion.semcompol.diputacionalicante.es</hostname>
639   </host>
640   <host>
641     <ip>195.53.69.184</ip>
642     <hostname>mysqlaccess.diputacionalicante.es</hostname>
643   </host>
644   <host>
645     <ip>195.53.69.184</ip>
646     <hostname>soportemunicipios.diputacionalicante.es</hostname>
647   </host>
648   <host>
649     <ip>195.53.69.146</ip>
650     <hostname>board.diputacionalicante.es</hostname>
651   </host>
652   <host>
653     <ip>95.61.88.71</ip>
654     <hostname>eformacion.diputacionalicante.es</hostname>
655   </host>
656   <host>
657     <ip>195.53.69.184</ip>
658     <hostname>semcompol.diputacionalicante.es</hostname>
659   </host>
660   <host>
661     <ip>195.53.69.184</ip>
662     <hostname>conductasadictivas.diputacionalicante.es</hostname>
663   </host>
664   <host>
665     <ip>195.53.69.160</ip>
666     <hostname>www.archivo.diputacionalicante.es</hostname>
667   </host>
668   <host>
669     <ip>195.53.69.160</ip>
670     <hostname>documentacion.diputacionalicante.es</hostname>
671   </host>
672   <host>
673     <ip>195.53.69.184</ip>
674     <hostname>glpi.diputacionalicante.es</hostname>
675   </host>
676   <host>
677     <ip>smtp.diputacionalicante.es</ip>
678     <hostname>diputacionalicante.es</hostname>
679   </host>
680   <host>
681     <ip>195.53.69.184</ip>
682     <hostname>agendacultural.diputacionalicante.es</hostname>
683   </host>
684   <host>
685     <ip>195.53.69.184</ip>
686     <hostname>jornadamoderniza.diputacionalicante.es</hostname>
687   </host>
688   <host>
689     <ip>195.53.69.184</ip>
```

```
690       <hostname>sede.diputacionalicante.es</hostname>
691     </host>
692     <host>
693       <ip>195.53.69.179</ip>
694       <hostname>xixona.diputacionalicante.es</hostname>
695     </host>
696     <host>
697       <ip>195.53.69.184</ip>
698       <hostname>europa.diputacionalicante.es</hostname>
699     </host>
700     <host>
701       <ip>195.53.69.157</ip>
702       <hostname>agendaculturalresources.diputacionalicante.es</hostname>
703     </host>
704     <host>
705       <ip>195.53.69.184</ip>
706       <hostname>1edicion.semcompol.diputacionalicante.es</hostname>
707     </host>
708     <host>
709       <ip>195.53.69.160</ip>
710       <hostname>concejalesayuntamientos.diputacionalicante.es</hostname>
711     </host>
712     <host>
713       <ip>195.53.69.179</ip>
714       <hostname>iter-iaf.diputacionalicante.es</hostname>
715     </host>
716     <host>
717       <ip>195.53.69.158</ip>
718       <hostname>abierta.diputacionalicante.es</hostname>
719     </host>
720     <host>
721       <ip>195.53.69.160</ip>
722       <hostname>holon.diputacionalicante.es</hostname>
723     </host>
724     <host>
725       <ip>ghs.google.com.</ip>
726       <hostname>blog.formacion.diputacionalicante.es</hostname>
727     </host>
728     <host>
729       <ip>195.53.69.184</ip>
730       <hostname>abiertaws.diputacionalicante.es</hostname>
731     </host>
732     <host>
733       <ip>195.53.69.179</ip>
734       <hostname>violenciasmachistas.diputacionalicante.es</hostname>
735     </host>
736     <host>
737       <ip>195.53.69.149</ip>
738       <hostname>www.premiosalbi.diputacionalicante.es</hostname>
739     </host>
740     <host>
741       <ip>195.53.69.184</ip>
742       <hostname>foroinnovatet.diputacionalicante.es</hostname>
743     </host>
744     <host>
```

```
    <ip>195.53.69.184</ip>
    <hostname>hemeroteca.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.155</ip>
    <hostname>smtp.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.179</ip>
    <hostname>curso1-iafalicante.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.184</ip>
    <hostname>aulavirtual-iafalicante.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.179</ip>
    <hostname>participando.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.184</ip>
    <hostname>1e1.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.184</ip>
    <hostname>parajesnaturales.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.184</ip>
    <hostname>euindustrydays.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.160</ip>
    <hostname>indicadoressam.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.152</ip>
    <hostname>ftpayuntamientos.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.184</ip>
    <hostname>wifi4eulosmontesinos.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.184</ip>
    <hostname>voluntariado.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.184</ip>
    <hostname>pruebasmariwpml.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.152</ip>
    <hostname>orxetamaps.diputacionalicante.es</hostname>
  </host>
```

```
  <host>
    <ip>195.53.69.179</ip>
    <hostname>curso2-iafalicante.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.145</ip>
    <hostname>tpvdes.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.184</ip>
    <hostname>participando.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.184</ip>
    <hostname>agendaphplist.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.152</ip>
    <hostname>mysqlayuntamientos.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.184</ip>
    <hostname>muro.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.146</ip>
    <hostname>clvprueba.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.184</ip>
    <hostname>podcastgilalbert.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.184</ip>
    <hostname>eurojuv.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.184</ip>
    <hostname>corporatepro.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.184</ip>
    <hostname>amigos.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.184</ip>
    <hostname>hipokrates1-iaf.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.162</ip>
    <hostname>clvpruebasdes.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.184</ip>
    <hostname>limenew.diputacionalicante.es</hostname>
```

```
  </host>
  <host>
    <ip>195.53.69.184</ip>
    <hostname>amigosphplist.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.184</ip>
    <hostname>partmurodev.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.152</ip>
    <hostname>mysqldiputacion.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.160</ip>
    <hostname>jornadaprocedimientoadministrativo.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.184</ip>
    <hostname>cajacredito.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.184</ip>
    <hostname>pruebasmari.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.14</ip>
    <hostname>pmh.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.146</ip>
    <hostname>nuevasede.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.184</ip>
    <hostname>foro.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.151</ip>
    <hostname>sededocs.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.184</ip>
    <hostname>abierta-iaf.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.146</ip>
    <hostname>pruebalime.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.157</ip>
    <hostname>aytosapp.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.1</ip>
```

```
910       <hostname>vpn.diputacionalicante.es</hostname>
911     </host>
912     <host>
913       <ip>195.53.69.152</ip>
914       <hostname>www.porqueesposible.diputacionalicante.es</hostname>
915     </host>
916     <host>
917       <ip>195.53.69.184</ip>
918       <hostname>accionvip-iaf.diputacionalicante.es</hostname>
919     </host>
920     <host>
921       <ip>195.53.69.145</ip>
922       <hostname>transparenciaws.diputacionalicante.es</hostname>
923     </host>
924     <host>
925       <ip>195.53.69.160</ip>
926       <hostname>ftpvideoactas.diputacionalicante.es</hostname>
927     </host>
928     <host>
929       <ip>195.53.69.184</ip>
930       <hostname>grupocompromis.diputacionalicante.es</hostname>
931     </host>
932     <host>
933       <ip>195.53.69.184</ip>
934       <hostname>acftest.diputacionalicante.es</hostname>
935     </host>
936     <host>
937       <ip>195.53.69.152</ip>
938       <hostname>clon.diputacionalicante.es</hostname>
939     </host>
940     <host>
941       <ip>195.53.69.184</ip>
942       <hostname>municipapp.diputacionalicante.es</hostname>
943     </host>
944     <host>
945       <ip>195.53.69.184</ip>
946       <hostname>iter-iaf.diputacionalicante.es</hostname>
947     </host>
948     <host>
949       <ip>smtp.diputacionalicante.es.</ip>
950       <hostname>diputacionalicante.es</hostname>
951     </host>
952     <host>
953       <ip>195.53.69.184</ip>
954       <hostname>grupopopular.diputacionalicante.es</hostname>
955     </host>
956     <host>
957       <ip>195.53.69.150</ip>
958       <hostname>mail.diputacionalicante.es</hostname>
959     </host>
960     <host>
961       <ip>195.53.69.179</ip>
962       <hostname>soportemunicipios.diputacionalicante.es</hostname>
963     </host>
964     <host>
```

```
    <ip>195.53.69.145</ip>
    <hostname>tpv.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.179</ip>
    <hostname>sedepre.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.149</ip>
    <hostname>transparencia.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.160</ip>
    <hostname>ftpcoronavirus.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.184</ip>
    <hostname>portal.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.160</ip>
    <hostname>descargaglpi.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.179</ip>
    <hostname>parajesnaturales.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.184</ip>
    <hostname>mesadelagua.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.184</ip>
    <hostname>tollos.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.184</ip>
    <hostname>international.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.184</ip>
    <hostname>premioazorin2020.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.151</ip>
    <hostname>gfwpreproductivo.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.160</ip>
    <hostname>formacion.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.184</ip>
    <hostname>torneodegolf.diputacionalicante.es</hostname>
  </host>
```

```
  <host>
    <ip>195.53.69.184</ip>
    <hostname>cocentaina.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.152</ip>
    <hostname>sanmigueldesalinas.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.179</ip>
    <hostname>clvpruebasdes.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>mail.diputacionalicante.es</ip>
    <hostname>autodiscover.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.184</ip>
    <hostname>expocreativa.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.184</ip>
    <hostname>violenciasmachistas.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.160</ip>
    <hostname>informacionbop.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.146</ip>
    <hostname>espublicofiles.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.179</ip>
    <hostname>sede.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.186</ip>
    <hostname>www2.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.184</ip>
    <hostname>consorcioresiduosa2.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.184</ip>
    <hostname>abierta.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.149</ip>
    <hostname>nueva.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.152</ip>
    <hostname>forobienestar.diputacionalicante.es</hostname>
```

```
  </host>
  <host>
    <ip>195.53.69.184</ip>
    <hostname>grupoesquerraunida.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.142</ip>
    <hostname>tramites.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.188</ip>
    <hostname>pruebassede.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.184</ip>
    <hostname>jornadaeuropea.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.10</ip>
    <hostname>moderniza.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.184</ip>
    <hostname>wpomiguel.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.146</ip>
    <hostname>predipupressres.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.179</ip>
    <hostname>preglpi.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.145</ip>
    <hostname>wsnominas.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.184</ip>
    <hostname>territoriointeligente.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.160</ip>
    <hostname>vm.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.152</ip>
    <hostname>villenaold.diputacionalicante.es</hostname>
  </host>
  <host>
    <ip>195.53.69.184</ip>
    <hostname>creama.diputacionalicante.es</hostname>
  </host>
  <host>datosabiertos.diputacionalicante.es</host>
  <host>new.diputacionalicante.es</host>
```

```
<host>aytosapp.diputacionalicante.es</host>
<host>cocentaina.diputacionalicante.es</host>
<host>glpi.diputacionalicante.es</host>
<host>parajesnaturales.diputacionalicante.es</host>
<host>gfw.diputacionalicante.es</host>
<host>soportemunicipios.diputacionalicante.es</host>
<host>formacion.diputacionalicante.es</host>
<host>www.archivo.diputacionalicante.es</host>
<host>documentacion.diputacionalicante.es</host>
<host>municipapp.diputacionalicante.es</host>
<host>consorcioresiduosa2.diputacionalicante.es</host>
<host>www.diputacionalicante.es</host>
<host>agendacultural.diputacionalicante.es</host>
<host>cesarsanchez.diputacionalicante.es</host>
<host>blog.formacion.diputacionalicante.es</host>
<host>voluntariado.diputacionalicante.es</host>
<host>registrypodman.diputacionalicante.es</host>
<host>registry.diputacionalicante.es</host>
<host>sede.diputacionalicante.es</host>
<host>portal.diputacionalicante.es</host>
<host>eformacion.diputacionalicante.es</host>
<host>pmh.diputacionalicante.es</host>
<host>1edicion.semcompol.diputacionalicante.es</host>
<host>planmoderniza.diputacionalicante.es</host>
<host>acftest.diputacionalicante.es</host>
<host>presistemas.diputacionalicante.es</host>
<host>europa.diputacionalicante.es</host>
<host>transparenciaws.diputacionalicante.es</host>
<host>new.diputacionalicante.es</host>
<host>violenciasmachistas.diputacionalicante.es</host>
<host>foro.diputacionalicante.es</host>
<host>congresotransparencia.diputacionalicante.es</host>
<host>nueva.diputacionalicante.es</host>
<host>premiosalbi.diputacionalicante.es</host>
<host>municipapp.diputacionalicante.es</host>
<host>planes.diputacionalicante.es</host>
<host>sededocsftp.diputacionalicante.es</host>
<host>amigos.diputacionalicante.es</host>
<host>espublicofiles.diputacionalicante.es</host>
<host>wifi4eulosmontesinos.diputacionalicante.es</host>
<host>graylog.diputacionalicante.es</host>
<host>predipupressres.diputacionalicante.es</host>
<host>vm.diputacionalicante.es</host>
<host>autodiscover.diputacionalicante.es</host>
<host>amigosphplist.diputacionalicante.es</host>
<host>ftpayuntamientos.diputacionalicante.es</host>
<host>sede.diputacionalicante.es</host>
<host>sedepre.diputacionalicante.es</host>
<host>portalproveedor.diputacionalicante.es</host>
<host>topcreation.diputacionalicante.es</host>
<host>moderniza.diputacionalicante.es</host>
<host>portal.diputacionalicante.es</host>
<host>agenda21.diputacionalicante.es</host>
<host>transparencia.diputacionalicante.es</host>
<host>mysqldiputacion.diputacionalicante.es</host>
```

```
<host>eformacion.diputacionalicante.es</host>
<host>abiertaws.diputacionalicante.es</host>
<host>foroinnovatet.diputacionalicante.es</host>
<host>tramites.diputacionalicante.es</host>
<host>porqueesposible.diputacionalicante.es</host>
<host>pruebalime.diputacionalicante.es</host>
<host>podcastgilalbert.diputacionalicante.es</host>
<host>abierta.diputacionalicante.es</host>
<host>villenaold.diputacionalicante.es</host>
<host>glpi.diputacionalicante.es</host>
<host>gfw.diputacionalicante.es</host>
<host>tpv.diputacionalicante.es</host>
<host>soportemunicipios.diputacionalicante.es</host>
<host>wsnominas.diputacionalicante.es</host>
<host>formacion.diputacionalicante.es</host>
<host>dwnmedios.diputacionalicante.es</host>
<host>participando.diputacionalicante.es</host>
<host>conductasadictivas.diputacionalicante.es</host>
<host>documentacion.diputacionalicante.es</host>
<host>eurojuv.diputacionalicante.es</host>
<host>xixona.diputacionalicante.es</host>
<host>hipokrates1-iaf.diputacionalicante.es</host>
<host>ftpcoronavirus.diputacionalicante.es</host>
<host>board.diputacionalicante.es</host>
<host>agendacultural.diputacionalicante.es</host>
<host>curso1-iafalicante.diputacionalicante.es</host>
<host>semcompol.diputacionalicante.es</host>
<host>ftpteleasistencia.diputacionalicante.es</host>
<host>registry.diputacionalicante.es</host>
<host>clvprueba.diputacionalicante.es</host>
<host>holon.diputacionalicante.es</host>
<host>gfwpreproductivo.diputacionalicante.es</host>
<host>partmurodev.diputacionalicante.es</host>
<host>tpvdes.diputacionalicante.es</host>
<host>informacionbop.diputacionalicante.es</host>
<host>pmh.diputacionalicante.es</host>
<host>orxetamaps.diputacionalicante.es</host>
<host>1edicion.semcompol.diputacionalicante.es</host>
<host>datosabiertos.diputacionalicante.es</host>
<host>mail.diputacionalicante.es</host>
<host>repo1.diputacionalicante.es</host>
<host>aytosapp.diputacionalicante.es</host>
<host>jornadaprocedimientoadministrativo.diputacionalicante.es</host>
<host>nuevasede.diputacionalicante.es</host>
<host>mysqlaccess.diputacionalicante.es</host>
<host>parajesnaturales.diputacionalicante.es</host>
<host>1e1.diputacionalicante.es</host>
<host>abierta-iaf.diputacionalicante.es</host>
<host>grupocompromis.diputacionalicante.es</host>
<host>iter-iaf.diputacionalicante.es</host>
<host>descargaglpi.diputacionalicante.es</host>
<host>consorcioresiduosa2.diputacionalicante.es</host>
<host>territoriointeligente.diputacionalicante.es</host>
<host>torneodegolf.diputacionalicante.es</host>
<host>sededocs.diputacionalicante.es</host>
```

```
<host>hemeroteca.diputacionalicante.es</host>
<host>expocreativa.diputacionalicante.es</host>
<host>mesadelagua.diputacionalicante.es</host>
<host>blog.formacion.diputacionalicante.es</host>
<host>jornadaeuropea.diputacionalicante.es</host>
<host>agendaculturalresources.diputacionalicante.es</host>
<host>lopd.diputacionalicante.es</host>
<host>corporatepro.diputacionalicante.es</host>
<host>voluntariado.diputacionalicante.es</host>
<host>preglpi.diputacionalicante.es</host>
<host>ftpvideoactas.diputacionalicante.es</host>
<host>eiel.diputacionalicante.es</host>
<host>creama.diputacionalicante.es</host>
<host>cajacredito.diputacionalicante.es</host>
<host>formacion2.diputacionalicante.es</host>
<host>pruebasmari.diputacionalicante.es</host>
<host>www2.diputacionalicante.es</host>
<host>limenew.diputacionalicante.es</host>
<host>acftest.diputacionalicante.es</host>
<host>3edicion.semcompol.diputacionalicante.es</host>
<host>cocentaina.diputacionalicante.es</host>
<host>forobienestar.diputacionalicante.es</host>
<host>indicadoressam.diputacionalicante.es</host>
<host>portalpre.diputacionalicante.es</host>
<host>curso2-iafalicante.diputacionalicante.es</host>
<host>archivo.diputacionalicante.es</host>
<host>international.diputacionalicante.es</host>
<host>pruebasmariwpml.diputacionalicante.es</host>
<host>tasasmunicipales.diputacionalicante.es</host>
<host>accionvip-iaf.diputacionalicante.es</host>
<host>wpomiguel.diputacionalicante.es</host>
<host>clvpruebasdes.diputacionalicante.es</host>
<host>agendaphplist.diputacionalicante.es</host>
<host>grupoesquerraunida.diputacionalicante.es</host>
<host>grupopopular.diputacionalicante.es</host>
<host>smtp.diputacionalicante.es</host>
<host>euindustrydays.diputacionalicante.es</host>
<host>vpn.diputacionalicante.es</host>
<host>tollos.diputacionalicante.es</host>
<host>mysqlayuntamientos.diputacionalicante.es</host>
<host>registrypodman.diputacionalicante.es</host>
<host>jornadamoderniza.diputacionalicante.es</host>
<host>azorinsv.diputacionalicante.es</host>
<host>muro.diputacionalicante.es</host>
<host>wpfordes.diputacionalicante.es</host>
<host>planmoderniza.diputacionalicante.es</host>
<host>sanmigueldesalinas.diputacionalicante.es</host>
<host>aulavirtual-iafalicante.diputacionalicante.es</host>
<host>clon.diputacionalicante.es</host>
<host>concejalesayuntamientos.diputacionalicante.es</host>
<host>busot.diputacionalicante.es</host>
<host>premioazorin2020.diputacionalicante.es</host>
<host>pruebassede.diputacionalicante.es</host>
<host>documentacion.diputacionalicante.es</host>
<host>municipapp.diputacionalicante.es</host>
```

```
  <host>datosabiertos.diputacionalicante.es</host>
  <host>consorcioresiduosa2.diputacionalicante.es</host>
  <host>www.diputacionalicante.es</host>
  <host>abierta.diputacionalicante.es</host>
  <host>glpi.diputacionalicante.es</host>
  <host>hemeroteca.diputacionalicante.es</host>
  <host>gfw.diputacionalicante.es</host>
  <host>sede.diputacionalicante.es</host>
  <host>mi.diputacionalicante.es</host>
  <host>soportemunicipios.diputacionalicante.es</host>
  <host>formacion.diputacionalicante.es</host>
  <host>concursocentrocongresosalicante.diputacionalicante.es</host>
  <host>portal.diputacionalicante.es</host>
  <host>conductasadictivas.diputacionalicante.es</host>
</theHarvester>
```

A continuación, se muestra el archivo JSON generado por theHarvester:

```
{
    "asns": [
        "AS13335",
        "AS24940",
        "AS3352",
        "AS8560"
    ],
    "emails": [
        "bolsa.arpa@diputacionalicante.es",
        "bolsa.contrabajo@diputacionalicante.es",
        "bolsa.trombontenor@diputacionalicante.es",
        "bolsa.trompa@diputacionalicante.es",
        "bolsa.violin@diputacionalicante.es",
        "buengobierno@diputacionalicante.es",
        "ciudadanosextranjeros@diputacionalicante.es",
        "conserva@diputacionalicante.es",
        "consorciobomberos@diputacionalicante.es",
        "consorcioresiduosa2@diputacionalicante.es",
        "contratacion@diputacionalicante.es",
        "cultura@diputacionalicante.es",
        "edictos.bop@diputacionalicante.es",
        "formacio@diputacionalicante.es",
        "francisco.cano@diputacionalicante.es",
        "fruizfe@diputacionalicante.es",
        "galbert@diputacionalicante.es",
        "hacienda@diputacionalicante.es",
        "hogarprovincial@diputacionalicante.es",
        "iaccursos@diputacionalicante.es",
        "iberna@diputacionalicante.es",
        "igualdad@diputacionalicante.es",
        "imagen.promocion@diputacionalicante.es",
        "jcacho@diputacionalicante.es",
        "juanfran.perez@diputacionalicante.es",
        "juventud@diputacionalicante.es",
        "lbernabe@diputacionalicante.es",
```

```
        "lsanchez@diputacionalicante.es",
        "lvilapla@diputacionalicante.es",
        "mamartim@diputacionalicante.es",
        "miguel.lopez@diputacionalicante.es",
        "mjrico@diputacionalicante.es",
        "motero@diputacionalicante.es",
        "oficinapd@diputacionalicante.es",
        "plaosa@diputacionalicante.es",
        "preinfraestructuras@diputacionalicante.es",
        "prensa@diputacionalicante.es",
        "presidente@diputacionalicante.es",
        "protocolo.adda@diputacionalicante.es",
        "registro@diputacionalicante.es"
    ],
    "hosts": [
        "*.diputacionalicante.es",
        "1e1.diputacionalicante.es",
        "1e1.diputacionalicante.es:195.53.69.184",
        "1edicion.semcompol.diputacionalicante.es",
        "1edicion.semcompol.diputacionalicante.es:195.53.69.184",
        "2edicion.semcompol.diputacionalicante.es",
        "2edicion.semcompol.diputacionalicante.es:195.53.69.184",
        "3edicion.semcompol.diputacionalicante.es",
        "3edicion.semcompol.diputacionalicante.es:195.53.69.184",
        "Alicantecocentaina.diputacionalicante.es",
        "abierta-iaf.diputacionalicante.es",
        "abierta-iaf.diputacionalicante.es:195.53.69.162",
        "abierta-iaf.diputacionalicante.es:195.53.69.184",
        "abierta.diputacionalicante.es",
        "abierta.diputacionalicante.es:195.53.69.158",
        "abierta.diputacionalicante.es:195.53.69.184",
        "abiertaws.diputacionalicante.es",
        "abiertaws.diputacionalicante.es:195.53.69.162",
        "abiertaws.diputacionalicante.es:195.53.69.184",
        "acceso.diputacionalicante.es",
        "acceso.diputacionalicante.es:195.53.69.30",
        "accionvip-iaf.diputacionalicante.es",
        "accionvip-iaf.diputacionalicante.es:195.53.69.179",
        "accionvip-iaf.diputacionalicante.es:195.53.69.184",
        "acftest.diputacionalicante.es",
        "acftest.diputacionalicante.es:195.53.69.184",
        "agenda21.diputacionalicante.es",
        "agenda21.diputacionalicante.es:195.53.69.160",
        "agendacultural.diputacionalicante.es",
        "agendacultural.diputacionalicante.es:195.53.69.179",
        "agendacultural.diputacionalicante.es:195.53.69.184",
        "agendaculturalresources.diputacionalicante.es",
        "agendaculturalresources.diputacionalicante.es:195.53.69.157",
        "agendaphplist.diputacionalicante.es",
        "agendaphplist.diputacionalicante.es:195.53.69.184",
        "amigos.diputacionalicante.es",
        "amigos.diputacionalicante.es:195.53.69.184",
        "amigosphplist.diputacionalicante.es",
        "amigosphplist.diputacionalicante.es:195.53.69.184",
        "archivo.diputacionalicante.es",
```

```
        "aulavirtual-iafalicante.diputacionalicante.es",
        "aulavirtual-iafalicante.diputacionalicante.es:195.53.69.184",
        "autodiscover.diputacionalicante.es",
        "autodiscover.diputacionalicante.es:mail.diputacionalicante.es",
        "autodiscover.diputacionalicante.es:mail.diputacionalicante.es.",
        "aytosapp.diputacionalicante.es",
        "aytosapp.diputacionalicante.es:195.53.69.157",
        "azorinsv.diputacionalicante.es",
        "azorinsv.diputacionalicante.es:195.53.69.184",
        "blog.formacion.diputacionalicante.es",
        "blog.formacion.diputacionalicante.es:ghs.google.com",
        "blog.formacion.diputacionalicante.es:ghs.google.com.",
        "board.diputacionalicante.es",
        "board.diputacionalicante.es:195.53.69.146",
        "busot.diputacionalicante.es",
        "busot.diputacionalicante.es:195.53.69.179",
        "cajacredito.diputacionalicante.es",
        "cajacredito.diputacionalicante.es:195.53.69.184",
        "cajacreditonew.diputacionalicante.es",
        "cajacreditonew.diputacionalicante.es:195.53.69.179",
        "cesarsanchez.diputacionalicante.es",
        "clon.diputacionalicante.es",
        "clon.diputacionalicante.es:195.53.69.152",
        "clvprueba.diputacionalicante.es",
        "clvprueba.diputacionalicante.es:195.53.69.146",
        "clvpruebasdes.diputacionalicante.es",
        "clvpruebasdes.diputacionalicante.es:195.53.69.162",
        "clvpruebasdes.diputacionalicante.es:195.53.69.179",
        "cocentaina.diputacionalicante.es",
        "cocentaina.diputacionalicante.es:195.53.69.184",
        "concejalesayuntamientos.diputacionalicante.es",
        "concejalesayuntamientos.diputacionalicante.es:195.53.69.160",
        "concursocentrocongresosalicante.diputacionalicante.es",
        "concursocentrocongresosalicante.diputacionalicante.es:195.53.69.179",
        "conductasadictivas.diputacionalicante.es",
        "conductasadictivas.diputacionalicante.es:195.53.69.184",
        "congresotransparencia.diputacionalicante.es",
        "consorcioresiduosa2.diputacionalicante.es",
        "consorcioresiduosa2.diputacionalicante.es:195.53.69.179",
        "consorcioresiduosa2.diputacionalicante.es:195.53.69.184",
        "corporatepro.diputacionalicante.es",
        "corporatepro.diputacionalicante.es:195.53.69.184",
        "creama.diputacionalicante.es",
        "creama.diputacionalicante.es:195.53.69.184",
        "cuesprev.diputacionalicante.es",
        "cuesprev.diputacionalicante.es:195.53.69.184",
        "curso1-iafalicante.diputacionalicante.es",
        "curso1-iafalicante.diputacionalicante.es:195.53.69.179",
        "curso2-iafalicante.diputacionalicante.es",
        "curso2-iafalicante.diputacionalicante.es:195.53.69.179",
        "datosabiertos.diputacionalicante.es",
        "datosabiertos.diputacionalicante.es:195.53.69.184",
        "descargaglpi.diputacionalicante.es",
        "descargaglpi.diputacionalicante.es:195.53.69.160",
        "diputacionalicante.es:smtp.diputacionalicante.es",
```

```
146         "diputacionalicante.es:smtp.diputacionalicante.es.",
147         "documentacion.diputacionalicante.es",
148         "documentacion.diputacionalicante.es:195.53.69.160",
149         "documentosregistro.diputacionalicante.es",
150         "documentosregistro.diputacionalicante.es:195.53.69.179",
151         "dwnmedios.diputacionalicante.es",
152         "dwnmedios.diputacionalicante.es:195.53.69.160",
153         "eformacion.diputacionalicante.es",
154         "eformacion.diputacionalicante.es:95.61.88.71",
155         "eiel.diputacionalicante.es",
156         "encuestasua.diputacionalicante.es",
157         "encuestasua.diputacionalicante.es:195.53.69.184",
158         "espublicofiles.diputacionalicante.es",
159         "espublicofiles.diputacionalicante.es:195.53.69.146",
160         "euindustrydays.diputacionalicante.es",
161         "euindustrydays.diputacionalicante.es:195.53.69.184",
162         "eurojuv.diputacionalicante.es",
163         "eurojuv.diputacionalicante.es:195.53.69.179",
164         "eurojuv.diputacionalicante.es:195.53.69.184",
165         "europa.diputacionalicante.es",
166         "europa.diputacionalicante.es:195.53.69.184",
167         "expocreativa.diputacionalicante.es",
168         "expocreativa.diputacionalicante.es:195.53.69.184",
169         "formacion.diputacionalicante.es",
170         "formacion.diputacionalicante.es:195.53.69.160",
171         "formacion2.diputacionalicante.es",
172         "formacion2.diputacionalicante.es:195.53.69.160",
173         "foro.diputacionalicante.es",
174         "foro.diputacionalicante.es:195.53.69.184",
175         "forobienestar.diputacionalicante.es",
176         "forobienestar.diputacionalicante.es:195.53.69.152",
177         "foroinnovatet.diputacionalicante.es",
178         "foroinnovatet.diputacionalicante.es:195.53.69.184",
179         "ftpayuntamientos.diputacionalicante.es",
180         "ftpayuntamientos.diputacionalicante.es:195.53.69.152",
181         "ftpcoronavirus.diputacionalicante.es",
182         "ftpcoronavirus.diputacionalicante.es:195.53.69.160",
183         "ftpteleasistencia.diputacionalicante.es",
184         "ftpvideoactas.diputacionalicante.es",
185         "ftpvideoactas.diputacionalicante.es:195.53.69.160",
186         "gfw.diputacionalicante.es",
187         "gfw.diputacionalicante.es:195.53.69.151",
188         "gfwpreproductivo.diputacionalicante.es",
189         "gfwpreproductivo.diputacionalicante.es:195.53.69.151",
190         "glpi.diputacionalicante.es",
191         "glpi.diputacionalicante.es:195.53.69.184",
192         "graylog.diputacionalicante.es",
193         "grupociudadanos.diputacionalicante.es",
194         "grupociudadanos.diputacionalicante.es:195.53.69.179",
195         "grupocompromis.diputacionalicante.es",
196         "grupocompromis.diputacionalicante.es:195.53.69.179",
197         "grupocompromis.diputacionalicante.es:195.53.69.184",
198         "grupoesquerraunida.diputacionalicante.es",
199         "grupoesquerraunida.diputacionalicante.es:195.53.69.184",
200         "grupopopular.diputacionalicante.es",
```

```
        "grupopopular.diputacionalicante.es:195.53.69.179",
        "grupopopular.diputacionalicante.es:195.53.69.184",
        "gruposocialista.diputacionalicante.es",
        "gruposocialista.diputacionalicante.es:195.53.69.179",
        "hemeroteca.diputacionalicante.es",
        "hemeroteca.diputacionalicante.es:195.53.69.179",
        "hemeroteca.diputacionalicante.es:195.53.69.184",
        "hipokrates1-iaf.diputacionalicante.es",
        "hipokrates1-iaf.diputacionalicante.es:195.53.69.179",
        "hipokrates1-iaf.diputacionalicante.es:195.53.69.184",
        "hipokrates2-iaf.diputacionalicante.es",
        "hipokrates2-iaf.diputacionalicante.es:195.53.69.179",
        "holon.diputacionalicante.es",
        "holon.diputacionalicante.es:195.53.69.160",
        "indicadoresinf.diputacionalicante.es",
        "indicadoresinf.diputacionalicante.es:195.53.69.160",
        "indicadoressam.diputacionalicante.es",
        "indicadoressam.diputacionalicante.es:195.53.69.160",
        "informacionbop.diputacionalicante.es",
        "informacionbop.diputacionalicante.es:195.53.69.160",
        "international.diputacionalicante.es",
        "international.diputacionalicante.es:195.53.69.184",
        "iter-iaf.diputacionalicante.es",
        "iter-iaf.diputacionalicante.es:195.53.69.179",
        "iter-iaf.diputacionalicante.es:195.53.69.184",
        "jornadadeasistenciamunicipios.diputacionalicante.es",
        "jornadadeasistenciamunicipios.diputacionalicante.es:195.53.69.179",
        "jornadaeuropea.diputacionalicante.es",
        "jornadaeuropea.diputacionalicante.es:195.53.69.184",
        "jornadamoderniza.diputacionalicante.es",
        "jornadamoderniza.diputacionalicante.es:195.53.69.184",
        "jornadaprocedimientoadministrativo.diputacionalicante.es",
        "jornadaprocedimientoadministrativo.diputacionalicante.es:195.53.69.160",
        "jornadarelacionesafectivas.diputacionalicante.es",
        "jornadarelacionesafectivas.diputacionalicante.es:195.53.69.184",
        "limenew.diputacionalicante.es",
        "limenew.diputacionalicante.es:195.53.69.184",
        "lopd.diputacionalicante.es",
        "lopd.diputacionalicante.es:82.98.148.168",
        "mail.diputacionalicante.es",
        "mail.diputacionalicante.es:195.53.69.150",
        "mesadelagua.diputacionalicante.es",
        "mesadelagua.diputacionalicante.es:195.53.69.184",
        "mi.diputacionalicante.es",
        "mico-presupuestariagfw.diputacionalicante.es",
        "moderniza.diputacionalicante.es",
        "moderniza.diputacionalicante.es:195.53.69.10",
        "municipapp.diputacionalicante.es",
        "municipapp.diputacionalicante.es:195.53.69.179",
        "municipapp.diputacionalicante.es:195.53.69.184",
        "muro.diputacionalicante.es",
        "muro.diputacionalicante.es:195.53.69.184",
        "myadmin.diputacionalicante.es",
        "myadmin.diputacionalicante.es:195.53.69.179",
        "mysqlaccess.diputacionalicante.es",
```

```
256         "mysqlaccess.diputacionalicante.es:195.53.69.184",
257         "mysqlayuntamientos.diputacionalicante.es",
258         "mysqlayuntamientos.diputacionalicante.es:195.53.69.152",
259         "mysqldiputacion.diputacionalicante.es",
260         "mysqldiputacion.diputacionalicante.es:195.53.69.152",
261         "new.diputacionalicante.es",
262         "new.porqueesposible.diputacionalicante.es",
263         "new.porqueesposible.diputacionalicante.es:195.53.69.152",
264         "newdatos.diputacionalicante.es",
265         "newdatos.diputacionalicante.es:195.53.69.162",
266         "newdipu.diputacionalicante.es",
267         "newdipu.diputacionalicante.es:195.53.69.179",
268         "nicasede.diputacionalicante.es",
269         "nueva.diputacionalicante.es",
270         "nueva.diputacionalicante.es:195.53.69.149",
271         "nuevasede.diputacionalicante.es",
272         "nuevasede.diputacionalicante.es:195.53.69.146",
273         "orxetamaps.diputacionalicante.es",
274         "orxetamaps.diputacionalicante.es:195.53.69.152",
275         "parajesnaturales.diputacionalicante.es",
276         "parajesnaturales.diputacionalicante.es:195.53.69.179",
277         "parajesnaturales.diputacionalicante.es:195.53.69.184",
278         "participando.diputacionalicante.es",
279         "participando.diputacionalicante.es:195.53.69.179",
280         "participando.diputacionalicante.es:195.53.69.184",
281         "participandonew.diputacionalicante.es",
282         "participandonew.diputacionalicante.es:195.53.69.179",
283         "partmurodev.diputacionalicante.es",
284         "partmurodev.diputacionalicante.es:195.53.69.184",
285         "phplist.diputacionalicante.es",
286         "phplist.diputacionalicante.es:195.53.69.146",
287         "planes.diputacionalicante.es",
288         "planes.diputacionalicante.es:195.53.69.184",
289         "planmoderniza.diputacionalicante.es",
290         "planmoderniza.diputacionalicante.es:195.53.69.162",
291         "planmoderniza.diputacionalicante.es:195.53.69.184",
292         "planmodernizanew.diputacionalicante.es",
293         "planmodernizanew.diputacionalicante.es:195.53.69.179",
294         "pmh.diputacionalicante.es",
295         "pmh.diputacionalicante.es:195.53.69.14",
296         "podcastgilalbert.diputacionalicante.es",
297         "podcastgilalbert.diputacionalicante.es:195.53.69.184",
298         "porqueesposible.diputacionalicante.es",
299         "portal.diputacionalicante.es",
300         "portal.diputacionalicante.es:195.53.69.162",
301         "portal.diputacionalicante.es:195.53.69.184",
302         "portalpre.diputacionalicante.es",
303         "portalpre.diputacionalicante.es.diputacionalicante.es:195.53.69.179",
304         "portalpre.diputacionalicante.es:195.53.69.179",
305         "portalproveedor.diputacionalicante.es",
306         "predipupressres.diputacionalicante.es",
307         "predipupressres.diputacionalicante.es:195.53.69.146",
308         "preglpi.diputacionalicante.es",
309         "preglpi.diputacionalicante.es:195.53.69.179",
310         "premioazorin2020.diputacionalicante.es",
```

```
311         "premioazorin2020.diputacionalicante.es:195.53.69.179",
312         "premioazorin2020.diputacionalicante.es:195.53.69.184",
313         "premiosalbi.diputacionalicante.es",
314         "premiosalbi.diputacionalicante.es:195.53.69.149",
315         "presistemas.diputacionalicante.es",
316         "presistemas.diputacionalicante.es:195.53.69.146",
317         "procesosparticipativos.diputacionalicante.es",
318         "procesosparticipativos.diputacionalicante.es:195.53.69.184",
319         "promyadmin.diputacionalicante.es",
320         "promyadmin.diputacionalicante.es:195.53.69.184",
321         "pruebalime.diputacionalicante.es",
322         "pruebalime.diputacionalicante.es:195.53.69.146",
323         "pruebasmari.diputacionalicante.es",
324         "pruebasmari.diputacionalicante.es:195.53.69.184",
325         "pruebasmariwpml.diputacionalicante.es",
326         "pruebasmariwpml.diputacionalicante.es:195.53.69.184",
327         "pruebassede.diputacionalicante.es",
328         "pruebassede.diputacionalicante.es:195.53.69.188",
329         "registry.diputacionalicante.es",
330         "registry.diputacionalicante.es:195.53.69.179",
331         "registrypodman.diputacionalicante.es",
332         "registrypodman.diputacionalicante.es:172.16.14.151",
333         "repo1.diputacionalicante.es",
334         "sanmigueldesalinas.diputacionalicante.es",
335         "sanmigueldesalinas.diputacionalicante.es:195.53.69.152",
336         "scpi.diputacionalicante.es:195.53.69.162",
337         "sede.diputacionalicante.es",
338         "sede.diputacionalicante.es:195.53.69.179",
339         "sede.diputacionalicante.es:195.53.69.184",
340         "sededocs.diputacionalicante.es",
341         "sededocs.diputacionalicante.es:195.53.69.151",
342         "sededocsftp.diputacionalicante.es",
343         "sededocsftp.diputacionalicante.es:195.53.69.160",
344         "sedepre.diputacionalicante.es",
345         "sedepre.diputacionalicante.es:195.53.69.179",
346         "semcompol.diputacionalicante.es",
347         "semcompol.diputacionalicante.es:195.53.69.184",
348         "smtp.diputacionalicante.es",
349         "smtp.diputacionalicante.es:195.53.69.155",
350         "soportemunicipios.diputacionalicante.es",
351         "soportemunicipios.diputacionalicante.es:195.53.69.179",
352         "soportemunicipios.diputacionalicante.es:195.53.69.184",
353         "tasasmunicipales.diputacionalicante.es",
354         "tasasmunicipales.diputacionalicante.es:195.53.69.13",
355         "territoriointeligente.diputacionalicante.es",
356         "territoriointeligente.diputacionalicante.es:195.53.69.184",
357         "tollos.diputacionalicante.es",
358         "tollos.diputacionalicante.es:195.53.69.184",
359         "topcreation.diputacionalicante.es",
360         "torneodegolf.diputacionalicante.es",
361         "torneodegolf.diputacionalicante.es:195.53.69.184",
362         "tpv.diputacionalicante.es",
363         "tpv.diputacionalicante.es:195.53.69.145",
364         "tpvdes.diputacionalicante.es",
365         "tpvdes.diputacionalicante.es:195.53.69.145",
```

```
        "tramites.diputacionalicante.es",
        "tramites.diputacionalicante.es:195.53.69.142",
        "transparencia.diputacionalicante.es",
        "transparencia.diputacionalicante.es:195.53.69.149",
        "transparenciaws.diputacionalicante.es",
        "transparenciaws.diputacionalicante.es:195.53.69.145",
        "villenaold.diputacionalicante.es",
        "villenaold.diputacionalicante.es:195.53.69.152",
        "violenciasmachistas.diputacionalicante.es",
        "violenciasmachistas.diputacionalicante.es:195.53.69.179",
        "violenciasmachistas.diputacionalicante.es:195.53.69.184",
        "vm.diputacionalicante.es",
        "vm.diputacionalicante.es:195.53.69.160",
        "voluntariado.diputacionalicante.es",
        "voluntariado.diputacionalicante.es:195.53.69.184",
        "vpn.diputacionalicante.es",
        "vpn.diputacionalicante.es:195.53.69.1",
        "webservice.diputacionalicante.es",
        "webservice.diputacionalicante.es:195.53.69.141",
        "wifi4eulosmontesinos.diputacionalicante.es",
        "wifi4eulosmontesinos.diputacionalicante.es:195.53.69.179",
        "wifi4eulosmontesinos.diputacionalicante.es:195.53.69.184",
        "wpfordes.diputacionalicante.es",
        "wpfordes.diputacionalicante.es:195.53.69.188",
        "wpomiguel.diputacionalicante.es",
        "wpomiguel.diputacionalicante.es:195.53.69.184",
        "wsnominas.diputacionalicante.es",
        "wsnominas.diputacionalicante.es:195.53.69.145",
        "www2.diputacionalicante.es",
        "www2.diputacionalicante.es:195.53.69.186",
        "xixona.diputacionalicante.es",
        "xixona.diputacionalicante.es:195.53.69.179"
    ],
    "interesting_urls": [
        "http:\/\/acftest.diputacionalicante.es\/wp-content\/languages\/dismarket\/bracteate
            %20_sleaziness.html",
        "http:\/\/www.asddates.info\/?utm_source=5af3ff4b5a797&s=P2VFv7mO&r=http%3A%2F%2
            Fparticipando.diputacionalicante.es%2Fwp-content%2Fcache%2Fempyromancy%2
            FCopaifera_tattva.html&fp=
            JTVCJTdCJTIya2V5JTIyJTNBJTIydXNlckFnZW50JTIyJTJDJTIydmFsdWUlMjIlM0ElMjJNb3ppbGxhJTJGNS4wJTIwKE1hY
            =",
        "https:\/\/planmoderniza.diputacionalicante.es\/"
    ],
    "ips": [
        "104.21.75.10",
        "144.76.30.237",
        "172.16.14.151",
        "173.194.195.121",
        "194.224.22.237",
        "195.53.69.14",
        "195.53.69.149",
        "195.53.69.151",
        "195.53.69.152",
        "195.53.69.157",
        "195.53.69.160",
```

```
        "195.53.69.162",
        "195.53.69.179",
        "195.53.69.184",
        "216.58.193.83",
        "216.58.213.147",
        "2606:4700:3033::6815:3cab",
        "2606:4700:3037::6815:3ed3",
        "82.223.111.50",
        "95.61.88.71"
    ],
    "shodan": []
}
```

Bibliografía

[1] *Infografía: El Big Bang del Big Data*. es. Oct. de 2021. URL: https://es.statista.com/grafico/26031/volumen-estimado-de-datos-digitales-creados-o-replicados-en-todo-el-mundo (visitado 15-10-2023).

[2] G.D. Singh. *Learn Kali Linux 2019: Perform powerful penetration testing using Kali Linux, Metasploit, Nessus, Nmap, and Wireshark*. Packt Publishing, 2019. ISBN: 978-1-78961-262-2. URL: https://books.google.es/books?id=H6a-DwAAQBAJ.

[3] RUBÉN G LÓPEZ. "El mejor amigo del ciberdelincuente es... usted". En: *Actualidad Economica (Madrid, Spain)* (2018). Place: Madrid Publisher: Unidad Editorial Revistas, S.L.U, pág. 14. ISSN: 0001-7655.

[4] "REGLAMENTO (UE) 2016/ 679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO - de 27 de abril de 2016 - relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/ 46/ CE (Reglamento general de protección de datos)". es. En: ().

[5] Javier Pastor-Galindo et al. "The Not Yet Exploited Goldmine of OSINT: Opportunities, Open Challenges and Future Trends". en. En: *IEEE Access* 8 (2020), págs. 10282-10304. ISSN: 2169-3536. DOI: 10.1109/ACCESS.2020.2965257. URL: https://ieeexplore.ieee.org/document/8954668/ (visitado 14-10-2023).

[6] Inés Sánchez-Muliterno Bleda. "El peligro de la exposición de información en los tiempos de las redes sociales". Tesis doct. Universitat Oberta de Catalunya (UOC), 2023.

[7] *Objetivos de Desarrollo Sostenible | Programa De Las Naciones Unidas Para El Desarrollo*. es. URL: https://www.undp.org/es/sustainable-development-goals (visitado 14-10-2023).

[8] Oscar Sánchez Belmont. *Ciberinteligencia y cibercontrainteligencia*. Ciudad de México: Instituto Mexicano de Contadores Públicos, 2021. ISBN: 607-563-094-5.

[9] fernando.diez. *La Inteligencia Artificial y su papel en la ciberinteligencia*. es. Sep. de 2023. URL: https://www.redseguridad.com/especialidades-tic/ciberinteligencia/la-inteligencia-artificial-y-su-papel-en-la-ciberinteligencia_20230912.html (visitado 29-10-2023).

[10] *¿Qué es la ciberinteligencia? Principales tipos y usos*. es. URL: https://www.unir.net/ingenieria/revista/ciberinteligencia/ (visitado 29-10-2023).

[11] *Ciberseguridad: amenazas principales y emergentes | Noticias | Parlamento Europeo*. es. Ene. de 2022. URL: https://www.europarl.europa.eu/news/es/headlines/society/20220120STO21428/ciberseguridad-amenazas-principales-y-emergentes (visitado 29-10-2023).

[12] *La IA y el machine learning en la ciberseguridad: cómo determinarán el futuro*. es. Section: Resource Center. Abr. de 2023. URL: https://www.kaspersky.es/resource-center/definitions/ai-cybersecurity (visitado 29-10-2023).

[13] United Nations. *Seguridad cibernética: un problema mundial que demanda un enfoque mundial | Naciones Unidas*. es. Publisher: United Nations. URL: https://www.un.org/es/desa/seguridad-cibernetica (visitado 29-10-2023).

[14] *Caza de ciberamenazas: todo lo que debes saber*. es. URL: https://ciberseguridad.com/servicios/caza-ciberamenazas/ (visitado 29-10-2023).

[15] *Desarrollo en cascada*. es. Page Version ID: 154583679. Oct. de 2023. URL: https://es.wikipedia.org/w/index.php?title=Desarrollo_en_cascada&oldid=154583679 (visitado 14-10-2023).

[16] *Contenidos de la asignatura: TFG - Seguridad informática - Aula 1*. URL: https://aula.uoc.edu/courses/7773/modules (visitado 14-10-2023).

[17] *Diagrama de Gantt*. es. Page Version ID: 153182377. Ago. de 2023. URL: https://es.wikipedia.org/w/index.php?title=Diagrama_de_Gantt&oldid=153182377 (visitado 14-10-2023).

[18] D.S. Orcero. *La Biblia de LaTeX: Aprende a Escribir Tesis, Artículos, Trabajos Fin de Grado y Presentaciones con Terminación Profesional*. Ed. Coronado, 2019. ISBN: 978-1-79540-971-1. URL: https://books.google.es/books?id=q0HSwQEACAAJ.

[19] Félix Brezo Fernández y Yaiza Rubio Viñuela. *Manual de Ciberinvestigación en Fuentes Abiertas: OSINT para Analistas*. es. Google-Books-ID: 9vUwzQEACAAJ. Independently Published, dic. de 2019. ISBN: 978-1-65089-574-1.

[20] José Lominchar Jiménez y Pablo Luis Gómez Sierra. *Principios de ciberinteligencia / José Lominchar Jiménez ; Pablo Luis Gómez Sierra*. Madrid: Centro de Estudios Financieros CEF, 2022. ISBN: 978-84-454-4469-6.

[21] *Glosario - Ministerio de Defensa de España*. URL: https://www.defensa.gob.es/defensa_yo/glosario/ (visitado 14-10-2023).

[22] Rafael Jiménez Villalonga. *El ciclo de Inteligencia: una explicación didáctica*. es. Abr. de 2020. URL: https://global-strategy.org/el-ciclo-de-inteligencia-una-explicacion-didactica/ (visitado 14-10-2023).

[23] *Inteligencia de imágenes (IMINT): misión, función y salidas profesionales*. es. URL: https://www.lisainstitute.com/blogs/blog/inteligencia-imagenes-imint (visitado 16-10-2023).

[24] *Measurement and signature intelligence*. en. Page Version ID: 1176087657. Sep. de 2023. URL: https://en.wikipedia.org/w/index.php?title=Measurement_and_signature_intelligence&oldid=1176087657 (visitado 16-10-2023).

[25] *Inteligencia electrónica - Wikipedia, la enciclopedia libre*. URL: https://es.wikipedia.org/wiki/Inteligencia_electr%C3%B3nica (visitado 18-10-2023).

[26] *Geospatial intelligence*. en. Page Version ID: 1148115600. Abr. de 2023. URL: https://en.wikipedia.org/w/index.php?title=Geospatial_intelligence&oldid=1148115600 (visitado 18-10-2023).

[27] *Strategic intelligence*. en. Page Version ID: 1135435580. Ene. de 2023. URL: https://en.wikipedia.org/w/index.php?title=Strategic_intelligence&oldid=1135435580 (visitado 18-10-2023).

[28] N.A. Hassan y R. Hijazi. *Open Source Intelligence Methods and Tools: A Practical Guide to Online Intelligence*. Ciando library. Apress, 2018. ISBN: 978-1-4842-3213-2. URL: https://books.google.es/books?id=AqNiDwAAQBAJ.

[29] *Sesgo cognitivo*. es. Page Version ID: 154210142. Sep. de 2023. URL: https://es.wikipedia.org/w/index.php?title=Sesgo_cognitivo&oldid=154210142 (visitado 25-10-2023).

[30] *Falacia*. es. Page Version ID: 154453353. Oct. de 2023. URL: https://es.wikipedia.org/w/index.php?title=Falacia&oldid=154453353 (visitado 25-10-2023).

[31] *Ciberinvestigación y técnicas OSINT en informática forense*. es. Section: Blog de peritaje informático. Oct. de 2021. URL: https://indalics.com/blog/ciberinvestigacion-osint (visitado 14-10-2023).

[32] *Wikipedia:Verificabilidad*. es. Page Version ID: 154568902. Oct. de 2023. URL: https://es.wikipedia.org/w/index.php?title=Wikipedia:Verificabilidad&oldid=154568902 (visitado 14-10-2023).

[33] *CCN-CERT BP/13 Desinformación en el Ciberespacio*. URL: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-buenas-practicas-bp/3549-ccn-cert-bp-13-desinformacion-en-el-ciberespacio.html (visitado 14-10-2023).

[34] *2023 Edelman Trust Barometer*. en. URL: https://www.edelman.com/trust/2023/trust-barometer (visitado 25-10-2023).

[35] Maria Inês Tomaél, Maria Elisabete Catarino y Marta Lígia Pomim Valentim. "Evaluación de fuentes de información en Internet: Criterios de calidad". es. En: 32.2 (2001).

[36] *Army Publishing Directorate – Publications/Forms Content Search*. URL: https://armypubs.army.mil/ProductMaps/PubForm/ContentSearch.aspx?q=humint (visitado 25-10-2023).

[37] Kai-Cheng Yang y Filippo Menczer. *Large language models can rate news outlet credibility*. arXiv:2304.00228 [cs]. Abr. de 2023. URL: http://arxiv.org/abs/2304.00228 (visitado 14-10-2023).

[38] *Media Bias/Fact Check News*. en-US. Oct. de 2023. URL: https://mediabiasfactcheck.com/ (visitado 14-10-2023).

[39] *Internet Archive: About IA*. URL: https://archive.org/about/ (visitado 15-10-2023).

[40] *Internet Archive: Wayback Machine*. URL: https://archive.org/web/ (visitado 15-10-2023).

[41] *Metadatos*. es. Page Version ID: 154521924. Oct. de 2023. URL: https://es.wikipedia.org/w/index.php?title=Metadatos&oldid=154521924 (visitado 15-10-2023).

[42] *Número mágico (informática)*. es. Page Version ID: 142411973. Mar. de 2022. URL: https://es.wikipedia.org/w/index.php?title=N%C3%BAmero_m%C3%A1gico_(inform%C3%A1tica)&oldid=142411973 (visitado 15-10-2023).

[43] *List of file signatures*. en. Page Version ID: 1177316390. Sep. de 2023. URL: https://en.wikipedia.org/w/index.php?title=List_of_file_signatures&oldid=1177316390 (visitado 15-10-2023).

[44] A. Roberts. *Cyber Threat Intelligence: The No-Nonsense Guide for CISOs and Security Managers*. Apress, 2021. ISBN: 978-1-4842-7219-0. URL: https://books.google.es/books?id=nD19zgEACAAJ.

[45] *Plataforma de inteligencia contra amenazas*. es. Page Version ID: 154488131. Oct. de 2023. URL: https://es.wikipedia.org/w/index.php?title=Plataforma_de_inteligencia_contra_amenazas&oldid=154488131 (visitado 16-10-2023).

[46] *Indicador de compromiso*. es. Page Version ID: 154333260. Oct. de 2023. URL: https://es.wikipedia.org/w/index.php?title=Indicador_de_compromiso&oldid=154333260 (visitado 16-10-2023).

[47] *Tácticas, técnicas y procedimientos*. es. Page Version ID: 154333305. Oct. de 2023. URL: https://es.wikipedia.org/w/index.php?title=T%C3%A1cticas,_t%C3%A9cnicas_y_procedimientos&oldid=154333305 (visitado 16-10-2023).

[48] CiudadRegion. *El crecimiento de Discord en los últimos años*. es. Feb. de 2022. URL: https://www.ciudadregion.com/entretenimiento/el-crecimiento-de-discord-en-los-ultimos-anos (visitado 24-10-2023).

[49] M. Bazzell. *Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information*. Independently Published, 2021. ISBN: 9798578577086. URL: https://books.google.es/books?id=WKAxzgEACAAJ.

[50] *Las Cookies: Todo lo que necesitas saber*. URL: https://www.techbuddy.es/post/las-cookies-todo-lo-que-necesitas-saber (visitado 11-11-2023).

[51] *Evercookie*. en. Page Version ID: 1169110760. Ago. de 2023. URL: https://en.wikipedia.org/w/index.php?title=Evercookie&oldid=1169110760 (visitado 11-11-2023).

[52] Norfi Carrodeguas. *Desactivar en Windows 10 la Telemetría y el seguimiento de Microsoft*. es. URL: https://norfipc.com/articulos/desactivar-windows-10-telemetria-seguimiento-microsoft.php (visitado 01-11-2023).

[53] *Pharming*. es. Page Version ID: 154742094. Oct. de 2023. URL: https://es.wikipedia.org/w/index.php?title=Pharming&oldid=154742094 (visitado 01-11-2023).

[54] *Shoulder surfing*. es-ES. Sep. de 2023. URL: https://www.ionos.es/digitalguide/servidores/seguridad/shoulder-surfing/ (visitado 05-11-2023).

[55] scooley. *Habilitar Hyper-V en Windows 10*. es-es. Jul. de 2023. URL: https://learn.microsoft.com/es-es/virtualization/hyper-v-on-windows/quick-start/enable-hyper-v (visitado 12-11-2023).

[56] Cl4r4. *OriON*. original-date: 2023-04-06T14:39:45Z. Nov. de 2023. URL: https://github.com/Cl4r4-5/OriON (visitado 14-11-2023).

[57] *Google dorks: ¿Qué son los Google Hacks y cómo se utilizan?* en. URL: https://www.avg.com/es/signal/google-dorks (visitado 28-11-2023).

[58] *¿Qué es el Internet de las cosas (IoT) y cómo funciona?* es. URL: https://www.redhat.com/es/topics/internet-of-things/what-is-iot (visitado 15-12-2023).

[59] Brayan José Maeso Mateos. "OSINT: estudio, automatización e integración de diferentes herramientas para la obtención de información de fuentes abiertas". Tesis doct. Universitat Oberta de Catalunya (UOC), 2023.

[60] *Have I Been Pwned: Pastes*. URL: https://haveibeenpwned.com/Pastes (visitado 29-11-2023).

[61] *EmailRep Alpha Risk API*. original-date: 2019-04-09T00:23:34Z. Dic. de 2023. URL: https://github.com/sublime-security/emailrep.io (visitado 14-12-2023).

[62] *sherlock/sites.md at master · sherlock-project/sherlock · GitHub*. URL: https://github.com/sherlock-project/sherlock/blob/master/sites.md (visitado 28-12-2023).

[63] *¿Qué es una superficie de ataque? | IBM*. es-es. URL: https://www.ibm.com/es-es/topics/attack-surface (visitado 14-12-2023).

[64] Jhon Heyder Murillo Mejia. "Técnicas de OSINT para la evaluación de la superficie de ataque". Tesis doct. Universitat Oberta de Catalunya (UOC), 2023.

[65] Sharon Abraham Ratna. *Descubra amenazas de los puertos abiertos y mejore la seguridad con herramientas de análisis de puertos*. en-US. Jul. de 2021. URL: https://blogs.manageengine.com/espanol/2021/07/07/descubrimiento-amenazas-puertos-abiertos-htas-analisis-puertos.html (visitado 14-12-2023).

[66] Pilar Muniesa Tomás et al. "Informe sobre la cibercriminalidad en España 2022". es. En: (2022).

[67] *La lista completa de todas las extensiones de archivo, formatos y significados*. es. URL: https://fileformats.org/es/file-types/ (visitado 15-10-2023).

[68] *Recommended Formats Statement - Resources (Preservation, Library of Congress)*. eng. web page. URL: https://www.loc.gov/preservation/resources/rfs/index.html (visitado 15-10-2023).

[69] *Archivo de texto*. es. Page Version ID: 147227232. Nov. de 2022. URL: https://es.wikipedia.org/w/index.php?title=Archivo_de_texto&oldid=147227232 (visitado 15-10-2023).

[70] *Archivo binario*. es. Page Version ID: 153939375. Sep. de 2023. URL: https://es.wikipedia.org/w/index.php?title=Archivo_binario&oldid=153939375 (visitado 15-10-2023).

[71] *JSON*. es. Page Version ID: 152887490. Ago. de 2023. URL: https://es.wikipedia.org/w/index.php?title=JSON&oldid=152887490 (visitado 15-10-2023).

[72] Tim Bray. *The JavaScript Object Notation (JSON) Data Interchange Format*. Request for Comments RFC 7159. Num Pages: 16. Internet Engineering Task Force, mar. de 2014. DOI: 10.17487/RFC7159. URL: https://datatracker.ietf.org/doc/rfc7159 (visitado 15-10-2023).

[73] *Extensible Markup Language*. es. Page Version ID: 146365513. Oct. de 2022. URL: https://es.wikipedia.org/w/index.php?title=Extensible_Markup_Language&oldid=146365513 (visitado 15-10-2023).

[74] *Extensible Markup Language (XML)*. URL: https://www.w3.org/XML/ (visitado 15-10-2023).

[75] *Valores separados por comas*. es. Page Version ID: 153277888. Ago. de 2023. URL: https://es.wikipedia.org/w/index.php?title=Valores_separados_por_comas&oldid=153277888 (visitado 15-10-2023).

[76] Yakov Shafranovich. *Common Format and MIME Type for Comma-Separated Values (CSV) Files*. Request for Comments RFC 4180. Num Pages: 8. Internet Engineering Task Force, oct. de 2005. DOI: 10.17487/RFC4180. URL: https://datatracker.ietf.org/doc/rfc4180 (visitado 15-10-2023).

[77] *IBM Generalized Markup Language*. es. Page Version ID: 154426649. Oct. de 2023. URL: https://es.wikipedia.org/w/index.php?title=IBM_Generalized_Markup_Language&oldid=154426649 (visitado 15-10-2023).

[78] *Gephi*. es. Page Version ID: 146186933. Sep. de 2022. URL: https://es.wikipedia.org/w/index.php?title=Gephi&oldid=146186933 (visitado 15-10-2023).

[79] *GraphML*. en. Page Version ID: 1060832076. Dic. de 2021. URL: https://en.wikipedia.org/w/index.php?title=GraphML&oldid=1060832076 (visitado 15-10-2023).

[80] *Expresión regular*. es. Page Version ID: 153778257. Sep. de 2023. URL: https://es.wikipedia.org/w/index.php?title=Expresi%C3%B3n_regular&oldid=153778257 (visitado 15-10-2023).

[81] *grep*. es. Page Version ID: 153884826. Sep. de 2023. URL: https://es.wikipedia.org/w/index.php?title=Grep&oldid=153884826 (visitado 15-10-2023).

[82] *grep(1) - Linux manual page*. URL: https://www.man7.org/linux/man-pages/man1/grep.1.html (visitado 15-10-2023).

[83] *egrep(1): print lines matching pattern - Linux man page*. URL: https://linux.die.net/man/1/egrep (visitado 15-10-2023).

[84] John C. Klensin. *Application Techniques for Checking and Transformation of Names*. Request for Comments RFC 3696. Num Pages: 16. Internet Engineering Task Force, feb. de 2004. DOI: 10.17487/RFC3696. URL: https://datatracker.ietf.org/doc/rfc3696 (visitado 15-10-2023).

[85] *Email address*. en. Page Version ID: 1179767636. Oct. de 2023. URL: https://en.wikipedia.org/w/index.php?title=Email_address&oldid=1179767636 (visitado 15-10-2023).

[86] *Internet Protocol*. Request for Comments RFC 791. Num Pages: 51. Internet Engineering Task Force, sep. de 1981. DOI: 10.17487/RFC0791. URL: https://datatracker.ietf.org/doc/rfc791 (visitado 25-10-2023).