ANÁLISIS DEL NIVEL DE EXPOSICIÓN Y PRIVACIDAD DE INFORMACIÓN PERSONAL EN FUENTES ABIERTAS A TRAVÉS DE LA METODOLOGÍA *OPEN SOURCE INTELLIGENCE* (OSINT)

DAVID ALFONSO VEGA PALACIO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
2021

ANÁLISIS DEL NIVEL DE EXPOSICIÓN Y PRIVACIDAD DE INFORMACIÓN PERSONAL EN FUENTES ABIERTAS A TRAVÉS DE LA METODOLOGÍA *OPEN SOURCE INTELLIGENCE* (OSINT)

DAVID ALFONSO VEGA PALACIO

Proyecto de Grado – Monografía presentado para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Yolima Mercado
Directora de Trabajo de Grado

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
2021

NOTA DE ACEPTACIÓN

Firma del presidente de Jurado

Firma del Jurado

Firma del Jurado

Riohacha, 07 de abril de 2022

DEDICATORIA

A mi padre por sus consejos de vida, a mis indígenas por qué podemos hacer país desde la inclusión y unidad nacional para el beneficio colectivo de nuestros pueblos.

AGRADECIMIENTOS

Agradezco a las directivas de la Universidad Nacional Abierta y a Distancia UNAD, quienes con su trabajo continuo nos brindan la oportunidad de estudiar y laborar, por otro lado a cada uno de los tutores y asesores que me acompañaron en el proceso les reconozco que sin su apoyo y colaboración éste logro no hubiera sido posible.

CONTENIDO

PÁG.

LISTA DE FIGURAS

Pág.

GLOSARIO

FUENTES ABIERTAS: canal de obtención de información de carácter público y de forma gratuita.

FUENTES CERRADAS: canal de obtención de información de carácter privado y limitado en su acceso.

INFORMACIÓN: conjunto de datos ordenados de forma lógica que trasmite una idea a quien lo interpreta, sirve para trasmitir un mensaje en general o especifico.

PRIVACIDAD: hace referencia a un contexto íntimo de carácter personal, y con limitaciones de acceso al público.

INTELIGENCIA: toma de decisión asertiva frente una información.

INTERNET: red global de transferencia de datos.

RED SOCIAL: comunidad virtual que tiene como objetivo compartir información general de carácter público.

TARGET: objetivo en concreto donde se centra los esfuerzos para la obtención de información.

TÉCNICA: conjunto de acciones para lograr un resultado.

EXPOSICIÓN: acción que busca presentar una información.

RESUMEN

El presente documento monográfico pretende contextualizar al lector en la importancia de la privacidad de su información personal en fuentes abiertas y permite recomendar acciones de buenas prácticas en la publicación de contenidos digitales en internet.

Se soporta en la recolección de distintas fuentes de información y busca la obtención de una visión general del comportamiento y percepción del internauta en la publicación de contenidos personales en fuentes abiertas, pretendiendo demostrar mediante técnicas de *Open Source Intelligence* (OSINT) el nivel de exposición de la privacidad personal en internet tomando como tesis principal que la vulnerabilidad más susceptible en cualquier sistema informático es el ser humano.

Por lo que conocer algunas de las múltiples herramientas brindadas por la metodología *Open Source Intelligence* (OSINT) para la correcta toma de decisión en el robustecimiento de la exposición y privacidad de información personal en fuentes abiertas, permite al internauta evitar ser víctimas como robo de identidad, ataques informáticos y otras circunstancias que vulneren el derecho de su intimidad y buen nombre.

ABSTRACT

This monographic document aims to contextualize the reader on the importance of the privacy of their personal information in open sources and recommend good practice actions in the publication of digital content on the internet.

It is supported by qualitative research as it seeks to obtain an overview of the behavior and perception of the user in the publication of personal content in open sources, trying to demonstrate through Open Source Intelligence (OSINT) techniques the level of exposure of personal privacy in these sources taking as the main thesis that the most susceptible vulnerability in any computer system is human ignorance in the manipulation of information tools.

In such a way that knowing some of the multiple tools provided by the Open Source Intelligence (OSINT) methodology for the correct decision-making in strengthening the exposure and privacy of personal information in open sources, allows the digital user to avoid being victims of theft. identity, impersonation, computer attacks and other circumstances that violate the right to privacy and good name.

INTRODUCCIÓN

La privacidad de la información hace referencia al ámbito personal desarrollado en un espacio reservado cuyo propósito es mantener la confidencialidad; dicha actividad en el uso de sistemas informáticos es confundida con el uso de contraseñas complejas de controles de acceso, sin embargo para la seguridad informática el termino de privacidad hace referencia al poder de autoridad de establecer acciones para su consulta, distribución y medios de propagación.

Existen situaciones en la que se desconoce cómo se trata la información de los datos personales en su almacenamiento, medios de consulta, amparo legal y otras consideraciones que pueden poner en riesgo la privacidad de la información en su alto grado de nivel de exposición al público en general.

El internauta promedio no tiene claro el conocimiento de que es una información sensible, poniendo en riesgo su privacidad personal en la publicación de contenidos digitales en las distintas fuentes abiertas como las redes sociales, permitiendo con esta acción que sea blanco de un perfilamiento que viole su confidencialidad en su ubicación geográfica, números de teléfonos, dirección residencial, actividad profesional entre otros aspectos valiosos para un investigador.

Hablar de la metodología *Open Source Intelligence* (OSINT) o en su traducción al español “Inteligencia en fuentes abiertas”, permite al internauta poder consultar el nivel de exposición y privacidad de una información contenida en fuentes abiertas y tomar decisiones asertivas sobre la misma que permita alcanzar el nivel de confidencialidad deseado.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

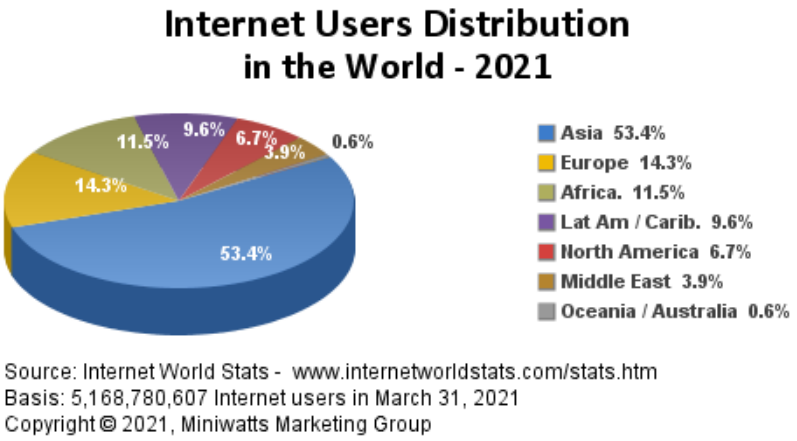
Las nuevas formas de comunicación del ser humano en el último siglo han sufrido un gran cambio desde comenzó a hacerlo, permitiendo hoy en día el uso de herramientas para tal propósito como los son dispositivos electrónicos que rompen las distancias iniciales de comunicación.

El Internet es un medio de comunicación de gran crecimiento global y una estupenda fuente de información para la sociedad actual, un estudio realizado en marzo del año 2021 por *Internet world stats*[1] se calcula que existen alrededor de cinco mil ciento sesenta y ocho millones setecientos ochenta mil seiscientos siete (5,168,780,607) de usuarios activos compartiendo datos, muchos de ellos sin restricción comprometiendo la privacidad personal en su alta exposición en fuentes abiertas.

En la Figura 1, se detalla en cantidad porcentual la distribución de los usuarios activos en los distintos continentes, que hacen uso de internet.

[1] Internet world stats [sitio web] Internet Usage Statistics World Internet -Users and 2021 Population Stats [Accedido el 20 de octubre 2021] Disponible en: https://www.internetworldstats.com/stats.htm

Figura 1 Distribución de usuarios activos en internet en el mundo año 2021



Fuente Internet World Stats [Sitio web] Imagen Internet Users Distribution in the world 2021[Formato png] Disponible en : https://www.internetworldstats.com/images/world2021PIE1.png

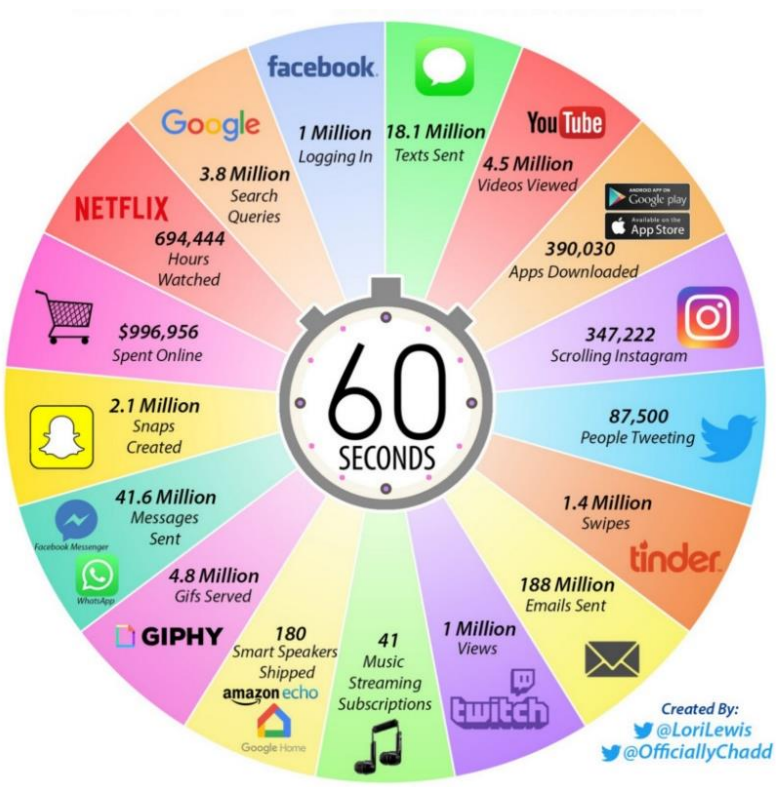
La Figura 2 es la realización de una infografía descriptiva expuesta por Lori Lewis[2], y agrega la actividad en línea de miles de millones de personas en todo el mundo, para ver cómo se ve un minuto en Internet durante el año 2019.

¿Cómo es posible que se envíen 188 millones de correos electrónicos por minuto? ¿Cómo procesa Google 3,8 millones de consultas de búsqueda en tan poco tiempo?

En pocas palabras, la cantidad de acciones agrupadas en solo 60 segundos es extraordinaria. Una comparación lado a lado internet es increíblemente dinámico, lo que significa que siempre hay segmentos nuevos e interesantes que surgen.
¿pero cuanta información de carácter personal están expuesta a la vulneración de la privacidad?

[2]twitter.com [sitio web] Perfil Lori Lewis [Accedido el 20 de octubre 2020] Disponible en: https://twitter.com/lorilewis

Figura 2 Esto es lo que pasa en un minuto en internet año 2019



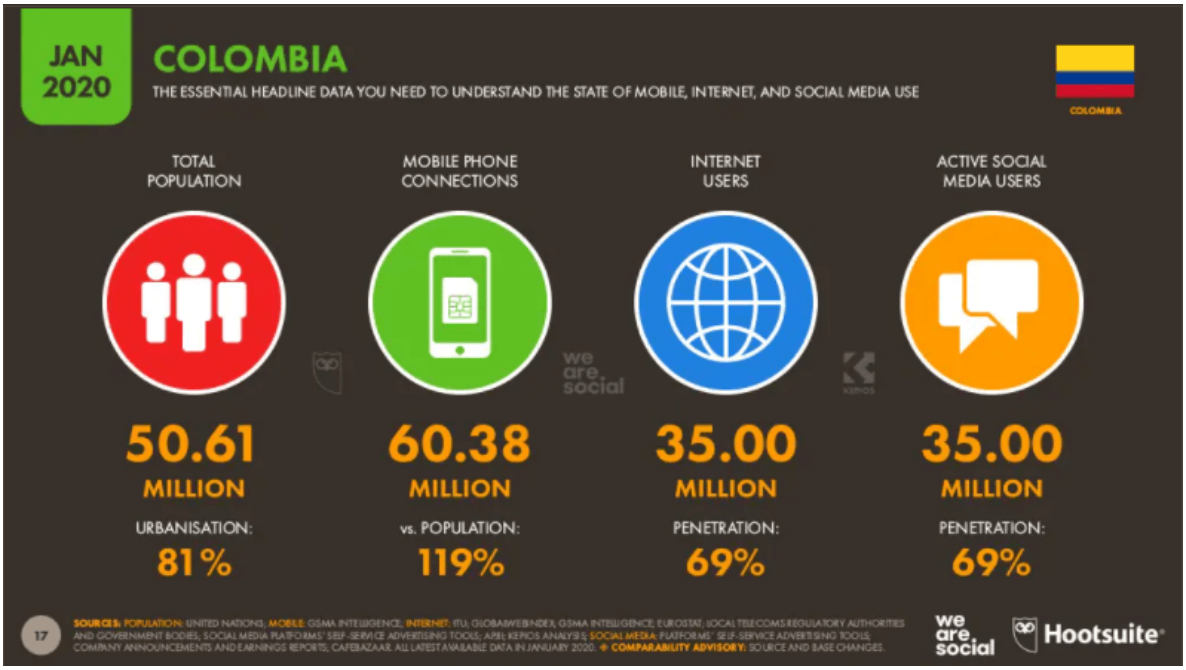
Fuente visualcapitalist.com [Sitio web] What Happens in an-Internet Minute in 2019? [Archivo en formato png] Disponible en: https://www.visualcapitalist.com/what-happens-in-an-internet-minute-in-2019/

En el contexto colombiano un reporte realizado a enero del año 2020 por *Datareportal*[3] para ayudar a las personas y organizaciones de todo el mundo a encontrar los datos, los conocimientos y las tendencias que necesitan para tomar decisiones mejor informadas, detalla que en Colombia existe treinta y cinco millones (35.000.000) de usuarios que hacen uso de internet equivalente al 69% de la población. En respuesta el gobierno colombiano ha implementado leyes para el control y aseguramiento de la información, sin embargo, éstas no han sido suficiente para la mitigación de diferentes delitos informáticos relacionados a la vulneración de la privacidad personal.

[3] KEMP, Simone. Digital 2020: Colombia. [sitio web] [accedido el 20 de octubre 2020] Disponible en: https://datareportal.com/reports/digital-2020-colombia

En la Figura 3 hace mención al reporte de *Datareportal* para Colombia en año 2020, realizando descripción del acceso a conexión de líneas de celulares, usuarios activos de internet y redes sociales.

Figura 3 Reporte de Colombia año 2020 acceso a internet



Fuente Datareportal [Sitio web] Archivo en formato jpg, Disponible en: https://datareportal.com/reports/digital-2020-colombia

De tal forma que es necesario contar con una metodología para el control y conocimiento de la exposición de la información personal en fuentes abiertas, que ayuden al internauta robustecer la privacidad en internet, por lo que surgen marcos de trabajo como *Open Source Intelligence* (OSINT) para tal propósito dando origen a la formación del problema de este documento.

1.2 FORMULACIÓN DEL PROBLEMA

¿Cómo incide en el internauta la implementación de la metodología *Open Source Intelligence* (OSINT) para el análisis del nivel de exposición y privacidad de información personal en fuentes abiertas?

2 JUSTIFICACIÓN

Dada la proliferación de información en internet es conveniente adoptar marcos de trabajo que brinden el conocimiento suficiente a los internautas de poder consultar el nivel de exposición y privacidad en las distintas fuentes abiertas.

La importancia del presente trabajo es de exponer la metodología *Open Source Intelligence* (OSINT) como herramienta propicia para tal objetivo, brindando al internauta el poder de decisión en la publicación de contenidos digitales en las distintas fuentes de información y brindando beneficios como:

- Mejoramiento del nivel de exposición de datos sensibles.
- Detección de datos falsificados.
- Reconocimientos de noticias falsas que puedan afectar la imagen personal.
- Controlar datos de carácter personal expuesta en fuentes abiertas.

De tal forma se permite relacionar un sin número de utilidades que justifican conocer la metodología en mención y su implementación en el área de seguridad informática, no obstante, también es aplicable en áreas como:

- *Marketing*: Permite realizar análisis de mercado en base a tendencias.
- Talento Humano: Permite reclutar perfiles cualificados para determinadas áreas de la organización.
- Fuerza pública: Permite anticiparse a futuros delitos o aplicar ingeniería social inversa sobre sospechosos.
- Jurídico: Permite recolectar evidencia digital en algunos casos.

3 OBJETIVOS

3.1 OBJETIVOS GENERAL

Analizar el nivel de exposición y privacidad de información personal en fuentes abiertas de un internauta utilizando la metodología *Open Source Intelligence* (OSINT) y proponer a través del área de seguridad informática recomendaciones para la publicación de contenidos digitales en fuentes abiertas.

3.2 OBJETIVOS ESPECÍFICOS

Identificar tipos de fuentes de obtención de información de carácter público necesarios para la aplicación de la metodología *Open Source Intelligence* (OSINT).

Inspeccionar el marco de investigación *Open Source Intelligence* (OSINT) dentro de sus aplicaciones, métodos y alcances en la recolección de información personal en fuentes abiertas.

Evaluar un caso práctico el nivel de exposición y privacidad de información personal en un internauta por medio de alguna de las herramientas brindada por la metodología open source intelligence (OSINT).

Proponer recomendaciones para el mejoramiento de la privacidad de la información personal en la publicación de contenidos digitales en fuentes abiertas y prevención de riesgos cibernéticos.

4 MARCO REFERENCIAL

4.1 MARCO TEÓRICO

4.1.1 Metodología Open Source Intelligence (OSINT). La metodología O*pen Source Intelligence* (OSINT) se traduce como la inteligencia en fuentes abiertas para la obtención y tratamiento de la información de forma ética y legal en diferentes fuentes de obtención de información de carácter público.

Otras definiciones expresadas por distintos autores en el documento de Rodriguez.Yago[4] son:

> *"La inteligencia derivada de una amplia gama de recursos abiertos, como la radio, la televisión, los periódicos, los libros; a los que el público tiene acceso".*
>
> *"La inteligencia que se produce a través de información disponible para el público, que es obtenida, explotada y diseminada en el tiempo y para la audiencia apropiada, a fin de satisfacer una petición de inteligencia concreta"*
>
> *"Información que no está clasificada, que ha sido intencionadamente descubierta, separada, tamizada y diseminada a una audiencia seleccionada a fin de responder a una pregunta específica."*

[4] Rodríguez, Yago. Inteligencia De Fuentes Abiertas (OSINT): Características, Debilidades Y Engaño. [Citado el 03 de septiembre de 2021] Disponible en Internet: http://www.seguridadinternacional.es/?q=es/content/inteligencia-de-fuentes-abiertas-osint-caracter%C3%ADsticas-debilidades-y-enga%C3%B1o

4.1.2 Fuentes de Información. Las fuentes de información como internet, radio, papel son medios principales para la metodología Open Source Intelligence, para MARANTO RIVERA una fuente de información es: “todo aquello que nos proporciona datos para reconstruir hechos y las bases del conocimiento”[5].

4.1.3 Tipos de Fuentes de Información. Dependiendo del tipo de fuente de información y los tipos de medios y acceso a los datos se pueden clasificar en:

- **Fuentes de Información primario:** “Este tipo de fuentes contienen información original es decir son de primera mano, son el resultado de ideas, conceptos, teorías y resultados de investigaciones. Contienen información directa antes de ser interpretada, o evaluado por otra persona. Las principales fuentes de información primaria son los libros, monografías, publicaciones periódicas, documentos oficiales o informe técnicos de instituciones públicas o privadas, tesis, trabajos presentados en conferencias o seminarios, testimonios de expertos, artículos periodísticos, videos documentales”[6]

- **Fuentes de Información secundario:** “Este tipo de fuentes son las que ya han procesado información de una fuente primaria. El proceso de esta información se pudo dar por una interpretación, un análisis, así como la extracción y reorganización de la información de la fuente primaria.”[7]

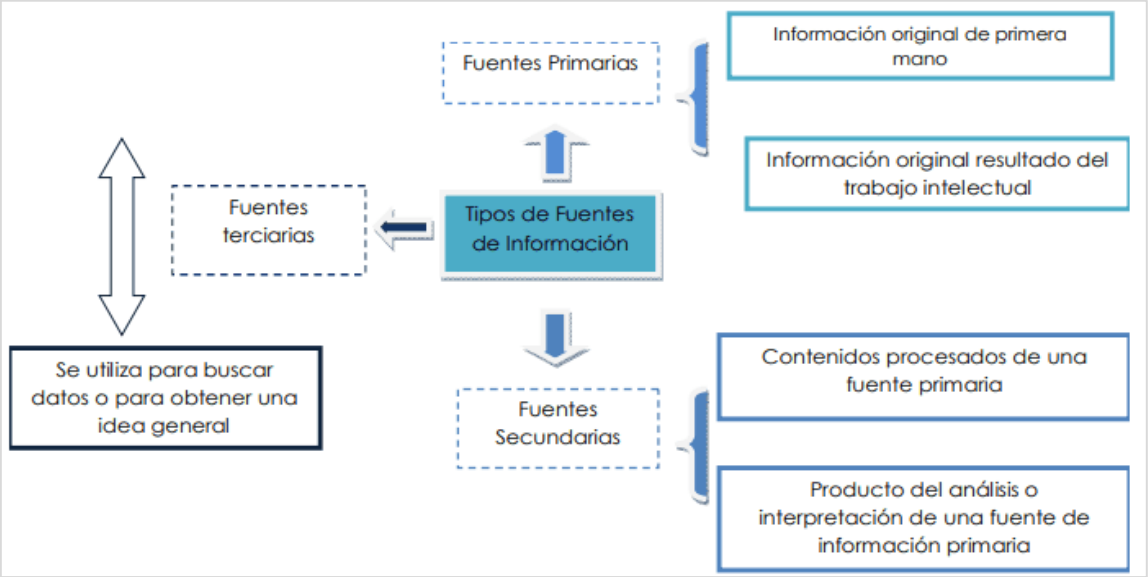
- **Fuentes de Información terciario:** “Este tipo de fuentes son las que recopilan fuentes de información primarias o secundarias. Estas fuentes son utilizadas para buscar datos o para obtener una idea general sobre algún tema, algunas son;

[5] MARANTO RIVERA. Marisol y GONZÁLEZ FERNÁNDEZ. Maria E. Fuentes de Información [En Linea] Universidad Autónoma del estado de Hidalgo,2015. Disponible en: https://repository.uaeh.edu.mx/bitstream/bitstream/handle/123456789/16700/LECT132.pdf
[6] Ibid, Pág. 23
[7] Ibid, Pág. 23

bibliografías, almacenes, directorios, donde se encuentran la referencia de otros documentos, que contienen nombres, títulos de revistas y otras publicaciones."[8]

4.1.4 Representación de tipos de fuentes de Información. La Figura 4 es una representación gráfica del esquema general de los tipos de fuentes de información y los medios de obtención de datos para su clasificación.

Figura 4 Tipos de fuentes de información



Fuente MARANTO RIVERA. Marisol y GONZÁLEZ FERNÁNDEZ. Maria E. Fuentes de Información [En Linea] Universidad Autónoma del estado de Hidalgo,2015. Disponible en: https://repository.uaeh.edu.mx/bitstream/bitstream/handle/123456789/16700/LECT132.pdf

[8] Ibid, Pág. 23

4.2 MARCO CONCEPTUAL

4.2.1 La Información. Se puede definir la información con un el conjunto de datos que organizados pueden trasmitir una idea y generar conocimiento para el portal web concepto defina la información como:

> *"conjunto organizado de datos relevantes para uno o más sujetos que extraen de él un conocimiento. Es decir, es una serie de conocimientos comunicados, compartidos o transmitidos y que constituyen por lo tanto algún tipo de mensaje"* 9

4.2.2 Usos de la Información. Actualmente los seres humanos tienen acceso a grandes volúmenes de información de cualquier tipo en consecuencia al desarrollo tecnológico por lo que se le denomina "Sociedad de la información".

El uso de la información reduce la incertidumbre en un contexto especifico y se considera como verdadera herramienta de obtención de conocimiento. No óbstate, esto no es garantía de obtener verdaderos conocimientos ya que depende de cada individuo en su análisis correcto y exhaustivo para la depuración de datos.

4.2.3 Características de la Información. Las características principales en la información son las siguientes:

- La información está conformada por datos ordenados.
- Tener gran volumen de información no garantiza obtención de conocimiento, esta última dependerá de la confiabilidad, relevancia y vigencia en su contenido.
- La información toma significado una vez que es analizado de forma estructurada y critica.
- La información debe estar disponible de forma oportuna para poder responder a dudas o situación específica.

[9] Concepto [Sitio web]. Concepto de Información [Consultado:03 de septiembre de 2021] Disponible en: https://concepto.de/informacion/

- La información ser precisa para exponer todos los detalles de los datos y poder comprender la naturaleza de su contenido.
- La información debe generar utilidad ya que de ella depende la toma de decisión y generación de nuevos conocimientos.

4.3 MARCO LEGAL

4.3.1 Ley 1273 De 2009. Esta ley se aplica en la metodología *Open Source Intelligence* ya que determina las acciones permitidas en la recolección de información de terceros y está conformada por artículos de las cuales describe cada uno de los diferentes delitos informáticos que son castigados según la legislación colombiana, estipulando las diferentes multas de 100 a 1000 salarios mínimos vigentes mensuales y penas de presión contemplados que pueden ir de cuarenta y ocho (48) a noventa y seis meses (96).

"*Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado de la protección de la información y de los datos- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones*"[10].

4.3.2 Ley Estatutaria 1581 De 2012. Esta ley se aplica en la *metodología Open Source Intelligence* por que regula la obtención y almacenamiento de datos personales recolectados en marco de investigación, aplicada en todas las entidades públicas, privadas e investigación personal en el contexto colombiano *"Por la cual se dictan disposiciones generales para la protección de datos personales"*[11].

[10] Secretariasenado.gov.co. [Sitio Web]. Ley 1273 De 2009. [Consulta 1 marzo 2021]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html.
[11] Secretariasenado.gov.co. [Sitio Web]. Ley estatutaria 1581 de 2012. [Consulta 14 abril 2021]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html.

5 DESARROLLO DE LOS OBJETIVOS

5.1 OBJETIVO1: IDENTIFICACIÓN DE TIPOS DE FUENTES DE OBTENCIÓN DE INFORMACIÓN DE CARÁCTER PÚBLICO NECESARIOS PARA LA APLICACIÓN DE LA METODOLOGÍA OPEN SOURCE INTELLIGENCE (OSINT).

Las fuentes abiertas son la materia prima de la metodología *Open Source Intelligence (OSINT)*, comprender su clasificación garantiza el éxito de la investigación, ya que de forma inicial se requiere definir el tiempo, el alcance, y los recursos necesarios para la ejecución de las tareas propias de recolección de datos, por tanto, la primera actividad del marco es limitar el ámbito de obtención de información.

Según Miranda Soberón, se define una fuente de información como "todos aquellos medios de los cuales procede la información, que satisfacen las necesidades de conocimiento de una situación o problema presentado y, que posteriormente será utilizado para lograr los objetivos esperados"[12]. Por lo que es necesario realizar una identificación de tipos de fuentes de obtención de datos de carácter público necesarios para ser aplicados dentro de la metodología *Open Source Intelligence* (OSINT).

5.1.1 Fuentes en medios físicos. Las fuentes de información abiertas en medios físicos hacen referencia aquellos contenidos que están impresos en papel para la obtención de datos, según el artículo escrito Cruz Vilain denominado "Los Medios Masivos de Comunicación y su papel en la construcción y deconstrucción de identidades" [13] se detalla que en los años 90 eran la fuente más confiables gozando de gran popularidad entre los

[12] MIRANDA SOBERÓN. Ubaldo E y ACOSTA. Zully E. Fuentes de información para la recolección de Información cuantitativa y cualitativa [En línea]. Universidad Nacional San Luis Gonzaga, 2008.Disponible en: https://docs.bvsalud.org/biblioref/2018/06/885032/texto-no-2-fuentes-de-informacion.pdf

[13] CRUZ VILAIN, Margarita Amalia. Los Medios Masivos de Comunicación y su papel en la construcción y deconstrucción de identidades: apuntes críticos para una reflexión inconclusa. [En Linea] Bibliotecas Anales de la investigación. 2013 . Disponible en: http://revistas.bnjm.cu/index.php/BAI/article/view/283/293

investigadores hasta la llegada de internet, sin embargo, los medios impresos presentan una serie de ventajas frente a nuevas tecnologías emergentes como:

La información siempre se encuentra disponible, sin depender de factores externos como la electricidad.

Aporta mayor grado de confiabilidad al momento de consulta dependiendo de la editorial de imprenta. Aunque es una fuente de obtención de datos que siempre ha estado presente desde la aparición de la revolución industrial su base de consulta ha venido disminuyendo en medida que la sociedad se digitaliza, por que presenta los siguientes inconvenientes:

- Su almacenamiento puede ocupar grandes volúmenes de espacio físico.
- Su mantenimiento puede resultar costoso a largo plazo.
- El tiempo de consulta es extenso y complejo para su depuración.
- Requiere mayor esfuerzo por parte del analista para el procesamiento de la información.

Ejemplos de las fuentes abiertas en medios físicos son: periódico, revistas, directorios públicos, artículos académicos, folletos entre otros.

La Figura 5, hace referencia al medio de consulta imprento más popular aún vigente en nuestros días como es el periódico.

Figura 5 El Periódico

Fuente. ABC MEDIOS, El periódico medio con mayor credibilidad que internet [sitio web] [Archivo imagen jpg] Disponible en: https://static1.abc.es/Media/201312/03/portadas-periodicos--644x362.jpg

5.1.2 Fuentes en medios digitales. Las fuentes abiertas en medios digitales son canales de obtención de datos que se encuentran administrados por dispositivos electrónicos para su consulta, se remonta desde los años 60 con la aparición de la computadora y hoy es el medio de consulta de información más popular estando al alcance de todos según una publicación contenida del sitio web características.co[14] proporcionando ventajas como:

- Accesibilidad a gran volumen de información de consulta.
- No requiere mayor gestión de almacenamiento en espacios físicos.
- Está presente en cualquier lugar geográficamente siempre que haya conexión a internet.

[14] Características.co [sitio web] Resumen historia de la computadora [en línea] [consultado el 23 de octubre de 2021] Disponible en: https://www.caracteristicas.co/historia-de-la-computadora/

La aparición de las redes sociales a principio del nuevo milenio, revoluciono la forma en cómo se consulta la información hoy en día, para el sitio web características.co en su publicación de contenido Resumen historia de las redes sociales[15]. La red social *Facebook* alcanzó los mil seiscientos cincuenta (1.650) millones de usuarios activos durante el año 2016, convirtiéndose en un medio de consulta de información personal más popular de carácter público.

No obstante, también el éxito de la red social se ha visto empañada por las severas acusaciones de no preservar la confidencialidad de los usuarios, y colaborar con terceras partes en otorgar información personal para el espionaje ciudadano como lo hace constar la BBC News en un artículo publicado el 10 de abril del año 2018.[16]

La metodología de obtención de información pública *Open Source Intelligence* (OSINT) está muy presente en las investigaciones de dichas redes sociales, ya que es la principal técnica utilizada por los investigadores para la obtención y manipulación de datos personales, garantizando su correcto tratamiento para la toma de decisión.

Las fuentes abiertas de consultas en medios digitales, aunque es un gran avance en nuestra era moderna presenta una serie de desventajas propias respecto a medios impresos como son las siguientes:

- Es necesario contar con un dispositivo electrónico para su consulta como computadoras o teléfonos inteligente u otro elemento con conexión a internet y electricidad.

[15] Características.co [sitio web] Resumen historia de las redes sociales [en línea] [consultado el 23 de octubre de 2021] Disponible en: https://www.caracteristicas.co/historia-de-las-redes-sociales/
[16] BBC News [sitio web] "Fue mi error y lo siento": Mark Zuckerberg, fundador de Facebook, comparece ante el Congreso de Estados Unidos por el escándalo de Cambridge Analytica [en línea] [consultado el 23 de octubre de 2021] Disponible en: https://www.bbc.com/mundo/noticias-internacional-43720004

- Su fiabilidad de información es menor por ser manipulado fácilmente por los usuarios a nivel general y en cualquier momento por lo que se requiere un mayor análisis al momento de tomar una decisión.

La Figura 6 enseña un dispositivo de comunicación moderno, con aplicaciones de acceso de redes sociales como fuente de consulta de información personal al alcance de todos.

Figura 6 Redes sociales en *Smart Phone*

Fuente Caracteristicas.co [sitio web] Archivo en formato png, Disponible en: https://www.caracteristicas.co/historia-de-las-redes-sociales/#Evolucion_de_las_redes_sociales

5.1.2 Fuentes en otros medios. La metodología *Open Source Intelligence* considera también otros medios de consulta para la obtención de información de carácter público como la radio, publicidad, conferencias, incluso una simple conversación es una fuente de obtención importante para una investigación.

Es quizás esta una de las ventajas y popularidad de la metodología siente versátil y al alcance de todos.

La Figura 7, enseña una conferencia expuesta por el banco Santander de España se puede apreciar una gran cantidad de asistente obteniendo información de carácter público, un claro ejemplo de otros medios de fuentes abiertas aplicables dentro de la metodología.

Figura 7 Conferencia en el banco Santander - España

Fuente Banco Santander, Archivo en Formato png, Disponible en: https://www.santander.com/es/sala-de-comunicacion/notas-de-prensa/XII-conferencia-internacional-de-banca

5.2 OBJETIVO 2: MARCO DE INVESTIGACIÓN OPEN SOURCE INTELLIGENCE (OSINT) SUS APLICACIONES, MÉTODOS, RETOS Y BENEFICIOS EN LA RECOLECCIÓN DE INFORMACIÓN PERSONAL EN FUENTES ABIERTAS.

Desde que el ser humano empezó a comunicarse, esta actividad ha sufrido constantes cambios, al principio podríamos pensar que utilizaban señas para trasmitir un mensaje o una idea, ahora se puede hacer por medios de dispositivos electrónicos interconectados a nivel global como el teléfono celular. En los años 80 la televisión, la radio y la prensa eran las principales formas de comunicación, para todos aquellos que necesitaban realizar una investigación.

Desde la aparición de internet a principios de los años 90 como fuente de consulta de información, se ha convertido en un elemento de comunicación imprescindible para la sociedad que se vive hoy, considerado muchas veces como el principal medio de obtención de datos de investigación.

Las siglas OSINT hacen referencia a *Open Source Intelligence* o Inteligencia en fuentes abiertas, pero cuando se acuña el término “inteligencia” no es sinónimo de mayor sinapsis cerebral, si no a la capacidad de tomar una decisión de forma acertada al manejo de la información, luego del procesamiento y análisis de datos en los distintos medios de comunicación de carácter público.

La metodología *Open Source Intelligence* (OSINT) nació a mediados del año 1941 en el gobierno de los Estados Unidos de América con el objetivo de obtener la mayor información relevante en fuente abiertas, inicialmente de carácter militar, pero con el tiempo se fue extendiendo a distintos sectores como el jurídico, marketing, talento humano y otros que han visto los beneficios de una metodología estructurada, sistemática y confiable para la obtención de información.

El en campo de la seguridad informática el *Open Source Intelligence* (OSINT) se comporta como fuente primaria de obtención información e insumo de la ingeniería social, proporcionando datos claves del objetivo en concreto y convirtiéndose en la primera metodología aplicar en un *pentesting*[17], es por ello la importancia tanto para investigadores, analistas de seguridad y hackers, lo utilicen como punto partida en la pesquisa de información.

5.2.1 Fases *Open Source Intelligence* (OSINT): Debido al gran volumen de datos que se puede obtener durante una investigación y el esfuerzo que este implica para un correcto análisis, la metodología *Open Source Intelligence* (OSINT) propone diferentes fases para una correcta toma de decisión.

La Figura 8 se detalla las fases para llevar a cabo la metodología *Open Source Intelligence* según el análisis realizado por el Instituto Nacional de Ciberseguridad de España INCIBE[18], en donde se mencionan 6 en total, las cuales son: Requisitos, Fuentes de información, Adquisición, Procesamiento, Análisis e Inteligencia.

[17] OpenWebinars [Sitio web]. Que es el pentesting. [Consultado:03 de septiembre de 2021] Disponible en: https://openwebinars.net/blog/que-es-el-pentesting/

[18] Instituto Nacional de Ciberseguridad de España INCIBE, archivo en formato png, Disponible en: https://www.incibe-cert.es/blog/osint-la-informacion-es-poder

Figura 8 Fases Open source intelligence (OSINT)

Fuente Instituto Nacional de Ciberseguridad de España INCIBE, archivo en formato png, Disponible en: https://www.incibe-cert.es/blog/osint-la-informacion-es-poder

5.2.1.1 Fase de Requisitos: Es la fase de partida del marco, en ella se define las condiciones iniciales de la investigación que han originado el *Open Source Intelligence* (OSINT) conteniendo las siguientes tareas:

- Seleccionar a quien o quienes se le aplicara el marco de la investigación.
- Estimar el tiempo de duración de la investigación
- Estimar los recursos físicos y económicos de la investigación para alcanzar los objetivos trazados.

5.2.1.2 Fase de Identificación de fuentes de información: Se determina cuales son las fuentes de obtención de datos a trabajar durante el desarrollo de la investigación, así como su alcance.

En la presente fase se cuenta con las siguientes actividades:

- Inspeccionar cuales son las fuentes de obtención de información de carácter público aplicables a la investigación.
- Proponer cuales fuentes de obtención de información son aplicables al marco de investigación.

5.2.1.3 Fase de adquisición de datos: Aunque la adquisición de fuentes de obtención de datos de carácter público se podría realizar de forma manual, esta implica un mayor esfuerzo y consumo de tiempo durante la investigación, sin embargo, el *Open Source Intelligence* (OSINT) es una metodología que brinda herramientas automatizadas para tal propósito proporcionando ventajas como:

- Mayor cobertura de adquisición de información.
- Mejor aprovechamiento del tiempo de investigación y recursos.

Existen una multitud de herramientas de adquisición de datos para la metodología, con diferentes propósitos algunas de ella son: Maltego, TheHarvester, Recon-Ng, Creepy, Google maps, LinkedIn.

5.2.1.4 Fase de procesamiento de datos: Adquirir un gran volumen de información, no garantiza al investigador resultados de calidad, por lo que la fase de procesamiento se encarga de homogenizar los datos para una fase de análisis.

En otras palabras, una información que proviene de un idioma distinto el investigador debe traducirla, sintetizarla y estructurarla. Lo que implica las siguientes ventajas para la metodología.

- Los datos están formateados, ordenados y estructurados.
- Los datos se encuentran clasificados.

5.2.1.5 Fase de análisis del procesamiento de la información: Esta fase de la metodología juega un papel muy importante la experiencia del investigador en los siguientes aspectos:

- Relacionar datos que formen una idea.
  Extraer patrones de datos en un contexto.
- Descartar datos irrelevantes para la investigación.
- Discernir datos relevantes para la investigación.

El resultado de calidad de la metodología está en el análisis de los datos, el investigador en esta fase puede volver a requerir nuevos datos y considerar otras fuentes de consultas abiertas antes de llegar a la fase de Inteligencia.

5.2.1.6 Fase de Inteligencia sobre la información: En la presente fase y luego del procesamiento de los datos se toman en cuenta si la información cumple con las expectativas de la investigación realizando la acción más importante “La toma de decisión” frente a los resultados obtenidos.

En conclusión, la metodología *Open Source Intelligence* (OSINT) es iterativa lo que define que contiene una serie de etapas o fases con el objetivo de alcanzar un resultado concreto. En cada nueva interacción la información obtenida es utilizada para

retroalimentar la siguiente fase representado un esquema cíclico en el que cada etapa es una oportunidad para de mejoramiento en los resultados obtenidos hasta el momento.

5.2.2 Aplicaciones en los campos de conocimientos: La información se ha diversificado en distintos medios de comunicación en los últimos años y sigue expandiéndose de manera vertiginosa en el que su volumen se hace incalculable, resultando difícil realizar una investigación y siendo necesario la implementación de una metodología de análisis.

Para satisfacer la gran demanda de análisis en la información pública se presenta *Open Source Intelligence* (OSINT) como metodología principal. Según el motor de búsqueda *Google Trends*[19] la tendencia de los usuarios en buscar elementos asociados al marco ha venido ha crecido en los últimos años por lo que se convierte en la principal herramienta para los investigadores al momento de obtener datos en fuentes abiertas de forma legal.

En la Figura 9, detalla la tendencia de búsqueda de la palabra OSINT desde el año 2018 hasta el año 2021.

[19] Google Trends [Pagina web] Disponible en: https://trends.google.es/trends/?geo=CO

Figura 9 Criterio de búsqueda OSINT en el motor de Google

Fuente Google Trends [sitio web] archivo en formato png, Disponible en: https://trends.google.es/trends/explore?date=all&q=OSINT

Para el autor Bertram[20] el *Open Source Intelligence* (OSINT) se ha extendido en otros campos de la sociedad como:

5.2.2.1 Gobierno: Los organismos gubernamentales, especialmente los departamentos militares, se consideran los más grandes consumidor de fuentes OSINT. Los enormes desarrollos tecnológicos y generalizados, el uso de Internet en todo el mundo ha convertido a los gobiernos en un gran consultor de OSINT.

Los gobiernos necesitan fuentes OSINT para diferentes propósitos, como seguridad, contraterrorismo, rastreo cibernético de terroristas, comprensión nacional y puntos de

[20] BERTRAM, S. K. The Tao of Open Source Intelligence. Ely, Cambridgeshire, United Kingdom: ITGP, 2015. ISBN 9781849287289. Disponible en: https://search-ebscohost-com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=nlebk&AN=1030094&lang=es&site=eds-live&scope=site.

vista del público extranjero sobre diferentes temas, proporcionando a los responsables políticos la información para influir en su política interna y externa, y la explotación de medios extranjeros como la televisión para obtener traducciones instantáneas de diferentes eventos que suceden en el exterior.[21]

5.2.2.2 Organizaciones internacionales: Las organizaciones como la ONU utilizan fuentes OSINT para apoyar el mantenimiento de la paz en las operaciones en todo el mundo. La ONU equilibra las preocupaciones de las superpotencias y las naciones emergentes al crear su política, que requiere que sea tan transparente como posible. Para lograr esto, la ONU encontró que es más conveniente explotar OSINT fuentes (incluidas imágenes de satélite comerciales) para necesidades de inteligencia en lugar de depender de los informes de sus estados miembros, que pueden tener políticas contradictorias.

5.2.2.3 Las fuerzas del orden: La policía utiliza fuentes de OSINT para proteger a los ciudadanos del abuso, la violencia sexual, el robo de identidad, y otros delitos. Esto se puede hacer monitoreando los canales de redes sociales para obtener información interesante. palabras clave e imágenes para ayudar a prevenir delitos antes de que se agraven.

[21] Ibid pág. 33

5.2.2.4 Corporaciones comerciales: La correcta toma de decisión en la información es el en poder comercial y las organizaciones empresariales utilizan las fuentes abiertas para investigar nuevas oportunidades de negocio, supervisar las actividades de la competencia, planificar las actividades de *marketing* y predecir todo lo que pueda afectar sus operaciones actuales y crecimiento futuro. En el pasado, la explotación de fuentes de OSINT se limitó a las grandes empresas con buenos presupuestos de inteligencia. Hoy en día, con el uso generalizado de Internet, las pequeñas empresas con presupuestos limitados pueden explotar fuentes de *Open Source Intelligence* (OSINT) de manera eficaz y fusionar la información adquirida en sus planes de negocio.

5.2.3 Perfiles de usuarios que hacen uso de la metodología: Una de las principales ventajas de este marco su flexibilidad de uso, ya que no se centra en ramas de conocimientos específicos por el contrario es una metodología adaptable a cualquier campo profesional, radicando allí su éxito para los distintos investigadores.

Es común encontrar una diversificación de profesiones que hacen uso de la metodología como gerentes, psicólogos de selección de personal, analista de seguridad, investigadores privados, docentes, personal jurídico, personal militar.

No existe segmentación alguna de especialidad profesional, sin embargo, para Vicente Aguilera,[22] es necesario contar con las siguientes cualidades para que un investigador OSINT realice de forma efectiva un análisis de datos dado que la información es volátil, variable e impredecible dispersa en los distintos medios de comunicación de carácter público, dichas cualidades son:

[22] Youtube [Sitio web] OSINT e Ingeniería Social: como vectores de ataque a la ciberseguridad. Instituto Nacional de Ciberseguridad de España. [consultado el 05 de septiembre 2020] Disponible en: https://www.youtube.com/watch?v=ZaivL8_J3j4&t=95s

- Capacidad Analítica: “Es la habilidad para descomponer sistemáticamente un problema complejo en sus elementos más asequibles y así, obtener las mejores soluciones”.[23]
- Observación Objetiva: Es la habilidad de poder fijar una meta fija, que pueda ser medible y auditable.
- Razonamiento deductivo: “es un tipo de argumento en que una premisa general conduce a una conclusión específica”.[24]
- Lógica: Hace referencia al sentido común.

5.2.4 Clasificación de tipos consultas de información dentro del marco: Hay diferentes tipos de información que puede encontrar al realizar un análisis de *Open Source Intelligence* (OSINT). De acuerdo con la (NATO) *Open Source Intelligence Handbook* V1.2[25] publicado en el año 2001, existen cuatros tipos de consultas de fuentes de información:

5.2.4.1 Open Source Data (OSD): En sus siglas en español Datos de código abierto son datos genéricos que provienen de una fuente. Los ejemplos incluyen imágenes de satélite, datos de llamadas telefónicas y metadatos, conjuntos de datos, datos de encuestas, fotografías y audio o video grabaciones que han registrado un evento.

5.2.4.2 Open source information (OSIF): En sus siglas en español Información de fuentes abiertas, estos son datos genéricos que tienen primero un sometimiento a algún filtrado para cumplir con un criterio o necesidad específicos; Estos datos también pueden denominarse fuente secundaria. Ejemplos incluyen libros sobre un tema específico, artículos, disertaciones, obras de arte y entrevistas.

[23] Youtube [Sitio web] MOOC Competencias digitales para profesionales - 7.1 Capacidad analítica y toma de decisiones. [consultado el 11 septiembre 2021] Disponible en: https://www.youtube.com/watch?v=ooc7GjEPLXo

[24] Significados [Sitio Web] ¿Qué es un razonamiento deductivo? [consultado el 11 septiembre 2021] Disponible en: https://www.significados.com/razonamiento-deductivo/

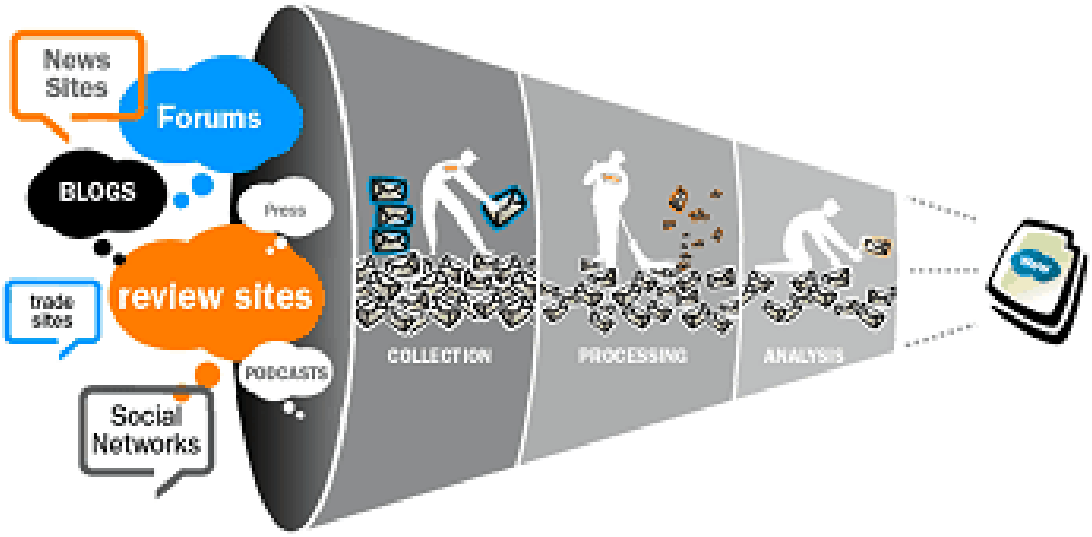
[25] KERNAN, W.F. NATO Open Source Intelligence Handbook V1.2 [En Línea] U.S. Army, 2001. Disponible en: https://www.academia.edu/4037348/NATO_Open_Source_Intelligence_Handbook

5.2.4.3 Open source intelligence (OSINT) En sus siglas en español Inteligencia en fuentes abiertas, esto incluye toda la información que ha sido descubierto, filtrado y designado para cumplir con una necesidad o propósito. Esta información se puede utilizar directamente en cualquier contexto de inteligencia. OSINT se puede definir en pocas palabras como el resultado del procesamiento de materiales de código abierto.

5.2.4.4 Validated OSINT (OSINT-V): Esto es Inteligencia en fuentes abiertas con un alto grado de certeza; los datos deben ser confirmados (verificados) utilizando un sistema que no sea OSINT como fuente o de una fuente OSINT de gran reputación. Esto es esencial, ya que algunos adversarios externos pueden difundir información OSINT inexacta con la intención de inducir a error el análisis del *Open Source Intelligence* (OSINT). Un buen ejemplo de esto es cuando una estación de televisión transmite en vivo la llegada de un presidente a otro país; dicha información es OSINT, pero tiene un alto grado de certeza.

La Figura 10 detalla la actividad del investigador OSINT en un esquema general donde se visualiza las fuentes de información de entrada, su procesamiento hasta llegar al resultado de inteligencia que es un documento simplificado para la toma de decisión.

Figura 10 Actividad de búsqueda de información aplicando OSINT



Fuente. Crónicas seguridad [sitio web] Archivo en formato png. Disponible en: https://cronicaseguridad.com/wp-content/uploads/OSINT.png

5.2.5 Métodos de obtención de información: La obtención de información del *Open Source Intelligence* (OSINT) se clasifican en tres métodos principales: pasivo, semipasivo y activo. El uso de uno a favor de otro depende del escenario donde se ve involucrado el investigador como consultorías, hacking ético, espionaje entre otros.

5.2.5.1 Método de obtención pasiva: quizás es una de las más empleada, esta tiene como particularidad en obtener información del objetivo sin que este último tenga conocimiento de ello, es necesario en este método de obtención pasivo adoptar precauciones desde un punto de vista técnico, pasando por desapercibido en la red, siendo una investigación anónima y segura para en analista del marco OSINT. La obtención de información de este tipo de obtención es limitada dado que solo depende del contenido generado por el objetivo.

5.2.5.2 Método de obtención semipasivo: Este tipo de obtención de información, el analista puede generar tráfico de red con distintas consultas a los servidores por ejemplo donde están resguardado la información de carácter público que le es de interés. Aunque las consultas en general se deben realizar lo más discreto posible. Emulando a un usuario consultando una información pública y de esta manera obtener información es posible que se vea descubierto por el objetivo, por que posiblemente existan medidas de seguridad como las *honeypot.*

5.2.5.3 Método de obtención activo: Este tipo obtención el analista del marco interactúa de forma directa con el objetivo u target. La obtención es llevada de forma consistente en los recursos del target (persona u organización), realizando consultas recurrentes a servidores lo que hace que este tipo de método no sea discreto para un análisis tipo OSINT, ya que interrumpe y pone en alerta al objetivo que toma medidas de seguridad sobre su información.

5.2.6 Beneficios de Open source intelligence (OSINT): La revolución tecnológica está en constante crecimiento a nivel global y la cantidad de información por parte de los usuarios producen de forma digital es masivo. Es en este contexto que Internet, los dispositivos tipos Internet de las Cosas (IoT) o tecnologías vulnerables se convierte en una herramienta aliada para el marco OSINT

En la actualidad la información está por doquier, nadie puede subestimar el papel vital que juega el *Open Source Intelligence* (OSINT) en las diferentes arenas de inteligencia. Los beneficios de la metodología abarcan muchas áreas en el mundo y sus principales ventajas son:

5.2.6.1 Menor riesgo en la integridad física: Utilizar datos de acceso libre para acumular conocimientos no tiene ningún peligro en comparación con otras metodologías de obtención de información, como utilizar la vigilancia a través de satélites o utilizar fuentes humanas para recopilar datos, particularmente en naciones hostiles.

5.2.6.2 Rentabilidad en el desarrollo de la investigación: recopilar información con el marco *Open Source Intelligence* (OSINT) en su mayor parte, es más asequible en comparación con otras metodologías de obtención de información. Por ejemplo, utilizar fuentes humanas o vigilar los satélites para recopilar información es costoso. Las empresas pequeñas con limitaciones de presupuestos pueden optar por la utilización del marco porque es menos costoso.

5.2.6.3 Facilidad de aplicación de la metodología: La información pública siempre estarán disponibles, sin importar donde se encuentre. Las fuentes abiertas pueden ser utilizado por diferentes actores en cualquier contexto de inteligencia; todo lo que necesita son las habilidades / herramientas necesarias para cosechar y analizar la información correctamente. Por ejemplo, los departamentos militares pueden predecir futuros ataques al analizar actividades en sitios de redes sociales, mientras que las corporaciones pueden utilizarlo para construir sus nuevas estrategias de expansión de mercado.

5.2.6.4 Legalidad en la recolección de datos: Los datos se pueden compartir entre pares sin que haya repercusión de derechos de autor dado que la información es de carácter publica, por supuesto con algunas limitaciones que no incurran en la privacidad organizacional o personal.

5.2.6.5 Detección de evasores de impuestos: *Open Source Intelligence* (OSINT) permite al gobierno que las agencias especializadas puedan detectar evasores de impuestos, por ejemplo. Muchas celebridades famosas y algunas empresas gigantes están involucradas en la evasión fiscal, y monitorear sus cuentas de redes sociales, vacaciones y estilos de vida ha resultado un gran valor para un inspector del gobierno que puede estar persiguiéndolos por ingresos no declarados.

5.2.6.6 Detección de datos falsificados: se pueden utilizar técnicas de *Open Source Intelligence* (OSINT) para descubrir productos y/o servicios falsificados y solicitar a la policía que cierre dichos locales o que envíe alertas a los clientes para que dejen de

consumirlos. Este es un beneficio increíble de la técnica, especialmente cuando se lucha contra medicamentos falsos y artículos que comprometa la salud pública.

5.2.7 Retos de la metodología Open source intelligence: Todos los marcos existentes de recopilación de información cuentan con algunas limitaciones y la Metodología *Open Source Intelligence* (OSINT) no está exento del mismo.Algunos retos a lo que se enfrenta quienes hacen uso de OSINT son los siguiente:

5.2.7.1 Tratar grandes volúmenes de información: Al recopilar una cantidad de datos y que puedan ser analizados para considerar su valor, aunque existan herramientas como *Maltego* por dar un ejemplo para tal propósito no deja de ser un desafío para el marco en general produciéndose un fenómeno llamado Infoxicación “La infoxicación es el exceso o sobrecarga de información, que te impide profundizar en los temas que abordas”[26]

5.2.7.2 Controlar la fiabilidad de los datos en las fuentes de información de carácter público: Tengamos en cuenta las fuentes de obtención del marco OSINT, cuando se realiza una investigación de inteligencia, se debe verificar de manera exhaustiva el origen de los datos en una clasificación de dichas fuentes antes de considerarse confiable. La evaluación y clasificación de las fuentes de información que servirán como entrada al marco es bastante compleja.

5.2.7.3 Estimar los esfuerzos humanos: como ya mencionamos, el gran volumen de datos se considera el mayor desafío para la colección OSINT. La necesidad de ver el resultado de las herramientas automatizadas para saber si los datos recopilados son fiables y dignos de confianza; ellos también necesitan comparar con algunos datos clasificados (esto es aplicable para algunos militares y información comercial) para asegurar su confiabilidad y relevancia. Esta consumirá efectivamente tiempo y valiosos recursos humanos.

[26] WebEmpresa - ¿Qué es la infoxicación digital y cómo puedes evitarla? (2017) Recuperado el 28 de agosto de 2021 de: https://www.webempresa.com/blog/que-es-infoxicacion.html#%C2%BFQue_es_la_infoxicacion

5.3 OBJETIVO 3: CASO PRÁCTICO DEL NIVEL DE EXPOSICIÓN Y PRIVACIDAD DE INFORMACIÓN PERSONAL EN UN INTERNAUTA POR MEDIO DE ALGUNA DE LAS HERRAMIENTAS BRINDADA POR LA METODOLOGÍA OPEN SOURCE INTELLIGENCE (OSINT).

El presente apartado tiene el propósito de mostrar al lector, algunas de las herramientas que tiene la metodología para la obtención de información personal en fuentes abiertas, se debe aclarar que los datos aquí expuestos son de carácter académico para la demostración del funcionamiento del marco.

Se opta por escoger la herramienta OSINT *Framework*[27] y según la página web ciberpatrulla[28] lo define como un repositorio web que contiene gran cantidad de recursos para la búsqueda de información en fuentes abiertas necesarias para el marco de trabajo del *Open Source Intelligence,* siendo de libre uso disponible en su sitio web.

Una de las ventajas de la presente herramienta es su facilidad de uso y accesibilidad ya que no requiere de instalación.

5.3.1 Aplicación del framework Open Source Intelligence (OSINT): Como se documentó en la sección 5.2, el marco de trabajo de la metodología *Open Source Intelligence* se divide en fases para la obtención de información en fuentes abiertas, se realiza a continuación un caso práctico de la aplicabilidad del marco en un contexto real de carácter académico.

5.3.1.1 Fase de Requisitos: Es necesario contar con un dato mínimo de partida para la investigación ejemplo: Nombre completo, número de teléfono, correo electrónico, imagen fotográfica, dirección residencial.

[27] OSINT Framework [sitio web] [Accedido el 14 de sept. de 2021] Disponible en: https://osintframework.com/

[28] Ciber patrulla [sitio web] [OSINT Framework] Qué es y cómo puedes utilizar sus recursos para acelerar tus investigaciones [Accedido el 14 de septiembre de 2021] Disponible en: https://ciberpatrulla.com/osint-framework/

Target u objetivo: Número de teléfono 310640XXXX.

Duración de la investigación: 4 horas.

Recursos disponibles: Computador, Internet.

Objetivo: Realizar un perfilamiento digital a partir de los datos de entrada y exponer su nivel exposición y privacidad en internet.

5.3.1.2 Fase de identificación de fuentes de información: Las fuentes abiertas de obtención de información que se consultaran durante la investigación son:

Fuente: Internet.

Medio: Digital.

Clasificación: *Open source intelligence* (OSINT).

5.3.1.3 Fase de adquisición de datos: Se realiza la investigación con el uso de la herramienta ***OSINT Framework***[29]***,*** para la evaluación del nivel de exposición y privacidad del objetivo.

Se toma como referencia de partida el dato minino del objetivo expuesto en la fase de requisito.

Número de teléfono celular: 310640XXXX

Proceda a ingresar a la página oficial de la herramienta de investigación *OSINT Framework*[30] , donde encontrara un mapa mental haciendo referencias a las distintas categorías de consulta de información en fuentes abiertas.

Dentro de la categoría *Telephone Numbers* se le presentara un repositorio de sitios web de fuentes abiertas disponible para consulta, cada una tiene sus particularidades de uso,

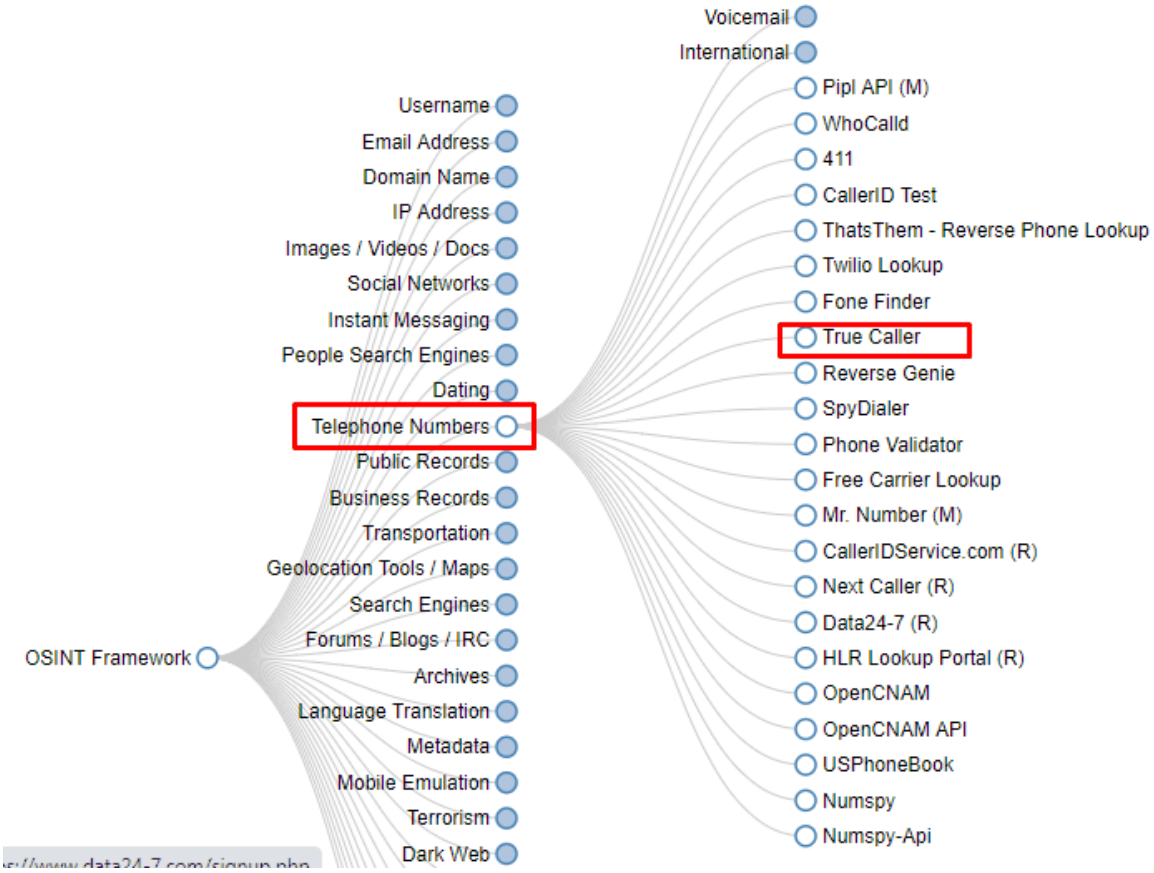
[29] OSINT Framework [Sitio web] Repositorio de fuentes abiertas Open Source Intelligence [Accedido el 15 de sept. de 21] Disponible en: https://osintframework.com/

[30] Ibid, Pag 42

sin embargo, para el contexto colombiano funciona excelente la herramienta *True Caller*[31].

En la Figura 11 se detalla de forma gráfica la categoría a elegir de la herramienta OSINT Framework para la obtención de información relacionado con el dato de partida de la investigación.

Figura 11 Herramienta OSINT FRAMEWORK



Fuente OSINT Framework [sitio web] archivo en formato png, Disponible en: https://osintframework.com/

[31] True Caller [Sitio web] Buscador de números telefónicos [Accedido el 15 de septiembre de 2021] Disponible en: https://www.truecaller.com/

Diríjase a la herramienta de consulta, en su casilla de texto de digite el número de teléfono que definió en la fase de requisitos y presione el botón en forma de lupa.

La herramienta realizara una consulta en sus bases de datos y si coincide con los datos introducidos arrojara información relevante asociado al número de teléfono.

La Figura 12 muestra el proceso de la herramienta de consulta, en la aplicación de los datos de entrada y los resultados arrojados asociados a ella.

Figura 12 Sitio web *true caller*

Fuente True Caller [sitio web] archivo en formato png, Disponible en https://www.truecaller.com/

En este punto disponga a recolectar datos como imagen de referencia, nombre y apellido, correo electrónico y país de residencia. Dicha Información es insumo para las demás categorías según sea su clasificación.

Es importante ir realizando un ordenamiento de la información hallada en cada una de las categorías.

Datos Relevantes Recopilados

Imagen: Registro fotográfico
Nombre y apellido: David Vega
correo electrónico: ingdavega@hotmail.com
país: Colombia

Proceda a seleccionar algún dato relevante recopilado hasta el momento, como se detalla a continuación se seleccionó la imagen obtenida en el paso anterior el cual será insumo para otra categoría en búsqueda de información relacionada a la misma.

La Figura 13 detalla parte de la información asociado a partir del dato de entrada del número de teléfono.

Figura 13 Dato relevante en formato imagen

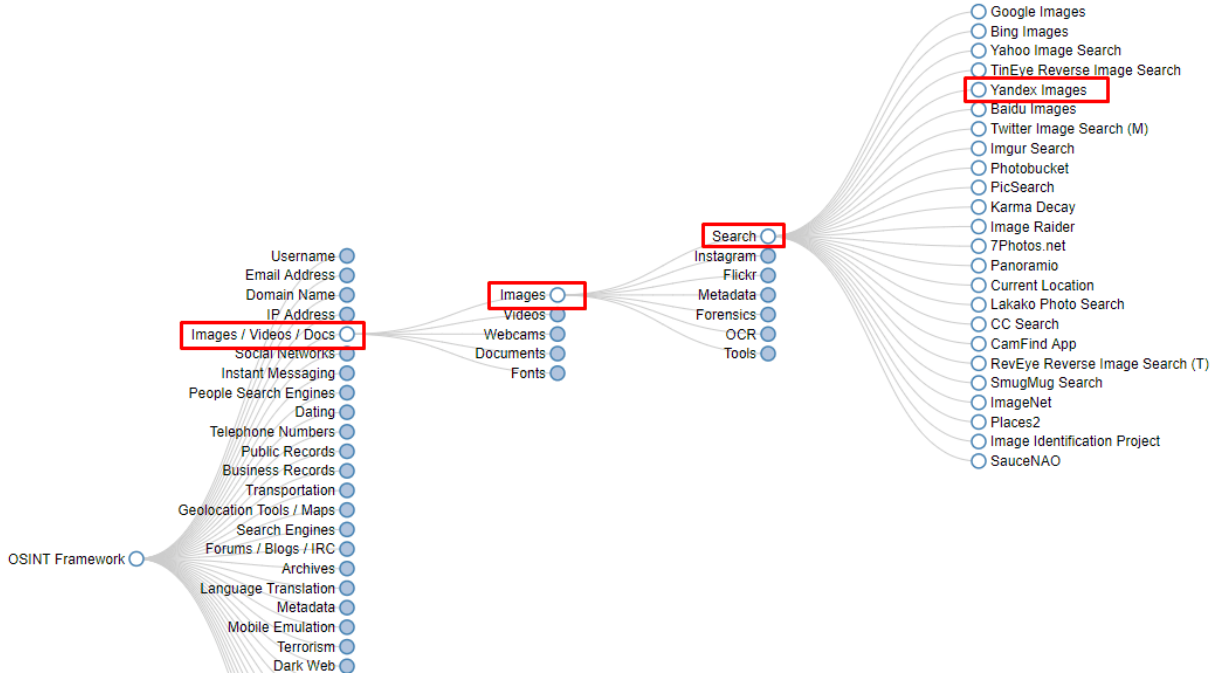
Fuente “Elaboración propia”

Dentro de la categoría *Images* / *Videos* / *Docs* seleccione la siguiente ruta *Images* /

Search la cual le presentara múltiples fuentes abierta de obtención de datos para consultar, una conocida y muy potente que tiene la particularidad de buscar imágenes similares o iguales con gran porcentaje de asertividad es *Yandex Images*[32] ; No obstante, no es la única recuerde en este punto que la herramienta OSINT *Framework* en un compendio de recursos disponibles en la obtención de información en fuentes abiertas.

La Figura 14 detalla los pasos a seguir dentro de la herramienta OSINT *Framework* para llegar al recurso *Yandex Images*.

Figura 14 Herramienta OSINT FRAMEWORK



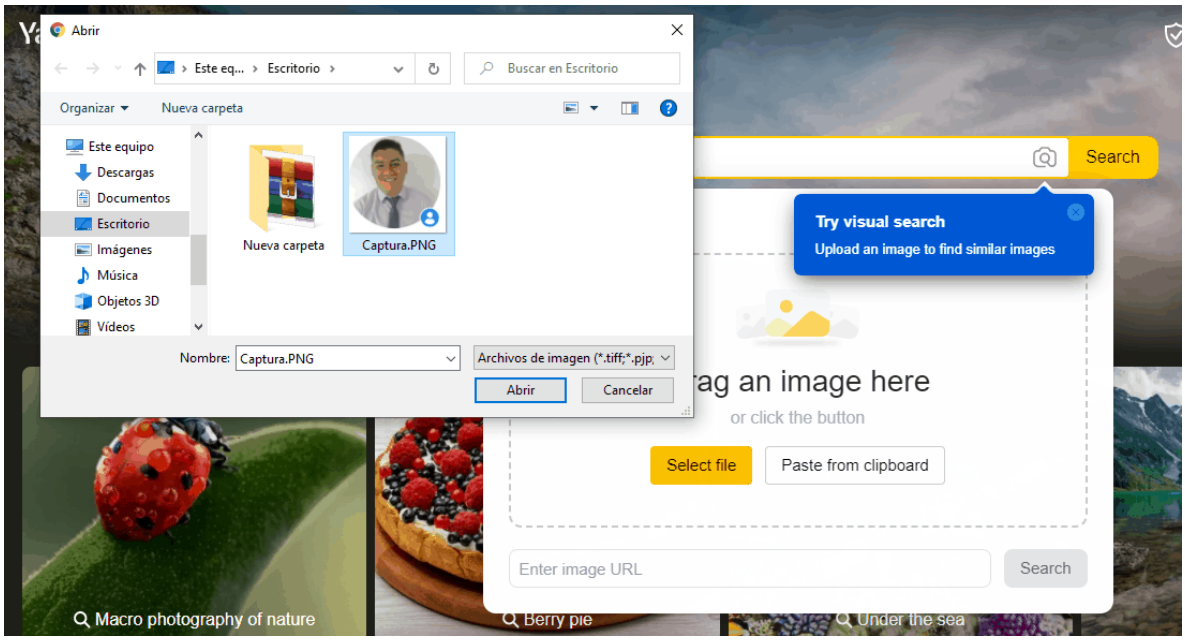
Fuente OSINT Framework [sitio web] archivo en formato png, Disponible en: https://osintframework.com/

[32] Yandex [sitio web] Motor de búsqueda [Accedido el 15 de septiembre de 2021] Disponible en: https://yandex.com/images/

Dentro del recurso seleccionado, proceda a cargar la imagen del dato relevante que definió anteriormente para realizar una búsqueda exhaustiva en las distintas fuentes de información carácter público.

La Figura 15 detalla los pasos a seguir en la utilización de la herramienta *Yandex Images* en la búsqueda de información relacionada con el dato de entrada.

Figura 15 Motor de búsqueda Yandex

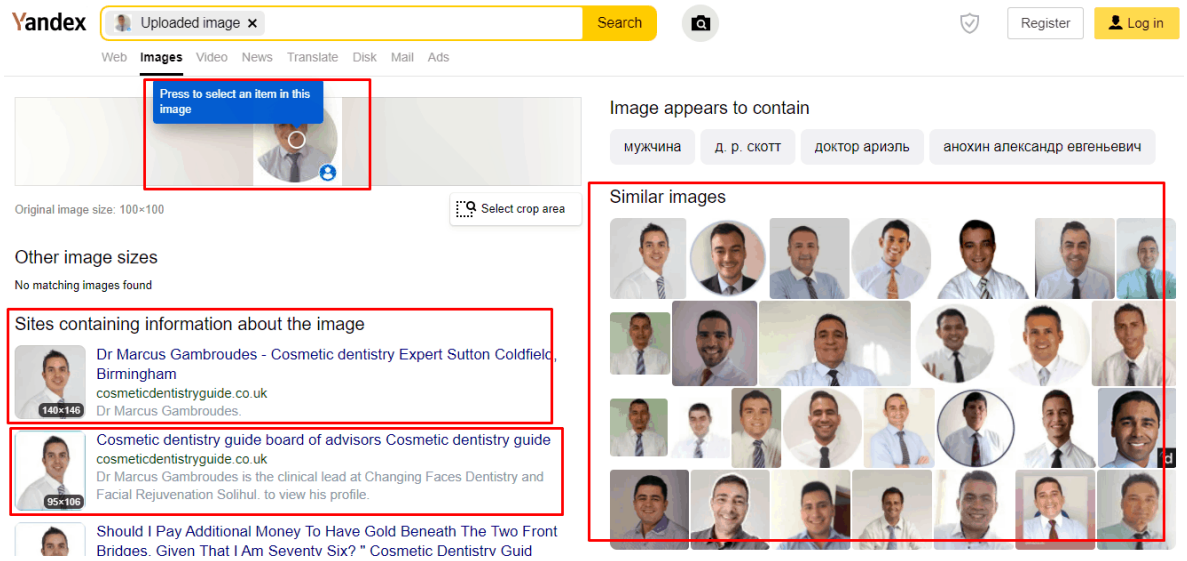


Fuente Yandex [sitio web] archivo en formato png. Disponible en https://yandex.com/images/

El recurso presentará imágenes similares al objeto de entrada, sin embargo, el dato relevante inicial está enmarcado en una esfera redonda con un icono de color azul en el costado inferior derecho, lo que disminuye el nivel de asertividad; Tenga en cuenta que estos detalles pueden afectar los resultados.

La Figura 16 detalla los resultados de asociados al dato de entrada, contenido en el motor de búsqueda.

Figura 16 Motor de búsqueda Yandex

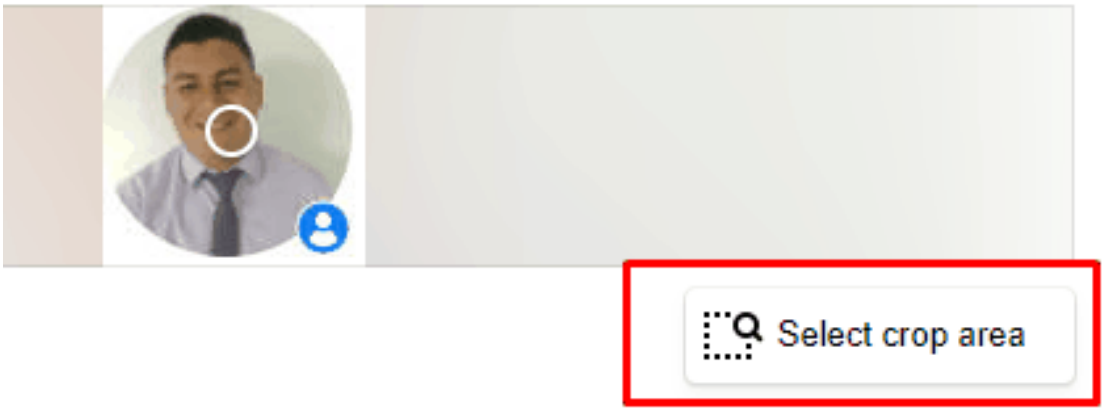


Fuente: Yandex [sitio web] archivo en formato png. Disponible en https://yandex.com/images/

No obstante, el recurso dispone de la opción de selección del área específica para poder corregir que pueden estar afectado su asertividad en la obtención de resultados.

La Figura 17 se muestra la opción de recorte de área de la imagen de entrada con el fin de optimizar los resultados asociados a la imagen.

Figura 17 Optimización de dato de entrada

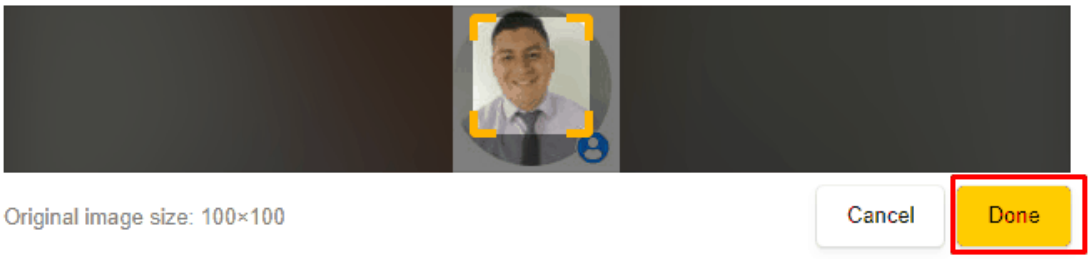


Fuente “elaboración propia”

Seleccione el área en particular de la imagen y oprima el botón *Done*.

La Figura 18 detalla la selección de área para la optimización de resultados asociados a la imagen.

Figura 18 Motor de búsqueda Yandex

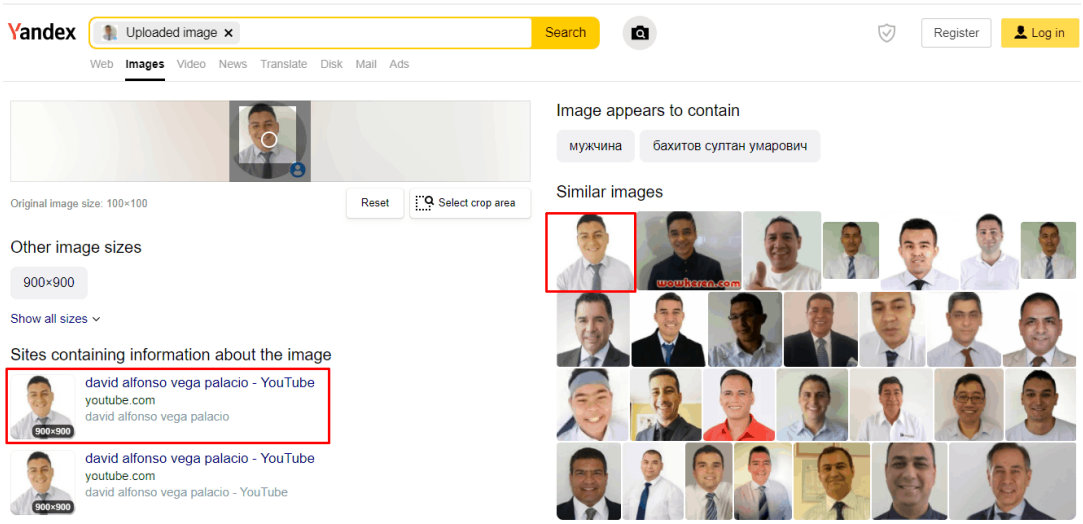


Fuente Yandex [sitio web] archivo en formato png. Disponible en https://yandex.com/images/

El recurso indexara de nuevo el recorte en su consulta en fuentes abiertas que coincida con el criterio de búsqueda, arrojando resultados con mayor precisión y asertividad en los datos de entrada.

La Figura 19 detalla los resultados optimizados de la imagen, luego de realizar el recorte de área.

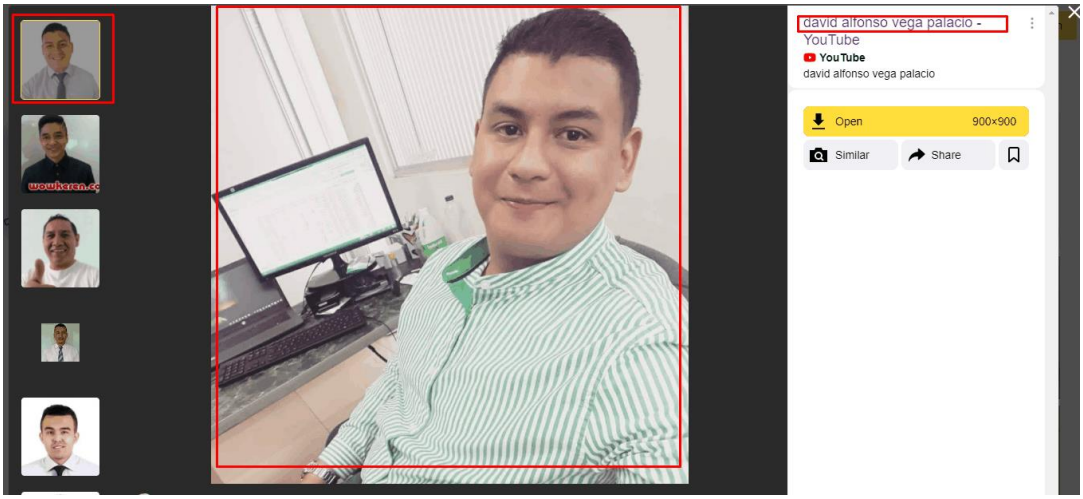
Figura 19 Motor de búsqueda Yandex



Fuente Yandex [sitio web] archivo en formato png. Disponible en https://yandex.com/images/

En esta parte de la investigación luego de la precisión de los resultados, disponga a tomar los nuevos datos relevantes asociados a los criterios definidos en la fase de requisito. La Figura 20 expone los resultados asociados la imagen de entrada, donde podemos aplicar un análisis para corroborar la información.

Figura 20 Motor de búsqueda Yandex



Fuente Yandex [sitio web] archivo en formato png. Disponible en https://yandex.com/images/

Datos Relevantes Recopilados

Imagen: Registro fotográfico

Nombres y apellidos: David Alfonso Vega Palacio

correo electrónico: ingdavega@hotmail.com

Canal YouTube: David A Vega

país: Colombia

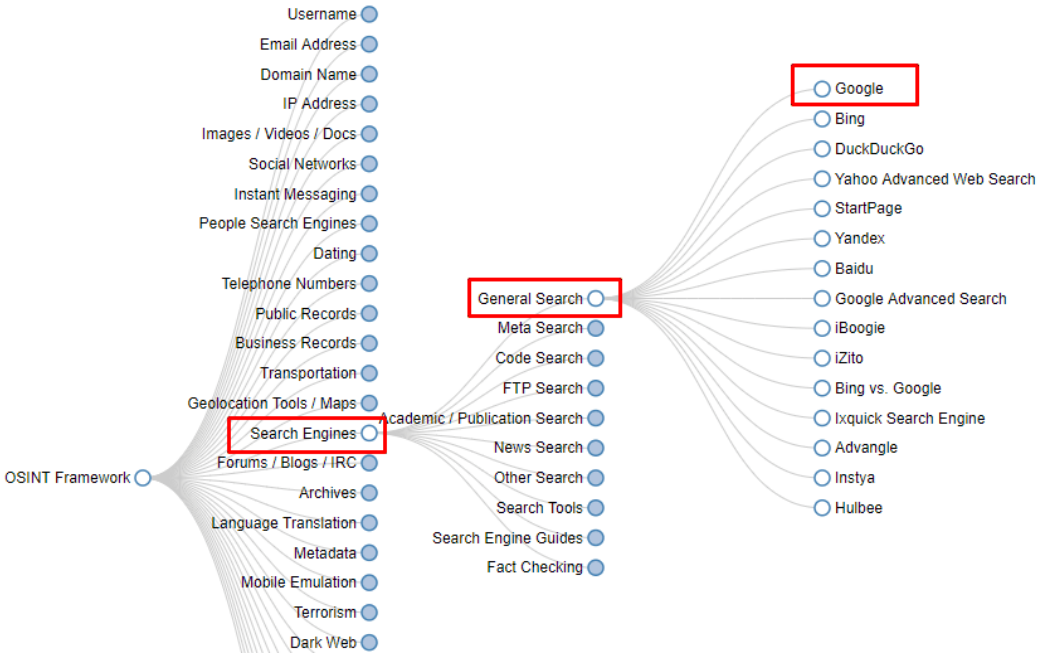
La herramienta OSINT *Framework* le seguirá presentando una gran variedad recursos clasificados en categorías de obtención de información en fuentes abiertas, uno de esos recursos y quizás el más utilizado dentro de los investigadores a nivel mundial es el motor de búsqueda *Google*[33], que se convierte por excelencia en el recurso con mayor popularidad en la metodología *Open Source Intelligence* (OSINT), para acceder a ella por

[33] Google [Sitio web] Motor de búsqueda [Accedido el 15 de septiembre de 2021] Disponible en: https://www.google.com/

medio de la herramienta diríjase en la siguiente ruta: *1-Search Engines 2-General Search 3-Google*

La Figura 21 detalla los pasos para llegar al recurso del motor de búsqueda de Google en la herramienta OSINT Framework.

Figura 21 Herramienta OSINT FRAMEWORK

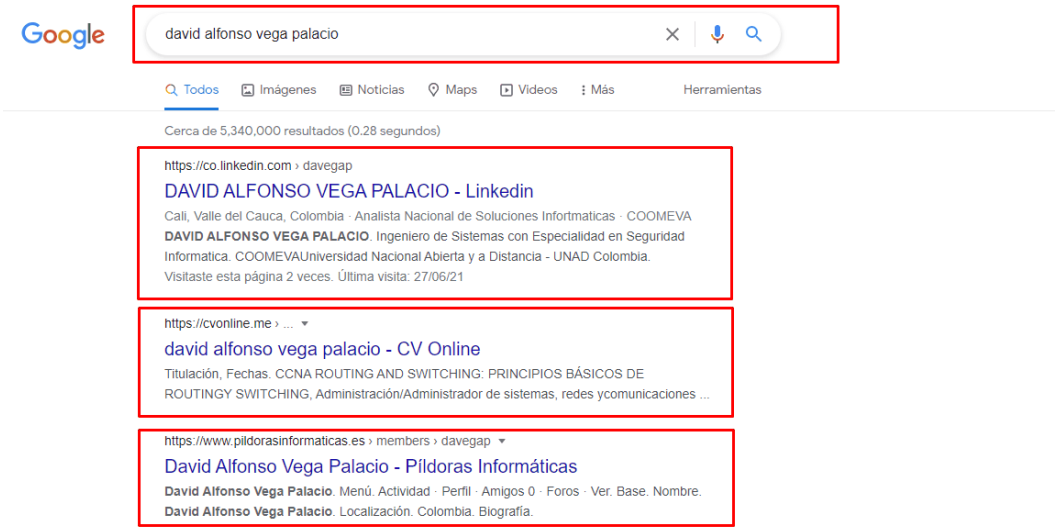


Fuente OSINT Framework [sitio web] archivo en formato png, Disponible en: https://osintframework.com/

Con los datos relevantes recopilados hasta este punto dentro de la investigación proceda a tomar alguno, como el nombre completo del objetivo e ingréselo al motor de búsqueda *Google* para obtener resultados asociados en las distintas fuentes de información.

La Figura 22 enseña el resultado de la búsqueda en el motor de Google de los datos de entrada, que fue el nombre completo del objetivo, detallando los la información asociada a él.

Figura 22 Motor de búsqueda Google



Fuente Google.com [sitio web] Archivo en formato png, Disponible en: www.google.com

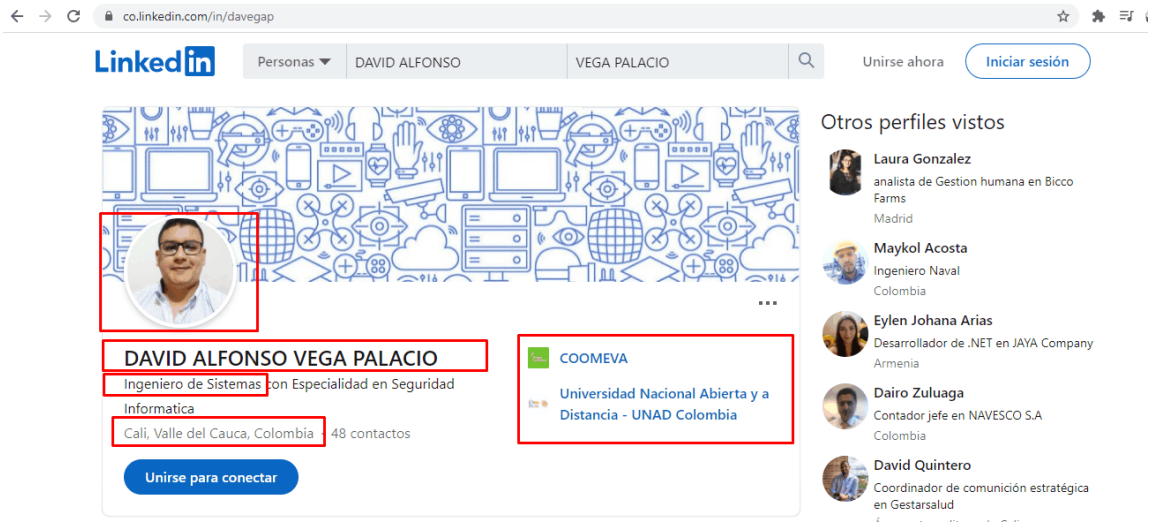
El recurso le presentara una serie de fuentes de obtención de información de carácter público como es el sitio web *LinkedIn*[34] que tiene la particularidad de ser una red social de perfiles profesionales y arroja los siguientes datos siempre que el usuario tenga su información actualizada: Profesión, Empleo actual, ciudad de residencia, universidad de estudio.

Elabore de nuevo en este punto sus nuevos datos relevantes para el perfilamiento digital del objetivo.

La Figura 23 enseña el perfil profesional de los datos de entrada con el nombre, es posible asociar la imagen, el nombre y demás elementos que sirven de insumo para la investigación.

[34] LinkedIn [sitio web] Red social de perfiles profesionales [Accedido el 15 de septiembre de 2021] Disponible en: https://www.linkedin.com/home

Figura 23 Perfil red social LinkedIn



Fuente LinkedIn [sitio web] archivo en formato png, Disponible en www.linkein.com

Datos Relevantes Recopilados

Imagen: Registro fotográfico

Nombres y apellidos: David Alfonso Vega Palacio

Profesión: Ingeniero de Sistemas

Educación: Universidad Nacional abierta y a distancia UNAD.

correo electrónico: ingdavega@hotmail.com

Canal YouTube: David A Vega

país: Colombia

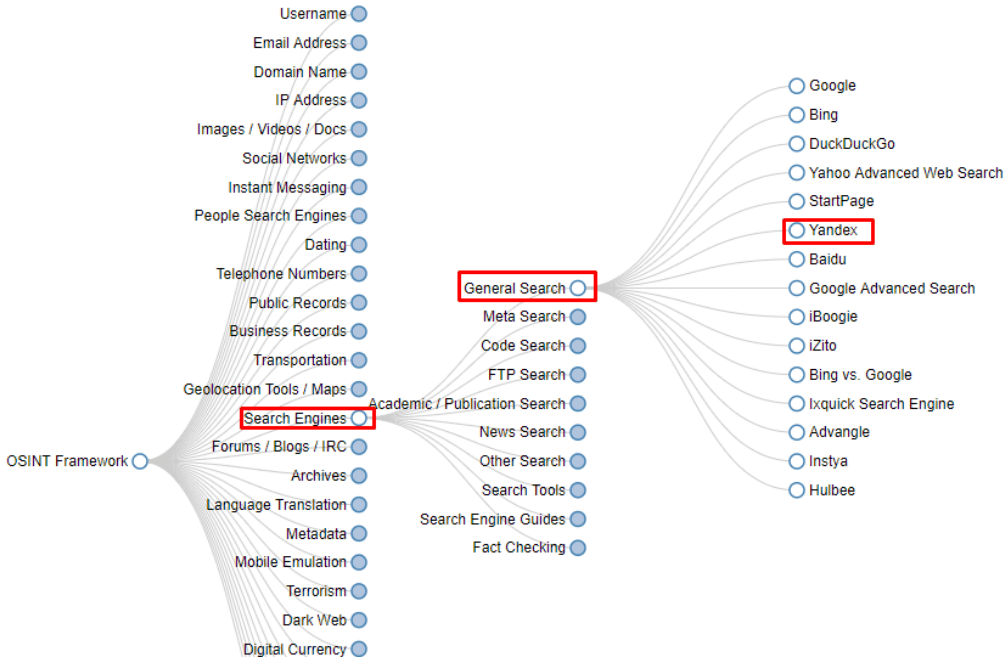
Ciudad: Santiago de Cali – Valle del Cauca

Empresa actual laboral: Coomeva.

Otros de los recursos para la obtención de información en fuentes abiertas contenida dentro de la categoría *General Search* y utilizada anteriormente es *Yandex* sin embargo la utilizaremos en la sección de páginas web, para la búsqueda de resultados, la ruta que dispone el recurso es: *1-Search Engines* *2-General Search* *3-Yandex*

La Figura 24 detalla la ruta para ingresar al recurso del motor de *Yandex.*

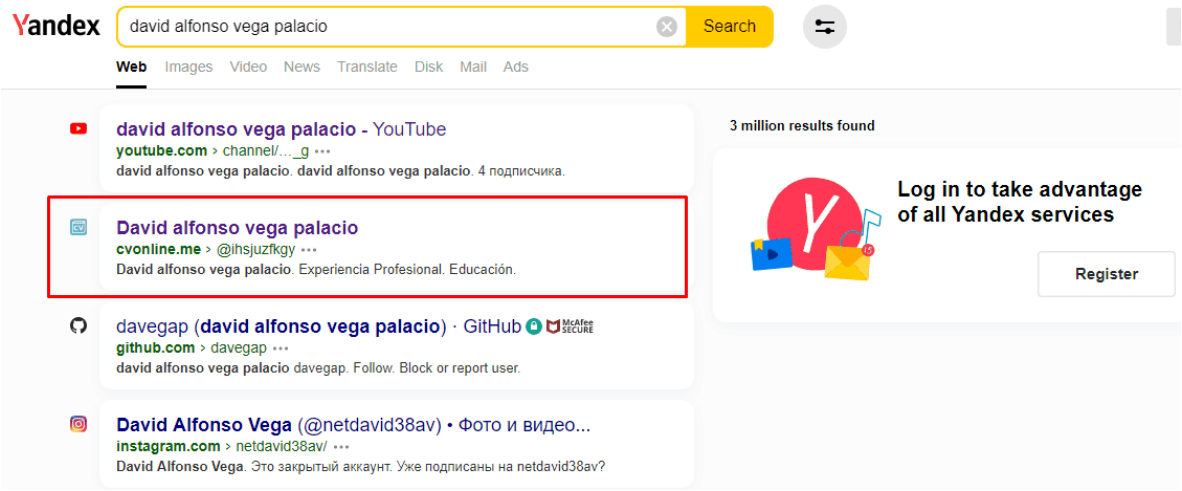
Figura 24 Herramienta OSINT FRAMEWORK



Fuente OSINT Framework [sitio web] archivo en formato png, Disponible en: https://osintframework.com/

Proceda a buscar en similitud con el recurso *Google,* e ingrese el dato relevante de Nombre completo del objetivo. Este recurso se diferencia del anterior en sus búsquedas ya que son más especializadas en fuentes abiertas, arrojando resultados con mayor precisión. La Figura 25 enseña los resultados de búsqueda del motor *Yandex.*

Figura 25 Motor de búsqueda Yandex



Fuente Yandex [sitio web] archivo en formato png. Disponible en https://yandex.com/images/

Escoja algunas de las fuentes de obtención de información de los resultados de búsqueda y proceda a tomar los nuevos datos relevantes asociados al objetivo. La Figura 26 enseña parte de los resultados expuesto por el motor *Yandex*, con la información relevante a los datos de entrada.

Figura 26 Resultados de búsqueda Yandex

Fuente Yandex [sitio web] archivo en formato png. Disponible en https://yandex.com/images/

Datos Relevantes Recopilados

Imagen: Registro fotográfico

Nombres y apellidos: David Alfonso Vega Palacio

Teléfono alterno: 30433XXXXX

Profesión: Ingeniero de Sistemas

Educación: Universidad Nacional abierta y a distancia UNAD.

correo electrónico: ingdavega@hotmail.com

Correo alterno: dxxxxxxxx@xxxxxx.com

Canal YouTube: David A Vega

país: Colombia

Ciudad: Santiago de Cali – Valle del Cauca

Ciudad alterna: Bogotá D.C

Empresa actual laboral: Coomeva.

5.3.1.4 Fase de procesamiento de datos: Durante de procesamiento de datos, estructure la información para la fase de inteligencia, es necesario ordenar la información hallada hasta este punto y realizar la siguiente pregunta.

¿Los datos recopilados hasta este punto satisface las necesidades del objetivo propuesto en la fase de requisitos?

Si la respuesta es negativa proceda a iterar los datos relevantes en cada una de las fases de la metodología hasta llegar de nuevo al procesamiento. Si la respuesta es positiva procesa con la estructuración y ordenamiento de los datos para la fase de análisis, se sugiere utilizar el siguiente patrón.

Datos de la investigación

Dato de entrada

Número de teléfono 310640XXXX

Objetivo del requerimiento

Realizar un perfilamiento digital a partir de los datos de entrada.

Datos de salida

Imagen: Registro fotográfico

Nombres y apellidos: David Alfonso Vega Palacio

Teléfono alterno: 30433XXXXX

Profesión: Ingeniero de Sistemas

Educación: Universidad Nacional abierta y a distancia UNAD.

correo electrónico: ingdavega@hotmail.com

Correo alterno: dxxxxxxxx@xxxxxx.com

Canal YouTube: David A Vega

país: Colombia

Ciudad: Santiago de Cali – Valle del Cauca

Ciudad alterna: Bogotá D.C

5.3.1.5 Fase de inteligencia: Aunque el marco de trabajo *Open Source Intelligence (OSINT)* es una metodología de investigación cualitativa y no cuantitativa para la medición de los niveles de exposición y privacidad de la información, es importante aclarar que este criterio es basado en la experiencia del investigador y de las necesidades que llevaron a la realización de la investigación.

Dado lo anterior se puede deducir que la información hallada a partir de un número telefónico es la siguiente:

- El nivel de exposición de la información personal es alto, ya que se determina nombres completos, ciudad de residencia, empleo actual, profesión, educación, teléfonos alternos, correos electrónicos alternos y registros fotográficos de identificación.
- El nivel de privacidad es relativo y depende del conocimiento que tenga el internauta del nivel de exposición de la información en las distintas fuentes abiertas y de los contenidos allí publicados, sin embargo, se logra determinar que su nivel es aceptable porque no se encontró datos sensibles como: Número de

identificación, datos bancarios y demás información que pueda poner en riesgo su intimidad.

La decisión de inteligencia sobre la información hallada es poder reducir al máximo el número de fuentes abiertas que puedan contener datos personales por lo que se recomienda aplicar las siguientes acciones necesarias al internauta como:

- Cerrar las fuentes abiertas que no sean útiles para el manejo de información personal.
- Documentar sitios web y aplicaciones donde aplique formularios de obtención de información personal.

La Figura 27 es un claro ejemplo de la fase de inteligencia, ya que se tomó una decisión sobre la exposición de la información personal sensible en internet, se cerraron aquellas cuentas que no eran necesarias.

Figura 27 Pagina de resultado después de la fase de inteligencia

Fuente “elaboración propia”

5.4 OBJETIVO 4: RECOMENDACIONES PARA EL MEJORAMIENTO DE LA PRIVACIDAD DE LA INFORMACIÓN PERSONAL EN PUBLICACIONES DE CONTENIDOS DIGITALES EN FUENTES ABIERTAS Y PREVENCIÓN DE RIESGOS CIBERNÉTICOS.

Las recomendaciones que se presentan a continuación proponen al internauta acciones necesarias para poder aumentar la seguridad en sus datos personales, mitigación del riesgo en ataques informáticos y fortalecimiento en el nivel de privacidad en fuentes abiertas.

Publicaciones en fuentes abiertas: Es necesario conocer los datos a publicar en fuentes abiertas y los riesgos que esto implica, según el subteniente del centro de investigación cibernética de la Policía Nacional Colombiana Jessica Sepulveda[35] se pueden evitar 4 grandes riesgos en internet como *grooming, sexting, ciberbullying,* ciberdependencia.

- ***Grooming*:** Es una modalidad criminal donde un adulto se hace pasar por un menor de edad, generando confianza en la victima para obtener información con contenido sexual en su mayoría de veces, sin embargo, también es aplicable para realizar inteligencia sobre las actividades de los padres, este tipo de modalidad nace de la publicación en menores de edad datos en fuentes abiertas como hobbies, estados de ánimos, actividades de ocio entre otros temas que puedan perfilar al menor edad pera ser víctima de esta modalidad.

  Recomendaciones: Es necesario poder capacitar a niños y adolescentes sobre el uso y publicación de contenidos en fuentes abiertas, supervisar el contenido de publicaciones y poder determinar acciones necesarias que pueda reducir el riesgo

[35] YouTube [Sitio web] Recomendaciones para el buen uso de las redes sociales, Policia Nacional Colombiana [Consultado el 17 de septiembre de 2021] Disponible en: https://www.youtube.com/watch?v=yrZqPPzFhTU

del Grooming sin afectar el derecho a la privacidad del niño o adolecente, la seguridad comienza en poder enseñar a nuestros menores el uso adecuado de la tecnología y la publicación de contenidos en fuentes abiertas.

- ***Sexting*:** Es una práctica de enviar o receptar contenidos de carácter sexual en fuentes abiertas como mensajería instantánea o redes sociales, el riesgo está en perder el control de estas pudiendo caer en manos inescrupulosa corriendo el riesgo de ser víctimas de chantajes y extorciones.

  Recomendaciones: La publicación de contenidos privados en fuentes abiertas es un gran riesgo, publicaciones como número de cuenta bancaria, contenido intimo no son recomendables que sean publicadas en fuentes abiertas para evitar ser víctimas de manos criminales que usen dicha información para perpetuar acciones en nuestra contra.

- ***Ciberbullying***: El matoneo cibernético es una práctica de odio o discriminación por raza, genero, hobbies y otros aspectos que hacen que internauta entre en estado de depresión; Aunque la publicación de contenidos en fuentes abiertas es quizás una expresión libre de pensamientos, aptitudes o actividades es necesario amoldarse al contexto social del entorno donde residimos para evitar ser víctimas de esta modalidad.

  Recomendaciones: Conocer el contexto social y cultural de nuestro entorno de vida para publicación de contenidos en fuentes abiertas, es quizás una de las recomendaciones más abierta en términos generales.

  Aunque muchas veces estamos amparados con bajo una figura constitucional como el derecho a la libre expresión en la práctica real no es aplicable de tal forma, publicaciones como contenidos políticos o religiosos causan mayor foco de atención en una sociedad que es diversa en pensamientos, muchas de ellas

peligrosa para nuestra integridad física, por lo que la recomendación es evitar al máximo este tipo de contenidos en fuentes abiertas asociados a nuestro perfil sin que haya antes un estudio previo del contexto tanto social y cultural que determine la viabilidad de publicación de contenidos.

- **Ciberdependencia:** Se puede definir como aquel comportamiento humano derivado del uso excesivo de la tecnología, y pese a que no está catalogado como un delito es quizás uno de los mayores riesgos que se encuentra expuesto el usuario promedio que hace uso de ella.

  La publicación de contenidos de carácter privado en fuentes abiertas como: estado actual de ubicación permite a un delincuente conocer si su hogar se encuentra solo, o la publicación de fotografías dentro del entorno laboral permite conocer las ubicaciones de cámaras de seguridad y vías de accesos a entornos restringidos son pequeños ejemplos que con el uso correcto del marco *Open Source Intelligence* (OSINT) un delincuente puede realizar una investigación para cometer de manera certera sus actos criminales.

  Recomendaciones: Reconocer de manera autónoma o con ayuda profesional la adicción a las tecnologías ya que es la consecuencia directa la publicación de contenidos privados o íntimos en fuentes abiertas, asesorarse y atender recomendaciones de expertos en seguridad para la evaluación de contenidos digitales que puedan afectar su privacidad e intimidad tanto personal como organizacional.

6 CONCLUSIONES

Se concluye que la metodología *Open Source Intelligence* (OSINT) es accesible al público en general, no es necesario tener una especialidad profesional para utilizarla en una recolección de datos en fuentes abiertas. Pero es de suma importancia que se deba llevar una adecuada clasificación de los tipos de fuentes de obtención de información ya que una investigación difiere de una planificación en tiempo y recursos y una adecuada selección de fuentes de datos garantiza el éxito de la inteligencia.

El marco de trabajo *Open Source Intelligence* (OSINT) es útil para exponer el nivel de privacidad de la información en fuentes abiertas y buscar tendencias hacia el futuro en los comportamientos de los internautas por lo que las organizaciones ven atractivo integrar la recopilación de datos con las técnicas OSINT en su toma de decisiones general de marketing. Las nuevas industrias podrán explotar los enormes datos resultantes de la revolución de la información para respaldar sus estrategias comerciales e inteligencia.

De tal forma que la metodología *Open source intelligence* (OSINT) es marco robusto y legal de obtención de información de carácter publica, pero aplicar las actividades que enmarcan una investigación con OSINT por sí solo no es suficiente para producir resultados precisos. Por ejemplo, para lograr los mejores resultados en fuentes abiertas, se deben considerar algunas tareas de valor agregado durante la fase de análisis, como utilizar asesorías de expertos para clasificar los datos y adoptar las técnicas adecuadas para adquirir inteligencia imparcial y objetiva.

En la era digital actual, es raro ver a un usuario de Internet que no tenga al menos una cuenta o más en redes sociales. Las personas utilizan los servicios de fuentes abiertas para publicar todo tipo de contenido en línea, como fotos, videos, mensajes de texto y datos de geolocalización. También mencionan su educación, historial de empleo y las direcciones donde viven. Información personal como conexiones sociales, lugares

visitados, hábitos, gustos y disgustos, miembros de la familia, cónyuge. Es por tanto que aplicar algunas de las recomendaciones dadas a tener en cuenta en la publicación de contenidos en fuentes abiertas minimiza la posibilidad de ser víctimas de ataques informáticos que vulneren la privacidad y pongan en riesgo la información tanto personal como organizacional.

RECOMENDACIONES

Ninguna metodología de recopilación de información se considera 100% completa; sin embargo, con una planificación adecuada, los recursos y la experiencia suficientes, la explotación de la metodología OSINT puede producir resultados precisos a gran escala.

Los principales motores de búsqueda de información permiten a sus usuarios encontrar contenidos multimedia como imágenes, videos, textos enriquecidos entre otros. No obstante, existen motores de búsqueda de información especializados para servidores FTP y contenidos multimedia que pueden devolver aún más resultados. Es importante tener en cuenta que las imágenes recuperadas de la web pueden contener información útil asociada a ellos: conocidos como metadatos, que deben recuperarse primero. Estos archivos también deben investigarse con herramientas especializadas para asegurarse de que no hayan sido manipulados de ninguna manera antes de considerarlos válidos.

Cuando se realice una búsqueda de información de carácter personal en línea, se recomienda probar diferentes sitios web para hacer el trabajo porque cada servicio agrega su información de diferentes bases de datos, la indexación y los mecanismos difieren entre distintos portales web. También es recomendable comenzar la búsqueda en diferentes redes sociales, medios de comunicación; Si encuentra información útil sobre el objetivo, se puede realizar un análisis más completo. Aunque algunos sitios permiten a sus usuarios reforzar sus controles de privacidad para evitar que otros vean el contenido publicado, pocas personas se preocupan por estos problemas y publican muchas de sus actividades, especialmente publicaciones de texto y registros en estado público. Esto permite acceder fácilmente a un gran volumen de datos disponible para diferentes tipos de investigaciones en línea.

BIBLIOGRAFÍA

ANTHONY OLCOTT. Open Source Intelligence in a Networked World. London: Continuum, 2012. ISBN 9781441166081. Disponible en: https://search-ebscohost-com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=nlebk&AN=450922&lang=es&site=eds-live&scope=site.

BERTRAM, S. K. The Tao of Open Source Intelligence. Ely, Cambridgeshire, United Kingdom: ITGP, 2015. ISBN 9781849287289. Disponible en: https://search-ebscohost-com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=nlebk&AN=1030094&lang=es&site=eds-live&scope=site.

Internet world stats [sitio web] Internet Usage Statistics World Internet -Users and 2020 Population Stats [Accedido el 20 de octubre 2020] Disponible en: https://www.internetworldstats.com/stats.htm

KERNAN, W.F. NATO Open Source Intelligence Handbook V1.2 [En Línea] U.S. Army, 2001. Disponible en: https://www.academia.edu/4037348/NATO_Open_Source_Intelligence_Handbook

Maltego [Sitio web] Página oficial [Accedido el 13 de septiembre de 2021] Disponible en: https://www.maltego.com/

MARANTO RIVERA. Marisol y GONZÁLEZ FERNÁNDEZ. Maria E. Fuentes de Información [En Linea] Universidad Autónoma del estado de Hidalgo,2015. Disponible en: https://repository.uaeh.edu.mx/bitstream/bitstream/handle/123456789/16700/LECT132.pdf

Rodriguez, Yago. Inteligencia De Fuentes Abiertas (OSINT): Características, Debilidades Y Engaño. [Citado el 03 de septiembre de 2021] Disponible en Internet:

http://www.seguridadinternacional.es/?q=es/content/inteligencia-de-fuentes-abiertas-osint-caracter%C3%ADsticas-debilidades-y-enga%C3%B1o

twitter.com [sitio web] Perfil Lori Lewis [Accedido el 20 de octubre 2020] Disponible en: https://twitter.com/lorilewis

Welivesecurity [Sitio web] Maltego, la herramienta que te muestra qué tan expuesto estás en Internet [Accedido el 13 de septiembre de 2021] Disponible en: https://www.welivesecurity.com/la-es/2014/02/19/maltego-herramienta-muestra-tan-expuesto-estas-internet/

Youtube [Sitio web] ¿Qué es OSINT? Fases y fuentes del proceso. Canal Palabras de hackers-Vicente Aguilera. [consultado el 05 de septiembre 2020] Disponible en: https://www.youtube.com/watch?v=Y5oHlQAAJjM

Youtube [Sitio web] OSINT e Ingeniería Social: como vectores de ataque a la ciberseguridad. Instituto Nacional de Ciberseguridad de España. [consultado el 05 de septiembre 2020] Disponible en: https://www.youtube.com/watch?v=ZaivL8_J3j4&t=95s

ANEXO

ANEXO A - ESTRUCTURA DEL DOCUMENTO PARA LA ESTRUCTURA DEL RESUMEN ANALÍTICA ESPECIALIZADO -RAE

Fecha de Realización:	30/10/2021
Programa:	Especialización en Seguridad Informática
Línea de Investigación:	Investigación Infraestructura tecnológica y seguridad en redes.
Título:	ANÁLISIS DEL NIVEL DE EXPOSICIÓN Y PRIVACIDAD DE INFORMACIÓN PERSONAL EN FUENTES ABIERTAS A TRAVÉS DE LA METODOLOGÍA OPEN SOURCE INTELLIGENCE (OSINT)
Autor(es):	David Alfonso Vega Palacio
Palabras Claves:	Fuentes abiertas Información digital Internet Inteligencia Metodología
Descripción:	El presente documento monográfico pretende contextualizar al lector en la importancia de la privacidad de su información personal en fuentes abiertas y permite recomendar acciones de buenas prácticas en la publicación de contenidos digitales en internet.

	Se soporta en la recolección de distintas fuentes de información y busca la obtención de una visión general del comportamiento y percepción del internauta en la publicación de contenidos personales en fuentes abiertas, pretendiendo demostrar mediante técnicas de *Open Source Intelligence* (OSINT) el nivel de exposición de la privacidad personal en internet tomando como tesis principal que la vulnerabilidad más susceptible en cualquier sistema informático es el ser humano. Por lo que conocer algunas de las múltiples herramientas brindadas por la metodología *Open Source Intelligence* (OSINT) para la correcta toma de decisión en el robustecimiento de la exposición y privacidad de información personal en fuentes abiertas, permite al internauta evitar ser víctimas como robo de identidad, ataques informáticos y otras circunstancias que vulneren el derecho de su intimidad y buen nombre.
Fuentes bibliográficas destacadas: ANTHONY OLCOTT. Open Source Intelligence in a Networked World. London: Continuum, 2012. ISBN 9781441166081. Disponible en: https://search-ebscohost-com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=nlebk&AN=450922&lang=es&site=eds-live&scope=site.	

<table>
<tr><td colspan="2">BERTRAM, S. K. The Tao of Open Source Intelligence. Ely, Cambridgeshire, United Kingdom: ITGP, 2015. ISBN 9781849287289. Disponible en: https://search-ebscohost-com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=nlebk&AN=1030094&lang=es&site=eds-live&scope=site

Youtube [Sitio web] ¿Qué es OSINT? Fases y fuentes del proceso. Canal Palabras de hackers-Vicente Aguilera. [consultado el 05 de septiembre 2020] Disponible en: https://www.youtube.com/watch?v=Y5oHlQAAJjM

Youtube [Sitio web] OSINT e Ingeniería Social: como vectores de ataque a la ciberseguridad. Instituto Nacional de Ciberseguridad de España. [consultado el 05 de septiembre 2020] Disponible en: https://www.youtube.com/watch?v=ZaivL8_J3j4&t=95s

Rodriguez, Yago. Inteligencia De Fuentes Abiertas (OSINT): Características, Debilidades Y Engaño. [Citado el 03 de septiembre de 2021] Disponible en Internet: http://www.seguridadinternacional.es/?q=es/content/inteligencia-de-fuentes-abiertas-osint-caracter%C3%ADsticas-debilidades-y-enga%C3%B1o</td></tr>
<tr><td>Contenido del documento:</td><td>En el documento se expone cuatro apartados generales que construyen el objetivo general del mismo.

El primer apartado denominado Identificación de tipos de fuentes de obtención de información de carácter público necesarios para la aplicación de la metodología open source intelligence (OSINT), aborda aquellas fuentes de información de carácter publico</td></tr>
</table>

	donde es posible sustraer datos de forma legal para el investigador. El segundo apartado denominado Marco de investigación *Open Source Intelligence* (OSINT) sus aplicaciones, métodos, retos y beneficios en la recolección de información personal en fuentes abiertas, aborda el concepto de la investigación con la metodología OSINT sus alcances, sus aplicaciones y e información necesaria para el abordamiento de una investigación legal de recolección de datos públicos. En el tercer apartado se encuentra un caso práctico de ejemplo dentro del contexto académico en aplicación de la metodología OSINT para el análisis del nivel de exposición y privacidad de datos personales en internet de un usuario a partir de un número de teléfono celular. En el cuarto apartado se encontrará con recomendaciones al internauta en tomar acciones necesarias para poder aumentar la seguridad en sus datos personales, mitigación del riesgo en ataques informáticos y fortalecimiento en el nivel de privacidad en fuentes abierta y prevención de riesgos en

	internet como el grooming, sexting, ciberbullying, y ciberdependencia
Conceptos adquiridos :	La era de la información actual ha dado lugar a una cantidad explosiva de inteligencia potencial en fuentes abiertas y dará forma al futuro de la recopilación del marco de trabajo *Open Source Intelligence* OSINT. En el campo de la inteligencia, se predijo que la práctica de recopilar datos en línea para combatir el nivel de exposición y privacidad personal en internet es efectivo para minimizar riesgos potenciales que afecten la información tanto organizacional como individual. Además, la metodología Open Source Intelligence OSINT seguirá ofreciendo un método económico para adquirir inteligencia sobre cualquier comunidad en todo el mundo. Desde una perspectiva de seguridad de la información, la recopilación del marco OSINT seguirá siendo un trampolín para la mayoría de las evaluaciones de pruebas de penetración para evaluar las debilidades del sistema en su factor humano y trabajar en inteligencia para solucionarlos rápidamente.
Conclusiones:	Se concluye que la metodología *Open Source Intelligence* (OSINT) es accesible al público en general, no es necesario tener una

	especialidad profesional para utilizarla en una recolección de datos en fuentes abiertas. Pero es de suma importancia que se deba llevar una adecuada clasificación de los tipos de fuentes de obtención de información ya que una investigación difiere de una planificación en tiempo y recursos y una adecuada selección de fuentes de datos garantiza el éxito de la inteligencia. El marco de trabajo *Open Source Intelligence* (OSINT) es útil para exponer el nivel de privacidad de la información en fuentes abiertas y buscar tendencias hacia el futuro en los comportamientos de los internautas por lo que las organizaciones ven atractivo integrar la recopilación de datos con las técnicas OSINT en su toma de decisiones general de marketing. Las nuevas industrias podrán explotar los enormes datos resultantes de la revolución de la información para respaldar sus estrategias comerciales e inteligencia. De tal forma que la metodología *Open source intelligence* (OSINT) es marco robusto y legal de obtención de información de carácter publica, pero aplicar las actividades que enmarcan una investigación con OSINT por sí solo no es suficiente para producir resultados

	precisos. Por ejemplo, para lograr los mejores resultados en fuentes abiertas, se deben considerar algunas tareas de valor agregado durante la fase de análisis, como utilizar asesorías de expertos para clasificar los datos y adoptar las técnicas adecuadas para adquirir inteligencia imparcial y objetiva. En la era digital actual, es raro ver a un usuario de Internet que no tenga al menos una cuenta o más en redes sociales. Las personas utilizan los servicios de fuentes abiertas para publicar todo tipo de contenido en línea, como fotos, videos, mensajes de texto y datos de geolocalización. También mencionan su educación, historial de empleo y las direcciones donde viven. Información personal como conexiones sociales, lugares visitados, hábitos, gustos y disgustos, miembros de la familia, cónyuge. Es por tanto que aplicar algunas de las recomendaciones dadas a tener en cuenta en la publicación de contenidos en fuentes abiertas minimiza la posibilidad de ser víctimas de ataques informáticos que vulneren la privacidad y pongan en riesgo la información tanto personal como organizacional.