UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR

POSGRADOS

MAESTRÍA EN
**SEGURIDAD DE LA INFORMACIÓN**
RPC-SO-28-NO.669-2021

OPCIÓN DE TITULACIÓN:

PROYECTO DE TITULACIÓN CON COMPONENTES DE INVESTIGACIÓN APLICADA Y/O DE DESARROLLO

TEMA:

# ESTUDIO DE HERRAMIENTAS OSINT PARA CIBERSEGURIDAD.

AUTOR:

DIEGO LEONARDO CHIMBO CHILLOGALLI

DIRECTOR:

RODOLFO XAVIER BOJORQUE CHASI

CUENCA – ECUADOR
2023

**Autor:**

**Diego Leonardo Chimbo Chillogalli**
Ingeniero de Sistemas.
Candidato a Magíster en Seguridad de la Información por la Universidad Politécnica Salesiana – Sede Cuenca.
dchimbo@est.ups.edu.ec

**Dirigido por:**

**Rodolfo Xavier Bojorque Chasi**
Ingeniero de Sistemas.
Magíster en Seguridad de las Tecnologías de la Información y Comunicación.
Magíster en Ciencias y Tecnologías de la Computación.
Doctor en Ciencias y Tecnologías de la Computación para Smart Cities.
rbojorque@ups.edu.ec

***DEDICATORIA***

A mi familia, por la paciencia y apoyo brindado sobre todo en los puntos más álgidos de este proceso de aprendizaje. Son ustedes quienes día a día me motivan para seguir superándome y plantearme nuevos retos.

***AGRADECIMIENTO***

Al terminar esta etapa de estudio, no puedo dejar de agradecer a cada una de las personas que participaron en ella. A mi tutor, por ofrecerme su guía y apoyo en este proceso. Su experiencia en el campo de la investigación fue muy útil en todo momento. Ha sido un privilegio contar con su tutoría a lo largo del desarrollo del proyecto. A mis amigos y compañeros, quienes de una u otra forma aportaron con su tiempo, ideas y criterios sobre el presente trabajo. A los docentes, que en cada una de las materias nos brindaron su esfuerzo por compartir de manera clara y concisa el conocimiento que hoy tenemos. A todas las personas les hago extensivo un agradecimiento de todo corazón.

# Tabla de Contenido

# ESTUDIO DE HERRAMIENTAS OSINT PARA CIBERSEGURIDAD


AUTOR:

DIEGO LEONARDO CHIMBO CHILLOGALLI

# Resumen

La tecnología ofrece varios beneficios a la humanidad. Pero, también se ha vuelto un punto crítico en la seguridad y privacidad de todos. Cada vez son más las personas que tienen acceso a internet y que generan una huella digital perfectamente rastreable en la web.

Este trabajo expone levemente la forma en la que cualquier individuo puede encontrar a otro haciendo uso de técnicas y herramientas OSINT. Como caso práctico se utiliza la página institucional de la Universidad Politécnica Salesiana para la búsqueda de la información primaria. Se recurre a las distintas redes sociales disponibles, como complemento en la búsqueda de información.

La sociedad enfrenta cada día más casos de ciberacoso, cyberbullying, estafas, secuestros, etc. En varios de los casos, son las mismas personas las que proporcionan la información necesaria para la planificación de los ataques de los que son víctimas.

Se busca la concientización de cada individuo para que este asuma responsablemente la información que comparte en internet de manera pública. De este modo se reduciría el alcance que una persona puede hacer dentro de una investigación con objetivos protervos.

La nueva ley de protección de datos personales trae varios cambios en la manera en la que se manejan estos. Se analizan los datos compartidos en la web institucional y la política de datos vigente.

**Palabras clave:**

OSINT, inteligencia en fuentes abiertas, sobreexposición, ciberseguridad.

# Abstract

Technology offers several benefits to humanity. But it has also become a critical point in the security and privacy of everyone. More and more people have access to the internet and generate a perfectly traceable digital footprint on the web.

This work briefly exposes the way in which any individual can find another using OSINT techniques and tools. The institutional website of the Salesian Polytechnic University is used as a practical case for the search of primary information. Different available social networks are used as a complement in the information search.

Society faces more and more cases of cyberbullying, scams, kidnappings, etc. In several of these cases, it is the same individuals who provide the necessary information for planning the attacks of which they are victims.

Awareness is sought from each individual so that they assume responsibly the information they share publicly on the internet. In this way, the scope that a person can have within an investigation with malicious objectives would be reduced.

The new law on personal data protection brings several changes in the way these are handled. The data shared on the institutional website and the current data policy are analyzed.

**Palabras clave:**
OSINT, open source intelligence, oversharing, cybersecurity.

# 1. Introducción

En el mundo digitalizado de hoy, la seguridad de la información se ha vuelto un tema fundamental en la vida de los seres humanos, ya sea esto a nivel empresarial, como a nivel personal. El crecimiento desmesurado de información disponible en la web abre la puerta a la aplicación de varias técnicas que permiten el filtrado y clasificación de la información con diferentes propósitos. El tema en el que se centra este trabajo es OSINT (siglas de Open Source Intelligence), y permitirá apreciar de manera clara como de manera voluntaria o involuntaria, nos encontramos expuestos en Internet.

De forma paralela se analizará cuan legal se vuelve el compartir datos de manera abierta luego de la aprobación de la nueva "Ley de Protección de Datos Personales" en Ecuador, sin que haya consentimiento expreso de difusión por parte del titular de la información que se encuentra disponible actualmente en fuentes públicas.

# 2. Determinación del Problema

Si bien la evolución de Internet como medio de comunicación e interacción presenta varias ventajas, no es menos cierto que también trae consigo complicaciones relacionadas a la privacidad de cada individuo/entidad que mantiene algún dato que lo hace identificable en la web. No todas las personas tienen la libre potestad de decidir la información suya que se expone públicamente, existen casos en los que filtraciones de hackers dejan vulnerables tanto a personas como instituciones, solo basta recordar la información que se expuso en un servidor administrado por Novaestrat, en el que se encontraban cerca de 18 GB de información personal de ecuatorianos [1]. También existen situaciones en las que una mala planificación, un mal diseño de software o un simple descuido deja expuesta información sensible de personas que confiaron su información personal a una institución, es justamente aquí donde las herramientas OSINT hacen su aparición y permitirán hacer un estudio que determine el nivel de riesgo al que se exponen las personas en la actualidad.

Como caso de estudio se ha tomado de ejemplo la página web de la Universidad Politécnica Salesiana, esta será analizada con el objetivo de identificar posibles fugas de información ya sea de sus colaboradores o alumnos.

# 3. Marco teórico referencial

Es imprescindible entender algunos conceptos que darán la perspectiva necesaria para analizar los casos que se vayan presentando con el uso de herramientas OSINT. Si bien el uso de herramientas será variado, los conceptos son muy generales al momento de estudiar un caso particular.

El actor principal que se identifica en el presente trabajo es el ser humano, por tal motivo, se empezará revisando la forma en la que se lo puede identificar en la red.

## 3.1 Identidad Digital

En los últimos años el ser humano se ha ido involucrando más en una vida digital, siendo así, interactúa socialmente, vende o compra servicios y bienes, escucha música, mira videos, estudia, realiza búsquedas de algún tema de su interés, etc.; todas estas actividades generan una identidad digital en Internet con el propósito de diferenciar a unas personas de otras. El termino de identidad digital es tan amplio, como variado; basta con abrir una pestaña en el navegador para generar una primera identidad digital conocida como "Browser Fingerprinting" que, basándose en cookies, direcciones IP, resoluciones de pantalla usadas con el navegador, sistemas operativos, fuentes, etc.; genera un identificador único para ese navegador y permite identificar las actividades y costumbres de navegación que una persona realiza, aunque no se conozca a ciencia cierta al individuo[2]. Cabe destacar que el identificador único del navegador se puede generar aún en el modo "incógnito" que ofrecen algunos navegadores, consecuentemente, el identificador sigue siendo el mismo aún después de haber reiniciado el navegador en dicho modo. Por otro lado, están las identidades digitales que se construyen con información proporcionada por las mismas personas y que dan mayor detalle para una identificación más exacta. Los datos pueden clasificarse como [3]:

- Datos de identidad individual

- Datos de comportamiento
- Datos derivados o calculados
- Datos de usuario para identificación propia

Cualquiera sea la naturaleza de los datos permite una identificación y la información puede ser usada con diferentes propósitos desde envío de publicidad dirigida o focalizada, hasta la creación completa de perfiles que identifique a una persona, familia o empresa. La fig. 01 muestra la evolución que ha tenido Internet y como se fue convirtiendo en un medio de socialización.

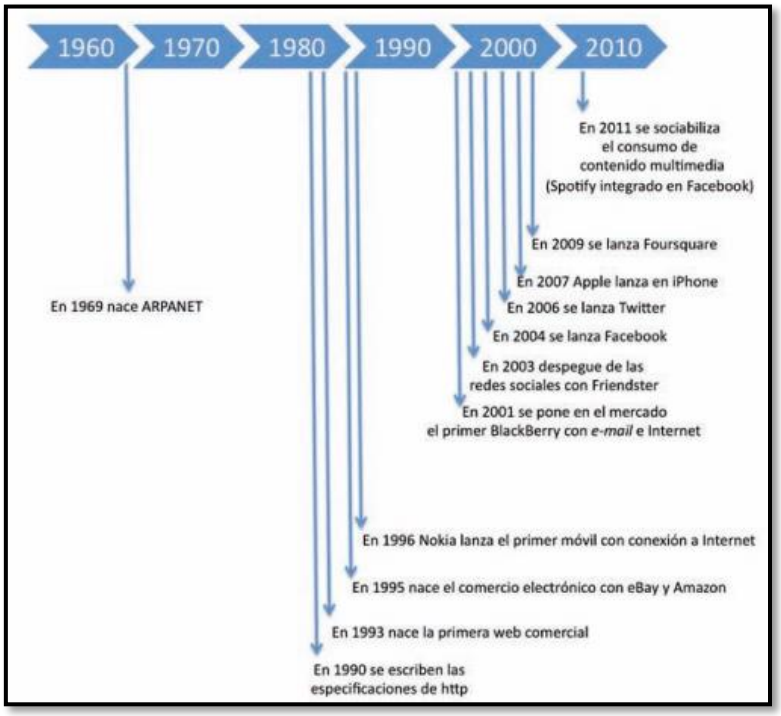


**Fig. 01** Hitos en la evolución de Internet (**Fuente:** Fundación Telefónica [3])

## 3.2 OVERSHARING

Un término para considerar cuando se habla de exposición de la información en redes sociales es el de “Oversharing” y trata la sobre exposición que algunas personas hacen de su vida privada. El término no se refiere a la sobre exposición en referencia a la cantidad de información compartida, sino más bien al tipo de información que se comparte, pues esta pone en riesgo la seguridad del individuo.

Indicar en la ubicación en la que se encuentra, quienes lo acompañan, a donde irá de viaje, días que se ausentará de casa, son algunos de los ejemplos de información que no se debe compartir y que, sin embargo, se encuentra a diario en las diferentes redes sociales. Se conoce que los adolescentes exponen cerca del 61% de su información personal en Internet [4].

Las consecuencias sobre lo descrito anteriormente pueden ser:

- Ciberacoso
- Grooming
- Phishing
- Sexting

A través del uso herramientas OSINT se podrá dar una mejor perspectiva sobre este apartado.

## 3.3 OSINT

Termino que proviene de "Open Source Inteligence", se refiere a todo tipo de información que se puede recopilar de fuentes públicas y que posteriormente se le puede aplicar un análisis (inteligencia), con el fin de exponer vulnerabilidades, crear perfiles sociales o determinar cualquier tipo de investigación sobre un tema particular [5]. Cabe notar que las técnicas de OSINT no es algo nuevo, y que su uso se remonta hacia varias décadas atrás donde las fuentes usadas eran periódicos, libros y medios de comunicación en general.

Con el crecimiento exponencial que tuvo el uso de internet con la reciente pandemia de COVID-19, las fuentes de información de OSINT también fueron en aumento. Hablamos de que el 63% de la población mundial llegó a estar conectada a internet [6] tal como se indica en la fig. 02.

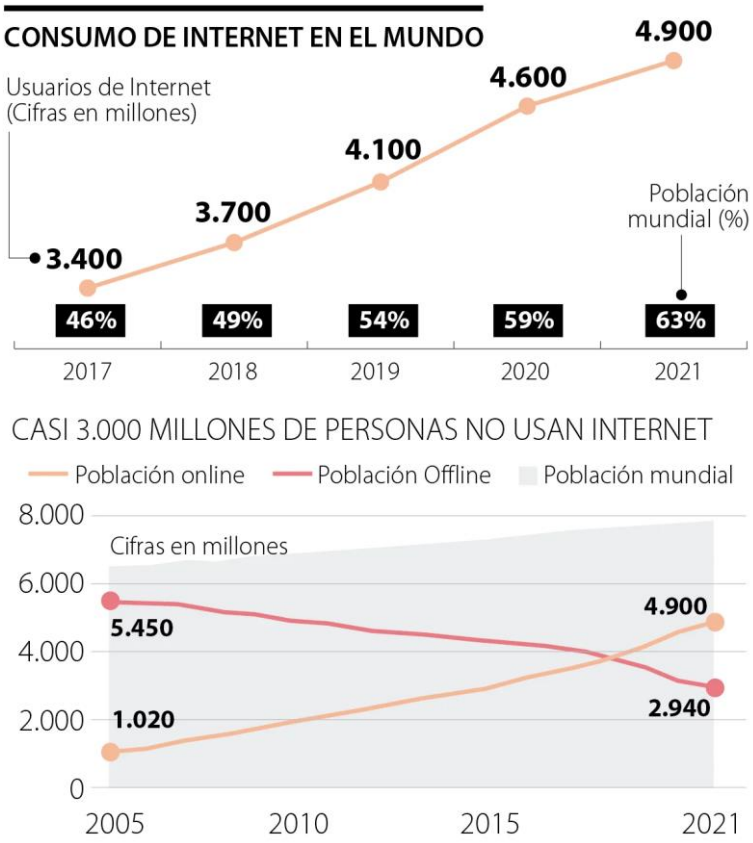


**Fig. 02.** Consumo de Internet en el mundo (**Fuente:** ITU [6])

De todos los medios usados en internet, las redes sociales continúan siendo las preferidas entre los usuarios que dedican un promedio de dos horas con veintisiete minutos al día, esto representa un incremento de tiempo de 1.4% en el año 2022 respecto del año 2021 [7].

Aunque OSINT permite recolectar información de cualquier persona o entidad que tenga una identidad digital en la web, hay que tener presente que el mayor uso del internet se da en personas que están en un rango de edad de entre 15 y 24 años y este representa el 71% del uso global [8]. Por lo tanto, a la hora de recolectar datos también hay que prestar atención de donde se puede obtener una mejor fuente de información, de acuerdo con el caso se pueden evaluar criterios como la edad, género, tendencias, etc. La aplicabilidad es muy extensa, sus usos más conocidos son: análisis de vulnerabilidades (pentesting), análisis de perfiles sociales, estudios de marketing y ciber investigación para procesos judiciales.

### 3.3.1 Ventajas y Desventajas de Usar OSINT

Como cualquier proceso de recolección de datos, OSINT cuenta con ventajas y desventajas. A continuación, se citan algunas de estas [9]:

- Recolección rápida de información desde distintas fuentes.
- La información obtenida es legal por provenir de fuentes abiertas.
- Fácil acceso a las fuentes.
- El costo del proceso es relativamente bajo en comparación a la cantidad de información que se puede obtener.
- Se puede complementar la investigación con otras fuentes distintas de OSINT.
- Demasiada información podría ser difícil de procesar.
- Los datos recolectados no están ordenados.
- Dependiendo del caso, la información puede ser subvalorada por instancias jurídicas.
- Dependiendo de las fuentes consultadas el resultado podría producir desinformación.
- OSINT también puede ser usado con fines maliciosos.

### 3.3.2 Proceso de OSINT

Es fundamental seguir un proceso organizado a la hora de recolectar información a través de herramientas OSINT, esto debido a la gran cantidad de datos que se puedan conseguir en las distintas fuentes que se han de consultar. Se recomienda seguir las fases (fig. 03) a continuación descritas [10, 11]:

**Requisitos:** Se analiza el caso particular de estudio y se establecen las necesidades que darán solución al problema.

**Fuentes de información:** de acuerdo con las necesidades que se revisaron en el punto anterior, se han de seleccionar las fuentes más confiables para la recolección de datos.

**Adquisición:** explotación de las fuentes de información.

**Procesamiento:** se organiza la información recogida con el objetivo de su posterior análisis.

**Análisis:** en base a la información recolectada se aplica inteligencia que deje ver claramente patrones o relaciones entre los datos, que han de ser de utilidad para la solución del caso de estudio.

**Presentación de la inteligencia:** consiste en la presentación de los datos depurados que ayudarán en la generación de conocimiento y/o solución de problemas.

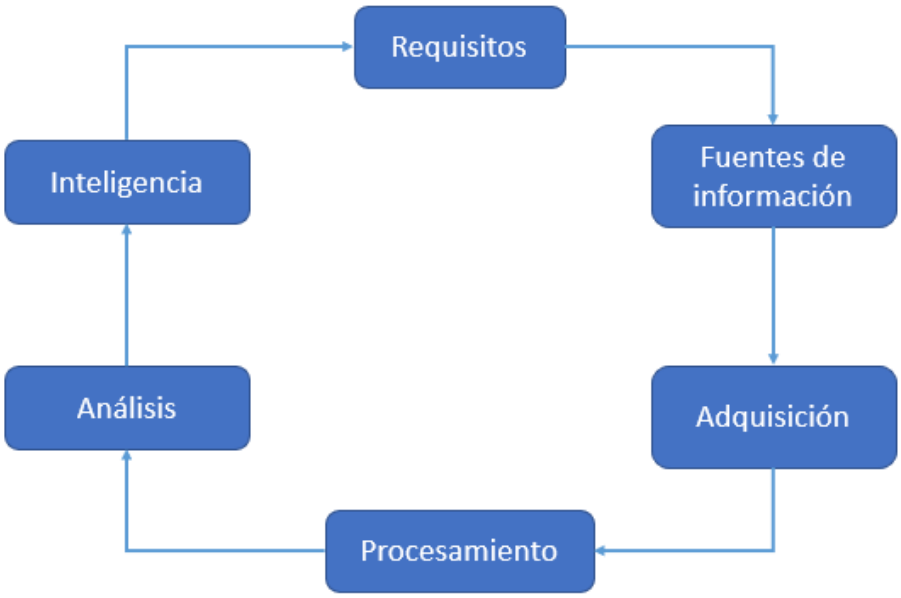


**Fig. 03** Fases de OSINT (Fuente: Hacking Web Intelligence [10])

## 3.4 Técnicas y Herramientas OSINT

Ante el incremento constante en el consumo de Internet y todos sus servicios interconectados, así como también el crecimiento de la inseguridad; surge la necesidad de extremar las medidas de protección, visto desde un punto de vista social es necesario analizar los diferentes escenarios que pudieran presentarse, es aquí donde aparecen varias técnicas para la recolección de datos.

La historia y uso de OSINT se ha ido extendiendo a lo largo de los años. Existen varios eventos a nivel mundial conocidos como “hackathon”, en dichos eventos participantes de varios lugares se reúnen para mostrar sus destrezas en el campo de la investigación haciendo uso de técnicas OSINT.

En mayo de 2022, se organizó la primera conferencia exclusiva de OSINT e ingeniería social denominada “Osintomático Conference 2022” y llevada a cabo en Madrid, España. Fueron 25 ponencias presenciadas por 550 asistentes al evento (Fig. 04). Las actividades estaban enfocadas en impartir conocimiento y crear conciencia entre los participantes. Como punto cumbre del evento, se tuvo una actividad denomina CTF (Capture The Flag), que no es más que un concurso en el que las personas que participan reúnen puntos al ir cumpliendo metas u objetivos, para esto se hace uso de herramientas OSINT y sus conocimientos particulares. El tema del concurso fue buscar pistas sobre personas desaparecidas en la vida real [12].


**Fig. 04** Ponencia de Mikel Rufián en el evento. (**Fuente:** Bidaidea[12])

Al hablar de técnicas usadas en la recolección de datos mediante el proceso de OSINT, se habla de un método global que puede tener distintas herramientas enfocadas en realizar un mismo trabajo para diferentes campos.

### 3.4.1 Técnica del buscador

Una técnica muy eficaz para OSINT consiste en realizar búsquedas a través de los diferentes motores de búsqueda que se pueden encontrar en la web. Como ejemplos y entre los más conocidos tenemos los buscadores de Google, Yahoo, Bing, Dogpile, Yandex, DuckDuckGo, Ask. La mayoría de los motores de búsqueda tienen un funcionamiento similar y permiten buscar palabras específicas, personas por nombre y fotografía, búsquedas dentro de un dominio particular, buscar perfiles en redes sociales, buscar archivos, buscar incluso contraseñas o diccionarios para ataques de fuerza bruta, etc.

El buscador de Google es de los más famosos alrededor del mundo, en dicho buscador hay algo conocido como “dorks” que ayudan a que las búsquedas puedan ser de lo más precisas. Citando algunos “dorks” [13] para una mejor comprensión tenemos: la búsqueda por términos específicos cuando se utilizan comillas, búsquedas dentro de un dominio concreto citando términos y la URL, búsqueda por tipo de archivo especificando la extensión, búsqueda por título de la página web, búsquedas con comodines que permiten por ejemplo buscar textos incompletos haciendo uso del comodín asterisco.

En referencia a la búsqueda de imágenes, está ha sido de gran utilidad en los últimos años, el reconocimiento facial se muestra como un recurso amplio con la aparición y uso de cámaras de seguridad, cámaras fotográficas de excelente calidad en teléfonos móviles y la consecuente exposición en el internet crea el ambiente perfecto para hacer comparaciones a través de inteligencia artificial para dar con alguien o al menos conocer datos más certeros que permitan su ubicación [14].

Los buscadores citados pueden ser usados como herramientas, aunque cabe destacar que hay buscadores especializados en la recolección de datos más específicos, es el caso del buscador Shodan que con sus filtros es capaz de encontrar

direcciones IP de varios dispositivos, con determinados puertos abiertos en internet [15].

Hay que saber que cualquiera de las técnicas de OSINT, es un buen complemento cuando se piensa en implementar un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001. En el artículo denominado "OSINT Techniques Integration with Risk Assessment ISO/IEC 27001" [16], se observa la aplicación de varias técnicas, entre ellas Google Dorking, para dejar expuestas las falencias de seguridad presentes en la empresa de nombre "Aramex International". El contexto de la aplicación es similar al que se pretende seguir en el presente trabajo.

### 3.4.2 Técnica de las Redes Sociales

Las redes sociales se han convertido en la mayor fuente de información abierta disponible en internet, por eso es usada para crear perfiles psicológicos que pueden evidenciar fortalezas y debilidades de una persona específica. La red social más utilizada a octubre 2021 (Fig. 05), sigue siendo Facebook [17] y por el contenido que ofrece es una de las que más aporta en la creación de un perfil.

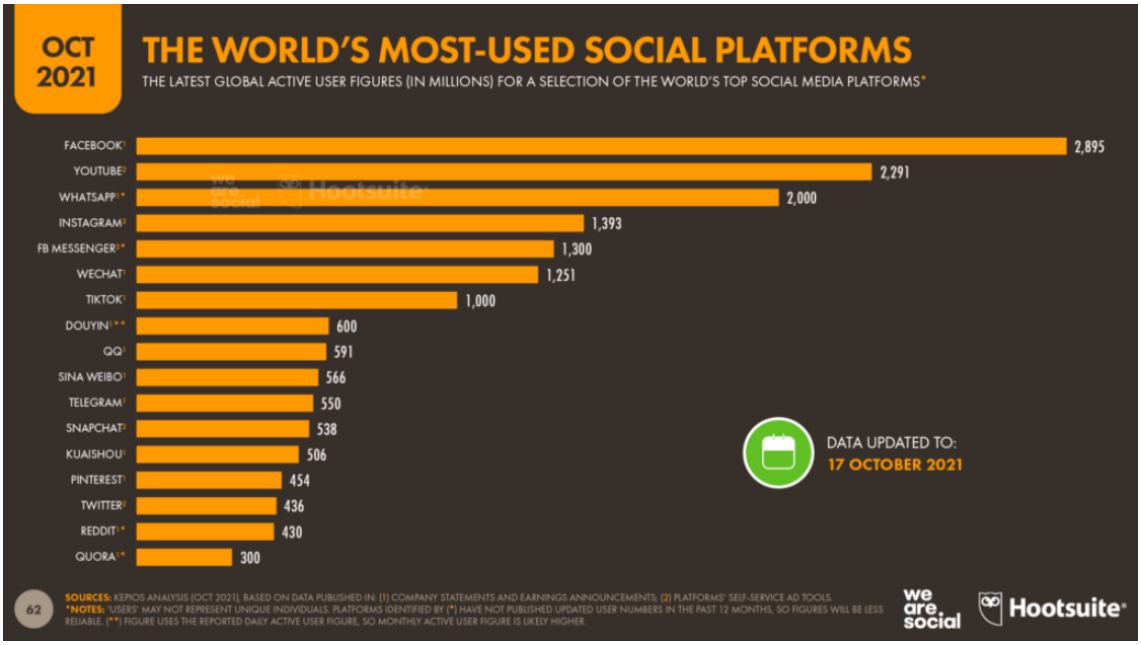


**Fig. 05** Usuarios activos de redes sociales (**Fuente:** We are social [17])

La información que se puede conseguir de las redes sociales es muy importante, a partir de esta se pueden determinar factores como: género, religión, tendencia política, rasgos de personalidad, edad, gustos, situaciones de su vida personal. Un estudio [18] basándose en la cantidad de "Me gusta" hechos en la red social Facebook, ha sido capaz de diferenciar con un 88% de exactitud el género de una persona, en un 82% se ha diferenciado a cristianos de musulmanes, en un 65% se ha coincidido con el estado civil y en un 73% se ha determinado si la persona hace uso de alguna sustancia adictiva; todo esto con una muestra de 58000 personas. El mismo estudio en menor proporción de aciertos consiguió establecer si un individuo era introvertido o extravertido y determinar si su perfil emocional podía ser estable o no.

Cada red social maneja su propio estilo y temática, a continuación, se presentan los contenidos de las principales redes sociales [19]:

LinkedIn. Información que ofrece:

- Historial de trabajo
- Lugar de estudios
- Títulos obtenidos
- Clubes y logros académicos
- Referencias personales

Facebook. Información disponible:

- Música favorita
- Películas favoritas
- Clubes a los que pertenece
- Listados de amigos y familia
- Vacaciones, lugares visitados, fechas
- Comida favorita
- Lugar de residencia

Twitter. En publicaciones de hasta 280 caracteres, ofrece:

- Que se está haciendo ahora mismo
- Hábitos alimenticios
- Geolocalización
- Estado emocional

Sin duda, la parte emocional y psicológica de un individuo determina su personalidad, no obstante, existen cientos de factores que componen esta característica. Para el caso del presente trabajo, no se pretende profundizar demasiado en la construcción de un perfil. Se hará uso únicamente de la interacción que puedan tener la persona a través del botón "Me Gusta" en redes sociales. Se hará el uso de la metodología de nodos y enlaces, por nodos entiéndase una persona en cualquier red social y por enlace, el vínculo que existe entre los nodos (personas) pudiendo ser este más fuerte que otro en determinadas circunstancias. La intensidad del enlace se mide en cantidad de interacciones entre los nodos. Visto de otro modo, las interacciones entre los nodos evidencian empatía y ayudan a perfilar la personalidad de un nodo. Es de tener muy presente que la interacción se debe dar de manera bidireccional, pues si esta llegase a ser unidireccional mostraría que no hay afinidad entre los nodos. Justamente es aquí donde la recolección de data con herramientas OSINT es de gran ayuda [20].

Cuando se habla de privacidad, intrínsicamente se toca la seguridad del individuo o entidad y es la razón fundamental por la que las personas deben tomar conciencia y aprender a manejar los ajustes de privacidad disponibles en las diferentes redes sociales, del mismo modo deben tomar conciencia de la información que comparten y si es relevante hacerlo.

### 3.4.3 Técnica del Correo Electrónico

Conocer la dirección de un correo electrónico al momento de empezar una investigación, representa un buen punto de partida dado que es un dato que está

ligado con varias cuentas de un mismo usuario. Ahora bien, si no se dispone del correo se debe hacer uso de alguna otra técnica que permita conocer este dato, un caso práctico sería hacer búsquedas por nombre en algún navegador. Hay casos en los que los sistemas de recuperación de contraseñas están implementados sin tener presentes controles de privacidad y exponen el dato del correo electrónico con simplemente conocer el número de documento de identificación personal o algún dato secundario como un número de teléfono, nombre de usuario, etc. [21].

Conociendo el dato del correo electrónico, se deben hacer algunas validaciones que aseguren su uso. Existen herramientas OSINT capaces de validar si una dirección aun esta activa, si esta se ha visto comprometida recientemente en alguna divulgación de datos, también se pueden conocer algunos datos personales como el nombre en el caso de haber partido investigando desde la dirección de correo. Algunas herramientas conocidas son: Pipl, Have I Been Pwned, Hunter.

### 3.4.4 Técnica del Nombre de Usuario

Ya sea en redes sociales, foros o cualquier otro medio de interacción; se permite el uso de sobrenombres con el propósito de ocultar el nombre real de un usuario y así no se expongan datos privados abiertamente. Otra de las técnicas propuestas por OSINT sugiere la búsqueda masiva en diferentes dominios por medio del nombre de usuario, de este modo se consiguen varias fuentes que pueden ser usadas para la extracción de información importante [22]. Name Checkr es una herramienta que ayuda con estas consultas.

### 3.4.5 Técnica del Nombre real

Partir con el dato inicial del nombre real, ya sea que este completo o parcial, dará buenas posibilidades para ir consiguiendo datos secundarios. En este apartado, hay que destacar que hay herramientas (varias de pago), que brindan un detalle muy completo de direcciones de domicilio, números de teléfono, correos electrónicos, direcciones IP, nivel de estudio, parentesco hablando del árbol genealógico, entre

otros [23]. El problema con la mayor parte de las herramientas es que las búsquedas están optimizadas para hacerse en EEUU y parte de Europa.

Hablando de Ecuador, están disponibles las páginas del: SRI, Registro Civil, Senescyt; que permiten hacer búsquedas y conocer datos personales complementarios.

### 3.4.6 Técnica de la Ubicación

Geolocalizar a una persona se vuelve una técnica que puede ofrecer considerable información dentro de una investigación, el requisito indispensable es conocer las coordenadas GPS. A este proceso también se le conoce como GEOINT, término que proviene de inteligencia geoespacial, para ser considerada una fuente de OSINT la información obtenida de ubicaciones tiene que provenir obligatoriamente de una fuente pública. Una de las formas de conseguir datos de coordenadas GPS, es analizando los metadatos de archivos; si se tiene una fotografía que fue tomada por un smartphone, es probable que esta haya lleve un registro del lugar en donde se tomó [24]. Ya con los datos procesados se pueden crear las rutas habituales del objetivo estudiado. El servicio más consultado es el de Google Maps, aunque también están Bing Maps y Apple Maps.

### 3.4.7 Técnica de la Dirección IP

Uno de los caminos que llevan a la ubicación física de una determinada persona o institución, pasa por el hecho de conocer su dirección IP. Existen varias maneras de conocer este dato, una de ella sería analizar el encabezado de un correo electrónico que generalmente contiene la dirección IP desde donde proviene, también es posible encontrar direcciones IP en filtraciones expuestas en foros o en la web profunda, todo en dependencia del perfil de investigación. Teniendo una dirección IP, se pueden consultar herramientas web que dejan conocer datos como el proveedor de internet y la ubicación aproximada desde donde se está haciendo uso de la IP; hay que tener en cuenta que varios ISP entregan direcciones IP dinámicas a sus clientes domiciliarios, razón por la que es posible que la dirección que hoy tiene un cierto personaje mañana no sea la misma [25]. En esta labor de búsqueda,

páginas como IP Location (www.iplocation.net), Cuál es mi IP (www.cual-es-mi-ip.net) o View DNS (www.viewdns.info), ayudan de buena forma en obtener información primaria.

### 3.4.8 Técnica de los Nombres de Dominio

Complementándose con el punto anterior, se tiene la técnica de los nombres de dominio. Cuando se registra un dominio se solicitan datos de contacto, algunos de ellos pueden ser consultados mediante herramientas e indican nombres, algún correo o número telefónico de contacto que puede ser usado para obtener otros datos a partir de ellos. Consultar el contenido de la página web del dominio en cuestión, también aporta datos interesantes a la investigación, algunos servicios en la web ofrecen copias de las versiones anteriores de la página web, cuando se revisan dichas versiones, es posible encontrar datos de contacto o filtraciones que fueron corregidas en las versiones más recientes del sitio [26]. Algunas herramientas conocidas para la búsqueda son: who.is (www.who.is), SecurityTrails (https://securitytrails.com/dns-trails), Internet Archive (www.web.archive.org).

Todas las técnicas se pueden complementar unas a otras, en un contexto de seguridad informática el propósito es generar el conocimiento oportuno que permita tomar las medidas atenuantes correspondientes con el fin de mantener un medio o a una persona seguros. Ventajosamente OSINT mediante su análisis ha podido identificar comportamientos inadecuados presentes en internet, ha identificado estafas, diferentes tipos de explotación, filtraciones de datos, robos de identidades y otros varios temas que pasan por la ciberseguridad [27].

Comprendiendo el funcionamiento de OSINT, con sus técnicas, procesos y diferentes matices para la aplicación, se espera realizar un aporte tras analizar la página institucional de la Universidad Politécnica Salesiana generando conciencia en sus usuarios.

# 4. Materiales y metodología

La metodología que se utiliza para desarrollar el presente trabajo sigue los pasos ya planteados en el punto anterior. Adicionalmente se siguen las recomendaciones para hacer que la investigación sea lo más anónima posible. Para los procesos siguientes se hará uso de un computador portátil, un módulo de conexión inalámbrica USB y un punto de conexión Wifi público.

## 4.1 Ocultamiento de la huella digital

Para el investigador es imprescindible pasar desapercibido, en este caso se hace una investigación de tipo pasivo, es decir, sin interacción directa con el objetivo. Tanto los equipos, como los procesos serán transparentes con el único fin de no generar una huella digital localizable del investigador.

### 4.1.1 Creación de la máquina virtual

Una máquina virtual brinda los recursos asignados a través del equipo anfitrión, ayudando en el ocultamiento de identificadores de hardware y de software.

Dentro de las principales características que tiene la máquina virtual están:

**Memoria RAM:** 4GB

**Núcleos de procesador:** 4

**Almacenamiento:** 30GB

**Controlador USB:** xHCI

Es importante tener en cuenta el controlador USB, pues se le dará una salida propia al sistema invitado a través de una tarjeta inalámbrica (Wifi) conectada por este medio.

El sistema operativo virtualizado a utilizar es Kali Linux, este contiene herramientas que serán de gran utilidad en el proceso de investigación.

Se usa el programa VirtualBox de Oracle para la virtualización (Fig. 06).

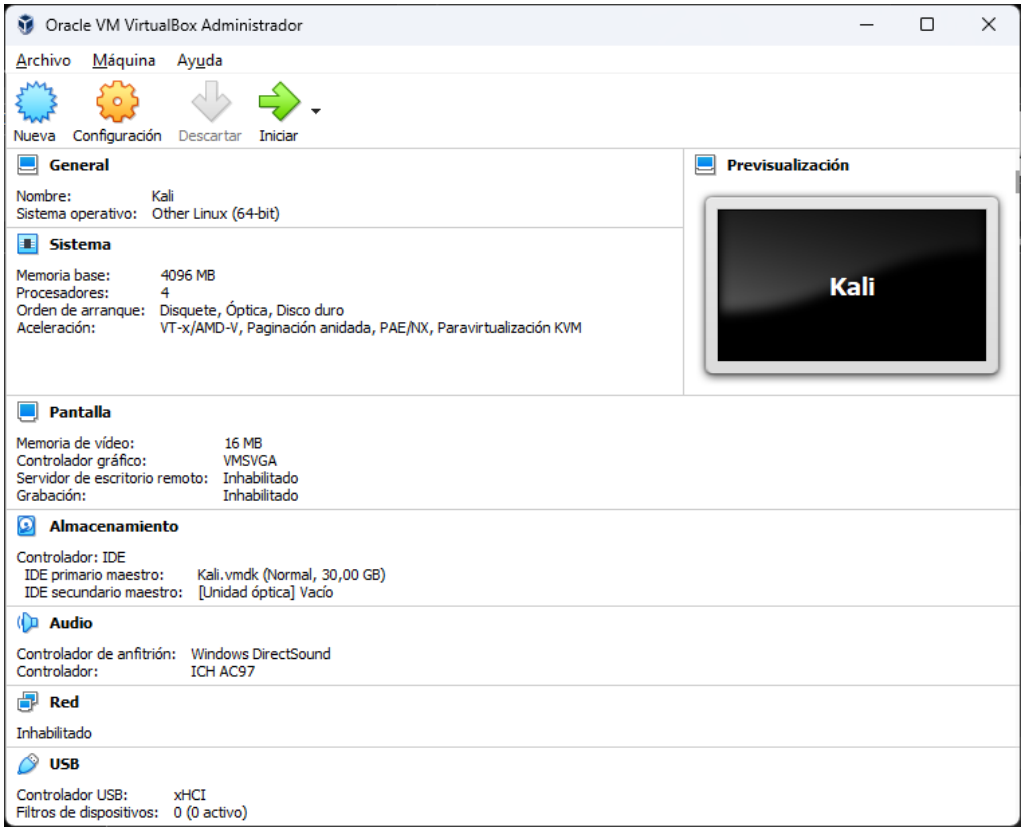


**Fig. 06** Creación de la máquina virtual (**Fuente:** El autor).

### 4.1.2 Ocultamiento de la dirección MAC

La máquina virtual tendrá una salida propia hacia internet con una tarjeta inalámbrica conectada por el puerto USB virtualizado y la dirección mac de este será cambiada para que no quede registro de la mac real en el access point público al que será enlazado.

El adaptador inalámbrico tomará una nueva dirección mac asignada de manera aleatoria (fig. 07), el comando para cambiar la dirección es:

*sudo macchanger -r wlan0*

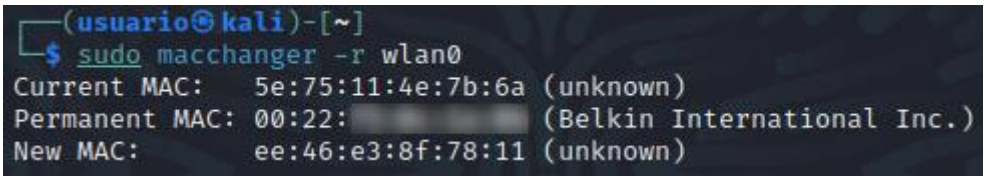


**Fig. 07** Cambio de dirección mac (**Fuente:** El autor).

### 4.1.3 Creación de cuenta de correo alterna

Varias de las herramientas que se usarán, están ligadas a una dirección de correo por lo que se manejarán dos alternativas según sea conveniente. La primera elección es hacer uso de una cuenta de correo de Gmail que no contenga ningún dato que permita la identificación del investigador, la segunda opción es usar correos temporales como los ofrecidos en el siguiente enlace:
https://temp-mail.org/

### 4.1.4 Creación de cuentas en redes sociales

Para mantener el anonimato es crucial no usar cuentas de redes sociales propias, aunque no se interactúe directamente con el objetivo de la investigación, los algoritmos de las redes sociales pueden tomar como referencia la visita del investigador para sugerir el perfil propio como posible conocido o amigo, con esto se revelaría de algún modo la identidad del investigador.
Para el caso de estudio que se trata en el presente trabajo es necesario la creación de perfiles en las redes sociales:

- Instagram
- Facebook
- Linkedin

## 4.2 Planteamiento de los requisitos

Se ha planteado como objetivo generar conciencia en la comunidad universitaria mediante el análisis de los datos públicos que se pueden encontrar en la web, tomando como punto de partida para esta investigación el portal web institucional. Los datos primarios de colaboradores, docentes y alumnos se obtendrán de diferentes modos a través de técnicas OSINT desde el mencionado portal.

## 4.3 Selección de fuentes de información

Para estructurar cada perfil de las personas investigadas, será necesario hacer uso de varias fuentes de información, se citan estas a continuación:

- Portal de la Universidad Politécnica Salesiana, https://www.ups.edu.ec/
- Portal de consultas del Senescyt, https://www.senescyt.gob.ec/web/guest/consultas
- Portal de servicios del SRI, https://srienlinea.sri.gob.ec/sri-en-linea/inicio/NAT
- Portal de servicios del Registro Civil del Ecuador, https://apps.registrocivil.gob.ec/portalCiudadano/index.jsf
- Red social Facebook, https://www.facebook.com/
- Red social Instagram, https://www.instagram.com/
- Red social LinkedIn, https://ec.linkedin.com/

## 4.4 Adquisición

Luego del análisis del portal web de la UPS se han encontrado dos secciones muy interesantes con información que permite la identificación de colaboradores y docentes. Estas secciones, a fecha 07 de noviembre de 2022 se encuentran bajo los siguientes enlaces:

- Directorio de colaboradores, https://www.ups.edu.ec/directorio-de-colaboradores?inicial=A
- Directorio de docentes, https://www.ups.edu.ec/directorio-docente?inicial=A

La información publicada destaca los nombres completos, departamento en el que labora dentro de la institución, educación, asignaturas dictadas (en el caso de los docentes), correo institucional y una fotografía de la persona.

Es importante respaldar la información encontrada para procesarla más adelante.

### 4.4.1 Web Scraping

Dado que ninguna de las herramientas encontradas en internet, es capaz de adquirir ordenadamente los datos hallados; se procede a programar una herramienta propia, valiéndose del lenguaje Python a través de un proceso llamado Web Scraping y con el procesador de texto Mousepad (fig. 08).

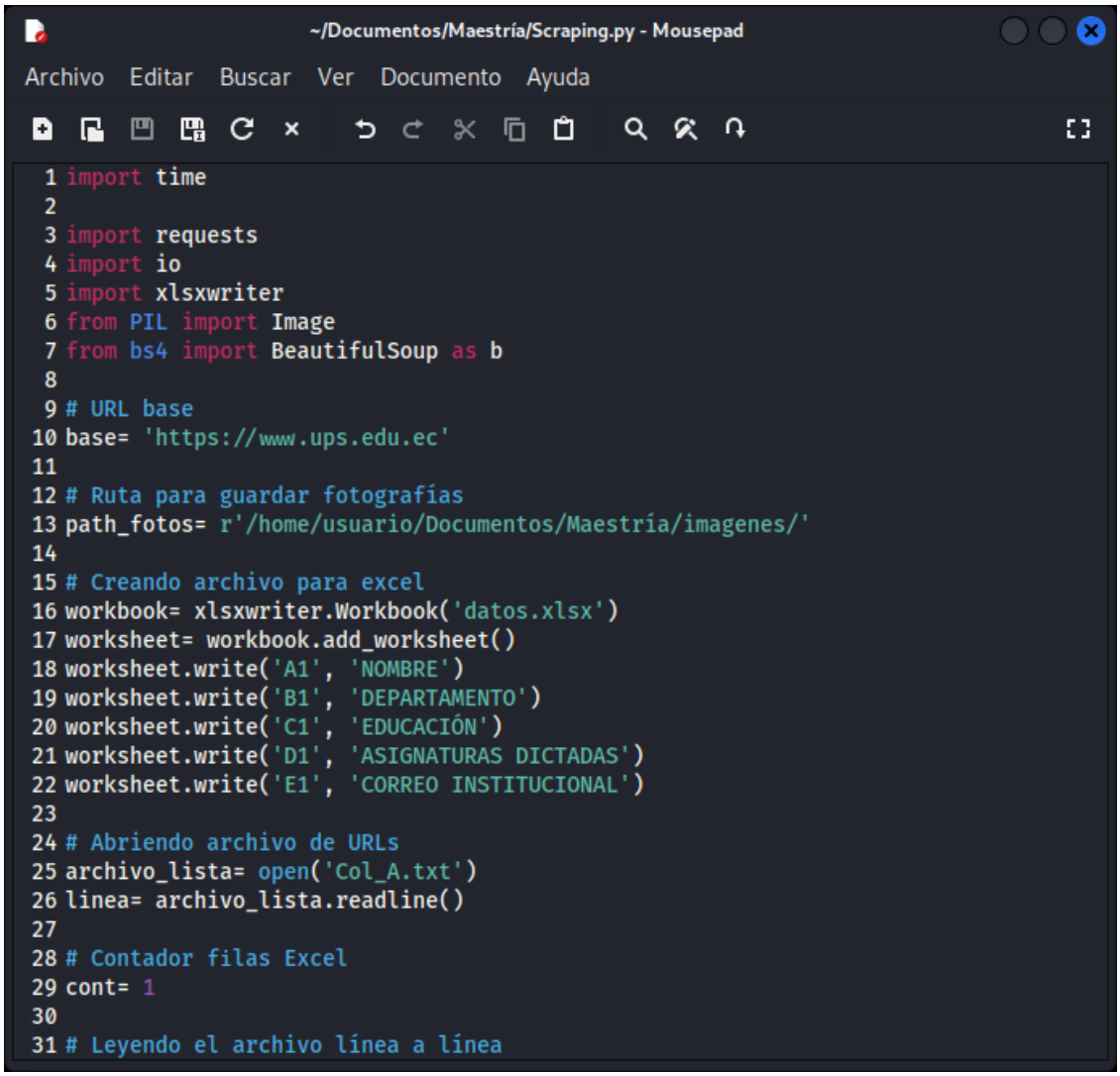


**Fig. 08** Web Scraping en Mousepad (**Fuente:** El autor).

La programación sigue los pasos detallados en la fig. 09. Cada persona listada en los enlaces antes citados tiene asignado una URL propia, se visitará de forma automática cada enlace para la extracción de los datos.

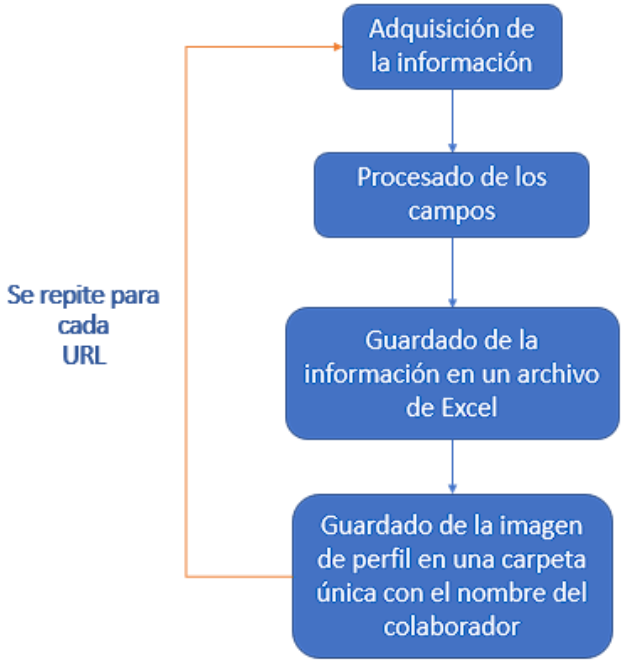


**Fig. 09** Proceso de Web Scraping (**Fuente:** El autor).

Los resultados obtenidos en el documento de Excel (fig. 10) muestran 783 registros para los colaboradores y 972 registros para docentes.

| | NOMBRE | DEPARTAMENTO | EDUCACIÓN | ASIGNATURAS DICTADAS | CORREO INSTITUCIONAL |
|---|---|---|---|---|---|
| 755 | STEFANY FERNA | DIRECCION DE CARRE | INGENIERA ELECTRICA | | s.edu.ec |
| 756 | MARTHA LUCIA Y | DIRECCION TECNICA D | INGENIERO EN SISTEMAS CON MENCION EN TELEMATICA, DIPLOMA SUPERIOR EN G | | s.edu.ec |
| 757 | ANA LUCÍA YANC | SECRETARIA DE CAMI | BACHILLER EN FISICO MATEMATICO | | s.edu.ec |
| 758 | JORGE OSWALD | DIRECCION TECNICA D | LICENCIADO EN PSICOLOGIA DEL TRABAJO, ANALISTA DE RECURSOS HUMANOS, I | | edu.ec |
| 759 | CARMEN ANGEL | DIRECCION DE CARRE | MEDICO VETERINARIO ZOOTECNISTA | | o@ups.edu.ec |
| 760 | EDGAR RODRIG | CENTRO DE CAPACIT | INGENIERO DE SISTEMAS, TECNOLOGO EN GESTION DEL RIESGO Y DEL DESASTRE | | s.edu.ec |
| 761 | PABLO ROBERT | CENTRO DE CAPACITACION EN SISTEMAS INFORMATICOS | | | s.edu.ec |
| 762 | LUIS FERNANDO | LABORATORIO DE SL | BACHILLER EN FISICO MATEMATICO | | s.edu.ec |
| 763 | IRENE ELIZABETH | CENTRO DE INVESTIG | INGENIERA EN BIOTECNOLOGIA DE LOS RECURSOS NATURALES | | edu.ec |
| 764 | MYRIAM ALEXAN | SECRETARIA TECNICA | INGENIERO DE SISTEMAS, MAGISTER EN SISTEMAS DE INFORMACION GERENCIAL | | s.edu.ec |
| 765 | EDWIN RENE YUI | DIRECCION DE CARRE | LICENCIADO EN COMUNICACION SOCIAL, TECNOLOGO FOTOGRAFÍA , I COMUNICA | | s.edu.ec |
| 766 | DIEGO GABRIEL | CENTRO DE CAPACIT | TECNOLOGO EN ANALISIS DE SISTEMAS INFORMATICOS | | ups.edu.ec |
| 767 | AXEL DANIEL ZA | DIRECCION TECNICA D | INFORMATICA | | l@ups.edu.ec |
| 768 | DIOGENES ALEX | DIRECCION TECNICA D | INGENIERO COMERCIAL Y EMPRESARIAL | | @ups.edu.ec |
| 769 | JOSE FERNANDO | DIRECCION TECNICA DE ADMINISTRACION E INVENTARIOS | | | ups.edu.ec |
| 770 | WILLIAN SANTIA | DIRECCION TECNICA D | LICENCIADO EN COMUNICACION SOCIAL | | ups.edu.ec |
| 771 | SAMUEL VITERV | DIRECCION TECNICA D | NINGUNA | | ups.edu.ec |
| 772 | ERIKA PRISCILA | SECRETARIA DE CAMI | INGENIERA EN CONTABILIDAD Y AUDITORIA, MAGISTER EN CONTABILIDAD Y AUDIT | | s.edu.ec |
| 773 | JAVIER PATRICIO | SECRETARIA TECNICA | LICENCIADO EN DESARROLLO SOCIAL, INGENIERO QUIMICO | | ps.edu.ec |
| 774 | ANGELICA VALE | DIRECCION TECNICA D | FISICO MATEMATICO | | s.edu.ec |
| 775 | ADRIANA ESTEF | DIRECCION TECNICA D | INGENIERA ELECTRICA | | s.edu.ec |
| 776 | DIEGO PATRICIO | DIRECCION DE CARRE | INGENIERO ELECTRONICO | | s.edu.ec |
| 777 | LUIS IVAN ZAPA | DIRECCION TECNICA D | NINGUNA | | s.edu.ec |
| 778 | DIEGO ANDRES | DIRECCION TECNICA DE ECOSISTEMA DE EMPRENDIMIENTO E INNOVACION | | | ps.edu.ec |
| 779 | VERONICA ALEX | SECRETARIA TECNICA | INGENIERA INDUSTRIAL, MAGISTER EN INGENIERIA INDUSTRIAL | | s.edu.ec |
| 780 | DIEGO FABRICIO | DIRECCION DE CARRERA FILOSOFIA | | | s.edu.ec |
| 781 | MARGOTH SOFI | DIRECCION TECNICA D | BACHILLER EN SECRETARIADO BILINGUE COMERCIO Y ADMINISTRACION | | @ups.edu.ec |
| 782 | NELSON DAVID | DIRECCION TECNICA D | INGENIERO EN ADMINISTRACION DE EMPRESAS, BACHILLER, MASTER UNIVERSITAR | | @ups.edu.ec |
| 783 | JESSICA ALEXAI | VICERRECTORADO AI | INGENIERA DE SISTEMAS, BACHILLER EN CIENCIAS , DIPLOMA SUPERIOR EN AUDIT | | .edu.ec |
| 784 | DIANA ESTEFANI | DIRECCION TECNICA D | INGENIERA EN COMPUTACION E INFORMATICA, TECNOLOGA EN COMPUTACION E IN | | .edu.ec |

**Fig. 10** Archivo de registro colaboradores (**Fuente:** El autor).

De igual forma se han conseguido 1755 fotografías relacionadas a los registros anteriores, cabe destacar que no todas las personas tienen una fotografía real registrada, en cuyo caso la fotografía asociada al perfil, ha sido reemplazada por un avatar.

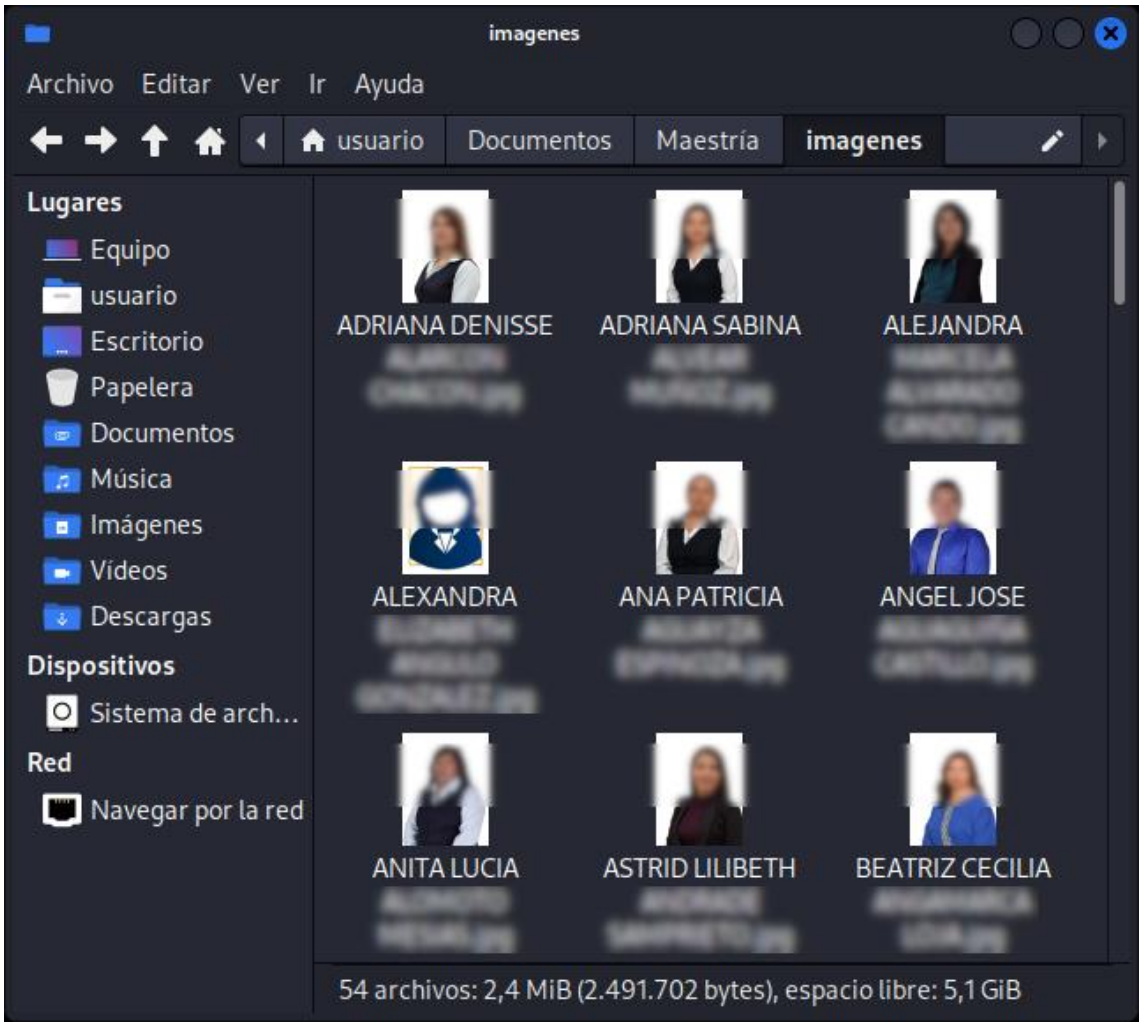


**Fig. 10** Registro fotográfico de colaboradores con apellido de inicial "a" (**Fuente:** El autor).

Este proceso únicamente representa uno de los métodos a través del cual se han conseguido los datos primarios para la elaboración de un perfil más complejo.

### 4.4.2 Sistema de recuperación de contraseñas

Al momento de plantear una investigación, siempre se ha de partir de un dato principal como puede ser: conocer el nombre, tener una fotografía, conocer su Nick de redes sociales, conocer el correo, conocer su dirección de domicilio, entre otros.

Para el siguiente caso se recupera la fotografía que aparece en la noticia del 18 de julio de 2022 (fig. 11) en la sección de noticias del portal institucional.


**Fig. 11** Noticia del portal institucional (**Fuente:** El autor).

En la fotografía se puede ver a una estudiante que exhibe su título obtenido, el nombre en el título es completamente legible; este se tomará como dato primario.

Consultando por los apellidos en la página del Senescyt, se consigue su número de cédula, así como los datos correspondientes de su título profesional (fig. 12).

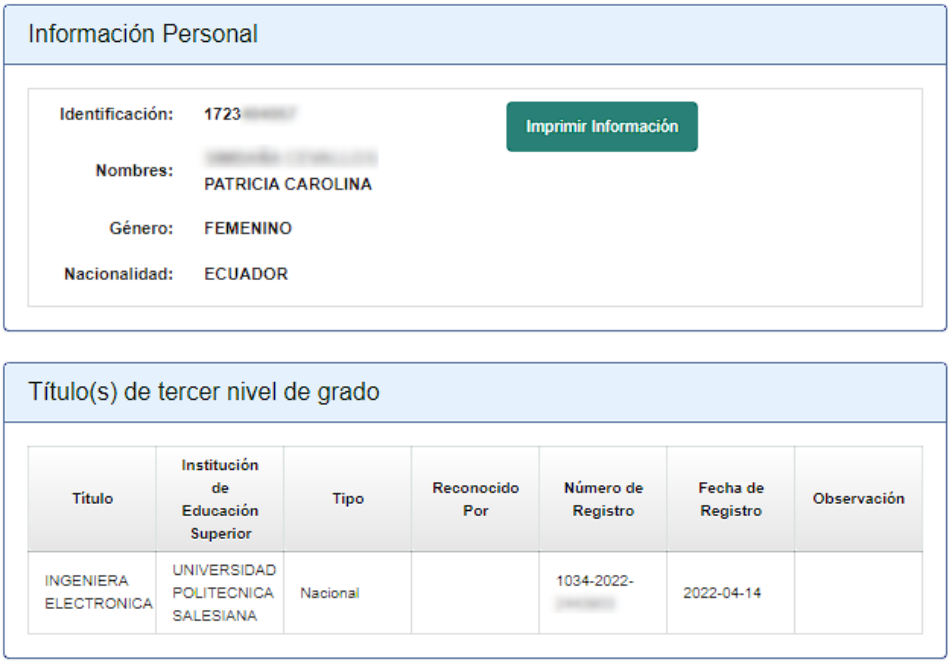


**Fig. 12** Datos encontrados en el portal del Senescyt (**Fuente:** El autor).

Esta información es útil para el siguiente paso en la investigación. De regreso al portal de la UPS, se ubicará la sección de "recordar usuario" en donde el campo requerido es el número de cédula del estudiante o colaborador, dato que ya se consiguió. Ingresado el número de cédula el sistema expone los correos institucionales y personales sin ningún tipo de cuidado (fig. 13).


**Fig. 13** Correo personal filtrado (**Fuente:** El autor).

Obteniendo el correo personal se puede ligarlo a cuentas de redes sociales y demás servicios en los que la persona haya registrado el e-mail encontrado.

### 4.4.3 Sistema de inscripción en línea

Otro de los servicios existentes en el portal web que exponen información personal es el servicio de inscripción en línea. El dato primario para este caso será el número de cédula de la persona a investigar. Mediante ingeniería social se ha obtenido un número de cédula de un estudiante activo, mismo que usaremos para probar el servicio como se indica en la figura 14.

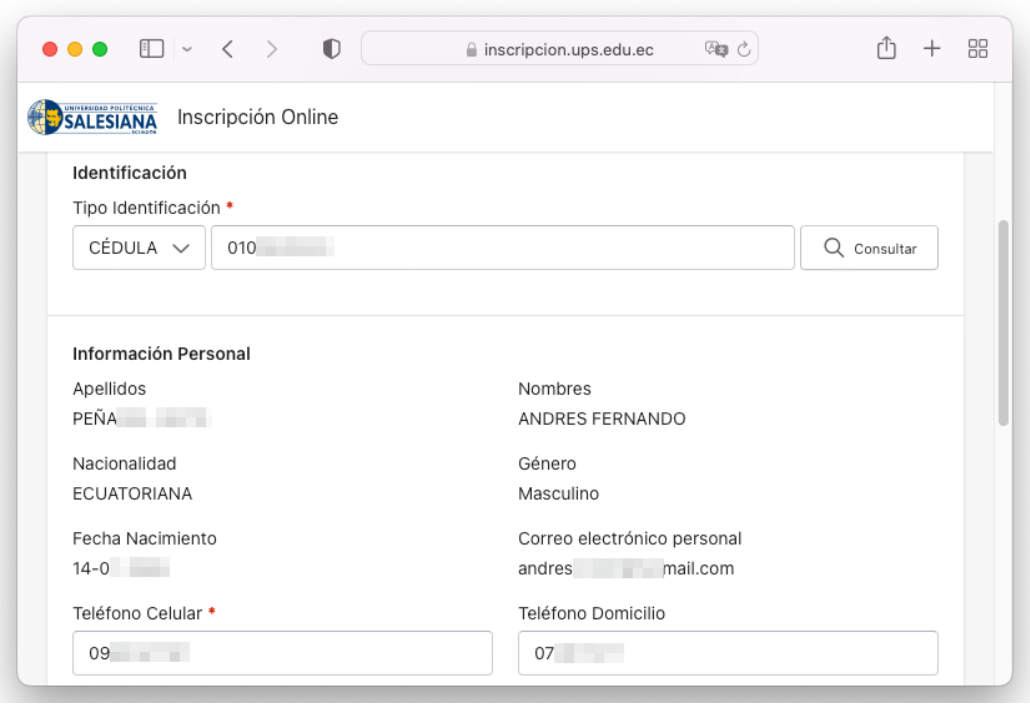


**Fig. 14** Datos expuestos del número de cédula consultado (**Fuente:** El autor).

En la misma página se pueden encontrar datos referentes a la residencia del estudiante (fig. 15).

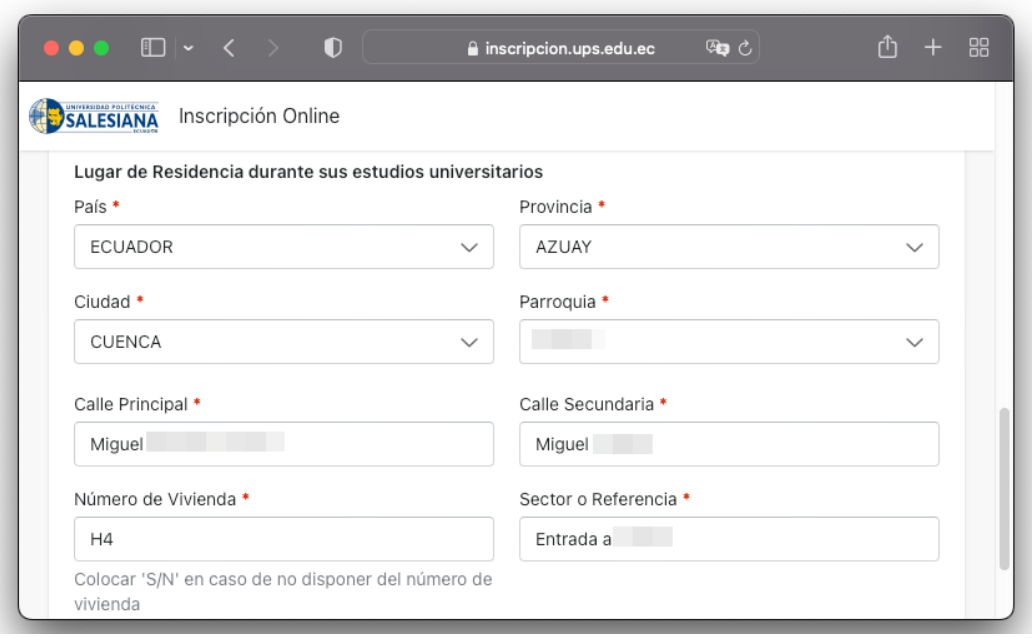


**Fig. 15** Datos de residencia (**Fuente:** El autor).

Los diferentes métodos utilizados en el análisis que se ha llevado a cabo en la página web institucional dejan en evidencia que los datos personales tanto de estudiantes, como de colaboradores se encuentran expuestos. Los datos que se pueden considerar de mayor sensibilidad son los relacionados con sus números de teléfono personales y la dirección de domicilio puesto que permiten un contacto directo con la persona vinculada a la institución educativa.

### 4.4.4 Creación de perfiles

La creación de cada perfil se obtiene a partir de varias fuentes. Todos los casos antes descritos pueden ser utilizados para encontrar datos primarios. Se analizan treinta perfiles de personas relacionadas con la institución, se empieza listando un apartado dedicado a quince colaboradores de la Universidad Politécnica Salesiana (fig. 16). El dato primario de este caso se obtuvo de la recopilación anterior realizada a través de web scraping.

| | Cédula | Apellidos | Nombres | Nacionalidad | Género | Correo Personal | Correo Institucional |
|---|---|---|---|---|---|---|---|
| C | 093 | NICC | MELANY | ECUATORIANA | Femenino | m ail.com | m @ups.edu.ec |
| O | 010 | VIVA | MAGNO | ECUATORIANA | Masculino | m ail.com | m s.edu.ec |
| L | 172 | GUA | JESSICA | ECUATORIANA | Femenino | je tmail.com | jg ups.edu.ec |
| A | 010 | LADI | WILLIAN | COLOMBIANO | Masculino | di l.com | wl ps.edu.ec |
| B | 171 | NAR | CRISTIN | ECUATORIANA | Femenino | sa ail.com | cn ps.edu.ec |
| O | 092 | MER | LUIGGI A | ECUATORIANA | Masculino | al an@yahoo.es | lm ups.edu.ec |
| R | 171 | SUA | FANNY E | ECUATORIANA | Femenino | fa 6@gmail.com | fs ps.edu.ec |
| A | 010 | PINC | EDUARD | ECUATORIANA | Masculino | ec gmail.com | ep s.edu.ec |
| D | 091 | PERE | RAFAEL | ECUATORIANA | Masculino | af nez@gmail.com | rp os.edu.ec |
| O | 110 | QUE | FERNAN | ECUATORIANA | Femenino | m mail.com | fq ups.edu.ec |
| R | 091 | LUCA | CARLOS | ECUATORIANA | Masculino | ca nail.com | cl .edu.ec |
| E | 010 | PERA | KARLA V | ECUATORIANA | Femenino | ka 3@hotmail.com | kp ps.edu.ec |
| S | 092 | GAR | SHEYLA | ECUATORIANA | Femenino | sh ail.com | sg s.edu.ec |
| | 171 | RAM | XIMENA | ECUATORIANA | Femenino | xi hotmail.com | xr ps.edu.ec |
| | 010 | ARC | MIGUEL | ECUATORIANA | Masculino | m yahoo.es | m s.edu.ec |

**Fig. 16** Perfiles de colaboradores (**Fuente:** El autor).

El dato de correo personal se usará para vincular a cada persona a perfiles de redes sociales.

De igual modo se ha elaborado un perfil de quince estudiantes de distintas carreras y ciudades (fig. 17). Las fuentes primarias de información fueron: redes sociales, Google Hacking, noticias del portal institucional, ingeniería social.

| | Cédula | Apellidos | Nombres | Nacionalidad | Género | Correo Personal | Correo Institucional |
|---|---|---|---|---|---|---|---|
| | 010 | PEÑA | ANDF | ECUATORIANA | Masculino | a ail.com | a est.ups.edu.ec |
| | 010 | FARF | DAVI | ECUATORIANA | Masculino | f .com | d .ups.edu.ec |
| E | 140 | LOPE | IRINA | ECUATORIANA | Femenino | l l.com | il ups.edu.ec |
| S | 172 | YEPEZ | MART | ECUATORIANA | Femenino | m mail.com | m st.ups.edu.ec |
| T | 015 | VENE | SHEYI | ECUATORIANA | Femenino | sl gmail.com | s est.ups.edu.ec |
| U | 172 | OCAÑ | JENN | ECUATORIANA | Femenino | je mail.com | jc ups.edu.ec |
| D | 172 | REVE | PABL | ECUATORIANA | Masculino | p il.es | p t.ups.edu.ec |
| I | 172 | ZULC | MARI | ECUATORIANA | Femenino | b @hotmail.com | m .ups.edu.ec |
| A | 080 | SANT | JOSE | ECUATORIANA | Masculino | s gmail.com | js st.ups.edu.ec |
| N | 172 | FREIR | ANAH | ECUATORIANA | Femenino | a nail.com | a t.ups.edu.ec |
| T | 095 | BRIO | DIAN | ECUATORIANA | Femenino | d gmail.com | d est.ups.edu.ec |
| E | 125 | BAJA | LUIS A | ECUATORIANA | Masculino | l .com | lb t.ups.edu.ec |
| S | 093 | OCAÑ | DANI | ECUATORIANA | Femenino | d @hotmail.com | d .ups.edu.ec |
| | 175 | ZURIT | BRYA | ECUATORIANA | Masculino | b mail.com | b t.ups.edu.ec |
| | 095 | BRUN | ANGI | ECUATORIANA | Femenino | a ail.com | al .ups.edu.ec |

**Fig. 17** Perfiles de estudiantes (**Fuente:** El autor).

Dentro de los perfiles constan datos de teléfonos fijos y móviles. Un dato muy importante es el referente a su dirección domiciliaria, datos que también se han conseguido y registrado como se indica en la figura 18.

| | RESIDENCIA | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | País | Provincia | Ciudad | Parroquia | Calle Principal | Calle Secundaria | # de vivienda | Referencia |
| COLABORADORES | ECUADOR | GUAYAS | GUAYAQUIL | FEB | 37 | LA | | |
| | ECUADOR | AZUAY | CUENCA | SAY | Car | De | S/ | Ur |
| | ECUADOR | PICHINCHA | QUITO | CHI | Ant | Co | D | |
| | ECUADOR | AZUAY | CUENCA | RIC | Sec | Se | | |
| | ECUADOR | PICHINCHA | QUITO | SAI | Gua | Bu | O | |
| | ECUADOR | GUAYAS | DURAN | ELC | Gua | Gu | 1 | N |
| | ECUADOR | PICHINCHA | QUITO | | Luc | | 7 | |
| | ECUADOR | AZUAY | CUENCA | | Chi | Ríc | | |
| | ECUADOR | GUAYAS | DAULE | ENI | Vill | | | |
| | ECUADOR | PICHINCHA | QUITO | LA I | San | Itu | S/ | A |
| | ECUADOR | GUAYAS | GUAYAQUIL | GAI | Av. | Fra | N | |
| | ECUADOR | AZUAY | CUENCA | CAÍ | Jorg | Pa | S/ | Pi |
| | ECUADOR | GUAYAS | GUAYAQUIL | SAI | Km | | S/ | Cc |
| | ECUADOR | PICHINCHA | QUITO | CHI | Chi | Isic | S | Ba |
| | ECUADOR | AZUAY | CUENCA | MC | Cuz | 24 | N | |
| ESTUDIANTES | ECUADOR | AZUAY | CUENCA | SID | Mig | Mi | H | En |
| | ECUADOR | AZUAY | CUENCA | SAI | Call | Au | 3 | M |
| | ECUADOR | AZUAY | CUENCA | SID | Call | El C | 3- | Ba |
| | ECUADOR | AZUAY | CUENCA | | El T | La I | 1 | Ur |
| | ECUADOR | AZUAY | CUENCA | YAI | Av. | Ga | 1- | Se |
| | ECUADOR | PICHINCHA | QUITO | CHI | Jose | Jos | O | |
| | ECUADOR | PICHINCHA | QUITO | CEN | Ver | Ma | N | Ce |
| | ECUADOR | PICHINCHA | QUITO | CUI | Juai | Joa | S( | Fa |
| | ECUADOR | PICHINCHA | QUITO | CHI | Av. | Av. | S: | Ch |
| | ECUADOR | PICHINCHA | QUITO | ITC | Mar | Tor | E: | La |
| | ECUADOR | GUAYAS | GUAYAQUIL | PAS | Muc | Mu | M | Ba |
| | ECUADOR | GUAYAS | GUAYAQUIL | | Flor | Flo | 1( | Su |
| | ECUADOR | GUAYAS | GUAYAQUIL | TAF | Aut | Av. | M | Pa |
| | ECUADOR | GUAYAS | GUAYAQUIL | XIM | Pra | Pra | V | |
| | ECUADOR | GUAYAS | GUAYAQUIL | FEB | 48 y | Sul | | Úl |

**Fig. 18** Lugares de residencia (**Fuente:** El autor).

Los datos presentados pueden ser muy específicos en algunos de los casos, de tal modo que, haciendo uso de Google Maps se ha podido localizar una de las viviendas que se encuentran en el listado de los perfiles que se han elaborado (fig. 19).


**Fig. 19** Dirección ubicada de modo virtual (**Fuente:** Google Maps).

## 4.4.5 Consulta de datos de Instagram

"Facebook & Instagram OSINT" es una extensión para "Mozilla Firefox" que permite visualizar el ID, dirección de correo electrónico y número de teléfono de cualquier usuario, estos últimos dos datos aparecen ofuscados. Esta extensión es de gran utilidad al momento de corroborar información. Habiendo encontrado un perfil de Instagram, ya sea a través de Google Hacking o directamente desde el buscador del propio Instagram, es posible comparar los datos que se encontraron mediante técnicas OSINT, con los datos que entrega la extensión. Como se muestra en la figura 20, el servidor de correo y los dos últimos dígitos del número de teléfono celular, han coincidido. Esto sumado al registro fotográfico que se mantiene, brinda una alta probabilidad de haber encontrado el perfil correcto.


**Fig. 20** Uso de la extensión "Facebook & Instagram OSINT" (**Fuente:** El autor).

## 4.4.6 Consulta de datos de FACEBOOK

La tarea de comparar dos imágenes se puede complicar cuando se tienen fotografías de diferentes años, se hace uso de maquillaje, distintos peinados, uso de accesorios, etc. Para facilitar el proceso de comparación se puede hacer uso de herramientas que se basan en inteligencia artificial, esto provee comparaciones más precisas que las que haría una persona a simple vista. "**A**mazon **W**eb **S**ervices"

cuenta con una herramienta llamada “Amazon Rekognition” que, entre una de sus múltiples funciones destaca la comparación de dos fotografías a fin de determinar la similitud de los rostros encontrados en estas. A manera de ejemplo se usará una de las fotografías que se pueden conseguir en el portal institucional de la UPS, sección de colaboradores (denominado en la herramienta como “Reference face”) y se la intentará ligar a un perfil de Facebook comparándola con la fotografía de perfil (denominado en la herramienta como “Comparison faces”). La figura 21 evidencia un 99.5% de similitud en la comparación de los rostros de las imágenes, con un porcentaje tan elevado en el resultado, se determina que se trata del perfil correcto.

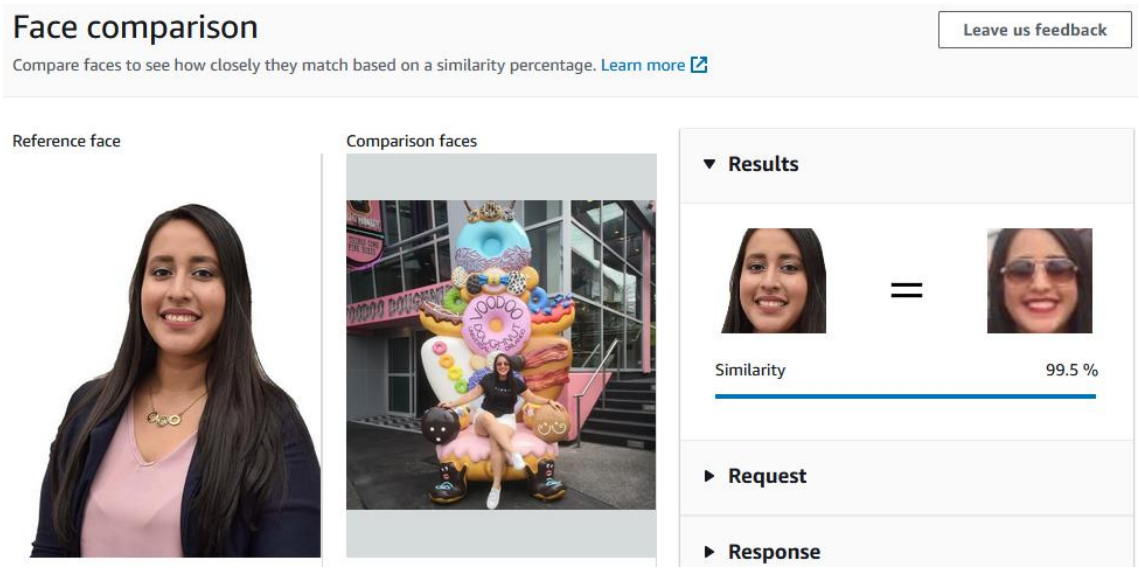


**Fig. 21** Comparación de imágenes (**Fuente:** El autor).

## 4.5 Procesamiento

Con el fin de demostrar las diferentes perspectivas de riesgo que pueden tener los datos recolectados, se hace un procesamiento categorizado por: colaboradores, docentes y perfiles generados.

Para los colaboradores se tomará como dato referencial el departamento al que están vinculados. Para este ejemplo de estudio se toman como referencia los diez departamentos con más colaboradores (fig. 22).

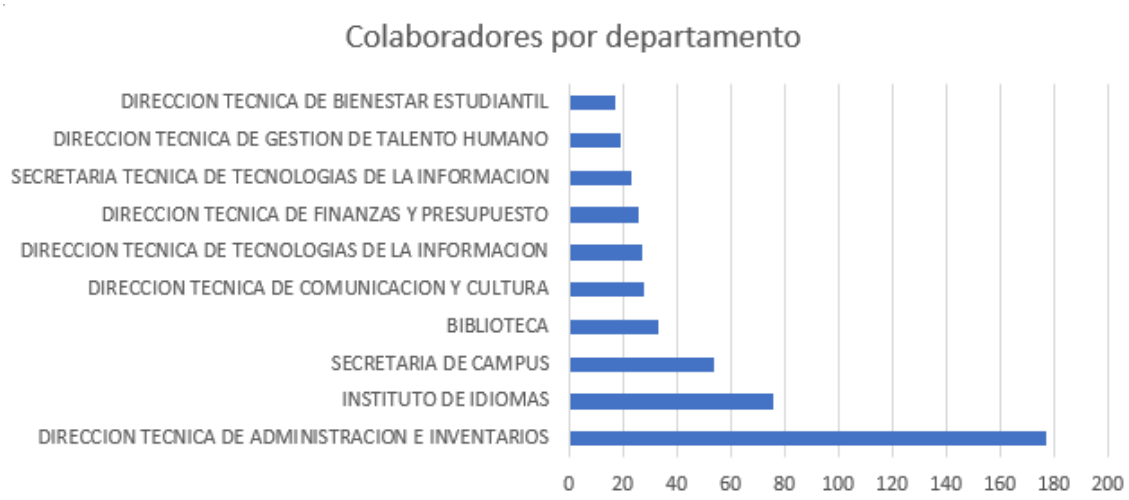


**Fig. 22** Listado de colaboradores por departamento (**Fuente:** El autor).

En el caso de los docentes, se ha identificado la cantidad de profesores vinculados a una misma carrera (10 carreras con más docentes) (fig. 23). Se debe tener en cuenta que los datos presentados corresponden a la totalidad de docentes a nivel nacional y se han clasificado según los datos expuestos en la página institucional.

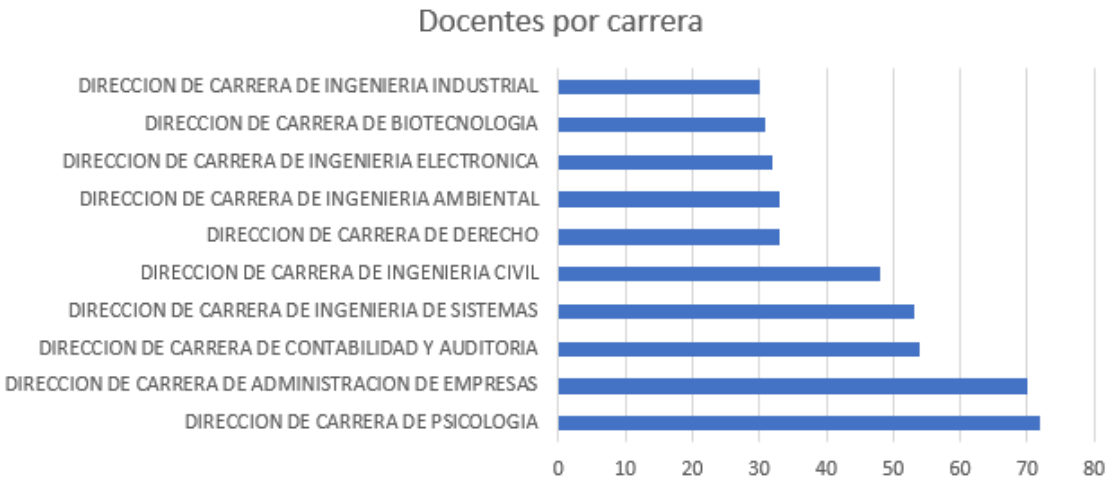


**Fig. 23** Listado de docentes por carrera (**Fuente:** El autor).

En lo que corresponde a perfiles generados, se creó una base de datos de treinta personas (15 colaboradores, 15 estudiantes) que incluye información de diferentes fuentes. En este caso se procesan la cantidad de datos personales que se pudieron obtener (fig. 24).

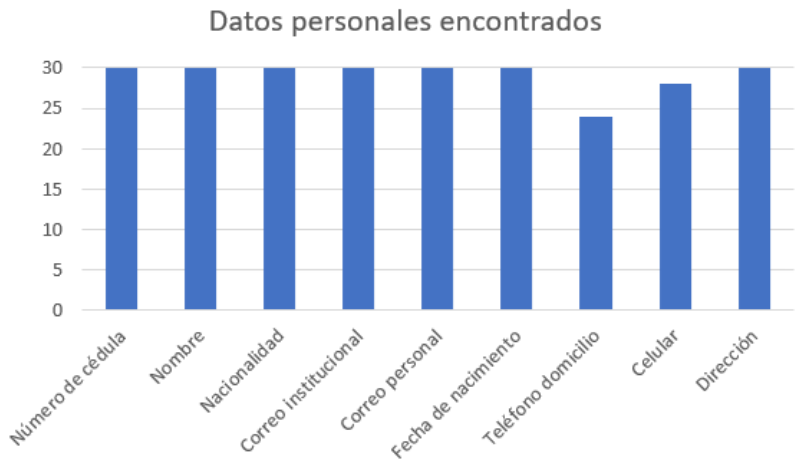


**Fig. 24** Cantidad de datos obtenidos por categoría (**Fuente:** El autor).

Con los datos obtenidos se procedió a buscar los perfiles personales de las redes sociales más usadas en la actualidad. El resultado de la investigación (fig. 25), evidencia diecinueve perfiles encontrados en la red social Facebook, esto corresponde a un 63% de resultados positivos con referencia a la base de datos que se usó para la búsqueda.

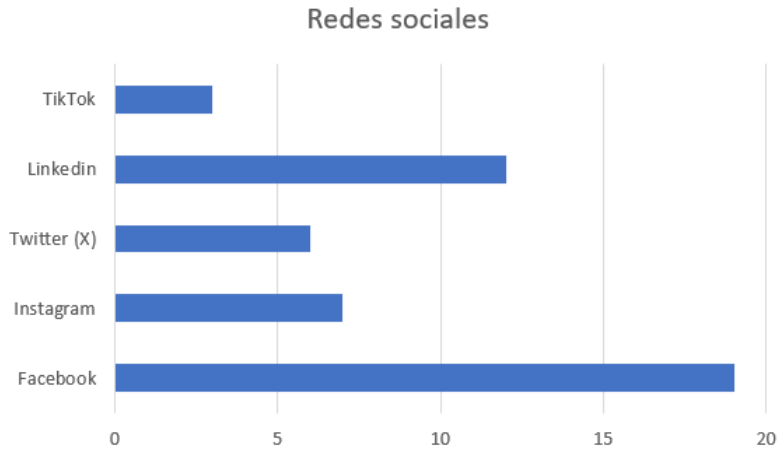


**Fig. 25** Perfiles de redes sociales encontrados (**Fuente:** El autor).

Para las búsquedas se tuvieron diferentes datos de partida. Los resultados correspondientes a las fotografías nos indican un 100% de fotos encontradas de colaboradores y un 87% de fotos localizadas de estudiantes (fig. 26).

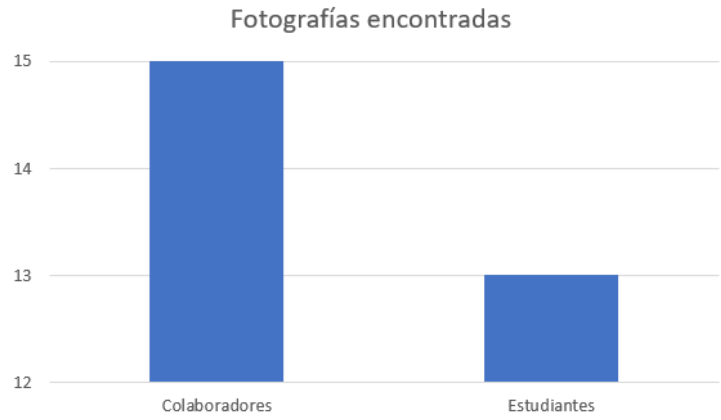


**Fig. 26** Fotografías encontradas de perfiles generados (**Fuente:** El autor).

Tomando como dato de análisis una persona de los perfiles que se generaron en base a la investigación, a quien para efectos prácticos se llamará “Alice”; se tiene que en la red social Facebook se pudieron establecer varios enlaces.

Para el análisis se considera a las personas como nodos y a la interacción que ocurre entre las personas se la llama enlace, pudiendo esta última variar en intensidad en función de la interacción que se da entre los nodos. En la figura 27 se muestran los resultados de la interacción ocurrida entre “Alice” y los cinco principales nodos que han interactuado con esta.

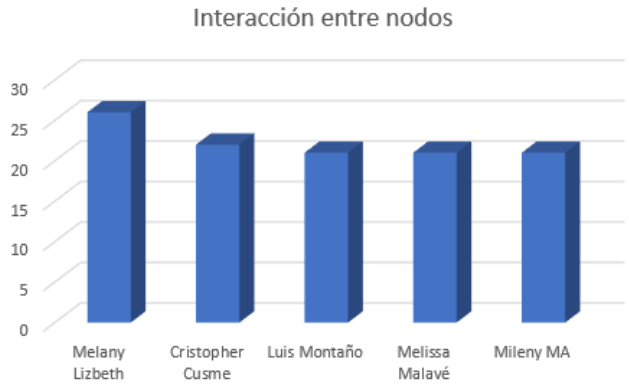


**Fig. 27** Interacción entre nodos (**Fuente:** El autor).

El método para determinar la interacción principal ha sido contando el número total de “Me gusta” en las publicaciones hechas por “Alice” en la red social Facebook, esto en el año 2022 y los meses transcurridos hasta septiembre del año 2023.

Para establecer la intensidad del enlace se debe considerar el lado opuesto, es decir, la interacción de “Alice” con la contraparte.

En una escala de 10, se establece un puntaje de 8.3 de interacción de “Melany Lizbeth” para “Alice”. En la misma escala se tiene una interacción de 7.7 de interacción de “Alice” con “Melany Lizbeth”. En promedio el enlace se establece con una intensidad de 8.

En el siguiente caso teniendo como protagonista al usuario “Cristopher Cusme”, se ha dado una interacción de 7.3 con “Alice”. En el caso inverso, no se ha encontrado interacción de “Alice” con “Cristopher Cusme” por lo que la interacción toma un valor de 0. La intensidad de la interacción para este caso es de 3.65.

## 4.6 Análisis

Con una base de 783 registros de colaboradores (datos a nivel nacional), se pudo determinar que en el departamento de la Dirección Técnica de Administración e Inventarios es donde se encuentra la mayor cantidad de personal (177 personas). Dato que por ejemplo resultaría útil en el caso de querer establecer lazos comerciales como proveedor de la institución.

Por parte de los docentes se obtuvieron 972 registros. Se pudo verificar que la carrera de Psicología tiene vinculados 72 docentes, siendo la carrera que sobresale ante las demás en cuestión de cantidad. Este dato sería de utilidad por ejemplo para ofrecer cursos de capacitación al personal docente, conociendo ya que temas son los mejores para su oferta en base a la carrera.

En estos dos casos la información que se tiene se puede usar con fines publicitarios, ya sea para uso propio o para la venta de la información a empresas de marketing.

Esta información es particularmente deseable al tener un medio de contacto directo entre los datos (correo institucional). Incluso se puede complementar la información base para enfocar la publicidad por rango de edad y género.

Los datos personales obtenidos en la página institucional son muy relevantes si se quisiera localizar a la persona. La búsqueda del número telefónico fijo tuvo una efectividad del 80%, seguido del número celular con una efectividad del 93%; para el resto de los datos la efectividad ha sido de un 100% según se indica en la figura 24. Se ha de tener en cuenta que el teléfono fijo ha caído en desuso y puesto que no es un dispositivo portable, se suele omitir el registro cuando los estudiantes han dejado su lugar de origen y han viajado solo para capacitarse en sus respectivas carreras.

Viendo los resultados obtenidos de redes sociales (fig. 25), se debe tener en cuenta que la variación de la cantidad de perfiles encontrados varía en función del público al que se dirige, la edad, la popularidad, etc. Un dato no menos importante a la hora de ubicar un perfil de red social es la técnica OSINT que se puede aplicar a dicha red social, e incluso entran en juego el perfil de privacidad aplicado por cada persona.

Las imágenes son un dato muy importante dentro de la investigación, pues ayudan a vincular el perfil investigado con la persona en la vida real e incluso es un medio de comparación que ayuda en la verificación de la información que se puede encontrar en otras fuentes. Como es sabido, en la página institucional se encuentran expuestos bajo el “directorio de colaboradores” los principales datos del personal de la UPS incluida una fotografía de perfil. En el caso de los estudiantes la cifra de éxito alcanzada ha sido resultado de encontrar fotografías en perfiles de redes sociales y la fotografía de contacto usada en la aplicación de mensajería WhatsApp.

Cuando se establecen valores de intensidad en la interacción de dos personas a través de redes sociales, se debe tener en cuenta que las intensidades que están por debajo de 5 en una escala de 10, evidencia que el vínculo afectivo es débil.

En el caso antes mostrado entre “Cristopher Cusme” y “Alice” se puede ver que a pesar de que “Cristopher Cusme” interactúa continuamente, “Alice” no lo hace.

En el caso opuesto, con un valor de 8 en la intensidad de enlace generada entre “Alice” y “Melany Lizbeth”, se tiene como resultado un valor afectivo fuerte.

Este tipo de información puede ser usado en las investigaciones para establecer parentescos y relaciones afectivas de amigos o parejas sentimentales.

## 4.7 Inteligencia

El resultado de las diferentes perspectivas analizadas evidencia lo expuestos que se encuentran todos los miembros de la comunidad universitaria. Aunque el fin comercial podría ser el más leve de los propósitos de la recolección de los datos, se puede llegar a casos de acoso de cualquier índole al exponer datos de ubicación.

La información obtenida se puede discriminar a conveniencia y en este caso es el investigador quien puede crear perfiles comerciales aún más complejos que pueden resultar ser muy invasivos en términos de la privacidad que debería tener cada participante de la comunidad universitaria.

Facebook, por la naturaleza misma de su contenido sigue siendo la red social que mayores datos permite recolectar. Tomando como referencia las redes sociales analizadas, es la red social que mayor cantidad de técnicas OSINT permitió aplicar, esto sin exponer la investigación realizada o a su investigador.

Hay que destacar que la privacidad de datos es algo que va tomando relevancia en las redes sociales y dentro de la investigación se han podido encontrar medidas de protección que pueden aplicar los usuarios para evitar el robo de información e incluso la pérdida de sus cuentas. Específicamente dos de los treinta usuarios investigados en la red social Facebook, tienen sus cuentas ligadas a dispositivos autorizados, es decir, no se permite iniciar sesión en cualquier dispositivo. Por ende, una investigación con dispositivos autorizados es más compleja.

## 4.8 Análisis de la política de uso de datos personales

La Universidad Politécnica Salesiana, actualmente ofrece su política de tratamiento y uso de datos personales en el siguiente enlace:

https://portal.ups.edu.ec/politica-tratamiento-uso-datos

La política vigente se ha socializado en mayo de 2023. Esta reforma se adapta conforme lo estipula la Ley Orgánica de Protección de Datos Personales, aprobada en 2021.

Dentro de la página web personal (de colaboradores y estudiantes), se presenta un aplicativo que proporciona la aceptación digital de la política expuesta y se registra la fecha y hora de aceptación. Del mismo modo, se permite enviar una solicitud de revocatoria del contrato aceptado y se facilita el correo usodedatos@ups.edu.ec en el caso de requerirse algún tipo de modificación.

Considerando la nueva Ley de Protección de Datos Personales; se ha hecho una variación en lo que se considera un dato personal. Se cita textual:

“Dato personal: Dato que identifica o hace identificable a una persona natural, directa o indirectamente.”

Por lo tanto, han pasado a ser datos personales que hacen identificable a una persona (en combinación con otra información), datos como: dirección domiciliaria, placas de un vehículo, coordenadas GPS que se podrían encontrar en una fotografía digital, entre otros.

Tomando como base el apartado “DEBERES DE LA UNIVERSIDAD COMO RESPONSABLE DEL TRATAMIENTO DE DATOS PERSONALES”; se estipulan una serie de medidas que se comprometen a salvaguardar la información personal de la comunidad universitaria.

Aunque en este caso no se está revelando ninguna información de carácter confidencial, hay datos que pueden atentar contra la privacidad de un individuo en especial si se tiene en cuenta la actual situación de inseguridad que atraviesa el país.

Se listan los datos sensibles encontrados que permiten entrar en contacto directo con la persona:

- Dirección de correo electrónico personal e institucional
- Números telefónicos (fijo y celular)
- Dirección de domicilio

Se resalta la característica que permite la revocatoria de la autorización concedida a la institución, pues esta es una opción que el usuario debe considerar en el caso de no estar de acuerdo con el tratamiento que se le están dando a sus datos.

Por otro lado, la política de la UPS establece que se tomaran las acciones necesarias para mitigar los riesgos que se hayan detectado producto de las vulnerabilidades encontradas a través de cualquier medida de evaluación. Este punto es favorable si se llega a considerar que los datos expuestos representan un riesgo para estudiantes y colaboradores.

# 5. Resultados y discusión

La privacidad es algo que ha pasado a ser fundamental en cualquier red social que tenga algo de difusión, y los responsables de cada organización prestan mucha atención a esta característica. Para todos los usuarios que no quieran ser víctimas de algún tipo de estafa o ataque, es imperativo tomarse el tiempo para entender y actualizar sus opciones de privacidad en cada una de sus cuentas de redes sociales.

Asimismo, hay que elevar el nivel de conciencia frente a una sociedad que cada día se vuelve más violenta. Ser selectivo con el contenido y público que se comparte en la web, es un buen arranque para limitar el alcance que puede tener una persona cuando ha escogido una víctima en la red para investigarla. Próximos viajes por realizar, fechas especiales, lugares en los que se encuentra ubicado en todo momento, parentescos, fotografías de hijos menores de edad; son algunos ejemplos de información que no se debería de compartir en un perfil público.

Como ya se había mencionado, las imágenes hoy en día constituyen una valiosa información dentro de una investigación. Limitar el acceso a la fotografía de perfil en cualquier aplicación de mensajería, para que se muestre solo a los propios contactos, es una buena práctica que favorece a la privacidad.

En la página institucional de la Universidad Politécnica Salesiana, se ha evidenciado que hace falta cuidar más los datos al momento de:

- Publicar una noticia
- Generar un proceso de inscripción en línea
- Restablecer una contraseña

La información que se puede recoger de los citados procesos deja vulnerables tanto a estudiantes como colaboradores en general.

La evolución tecnología que se ha tenido en herramientas de tratamiento de imágenes es algo para tener en cuenta. Aunque su uso puede contribuir en varios aspectos al desarrollo de la sociedad, hay que notar el riesgo que puede darse al ser víctima de una suplantación de identidad o cualquier otro tipo de alteración que de pie a un fraude. Cuidar de la imagen propia se vuelve un tema complejo cuando las actividades de la vida diaria involucran tantos dispositivos de captura a nuestro alrededor, por ejemplo, las cámaras de seguridad. Tomando en consideración lo anterior, al menos en donde el control este de parte de cada individuo, se deberían manejar las cosas con la cautela necesaria.

# 6. Conclusiones

Ante un modelo de vida cada vez más digitalizado, es fundamental tener mayores normas de prevención que resguarden los datos con el mayor sigilo posible. Como se ha constatado, las técnicas OSINT pueden ser usadas en beneficio de una investigación que exponga los puntos débiles que podría tener una institución. A partir de ese punto se pueden ya establecer criterios que subsanen las falencias encontradas.

Antes de aplicar el estudio se deben de valorar muy bien los campos que se van a cubrir y las fuentes de información abiertas que serán consultadas, parte del éxito del estudio radica en la calidad de la información recogida con las herramientas OSINT.

Todas las técnicas OSINT utilizadas en el presente trabajo, sirvieron para la extracción de datos personales y posterior creación de perfiles de miembros de la comunidad universitaria. Relacionando la Ley de Protección de Datos Personales con los datos obtenidos, se puede ver que aún hay trabajo pendiente para cubrir las brechas que exponen información sensible a nivel de la página institucional y de redes sociales. Es deber de cada persona tomar conciencia sobre lo que expone de su vida personal en medios digitales que están bajo su administración y del mismo modo exigir a quien corresponda que sus datos estén a buen recaudo cuando no se tienen las herramientas tecnológicas para cambiarlo.

Tanto las técnicas OSINT, como las herramientas para su aplicación, contribuyen de manera positiva en la evaluación del nivel de seguridad y pueden ser utilizadas como recurso tecnológico dando cumplimiento a lo estipulado en la Política de Privacidad de la Universidad Politécnica Salesiana.

El uso de herramientas OSINT no constituye un gasto elevado en el pago de licencias para uso de software, se tienen alternativas de código abierto que generan buenos resultados. Siempre estarán disponibles herramientas de pago que cumplen con

mayores beneficios a la hora de su ejecución, queda ya en el criterio del investigador implementar o no su uso en función del resultado esperado.

# Referencias


[1] BBC News Mundo (2019, septiembre 16), "'Filtración de datos en Ecuador: la "grave falla informática" que expuso la información personal de casi toda la población del país sudamericano" [Online]. Available: https://www.bbc.com/mundo/noticias-america-latina-49721456

[2] P. Laperdrix, N. Bielova, B. Baudry, G. Avoine, "Browser Fingerprinting: A Survey", ACM Transactions on the Web, vol. 14, no. 2, pp. 1-33, Mayo 2020, doi: https://doi.org/10.1145/3386040

[3] Fundación Telefónica, "Capítulo 2 La identidad digital" in Identidad Digital: El nuevo usuario en el mundo digital. Barcelona, España: Editorial Ariel, 2013, pp. 9-21

[4] A. López (2020, febrero 18), "'Oversharing', el riesgo de la sobreexposición en las redes sociales" [Online]. Available: https://www.abc.es/contentfactory/post/2020/01/23/orange-love-oversharing-riesgo-de-la-sobreexposicion-en-redes-sociales/

[5] Y. Rodríguez (2019, junio 06), "INTELIGENCIA DE FUENTES ABIERTAS (OSINT): CARACTERÍSTICAS, DEBILIDADES Y ENGAÑO" [Online]. Available: http://www.seguridadinternacional.es/?q=es/content/inteligencia-de-fuentes-abiertas-osint-caracter%C3%ADsticas-debilidades-y-enga%C3%B1o

[6] B. Becerra (2021, diciembre 11), "Consumo de internet en el mundo aumentó 19,5% durante la pandemia de covid-19" [Online]. Available: https://www.larepublica.co/consumo/consumo-de-internet-en-el-mundo-aumento-19-5-durante-la-pandemia-de-covid-19-3274945

[7] We Are Social (2022, enero 26), "DIGITAL REPORT 2022: EL INFORME SOBRE LAS TENDENCIAS DIGITALES, REDES SOCIALES Y MOBILE." [Online]. Available: https://wearesocial.com/es/blog/2022/01/digital-report-2022-el-informe-sobre-las-tendencias-digitales-redes-sociales-y-mobile/#:~:text=En%20enero%20de%202022%2C%20hab%C3%ADa,a%C3%B1o%3A%20192%20millones%20de%20personas.

[8] ITU (2021, noviembre 30), “2.900 millones de personas siguen careciendo de conexión” [Online]. Available: https://www.itu.int/es/mediacentre/Pages/PR-2021-11-29-FactsFigures.aspx

[9] L. Im-Yeong, K. Hwankuk, H. Yong-Woon, L. Hyejung, “Current Status and Security Trend of OSINT”, Wireless Communications and Mobile Computing, vol. 2022, Febrero 2022, https://doi.org/10.1155/2022/1290129

[10] S. Chauhan, N. K. Panda, “OSINT Tools and Techniques” in Hacking Web Intelligence. Waltham, MA, USA: Elsevier Science & Technology Books, 2015, pp. 113-130

[11] A. Martínez (2014, mayo 28), “OSINT - La información es poder” [Online]. Available: https://www.incibe-cert.es/blog/osint-la-informacion-es-poder

[12] Bidaidea (2022, mayo 23), “Osintomático Conference 2022. Bidaidea protagonista de su primera edición” [Online]. Available: https://ciberseguridadbidaidea.com/osintomatico-conference-2022/

[13] A. Roberts, “Chapter 7 The Importance of OSINT” in Cyber Threat Intelligence, UK, London: Apress Media LLC, 2021, pp. 131-152

[14] A. Toler (2019, diciembre 26), “Guide to Using Reverse Image Search for Investigations” [Online]. Available: https://www.bellingcat.com/resources/how-tos/2019/12/26/guide-to-using-reverse-image-search-for-investigations/

[15] J. Muniz, A. Lakhani, “Initial Research”, Web Penetration Testing with Kali Linux, Birmingham, Reino Unido: Packt Publishing, Limited, 2013, pp. 59-67

[16] H. Alkilani, A. Qusef, “OSINT Techniques Integration with Risk Assessment ISO/IEC 27001”, DATA'21: International Conference on Data Science, E-learning and Information Systems 2021, pp. 82-86, Abril 2021, doi: https://doi.org/10.1145/3460620.3460736

[17] We are social (2021, octubre 21), “LOS USUARIOS DE LAS REDES SOCIALES SUPERAN LA MARCA DE LOS 4.500 MILLONES” [Online]. Available: https://wearesocial.com/uk/blog/2021/10/social-media-users-pass-the-4-5-billion-mark/

[18] M. Kosinski, D. Stillwell, T. Graepel, “Private traits and attributes are predictable from digital records of human behavior”, Proceedings of the National Academy of Sciences, vol. 110, no. 15, Abril 2013, doi: https://doi.org/10.1007/978-3-319-47671-1_14

[19] C. Hadnagy, “Chapter 2 Do You See What I see” in Social Engineering, Second Edition. Indianapolis, IN, USA: John Wiley & Sons, Incorporated, 2018, pp. 33-34

[20] R. Gupta, H. Brooks, “Chapter 5 Mapping and Analyzing Social Networks” in Using Social Media for Global Security, First Edition. Indianapolis, IN, USA: John Wiley & Sons, Incorporated, 2013, pp. 126-131

[21] M. Bazzell, “Chapter Eight: Email Addresses” in Open Source intelligence techniques: Resources for searching and analyzing online information, Sixth Edition. Great Britain, United Kingdom: Amazon Digital Services, 2018, pp. 207-216

[22] M. Bazzell, “Chapter Nine: User Names” in Open Source intelligence techniques: Resources for searching and analyzing online information, Sixth Edition. Great Britain, United Kingdom: Amazon Digital Services, 2018, pp. 217-226

[23] B. Akhgar, P. Saskia, “Acquisition and Preparation of Data for OSINT Investigations”, Open Source Intelligence Investigation From Strategy to Implementation, Morgantown, WV, USA: Springer International Publishing AG, 2016, pp. 69-94

[24] N. Hassan, R. Hijazi, “CHAPTER 7 Online Maps”, Open Source Intelligence Methods and Tools, California, USA: Apress Media LLC, 2018, pp. 285-312

[25] M. Bazzell, “Chapter Seventeen: IP Addresses” in Open Source intelligence techniques: Resources for searching and analyzing online information, Sixth Edition. Great Britain, United Kingdom: Amazon Digital Services, 2018, pp. 339-352

[26] V. Troia, “Chapter 9 WHOIS”, Hunting Cyber Criminals, Indianapolis, Indiana: John Wiley & Sons, Inc, 2020, pp. 175-200

[27] F. Tabatabaei, D. Wells, “OSINT in the Context of Cyber-Security”, Open Source Intelligence Investigation: From Strategy to Implementation, Cham, Switzerland: Springer International Publishing, 2016, pp. 213-231