UNIVERSIDAD TECNOLÓGICA NACIONAL

Facultad Regional Santa Fe

MAESTRÍA EN INGENIERÍA EN SISTEMAS DE INFORMACIÓN

Tesis de Maestría

"ESTRATEGIA PARA LA PROTECCIÓN DE LA EXPOSICIÓN DE LAS PERSONAS Y DE SU ENTORNO EN REDES SOCIALES DIGITALES"

Autor: Ing. Román Pablo Zenobi

Directora: Dra. María Luciana Roldán

Dedicatoria

El desarrollo de esta Tesis está dedicado a mi familia, por el apoyo incondicional desde el momento inicial. Como diría mi abuela Mamina, “el estudio es lo único que no te pueden quitar”. Para ellos, gracias por estar presentes y ser la fuente de inspiración.

Además, dedico esta Tesis a todas las personas que se brindan día a día a lograr que la protección de los datos personas y la privacidad sean una prioridad, contribuyendo al desarrollo de la Seguridad Informática en todos los ámbitos.

Agradecimientos

Para concretar el desarrollo de esta Tesis, muchas personas fueron importantes y claves para lograr el objetivo. Fue un camino largo, con pausas y reinicios. Como diría la canción, fue un “Volver a empezar”. De este grupo de personas, primero está mi familia, sostén fundamental. Para mis padres y mi hermana, muchas gracias por acompañarme.

Agradezco a todos los docentes y compañeros de estudio a lo largo de mi carrera académica. Fundamental fue mi formación en ICES de Sunchales (Instituto Cooperativo de Enseñanza Superior). Fueron las primeras materias, experiencias de estudio y el cruzarme con profesores y personal de apoyo no docente clave en apuntalar el camino. Especial agradecimiento para Andrea Assone.

Continuando con mi trayecto de estudiante, agradezco a todos los docentes y personal no docente de la Universidad Católica de Santiago del Estero, Departamento Académico Rafaela (UCSE-DAR). Especialmente quiero agradecer por el apoyo incondicional y la motivación brindada en todo momento por Darío Karchesky. Fueros las dos instituciones educativas que confiaron en mí para que inicie mi carrera docente y mi incursión en el mundo de la investigación. Desde aquí surgieron los primeros temas de investigación que marcaron el tema principal de esta Tesis.

Durante mi trayecto laboral, agradezco a los referentes que escucharon mis ideas y brindaron el apoyo para iniciar con los primeros temas que asomaban con la Tesis: Matias Maretto, Leandro Lamberti, Jorge Goitre, Claudio Borra y Luis Lehmann.

Cuando inicié mi camino de posgrado, me crucé con compañeros de estudio excelentes que me orientaron y ayudaron. Agradezco a Luis Stroppi por su rol fundamental.

Inicialmente, durante el cursado de la Maestría, agradezco la ayuda de Marcelo Montagna, con quien tuve las primeras conversaciones para determinar posibles temas de desarrollo. Luego, quiero agradecer a Pablo Villareal, quien fue el primer director de Tesis que me orientó y con quien iniciamos las bases de la Tesis.

Finalmente, quiero agradecer especialmente a quien es la directora de la Tesis, Luciana Roldan. Muchas gracias por aceptar la dirección y por permitir que el tema de desarrollo pueda continuar vinculado con mi pasión que es la Seguridad Informática. Excelente acompañamiento, predisposición y guía en cada etapa e instancia de este proceso del desarrollo de la Tesis.

Índices

Índice General

Índice de Figuras

Índice de Tablas

Nomenclatura / Definiciones

1. OSINT: Open-Source Intelligence - Inteligencia de Fuentes Abiertas
2. Agencia de Seguridad Nacional (NSA)
3. Agencia Española de Protección de Datos (AEPD)
4. SMS (Mensajes de Texto)
5. GPS: Global Positioning System - Sistema de Posicionamiento Global
6. API: Application Programming Interface - Interfaz de Programación de Aplicaciones
7. SDK: Software Development Kit - Kit de Desarrollo de Software
8. URL: Uniform Resource Locator - Localizador de Recursos Uniforme
9. IP: Internet Protocol
10. US-CERT: United States Computer Emergency Readiness Team
11. Health Sector Cybersecurity Coordination Center (HC3)
12. OCMINT es el acrónimo de Social Media Intelligence
13. IMINT o “Inteligencia de Imágenes”.
14. SOCMINT - Inteligencia basada en las Redes Sociales
15. EXIF (Exchangeable Image File)
16. Perfil Biográfico Digital (PBD)
17. RSD (Red Social Digital)
18. FactorIncrementoExposición (FIE).
19. Factores de Mitigación de la Exposición (FME),
20. Métrica para calcular el valor de exposición de un atributo i en una publicación p: VE_ip
21. Métrica para calcular el valor de exposición en una publicación p: VE_p
22. Métrica para calcular el nivel de exposición de un PBD pbd: VE_ pbd
23. PIN: Personal Identification Number - Número de Identificación Personal
24. Múltiple Factor de Autenticación (MFA)
25. OCL (Object Constraint Language)

Los resultados de este trabajo de tesis han sido plasmados y divulgados a través de las siguientes publicaciones y congresos:

1. *Zenobi R., Roldan M. L., Perfiles Biográficos Digitales: Un Modelo Conceptual de la Exposición en Redes Sociales.* **Jornadas Argentina de Informática (JAIIO), Simposio Argentino de Ciberseguridad (SACS),** Universidad Nacional de Tres de Febrero (UNTREF), 2023.

2. *Zenobi R., Roldan M. L., Perfiles Biográficos Digitales: Identificación de Atributos de Exposición y su Mitigación en Redes Sociales.* I **Jornada de Ciberseguridad y Sociedad (JCyS),** Universidad Tecnológica Nacional – Facultad Regional Santa Fe (UTN-FRSF), octubre 2023.

3. *Zenobi R., Roldan M. L. , Perfiles Biográficos Digitales: Un Modelo Conceptual de la Exposición en Redes Sociales,* **Ekoparty - Security Conference, Social Engineering Space,** noviembre 2023.

4. *Zenobi R., Roldan M. L. A Conceptual Model of Privacy Exposure on Digital Social Networks. SADIO Electronic Journal of Informatic and Operation Research; Lugar: Buenos Aires; Año: 2024 vol. 23 p. 90 – 110.*

Capítulo 1: Introducción

1.1. Definición del problema

Cada persona en su vida tiene un perfil psicológico dado por su personalidad, que la identifica y hace única en relación con otras personas. En informática, cuando se habla de una red social digital se hace referencia a un grupo de personas que están conectadas entre sí por medio de una plataforma de software que oficia de mediadora y brinda el soporte para que cada individuo tenga definido su perfil y pueda entablar comunicación con otros seres humanos. Ese perfil que una persona define en dicha red social digital se denomina “perfil biográfico digital” o simplemente “perfil digital”.

Como indica el autor Andy Stalman (Stalman, 2016), las redes sociales son un amplificador de lo que las personas ya son como sociedad, en el sentido de que su forma de actuar en su vida física o terrenal debería ser la misma con la que se desarrollan, también de manera digital. Es decir, son las mismas personas, pero amplificando su vida en redes sociales digitales”.

Por ende, las personas deben ser conscientes de que las redes sociales digitales también implican la amplificación de su nivel de exposición, aumentando así la vulnerabilidad de sufrir ataques a su privacidad y la de su entorno.

Andy Stalman, además, recalca que esta nueva era, la era digital, está viendo el nacimiento de un nuevo hombre, cuyo desafío es aprender a vivir entre dos mundos: el online y el offline (Stalman, 2016).

En base a lo anterior, se puede afirmar que el mundo “online” de las personas es aquel que llevan adelante por medio de las redes sociales digitales, siendo Internet el principal motor y medio para que sea desarrollado. Por otro lado, el mundo “offline”, es aquel físico, terrenal, del día a día de las personas con sus relaciones sociales interpersonales, sin un medio electrónico de por medio.

En el mundo digital, en el que las redes sociales son una de las plataformas más utilizadas para interactuar entre pares, las personas se exponen. Esa exposición, es la forma en que sus características personales, su perfil biográfico, su privacidad y cuestiones propias de su vida son mostradas a otros, dejándose accesibles para que desde una plataforma de red social digital otros sujetos puedan conocerlas.

Yuval Nh Harari menciona en el artículo “Las dos únicas destrezas que necesitarás para el resto de tu vida” (Harari, 2020) que la mente humana es una máquina que produce relatos constantemente, y, sobre todo, un relato muy importante que es la identidad. Por otro lado, la tecnología recoge datos del sistema humano. Según Harari, eso producirá que en un futuro los algoritmos “puedan conocer a una persona mucho más de lo que ella se conoce a sí misma”. Además, en este artículo, afirma lo siguiente: “El yo es un relato, no es algo real”, es decir, “si tomamos el perfil que la gente crea sobre sí misma en Facebook o Instagram,

veremos que no refleja su existencia real". En consiguiente, el ser humano tiende a pensar que él realmente es ese relato que ha construido en un perfil de una red social digital.

Cuando una persona se encuentra expuesta en una red social digital, es posible que "alguien" encuentre la forma de sacar provecho de la información que la persona ha compartido. Esta persona malintencionada podría seguir una serie de pasos en un determinado orden que le permitan revelar el grado de exposición que tiene usuario en sus redes sociales digitales y concretar un ataque a su privacidad.

Un ataque a la privacidad de los usuarios puede ocurrir de variadas maneras. Los atacantes usan diferentes técnicas y herramientas para explotar la manera en que una persona se expone en una red social digital, aprovechando las características que estas plataformas tienen para describir a un perfil de usuario. Expresado en otras palabras, un atacante puede valerse de la información expuesta en el perfil de un usuario con un fin malicioso, obteniendo detalles de la vida privada de una persona con el fin de llegar a concretar ciertos delitos, como puede ser una extorsión o simplemente nutrirse de datos para conocer la forma de vida y hábitos de un individuo, sus gustos y preferencias, para concretar otro tipo de delito o ciberdelito (por ejemplo, un robo o secuestro, realizar una acción en una aplicación web como si fuera esa persona, ejecución de código malicioso, etc.).

Como se indica en el trabajo "What Anyone Can Know: The Privacy Risks of Social Networking Sites" (Rosenblum, 2007), hay dos tipos de adversarios o de atacantes: los internos, y los externos o intrusos. Los atacantes internos son otros usuarios que forman parte de la red social, legítimos en sí mismos ya que cuentan con algún perfil válido y por consiguiente son considerados "usuarios" habilitados para el uso de la red social digital. Los adversarios o intrusos externos son aquellos usuarios que acceden como "visitantes" a las redes sociales, es decir, no necesitan un perfil propio, sino que navegan por la información pública que encuentran en los perfiles de los usuarios activos de cada red social. Entonces, en su esencia, son usuarios normales de Internet, pero que, gracias a la exposición inadecuada de los usuarios en las redes sociales, se convierten en potenciales atacantes externos.

En base a lo anterior, como se menciona en "Embarrassing Exposures in Online Social Networks"(Choi y colab., 2015), se hace presente el efecto de diseminación de la exposición con efecto dominó. Estos autores utilizan el concepto de "usuarios expuestos pasivos", es decir, aquellas personas que son expuestas simplemente por estar mencionadas en un perfil de un usuario expositor. Esta situación suele presentarse, sin que estos usuarios tengan completa conciencia o conocimiento de ello.

En los últimos años ha cobrado importancia un tipo nuevo de trabajo de "inteligencia" relacionado con la exposición de los usuarios en redes sociales digitales, el cual es denominado con la sigla OSINT (Open Source Intelligence).

Tomando como base la definición del INCIBE (Instituto Nacional de Ciberseguridad de España[1]), OSINT hace referencia al conocimiento recopilado a partir de fuentes de acceso público. El proceso incluye la búsqueda, selección y adquisición de la información, así como el posterior procesado y análisis de la misma con el fin de obtener conocimiento útil y aplicable en distintos ámbitos. Reforzando el concepto, OSINT (CiberPatrulla, 2020) es considerada una metodología con el fin de obtener información sobre una determinada persona, institución o grupo. Esta actividad abarca el uso de un conjunto de herramientas y técnicas que permiten explotar el flujo de exposición de un usuario en una red social u otra plataforma en la que el usuario exponga sus datos.

Se considera fuente abierta o fuente de dato pública a cualquier vía accesible a través de la cual que se pueden conseguir datos, es decir, que esos datos no estén cifrados (sean entendibles) y sean posible de ver por cualquier ciudadano (dominio público).

Considerando lo expresado por Sun Tzu en su libro "El Arte de la Guerra" (1994), “no hay mejor defensa que un buen ataque”; por lo que conocer la metodología de OSINT es una herramienta necesaria para armar una estrategia que permita a los usuarios cuidar sus perfiles digitales de las redes sociales y poner las restricciones adecuadas evitar posibles los ataques. Siguiendo con esa línea, el Instituto SANS (SysAdmin Audit, Networking and Security Institute), menciona en un artículo que para encontrar la mejor manera de proteger a una organización de posibles ataques que se aprovechen de la exposición de sus miembros, es necesario entender qué clase de información está disponible públicamente. Este instituto, además, indica que es importante conocer las herramientas, habilidades y técnicas disponibles para explorar la gran cantidad de información que se encuentra en Internet (SANS Institute, 2020).

Derivado de OSINT, surge un concepto crucial: el de la *Ingeniería Social*. Este término hace referencia a las técnicas y herramientas que se usan para obtener información sensible y privada a través de ganar la “confianza” del propio dueño o de personal clave que podría hacer de puente para lograr el objetivo final. Los atacantes combinan esta técnica con herramientas directas ofrecidas por la metodología OSINT para hacerse de información de sus víctimas. Es importante aclarar, que OSINT tiene un objetivo benévolo: servir de base para investigar a los atacantes y ser usado para conocer y llegar a los antecedentes de un delito cometido hacia una persona. Por eso, conocer cómo un atacante piensa, es la herramienta para una buena defensa.

Existe un marco de referencia llamado OSINT Framework que contiene un índice con las categorías de información que se pueden encontrar en fuentes públicas y las herramientas asociadas para obtener dicho

[1] Sitio Web INCIBE: https://www.incibe.es/

material (OSINT Framework, 2016). En idioma español, existe un sitio denominado “Ciber Patrulla” que también contiene una extensa lista de herramientas y material asociado a esta técnica (CiberPatrulla, 2020).

La problemática en relación con la privacidad en redes sociales digitales constituye la motivación del trabajo a abordar durante el desarrollo de la tesis. Dado a que el universo de redes sociales digitales es amplio, se acotará el trabajo de investigación a un grupo de ellas, determinado por una serie de estudios estadísticos particulares sobre la popularidad y nivel de usuarios. El estudio de estas redes se tomará como base para definir una visión genérica que sirva como lineamiento general para toda red social digital que pueda emplearse para definir un perfil biográfico digital de una persona.

En base a lo mencionado anteriormente, se hace necesario, proponer estrategias que posibiliten la protección de los niveles de exposición de las personas en las Redes Sociales Digitales, de manera que el conjunto de acciones privadas de una persona pueda quedar efectivamente contenida en su esfera íntima y bajo el resguardo de los usuarios, quedando en su exclusiva voluntad si se desean compartir con otros ciertos aspectos y en qué condiciones.

La exposición de las personas en una red social en un perfil digital sobre una plataforma que así lo permita, conlleva una gran responsabilidad. La misma radica en que las personas son los principales custodios de su información personal, ya que son los dueños de esta, y, por lo tanto, son los principales interesados en proteger algo tan valioso como su privacidad.

En su libro “Vigilancia Permanente” (Snowden, 2019), el ex-agente de la Agencia de Seguridad Nacional (NSA) Edward Snowden puso de manifiesto el valor de la información y el poder que tiene cuando es manejada por una entidad de Gobierno, para un fin que va más allá de evitar el terrorismo, sino que es empleada para vigilar a cada persona, sus vínculos y su entorno. Él mismo renunció de su rol como especialista informático, al ver en primera persona “toda la información” que pasaba por delante de sus ojos. Esta decisión lo llevó a hoy encontrarse exiliado de su país de origen, Estados Unidos, acusado de espionaje por dar a conocer información “sensible” de dicha Agencia de Seguridad con supuestos planes de ciber espionaje.

Cada usuario de una red social digital dispone de variados elementos para construir sus perfiles de exposición, y, en dicho contexto, existen ciertos factores que pueden incrementar la forma en que la privacidad de una persona se ponga al descubierto, es decir, sea proclive a ser atacada.

La situación de vulnerabilidad respecto de su privacidad puede ser desconocida por parte de los usuarios, en cuanto a no ser conscientes de los riesgos a los que se exponen, ya que suponen que están respaldados por una plataforma de red social digital “con ciertas condiciones establecidas en cuanto al cuidado de privacidad”. Esta situación, es otro aspecto de la problemática que motiva el presente trabajo de

tesis, en el cual se propondrán herramientas para generar conciencia sobre la protección de la exposición de las personas usuarias de redes sociales y su mitigación frente a ataques que comprometan su intimidad y la de su entorno.

Por medio del conocimiento y relevamiento de técnicas como la Ingeniería Social y el esquema OSINT, se buscará en el trabajo de tesis propuesto, identificar los diferentes aspectos que constituyen el modo en que los usuarios generan exposición en las redes sociales digitales, y brindar las herramientas necesarias para que los usuarios tomen conciencia del significado de mostrar información privada en ambientes de uso público, y puedan tomar acciones para una adecuada defensa de su privacidad.

Dentro del esquema OSINT antes mencionado, existen herramientas específicas para llevar adelante distintas fases de un análisis de exposición de usuarios. Es decir, existe software que brinda soporte a las diferentes etapas de recolección de la información que permiten evaluar cómo un usuario se expone en sus Redes Sociales Digitales. Con el presente trabajo de tesis, se busca analizar y sistematizar este proceso poniendo foco en la capacidad de evaluación, razonamiento e inducción humana, para lograr reconocer y cuantificar el nivel de exposición de una persona. Sin bien la propuesta ofrece una perspectiva “artesanal” o manual del proceso de recolección de información, como línea futura se puede implementar como un proceso computacional, empleando técnicas de diferentes disciplinas como la Inteligencia Artificial, Machine Learning, reconocimiento de patrones de imágenes y lenguaje natural, entre otras.

1.2. Objetivos

El objetivo general de la presente tesis es definir una estrategia de protección de la exposición de las personas en redes sociales digitales, que permita mitigar ataques que comprometan su privacidad y su entorno. Este objetivo se desglosa en los siguientes objetivos específicos:

1. Conocer las condiciones de privacidad generales que ofrecen las plataformas de Redes Sociales Digitales.
2. Identificar y definir los conceptos de *Flujo de Exposición* de los usuarios en las Redes Sociales Digitales, los *Factores de Incremento* que afectan a dicho flujo y los elementos de Mitigación recomendados para atenuar riesgo de exposición.
3. Generar una base de conocimiento de ataques existentes a la privacidad y sus consecuencias, y las posibles estrategias de mitigación de exposición de usuarios a fin de evitarlos.
4. Proponer herramientas que puedan ser usadas en el contexto de uso de redes sociales, para que los usuarios conozcan sus niveles de exposición y puedan administrar su privacidad.
5. Plantear un modelo conceptual de características de perfiles en redes sociales digitales, los posibles flujos de exposición, potenciales ataques a la privacidad, y formas de mitigación asociadas, el

cual pueda ser usado como la base para el desarrollo de una aplicación informática integrada a un browser web que asista a los usuarios en el uso de Redes Sociales digitales.

1.3. Metodología de desarrollo

Mediante el recorrido y análisis de un conjunto de redes sociales digitales seleccionadas, se trabajará en la identificación de un conjunto de factores que incrementan la exposición de los usuarios. Se trabajará con una muestra de perfiles digitales diversos, los cuales se tomarán como base para el relevamiento y caracterización de las redes sociales seleccionadas, considerando la parte pública de los mismos. Es decir, se tomará la información que tienen en los perfiles digitales y es directamente visible independientemente si se tiene o no contacto conocido con dicha persona en la plataforma.

Considerando lo mencionado en (Arshad y colab. 2018), la información que se encuentra en las redes sociales digitales se categoriza en 4 clases: Usuario (información personal del usuario), Actividad (tiene que ver con cada información vinculada a las publicaciones o eventos que hace el usuario y donde se especifica la locación y tiempo de ocurrencia), Red (la información de contacto del usuario, como su teléfono o enlaces a otras redes sociales) y Contenido (todo lo que el usuario publica en sus perfiles). Estas categorías de información serán las estudiadas durante el relevamiento. En este sentido, es importante remarcar la diversidad del universo de redes sociales digitales seleccionadas para este trabajo. Si bien cada una tiene un enfoque particular (un objetivo a cumplir que se propone a los usuarios), en su cimiento la información que se maneja se categoriza de la misma manera en todos los tipos de redes. Se puede decir que, si bien hay una heterogeneidad en las redes sociales digitales, existe una homogeneidad en el tipo de información que administran de los usuarios.

En cuanto a la metodología de investigación a seguir, se toma la propuesta en (Espinoza Montes, 2014) Esta metodología considera un enfoque del estudio de manera sistémica, lo cual posibilitará dividir el análisis de las redes sociales digitales en componentes que luego se acoplarán unos con otros para definir el modelo propuesto. Tal como menciona el autor, la metodología referenciada permite abordar el proceso de investigación tecnológica y científica con un enfoque sistémico, experimental y creativo en todas sus etapas desde el surgimiento de las ideas hasta el reporte y comunicación de los resultados obtenidos del trabajo.

Esta metodología es adecuada para el desarrollo del trabajo de tesis dado que una red social digital puede considerarse como un sistema compuesto por un conjunto de elementos que se relacionan y tienen un propósito en general. Estos elementos pueden ser: las publicaciones, los datos personales, los contactos, los intereses, los atributos de configuración del perfil, etc. Cada uno de estos elementos forman su perfil y según la forma en que cada uno de ellos se use y desarrolle, generará un nivel de exposición determinado. Según Espinoza Montes (2014), este pensamiento sistémico es integrador, y permite abordar la problemática

proponiendo soluciones en las cuales se tienen que considerar diversos elementos y relaciones que conforman la estructura de lo que se define como "sistema" y todo aquello que conforma su entorno.

Se llevarán a cabo las siguientes actividades para alcanzar los objetivos propuestos:

1. **Revisión de bibliografía relacionada a los conceptos del proyecto**
   a. Procedimiento: análisis de repositorios de bibliografía relacionada a la temática, considerando trabajos de investigación en revistas o reuniones científicas, libros, artículos, estadísticas y otro material vinculado.
   b. Aporte: conjunto de bibliografía seleccionada para su estudio y guía para el desarrollo del trabajo.
2. **Clasificación de la bibliografía según tópicos referenciados en los objetivos del proyecto.**
   a. Procedimiento: Categorizar la información obtenida en la revisión bibliográfica, según diferentes criterios. En ese sentido, se considerará si la bibliografía es sobre una red social en particular, si abarca conceptos propios de ciberseguridad, si se relaciona con protección de datos personales y marco normativo, si tiene vínculo con material de técnicas de análisis de información expuesta, si se relaciona a ataques y mitigaciones o en su defecto, contempla algún concepto en general que se requiera para el trabajo.
   b. Aporte: conjunto de bibliografía clasificada según ciertos criterios. Esta información organizada servirá de base para etapas posteriores en el trabajo de investigación.
3. **Selección de las Redes Sociales Digitales de marco referencial.**
   a. Procedimiento: Revisar una serie de estudios estadísticos globales que muestran las redes sociales digitales más usadas según ciertos criterios de evaluación.
   b. Aporte: obtener un conjunto de redes sociales digitales a ser estudiadas en relación con cuestiones de privacidad, las cuales definirán el alcance de la tesis.
4. **Revisión de las condiciones de privacidad de cada Red Social Digital seleccionada.**
   a. Procedimiento: para cada red social seleccionada, se revisará su programa de condiciones de privacidad para conocer cómo son sus políticas vinculadas al tratamiento que hacen de los datos personales de los usuarios y del material que ellos comparten.
   b. Aporte: conocimiento de las condiciones de privacidad para continuar con la identificación de los aspectos relevantes.
5. **Identificación de los puntos relevantes vinculados a la exposición de las personas en cada una de las condiciones de privacidad revisadas.**

a. Procedimiento: en base al relevamiento de las condiciones de privacidad, se enumerarán los puntos principales que tienen relación a las normas y protocolos que brindan las redes sociales digitales seleccionadas, sobre el tratamiento de los datos propios de los usuarios.
b. Aporte: detectar aquellos puntos de las condiciones de privacidad que los usuarios deberían conocer para el entendimiento de cómo los datos que comparten en estas redes sociales digitales son administrados y mantenidos.

6. **Descripción de cada uno de los elementos que favorecen o son causa de la exposición de los usuarios en las redes sociales digitales.**
   a. Procedimiento: En base a los puntos detectados como relevantes en las condiciones de privacidad, se analizarán aquellos particulares que favorecen o son el puente para facilitar una exposición de la información de los usuarios en las redes sociales digitales. Ver si no sería: En base a los puntos detectados como relevantes en las condiciones de privacidad, se analizará si éstos favorecen o son el puente para facilitar una exposición de la información de los usuarios en las redes sociales digitales.
   b. Aporte: Detectar de qué manera, cada una de las redes sociales digitales, por medio de las condiciones de privacidad, pueden contribuir a que la exposición de los usuarios sea mayor y en consiguiente se incremente sin conocimiento por parte de los mismo.
7. **Relevamiento de los factores que incrementan la exposición de los usuarios en sus perfiles biográficos digitales.**
   a. Procedimiento: Se revisarán las estructuras de los perfiles biográficos digitales de las redes sociales digitales, tomando como base los contenidos públicos, para determinar los factores que facilitan el incremento de la exposición de los usuarios.
   b. Aporte: detectar cada uno de los factores que incrementan la exposición de los usuarios en las redes sociales digitales de manera de comenzar el relevamiento de medidas de mitigación y protección de su privacidad.
8. **Descripción de los principales ataques que se efectúan con el aprovechamiento de una exposición inadecuada de los usuarios.**
   a. Procedimiento: En base a la bibliografía seleccionada, se detallarán los ataques que se efectúan en base al nivel de exposición de los usuarios en las redes sociales digitales. Ver de cambiar por: Se realizará una búsqueda bibliográfica para identificar y recopilar los principales ataques a la seguridad y privacidad de usuarios, que ocurren a partir de la explotación de los niveles de exposición de los usuarios en redes sociales digitales.

b. Aporte: Contar con una base de conocimiento de los distintos tipos de ataques que se efectúan aprovechando la exposición de los usuarios, y a partir de ello elaborar un conjunto de medidas de mitigación y concientización a los usuarios.

9. **Relevamiento de la metodología OSINT como base para el análisis de fuentes de información de los perfiles digitales.**
   a. Procedimiento: Análisis y relevamiento de material vinculado a la metodología OSINT, considerando plataformas y herramientas informáticas que se utilizan, efectuando pruebas y validaciones al respecto.
   b. Aporte: selección de recursos de la técnica OSINT que permitirán hacer el análisis de la exposición de la información de casos de testigos de exposición de usuarios en las redes sociales digitales.
10. **Descripción de las medidas de mitigación y protección para la reducción de los ataques a la exposición y privacidad de los usuarios.**
    a. Procedimiento: elaboración del compendio de medidas de mitigación y protección en base a los distintos tipos de ataques y las técnicas de OSINT analizadas.
    b. Aporte: alimentar la base de conocimiento con el conjunto de medidas de protección y mitigación que pueden ser aplicadas por los usuarios para reducir su exposición y lograr reducir la superficie de ataque.
11. **Definición de un modelo conceptual de perfiles, amenazas y formas de mitigación.**
    a. Procedimiento: Elaboración de un modelo conceptual empleando diferentes tipos de diagramas expresados en el Lenguaje de Modelado Unificado (UML).
    b. Aporte: Modelo conceptual que exprese los conceptos sobre la exposición de usuarios en redes sociales, riesgos asociados (ataques potenciales), y medidas de mitigación.
12. **Creación de un prototipo de herramienta informática:**
    a. Procedimiento: Generación de un prototipo visual de la herramienta informática que contempla las funcionalidades para analizar una foto publicada por el usuario y facilitar la detección de los factores de incremento de exposición.
    b. Aporte: Prototipo de la herramienta informática que muestre cómo se puede ayudar al usuario a determinar el nivel de exposición de una foto en su perfil biográfico digital.
13. **Realización de conclusiones.**
    a. Procedimiento: confección de los resultados finales del trabajo en base a los objetivos planteados y el desarrollo de cada una de las tareas efectuadas.
    b. Aporte: detalle del cumplimiento de los objetivos planteados en el trabajo.

Capítulo 2: Estado del arte

En el presente capítulo, se hará un repaso de los principales sucesos en la historia de las Redes Sociales Digitales, en los que de alguna u otra manera la protección de la información que manejan se vio comprometida y, en consiguiente, la reputación de la red afectada. Además, se repasarán antecedentes en materia de investigación sobre de las Redes Sociales Digitales en lo que respecta a su aspecto de exposición de información de los usuarios. Para complementar el estudio del estado del arte se enunciarán las principales leyes, decretos, disposiciones, etc. de la República Argentina que son relativas a la privacidad de las personas.

2.1 Antecedentes de ataques a la privacidad de los usuarios en Redes Sociales Digitales.

En la historia del desarrollo de las Redes Sociales Digitales, han ocurrido sucesos impactantes que constituyen ejemplos en donde la privacidad de los usuarios no ha sido cuidada por esas plataformas en las cuales las personas confiaban. Esa confianza que los usuarios depositaron construyendo sus perfiles, creyendo que estaban custodiados por tales redes sociales digitales se ha visto comprometida con frecuencia. A partir de estas olas de sucesos, diferentes grupos de personas han ido ajustando sus condiciones de privacidad y discerniendo acerca del verdadero valor que le dan a ésta.

En el mundo de las redes sociales consideradas “laborales”, LinkedIn es la plataforma estrella para tal fin. Millones de usuarios arman sus perfiles profesionales, al estilo Curriculum Vitae digital y generan contactos con pares vinculados por sus especialidades y disciplinas de trabajo. En ese sentido, existe un perfil digital para cada usuario, donde el objetivo es dar a conocer sus antecedentes profesionales y laborales.

En el caso de LinkedIn, un usuario, mediante una red social digital profesional, no sólo puede exponer su propia información personal sino también la de su entorno laboral. Es común que los usuarios comenten en dichos perfiles cuál es su trabajo actual, puesto, tareas, tecnologías usadas y vínculos internos dentro de su lugar de empleo. Como menciona el autor Wu He (2012), las empresas deben diseñar una estrategia para mitigar la exposición de información confidencial por parte de sus empleados, en el uso que ellos hacen de sus redes sociales. En ese sentido, indica la necesidad de construir una política de uso de redes sociales y que sea comunicada de manera periódica. Si se toma como base lo mencionado por este autor, la conducta o comportamiento de una persona en las redes sociales, la forma en cómo se expone, puede superar los límites de su propia privacidad y llegar a la confidencialidad de su trabajo dentro de la organización en la que se inserta.

En el año 2012, LinkedIn reconoció que la empresa sufrió un acceso no autorizado y, en consecuencia, se produjo la filtración de aproximadamente 6,5 millones de credenciales de usuario. En respuesta a este ataque, la acción tomada por la plataforma fue el reseteo de claves de aquellas cuentas que habían sido comprometidas. Esto fue confirmado por la misma red social en un comunicado oficial (Scott, 2016). Estos tipos de brechas de seguridad en la aplicación que sostiene a la red social, combinados con una pobre gestión en la privacidad de una persona y su entorno, puede conducir a comprometer a toda una organización cuyos miembros participan en dicha red.

Recientemente, durante enero 2024, investigadores de ciberseguridad de las empresas Cybernews y Security Discovery, identificaron una filtración masiva con más de 26.000 millones de registros con datos de usuarios de plataformas sociales en la que se encuentra LinkedIn. Para esta plataforma, se menciona una filtración de 251 millones de cuentas. Por ende, se recomienda en cambio de contraseña para prevenir un compromiso de la cuenta si la misma está en dicho listado [13].

Por otro lado, la red social Facebook es, tal vez, el exponente principal del tipo de plataformas en las cuales los usuarios crean sus perfiles y comparten con otras personas, creando sociedades digitales. En el año 2014, se produjo un hecho que puso en cuestión hasta qué punto los datos que brindan los usuarios quedan protegidos y no son usados para otros fines. La consultora Cambridge Analytica fue acusada de haber obtenido información de millones de usuarios de Facebook sin permiso, es decir violando las políticas de uso de la red social (Infobae, 2018). Para ello diseñaron una aplicación llamada "*This is your digital life*" para que usuarios la usen para responder una serie de preguntas a cambio del pago de algunos dólares y de esa manera conocer un poco más sobre conductas asociadas a los mismos. Hasta ese punto, se habían conseguido aproximadamente 270000 perfiles de usuarios con su consentimiento para hacer el test de referencia. Esta aplicación necesitaba que se inicie sesión en Facebook y que se le otorguen ciertos privilegios. Lo que pasó realmente es que uno de los permisos que pedía la aplicación era el acceso a los datos de los "amigos" de los perfiles aceptados en primera instancia. Eso produjo una recopilación total de información de 50 millones de perfiles, siendo que éstos, en su mayoría no habían brindado la aprobación para eso. La información que se obtuvo fue enviada a la consultora Cambridge Analytica, pero no sólo para fines académicos (como había sido aclarada a los usuarios) sino para ser usada para conocer otras cuestiones y que, por ejemplo, pueda usarse para campañas políticas. El descubrimiento de estos hechos llevó a que la opinión pública e instituciones de gobierno cuestionaran la falta de transparencia que implica el uso de los datos sin permiso de los perfiles de los usuarios (Infobae, 2018).

Este suceso de 2014 puso en el ojo de la mira a esta red social, la cual puede ser un instrumento para que se concrete el acceso masivo a datos personales sin consentimiento explícito de las personas. En este

caso, las características de privacidad que Facebook pregonaba no alcanzaron para justificar su rol en este evento. Desde esa fecha, esta plataforma revisó y actualizó sus condiciones de uso y privacidad de los datos de usuarios.

En el año 2016, más precisamente en el mes de agosto, WhatsApp hizo un cambio en la política de privacidad agregando que la plataforma podría compartir información de los usuarios de WhatsApp con Facebook. A continuación, un extracto de dicha política:

"Como parte de la familia de empresas de Facebook, WhatsApp recibe información de esta familia de empresas y comparte información con ellas. Podemos usar la información que recibimos de ellas, y ellas pueden usar la información que compartimos con ellas, para ayudar a operar, proveer, mejorar, entender, personalizar y comercializar nuestros Servicios y sus ofertas, así como ofrecer servicios de ayuda para nuestros Servicios... Facebook y las demás empresas de la familia de Facebook también pueden usar nuestra información para mejorar tus experiencias con sus servicios..." (WhatsApp, 2016).

Este cambio de política hizo que la Agencia Española de Protección de Datos (AEPD) impusiera una multa a las dos plataformas por considerar que las condiciones establecidas de privacidad no se ajustan a la normativa vigente (AEPD, 2018). Para el caso de WhatsApp, dicha agencia consideró a esta política como una intención de brindar datos de los usuarios a Facebook sin su aprobación previa, y por el lado de Facebook, se consideró la intención de usar esa información para sus propios usos y beneficios.

Continuando con el año 2016, aquel suceso que presentó LinkedIn en 2012 tuvo irrigación mayor y finalmente se descubrió que un mayor número de credenciales de usuarios había sido expuesto en Internet. Aproximadamente, más de 100 millones de datos de cuentas de perfiles fue filtrada y publicada. Tal como comentan en el comunicado oficial (Scott, 2016), al identificar los usuarios comprometidos, se les pidió que reseteen sus contraseñas y, además, se promovió al uso del Doble Factor de Autenticación y la construcción de contraseñas robustas. Esta declaración, puede ser vista como un posible traslado de la responsabilidad de la seguridad de los perfiles a cada uno de los usuarios. Sin embargo, es importante considerar la siguiente analogía en el caso de LinkedIn: la red social brinda a los usuarios una "habitación" para sus perfiles profesionales, lo que significa que cada usuario tiene su llave. Pero la seguridad de todo el edificio, es decir, las condiciones que propiciarían que una persona no autorizada ingrese en una "habitación" que no le pertenece, tiene que recaer sin duda en el dueño o propietario de esa locación, es decir la plataforma de la red social.

La red social Twitter fue noticia en el año 2020, durante el mes de Julio. La situación consistió en que numerosos perfiles de personas de renombre mundial fueron víctimas de una publicación sin su consentimiento en la que indicaban que donarían el doble de monedas digitales a los usuarios que hagan un

depósito en un determinado período. Durante el lapso en que estos comentarios estuvieron activos, existió recaudación de dinero. Lo que queda en limpio y se sospecha de este ataque es que se basó en manipulación que hicieron los atacantes a empleados internos de Twitter mediante la técnica de Ingeniería Social, y, en consiguiente, lograron el acceso mediante sus credenciales a sistemas de administración internos para alterar las cuentas afectadas. Según el comunicado oficial de Twitter, sobre las cuentas comprometidas, los atacantes pudieron tomar datos de números telefónicos y correos electrónicos de los usuarios que sólo son conocidos internamente por la empresa para administración. Asimismo, se comprobó por estudios forenses, que los atacantes pudieron obtener otra información privada de las cuentas comprometidas (Twitter, 2020).

Es importante destacar que la empresa Meta, la propietaria de Instagram, desde junio de 2023, ha incorporado una restricción en el envío de mensajes a perfiles de usuarios adolescentes, menores de edad. En ese sentido, para poder mandar un mensaje directo, el interesado primero debería seguir a la otra persona. Es decir, tiene que haber una aceptación. Esta medida se suma a otras adicionales que Meta fue implementando a lo largo del tiempo para proteger al público adolescente. Por ese camino, desde enero de 2024, Instagram automáticamente comenzó a pedir a los usuarios de esta franja horaria, que actualicen sus condiciones de privacidad de manera simplificada.

Además, poniendo el foco en el control de las Redes Sociales Digitales, en sintonía con lo mencionado por Snowden en [14], actualmente existen una serie de países en los cuales sus gobiernos han bloqueado el acceso a dichas plataforma para su población. Para nombrar unos ejemplos, en Corea del Norte, todas las redes sociales digitales están prohibidas; en China, el bloqueo es para las plataformas de origen occidental; en Rusia, se prohíbe Twitter, Facebook, Instagram y LinkedIn.

2.2 Antecedentes de investigación sobre privacidad en redes sociales

En la historia de esta temática particular sobre la exposición de la privacidad, Rosenblum y colab. (2007) refieren a lo que en ese momento comenzaba a producirse a nivel global: la propagación y adopción de las redes sociales digitales. Como indican estos autores, los albores de las comunicaciones digitales permitían expresarse mediante blogs, realizar algunas video conferencias con la webcam, y el uso de emoticones para mostrar los sentimientos. En esos inicios, los perfiles de una persona en esos sitios webs se circunscribían únicamente a su nombre, edad, ciudad, correo electrónico y alguna imagen identificatoria.

Como se menciona en (Rosenblum y colab., 2007), las redes sociales como Facebook y MySpace (precursoras en los inicios), propiciaron el gran salto, es decir, lograr que cada usuario cree su propio perfil, indique sus preferencias de exposición, mostrando lo que, en principio, quedaba en el plano de las redes sociales humanas convencionales. Se podría decir que ese “pequeño salto” para las redes sociales digitales

fue un “salto al vacío” para la privacidad de las personas. Realmente, paso a paso, la cornisa de la exposición asomaba en el horizonte. Como se indica en ese trabajo de 2007, surge el concepto de la “intimidad online”. Por ende, ya no se hablaba de la intimidad en el mundo físico, sino que, desde ese momento, con el nacimiento de Facebook, se comenzó a pensar en que digitalmente, mediante una plataforma web, las personas podían exponer sus cuestiones privadas sin control aparente.

En el trabajo "Privacy and security for online social networks: challenges and opportunities" (Zhang y colab., 2010) dentro de las redes sociales analizadas, se considera Twitter. Es un punto importante dado a que esta red social se comienza a observar como una plataforma en donde la privacidad de los usuarios también está en juego y no se limita únicamente a la publicación de comentarios informativos o novedades de temas particulares. Esto quiere decir que los perfiles de usuarios se comienzan a empoderar en Twitter. Continuando con los aspectos comentados en (Rosenblum y colab., 2007), los autores detallan los alcances de la privacidad en el contexto de las redes sociales digitales:

- Anonimato de la identidad del usuario.
- Privacidad del espacio personal del usuario, su perfil.
- Privacidad de la comunicación del usuario.

Como remarca este trabajo, la privacidad implica confidencialidad y que el usuario sea el único dueño de su perfil y por ende administre los permisos en el mayor nivel de granularidad posible. Esto es, al mayor detalle, tópico por tópico de su espacio de perfil.

En las conclusiones de esa investigación se menciona la necesidad de trabajo colaborativo entre expertos en ciencias sociales, las comunidades de seguridad, la industria y las regulaciones a fin de tomar decisiones sobre la manera de aplicar seguridad en los mecanismos y políticas que permitan preservar la privacidad en las redes sociales digitales. Tal vez como desafío identificado en este desarrollo, se puede mencionar a cómo enriquecer una relación en una red social digital, superando el mero concepto de “amigo o no” como contacto dentro de un perfil de usuario. Este desafío menciona factores como: tipos de relación (bidireccional o unidireccional), confianza entre usuarios y la intensidad de la interacción en calidad y cantidad. En definitiva, cómo nutrir a este tipo de relaciones de un componente de confianza de manera que cada usuario sienta la privacidad en las comunicaciones, en sus exposiciones y modos de interactuar con los demás, como si fuera la vida real cara a cara.

Otro antecedente relevante, es el trabajo de (Aghasian y colab., 2017) cuyo objetivo es cuantificar el nivel de privacidad que un usuario tiene considerando múltiples redes sociales. Desde ese punto, en este trabajo, se mencionan los factores de exposición que se ponderan para obtener el cálculo final y que son decisivos, para validar el nivel de privacidad general. De dicho trabajo, se destaca la definición de dos factores

principales que se toman como entrada para medir el puntaje de exposición de la privacidad: visibilidad y sensibilidad de la información. Con estos factores se hace referencia a qué información se puede obtener de un perfil de la red social de un usuario y qué tan sensible y crítica se vuelve su exposición. Para el desarrollo del presente trabajo de tesis, se tomará en cuenta el análisis de estos factores que influyen en el nivel de riesgo en la exposición de un usuario. Se busca como factor diferenciante, que, con este desarrollo, el usuario tenga un procedimiento simplificado para evaluar la exposición de su perfil y que además se permita ponderar el riesgo por cada elemento en particular, por ejemplo, de una foto. Con dicho escenario, el usuario podrá identificar cuál elemento de exposición es el crítico para determinar el riesgo.

Los autores Choi y colab. en su trabajo "Embarrassing Exposures in Online Social Networks: An Integrated Perspective of Privacy Invasion and Relationship Bonding" (2015) presentan un esquema de "audiencia" en torno a un usuario de una red social digital con los siguientes roles de participantes: "Usuario objetivo" (Target), "Amigos diseminadores" (DF), "Amigos del usuario objetivo" (TF) y "Amigos en común" (CF). En la Figura 1, se presenta el diagrama gráfico de dicho esquema.

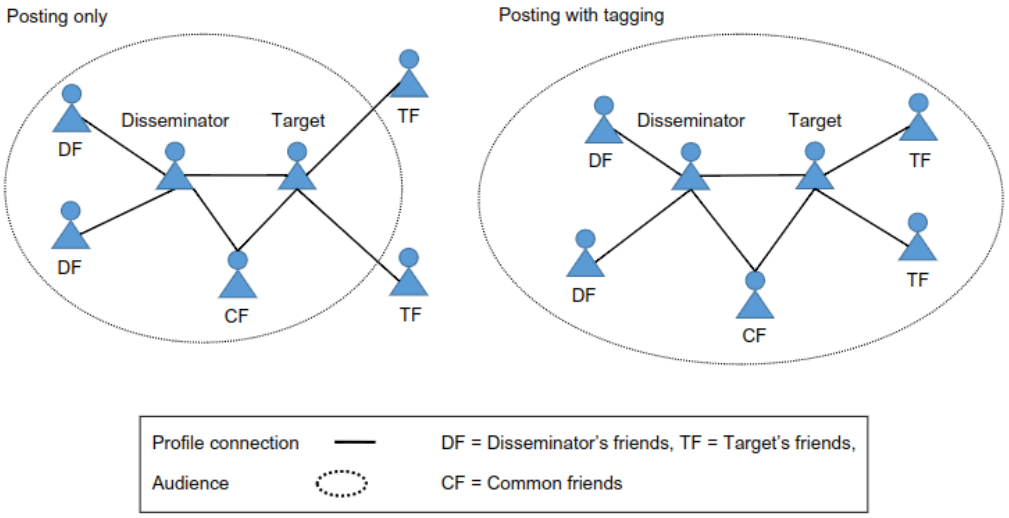


Figura 1. Esquema de diferencia en la audiencia entre sólo posteo (Posting Only) y posteo con etiquetado (Posting with Tagging), (Choi y colab., 2015).

Como se puede observar, se evidencia el poder de "propagación" del perfil del Usuario objetivo entre los distintos usuarios y roles que se conectan. Se hace la distinción con el modo de propagación en donde los usuarios "etiquetan" a otros usuarios en las publicaciones de los perfiles. En esos casos, se amplía la exposición porque explícitamente los usuarios son nombrados por las etiquetas.

Para comprender el contexto que presentan las redes sociales digitales, es interesante destacar lo que afirman los autores Srivastava y Geethakumari (2013) en su trabajo "Measuring Privacy Leaks in Online Social Networks": las redes sociales digitales se movieron desde un fenómeno de nicho hacia una adopción masiva por la población de usuarios. Esto significa que, en la última década, se usaron a las redes como plataformas para que los usuarios puedan comunicarse entre sí, intercambiar información, expresar sus sentimientos y construir relaciones con otros miembros de Internet. En el trabajo mencionado se presentan los resultados de una encuesta a un grupo de usuarios de un rango etario entre 16 y 45 años. En ella, se indagó sobre el nivel de conocimiento que tienen las personas sobre cómo una red social puede exponer la privacidad y hasta qué punto los usuarios conocen ese nivel de exposición. Lo que se obtuvo como información de interés, es que un 88% de ese grupo de personas frenarían el uso de una red social si encuentran que sus datos personales sensibles son usados de una manera no esperada por ellos. En contraposición, por medio de otra pregunta, los usuarios comentaron en su mayoría (63,3%) que el proceso de ajustar la privacidad de un perfil de una red social les genera una pérdida de tiempo y además es complejo o difícil de entender.

Uno de los conceptos interesantes propuestos en el trabajo de Srivastava y Geethakumari (2013) es el de "cálculo de la sensibilidad", el cual será empleado en este trabajo de tesis. La sensibilidad es la propiedad de la información que la convierte en privada. Empleando este concepto, se espera que, a mayor nivel de privacidad requerida, la sensibilidad de la información se incrementa. Por ende, es la información sensible, la que debe ser fuertemente protegida por parte de los usuarios. En relación con ello, los autores, proponen una tabla con los atributos de los perfiles que hacen a la sensibilidad de la información, la cual se presenta en la Figura 2.

Response	Percentage
1	Contact Number
2	E mail
3	Address
4	Birthdate
5	Home Town
6	Current Town
7	Job Details
8	Relationship status
9	Interests
10	Religious Views
11	Political Views

Figura 2. Lista de atributos de un perfil (Srivastava y Geethakumari, 2013)

Considerando cada uno de los ítems de la tabla mencionada (Número de contacto, E-mail, Domicilio, Fecha de nacimiento, Ciudad de origen, Ciudad de residencia, Detalles laborales, Estado de relación, Intereses, Preferencias religiosas, Preferencias políticas), se puede determinar el nivel de privacidad que el

usuario le brinda, según los hacen públicos o exponen, en contraposición con la sensibilidad asociada. Teniendo en cuenta los datos que se depositan en un perfil de una red social digital, todo ese contenido es catalogado según categorías, tal como se muestra en la anterior figura 2.

En relación con los atributos más sensibles de un perfil de usuario, aparece el concepto de “crawler” o “rastreador web”. Estos componentes, también llamados “bots de motor de búsquedas”, descargan e indexan contenido de la Web. Tienen como objetivo averiguar de qué tratan las páginas web, para que la información pueda ser recuperada cuando se necesite, por ejemplo, desde un buscador como Google o Bing. Como generalmente son operados por los motores de búsqueda, los datos recopilados por estos crawlers permiten proporcionar enlaces relevantes en respuesta a las consultas de búsquedas que hacen los usuarios y generar una lista de páginas web que coinciden con una búsqueda en Google, Bing u otro motor de búsqueda (Cloudflare, 2021).

Los rastreadores web son usados también para recopilar información de los perfiles existentes de usuarios en las redes sociales digitales. Existe un variado número de estos “bots” que se podrían considerar “aprovechadores” del nivel de exposición de los perfiles, ya que logran nutrirse de un conjunto importante de datos de distintos usuarios. El concepto de “crawler” en sí mismo no es malo, sino que su uso puede ser malicioso si se los utiliza para rastrear perfiles de personas expuestas con fines no éticos.

Continuando con los atributos sensibles que se pueden exponer en un perfil biográfico digital, las plataformas Instagram y Facebook tienen tecnología para hacer reconocimiento facial, es decir, reconocer las caras de las personas en una foto y de esa manera, etiquetar al usuario correspondiente. En el trabajo de investigación “Facial Recognition and Privacy Concerns on Social Media: A Study of Facebook and Instagram”, los autores mencionan cómo la tecnología de reconocimiento facial afecta la privacidad de los usuarios en estas plataformas. Se expone sobre el uso de algoritmos de reconocimiento facial para etiquetar a personas en fotos sin su consentimiento, y cómo esto puede aumentar la exposición de información personal. Además, pone en juego el concepto de vulnerabilidad de terceros. Es decir, cómo el uso de reconocimiento facial no solo afecta a quien publica una foto, sino también a usuarios relacionados que aparecen en esas imágenes y que no dieron consentimiento explícito para que sean identificadas.

La empresa Meta, creadora de Facebook, tiene su foco de desarrollo en el metaverso, mundo inmersivo por medio de realidad virtual y uso de avatares. En esos ámbitos, la privacidad también está en juego. De este tema, en el trabajo *"Privacy in the Metaverse: Addressing the Risks of Biometric Data Exposure in Immersive Social Networks"*, los investigadores analizan los riesgos de privacidad en el metaverso, específicamente relacionados con la exposición de datos biométricos en entornos inmersivos. El trabajo explora cómo las redes sociales inmersivas dentro del metaverso manejan la recolección y uso de datos

biométricos, y los riesgos que esto conlleva para la privacidad. Se destaca que la captura constante de datos para crear experiencias más realistas puede llevar a vulnerabilidades complejas sin precedentes. Además, los autores indican que las tecnologías inmersivas hacen más difícil mantener el anonimato de los usuarios, ya que la recopilación de datos biométricos puede identificar y rastrear a los individuos, incluso cuando no proporcionan información personal explícita. En conclusión, este trabajo de investigación evidencia los riesgos emergentes y las preocupaciones de privacidad asociados con el uso de tecnologías inmersivas y la recopilación de datos biométricos en redes sociales del metaverso, como el cao de las desarrolladas por Meta.

En relación con las redes sociales digitales vinculadas al ámbito profesional, de empleo, considerando LinkedIn como el exponente principal, existe un trabajo denominado *"Privacy Concerns in Professional Social Networks: An Analysis of LinkedIn Users' Perceptions and Practices"*, que analiza las percepciones y prácticas de privacidad de los usuarios de LinkedIn. Los autores destacan el concepto de equilibrio entre visibilidad y privacidad. Es decir, el análisis del dilema al que se enfrentan los usuarios entre maximizar su visibilidad para obtener oportunidades profesionales y, al mismo tiempo, proteger su privacidad. Se señala que muchos usuarios optan por compartir más información de la que les gustaría para obtener mejores conexiones o visibilidad laboral. Otro aspecto clave que el trabajo menciona, es la falta de transparencia en políticas de privacidad. Esto se muestra en que los usuarios a menudo no son conscientes de cómo se utiliza su información, lo que genera desconfianza hacia la plataforma.

En estos tiempos de desarrollo de la Inteligencia Artificial, también existe una relación con los conceptos de protección de la privacidad. Existe un trabajo llamado *"Artificial Intelligence and Privacy in Social Media: Opportunities and Risks"*, en donde se examina el impacto de la inteligencia artificial (IA) en la privacidad dentro de las redes sociales digitales. Los autores comentan al respecto del uso de la IA en plataformas como Facebook, Twitter e Instagram para mejorar la experiencia del usuario, personalizar contenidos y dirigir publicidad de manera más eficiente. Destacan que la IA permite analizar grandes volúmenes de datos y crear modelos predictivos sobre el comportamiento de los usuarios. Esto fomenta una recopilación de datos masiva y puede comprometer la privacidad. Un dato interesante que destacan los usuarios es que existen riesgos de manipulación dado a que se analiza cómo la IA puede ser utilizada para manipular el comportamiento de los usuarios, ya sea a través de la personalización extrema del contenido o la publicidad. Así mismo, los autores destacan las oportunidades de mejora en la privacidad que la IA puede aportar ayudando a minimizar la exposición de datos personales al entrenar modelos sin necesidad de acceder a los datos en bruto de los usuarios.

A nivel regional, durante el año 2014, como trabajo de investigación desarrollado en el Departamento Académico Rafaela de la Universidad Católica de Santiago del Estero, se llevó a cabo un proyecto investigación sobre la relación de los perfiles biográficos digitales frente a la personalidad real de una persona. Este trabajo fue una investigación interdisciplinaria en la que intervinieron especialistas de Psicología, Abogacía e Ingeniería en Informática. El objetivo se centró en la indagación sobre cuestiones como: las personalidades y el desarrollo de los perfiles de personas, las redes sociales y los perfiles virtuales, la incidencia en el desarrollo de la personalidad, la forma de exposición de las personas en un ambiente virtual y su relación con los conceptos de seguridad de la información, la garantía de privacidad y autenticidad de los contenidos publicados, y la vulnerabilidad de los datos presentados y publicados. El estudio estuvo dirigido a adolescentes entre los 16 y los 18 años de escuelas secundarias de la ciudad de Sunchales y Rafaela, a fin de lograr describir sus perfiles biográficos digitales.

Considerando este trabajo de referencia, es importante mencionar algunas de las conclusiones a las que se arribó, las cuales son relativas a la problemática de la privacidad y la exposición de los usuarios (Balbiano y colab., 2014):

- En los perfiles del grupo estudiado se detectó un número considerable de fotos publicadas con acceso público y alto acceso a la lista de amigos de los perfiles (efecto dominó, pasar de un perfil a otro).
- Facilidad para crear perfiles ficticios dentro de Facebook, con el único requisito de contar con una dirección de correo electrónico y definir un nombre asociado, sin tener que hacer una validación de la existencia de dicha identidad. Esto facilita que un usuario pueda crear perfiles que no correspondan específicamente con una persona real y de esa manera que sean de identidades ficticias.
- La mayoría de los adolescentes consideran que pronto Facebook será reemplazada por otra red social (incidencia de Twitter y comunicaciones por WhatsApp).
- Vulnerabilidad de los perfiles en cuanto a cuestiones legales: honor, propiedad intelectual, privacidad, injurias. Esto se debe a que, por la exposición de los perfiles analizados, los usuarios pueden estar sujetos a comentarios, descarga de sus fotos y otras acciones que atentan contra su real privacidad. Si bien sus perfiles están configurados de una manera “expuesta”, se requiere fortalecer la concientización de los usurarios para que limiten y cuiden lo que publican.
- Facilidad para realizar el rastreo de perfiles, sin otra herramienta más que el tiempo.
- Necesidad de realización de charlas/jornadas para generar conciencia sobre el uso seguro de las redes sociales.

El trabajo de investigación antes mencionado, continúa con una línea de trabajo iniciada en la misma institución académica en relación con la Seguridad de la información y conciencia en relación con el valor de los datos sensibles y críticos que manejan ciertas entidades. En ese sentido, durante el año 2012, se concretó un proyecto de investigación denominado “Cultura de la información digital en el ámbito empresarial”. Se trató de un trabajo encarado en forma interdisciplinaria entre especialistas del área Jurídica e Ingenieros en Computación. El objetivo fue indagar a partir de la aplicación de instrumentos cualitativos y cuantitativos sobre el conocimiento y la utilización de los conceptos asociados con la seguridad de la Información Digital enmarcados dentro de los ámbitos empresariales de la ciudad de Rafaela para determinar la cultura de la información que caracterice la forma de manejar este recurso (Zehnder y colab., 2012).

2.3 Normativa nacional con respecto a la privacidad de las personas

Dentro del análisis bibliográfico, cabe mencionar normativa argentina vigente con respecto a la privacidad de las personas, lo que define el marco legal dentro del cual se desarrolla la presente tesis.

Para empezar, es importante traer a colación lo que la Constitución Nacional argentina establece en cuanto a este preciado derecho en su artículo 19: “Las acciones privadas de los hombres que de ningún modo ofendan al orden y a la moral pública, ni perjudiquen a un tercero, están sólo reservadas a Dios, y exentas de la autoridad de los magistrados. Ningún habitante de la Nación será obligado a hacer lo que no manda la ley, ni privado de lo que ella no prohíbe.” (Constitución Nacional de la República Argentina, 1853).

Continuando con la legislación de Argentina, la Ley 25.326 de Protección de los Datos Personales, tiene por objeto la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean estos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el artículo 43, párrafo tercero de la Constitución Nacional (Ley 25.326, 2000). En su Artículo 2, se definen los siguientes conceptos:

- Datos personales: Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables.
- Datos sensibles: Datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual.

Considerando la definición de los dos tipos de datos, la exposición en una red social digital puede poner en riesgo el propósito que se busca con esta Ley, la de la protección integral de las personas. Principalmente, los datos sensibles son sobre los cuales deben hacer énfasis las medidas de seguridad y sobre los que es necesario generar conciencia en los usuarios para que consideren las posibles consecuencias de compartirlos en ámbitos que indudablemente salen del círculo íntimo, como una red social digital.

En el año 2006, la Dirección Nacional de Protección de Datos Personales, formuló la disposición 11/2006 titulada “Medidas de Seguridad para el Tratamiento y Conservación de los Datos Personales Contenidos en Archivos, Registros, Bancos y Bases de Datos Públicos no estatales y Privados”. En la misma se establecen tres niveles de seguridad: Básico, Medio y Crítico, conforme la naturaleza de la información tratada. Además, dicha disposición indica para cada uno de esos niveles distintas medidas de seguridad, teniendo en cuenta la mayor o menor necesidad de garantizar la confidencialidad e integridad de la información contenida en el banco de datos, la naturaleza de los datos y la correcta administración de los riesgos a los que están expuestos, así como también el mayor o menor impacto que tendría en las personas el hecho de que la información registrada en los archivos no reúna las condiciones de integridad y confiabilidad debidas (Disposición 11/2006, 2006).

Considerando lo expresado en la disposición, se puede reconocer toda la información contenida en una red social digital en relación con una persona como “información registrada en archivos”, ya que los perfiles permiten “registrar” todos sus datos “personales”. Por ende, y tomando como base esta disposición amparada por la Ley 25326, cada uno de los repositorios en los cuales se depositen datos personales de las personas tendrían que ofrecer las garantías sobre la confidencialidad, integridad y disponibilidad. Más allá de la importancia que tiene la ley, para que ésta pueda implementarse y cumplirse debería instaurarse un esquema de auditoría y control sobre cada repositorio, siendo esto muy complejo para alcanzar a las redes sociales digitales, dado que salen de la jurisdicción propia de Argentina, por sus orígenes en otros países donde rigen sus propias políticas.

Un dato interesante y tener en cuenta sobre la Disposición 11/2006 reside en su última nota: “Quedan exceptuados de aplicar las medidas de seguridad de nivel crítico, los archivos, registros, bases y bancos de datos que deban efectuar el tratamiento de datos sensibles para fines administrativos o por obligación legal. No obstante, ello no excluye que igualmente deban contar con aquellas medidas de resguardo que sean necesarias y adecuadas al tipo de dato”. Podría considerarse una “puerta abierta” para que la exposición y acceso a datos personales sea permitido bajo “las órdenes de la Ley”. Sin embargo, la misma Dirección Nacional de Protección de Datos Personales, formuló la disposición 39/2015 que establece un procedimiento de “Inspección electrónica” de control de las actividades de los responsables de bases de datos, los datos personales que administran, los medios y la forma con los que lo hacen y el nivel de cumplimiento de las obligaciones que surgen de la Ley N° 25.326 (Disposición 39/2015, 2015). Con este esquema se podría indicar que, si se cumpliese este procedimiento, existiría alguna garantía para los usuarios de plataformas en las que depositan su información personal, y podría constituir una herramienta para las personas, para proteger y salvaguardar sus datos personales y, por ende, su exposición.

Un dato importante para mencionar es que la ley 25.326 de protección de datos personales data del año 2000 por lo que requiere de una revisión de la misma. Actualmente existe un proyecto de ley para reemplazar esta ley con una más moderna.

En primera instancia hubo un intento de actualización de la actual Ley en el año 2018. Sin embargo, perdió estado parlamentario.

Luego, se presenta la nueva propuesta para el año 2022. En base a lo publicado en el Sitio Web oficial Argentina.gob.ar, este proceso de actualización se inició en septiembre del mencionado año por medio de una instancia de consulta pública, buscando garantizar la participación de la ciudadanía. Como resultado de ese proceso, se recibieron **173 opiniones, aportes y comentarios** presentados por **123 participantes** correspondientes a la ciudadanía en general, organizaciones de la sociedad civil, universidades e investigadores, sector privado y sector público nacional e internacional. Tomando ese debate como resultado, se presentó un **Nuevo Proyecto de Ley de Protección de Datos Personales**[2][3][4][5].

A continuación, se enumeran alguno de los cambios propuestas en esta nueva Ley:

- Incorporación de nuevas definiciones de conceptos como: Anonimización, Datos Biométricos y Datos genéticos, entre otros.
- Regula la aplicación extraterritorial de la Ley.
- Regula específicamente el tratamiento de los datos personales de los menores de edad.
- Introduce la figura del delegado de protección de datos y la obligación de nombrarlo en ciertos supuestos.
- Establece la obligatoriedad para el responsable de reportar incidentes de seguridad a la autoridad de control y, dependiendo de las circunstancias, al titular del dato.
- Define la Agencia de Acceso a la Información Pública como autoridad de control y aplicación de la ley, encargada de supervisar el cumplimiento de las disposiciones de protección de datos.
- Establece sanciones para quienes incumplan la ley, que pueden incluir multas económicas, suspensiones temporales o definitivas de la posibilidad de tratamiento de datos, y otras medidas correctivas.

[2] https://www.argentina.gob.ar/aaip/datospersonales/proyecto-ley-datos-personales
[3] proyecto_de_ley_de_datos_personales_aaip.pdf (argentina.gob.ar)
[4] proyecto_leypdp2023.pdf (argentina.gob.ar)
[5] https://www.marval.com/publicacion/nuevo-anteproyecto-busca-reemplazar-la-ley-de-proteccion-de-datos-argentina-14307&lang=es

Capítulo 3: Condiciones de privacidad de cada Red Social Digital seleccionada.

El desarrollo de este trabajo iniciará con el análisis de un conjunto de Redes Sociales Digitales, colocando el foco en sus políticas de privacidad, las opciones provistas que permiten al usuario configurar los atributos de su privacidad y la de su entorno de contactos, y la manera en que diferentes tipos de personas hacen uso de este escenario, determinando los niveles de exposición de la información que publican.

3.1. Alcance

El grupo de Redes Sociales Digitales seleccionadas para ser estudiadas se define considerando un conjunto de estadísticas de uso de éstas a nivel mundial. Las fuentes de estos estudios se basan en las siguientes entidades de estudios estadísticos:

- We Are Social: https://wearesocial.com/: Esta empresa inició sus trabajos en colaboración con la plataforma Hootsuite (https://hootsuite.com). Se debe destacar que este producto Hootsuite nació como herramienta para gestionar múltiples plataformas de redes sociales en un mismo portal pensado específicamente para el ámbito profesional / empresarial, de manera de mantener centralizada la administración de los perfiles biográficos digitales y potenciar la relación con clientes y contactos en general. En la actualidad, We Are Social está asociada con la empresa Meltwater (https://www.meltwater.com/). La misma ofrece servicios de inteligencia de medios, redes sociales, consumidores y ventas. Todos los años, We Are Social genera el reporte "Global Digital Report", partiendo de varias fuentes de datos, mencionadas dos en esta lista a continuación. De ese reporte mencionado, una sección particular es sobre las redes sociales digitales y tienen elaborado un ranking de las más utilizadas. En particular para este proyecto de Tesis se toma el reporte del año 2023. (Kemp, 2020)
- Statista: https://www.statista.com/. Según la información de su sitio corporativo, es una plataforma global de datos e inteligencia empresarial con una amplia colección de estadísticas, informes e información sobre más de 80.000 temas de 22.500 fuentes en 170 industrias. Incluye reportes específicos sobre la tendencia en el uso de las Redes Sociales.
- Global Web Index: https://www.globalwebindex.com/. Como se describen, indican que son la empresa líder en segmentación de audiencias para la industria del marketing global, mostrando cómo piensan los consumidores. Cuenta con un reporte anual que se denomina "The ultimate social media trends report".

Tomando como base el análisis de Statista en relación a la cantidad de usuarios por cada Red Social Digital, se tiene el siguiente ranking (Figura 3) tomado en enero de 2024:

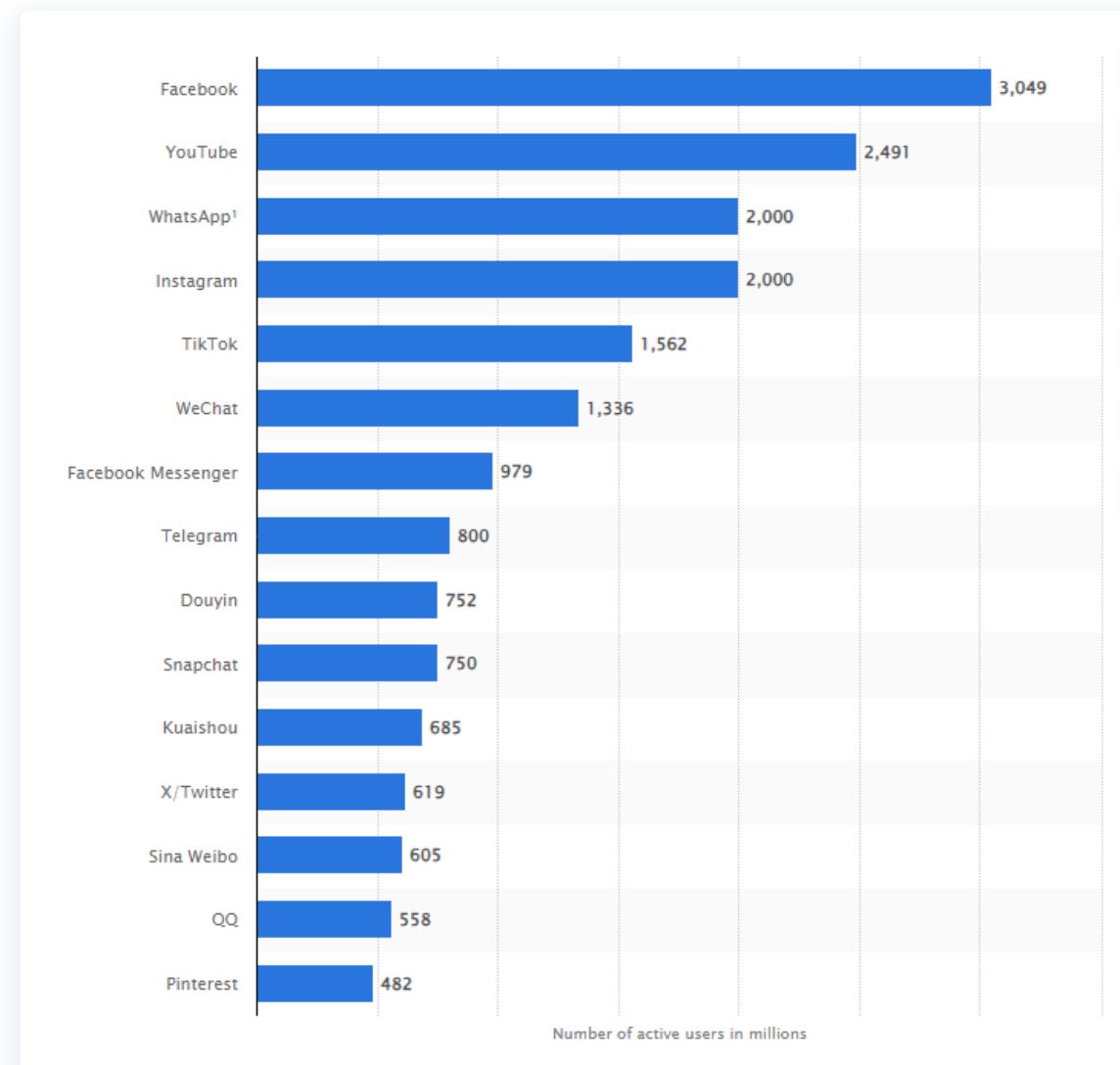


Figura 3. Ranking Cantidad de Usuarios por Red Social Digital (Statista, 2024)

Considerando el estudio estadístico de “We Are Social” del año 2024 (Figura 4), se indica que del total de usuarios de Internet a nivel mundial (5,35 billones), unos 5,04 billones son usuarios activos de redes sociales. En consiguiente se evidencia una penetración aproximada del 94.2%. Es un alto valor que muestra qué lugar ocupan las redes sociales digitales en los usuarios de Internet hoy en día.

En el mismo estudio, se indica que, en promedio, un usuario pasa 6 horas y 40 minutos usando Internet y que, sobre ese tiempo, dedica 2 horas y 23 minutos en promedio para usar redes sociales (Figura 5).

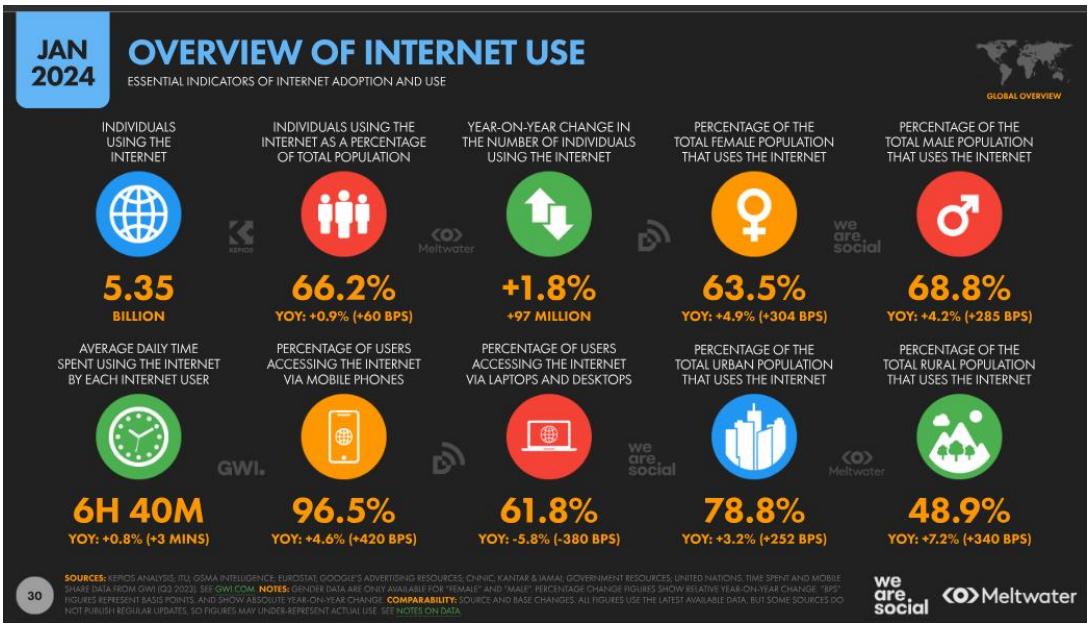


Figura 4. Resumen Global de Uso de Internet (We Are Social, 2024)

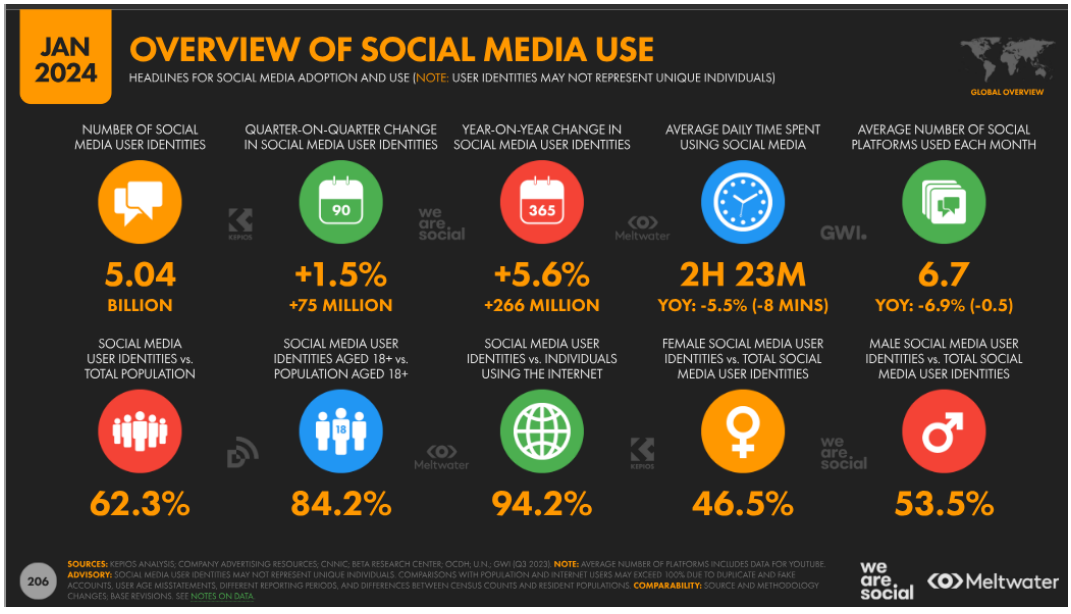


Figura 5. Resumen Global de Uso de las Redes Sociales (We Are Social, 2024)

En conclusión, una tercera parte del tiempo que pasa un usuario en Internet lo hace con Redes Sociales Digitales.

Siguiendo con el estudio de “We Are Social” mencionado, en relación con las plataformas de redes sociales más utilizadas en el mundo, el predominio lo tiene Facebook en cuanto a cantidad de usuarios en millones. A continuación, en la Figura 6, se muestra una captura de dicha sección del reporte:

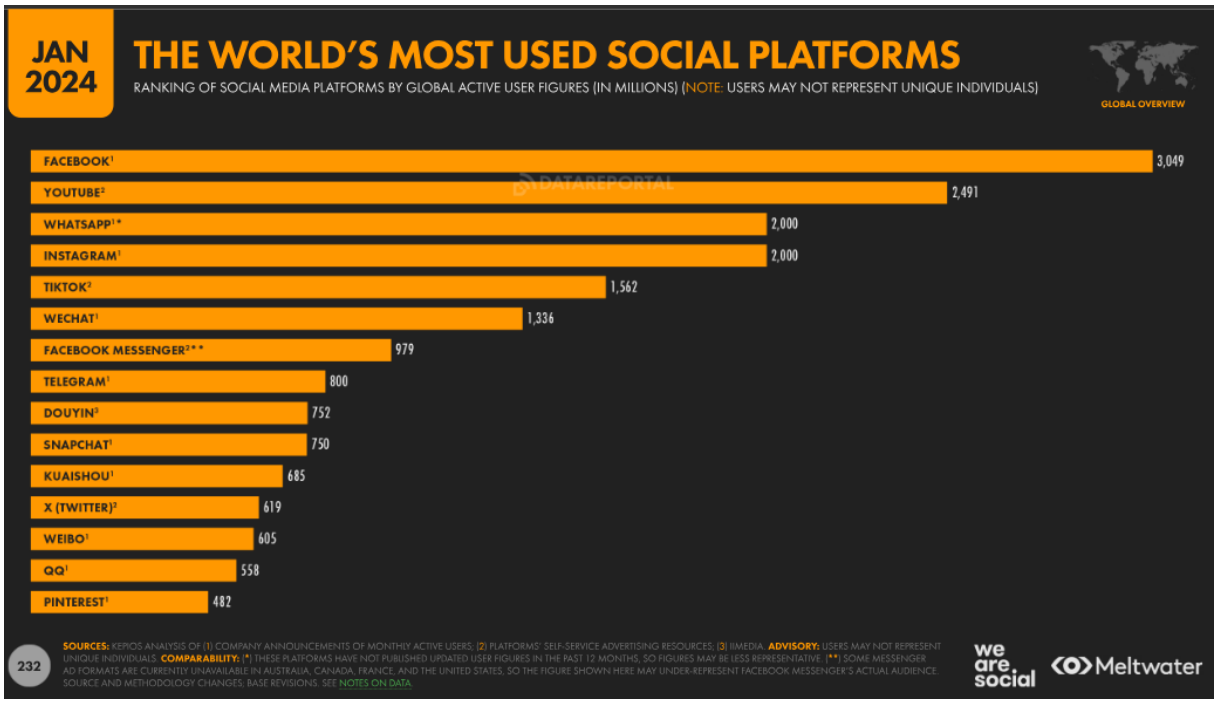


Figura 6. Ranking de Plataformas de Redes Sociales Digitales más Usadas (We Are Social, 2024)

Del estudio de "The Global Web Index", en promedio una persona invierte entre 2 y 3 horas y 32 minutos en una red social, según la región mundial. Este reporte clasifica las mediciones en las regiones de Latinoamérica, África y Medio Oriente, Norteamérica, Europa y Asia. Dicho valor se corresponde con el reportado por "We are social". Por otro lado, como se observa en la siguiente Figura 7, con el extracto del reporte, ese valor se fue incrementando desde el año 2020 a la fecha.

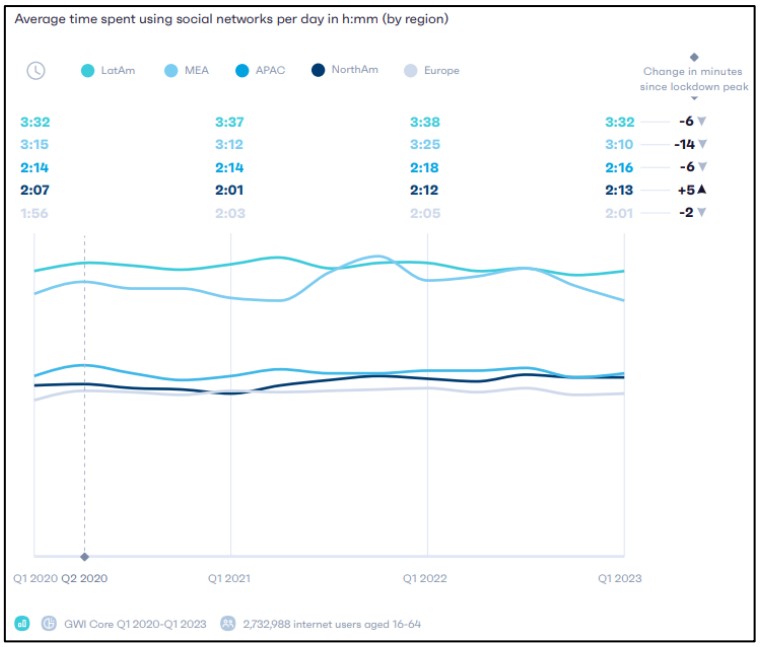


Figura 7. Tiempo Promedio Invertido por Red Social Digital (The Global Web Index, 2024)

En particular, este valor es importante ya que representa el momento en el que la exposición de una persona entra en juego, donde es importante que la persona tenga el criterio para cuidar y saber qué y cómo publicar lo que se necesita, pero sin pasar la línea de la privacidad y dejar la puerta abierta para un ataque.

"We Are Social" también ha elaborado un reporte que considera a la preocupación general de las personas en relación a cómo su información personal es manejada por las compañías, incluyendo las Redes Sociales Digitales. Se muestra continuación en la Figura 8.

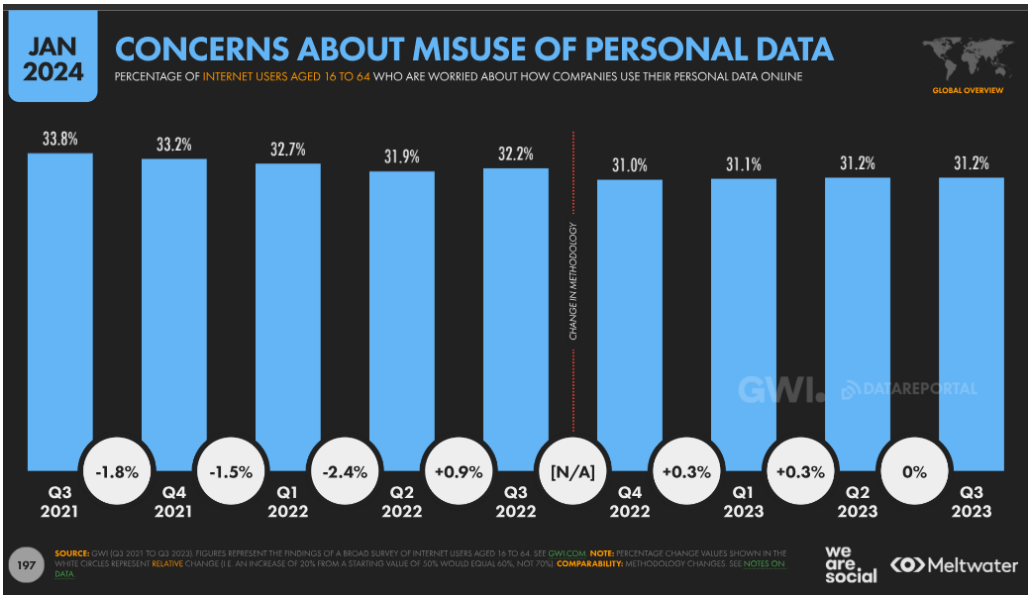


Figura 8. Evolución porcentual sobre las preocupaciones de los usuarios por el uso indebido de datos personales (We Are Social, 2024).

En dicho el reporte, se muestra el porcentaje de usuarios de Internet de entre 16 y 64 años que están preocupados por cómo las empresas utilizan sus datos personales en línea. Lo llamativo es que, a lo largo del tiempo, desde 2021, prácticamente no se evidencia un crecimiento sino un valor estacionado. El mismo no supera el 33%.

De la mano del estudio presentado anteriormente, We Are Social incluyó también el reporte sobre las preocupaciones de los usuarios en relación a la información no real o falsa que circula por Internet. Se muestra en la siguiente Figura 9:

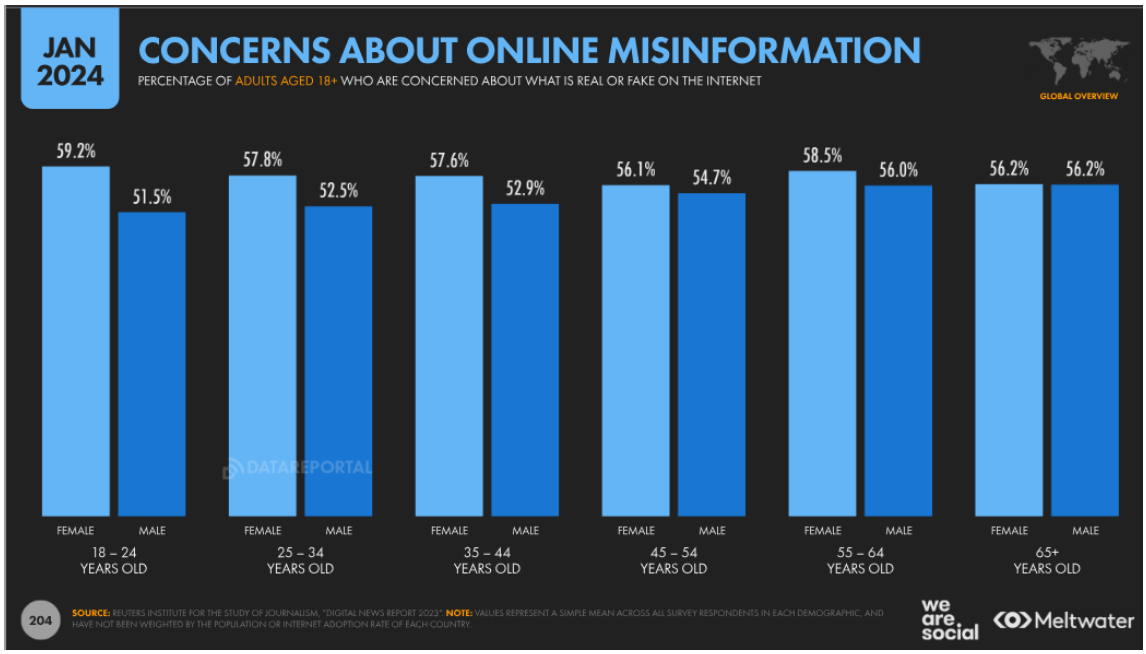


Figura 9. Porcentaje de adultos mayores de 18 años a quienes les preocupa lo que es real o falso en Internet (We Are Social, 2024).

De la figura presentada, se evidencia que el porcentaje de usuarios preocupados por la desinformación online publicada en Internet es uniforme para cada rango etario de adultos mayores a 18 años, no superando el 60%. Por ende, y considerando los estudios en relación a la cantidad de usuarios globales que usan Redes Sociales, el tiempo promedio diario invertido y su nivel de preocupación en relación a cómo su información personal es administrada por las empresas, se presenta un punto de análisis y desarrollo que motiva al desarrollo de esta Tesis.

Teniendo en cuenta los reportes de análisis de redes sociales presentados, por la presencia de utilización a nivel global, se decide considerar a las siguientes plataformas para el relevamiento de esta Tesis:

- Facebook
- Instagram
- LinkedIn

En el caso de LinkedIn, esta red social se incluye en el desarrollo de esta Tesis porque representa la plataforma más importante para el ámbito laboral / profesional. Es el lugar usado para presentar los perfiles de trabajo de los usuarios y es donde las empresas ponen foco a la hora de nuevas incorporaciones a sus carteras de empleados. Así mismo, la bolsa de empleo es muy consultada por las personas, incluyendo procesos ágiles para las postulaciones.

Es importante mencionar que, en el año 2012, Facebook adquirió Instagram. En el momento de la adquisición, Instagram tenía alrededor de 30 millones de usuarios. Facebook detectó en Instagram una

plataforma complementaria que podría ayudar a fortalecer su posición en el mercado de las redes sociales móviles y atraer a un público más joven que estaba utilizando cada vez más Instagram en lugar de Facebook. Tras la compra, Instagram siguió operando como una entidad separada dentro de Facebook, manteniendo su marca y su aplicación independiente. Lo que sucedió posteriormente, fue que Facebook ha integrado gradualmente algunas funciones y características de Instagram en su plataforma principal, como la posibilidad de compartir publicaciones de Instagram en Facebook. En su camino de expansión, Facebook compra WhatsApp durante 2014, ampliando así su universo de las Redes Sociales Digitales.

Continuando con el desarrollo de Facebook, durante el mes de octubre de 2021, dicha empresa anunció que cambiaba su nombre corporativo a Meta Platforms, Inc., reflejando su enfoque en la creación de un metaverso. Se puede definir a metaverso como un espacio virtual compartido en línea donde las personas pueden interactuar entre sí con contenido digital en tiempo real. Las aplicaciones y servicios existentes de la empresa, como Facebook, Instagram, WhatsApp y Oculus (la división de realidad virtual) no tuvieron cambios y siguieron operando normalmente. Como complemento, existió un rediseño de la identidad visual de la empresa, con un nuevo logotipo y una nueva imagen de marca que reflejan la visión del metaverso. Tal como se presenta en el sitio web oficial de Meta[6], hay un apartado especial para mostrar todo los relacionado a esta tecnología. Como dice el fabricante el metaverso es la evolución de la conexión social y el sucesor de internet en el celular. Al igual que internet, el metaverso ayuda a las personas conectarse cuando no están físicamente en el mismo lugar y las acerca aún más a la sensación de estar juntas en persona.

3.2. Análisis de las condiciones de privacidad en cada Red Social Digital seleccionada

A continuación, se describirán los aspectos más relevantes vinculados a la exposición de las personas que se identifican en cada una de las condiciones de privacidad analizadas para las redes sociales digitales que forman parte de este trabajo: Facebook, Instagram y LinkedIn. Además, se enumerarán los puntos principales que tienen relación a las normas y protocolos que brindan las redes sociales digitales seleccionadas, sobre el tratamiento de los datos propios de los usuarios.

El recorrido por cada una de las condiciones de privacidad tiene base en los siguientes puntos de análisis:

1. Fecha última actualización de las políticas de privacidad

[6] Sitio Web oficial de Meta sobre el Metaverso: ¿Qué es el metaverso? | Meta

2. ¿Notificación previa de cambio de política?
3. Datos que se recopilan
4. Objetivo de los datos que recopilan
5. Posibilidad de eliminación de cuenta / datos
6. Posibilidad de consulta / reclamo

3.2.1. Facebook + Instagram[7]

En el caso de Facebook, la política de privacidad aplica también para Instagram por considerarse un producto asociado. Dichas Redes Sociales Digitales son parte de la empresa Meta. El nombre que usan es “Política de Privacidad”.

3.2.1.1. Fecha de última revisión: 26 junio de 2024

A continuación, se comparte la introducción que describe el propósito de la política. Con la siguiente frase, Meta presenta su política de Datos: “En Meta, queremos que comprendas qué información recopilamos y cómo la usamos y compartimos. Por eso, te recomendamos leer nuestra Política de privacidad. Esto te ayudará a usar los “Productos de Meta” de un modo que te resulte conveniente. En la Política de privacidad, se explica cómo recopilamos, usamos, compartimos, retenemos y transferimos información. También te informamos cuáles son tus derechos. Cada sección de la Política incluye ejemplos útiles y un lenguaje más simple para que nuestras prácticas sean más fáciles de comprender. También agregamos enlaces a recursos que ofrecen más información sobre los temas de privacidad que pueden interesarte.”

A continuación, se enumeran los “Productos de Meta” que se relacionan con esta Política de Privacidad:

- Facebook
- Messenger
- Instagram
- Productos de Facebook Portal
- Los productos de Meta Platforms Technologies, como Meta Horizon Worlds o Meta Quest (cuando se usa una cuenta de Facebook o Meta)
- Tiendas
- Marketplace
- Meta Spark

[7] Link acceso “Condiciones de Facebook + Instagram”: https://www.facebook.com/policy.php/

- Productos comerciales, como las herramientas empresariales de Meta y Meta Business Suite
- Meta Audience Network
- Facebook View
- Meta Pay
- Experiencias de finalización de compra de Meta

3.2.1.2. Notificación previa de cambio de política:

Según mencionan en la política, se tiene en cuenta una notificación previa a los usuarios: "Antes de realizar cambios sustanciales en esta política, te lo notificaremos. Tendrás la oportunidad de leer la política revisada antes de decidir continuar usando nuestros Productos."

3.2.1.3. Datos que se recopilan:

"La información que recopilamos y tratamos sobre ti depende de la forma en la que usas nuestros Productos."

Considerando la introducción a esta sección, Facebook deja en claro que los usuarios son responsables de qué nivel de información se recopila, todo dependiente de cómo usan la plataforma.

A continuación, se enumera la información recopilada por esta red social, la cual se presenta clasificada en categorías:

Tu actividad y la información que proporcionas.

Se indica que "actividad" significa todo lo que el usuario puede hacer a través de los productos de Meta. Esto incluye los siguientes tópicos:

a) Información que proporciona el usuario: por ejemplo, al momento de crear una cuenta de Facebook o Instagram se recopila:
   I. Contraseña
   II. Correo electrónico
   III. Número de teléfono
   IV. Toda información solicitada en el proceso.

   En este tópico se recopila también información cuando el usuario crea su Avatar, completa un formulario o se contacta por algún motivo con Facebook o Instagram.
b) Contenido que se crea, como publicaciones, comentarios o audio.
c) Contenido que se proporciona a través de la función de cámara o la configuración de la galería, o mediante funciones de voz. Esto incluye:

I. Manera en que se usan las funciones de la cámara. Ejemplo: si se selecciona un efecto de fondo para la foto a tomar entonces se recopila información de la cámara para poder aplicar correctamente dicho filtro.
II. Interacción de voz con el asistente de funciones por voz.

d) Los mensajes que se envían y reciben, incluido su contenido, conforme a la legislación aplicable. Aclara Meta que no pueden ver el contenido de los mensajes cifrados de extremo a extremo, a menos que los usuarios los reporten para que la empresa los revise.
e) Metadatos sobre contenido y mensajes, conforme a la legislación aplicable. Esto incluye:
   I. Información sobre el contenido en sí mismo, como la ubicación donde se tomó una foto o la fecha en la que se creó un archivo.
   II. Información sobre el mensaje en sí mismo, como el tipo de mensaje o la fecha y la hora en la que se envió.
f) Tipos de contenido, incluidos anuncios, que el usuario veo o con el que interactúa, y la manera en que lo hace.
g) Apps y funciones que se usan, y las acciones que el usuario realiza en ellas. Esto incluye:
   I. Apps, publicaciones, videos, anuncios, juegos, tiendas y otro contenido que el usuario ve o con los que interactúa en los Productos.
   II. Funciones a las que se accede desde los productos de mensajes.
   III. Cuando se usan plugins sociales, inicio de sesión con Facebook, autocompletar o historial de enlaces del navegador de la aplicación.
   IV. Información sobre sitios web que visita el usuario o con los que interactúa cuando se emplea el navegador de la aplicación. El navegador de Facebook o Instagram utiliza la tecnología estándar del sector para que los usuarios puedan ver y realizar acciones en los sitios web sin salir de la plataforma de Red Social Digital.
h) Compras u otras transacciones que se realizan, por ejemplo, a través de experiencias de finalización de compra de Meta, incluida la información de tarjetas de crédito. Ejemplos:
   I. Compras dentro de un juego online.
   II. Donaciones a la recaudación de fondos de un amigo.
   III. Compras en Marketplace, tiendas o grupos.
   IV. Compras realizadas utilizando Meta Pay u otras experiencias de finalización de compra de Meta.
   V. Transferencias de dinero a amigos y familiares.

i) Hashtags que los usuarios emplean.

j) El tiempo, la frecuencia y la duración de las actividades en cada Producto.

Amigos, seguidores y otras conexiones.

a) Información que se recopila sobre amigos, seguidores y otras conexiones.
   I. Esto incluye información sobre amigos, seguidores, grupos, cuentas, páginas de Facebook y otros usuarios y comunidades con los que los usuarios se conectan e interactúan.
   II. Además, incluye cómo es la interacción en los Productos y con cuáles se interactúa más.

b) Información que se recopila sobre los contactos. Se incluye:
   I. Nombre y dirección de correo electrónico o número de teléfono
   II. En el caso de elegir subir o importar la información desde un dispositivo (por ejemplo, al sincronizar la libreta de direcciones). Los dispositivos incluyen computadoras, teléfonos, hardware, televisores conectados, dispositivos Portal y otros dispositivos conectados a la web.

c) Información que se recopila o se infiere sobre los usuarios en función de la actividad de otras personas.
   I. En cuanto a recopilación. Por ejemplo, cuando otras personas:
      i. Comparten o comentan una foto en la que se etiquetó al usuario.
      ii. Envían un mensaje al usuario.
      iii. Invitan al usuario a unirse a una conversación.
      iv. Suben su libreta de direcciones, que tiene la información de contacto del usuario.
      v. Invitan al usuario a jugar un juego.
   II. En cuanto a ingerir, se toman algunos aspectos sobre el usuario en función de la actividad de otros. Por ejemplo:
      i. Sugerir un amigo a través de la función "Personas que quizá conozcas" de Facebook si ambas personas aparecen en la lista de contactos que alguien subió.
      ii. Se tiene en cuenta si los amigos del usuario pertenecen a un grupo cuando Facebook sugiere su unión.

Información de la aplicación, el navegador y el dispositivo

Se menciona que Facebook e Instagram recopilan y reciben información de los diferentes dispositivos que los usuarios emplean, la manera en que se utilizan, así como datos sobre dichos dispositivos. Dentro de estas categorías se incluye:

a) El dispositivo y el software junto con otras características del dispositivo:

I. Tipo de dispositivo
II. Detalles sobre su sistema operativo
III. Detalles sobre su hardware y software
IV. Marca y modelo
V. Nivel de la batería
VI. Intensidad de la señal
VII. Almacenamiento disponible
VIII. Tipo de navegador
IX. Nombres y tipos de aplicaciones y archivos
X. Plugins

b) Lo que el usuario está haciendo en su dispositivo. Ejemplo: si Facebook/Instagram está en primer plano o si el mouse se está moviendo.
c) Identificadores que diferencian a cada dispositivo de los dispositivos de los demás usuarios, incluidos los identificadores de dispositivo de la familia:
    I. Identificadores de dispositivos.
    II. Identificadores de anunciantes en celulares, juegos, aplicaciones o cuentas que se usan.
    III. Identificadores de dispositivos de la familia.
    IV. Identificadores exclusivos de los productos de las empresas de Meta asociados con la misma cuenta o el mismo dispositivo.
d) Señales de los dispositivos:
    I. GPS.
    II. Señales de Bluetooth.
    III. Puntos de acceso a wifi cercanos.
    IV. Balizas y torres de telefonía celular.
e) Información que el usuario compartió con Facebook/Instagram a través de la configuración del dispositivo. Ejemplos:
    I. Ubicación GPS.

II. Acceso a la cámara, fotos y metadatos relacionados. Estos metadatos provienen de las fotos y videos de los usuarios que tienen en sus galerías. Incluyen la fecha y la hora en la que se crearon. La plataforma indica que usan esa funcionalidad, por ejemplo, para recordar a los usuarios cuando tienes fotos nuevas que subir.

f) Información sobre la red a la que los usuarios conectan sus dispositivos, incluida la dirección IP:

I. Nombre del operador de telefonía celular o proveedor de servicios de internet.

II. Idioma.

III. Zona horaria.

IV. Número de teléfono celular.

V. Dirección IP.

VI. Velocidad de conexión y descarga.

VII. Capacidad de la red.

VIII. Información sobre otros dispositivos que están cerca de la red o en la misma red.

IX. Zonas wifi con las que los usuarios se conectan al usar los Productos de Meta.

La plataforma indica que uno de los motivos por los recopilan esta información es para mejorar la experiencia. Por ejemplo, si saben que el teléfono y el televisor del usuario están conectados a la misma red, entonces pueden ayudar a usar el teléfono para controlar una transmisión de video en el televisor.

g) Cierta información relacionada con la ubicación, aunque los servicios de ubicación estén desactivados en la configuración del dispositivo. Esto incluye:

I. Usar direcciones IP para estimar la ubicación general del usuario.

II. Actividad y la de otros en los Productos, como el case de registros de visitas y eventos.

III. Información que los usuarios proporcionan directamente, como cuando ingresan su ciudad actual en el perfil o proporcionan la dirección en Marketplace (espacio de compra/ventas de productos).

IV. Lugares que les gusta visitar a los usuarios.

V. Negocios y las personas que se encuentran cerca de los usuarios.

h) Información sobre el rendimiento de los Productos en los dispositivos de los usuarios. Esto incluye:

I. Tiempo en que la aplicación estuvo funcionando.

II. Modelo de dispositivo que se estaba usando.

i) Información de cookies (pequeños fragmentos de texto que se utilizan para almacenar información en navegadores web) y tecnologías similares.

Información de socios, proveedores y otros terceros

La plataforma indica que recopilan y reciben información de socios, proveedores de medición, proveedores de marketing y otros terceros sobre una variedad de información y actividades que los usuarios realizan dentro y fuera de los Productos como Facebook e Instagram.

Los Socios pueden ser personas, empresas, organizaciones o entidades que utiliza o integran los Productos de Meta para promocionar o anunciar sus productos o servicios, u ofrecer soporte en relación con ellos. Estos son algunos ejemplos:

- Anunciantes
- Negocios y personas que usan los Productos para vender u ofrecer bienes y servicios
- Editores y sus proveedores de servicios de medición
- Desarrolladores de aplicaciones
- Desarrolladores de juegos
- Fabricantes de dispositivos, proveedores de servicios de internet y operadores de red móvil
- Plataformas de comercio electrónico

Los **proveedores de marketing** respaldan las iniciativas de marketing y publicidad de Meta por medio de lo siguiente:

- Publican los anuncios en internet, incluido en celulares, computadoras y televisores conectados.
- Hacen un seguimiento de la actividad online de los usuarios y en la aplicación para celulares.
- Brindan información a Meta sobre los intereses de los usuarios y las interacciones publicitarias y de la comunidad.

En el caso de **Otros terceros**, se incluye:

- Fuentes públicas, como documentos académicos y foros públicos.
- Colegas del sector, como otras plataformas online y empresas de tecnología.

- Proveedores de servicios de marketing y publicidad y de datos, que tienen derecho a proporcionar la información de los usuarios.
- Empresas u organizaciones que proporcionan contenido, incluidos videos, fotos y audio.
- Autoridades policiales.
- Autoridades gubernamentales.
- Grupos de profesionales y grupos sin fines de lucro, como ONG, y organizaciones benéficas.
- Instituciones académicas y de investigación, como universidades, grupos de investigación sin fines de lucro y grupos de expertos.

A continuación, se muestran algunos ejemplos de información que Meta recibe de los usuarios:

- Información de los dispositivos. Descripta en sección 3.3:
- Sitios web que el usuario visita y datos de cookies.
- Aplicaciones que emplea el usuario.
- Juegos que se usan.
- Compras y transacciones que los usuarios realizan fuera de los Productos a través de experiencias de finalización de compra que no son de Meta.
- Datos demográficos, como el nivel de formación.
- Anuncios que los usuarios ven y cómo interactúan con ellos.
- Cómo se usan los productos y los servicios de los socios online o en persona.
- Dirección de correo electrónico
- Cookies e identificador de publicidad en el dispositivo.
- Comunicaciones que los Socios mantienen con los usuarios.

Información que se recopila y recibe si los usuarios interactúan con Facebook e Instagram, pero no tienen una cuenta

La plataforma indica que los usuarios pueden utilizar los Productos de Meta o interactuar con ello incluso sin tener una cuenta asociada. Esto significaría que esos usuarios no tendrían un perfil biográfico digital definido para Facebook / Instagram. En esos casos, se recopila información como las siguientes:

I. Registros de navegadores y aplicaciones de las visitas de los usuarios a contenido público, como páginas de Facebook, videos y salas.

II. Información básica sobre dispositivos que descargaron las aplicaciones de Meta, como el modelo y sistema operativo.

III. Información por medio de cookies y tecnologías similares; cuando se visitan otras aplicaciones y sitios web que usan las herramientas empresariales u otros Productos de Meta.

3.2.1.4. Objetivo de los datos que recopilan.

- Proporcionar, personalizar y mejorar los productos de Facebook / Instagram.
- Hacer sugerencias (a grupos o eventos) de interés.
- Crear productos personalizados únicos y relevantes para los usuarios.
- Personalizar las funciones y el contenido (incluidos la sección de noticias, el feed de Instagram, Instagram Stories y los anuncios)
    - El feed es la página principal de Instagram en la que se muestran las publicaciones en modo de cuadrícula ordenadas de manera cronológica por fecha de publicación.
    - Las Stories o historias son publicaciones que hace el usuario por una duración de 24 horas. Luego, se eliminan públicamente del perfil. En algunas ocasiones el usuario puede “destacar” una historia de manera que quede visible en una sección especial del perfil.
- Hacer sugerencias (como grupos o eventos).
- Sugerir temas para seguir tanto dentro como fuera de los Productos de Meta.
- Proporcionar una experiencia más personalizada. Ejemplo: sugerencia de unión a un grupo en Facebook que incluye a personas que un usuario sigue en Instagram o con las que se comunica por medio de Messenger
- Proporcionar productos y personalizarlos según la información relacionada con la ubicación.
- Investigación y desarrollo de productos. En este apartado se menciona el uso de encuestas e investigaciones para recopilar información.

- Reconocer usuarios en fotos, videos y experiencias de la cámara por medio de las funciones de reconocimiento facial. Para este propósito, se detecta una posible "mitigación" considerando el siguiente comentario:
  - "Las plantillas de reconocimiento facial que creamos pueden constituir datos con protecciones especiales en virtud de la legislación de tu país "
  - En caso de que se introduzca la tecnología de reconocimiento facial en la experiencia del usuario de Instagram, Facebook indica que lo informarán previamente y que el usuario podrá decidir si quiere que la usen.
- Realizar mediciones, análisis y otros servicios comerciales
  - Ayudar a los anunciantes y otros socios a medir la eficacia y distribución de sus anuncios y servicios
  - Entender qué tipo de personas usan los servicios y cómo estas interactúan con sus sitios web, aplicaciones y servicios.
- Fomentar la seguridad, la integridad y la protección, lo cual abarca:
  - Verificar cuentas y actividades
  - Detectar y Combatir conductas perjudiciales
  - Investigar actividades sospechosas
  - Detectar, prevenir y combatir comportamientos dañinos o ilícitos
  - Identificar y combatir disparidades y prejuicios raciales contra comunidades históricamente marginadas
  - prevenir spam y otras experiencias negativas
  - Detectar cuando alguien necesita ayuda y brindar asistencia
  - Conservar la integridad de los Productos
  - Fomentar la seguridad tanto dentro como fuera de los Productos de Meta
- Comunicación con los usuarios
  - Enviar mensajes de marketing, comunicar sobre Productos e información acerca de las políticas y condiciones.
- Realización de investigaciones e innovación en beneficio del bienestar social
  - Llevar a cabo y respaldar investigaciones e innovaciones relacionadas con el bienestar social general, los avances tecnológicos y el interés, la salud y el bienestar públicos.

3.2.1.5. Posibilidad de eliminación de cuenta / datos

Tanto Facebook como Instagram brindan la posibilidad de acceder a los datos de los usuarios, rectificarlos, transferirlos y suprimirlos.

Indican que los datos se almacenan hasta que ya no son necesarios para brindar sus servicios o hasta que se elimina la cuenta. Según el tipo de información que se comparta, existen diferentes tiempos en los cuales la plataforma elimina los registros. Por ejemplo, indican lo siguiente: si un usuario hace una búsqueda en Facebook, el mismo puede acceder a esa consulta y eliminarla del historial de búsqueda en cualquier momento, pero el registro de dicha búsqueda se elimina después de seis meses dentro de la Red Social.

Al eliminar la cuenta, indican en la Política que se eliminará el contenido que el usuario publicó. Aclaran que no se eliminará la información sobre un usuario que otros compartieron por su cuenta. Esto es así, porque dichas publicaciones no forman parte del perfil original del usuario que está queriendo eliminar su cuenta.

Existe la posibilidad de "Desactivar" la cuenta. Esto significa que no se elimina la cuenta, sino que se deja de usar los Productos de estas Redes Sociales por un tiempo.

En base a lo que comentan estas plataformas en su Política, aclaran que accederán a la información de los usuarios, la conservarán y/o compartirán con organismos reguladores, autoridades u otras partes según sea el caso:

- En respuesta a un requerimiento legal.
- Si se cree necesario para detectar, impedir y abordar casos de fraude, usos no autorizados de los Productos, incumplimientos de las condiciones o las políticas aplicables, así como otras actividades perjudiciales o ilegales.
- Como parte de investigaciones o indagaciones reglamentarias
- Para evitar la muerte o lesiones físicas inminentes.
- Por una investigación gubernamental o investigaciones relacionadas con incumplimientos de la política de la plataforma.

Mencionan un período de retención de la información de una cuenta que se haya inhabilitado por incumplir sus propias condiciones. Este período es de al menos un año.

Indican también que podrán compartir información de forma internacional. Es decir, la información proporcionada por un usuario puede transferirse, transmitirse, almacenarse y tratarse en un lugar distinto al de la residencia del propietario.

3.2.1.6. Posibilidad de consulta / reclamo

La plataforma menciona que, si los usuarios tienen preguntas acerca de la política, se pueden contactar por medio de correo electrónico o por correo postal. Ofrecen las direcciones correspondientes.

Para el caso del contacto electrónico, ofrecen un formulario predefinido con opciones específicas de consulta. Es decir, no se permite que el usuario haga una consulta abierta. Se evidencia en la siguientes Figuras 9, 10 y 11:

Figura 10. Formulario para efectuar preguntas sobre la Política de Privacidad de Facebook

Figura 11. Formulario para efectuar preguntas sobre la Política de Privacidad de Instagram

Figura 12. Ampliación de formulario para efectuar preguntas sobre la Política de Privacidad de Instagram

3.2.2. LinkedIn[8]

3.2.2.1. Fecha última revisión: 18 septiembre de 2024

3.2.2.2. Notificación previa de cambio de política:

Al inicio del documento se indica la fecha de la entrada en vigencia de la política. Desde esa información se puede acceder a la página específica donde comentan la historia de actualizaciones[9].

En base a lo indicado, mencionan que "periódicamente" actualizarán las condiciones de uso y la Política de privacidad.

Actualizaciones de las Condiciones de uso y Política de privacidad

Última actualización: Hace 4 semanas

Periódicamente actualizamos nuestras Condiciones de uso y la Política de privacidad para asegurarnos de que nuestros usuarios comprendan sus derechos y responsabilidades cuando usan LinkedIn, además de conocer cómo recopilamos, usamos y protegemos su información personal.

Estos documentos se actualizaron el 6 de enero de 2020, con revisiones menores el 11 de agosto de 2020, incluida la eliminación de referencias al negocio de SlideShare , que ya no operamos; el 1 de febrero de 2022, para aclarar cómo y dónde resolveremos cualquier disputa que pueda surgir con nuestros miembros; el 6 de marzo de 2024, para proporcionar más detalles sobre la información enviada para crear una cuenta; y el 31 de julio de 2024, proporcionar ejemplos adicionales para ilustrar el intercambio de datos en la Sección 3 y agregar hipervínculos a los recursos existentes sobre cómo nuestros usuarios pueden ejercer sus derechos. El 18 de septiembre de 2024, 1) agregamos ejemplos y otros detalles a nuestra Política de privacidad para aclarar cómo usamos los datos personales para desarrollar y proporcionar servicios impulsados por IA y compartir datos con nuestros afiliados, y para proporcionar enlaces adicionales a información que puede ser relevante para las personas en ciertas regiones y 2) compartimos próximas actualizaciones adicionales de nuestro Acuerdo de usuario, incluyendo más detalles sobre nuestras funciones de IA generativa y cómo recomendamos y moderamos el contenido y las actualizaciones de nuestra licencia.

Sabemos que cumplir satisfactoriamente nuestra misión de conectar a profesionales de todo el mundo para que aumenten su productividad y éxito se basa en gran parte en la confianza depositada por los usuarios en LinkedIn. Luchamos por fomentar esta confianza actuando de forma abierta y transparente. Recomendamos a nuestros usuarios leer la versión revisada de las Condiciones de uso y la Política de privacidad.

Figura 13. Captura sección sitio LinkedIn sobre las actualizaciones a las Condiciones de uso y Política de privacidad. (Fecha de la captura: 13/10/2024).

Complementando lo antes explicitado, la política menciona lo siguiente:

"LinkedIn («nosotros») puede modificar esta Política de privacidad y, si introducimos algún cambio importante, te avisaremos a través de nuestros Servicios, o por otros medios, para ofrecerte la oportunidad de revisar los cambios antes de que se hagan efectivos. Si no estás de acuerdo con cualquiera de los cambios, puedes cerrar tu cuenta". Además, se menciona lo siguiente: "Declaras que tu uso continuado de nuestros

[8] Link acceso "Condiciones de Privacidad" LinkedIn: https://es.linkedin.com/legal/privacy-policy
[9] Link acceso "Historial de actualizaciones" LinkedIn: https://www.linkedin.com/help/linkedin/answer/a1341216/updates-to-user-agreement-and-privacy-policy

Servicios, tras publicar o enviar un aviso acerca de nuestros cambios en esta Política de privacidad, implica que la recopilación, la utilización y el uso compartido de tus datos personales están sujetos a dicha Política de privacidad actualizada, desde su fecha de entrada en vigor".

3.2.2.3. Datos que recopilan:

El siguiente es el lema que esta Red Social indica en su política de privacidad: "Somos una red social y una plataforma en línea para profesionales". Por medio de esta sentencia, se orienta su funcionalidad a "profesionales". En otras palabras, el objetivo es centralizar los perfiles en la trayectoria laboral / profesional de las personas y empresas. Ampliando este concepto, esta política menciona que el objetivo de LinkedIn es conectar a los profesionales de todo el mundo para ayudarles a ser más productivos y a alcanzar sus metas laborales.

Continuando con lo que menciona la política de privacidad, en relación con los usuarios de la Red indica: "Los usuarios registrados («Miembros») comparten su identidad profesional, interactúan con su red de contactos, intercambian información y conocimientos profesionales, publican y ven contenido relevante, adquieren y desarrollan aptitudes, y encuentran oportunidades profesionales y de negocio. El contenido y los datos de algunos de nuestros Servicios están disponibles para personas que no son miembros («Visitantes»)."

En base a lo anterior, un usuario en LinkedIn es llamado "Miembro". Eso significa que está registrado en la plataforma habiendo elaborado un perfil particular. Por otro lado, refieren como "Visitantes", a aquellas personas que usan los servicios de la Red Social, pero sin tener un perfil creado, es decir, sin estar registradas con credenciales y necesidad de un proceso de inicio de sesión (login).

Un detalle para considerar en la política de privacidad es sobre estos usuarios "Visitantes". Se indica: "El contenido y los datos de algunos de nuestros Servicios están disponibles para personas que no son miembros («Visitantes»)". Por medio de este punto, se detecta una necesidad de prevención de lo que se publica porque existen otras personas, no del círculo de contactos, que podrían acceder a la información sin ser usuarios registrados en la plataforma.

A continuación, se enumera la información recopilada por esta red social:

3.1 Los datos que los usuarios proporcionan:

Registro

- Nombre
- Dirección de email
- Número de móvil

- Contraseña
- Información de pago y facturación (en el caso de optar por el Servicio Premium)

Perfil

- Educación
- Experiencia laboral
- Aptitudes
- Fotografías
- Ciudad o ubicación
- Validaciones
- Datos provenientes de la sincronización de Agenda de Direcciones o Calendario.
    - Contactos
    - Agenda de direcciones
    - Información de reuniones del calendario
    - Información sobre eventos, como la hora, el lugar, los asistentes y los contactos.
- Información Delicada: información personal sensible como, raza, origen étnico, opiniones políticas, creencias religiosas o filosóficas, afiliación a un sindicato, salud física o mental, vida sexual o antecedentes penales.
- Información que otros publican de un usuario. Como parte de artículos, publicaciones, comentarios o vídeos) en nuestros Servicios.
- Información pública, como noticias y logros profesionales
- Datos personales (entre los que se incluye la información de contacto) sobre los usuarios cuando otras personas importan o sincronizan sus contactos o su calendario con los propios Servicios de LinkedIn. A esta categoría LinkedIn la llama “Datos de terceros”. (Estos “terceros” puede ser expuestos pasivos y convertirse en la puerta de entrada a un perfil víctima).
- En el caso de que un usuario opte u otros opten por sincronizar cuentas de email con los Servicios de esta plataforma, también se recopilará información del «encabezado del email» que está asociada perfiles de Miembros de LinkedIn.
- Visitas y uso de Servicios de servicios de la plataforma, incluidas las aplicaciones móviles. Esto incluye sitios web, aplicaciones y la tecnología de la plataforma):
    - Registro de los clics en un contenido (ejemplo: video de formación)
    - Registro de los clics en un anuncio

- Búsquedas realizadas
- Instalación o actualización de las aplicaciones móviles
- Cuando se comparten artículos
- Solicitudes de empleo.
- Registros de inicio de sesión
- Información de dispositivos
- Direcciones IP para identificar al usuario y uso en LinkedIn.

- Datos a través de cookies y tecnologías similares (balizas web y etiquetas de anuncios):
  - Información sobre dispositivos de los usuarios (ID del anuncio, dirección IP, sistema operativo e información del navegador).
- Dispositivo y ubicación (por medio de cookies y tecnologías similares):
  - URL tanto del sitio del que se ha llegado como del sitio al que se está dirigiendo
  - Hora de la visita
  - Información sobre la red
  - Información sobre los dispositivos
    - Dirección IP
    - Servidor proxy
    - Sistema operativo
    - Navegador web y los complementos
    - Identificador y las funciones del dispositivo
    - Identificadores de las cookies
    - Proveedor de servicios de Internet
    - Operador de red móvil).
    - Ubicación en función de la configuración del teléfono. Indican que “pedirán” que se marque la opción de auto inclusión para que la plataforma pueda usar el GPS para identificar la ubicación exacta.
- Mensajes: al enviar, recibir e interactuar con el servicio de mensajes.
  - Al recibir una solicitud de contacto, identificar las acciones efectuadas, enviando recordatorios.
  - Escaneo automático de los mensajes, para mantener y proteger el sitio; para generar sugerencias de respuesta a mensajes; para bloquear contenido que infrinja las condiciones de uso.

- Datos proporcionados por la empresa y la institución educativa:
  - Cuando estas organizaciones adquieren un servicio Premium para que sus "usuarios" / "empleados", los usen. En ese caso se proporcionan esos datos de usuarios a LinkedIn.
  - Información de contacto de los Administradores de los Perfiles de LinkedIn y de los usuarios autorizados para usar los servicios Premium.

Si bien se menciona que no es necesario que los usuarios proporcionen información adicional sobre sus perfiles, comentan que el hecho de hacerlo ayuda a sacar más provecho de su plataforma e incluso "se limite tu capacidad para crecer e interactuar con tu red a través de nuestros Servicios". En ese sentido, la Política indica que la información del perfil ayuda en tareas como facilitar que los técnicos de selección de personal y las oportunidades laborales encuentren a los "miembros". El desafío aquí es pensar en mayor provecho versus mayor riesgo de exposición.

En general, se observa que, dentro de la plataforma, las empresas que ofertan empleo usan el concepto de Solicitud Rápida en la cual se puede responder un cuestionario y cargar el CV directamente. Esa información, según la política de privacidad, será recuperada por la plataforma.

3.2.2.4. Objetivo de los datos que recopilan

Según expresan en la política, LinkedIn utiliza los datos de los usuarios para proporcionar, apoyar, personalizar y desarrollar sus Servicios.

Indican que el modo en que utilicen los datos personales dependerá de los Servicios que cada usuario utilice, de la forma en que se usen dichos servicios y de la configuración propia de cada miembro. Además, indican que emplean los datos personales para proporcionar y personalizar sus servicios (incluidos los anuncios), con la ayuda de sistemas automatizados y de las deducciones que efectúan, de manera que puedan resultar más relevantes y útiles.

Otros usos que tienen los datos de los usuarios:

- Para autorizar acceso a sus servicios según la configuración personal de cada usuario.
- Para generar y mantener "conectados" a los usuarios entre sí.
- Para que otras personas encuentren un perfil, para sugerir contactos y a otras personas (por ejemplo, Miembros que tienen contactos o experiencias profesionales en común).
- Para ofrecer la posibilidad de invitar a otras personas a hacerse Miembros y conectar con los usuarios.
- Hacer uso de la ubicación exacta o de la proximidad con otras personas para determinadas tareas.

- Para enviar recordatorios de contacto a las personas a las cuales se haya puesto interés en generar “contacto” como miembros en la Red.
- Para mantener informado a los usuarios, personalizando los servicios mediante recomendaciones o clasificando contenido y conversaciones relevantes.
- Para sugerir aptitudes para añadir a los perfiles y otras aptitudes que se podrían necesitar para postular a nuevas oportunidades laborales.
- Para mostrar capacitaciones relacionadas.
- Para sugerir el contacto con ciertos miembros de la Red.
- Para comunicar a otros usuarios de las actividades de otros miembros. Aclaran que esto depende de la configuración de cada usuario.
- Para fines de publicidad y anuncios. Ejemplo, usan información como el historial de búsqueda, el feed de actividad, el contenido que leen los usuarios, a quienes se están siguiendo, los contactos, la participación en grupos, visitas a páginas, los vídeos que se visualizan, los clics en anuncios, etc.
- Para tareas de Marketing, promover servicios ante los usuarios: invitaciones y comunicaciones que promueven el crecimiento de la red, una mayor adhesión y un mayor grado de compromiso.
- Para desarrollo de los servicios e investigación (tendencias sociales, económicas y corporativas). Indican que también destinan parte de la investigación con controles diseñados para proteger la privacidad de los usuarios.
- Como herramienta para la Atención al cliente: investigar, responder y resolver quejas, así como para problemas con el Servicio (por ejemplo, errores).
- Por motivos de seguridad, para la prevención de casos de fraude e investigaciones.
- Como parte de los servicios de terceros. Se permite que el perfil se vincule con un servicio externo. Por ejemplo, un cliente de correo electrónico. En ese caso, estos servicios estarán accediendo información de los usuarios. Se aclara que estos servicios externos tienen sus propias políticas de privacidad y que no necesariamente serán iguales que las de LinkedIn.
- Por motivos relacionados con la Ley y para proteger derechos y seguridad de los usuarios, de la propia Red Social o los de terceros.
- Por la relación con Servicios de Terceras partes que ayudan a LinkedIn en la prestación de sus funciones. Dichas terceras partes tendrán un acceso limitado a la información de los usuarios en

la medida necesaria para ejecutar estas tareas en representación de la Red Social y están obligadas a no desvelarla ni utilizarla para otros fines.

- Como parte de una venta, fusión o cambio de control, o para preparar cualquiera de estas circunstancias.

3.2.2.5. Posibilidad de eliminación de cuenta / datos

Administración de los datos

La plataforma LinkedIn ofrece estas acciones como control de los datos de los usuarios:

- Eliminar datos: borrar o eliminar todos o parte de los datos personales (por ejemplo, si ya no es necesario ofrecer Servicios).
- Cambiar o rectificar datos: editar parte de los datos personales a través de la cuenta.
- Rechazar, limitar o restringir el uso de datos: solicitar que se dejen de usar la totalidad o parte de los datos personales o que se limite su uso.
- Derecho de acceso y/o toma en posesión de los datos: se puede solicitar una copia de los datos personales.

Posibilidad de cerrar la cuenta

La plataforma aclara que podrán conservar algunos de los datos de los usuarios incluso después de haber cerrado la cuenta. Si un usuario decide cerrar su cuenta de LinkedIn, los datos personales dejarán de verse en los Servicios, por lo general, en un plazo de 24 horas. Indican que normalmente se borra la información de las cuentas cerradas en un plazo de 30 días desde el cierre de esta, salvo en los casos citados a continuación:

- Para cumplir con obligaciones legales (incluidas, las peticiones de las fuerzas del orden), reunir los requisitos reglamentarios, resolver disputas, mantener la seguridad, evitar casos de fraude y abuso.
- La información que un usuario haya compartido con otras personas (por ejemplo, a través de mensajes InMail, actualizaciones o publicaciones de grupo) seguirá viéndose después de cerrar la cuenta o borrar la información del propio perfil o buzón. LinkedIn aclara que no controlan los datos que otros Miembros hayan copiado de sus Servicios.
    - Definición: InMail es el sistema de mensajería privada entre usuario de LinkedIn. Por medio de esta función, las personas pueden intercambiar mensajes como si fuera un correo electrónico.

▪ El perfil de los usuarios podría seguir mostrándose en los servicios de terceros (por ejemplo, los resultados de motores de búsqueda) hasta que actualicen su memoria caché.

3.2.2.6. Posibilidad de consulta / reclamo

La plataforma ofrece la posibilidad de hacer un contacto para resolver alguna pregunta o queja, como se menciona en la política: “Si tienes alguna pregunta o queja sobre esta Política, contacta con LinkedIn en línea primero. También puedes contactarnos por correo postal. Si tras contactarnos no se resuelve tu queja, existen otras opciones disponibles”.

Ofrecen la posibilidad de usar un correo postal para mandar una carta escrita o por medio de un contacto electrónico utilizando una serie de preguntas predefinidas de una lista con la posibilidad de escribir a texto abierto en la categoría “otros”.

A continuación, se muestran los tópicos que se pueden seleccionar para la consulta electrónica:

- Solicitar mis datos personales en LinkedIn.
- Eliminar mis datos personales en LinkedIn.
- Rectificar / cambiar mis datos personales en LinkedIn.
- Oponerse al tratamiento de mis datos en LinkedIn
- Transferir mis datos personales en LinkedIn a otro controlador de datos.
- Administrar mi cuenta y/o configuración de privacidad.
- Cerrar mi cuenta
- Recuperar acceso a mi cuenta
- Combinar dos o más de mis cuentas

Figura 14. Formulario para efectuar preguntas sobre la Política de Privacidad de LinkedIn.

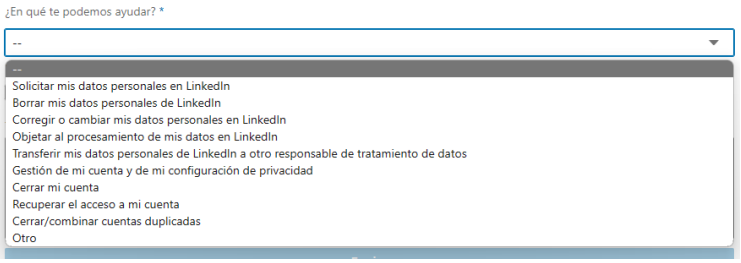


Figura 15. Vista de las categorías de consultas para el formulario para efectuar preguntas sobre la Política de Privacidad de LinkedIn.

Conclusiones

Como se analizó, todas las redes sociales seleccionadas detallan la información que pueden recopilar y compartir de los usuarios.

Además, establecen y dejan en claro que el usuario es el responsable de determinar y aceptar la información que se recopilará y compartirá. Incluso mencionan el hecho de considerar qué hay información "sensible" en los perfiles.

A continuación, se detalla una tabla comparativa considerando los criterios empleados para hacer el análisis de cada condición de privacidad.

Criterios	Facebook / Instagram	LinkedIn
Fecha última actualización	26 junio 2024	18 septiembre 2024
¿Notificación previa de cambio de política?	Si.	Indican que "periódicamente" harán cambios en la Política. Detallan los cambios aplicados.
Datos que recopilan	Orientado a temas personales, amistades, familias, intereses.	Orientado a temas laborales, de contactos profesionales.
Objetivo de los datos que recopilan.	Proporcionar, personalizar y mejorar los productos de Facebook.	Proporcionar, apoyar, personalizar y desarrollar sus Servicios.
Posibilidad de eliminación de cuenta / datos	Si.	Si. Suman posibilidad de "Desactivar" cuenta. Sólo limita el acceso a los servicios, pero los datos del perfil permanecen.
Posibilidad de consulta / reclamo	Si. Por medio de correo postal y medio electrónico (formulario con preguntas predefinidas)	Si. Incluyen la posibilidad de escribir una propia consulta.

Tabla 1. Tabla comparativa considerando los criterios empleados para hacer el análisis de cada condición de privacidad.

Se puede observar, que las redes sociales analizadas se amparan en que la información que recopilan ayudará a brindar una mayor experiencia y servicios al usuario. Además, las condiciones de privacidad son documentos extensos, con uso exclusivo de texto, lo que significa que, para el usuario promedio, no son de sencilla lectura y comprensión.

Como punto a destacar es que las 3 plataformas ofrecen la posibilidad de eliminar las cuentas de los usuarios. Aclaran que la información que se menciona de un usuario por parte de otros miembros de estas redes queda en el espectro de control del usuario que hizo la publicación. En este punto se vincula el concepto de "Usuarios Expuestos Pasivos" que se mencionó previamente.

Con respecto a la dificultad de lectura y comprensión de las políticas para el usuario promedio, se proponen a continuación algunas oportunidades de mejora que se podrían incorporar:

1. Que al momento de hacer una publicación o cambiar un parámetro de la configuración de la cuenta, se alerte al usuario de los riesgos asociados o niveles de incremento en la exposición.
2. Que el diseño de las condiciones de privacidad sea más orientado a los aspectos claves de lo que se recopila y comparte, reduciendo el texto y haciendo uso de mayores señales de advertencia. En este sentido, potenciar el uso de gráficos o expresiones de resalte de conceptos vinculados a los riegos de la exposición.

Luego del análisis exhaustivo de las redes sociales seleccionadas, se observa que son las mismas plataformas las que llevan a que los usuarios se expongan más, atentando con su privacidad. Esta tendencia de las plataformas a incitar al usuario a aumentar su exposición se justifica con el siguiente enunciado (que se repite en muchas políticas de redes sociales): "mayor exposición implica mayores beneficios". Se puede decir que ésta es la ecuación de la justificación para una alta exposición. Según las plataformas, luego de analizar las condiciones de privacidad, la exposición es directamente proporcional a los beneficios que el usuario puede obtener con la plataforma. Se crea entonces una "falsa" sensación de que la exposición es necesaria para lograr mejores resultados, según la red social que se trate. Por ejemplo:

- Mayor popularidad en Facebook e Instagram
- Mejores posibilidades de conseguir empleo en LinkedIn

Las plataformas indican que ellas efectúan análisis de mensajes y de chats de los usuarios. Además, existen procesos automatizados que se ejecutan "por detrás" o en "background" (sin que el usuario lo perciba) en busca de situaciones no permitidas. El concepto y su justificación es genuino y necesario, sin embargo, abre la puerta para que la plataforma haga un uso inadecuado exponiendo todas las comunicaciones de los usuarios.

Otro punto crítico está relacionado a la información recopilada de los dispositivos. Esto incluye, por ejemplo, la información del GPS (si está activado). En este caso, se está compartiendo la ubicación del usuario.

Además, otro factor crítico es el vínculo con los proveedores de servicios externos a las redes sociales. Hay un intercambio de datos de los usuarios para que estos proveedores puedan personalizar la oferta de servicios.

Se destaca que las páginas donde se detallan las condiciones de privacidad son extensas y en formato texto. Si las mismas tuvieran un formato personalizado que reduzca el contenido, mostrando un resumen de los puntos fundamentales de la exposición, tal vez se mejoría la toma de conciencia por parte de los usuarios.

Las condiciones de privacidad deberían considerarse una herramienta de concientización para los usuarios. Las plataformas de Redes Sociales podrían implementar un entrenamiento esencial y obligatorio a usuarios para enseñar el valor de la exposición, explicar cómo cada plataforma opera con los datos de los usuarios y qué medidas básicas se deben tomar para hacer un perfil más seguro, con un nivel mínimo (o deseable) de exposición.

La importancia de que las condiciones de privacidad sean conocidas y entendidas por los usuarios radica en que puede reducir la existencia de usuarios “Expuestos Pasivos”. Esto es porque un usuario responsable leerá y entenderá los riesgos de la exposición posible, cuidando así lo que publicará de sí mismo y de sus contactos. Sin embargo, puede suceder que otros usuarios tomarán a las condiciones de privacidad como un obstáculo, decidiendo “aceptar” sólo para avanzar con la creación del perfil. Esto abre la puerta a que, por no hacer una lectura a conciencia, se haga uso de su perfil exponiendo a otros usuarios sin su consentimiento.

El hecho de no reconocer en las condiciones de privacidad cómo es el esquema de recolección y compartición de la información en las Redes Sociales, genera en los usuarios una conducta menos preventiva, es decir, sin considerar los efectos de la información que se expone. En cierta manera, las condiciones de privacidad y su existencia como tal generan una falsa sensación de seguridad y protección por parte de las Redes Sociales. Sin embargo, estas condiciones de privacidad tienen por objetivo, principalmente, proteger a las Redes Sociales, por cualquier suceso que tengan los usuarios en relación con la exposición de sus datos. Es el concepto de “Yo Plataforma, aviso a los usuarios …” “dejando a su responsabilidad …”. Por ende, las plataformas de Redes Sociales terminan siendo los vehículos para que sucedan los problemas vinculados a la exposición. En definitiva, dejan puertas abiertas para la concreción de ataques.

A continuación, se muestran extractos de las condiciones de privacidad de LinkedIn que respaldan estas afirmaciones:

- *"Todos los datos que incluyas en tu perfil y cualquier contenido que publiques o acción social (por ejemplo, recomendaciones, contenido seguido, comentarios o contenido compartido) que realices en nuestros Servicios serán vistos por otras personas, de acuerdo con tu configuración".*
- *"Tu perfil es visible para todos los Miembros y clientes de nuestros Servicios. En función de tu configuración".*

Por otro lado, en las condiciones de privacidad de las plataformas estudiadas no se observa referencia a medidas preventivas o de advertencias al usuario cuando publica una foto de manera de que se prevenga o asesore para evitar exponer información relacionada como parte de esa foto o imagen.

En los próximos capítulos se trabajará en este sentido: lograr una caracterización y valoración de los perfiles digitales que posibilite al usuario conocer y ser consciente su nivel de exposición en una red social digital.

Capítulo 4: Aprovechamiento de la exposición de usuarios: Principales ataques.

En este capítulo, mediante un relevamiento bibliográfico, se identificarán y detallarán los ataques que se efectúan aprovechando nivel de exposición inadecuados de los usuarios de redes sociales digitales.

“La mejor defensa es un buen ataque”. Con esta frase, el estratega y filósofo chino Sun Tzu, expone en su obra “El arte de la guerra” el delicado concepto que separa la victoria de la derrota en una batalla.

Haciendo una analogía entre dicha afirmación y los perfiles biográficos digitales, un "buen ataque" se equipara con efectuar una adecuada exposición, cuidando los detalles que eviten un ataque hacia tan preciado bien como lo es la privacidad de las personas. De esta manera, configurar correctamente los perfiles biográficos digitales en cada red social es un ataque directo a las amenazas externas provocadas por aquellos intrusos que buscan debilidades y se aprovechan la exposición desmedida de los usuarios.

En la siguiente sección se describirán los componentes que conforman un ataque.

4.1 Actores de un Ataque

Los actores que intervienen en un ataque en el que se aprovecha una inadecuada exposición de usuario de red social son los siguientes:

1. Atacante
2. Usuario Víctima
3. Usuario Expuesto Pasivo -> Posible Víctima Indirecta para nuevo Ataque
4. Usuario Puente –> Es usado por el Atacante para conseguir más información sobre la Víctima. Por ejemplo, es un “Amigo”, “Contacto” -> Posible Víctima Directa para nuevo Ataque.

A partir de un “Ataque directo” hacia una Víctima particular, se podrían luego originar “Ataques indirectos” hacia los usuarios Expuestos Pasivos y/o Usuarios Puente que se utilizan durante el accionar del atacante.

La Ingeniería Social es una herramienta que permite obtener información y brinda una metodología para abordar la recolección de información. La utilización de Ingeniería Social de manera incorrecta, es decir desde el lado malicioso o con malas intenciones, ofrece potenciales métodos para aprovechar la exposición de las personas en una red social.

La Ingeniería Social es una técnica para producir un engaño a partir del conocimiento de cierta información que permite generar confianza y/o cercanía en el sujeto objetivo del ataque. La materia prima

de este tipo de técnica es principalmente todo el conjunto de información sobre la persona / objetivo del ataque, que permite crear la sensación de que realmente se conoce a esa persona y a su entorno, y con esa confianza ganada, perpetrar un ataque determinado.

Cuando mayor sea la información que una persona exponga de su vida personal/laboral, más probabilidades existirá de que un ataque por Ingeniería Social sea efectivo.

Es importante mencionar la definición de Kevin Mitnick, considerado un hacker pionero en el uso de la Ingeniería Social. Este referente indica que la ingeniería social utiliza la influencia y la persuasión para engañar a las personas convenciéndolas de que el ingeniero social es alguien que efectivamente no es quien dice ser. Como resultado, el ingeniero social puede aprovecharse de las personas para obtener información con o sin el uso de tecnología. Mitnick considera a la Ingeniería Social como el arte de la manipulación e influencia, con el fin de ganar control sobre un sistema informático[10].

En forma complementaria, la US-CERT indica que, en un ataque por Ingeniería Social, un atacante usa la interacción humana y las habilidades sociales para obtener información acerca de una persona, organización o sistema informático[11].

Considerando la definición del fabricante de tecnología de seguridad Kaspersky, se menciona que la Ingeniería Social es una técnica de manipulación para explotar el error humano, para lograr obtener información privada. Este tipo de ataques pueden ocurrir tanto de manera online como en persona.

Kaspersky describe las siguientes fases del proceso de un ataque por Ingeniería Social[12]:

- Preparación: el atacante reúne información de antecedentes de la víctima y/o de los grupos que forma parte.
- Infiltración: el atacante establece una relación o inicia una interacción con la víctima de manera de generar confianza.
- Explotación: el atacante concreta su cometido una vez que se establezca la confianza con la víctima y se evidencie una debilidad para avanzar. Se detecta una vulnerabilidad humana, se explota el error en el comportamiento de la víctima.
- Desconexión: el atacante desaparece una vez que haya concretado la acción de ataque requerida.

[10] Definición Kevin Mitnick: https://www.knowbe4.com/what-is-social-engineering/
[11] Definición US-CERT: https://us-cert.cisa.gov/ncas/tips/ST04-014
[12] Descripción Kaspersky: https://usa.kaspersky.com/resource-center/definitions/what-is-social-engineering

Para complementar el proceso anterior, según la definición de TechTarget[13], el primer paso en general para concretar un ataque de Ingeniería Social es comenzar, por parte del atacante, con la investigación y reconocimiento de la persona objetivo, la víctima. Además, TechTarget menciona que una táctica común de la Ingeniería Social es colocar el foco en los patrones de comportamiento de las personas. Por eso, al identificar a las personas objetivo, el atacante recorrerá los perfiles de redes sociales en busca de información personal y conductas / hábitos de cada individuo. Esa información será la que usará para perpetrar el ataque, usando lo recolectado para ganar la confianza de la víctima y así obtener lo que desea.

4.2 Anatomía de un ataque a una Red Social

Según la plataforma de la red social, las opciones de un ataque pueden variar. Con una adecuada configuración de la privacidad, el atacante deberá encontrar vulnerabilidades que quedan expuestas debido a una inadecuada configuración de privacidad.

En el caso de las tres Redes Sociales contempladas en este trabajo, tanto Facebook, Instagram como LinkedIn, permiten que los usuarios definan a sus cuentas como privadas, sólo accesible por los contactos, amigos o miembros" aceptados para tal fin.

Uno de los indicadores de "confianza" o "fidelidad" de una solicitud de contacto por parte de un usuario a otro es la cantidad de "amigos" comunes o compartidos. Este constituye el factor analizado por un usuario para encontrar cierta cercanía que pueda dar la certeza de que una persona que ha enviado una invitación a ser su "amigo" es de confianza. Por ese mismo motivo, un atacante, como primera medida de su análisis, buscará conocer quiénes son los amigos y contactos comunes con la víctima. Con esa información, intentará primero lograr el "contacto" con ese grupo de personas. De esa manera, incrementará la sensación de confianza que tendrá la víctima al recibir la notificación de contacto por parte del atacante.

Considerando lo anterior, entra en juego y cobra preponderancia el concepto de "Usuario Expuesto Pasivo". Esto significa que un usuario víctima a través de "contactos / amigos" que poseen un nivel de exposición no adecuada y sin concientización de control sobre sus perfiles, permite la entrada del atacante. Estos amigos o contactos se convierten en "Usuarios Puentes" para llegar al objetivo real que se quiere comprometer.

Una estrategia que toma el atacante es la creación de un Perfil falso en una determinada red social digital. Con ese perfil ficticio creado, el atacante comenzará a definir atributos que lo hagan "cercano", de "confianza" con la víctima y su grupo de contactos previamente identificado. Ejemplos:

[13] Definición de TechTarget: https://www.techtarget.com/searchsecurity/definition/social-engineering#:~:text=What%20is%20social%20engineering%3F,locations%20or%20for%20financial%20gain.

- Definición de mismas instituciones educativas, clubes, asociaciones, lugares de trabajo, ciudades, etc.
- Establecimiento de mismos intereses y o grupos de pertenencia sobre ciertos temas.
- Carga de fotos de lugares visitados y/o conocidos, buscando coincidencia con elementos similares publicados por la víctima y su grupo.
- Publicación de comentarios y postes compartidos, es decir, que son parte de alguna cadena que el mismo usuarios víctima o su grupo cargó previamente. Por ejemplo, por alguna campaña o evento en particular.

Un paso importante y a la vez arriesgado para el atacante será el de pedir solicitud de "contacto", "amistad", o "seguimiento" a una persona que sea parte del grupo de confianza del usuario víctima. Aquí es donde cobrará importancia el nivel de concientización y protección de los usuarios de cada red social que recibirán las peticiones de contacto. Esta es la modalidad de ataque donde se aprovecha de un usuario conocido por la víctima, el cual oficia de "Usuario Puente".

Una vez que el atacante configure su perfil falso, especialmente diseñado para su víctima, intentará el contacto directo con su objetivo y buscará pedir "amistad", "contacto" o "seguimiento" a la persona de interés (usuario objetivo o víctima). Si esto se concreta de manera positiva, entonces la puerta queda abierta y la exposición que la víctima tenga será la materia prima sobre la cual el usuario malintencionado empezará su ataque y/o la búsqueda de información para diagramar su objetivo final. Eso es así porque no necesariamente el ataque será hacia el perfil de la red social, sino que ese mismo perfil con un alto nivel de exposición, será el medio para obtener información que servirá posteriormente para un ataque en el mundo físico, como su casa, su vehículo e incluso a la persona misma.

Continuando con la descripción de la anatomía de un ataque orientado a una Red Social, el Health Sector Cybersecurity Coordination Center (HC3) del Departamento de Health and Human Services de Estados Unidos[14], describen un proceso de 4 actividades:

1. Footprinting: es la actividad de recopilar toda la información posible acerca del objetivo víctima para encontrar los puntos débiles o vulnerables.
2. Monitoring: consiste en la observación de los hábitos en las redes sociales que permiten un ataque más efectivo. Por ejemplo, lo que los atacantes hacen es buscar conexiones entre individuos en una red social. Es decir, identifican el grupo de confianza; Usuarios Puentes o Usuarios Expuestos Pasivos.

[14] Descripción anatomía de ataque de HC3: https://www.hhs.gov/sites/default/files/social-media-attacks.pdf

3. Impersonate / Hijack: En este caso se buscar generar un perfil falso, una identidad ficticia para poder concretar el contacto con el usuario víctima y su entorno.

4. Attack: Consiste en lanzar el ataque al perfil del usuario víctima en la Red Social, ya con las herramientas e información para aprovechar la exposición. Aquí se puede incluir el ataque a Usuarios Expuestos Pasivos.

Además, el HC3, presenta en el siguiente diagrama, los elementos primarios en un perfil de una Red Social, que son las puertas para este proceso de ataque antes mencionado:

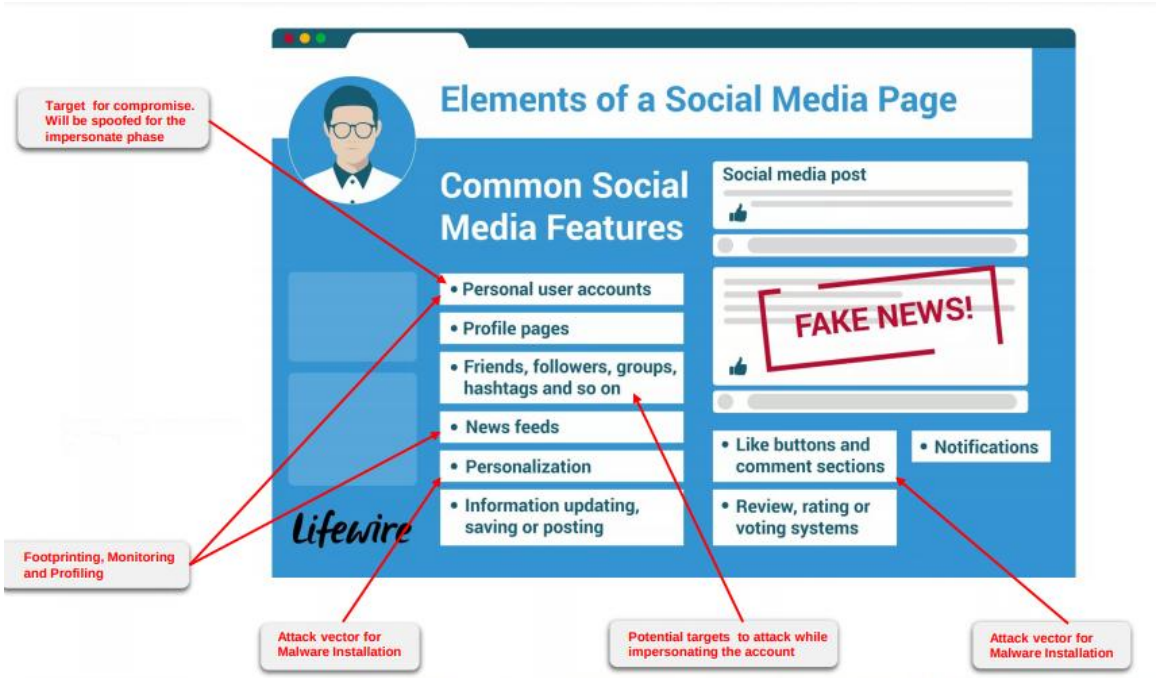


Figura 16. Elementos de un Perfil Biográfico Digital de una Red Social junto a los Ataques más comunes.

Elementos de una página de Red Social:

- Cuentas de usuarios
- Páginas de los perfiles
- Amigos, seguidores, grupos, etiquetas, contactos.
- Información posteada, almacenada y actualizada
- Posteos o Publicaciones
- Comentarios
- “Me Gusta’s” o “Likes”
- Notificaciones

Continuando con lo que describe el HC3, a continuación, se identifican posibles ataques relacionados que se pueden derivar de aplicar el proceso de obtención de información sobre los perfiles de las Redes Sociales.

En primer lugar, se identifica la Ingeniería Social. Es una forma de ataque basado en generar un contacto con la víctima y/o su entorno haciendo uso de toda la información relevada anteriormente de los diferentes perfiles. Es clave para este ataque, la confianza que el atacante busca generar en su víctima para que se minimice todo tipo de sospechas.

En este punto, entra también en juego el ciberacoso o ciber hostigamiento. Esto es cuando el atacante, una vez determinado el usuario víctima, usa las redes sociales para entablar contacto y por medio de mensajes y publicaciones busca amenazar, molestar, hostigar a las personas dueñas del perfil biográfico digital. El detalle de este tipo de ataque es que las pruebas, evidencias quedarán visibles en el caso de que se manden mensajes en los sistemas de chat de las plataformas. Eso será clave para una posible denuncia.

Relacionado a este tipo de ataque, se debe incluir al ciber grooming. Este tipo de ataque y delito es perpetrado contra usuarios menores de edad. En este caso, el atacante se hace pasar por un menor y establece confianza con la víctima buscando un contacto frecuente y queriendo llegar a concretar exposición de los menores en por medio de intercambio de fotos, mensajes subidos de tono y un eventual encuentro físico. Es un delito penal que requiere mucha atención y supervisión de los adultos a cargo en el uso adecuado de sus perfiles en las redes sociales.

Un ataque derivado de obtener información particular de la víctima se denomina “Phishing”. En este caso, el atacante confecciona un correo electrónico relacionado a un tema particular vinculado a la víctima. Este correo puede ser relacionado a una entidad bancaria del cual la víctima es cliente, un servicio de películas, etc. Por medio de ese correo, el atacante busca que la víctima confíe en el contenido y en el motivo del contacto, el cual parece ser genuino. Generalmente, este tipo de correo electrónico invita o incita al receptor a ingresar a un enlace a un sitio web que parece auténtico, lo cual se traduce en una solicitud de acceso que pedirá credenciales y datos confidenciales para ser robados.

Considerando el Phishing como ataque basado en un correo electrónico como plataforma de envío tradicional, cuando esa comunicación se confecciona haciendo parecer que proviene de una determinada marca de alguna empresa o servicios, entonces se puede hablar de un ataque del tipo “Imitación de Marca” (Brand impersonation). Como la comunicación viene de una “marca” conocida por los usuarios, gana la confianza de la víctima que puede caer en la trampa.

Cuando un atacante genera contenido relacionado a alguna marca / empresa / servicio y desarrolla un sitio web específico para su promoción, se está hablando de un ataque llamado “Spread malware”. El objetivo es buscar que los usuarios víctimas accedan a dichos portales y transaccionen depositando información sensible y confidencial. En este caso el atacante busca que la víctima descargue algún programa malicioso (malware) y con eso se comprometa su seguridad.

Como consecuencia de los ataques antes mencionados, se puede concretar un llamado “Data breach”, que significa “filtración de información”, como ser el robo de datos confidenciales y sensibles de la víctima. Este tipo de ataque puede deberse a que la víctima propició sus credenciales de la Red Social en un sitio falso creado para tal fin o porque las brindó como respuesta a un correo que las pedía. Además, un robo de información se puede deber directamente a la inadecuada exposición de una víctima en una red social, cuando ésta ha dejado información sensible a la vista, simplemente por una no adecuada configuración de los atributos de protección de la privacidad.

4.3 OSINT

Luego de haber entendido cómo opera un ataque que se aprovecha de la exposición de los usuarios, se presenta la metodología OSINT, la cual se toma como base para el análisis de fuentes de información de los perfiles digitales.

OSINT significa Open Source Intelligence (Inteligencia de Fuentes Abiertas). Según la definición del proveedor de Seguridad ESET[15], OSINT se trata de un conjunto de técnicas y herramientas para recopilar información pública, correlacionar los datos y procesarlos. El objetivo de la metodología OSINT es aplicar análisis e inteligencia a gran cantidad de información públicamente accesible en Internet con el objetivo de extraer conclusiones útiles. Teniendo en cuenta lo descripto hasta el momento sobre cómo opera un ataque a un perfil de una red social, puede observarse cómo OSINT ofrece una metodología para extraer información sobre un sujeto u organización, que constituye la materia prima para perpetrar un ataque al objetivo.

La metodología OSINT se estructura por medio de un proceso. Las fases de ese proceso son las siguientes[16]:

1. Establecer objetivos: en esta fase se busca saber para qué va a servir la información que se busca y de qué tipo va a ser.
2. Identificar fuentes relevantes de información que se encuentran abiertas (accesibles).
3. Obtención de la información: en esta fase, en base a la información que se desea obtener, se trabaja con un conjunto de herramientas específicas para concretar ese objetivo. Existen herramientas especiales para obtener información de Redes Sociales.

[15] Fuente ESET: https://www.welivesecurity.com/la-es/2019/10/07/tecnicas-herramientas-osint-investigacion-internet/#:~:text=OSINT%20significa%20Open%20Source%20Intelligence,correlacionar%20los%20datos%20y%20procesarlos.

[16] Fuente fases proceso OSINT: https://ciberpatrulla.com/que-es-osint/

4. Procesamiento y análisis: esta fase se enfoca en procesar la información mediante un análisis que revele los niveles de importancia de todos los datos obtenidos.

5. Presentación de inteligencia: el objetivo de esta fase es dar un formato a los datos obtenidos para que sean fácilmente interpretables.

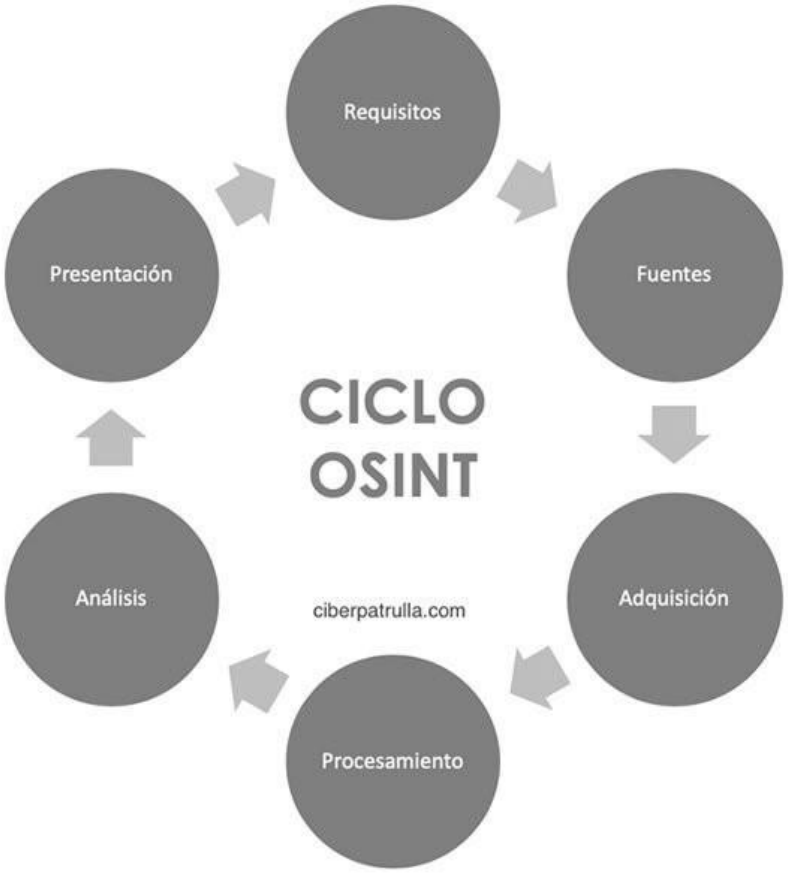


Figura 17. Fases del proceso OSINT.

A continuación, se identifican los tipos de herramientas OSINT para obtener información relevante, mencionados por Ciberpatrulla:

1. Motores de búsqueda genéricos: son los buscadores web convencionales como Google, Yahoo!, Bing, etc. En este tipo de buscadores se requiere del uso de formas de búsqueda avanzada (empleando un tipo de expresiones regulares) que permita encontrar información de interés. Esta forma de búsqueda se llama “Hacking con buscadores”.

2. Buscadores especializados: estos motores de búsqueda están diseñados para efectuar búsquedas de información específica. Por ejemplo, sobre personas, para encontrar

direcciones de email y por detección de información en base a imágenes. Este tipo de búsqueda se llama “búsqueda inversa”.

Algunos ejemplos de este tipo de buscadores:

- Buscador personalizado de Google para OSINT: https://cse.google.com/cse/publicurl?cx=012209864558240645678:orirysy9yqk
- eTools - Buscador en simultáneo sobre 16 motores de búsqueda: eTools.ch - The Transparent Metasearch Engine from Switzerland
- Carrot2 -Buscador que agrupa los resultados por categorías: Carrot2 search results clustering engine

3. Social Media Intelligence: existen herramientas para recopilar información a través de las redes sociales. En particular, SOCMINT es el acrónimo de Social Media Intelligence y se puede traducir como inteligencia basada en las redes sociales[17]. Esta utilidad se basa en obtener información a través de redes sociales para analizarla y convertirla en conocimiento. La información abarca conversaciones, mensajes, publicaciones, imágenes, videos y cualquier otro tipo de elemento publicado.

4. Extracción de metadatos: corresponde con el análisis de metadatos de una imagen. Estos datos son los que se encuentran ocultas en el código informático de los archivos. En particular, se encuentra una técnica específica llamada IMINT[18] o “Inteligencia de Imágenes”. Esta técnica se basa en analizar imágenes terrestres, aéreas y satelitales para analizar las zonas, identificar puntos de interés y ubicar lugares propios de la víctima según sus publicaciones.

5. Protección de identidad: se trata de herramientas para no dejar expuestos los datos de la persona que está haciendo uso de esta metodología OSINT. En ese caso, si es un atacante, serán las herramientas que podrá usar para que no sea detectado. Dentro de estas herramientas, se pueden mencionar aquellas que permiten crear un “avatar anónimo”[19], ocultar la dirección IP, crear emails o número de celular falsos, etc. Se denomina "avatar” a una identidad ficticia que permite asumir una descripción de persona para registrarse en webs específicas, servicios de correo electrónico y redes sociales siendo otra persona.

[17] Fuente SOCMINT: https://ciberpatrulla.com/socmint-social-media-intelligence/
[18] Fuente IMINT: https://ciberpatrulla.com/imint-inteligencia-de-imagenes/
[19] Fuente avatar anónimo: https://ciberpatrulla.com/fakenamegenerator/

6. Geolocalización: se trata de herramientas para detectar la ubicación de una persona, sitio web, saber desde qué lugar se tomó una foto, etc.

En la siguiente sección se describen con mayor detalle las herramientas mencionadas.

4.4 Herramientas OSINT empleadas para recolección de información

4.4.1 SOCMINT - Inteligencia basada en las Redes Sociales

La búsqueda basada en Redes Sociales tiene 4 fundamentos básicos:

- Escucha activa: este fundamento es el principal porque se basa en establecer el objetivo del análisis de la Red Social. Aquí el atacante identificará a la víctima, a su grupo de confianza, a la empresa de trabajo asociada, a otras locaciones, etc. Con este objetivo identificado, el foco se pone en prestar atención a todo aquello que los usuarios de las redes sociales publican y mencionan.
- Gestión de datos: corresponde con la organización y segmentación de los datos obtenidos en el punto anterior mediante la escucha activa. Esto incluye ordenar la información de manera de facilitar la comprensión. Algunos parámetros que se pueden recopilar y ordenar:
  - Número de comentarios de las publicaciones
  - Comentarios destacados
  - Cantidad de "Me gusta"
  - Veces que se comparten las publicaciones
  - Hora y fecha de las publicaciones
- Analítica avanzada: consiste en hacer un análisis profundo y seleccionar los datos relevantes para la investigación de la Red Social. En este punto, un atacante aplicará su sentido para identificar la información más valiosa que necesita para perpetrar su cometido.
- Conclusión y elaboración de informe: la finalidad del atacante será tener toda la información compilada para diagramar su plan de ataque.

El atacante seguirá este proceso SOCMINT definido especialmente para las Redes Sociales dado a que aprovechará la exposición de la víctima todas las plataformas donde tenga definido perfiles. Por ende, su plan de ataque requerirá de la mayor cantidad posible de información recopilada, ordenada, clasificada y categorizada para empezar sus acciones aprovechando la exposición de la víctima y de su grupo de confianza. Esto incluirá también indagar sobre los perfiles de las Redes Sociales vinculados a las locaciones de interés del usuario objetivo, como domicilios de trabajo, educativos, deportivos, etc.

4.4.2 Creación de una Identidad Falsa

La herramienta que se promociona como básica para la creación de identidades ficticias es Fake Name Generator[20].

Por medio de este sitio web, un atacante puede definir los datos particulares de una persona ficticia que podrá usar para registrarse en otros servicios como, por ejemplo, crear su perfil asociado en una Red Social. Simplemente indicando el género de interés, la nacionalidad del nombre más el país de origen, esta plataforma generará una persona falsa con variados atributos que se podrán usar para diferentes motivos.

Según el propio sitio de este servicio, indican que no es una funcionalidad ilegal y que particularmente sirven a las fuerzas de seguridad. Incluso mencionan que los datos que usan para crear la identidad falsa son totalmente no reales y no se podrían usar para operar en servicios como compras online o para buscar empleo bajo ese perfil.

Uno de los atributos que se pueden obtener con esta plataforma es un correo electrónico "descartable". Es decir, usado para fines de registro en los sitios de las redes sociales. Esta herramienta ofrece el servicio Fake Mail Generator[21]. Desde este nuevo sitio, se puede acceder y ver los correos electrónicos recibidos en la dirección creada especialmente para la identidad falsa.

4.4.3 Extracción de "Metadatos"

Tal como se mencionó anteriormente, una parte de las herramientas usadas en OSINT tienen que ver cómo obtener la información "oculta" en las imágenes ("metadatos"). Los datos EXIF (Exchangeable Image File) o metadatos son unos parámetros informativos que contienen todas las fotografías digitales que se almacenan en un dispositivo informático.

La información que se puede obtener por medio de los metadatos comprende[22]:

- El modelo de la cámara o del teléfono móvil con el que se ha hecho la foto.
- La sensibilidad del diafragma.
- La distancia focal (si llevaba o no zoom).
- El tamaño y la resolución.
- Si se ha hecho en modo manual o automático.
- La hora y la fecha.
- Geoposición: latitud, longitud y altura desde donde se ha tomado la imagen. Puede saberse si el usuario tenía activo el GPS en el momento de hacer la foto.

[20] Herramienta Fake Name Generator: https://www.fakenamegenerator.com/
[21] Servicio Fake Mail Generator http://www.fakemailgenerator.com/
[22] Información de metadatos: https://ciberpatrulla.com/metadatos-de-fotos/

En general las herramientas para este tipo de análisis son sitios web en donde se debe subir la imagen para que se haga la revisión. Uno de ellos es Metadata2Go[23]. Básicamente, se pueden escanear distintos tipos de archivos en busca de metadatos.

Como se puede observar, el valor de un metadato para un atacante es alto. Es decir, si los usuarios toman fotografías sin tomar medidas preventivas, esos archivos digitales contendrán información adicional que le servirá a la persona malintencionada para recabar datos concretos que ayuden a identificar aún más a la persona víctima, sus locaciones y su entorno. Directamente con un metadato se podría saber desde qué coordenadas se tomó la fotografía, cual es el dispositivo incluyendo la fecha y hora. Con eso se evidencia que se puede dar con el paradero físico, en tiempo y espacio, de la víctima o persona que tomó la fotografía. Aquí aparece nuevamente el concepto de Usuario Puente y el concepto de Usuario Expuesto Pasivo. Esto es así, porque una fotografía puede incluir a otras personas vinculadas a la víctima y por medio de los metadatos, dar con datos concretos sobre la locación y entornos vinculado a esos contactos relacionados con el objetivo.

En definitiva, también al tomar fotografía y subirla, se evidencia una exposición inherente a ese elemento a subir que se suma junto con la forma en que esa imagen se mostrará en el perfil particular del usuario. Es decir, si un usuario expone una foto en su perfil de manera pública, sin restricciones y, además, esa foto fue tomada sumando metadatos, entonces se estaría frente a la presencia de un Factor de Incremento de Exposición.

4.4.4. Scraping en las Redes Sociales

Existe un concepto vinculado a la recopilación de información de las Redes Sociales denominado Scraping, cuya traducción es “raspado”.

Considerando lo que define el proveedor de herramientas de seguridad Proofpoint[24], esta técnica se hace "raspando" la superficie pública de las plataformas por medio de programas automáticos para tomar cualquier información que esté disponible sobre los usuarios. En teoría, la mayoría de los datos se pueden encontrar simplemente seleccionando perfiles individuales de redes sociales.

Lo interesante de esta técnica es que los datos obtenidos son públicos. Es decir, si bien el usuario que busca “raspar” los perfiles digitales necesita tiempo y uso de herramientas, esa información es la que lo dueños de los perfiles deja como pública sin restricciones. Por ende, no se puede hablar de un delito o acción punible. En un artículo de la BBC[25] se comparte la opinión del experto en seguridad Troy Hunt. Este profesional indica que no le preocupan tanto los incidentes de scraping y afirma que debemos aceptarlos

[23] Metadata2Go: https://www.metadata2go.com/
[24] Proofpoint: https://www.proofpoint.com/us/threat-reference/social-media-threats
[25] Artículo BBC: https://www.bbc.com/mundo/noticias-57835205

como parte del hecho de que nuestro perfil es público. Citando textualmente: “Definitivamente, no se trata de infracciones. La mayoría de estos datos son públicos de todos modos. La pregunta que debe formularse en cada caso es cuánta de esta información es de acceso público por elección del usuario y cuánta no se espera que lo sea".

Dicho artículo menciona también el evento de scrapping que sufrió LinkedIn. En junio de 2021, un hacker llamado Tom Liner, compiló en una base de datos la información de 700 millones de usuarios de LinkedIn de todo el mundo y la puso a la venta por US$5.000. Según sus declaraciones, lo hizo "por diversión".

La esencia de un ataque no discrimina por objetivos. Si hay algo que identifica a un atacante es que no tiene restricciones para lograr sus objetivos a cualquier precio. Internet es el gran medio que permite que cualquier ataque se pueda perpetrar desde cualquier lugar del mundo y que los delincuentes tengan en su poder el mapa completo para encontrar a sus víctimas. La clave está en la conducta como usuarios de las personas; en entender, aprender y aplicar las medidas posibles de mitigación y protección sobre las redes sociales digitales.

La exposición inadecuada de información personal en redes sociales digitales no solo representa un riesgo para la privacidad de las personas, sino que también ofrece a las atacantes oportunidades para iniciar sus ataques. La comprensión de las dinámicas de los ataques basados en ingeniería social es fundamental para desarrollar estrategias defensivas que protejan tanto a los usuarios como a sus círculos sociales. Es importante fomentar una cultura de prevención y responsabilidad en el uso de las plataformas sociales digitales, donde cada publicación y cada interacción se consideren con un enfoque crítico, garantizando así la seguridad en un entorno cada vez más vulnerable.

Adicionalmente, es importante destacar que la anatomía de un ataque a redes sociales revela un panorama en el que la inadecuada gestión de la privacidad puede abrir la puerta a una variedad de amenazas. La interacción entre usuarios, los perfiles digitales y la información expuesta se convierten en un terreno fértil para los atacantes, quienes explotan la confianza y las conexiones sociales para llevar a cabo sus ataques. Es esencial que tanto los usuarios como las plataformas de redes sociales digitales adopten una postura proactiva en la educación y la implementación de medidas de seguridad.

También, como parte de este capítulo, se analizó OSINT (Open Source Intelligence). Este conjunto de técnicas y herramientas son destinadas a recopilar y analizar información pública disponible en Internet, con el objetivo de extraer conclusiones que pueden ser utilizadas en diversas aplicaciones, incluidos ataques a perfiles digitales. El uso de estas metodologías destaca la importancia de la educación del usuario sobre la exposición de su información en redes sociales y la necesidad de implementar medidas de protección para mitigar los riesgos asociados.

Capítulo 5: Modelo conceptual de perfiles, amenazas y formas de mitigación.

Para caracterizar las diferentes formas en que las personas se exponen en redes sociales digitales, es importante introducir y desarrollar el concepto de Perfil Biográfico Digital. Un Perfil Biográfico Digital, tal como se describe en el trabajo de investigación "Caracterización de los perfiles biográficos digitales en Facebook de adolescentes de Rafaela y Sunchales" (Balbiano y colab., 2014), abarca al conjunto de datos propios de una persona que publica en una plataforma de Red Social, en una página que lo identifica. Generalmente se lo conoce directamente como el "perfil" de una persona. Con la proliferación de las Redes Sociales Digitales, las personas comenzaron a mostrar sus perfiles, sus personalidades y estilos de vida mediante la exposición en dichas plataformas ampliando los límites de la privacidad.

El concepto de Perfil Biográfico (sin enmarcarlo en el contexto digital) está asociado a las características, gustos, formas de pensar e intereses que una persona tiene y de alguna manera busca compartir con otros. Si se unen los conceptos de perfil con el de red social, se conjugan entonces los objetivos comunes: las redes sociales surgen para compartir entre personas diferentes tipos de información que hacen a la esencia de cada una, y cada persona tiene un perfil dado y busca relacionarse con quienes de alguna manera tienen intereses similares. En ese deseo por compartir gustos e intereses entre personas, aparece el riesgo de la sobreexposición, que significa una manera no adecuada de armar un perfil biográfico digital sobre una red social que puede comprometer a la privacidad de una persona y ser la ventana abierta a diferentes ataques.

En esta sección se presenta un modelo conceptual (Fig. 21) para publicaciones en perfiles biográficos digitales. El modelo permite identificar los principales conceptos y relaciones para comprender el dominio de la privacidad en redes sociales y sirve de base para la implementación de herramientas informáticas de concientización de usuarios.

Se parte del concepto de Red Social Digital, que refiere a un grupo de personas que están conectadas entre sí por medio de una plataforma de software que oficia de mediadora y brinda el soporte para que cada individuo tenga definido su Perfil Biográfico Digital (PBD) y pueda entablar comunicación con otros individuos en la red. Este perfil constituye la configuración inicial que un Usuario (persona) crea para empezar a utilizar las funcionalidades de la plataforma de RSD. Contar con un Perfil Biográfico Digital es el primer paso para comenzar a adquirir exposición. Para comenzar a describir el modelo, se presenta la primera parte en la siguiente figura 18.

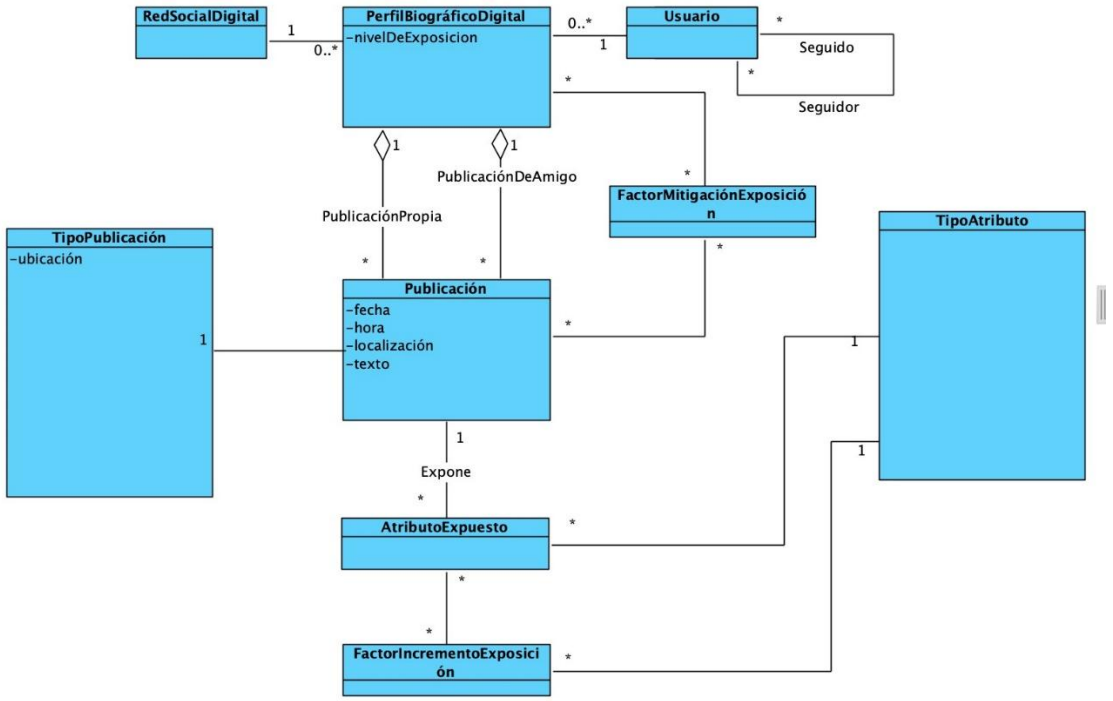


Figura 18. Conceptos fundamentales de un Perfil Biográfico Digital.

Un *Usuario* de una red social digital presenta algún tipo de relación con otro/s *Usuario/s* de la misma red, y, en consiguiente puede generar interacción y compartir contenido como si fueran "conocidos". Dependiendo de la RSD, esta relación se conoce con el término de *contacto*. En el caso de Facebook, los contactos son llamados "Amigos". Para el caso de Instagram, un contacto es llamado "Seguidor" (o "Follower"). En ese sentido, un determinado usuario tendrá un número de "Seguidores" y un número de "Seguidos" ("Following"). Para el caso de Instagram, el tipo de Contacto es unidireccional. Si un usuario A solicita seguir a un Usuario B, y si el Usuario B acepta, no significa que ese Usuario B puede ahora ver los contenidos del Usuario A, es decir el Usuario A se convierte en *Follower* del Usuario B. Por otro lado, tiene que haber un pedido del Usuario B para seguir al usuario A, y la aceptación correspondiente, para que el Usuario B se transforme en *Follower* del Usuario A, y así emparejar el acceso. Para la red LinkedIn, los contactos son llamados "Conexiones". Un usuario puede optar por conectarse con otro usuario para convertirse en *contacto,* comenzar a interactuar directamente, y ver los contenidos publicados. En la Fig. 1.1 se simplifican todas estas variaciones considerando un RSD genérica, y estableciendo una relación entre usuarios indicando los roles *seguidor* y *seguido.*

Continuando con la descripción del modelo, en la siguiente figura 19, se observa que, en cada *PBD*, un usuario comienza a efectuar publicaciones (*Publicación*). Las mismas se clasifican en tipos (*TipoPublicación*)

y tienen una propiedad denominada *Ubicación* que indica el lugar o sección que tiene la publicación en el *PBD*.

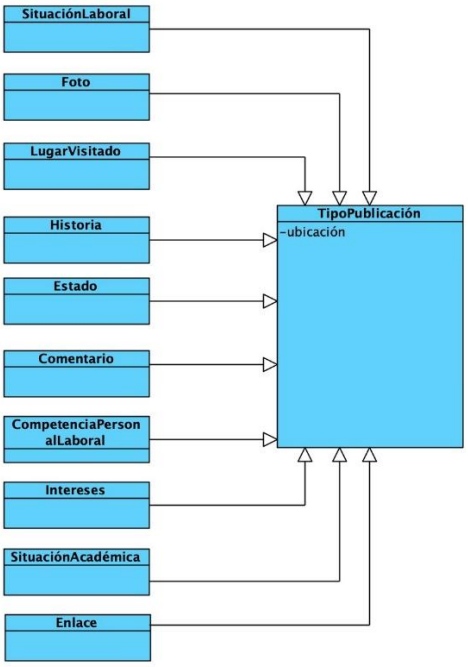


Figura 19. Segunda parte Modelo conceptual de Perfil Biográfico Digital.

Esta clasificación de tipo de publicaciones se presenta en la Tabla 2, y se define el correspondiente tipo como especializaciones del concepto *TipoPublicación* en la Fig. 19.

Tabla 2. Tipos de publicaciones y sus atributos.

TipoPublicación	Ubicación
1. Comentario	1.1. Muro / Página central perfil
	1.2. En otro tipo de publicación (fotos)
2. Foto	2.1. Portada
	2.2. Perfil
	2.3. En muro / página central perfil
3. Enlace	
4. Intereses	4.1. Personales
	4.2. Laborales
5. LugarVisitado	
6. Historia	
7. Estado	
8. SituaciónLaboral	8.1. Actual
	8.2. Antecedentes
9. SituaciónAcadémica	9.1. Nivel de estudios
	9.2. Institución educativa
10. CompetenciaPersonalProfesional	

En la Tabla 2 también se presentan los posibles valores que puede tomar la propiedad *Ubicación* según el tipo de publicación que se trate. Puede observarse que para ciertos tipos de publicaciones el valor de la ubicación no es relevante.

Cada Publicación en un PBD puede implicar la exposición de ciertos atributos o de aspectos del PBD (representado por AtributoExpuesto, Fig. 18). Por ejemplo, cuando un usuario publica la foto de portada de un perfil, se estará efectuando una cierta exposición dependiendo de qué se identifique en esa foto. A continuación, se observa la Figura 20 que representa la tercera parte de la descripción del modelo.

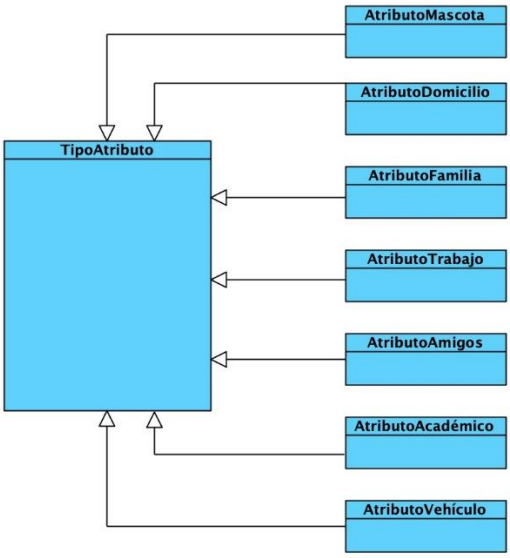


Figura 20. Tercera parte del Modelo conceptual de Perfil Biográfico Digital.

En el modelo conceptual se describe que un *AtributoExpuesto* es de cierto tipo (*TipoAtributo*). El tipo de atributo indica a qué conjunto de aspectos relativos al usuario o su perfil biográfico digital corresponde un atributo. Por ejemplo, el nombre de la mascota del usuario, la raza, la veterinaria en donde es asistido, etc. corresponden al tipo *AtributoMascota;* el nombre de los hijos, la escuela a la que asisten, si tiene pareja o su estado civil, datos sobre sus padres, etc. corresponden al tipo *AtributoFamilia.* Para catalogar los posibles tipos de atributos que pueden ser expuestos, se propone una tipificación de los tipos mismos. Esta tipificación se explicita en la primera columna de la Tabla 3. Se debe considerar que, para una Publicación, se pueden tener más de un tipo de atributo expuesto.

Vale aclarar que, en el alcance de este trabajo, no es de interés conocer qué datos privados son expuestos (o podrían ser expuestos) en una publicación, es decir, conocer el valor de un atributo expuesto. Lo que es de interés es qué tipo de datos son expuestos (o podrían ser expuestos) en una publicación por el usuario de una RSD, ya que el objetivo final del modelo conceptual es generar herramientas para alertar a

un usuario sobre qué tipos de datos podría dar a conocer con una potencial publicación, y crear conciencia de si es realmente su voluntad hacerlo.

Por otro lado, un tipo de atributo puede verse potenciado por diversos factores que generen un incremento en la exposición propia de ese tipo de atributo. En la Fig. 18 esto es representado por el concepto *FactorIncrementoExposición* (FIE). El concepto de *Factor de Incremento de Exposición se* refiere a aquellas características y comportamientos de los usuarios en las redes sociales digitales que potencian el nivel en que se expone su persona. Es decir, estos factores son elementos que facilitan que un flujo de exposición tenga resultados satisfactorios para un potencial atacante que quiere aprovecharse de la información, que, tal vez, un usuario involuntariamente o sin conocimiento deja expuestos.

Tabla 3. Tipos de atributos y sus Factores de Incremento de Exposición.

Tipo de Atributo	Factor de Incremento de Exposición
1. Datos de Domicilio (Casa, Departamento, Oficina de Trabajo, Locación temporal) representado por *AtributoDomicilio*	1. Existencia de puertas y/o ventanas 2. Tipo de puertas y ventanas 3. Existencia de sensores de alarmas 4. Existencia de cámaras de seguridad 5. Tipo de habitación: dormitorio, comedor, living, patio. 6. Cantidad de habitaciones 7. Tipo / Estilo de mobiliario: por semejanza en distintas fotos, se puede inferir la cantidad de habitaciones del domicilio. 8. Logos / Marcas en objetos y/o prendas de vestir depositadas en la habitación que lleven alguna identificación de una institución como puede ser escolar, un club, empresa, etc. 9. Reflejos por superficies como vidrios, espejos, cromados y otras superficies brillosas. Pueden mostrar otras partes, personas y objetos identificatorios de donde se encuentra el usuario.
2. Datos de Vehículos. Representado por *AtributoVehículo*	1. Marca, modelo, color. 2. Patente / Dominio. 3. Rasgos particulares únicos (calcomanías, marcas, rayones, choques, etc.). 4. Referencias a ciudades / locaciones / empresas en el caso de un vehículo de flota laboral. 5. Lugar de estacionamiento. Ej.: una playa de estacionamiento particular. 6. Zonas aledañas al lugar de estacionamiento. 7. Puntos de referencias (negocios, casas, otros vehículos)
3. Datos de Familia. Representado por *AtributoFamilia*	1. Cantidad de integrantes y posible parentesco. 2. Identificación de menores. 3. Fechas y/o acontecimientos particulares (cumpleaños, casamientos, etc.)

	4. Locaciones relacionadas a la familia (casas de padres, vecinos, etc.) 5. Mascotas de familia 6. Vehículos de familia
4. Datos de Amigos. Representado por *AtributoAmigos*	1. Cantidad de amigos. 2. Rangos etarios. 3. Viviendas y locaciones relacionadas. 4. Familiares y/o contactos de los amigos. 5. Vehículos de amigos 6. Mascotas de amigos 7. Lugares de uso común como clubes, negocios, etc. 8. Eventos / Acontecimientos (cumpleaños, encuentros, aniversarios).
5. Datos de Mascotas. Representado por *AtributoMascota*	1. Cantidad y tipo con raza. 2. Rasgos distintivos únicos: collar, cadenitas, colgantes, tapados, ropa especial. 3. Locaciones de las mascotas. 4. Conductas relacionadas al paseo de las mascotas. 5. Personas con mayor afinidad a las mascotas.
6. Datos de Trabajo. Representado por *AtributoTrabajo*	1. Nombres de otros empleados de la misma empresa y sector (pueden venir por comentarios de colegas y usos de hashtag). 2. Correos electrónicos y la derivación de la estructura del "usuario" que se usa en la empresa para los correos electrónicos. 3. Fotos de presentación, primer día, onboarding en redes sociales. Es más común en la red social LinkedIn. (Puede incluir pantalla con aplicaciones, tipo de computadora, metodología o pasos a seguir (hoja de bienvenida) y la tarjeta de fichaje o identificación personal: nombre completo, foto, sector). 2. Presentaciones con información corporativa. 3. Escritorio de la computadora, evidenciado los programas que se usan. 4. Espacios físicos de la empresa y/o usuarios. 5. Software institucional de uso entre empleados. Ej.: G-Suite, MS Teams, Cisco. 6. Plataformas de correo electrónico. 7. Interfases de desarrollo de software. 8. Marca y modelo de la computadora. 9. Sistema Operativo. 10. Navegador de Internet: URL de páginas abiertas 11. Estructura de las páginas web, secciones 12. Contactos vinculados / corporativos 13. Aplicaciones instaladas y/o en ejecución 14. Disposición de las oficinas, escritorios. 15. Tipos de computadoras y posición según pasillos, ventanas. 16. Personas en la misma locación trabajando: cantidad, ubicaciones, posible identificación de sector. 17. Personal relacionado: mantenimiento, limpieza, etc.

	18. Posición de máquinas de impresión, escáneres, trituradoras de papel, máquinas de café, etc. 19. Ubicación de cámaras de seguridad y sensores de alarma / incendio. 20. Ubicación de puertas, ventanas y sistema de control de acceso físico. Ejemplo: presencia de vigilancia y uso de tarjeta magnética para aperturas de puertas.
7. Datos de Académicos (*AtributoAcadémico*)	1. Nombre y locación de institución educativa. 2. Nombres de profesores y alumnos. 3. Disposición física de las aulas. 4. Ubicación de las aulas. 5. Nombres de personal perteneciente a la institución educativa. 6. Ubicaciones físicas de las distintas dependencias de la institución: Secretarías, Alumnado, Dirección, etc. 7. Datos presentados en los pizarrones de las aulas. 8. Disposición de las puertas de ingreso y ventanas. 9. Existencia de guardias de seguridad. 10. Existencia de control de acceso con molinete u otro sistema. 11. Existencia y ubicación de cámaras de seguridad.

En la Tabla 3, esto es detallado en la segunda columna, catalogándose de esta manera un conjunto de posibles factores de incremento de la exposición por tipo de atributo.

Cada tipo de atributo expuesto implica un incremento en el nivel de exposición que tendrá el perfil de la red social. Por ejemplo, cuando en la foto de portada que selecciona un usuario (instancia de *Publicación,* cuya propiedad *ubicación* toma valor *Portada*), se exponen datos relativos a familia (en este caso, el tipo de atributo expuesto es *AtributoFamilia*). Pero, además, frecuentemente se está frente a otros Factores de Incremento de Exposición, cuando se pueden identificar por medio de esa foto otros aspectos como nombre de los menores en la familia, cantidad de integrantes, etc. para obtener información adicional del grupo familiar (instancias de *FactorIncrementoExposición*). En conclusión, desde una determinada publicación seleccionada por el usuario, la misma puede incrementar su nivel de exposición por intermedio de estos factores adicionales, que son pertenecientes de manera inherente al tipo de atributo expuesto utilizado. El concepto *Atributo Expuesto* agrega (reúne) todos *los Factores de Incremento de la exposición* que pueden existir para ese tipo de atributo expuesto en la publicación.

Considerando lo presentado sobre el modelo, se establece el concepto de “Flujo de exposición”. Hace referencia a un conjunto de pasos que pueden aplicarse para descubrir información privada de un usuario que ha quedado expuesta, o, para conocer cuál es el nivel de exposición que posee un usuario en sus redes sociales.

Este concepto se relaciona al conjunto de pasos que, al seguirlos en un determinado orden, pueden determinar cómo se releva la exposición de un usuario y en su defecto, cuál es el nivel de esta. Esto significa, cuán expuesto está un usuario por medio de sus redes sociales.

Los buscadores de Internet son las principales herramientas para llevar a cabo el primer paso de un flujo de exposición (Google, es uno de los buscadores más reconocidos y utilizados). Por lo tanto, el primer paso de este flujo es "googlear" al objetivo, a la persona sobre la cual se quiere averiguar su nivel de exposición.

Generalmente, como primer resultado de una búsqueda por "Nombre y Apellido", se obtienen los vínculos a perfiles de Facebook o LinkedIn.

A continuación, para definir los siguientes pasos, se deben conocer los factores que incrementan la posibilidad de éxito para un proceso de rastreo de exposición. Aquí entran en juego los antes mencionados Factores de Incremento de Exposición. Retomando dicho tema, se demuestra que os factores de exposición más frecuentes están dados por la existencia de perfiles en redes sociales y el uso de fotos de perfil, es decir, cargadas como identificatorias del usuario, que confirmen explícitamente que la persona hallada es el objetivo deseado. En estos casos, el descubrimiento es "directo". Este primer factor de exposición se denomina "Indicio de Exposición", ya que es la primera condición para iniciar un flujo de exposición de un usuario. Es el punto de partida para tener una sospecha de que el usuario puede tener un nivel de exposición inadecuado que podría ser explotado. El hecho de que la exposición de un usuario pueda ser explotado, implica que un posible atacante tendrá la forma de obtener información de su perfil para usarla en beneficio de un acto malicioso.

El siguiente paso en el flujo de exposición será ingresar a cada perfil biográfico digital de la red social (PBD) detectado por medio de la búsqueda en Internet, para continuar con el descubrimiento de factores de exposición adicionales. Una ventaja importante que se relaciona a este paso se presenta si el atacante cuenta con un perfil en cada red social a verificar. Esto constituye un nuevo factor de incremento a la hora de tener éxito en el rastreo del usuario. Esto significa que, si se desea explotar la información expuesta por el perfil del objetivo en la red social Facebook, entonces se incrementarán las chances de lograr resultados si quien realizará la verificación ya cuenta con un perfil en esa misma plataforma.

En resumen, sobre el Flujo de Exposición, existen tres puntos clave en cómo los atacantes engañan a los usuarios para que caigan en la trampa:

1- Captación de Factores de Exposición
2- Generación de perfiles ficticios de manera personal o basándose en entidades
3- Establecimiento de contacto

Además de los Factores de Incremento de Exposición, existen otros factores que impactan sobre las publicaciones del usuario, atenuando o mitigando los efectos de la exposición. Éstos se denominan Factores de Mitigación de la Exposición (FME), representado en el modelo conceptual con el concepto *FactorMitigaciónExposición*, y como puede observarse en la Fig. 1, se relaciona directamente con *Publicación* o *con el Perfil Biográfico Digital*. Por ejemplo, publicar una foto y que ésta sólo sea accesible por los "amigos" del usuario, es una forma de mitigar una exposición. Este tipo de mitigaciones actúan a nivel de Publicación en general y a nivel del perfil biográfico del usuario, siendo configuraciones propias de cada plataforma.

Cada uno de los Atributos que una persona expone en su Perfil Biográfico Digital, forma parte de un elemento utilizable para tal fin en la plataforma de la Red Social elegida. Sobre ese Atributo en particular, accionarán los Factores de Incremento de Exposición y los Factores de Mitigación. En ese sentido, dada una determinada foto publicada, si en la misma se observa información adicional que genera mayor exposición, se puede ir incrementando la misma considerando los distintos factores que se exponen. Ejemplo: Si en una foto de Instagram de un usuario, en la misma se puede observar la vista de su domicilio y se acompaña de una vista de su auto más una mascota, entonces se está frente a una exposición incrementada por dichos factores presentes en la fotografía.

Para minimizar la exposición en una publicación, se debe alcanzar una solución de compromiso que tienda a anular a los factores de incremento de exposición, para balancearlos con los factores de mitigación y lograr una exposición adecuada. Una buena práctica para lograr una adecuada exposición es que el usuario al momento de hacer una publicación o configuración favorezca a los factores que atenúan la exposición y minimice los factores de incremento de exposición.

Adicionalmente, el modelo conceptual planteado, permite a partir del concepto Perfil Biográfico Digital calcular lo que se denomina una *Exposición en cadena.* Así, observando los diferentes tipos de atributos expuestos en diferentes publicaciones de un perfil, podría inferirse información del usuario más amplia, que abarque diversos tipos de atributos con varios factores de incremento de la exposición. Un ejemplo de exposición en cadena es el siguiente: un usuario publica una foto con su grupo de amigos, mencionando los nombres de cada uno de ellos. Posteriormente, pasado un tiempo, publica una nueva foto mostrando una locación de un club, en donde hará un deporte en particular. Luego de esa publicación, a un tiempo posterior, genera una nueva fotografía de una cena con el mismo grupo de amigos en donde se puede apreciar y se menciona el lugar. Con esas tres fotos, correspondientes a Atributos Expuestos de su Perfil Biográfico Digital, dicha persona está brindando información valiosa para un atacante. Entonces, el atacante conocerá: el grupo de amigos con sus nombres, el horario y lugar de las fotos, el deporte que practican con sus amigos, el hábito de cenar luego de la actividad deportiva con sus amigos.

Dentro del grupo de usuarios vinculados con las redes sociales digitales, existe un grupo particular que se compone de los “Usuarios Expuestos Pasivos”. Son aquellas personas (usuarios) cuya privacidad es expuesta por intermedio de publicaciones de otras personas (usuarios) vinculadas a su perfil en una red social digital. Estas personas no se exponen por sí mismas, sino que son expuestas por intermedio del perfil digital que es propiedad de otra persona.

El concepto de “Usuario expuesto pasivo” es análogo al de “fumadores pasivos”, es decir, el grupo de personas que por sí mismas no fuman pero que están en contacto en ambientes con personas fumadoras y por ende perciben los mismos efectos que el tabaco al igual que si lo consumirían. Esta situación se presenta cuando desde un perfil digital determinado se exponen a personas, sin su autorización y elevando el riesgo vinculado a la exposición. Esto implica que, si se desea medir o cuantificar la exposición de un usuario de redes sociales, no solo debe considerarse la configuración de privacidad y puntos de exposición del usuario, sino también cómo otros usuarios pueden contribuir a la exposición.

En base a lo expresado anteriormente, el modelo, además, permite inferir para un PBD esta condición de *SujetoExpuestoPasivo*. En este caso, a través de la presencia de instancias de publicaciones con alta exposición realizadas por amigos de un PBD, sería posible inferir que un usuario tiene cierto nivel de exposición debido a publicaciones en donde se encuentra arrobado o etiquetado. Una persona, en su perfil de la red social digital, podría incurrir en una exposición involuntaria de un amigo o familiar que no necesariamente quiere o desea ser expuesto. Cuando se comparte una foto de un familiar, por ejemplo, en la misma puede haber presencia de niños y, con ello, se exponen sus características físicas o identidades a un posible atacante. Lo mismo sucede cuando se comparte una foto de un evento en una escuela, en la que aparecerán posiblemente niños vinculados.

En conclusión, el capítulo establece un marco conceptual para analizar cómo los perfiles biográficos digitales en redes sociales pueden implicar riesgos de exposición de información privada. A través del desarrollo de un modelo conceptual, se identifican los tipos de publicaciones, los atributos expuestos y los factores de incremento de exposición, que permiten comprender las vulnerabilidades inherentes a cada perfil de usuario. Además, se introduce la idea del "Flujo de Exposición" como un proceso de pasos sistemáticos que podría ser utilizado tanto para rastrear la exposición del usuario como para concienciarlo respecto al tipo de información que comparte. El modelo también presenta factores de mitigación como una capa adicional de control, destacando la importancia de la configuración de privacidad y el uso responsable de las plataformas digitales. Este análisis sirve de base para futuras herramientas de concientización en seguridad y privacidad, promoviendo prácticas de publicación seguras y protegiendo la integridad de la información personal en el entorno digital.

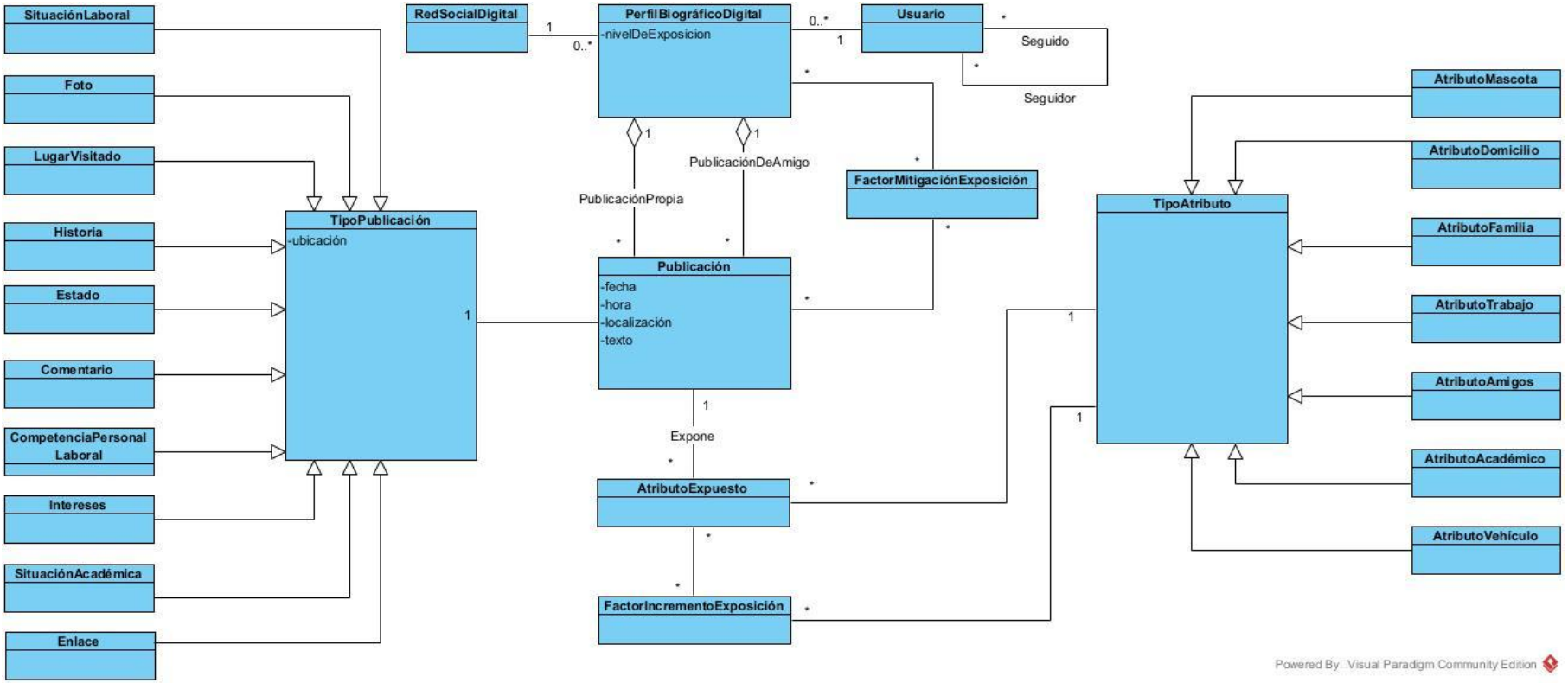


Figura 21. Modelo conceptual de Perfil Biográfico Digital.

Capítulo 6: Métricas propuestas para cuantificar la exposición de un Perfil Biográfico Digital

El creciente uso de redes sociales digitales ha dado lugar a una amplia exposición de información personal, lo que plantea riesgos para la privacidad de los usuarios. Con la finalidad de evaluar esta exposición, el modelo conceptual de PerfilBiográficoDigital incorpora el atributo nivel de exposición, cuyo valor puede calcularse mediante un conjunto de métricas diseñadas para tal fin. Estas métricas permiten medir el grado de exposición de diversos atributos de un perfil y de sus publicaciones, proporcionando una comprensión del nivel de privacidad comprometido.

Conocer el nivel de exposición de un perfil es fundamental, ya que permite a los usuarios comprender mejor cómo ciertos aspectos de su vida personal pueden estar siendo exhibidos más allá de lo que desean o incluso sin su conocimiento. Las métricas no solo facilitan esta identificación, sino que también permiten tomar acciones para reducir o mitigar la exposición. Al ofrecer un valor cuantificable del nivel de exposición, estas herramientas posibilitan una autogestión de la privacidad y fomentan una interacción más segura en las redes sociales.

En el modelo conceptual para PerfilBiográficoDigital se definió el atributo *nivel de exposición* (*nivelDeExposición*).

Para calcular el valor de este atributo se definen un conjunto de métricas que se basan en los conceptos representados.

1. Métrica para calcular el valor de exposición de un atributo *i* en una publicación *p*

*VE_ip = AtributoExpuesto_i * Sumatoria(FIE_ip)/Cantidad total de FIE para el tipo de atributo de i.*

AtributoExpuesto_i toma valor 1 o 0, si hay presencia o no de ese tipo de atributo en la publicación *p*. Se calcula como la sumatoria de todos los factores de incremento de la exposición que posee el atributo expuesto, dividido la cantidad de factores de incremento de la exposición posibles por tipo de atributo.

Se supone que si se calcula esta métrica es porque la publicación *p* expone el atributo *AtributoExpuesto_i .* Caso contrario el valor de la métrica es 0. Interpretación: se obtiene un valor entre 0 y 1, cuanto más cercano a 1, mayor es la exposición del tipo de atributo expuesto.

2. Métrica para calcular el valor de exposición en una publicación p

*VE_p = FME_p * Sumatoria(*VE*_ip) / Cantidad total de TipoAtributo*

FME_p toma valor 1 o 0 si un factor de mitigación es aplicado o no para la publicación *p.* Este valor de mitigación es aplicado como producto a una sumatoria. La sumatoria se calcula sobre los resultados obtenidos en el cálculo de todas las métricas *VE_ip* para todos los atributos expuestos *i* por la publicación *p*, obteniéndose un valor de exposición para la publicación. Si existe mitigación, el valor de *VE_p* se anula, caso contrario, será mayor a cero. Dado que los tipos de atributos posibles de encuentran tipificados, se conoce la cantidad total de ellos. Dividiendo la sumatoria por esta cantidad, se obtiene un valor entre 0 y 1.

Interpretación: cuanto más cercano a 1 sea el valor de *VE_p* más aspectos de privacidad del usuario son expuestos en la publicación.

3. Métrica para calcular el nivel de exposición de un PBD pbd

VE_ *pbd = FME_pbd * (Sumatoria(VE_p) + Sumatoria(VE_pp))*

FME_pbd toma valor 1 o 0 si un factor de mitigación es aplicado o no para al perfil biográfico digital. Este valor de mitigación es aplicado como producto a la suma de dos sumatorias. La primera sumatoria se calcula sobre los resultados obtenidos en el cálculo de todas las métricas *VE_p* para todas las publicaciones *p* de un perfil biográfico digital *pbd*, obteniéndose un valor de exposición para el *pbd*. La segunda sumatoria, se calcula sobre los resultados obtenidos en el cálculo de todas las métricas *VE_p* para todas las publicaciones *pp* de los amigos del perfil biográfico digital *pbd* en los cuales ha sido etiquetado, obteniéndose un valor de exposición para el *pbd* como sujeto expuesto pasivo. Si existe mitigación a nivel del PBD, el valor de *VE_pbd* se anula (o disminuye), caso contrario, será mayor a cero. Dado que la cantidad de publicaciones de un perfil es variable, la interpretación de esta métrica es: el valor de *VE_pbd* puede ser 0, si se aplica correctamente mitigación, o mayor a 0 si no se aplica mitigación, siendo más alto cuando más publicaciones con exposición existen.

Podría proponerse una variación de esta métrica si se considera que existen más de un nivel de mitigación posible *FME_pbd,* pudiendo tomar valores entre 0 y 1.

La métrica *VE_pbd* es la que se emplea para calcular el *NivelExposición* de un PBD. Se pueden definir rangos para indicar niveles de exposición Alto, Medio, y Bajo.

Casos de estudio

A continuación, se desarrollan casos de estudio en la red social Facebook donde se aplican los conceptos definidos (Fig. 2). En una primera muestra, se considera un PBD que contiene una publicación del tipo *Foto*, cuyo valor de atributo *ubicación* es el Muro del usuario. Se presenta además el diagrama de objetos para este PBD basado en el modelo conceptual. A partir de la fotografía se pueden identificar los siguientes

tipos de atributos expuestos: *ADomicilio1:AtributoDomicilio* (valor igual a 1) y *AVehiculo1:AtributoVehiculo* (valor igual a 1).

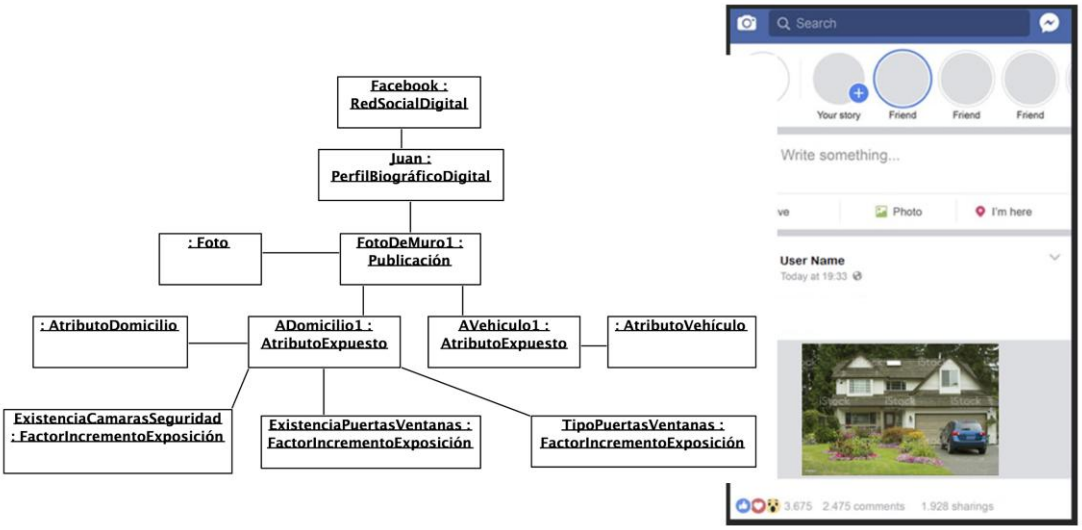


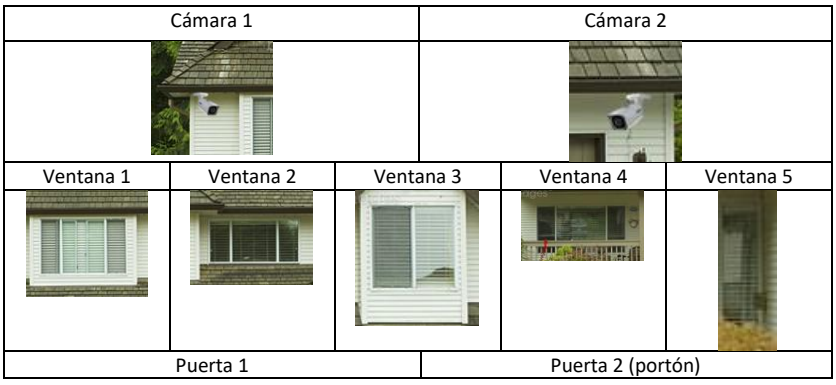
Figura 22. Instancias intervinientes en una publicación en Facebook con foto en muro. Fuente[26]

A continuación, en la Fig. 3 se identifica los factores de incremento de la exposición que pueden identificarse para el atributo expuesto *ADomicilio1* (*AtributoDomicilio*).

FIE_ ADomicilio1_1: Existencia de Cámaras de Seguridad (Descripción: se detectan dos cámaras de seguridad en el frente de la casa)

FIE_ ADomicilio1_2: Existencia de Puertas y Ventanas (Descripción: se detectan 5 ventanas y 2 puertas (un portón incluido).

FIE_3_ADomicilio1_3: Tipo de Puertas y Ventanas (Descripción: se detectan puertas/portón de madera. Además, se distinguen materiales de puertas y ventanas, tipo de portón, la inexistencia de rejas y/o celosías, entre otra cosas).



[26] Fuente foto: Hermosos Casa Y Jardín Foto de stock y más banco de imágenes de Coche - Coche, Camino de entrada, Casa - iStock (istockphoto.com)

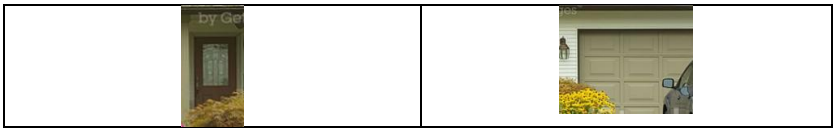


Figura 23. Ejemplo de Factores de incremento de exposición en la publicación.

Por otro lado, para el atributo expuesto *AVehiculo1* (de tipo *AtributoVehiculo*) se identifican los factores de incremento de exposición: *FIE_ AVehiculo1_1*: Marca, color y modelo, y *FIE_ AVehiculo1_2*: Patente / Dominio (Fig. 4).

Figura 24. Ejemplo de Factores de incremento de exposición en la publicación.

A continuación, se aplican las métricas definidas para el caso de estudio:

- **Métrica para calcular el valor de exposición de atributo "ADomicilio1:AtributoDomicilio" en la publicación *FotoDeMuro1.***

*VE_AtributoDomicilio_FotoMuro1 = ADomicilio1:AtributoDomicilio ** Sumatoria(*FIE_i_ AtributoDomicilio_FotoMuro1*)*/Cantidad total de FIE para tipo de atributo de AtributoDomicilio* = 1 * 3 / 8 **= 0,375**

- **Métrica para calcular el valor de exposición de atributo "AVehiculo1:AtributoVehiculo" en la publicación *Foto de muro 1.***

*VE_AtributoVehiculo_FotoMuro1 = AVehiculo:AtributoVehiculo ** Sumatoria(*FIE_i_AtributoVehiculo_FotoMuro1*) / *Cantidad total de FIE para el tipo de atributo AtributoVehiculo* = FotoMuro1 = 1 * 2 / 7 **= 0,285**

- **Métrica para calcular el valor de exposición en la publicación *FotoMuro1***

Para el cálculo se considera que *FME_FotoMuro* es 1, es decir, que la foto se publicó de manera pública, sin restricción de acceso. Se emplean, además, los resultados de las métricas calculadas previamente.

*VE_FotoMuro1 = FME_FotoMuro1 * (VE_AtributoDomicilio1_FotoMuro1 + VE_AtributoVehiculo_FotoMuro1) / Cant. total TipoAtributo*

*= 1 * (* 0,375 + 0,285*) / 7* = 0,66 / 7= **0,09**

Luego de presentar este primer caso, a continuación, se comparten dos escenarios similares bajo el mismo concepto: análisis de publicaciones de fotos dentro de un determinado perfil de una red social digital.

Caso de Estudio 2#: Datos de Trabajo

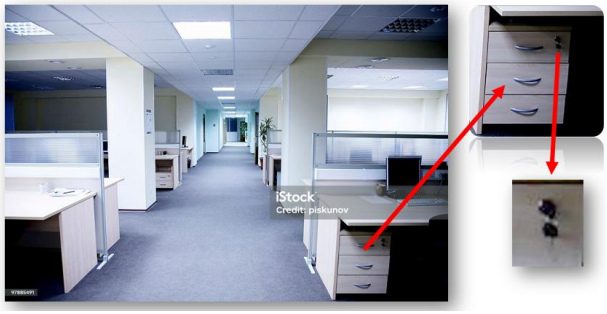


Figura 25. Imagen ejemplo Caso de estudio 2 – Datos de Trabajo. Facto de Incremento de Exposición #1 y #2.

- Factor de Incremento de Exposición #1
  - *Espacios físicos de la empresa y/o usuarios*

- Factor de Incremento de Exposición #2:
  - *Disposición de las oficinas, escritorios.*

Figura 26. Imagen ejemplo Caso de estudio 2 – Datos de Trabajo. Facto de Incremento de Exposición #3.

- Factor de Incremento de Exposición #3:
  - *Documentación en escritorios, impresoras, mesas reuniones, paneles.*

- **Valor de exposición de atributo: "ATrabajo1:AtributoTrabajo" en Foto Práctica #1.**

*VE_AtributoTrabajo_FotoPractica1 = ATrabajo1:AtributoTrabajo * Sumatoria(FIE_i_ AtributoTrabajo_FotoPractica1)/Cantidad total de FIE para tipo de atributo de **Trabajo.***

*VE_AtributoTrabajo_FotoPractica1 = 1 * (3 / 20) = 0,15*

Caso de Estudio #3: Datos de Familia

Figura 27. Imagen ejemplo Caso de estudio 3 – Datos de Familia. Facto de Incremento de Exposición #1, #2, 3# y 4#.

- Factor de Incremento de Exposición #1:
  - Cantidad de integrantes y posible parentesco.

- Factor de Incremento de Exposición #2:
  - Identificación menores.

- Factor de Incremento de Exposición #3:
  - Locaciones relacionadas.

- Factor de Incremento de Exposición #4:
  - Vehículos familia.

- **Valor de exposición de atributo: “AFamilia1:AtributoFamilia” en Foto Práctica #2.**

VE_AtributoFamilia_FotoPractica2 = AFamilia1: AtributoFamilia * Sumatoria(FIE_i_ AtributoFamilia_FotoPractica2)/Cantidad total de FIE para tipo de atributo de Familia.

VE_AtributoFamilia_FotoPractica2 = 1 * (4 / 6) = 0,66

El modelo conceptual propuesto, junto con las métricas definidas, establece un marco integral para medir y evaluar el nivel de exposición de información personal en redes sociales digitales. Las métricas definidas permiten cuantificar la exposición de atributos específicos, publicaciones individuales y, en última instancia, del perfil en su totalidad, otorgando un enfoque basado en datos para la gestión de la privacidad. A través de la implementación de factores de mitigación y una interpretación de los atributos de exposición, el modelo ofrece una herramienta de análisis y un recurso educativo que impulsa a los usuarios a adoptar prácticas más seguras y conscientes. Estas métricas también pueden ser implementadas en una herramienta informática integrada en navegadores web, asistiendo a los usuarios en conocer su nivel de exposición antes de realizar una publicación o en publicaciones posteriores, proporcionando una capa adicional de protección. En los casos de estudio analizados, los conceptos y métricas ayudan para identificar y gestionar la exposición de atributos sensibles, proporcionando una base para futuros desarrollos en la protección de la privacidad en entornos de redes sociales digitales.

Capítulo 7: Medidas de mitigación y buenas prácticas para reducir ataques a la exposición y privacidad de los usuarios.

Se inicia el capítulo con la siguiente pregunta dirigida a cualquier persona: "¿Usted colocaría en las paredes de afuera de su casa, un conjunto de fotos de sus vacaciones, sus salidas, y textos contando lo que va a hacer con su familia?" Cada individuo que pase por enfrente de su vivienda conocerá un poco de su vida privada. Algunos que pasen tal vez sean sus amigos o familiares; otros, perfectos desconocidos, y algunos de ellos, potenciales atacantes dispuestos a hacer de "su exposición" el motor de su obra maliciosa.

La exposición de la vida de una persona en una red social, es decir, en un perfil digital sobre una plataforma que así lo permita, conlleva una gran responsabilidad. La misma radica en que los usuarios son los principales custodios de su información personal, siendo los dueños de ésta y los principales interesados en proteger ese bien tan preciado que es la privacidad.

Se puede denominar, entonces, "mundo online" a aquel en donde los individuos se comunican por medio de las redes sociales digitales, siendo Internet el principal motor y medio para que sea desarrollado. Por otro lado, el "mundo offline", al mundo físico o terrenal, en donde los individuos mantienen relaciones sociales interpersonales, sin un medio electrónico de por medio.

El objetivo de este capítulo es la elaboración del catálogo de medidas de mitigación y protección en base a los distintos tipos de ataques y las técnicas de OSINT analizadas en el Capítulo 4: Aprovechamiento de la exposición de usuarios: Principales ataques.

Como una regla de oro en relación con las Redes Sociales Digitales, cuando un usuario decida crear un perfil y publicar información, en primer lugar, debe saber que ya está ingresando a una plataforma de acceso público. Esto significa que su perfil estará en Internet y la superficie de exposición y posterior ataque será más alta en dicho ambiente. Por lo anterior mencionado, la clave está en cómo minimizar la exposición y tomar las medidas adecuadas para que la información compartida en las Redes Sociales Digitales esté protegida y se tenga control sobre la privacidad.

Como primera medida de mitigación, se debe proteger el dispositivo sobre el que se accede al perfil de la red social y el inicio de sesión concreto a la plataforma. Vale considerar que la Seguridad Informática actúa por capas, colocando medidas de seguridad en diferentes niveles, para proteger desde diferentes posiciones, de tal manera que, si un atacante logra superar una barrera, todavía existen otras que debe superar.

En base a lo anterior, el concepto de capas de seguridad aplicará a la protección del acceso a la Red Social para el usuario. Las siguientes capas de seguridad deben ser consideradas:

1. Seguridad a nivel de dispositivo:

A. Contar con el sistema operativo vigente, con soporte y actualizado. Constatar que las últimas actualizaciones hayan sido aplicadas.

B. Aplicaciones de uso actualizadas y con sus versiones actualmente soportadas por el fabricante.

C. Inicio de sesión al Sistema Operativo con credenciales. Esto puede incluir usuario / contraseña, PIN, acceso biométrico y patrón.

D. Bloqueo de sesión cuando el equipo queda desatendido. Al alejarse de la computadora, notebook o al dejar el celular, hay que asegurar de que se bloquea el dispositivo.

E. Evitar escribir las contraseñas de acceso al dispositivo y/o plataformas en papeles o lugares visibles como ayudas memoria.

2. Seguridad de la Plataforma de Red Social:

A. Habilitar el Múltiple Factor de Autenticación (MFA) para el inicio de sesión. Este mecanismo agrega factores adicionales a la contraseña para confirmar la identidad de los usuarios.

B. Definir distintas contraseñas para cada Red Social. Es importante no repetir las contraseñas y no emplear patrones repetidos como, por ejemplo, mes del año, número de día, año, etc.

C. Considerar el uso de una plataforma de Gestión de Contraseñas. Estos programas permiten armar una biblioteca de todas las contraseñas de los sistemas con los que se opera. Sólo se debe usar una contraseña maestra junto con MFA para acceder a este servicio. Luego, dentro se podrá consultar por las contraseñas según cada sistema. Además, ofrecen herramientas para generar contraseñas robustas.

D. Evitar almacenar las contraseñas de inicio de sesión en el navegador web del dispositivo. Con cada intento de acceso se deberían de aplicar las credenciales.

E. Cerrar la sesión de la Red Social cuando se deja de usar la misma en el dispositivo.

3. Seguridad a nivel de “uso” de las Plataformas de Redes Sociales

Por otro lado, para mitigar la exposición de un perfil, se deben aplicar una serie de prácticas que ayudan a la “limpieza” de la exposición de un perfil en una red social digital. Con estas prácticas, lo que se busca es controlar los factores de exposición que posee el perfil. Este concepto se denomina también “sanitización” y hace referencia a articular las medidas y cambios necesarios para lograr un nivel de exposición adecuado.

Es importante mencionar que la exposición no se puede eliminar completamente y que, una vez que se publica información, ya no se tiene control de su ciclo de vida. En el caso de buscar la "máxima sanitización" posible, entonces se debería eliminar el Perfil completo de la Red Social.

Es importante mencionar que la exposición no se puede eliminar completamente y que, una vez que se publica información, ya no se tiene control de su ciclo de vida. En el caso de buscar la "máxima sanitización" posible, entonces se debería eliminar el Perfil completo de la Red Social.

Por lo tanto, considerando un perfil biográfico digital, se deben tener en cuenta las siguientes prácticas de sanitización:

1. Repasar cada una de las secciones de la definición del perfil en la red social digital. Un punto importante es el estado del perfil en Facebook. Con el incremento en el uso de Instagram, se evidencia que los usuarios tienden a "dejar de usar" o "abandonar" el uso de la red creada por Mark Zuckerberg. Eso genera que los perfiles vinculados en esta red social queden en un estado no actualizado y, tal vez, con información proporcionada que deba revisarse.

- **1.1.** Factor importante: Dada la conexión entre Facebook e Instagram, revisar la opción que permite que las publicaciones entre una red y otra sea compartidas. Es decir, cuando se publica en una red, automáticamente sale en la otra.
- **1.2.** Los "contactos" / "amigos" que están en Facebook, no necesariamente son los mismos que están en Instagram. Por eso, cobra importancia hacer una revisión completa de cada uno de los contactos que están en la red social y tomar acciones pertinentes.

2. De la revisión de cada perfil de las redes sociales, poner el foco en identificar los atributos de exposición del perfil y desde ese punto identificar los Factores de Incremento de estos.

3. Como resultado del punto anterior, proceder a eliminar información con exposición detectada.

- **3.1.** Factor importante: aprovechar la situación de detección de exposición no adecuada para generar un proceso de concientización sobre el tema a los usuarios. Es decir, a los propios contactos de la red social. Reemplazar aquellas publicaciones que tenían esa exposición mitigada por mensajes de buenas prácticas y/o recomendaciones sobre cómo prevenir una exposición proclive a ataques.

4. Derivado del punto 3, es importante revisar la configuración de las publicaciones para determinar el alcance permitido. Confirmar entonces que las personas que se deseen tengan acceso a las publicaciones del perfil biográfico digital, siendo conscientes en todo momento quienes tienen accesos y a quienes se restringe.

- **4.1.** Factor clave: revisar si los perfiles de las Redes Sociales Facebook e Instagram están debidamente restringidos para que no cualquier persona que los encuentra pueda ver el contenido completo. En

el caso de Instagram, revisar que se requiera de manera obligatoria la solicitud de "seguimiento" para acceder al contenido del perfil. Lo mismo para Facebook, que se requiera ser "amigo" para ver el detalle completo del perfil.

4.2. Revisar y prestar debida atención a las solicitudes de "seguidores", "amigos", "contactos" recibidos en las Redes Sociales digitales de análisis. Antes de aceptar, tomar el tiempo necesario para reconocer y confirmar si la persona, entidad o empresa que nos contacta es verídica. Para ellos, buscar referencias en Internet o consultar a otras personas que puedan estar vinculadas.

5. Realizar una búsqueda del nombre del usuario en cada una de las redes sociales, en su propio buscador. Considerando sus motores de búsqueda, se mostrarán los resultados en donde haya alguna mención sobre el usuario. Esto evidenciará, por ejemplo, aquellas fotos en que la persona fue "mencionada" / "etiquetada" / "arrobada".

5.1. Factor importante: en este punto, aparecen los Expuestos Pasivos. El mismo usuario puede ser un Expuesto Pasivo, así como también, se puede descubrir que otras personas también están siendo expuestas, tal vez, sin consentimiento.

6. Efectuar una búsqueda del usuario en los buscadores, como Google, Bing, etc.

6.1. En una primera instancia, los buscadores pueden tener indexadas las fotos de los perfiles de cada red social.

6.2. De los resultados obtenidos, es importante detectar qué tipo de información está expuesta, es decir, qué detalles se muestran en el buscador de cada perfil. En la lista de resultados, hay una pequeña reseña del contenido. Eso permite ver información del usuario sin necesidad de ingresar concretamente a la plataforma de la red social.

6.3. Cuando se detecta que hay información que evidencia una exposición, buscar el origen de esta:

6.3.1. Si es de una Red Social reconocida, si se tiene perfil activo: intentar acceder para sanitizar (reducir / atenuar exposición).

6.3.2. Se uno no es usuario de esa Red Social: identificar si uno no es un expuesto pasivo de esa red.

6.3.2.1. Identificar el dueño de ese Perfil, quién originó la exposición.

6.3.2.2. Factor importante: denunciar al Perfil si no se puede determinar el origen verídico de la exposición.

6.3.2.3. Cambiar la contraseña de las redes sociales.

7. Considerando los puntos 4 y 5, con el uso de las búsquedas, luego de los resultados, proceder a aplicar lo mencionado en los puntos 2 y 3.

A continuación, se resumen las medidas de “sanitización” para un perfil biográfico digital:

Medida de Sanitización	Descripción	Acción
S1: Revisión de contactos en redes sociales	Los contactos de Facebook y Instagram pueden no coincidir; es necesario revisar individualmente cada contacto de cada red social.	Revisar cada contacto y tomar las acciones adecuadas según el nivel de confianza y seguridad.
S2: Identificación de atributos de exposición	Evaluar los perfiles de cada red social para identificar los atributos del perfil que están expuestos. Detectar los Factores de Incremento de la exposición.	Realizar un análisis de los atributos expuestos y clasificar el nivel de exposición.
S3: Eliminación de información expuesta y concientización	Suprimir información que se detecte con alto riesgo de exposición. Utilizar esta oportunidad para educar a los contactos sobre seguridad.	Reemplazar publicaciones expuestas por mensajes de buenas prácticas de seguridad.
S3: Búsqueda de menciones externas	Usar el buscador de cada red social para detectar menciones o etiquetas del usuario en publicaciones de terceros, identificando a los Sujetos Expuestos Pasivos.	Verificar y gestionar etiquetas no deseadas y considerar comunicar la exposición a los Sujetos Expuestos Pasivos.

Tabla 4. Resumen las medidas de “sanitización” para un perfil biográfico digital.

Capítulo 8: Requerimientos y arquitectura de una herramienta informática para protección de la exposición

El objetivo de esta herramienta es proporcionar una capa adicional de seguridad y privacidad para los usuarios de Redes Sociales Digitales al ayudarles a tomar decisiones informadas sobre sus potenciales publicaciones. Permitirles conocer y controlar el nivel de exposición de su privacidad antes de publicar puede ayudar a prevenir situaciones no deseadas o inseguras.

La herramienta se propone a nivel de prototipo como una extensión o complemento a agregar a los navegadores de internet. Al momento de que el usuario ingrese a la RSD (Facebook, Instagram o LinkedIn) y decida efectuar una publicación, la herramienta propuesta podrá ser usada antes para analizar y conocer el nivel de exposición que dicho elemento tiene para con su privacidad y la de su entorno. En una primera versión de la herramienta, la aplicación será sólo para el análisis de tipos de publicaciones “fotos”.

Una versión avanzada de tal aplicación ofrece la posibilidad de cargar una determinada foto a la herramienta y por medio de una tecnología de reconocimiento de imágenes basada en Inteligencia Artificial, detectar y categorizar a la publicación según el atributo expuesto correspondiente. A sí mismo, la herramienta puede presentar al usuario una lista de posibles factores de incremento de la exposición o checklist, a fin de que éste realice una verificación, y obtenga el nivel estimado de exposición de la potencial publicación. A partir del valor o nivel de exposición obtenido, el usuario decide si desea proseguir o no con la publicación.

La herramienta está basada en el modelo conceptual planteado en esta tesis en el Capítulo 5 e implementa las métricas definidas en el Capítulo 6 para evaluar la exposición de una publicación en una Red Social Digital.

1. Arquitectura de la Herramienta

A continuación, se propone la arquitectura inicial de la herramienta propuesta.

Figura 28. Diagrama de la arquitectura inicial de la herramienta propuesta.

1. Interfaz de Usuario: Es el punto de interacción del usuario con la herramienta. Se piensa como una extensión del navegador web, permitiendo al usuario interactuar con la herramienta antes de realizar una publicación en redes sociales.
2. Extensión del Navegador: Se integra con los navegadores web para capturar el contenido que el usuario desea publicar en redes sociales y ser el nexo con el Backend para su análisis antes de la publicación.
3. Backend: Es el servidor que procesa las solicitudes del Frontend. Se necesita definir el servidor de la aplicación para el manejo de la lógica de negocio y la comunicación con los servicios externos. Así mismo, se necesita de una Base de Datos para almacenar la información relevante para la herramienta, como configuraciones del usuario y datos analíticos / historial / logs / métricas.

4. Integración de API Externa: Es necesaria porque se conecta con las API de Facebook, Instagram o LinkedIn para obtener información de las publicaciones y realizar el análisis de exposición.
5. Servicios de Procesamiento de Imágenes IA: En este caso se relaciona con el servicio específico de Inteligencia Artificial para analizar las imágenes y detectar factores que puedan incrementar la exposición de la publicación.
6. Base de Datos: el objetivo es almacenar los datos relacionados con el uso de la herramienta. Incluye el almacenamiento de los resultados de análisis para referencias futuras, configuraciones personalizadas de los usuarios y sus preferencias de privacidad. Facilita el aprendizaje continuo del sistema, mejorando los modelos de IA con datos históricos.
7. Sistema de Notificaciones: Permite al usuario recibir alertas y recomendaciones sobre su privacidad. El objetivo es notificar a los usuarios sobre los niveles de exposición de sus publicaciones y enviar recordatorios para revisar y ajustar las configuraciones de privacidad.
8. Seguridad: Factor sumamente importante de la Arquitectura. Se requiere una gestión de Tokens de Acceso para la autenticación y autorización en las API de redes sociales. Además, se necesita cifrado de datos para proteger la información sensible almacenada en la base de datos.

2. Flujo de trabajo de la Herramienta

Considerando el objetivo de la herramienta, se presenta el flujo resumido de trabajo siguiendo la arquitectura planteada:

I. El usuario inicia la extensión del navegador web antes de realizar una publicación en la red social digital Facebook, Instagram o LinkedIn.
II. La extensión solicita la información de la publicación al servidor de aplicaciones.
III. El servidor de aplicaciones obtiene la imagen y otros datos relevantes de la publicación a través de la API de la red social.
IV. La imagen se envía al servicio de con tecnología de reconocimiento de imágenes IA para su análisis.
V. El servicio de procesamiento y reconocimiento de imágenes IA devuelve los resultados al servidor de aplicaciones.
VI. El servidor de aplicaciones presenta los resultados al usuario a través de la interfaz de usuario de la extensión, permitiéndole tomar una decisión informada sobre la publicación. Esto incluye el resultado de las métricas de exposición, así como el listado de factores de incremento de exposición detectados.

3. Requerimientos Funcionales para la Herramienta

A continuación, se presentan los Requerimientos Funcionales para desarrollar la herramienta:

1. Relacionados con la Interfaz de Usuario:
    a. Integración con Navegadores: Se integra como una extensión en los navegadores web para analizar publicaciones en redes sociales digitales antes de ser expuestas.
    b. Complemento: Integración con plataformas de Redes Sociales Digitales. La extensión podría integrarse con las API de las redes sociales seleccionadas (Facebook, Instagram, LinkedIn) para poder acceder a las publicaciones y mostrar la interfaz de la extensión en el momento adecuado.
    c. El usuario, al hacer click en la extensión, se abre una ventana o panel lateral con la interfaz de la herramienta, que muestra opciones para cargar una foto que será la deseada para ser publicada en el perfil de la red social digital.
2. Relacionados con el Análisis de Publicaciones:
    a. Tipo de Publicación: La herramienta identifica el tipo de publicación que el usuario está a punto de realizar, centrándose en publicaciones que contienen fotos. En futuras versiones se podría incluir la capacidad de análisis de textos (comentarios, descripciones de fotos), videos y otro tipo de publicación.
    b. Análisis de Fotos: En esta funcionalidad, se piensan dos escenarios de implementación:
        1. Escenario Básico: Presentar al usuario la publicación seleccionada, inicialmente una foto, para que de manera “visual”, sin asistencia tecnológica, la persona analice el contenido de esta en base a los factores de incremento de exposición.
        2. Escenario Avanzado: Utilizar tecnología de reconocimiento de imágenes basada en Inteligencia Artificial para analizar las fotos y detectar posibles atributos expuestos.
3. Relacionados con la detección de Atributos Expuestos:
    a. Reconocimiento de Imágenes: Identifica elementos en las fotos que podrían exponer información sensible, como rostros, lugares, objetos, etc. En este punto se basa en los Factores de Incremento de Exposición presentados en el Capítulo 5.
    b. Este punto aplica para los dos escenarios antes mencionados. La diferencia radica en que, con el escenario Básico, el usuario es quien tiene que manualmente revisar visualmente la publicación (foto) para detectar los atributos expuestos.
4. Relacionados con el cálculo de Nivel de Exposición:

   a. Factores de Incremento de Exposición: Considera los Factores de Incremento de Exposición del modelo presentado en esta tesis como punto de entrada para el cálculo de las métricas.
   b. Estimación de Exposición: Aplica las métricas presentadas en el Capítulo 6, obteniendo el nivel de exposición para la publicación en base a los atributos detectados y los factores de incremento.
5. Relacionados con la alerta al Usuario y acciones Sugeridas:
   a. Alerta de Concientización: Alerta al usuario sobre el nivel de exposición estimado y los posibles riesgos.
   b. Acciones Sugeridas: Proporciona recomendaciones sobre cómo ajustar la configuración de privacidad o editar la publicación para reducir la exposición ocultando información sensible relacionada a los Factores de Incremento de Exposición.
6. Relacionados con el registro de Análisis y Decisiones del Usuario:
   a. Historial de Análisis: Registra los análisis realizados por el usuario para futuras referencias.
   b. Decisiones del Usuario: Registra las acciones tomadas por el usuario en respuesta a los análisis, como modificar la publicación o cancelarla. En este apartado, le podría decir al usuario cuál fue la acción tomada previamente para una foto similar en el nivel de exposición.

4. Requerimientos de Calidad para la Herramienta

A modo de complemento, se presentan los siguientes Requerimientos de Calidad para la herramienta: para desarrollar la herramienta:

1. Relacionados con la Interfaz de Usuario:
   a. Componentes Visuales: La interfaz debe ser intuitiva y fácil de usar, ayudando a los usuarios a emplearla de una manera sencilla.
2. Relacionados con la Privacidad y Seguridad:
   a. La herramienta debe diseñarse para garantizar la privacidad y seguridad de los datos del usuario durante el análisis de las publicaciones, asegurando que no se comparta información sensible con terceros sin consentimiento.
   b. Considerar el seguimiento de las regulaciones globales de protección de datos y privacidad pertinentes como GDPR, así como las normas de seguridad de la información como ISO-27001.

Luego del detalle de requisitos funcionales y de calidad, se desarrolla en un Modelo de Datos preliminar. Este tipo de modelo consiste en una representación abstracta y organizada de los datos que la

herramienta necesita almacenar y administrar, así como de las relaciones entre los mismos. Además, describe los atributos que cada uno de los datos debe mantener para garantizar el funcionamiento de la herramienta.

5. Modelo de Datos de la Herramienta

Inicialmente se presentan los siguientes componentes para el **Modelo de Datos**:

1. Usuario:
    a. ID: Identificador único del usuario. Es propio de esta herramienta.
    b. Nombre: Nombre del usuario en la Plataforma de la Red Social Digital. Va a depender de la forma en que el usuario se registró en cada plataforma. Por eso, no será la "razón social" sino el valor que se definió como nombre para el perfil
    c. Email: Correo electrónico del usuario. El mismo usado en la Red Social Digital.
2. Publicación:
    a. ID: Identificador único de la publicación.
    b. Usuario ID: ID del usuario que realiza la publicación.
    c. Red Social Digital: Nombre de la red social en la que se realiza la publicación.
    d. Fecha y Hora: Fecha y hora de la publicación.
    e. Contenido: Texto de la publicación. En el caso de que haya agregado algún comentario o dato adicional como título.
    f. URL de la Foto: URL de la foto adjunta a la publicación.
3. Análisis de Foto:
    a. ID: Identificador único del análisis.
    b. Publicación ID: ID de la publicación a la que pertenece el análisis.
    c. Atributos Detectados: Lista de atributos detectados en la foto (rostros, objetos, texto, etc.). Con el escenario Avanzado de la herramienta, se aplica la Inteligencia Artificial por intermedio del reconocimiento de imágenes. Para el escenario Básico, es el usuario quien visualmente identifica lo atributos que será presentados en la herramienta.
    d. Factores de Incremento de Exposición: Lista de factores que pueden incrementar la exposición de la foto.
    e. Nivel de Exposición según Métricas: Nivel calculado de exposición de la foto según Métricas.
4. Acciones del Usuario:
    a. ID: Identificador único de la acción.

b. Usuario ID: ID del usuario que realiza la acción.
c. Tipo de Acción: Tipo de acción realizada por el usuario (editar publicación, cambiar configuración de privacidad, etc.).
d. Fecha y Hora: Fecha y hora de la acción.
e. Detalle: Detalle adicional sobre la acción realizada.

Tabla Usuario

Nombre Campo	Tipo Dato	Descripción
ID	INT	Identificador único del usuario (PK).
Nombre	VARCHAR	Nombre del usuario en la red social.
Email	VARCHAR	Correo electrónico del usuario.

Tabla Publicación

Nombre Campo	Tipo Dato	Descripción
ID	INT	Identificador único de la publicación (PK).
Usuario_ID	INT	ID del usuario que realiza la publicación (FK).
Red_Social_Digital	VARCHAR	Nombre de la red social.
Fecha_Hora	DATETIME	Fecha y hora de la publicación.
Contenido	TEXT	Texto de la publicación.
URL_Foto	VARCHAR	URL de la foto adjunta a la publicación.

Tabla Análisis_Foto

Nombre Campo	Tipo Dato	Descripción
ID	INT	Identificador único del análisis (PK).
Publicación_ID	INT	ID de la publicación analizada (FK).
Atributos_Detectados	TEXT	Lista de atributos detectados en la foto.
Factores_Incremento_Exposición	TEXT	Lista de factores de incremento de exposición.
Nivel_Exposición_Según_Métricas	INT	Nivel de exposición calculado según métricas.

Tabla Acciones_Usuario

Nombre Campo	Tipo Dato	Descripción
ID	INT	Identificador único de la acción (PK).
Usuario_ID	INT	ID del usuario que realiza la acción (FK).
Tipo_Acción	VARCHAR	Tipo de acción realizada por el usuario.
Fecha_Hora	DATETIME	Fecha y hora en que se realizó la acción.
Detalle	TEXT	Detalles adicionales sobre la acción realizada.

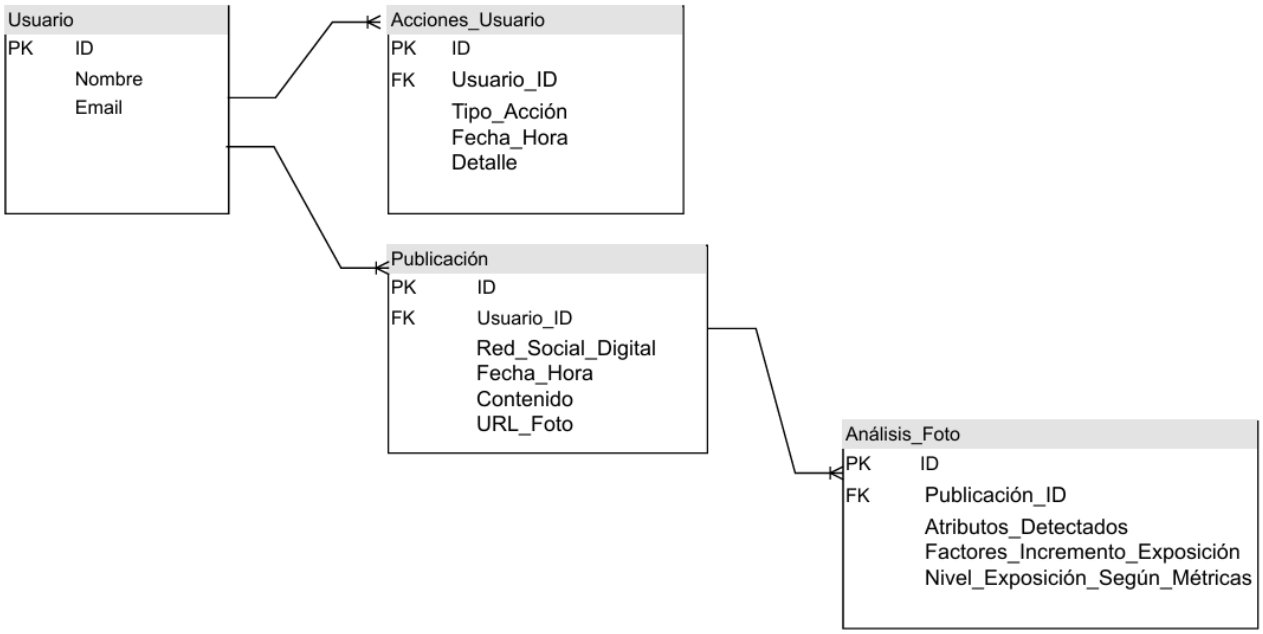


Figura 29. Modelo de Datos con sus relaciones.

6. Descripción de los escenarios posibles de implementación: Básico y Avanzado.

El desarrollo de la herramienta se puede abordar desde dos enfoques distintos: un escenario básico y un escenario avanzado. Los dos ofrecen distintas ventajas y desafíos.

Escenario Básico: Análisis Visual de Publicaciones

En este escenario, el usuario selecciona una foto para su publicación en redes sociales digitales, y la herramienta le proporciona una interfaz para que evalúe visualmente la exposición del contenido sin asistencia tecnológica avanzada por medio de Inteligencia Artificial. Es un pensado para la primera versión

de la herramienta. Este enfoque se basa en la participación activa del usuario, quien evalúa manualmente los factores de exposición presentados por la herramienta.

Proceso de funcionamiento del escenario Básico:

1) El usuario ingresa a una red social (Facebook, Instagram, LinkedIn).
2) Activación de la herramienta:
    a) Usuario activa la extensión en el navegador web que se usa para acceder a la RSD.
3) Selección de la Foto:
    a) Usuario selecciona la foto que desea publicar. Se puede copiar la ubicación (URL) de la misma o seleccionar la misma en la ubicación local que tiene el usuario.
    b) La herramienta presenta la foto seleccionada en una interfaz de análisis.
4) Presentación de Factores de Incremento de Exposición: La herramienta muestra una lista de factores de incremento de exposición que el usuario debe considerar.
5) Evaluación Visual:
    a) El usuario revisa visualmente la foto y marca los factores de exposición relevantes.
    b) La herramienta proporciona casillas de verificación para cada factor, permitiendo al usuario marcar aquellos que se aplican a la foto.
6) Resumen del análisis:
    a) Una vez que el usuario seleccionó los factores de incremento de exposición relevantes, la herramienta presenta un resumen del análisis, indicando los posibles riesgos de exposición.
    b) La herramienta calcula un "Nivel de Exposición" basado en los factores seleccionados y con base en las métricas definidas en este proyecto.
7) Decisión del Usuario:
    a) El usuario revisa el nivel de exposición y decide si desea proceder con la publicación, modificar la foto, o cancelarla.
    b) La herramienta puede ofrecer sugerencias sobre cómo reducir el nivel de exposición (por ejemplo, editar la foto para eliminar información sensible, tomarla desde otro ángulo, aplicar algún filtro para ocular zonas de exposición, etc.).

Como desafío para este escenario, se tiene el análisis subjetivo que tiene que efectuar el usuario. Es decir, la precisión del análisis depende de la capacidad del usuario para identificar correctamente los factores de exposición, lo que puede variar entre distintas personas.

Escenario Avanzado: Análisis de Publicaciones con Tecnología IA

En este escenario, se utiliza tecnología de reconocimiento de imágenes basada en Inteligencia Artificial (IA) para analizar las fotos y detectar automáticamente posibles factores de incremento de exposición. Cuando se describió la arquitectura inicial, se pensó en este escenario avanzado.

Proceso de funcionamiento del escenario Avanzado:

1) El usuario ingresa a una red social (Facebook, Instagram, LinkedIn).
2) Activación de la herramienta:
    a) Usuario activa la extensión en el navegador web que se usa para acceder a la RSD.
3) Selección de la Foto:
    a) Usuario selecciona la foto que desea publicar. Se puede copiar la ubicación o URL de la misma (si la foto ya se encuentra publicada) o seleccionar la misma en la ubicación local que tiene el usuario.
    b) La herramienta presenta la foto seleccionada en una interfaz de análisis.
4) Análisis Automático con Inteligencia Artificial (IA):
    a) La herramienta utiliza algoritmos de reconocimiento de imágenes para escanear la foto.
    b) Se detecta y categorizan atributos expuestos con los deferentes factores de incremento de exposición.
5) Presentación de resultados:
    a) La herramienta muestra los resultados del análisis, destacando visualmente los elementos detectados en la foto. Por ejemplo, mediante un recuadro, indica los factores de incremento de exposición presente, como podría ser, la existencia de cámaras de seguridad.
    b) En base a lo anterior, la herramienta enumera la lista de factores de exposición detectados automáticamente por la IA.
6) Resumen del análisis:
    a) La herramienta calcula un "Nivel de Exposición" basado en los factores de incremente detectados y presenta un resumen al usuario.
    b) Para finalizar, se proporciona una explicación detallada de cada factor detectado y su impacto potencial en la exposición de la privacidad.
7) Checklist y decisión final del Usuario:
    a) El usuario puede revisar y confirmar los factores de incremento de exposición detectados. En este punto, se recomienda que el usuario haga un análisis adicional, visual, para validar los resultados obtenidos por la aplicación de tecnología de IA.
    b) El usuario decide si desea proceder con la publicación, modificar la foto, o cancelarla.

8) Sugerencias de mitigación de la exposición y buenas prácticas:
    a) La herramienta ofrece sugerencias específicas para reducir el nivel de exposición, como:
        i) Desenfocar o eliminar elementos sensibles, vinculados a los factores de incremento de exposición.
        ii) Ajustar configuraciones de privacidad en la red social. Por ejemplo, seleccionar los destinatarios posibles con acceso a esta publicación.
        iii) Utilizar herramientas de edición de fotos para ocultar información sensible, que favorece al incremento de exposición.

Como desafío para este escenario Avanzado se tiene la complejidad técnica relacionada al uso de tecnologías de Inteligencia Artificial. Esto conlleva cuestiones propias de la integración de dichos algoritmos con la herramienta, así como un adecuado manejo de los recursos que se insumen para un rendimiento acorde a las exigencias de los usuarios.

A modo de ejemplo para el caso de Facebook, es posible aplicar los algoritmos de Inteligencia Artificial de reconocimiento de imágenes directamente a las publicaciones del tipo “fotos” sin necesidad de descargarlas, utilizando la API que tiene esta plataforma. La misma proporciona “endpoints” que permiten acceder a la información de las imágenes y realizar operaciones como el reconocimiento de objetos, rostros o contenido visual similar. Los “endpoints” son las direcciones específicas a las que se pueden enviar solicitudes para interactuar con un servicio web o una aplicación. Cada endpoint puede representar una función o un recurso específico que la API proporciona. Para este caso de Facebook, hay endpoints para realizar diferentes acciones, como obtener información de perfil, subir una foto, publicar un comentario, etc.

Para lograr el objetivo antes mencionado, se nombran algunos de los requisitos:

1) Autenticación y Autorización: Necesidad de contar con un token de acceso válido para utilizar la API de Facebook. Es necesario un registro como desarrollador en la plataforma de desarrolladores de las redes sociales digital y obtener permisos adecuados.
2) Acceso a la Información de la Imagen: Utilizando la API de Facebook, se puede acceder a la información de las imágenes publicadas en la red social. Esto puede incluir el ID de la imagen, su dirección (UTL), metadatos y otra información relevante.
3) Envío de la Imagen a la Servicio de Procesamiento y Reconocimiento de Imágenes con IA: Luego de obtener la información de la imagen, se puede enviarla directamente al servicio de IA de reconocimiento de imágenes a través de la API de dicha tecnología. Esto puede implicar enviar la URL de la imagen o los datos de la imagen, dependiendo de cómo esté diseñada la API de la tecnología de IA.

4) Análisis de la Imagen: El servicio de reconocimiento de imágenes con IA, procede a analizar la imagen y devolver los resultados correspondientes, como la detección de objetos, reconocimiento de rostros, clasificación de contenido, etc. Esto constituye luego la base para la determinación de los factores de incremento de exposición y posterior cálculo de métricas.

A continuación, se hace una breve conclusión sobre los dos escenarios planteados para la herramienta. En el escenario básico, la simplicidad y rapidez de implementación permiten desplegar rápidamente la herramienta. Para el caso del escenario avanzado, el uso de tecnologías de Inteligencia Artificial lleva a la herramienta a otro nivel de precisión y eficiencia, automatizando la detección de factores de incremento de exposición y proporcionando un análisis detallado que ahorra tiempo a los usuarios. Es un enfoque más complejo de desarrollo, pero ofrece un valor añadido significativo al usuario.

El hecho de pensar la implementación con dos enfoques posibilita un desarrollo gradual de la herramienta. Desde el escenario básico se pueden sentar las bases para potenciar las funcionalidades con el uso de IA. Se puede aplicar un proceso de desarrollo ágil, iterativo, y de mejora continua, para garantizar que la herramienta permanezca relevante y alineada con las necesidades y expectativas de los usuarios. Al fin y al cabo, el desafío principal es colaborar con los usuarios, en la gestión de privacidad y exposición en las redes sociales. Esto será la base para la concientización de los usuarios sobre los riesgos de la exposición inadecuada de su privacidad y la promoción buenas prácticas y medidas de mitigación.

Un detalle importante y quizás el más relevante en la implementación de esta herramienta considerando los dos escenarios, es la participación del usuario, proporcionando un camino de educación sobre la privacidad de la exposición y sus consecuencias. Dado a que las personas tienen que usar la herramienta y seleccionar la foto que se desea publicar, fomenta una mayor conciencia y ayuda a que los usuarios se vuelven más críticos y cautelosos al evaluar sus publicaciones, lo que puede derivar en un comportamiento más seguro y responsable. Como se dijo en la introducción de este trabajo, un gran poder conlleva una gran responsabilidad: publicar, exponer, conlleva riesgos y son los usuarios los que deben ser responsables de ese poder que tienen para definir el comportamiento final.

Por eso, es importante destacar el valor que se busca en la educación y concientización, intentando se convierta esta herramienta, en un elemento multiplicador de buenas prácticas para los usuarios, enseñando cómo identificar y entender los diferentes factores de exposición y promoviendo buenas prácticas de seguridad y protección de la privacidad.

En base a la Modelo Conceptual y de Datos, se presentan los prototipos visuales de lo que contemplaría la herramienta en sus dos Escenarios:

Prototipo Escenario A:

Figura 30. Pantallas 1 y 2 de la herramienta informática para el Escenario A.

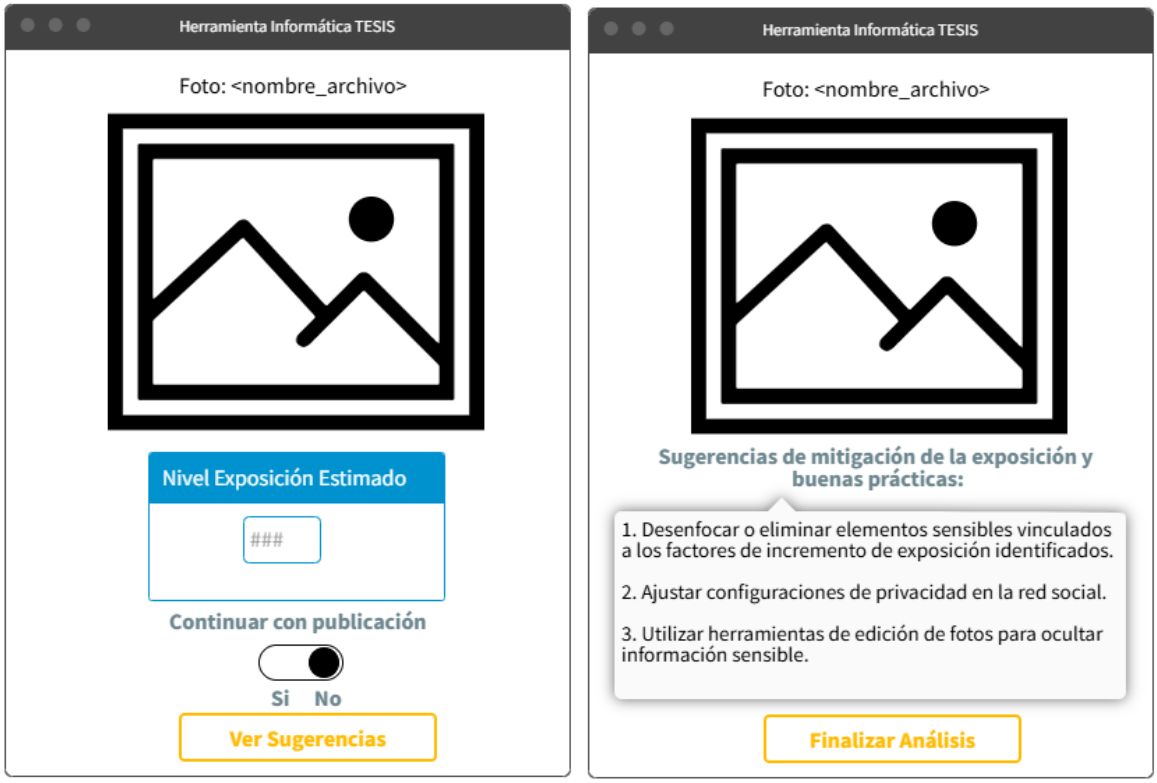


Figura 31. Pantallas 3 y 4 de la herramienta informática para el Escenario A.

Prototipo Escenario B:

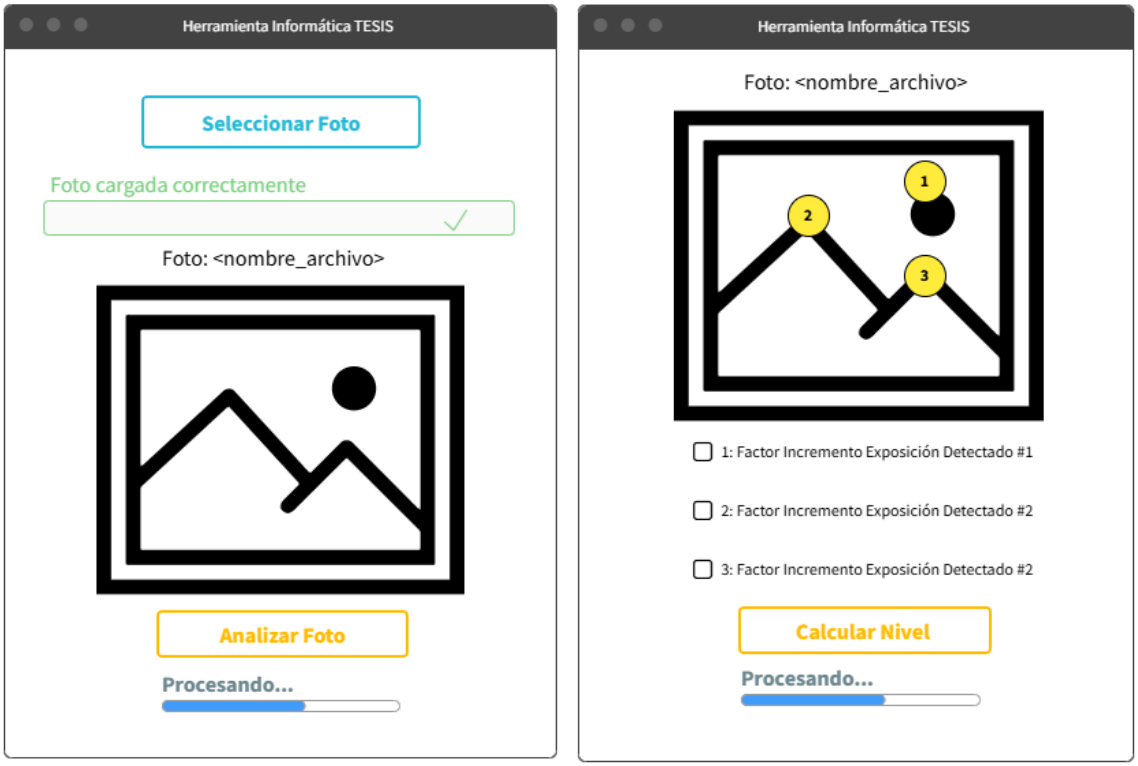


Figura 32. Pantallas 1 y 2 de la herramienta informática para el Escenario B.

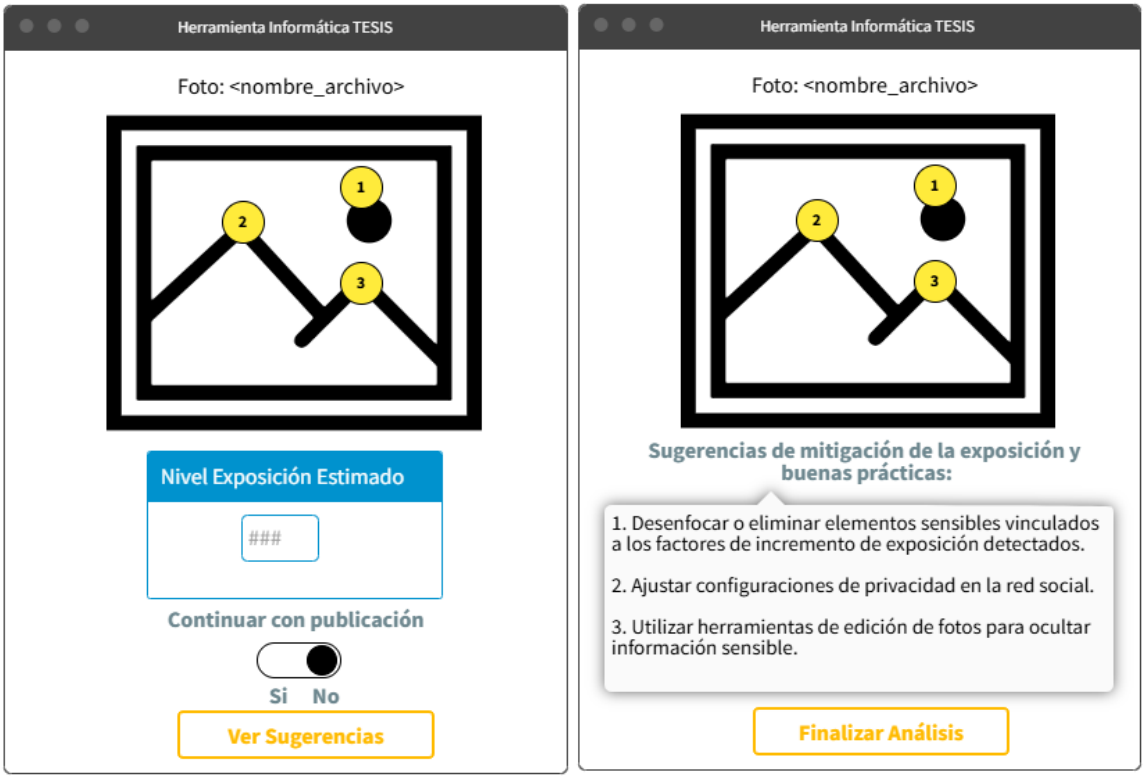


Figura 33. Pantallas 3 y 4 de la herramienta informática para el Escenario B.

7. Ejemplo de análisis de Publicaciones con Tecnología IA

Considerando el Escenario Avanzado relacionado al uso de Tecnología IA, se muestran a continuación 5 soluciones existentes y sus pruebas en el contexto de esta tesis. La herramienta informática presentada podrá hacer uso de las librerías propuestas por estas soluciones para su funcionamiento.

- Azure AI - Vision Studio (Microsoft)

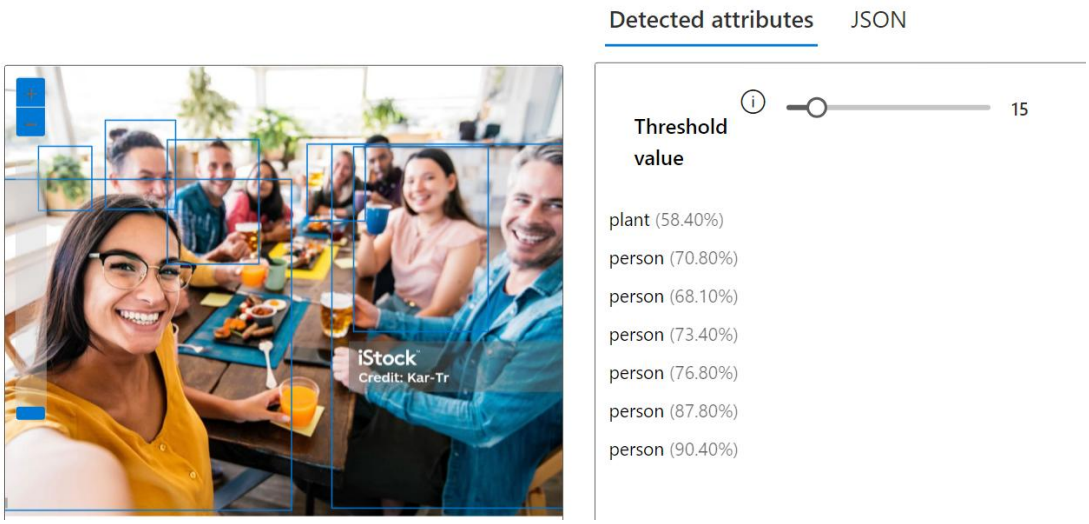


Figura 34. Prueba de librería Azure AI – Vision Studio.

- Google Cloud Vision API:

Figura 35. Prueba de librería Google Cloud Vision API.

- (Open-Source Computer Vision Library):

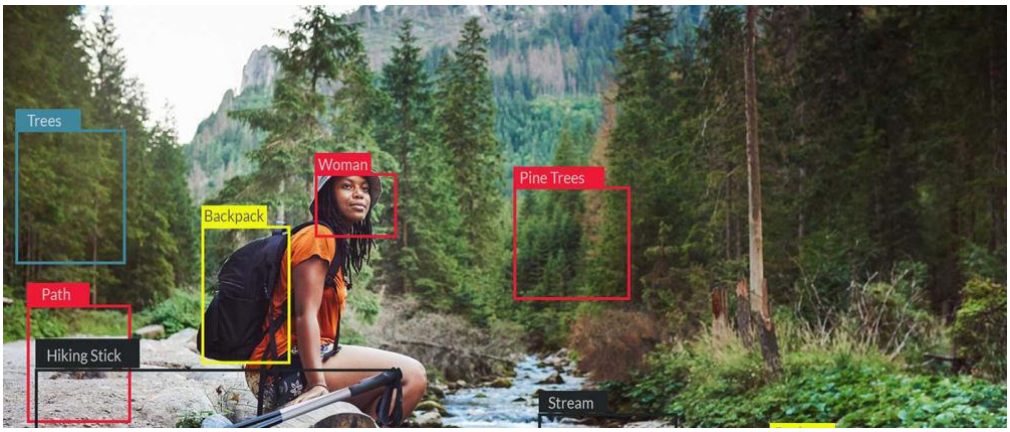


Figura 36. Prueba de librería OpenCV.

- Image Recognize:

Party
- Confidence: 100 %

Adult 2
- Confidence: 99 %

Male 3
- Confidence: 99 %

Man 4
- Confidence: 99 %

People
- Confidence: 100 %

Person 1
- Confidence: 100 %

Fun
- Confidence: 100 %

Figura 37. Prueba de librería Image Recognize.

- Astica Object Detection API:

Description New v2.0_full

A family standing in front of a house

asticaVision v2.0 full

- a family standing in front of a house (0.8305110335350037%)
- a girl wearing a dress

GPT-S Description
Preview

In this image, we see a family of four standing in front of their house. The house is a two-story building with white siding and a brown roof. It has large windows on the first floor and smaller ones on the second floor. The family is posing in front of the porch, which has white railings and steps leading up to it.

The parents are standing side by side with their young daughter wearing a dress between them. She looks adorable with her curly hair and big smile. Their toddler son stands in fron of them, wearing white overalls and looking curious as he gazes at the camera.

Figura 38. Prueba de librería Astica Object Detection API.

- Eden AI: tiene capacidad de integrar múltiples librerías en un solo entorno.

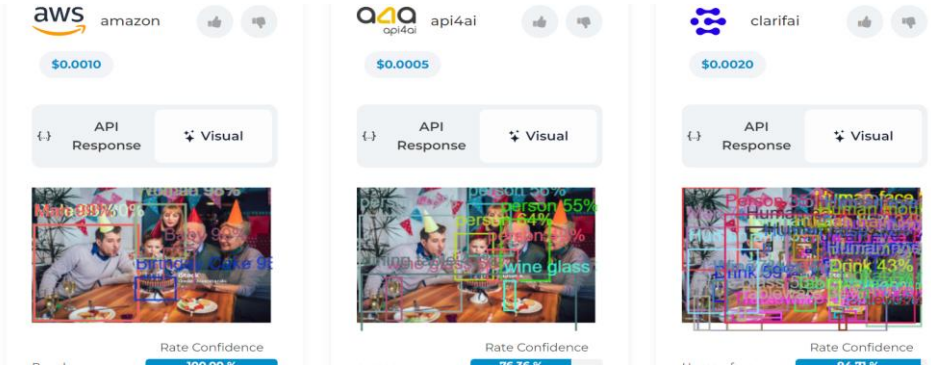


Figura 39. Prueba de librería Eden AI.

8. Elección de Librería OpenCV para su utilización mediante el desarrollo de un script.

Considerando que OpenCV es una librería de código abierto y que necesita ser instalada de manera local en la computadora para su utilización, se decidió avanzar en la prueba del prototipo de la herramienta utilizando dicha tecnología. Además, se empleó un modelo preentrenado de la red neuronal YOLOv4 para detectar diversos objetos dentro de una imagen.

Una ventaja importante de este enfoque es que todo el procesamiento se realiza localmente en la computadora del usuario. Esto significa que las fotos no se deben enviar a servidores externos a través de internet, garantizando que el análisis sea completamente privado. Dado el objetivo de la Tesis, este aspecto resulta relevante cuando se desean evaluar fotos que pueden contener información sensible y exponer a las personas y su entorno.

Para llevar a cabo la utilización de la librería se utilizó un script desarrollado en Python. Este script fue desarrollado y aplicado únicamente a modo de prueba para la detección de Factores de Incremento de Exposición relacionados al atributo "Familia". En el futuro, puede ser personalizado y adaptado para evaluar adecuadamente otras categorías como Trabajo, Amigos, Académico, Laboral, Mascotas y Vehículos.

Este script se generó usando como referencia ejemplos de código existentes disponibles en la documentación oficial de OpenCV y repositorios públicos en Internet. Los ejemplos brindaron la estructura básica para la carga de fotos, la preparación del modelo YOLOv4 y la visualización de resultados.

El script comienza cargando las clases de objetos que el modelo puede detectar, que son definidas en un archivo llamado coco.names.La foto a analizar se selecciona a través de un cuadro de diálogo proporcionado por la librería tkinter.

Luego de ello, se realiza un preprocesamiento de la foto para ajustarla al formato compatible con la red neuronal YOLOv4. Finalmente, las detecciones se agrupan y se presentan en un informe que detalla los

objetos detectados, resaltando especialmente aquellos que corresponden a posibles niños y categorizando otros elementos relevantes como personas adultas, vehículos (autos, bicis, motos), mascotas (perros/gatos), plantas, copas, tortas, puertas, ventanas, etc (Figura 41). Además, el script permite visualizar la imagen con los objetos detectados resaltados mediante recuadros de colores y genera una réplica de la foto con todas las marcas de las detecciones. Es importante destacar que las detecciones son filtradas con un umbral de confianza y un proceso que ayuda a que se evite encontrar objetos duplicados.

En relación a la detección de “niños” en las fotos, esta librería OpenCV no contiene de manera nativa los desarrollos para distinguir entre persona adulta y niños. Por es motivo, se aplicó un ejemplo basado en las posiciones absolutas de los objetos “personas” en las fotos. Para ello, se consideran “niños” a los objetos personas que se detectaron en cierta posición absoluta que otros objetos también “personas” pero que se encuentran posicionados más arriba en la foto.

A continuación, se muestran algunas capturas del uso del Script:

- En esta prueba el análisis se realiza a la categoría bajo el Atributo “Familia” (atributo Familia). Sin embargo, una herramienta futura completamente funcional, daría la posibilidad de indicar otra categoría. Aquí se escribe “Familia” (Figura 40).

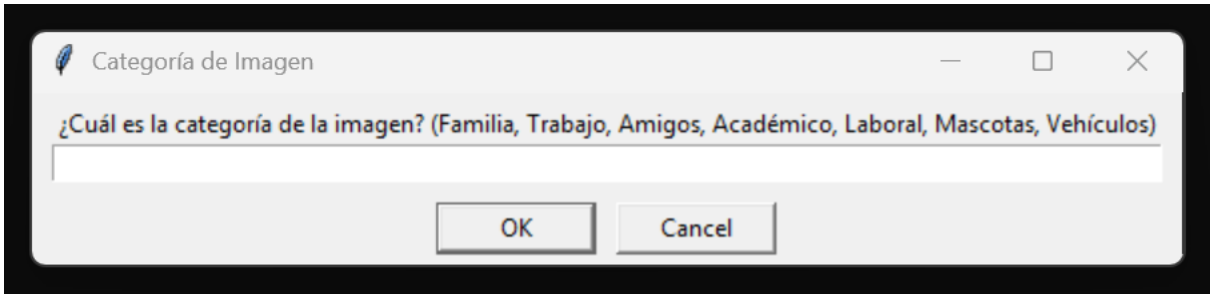


Figura 40. Script para OpenCV – Ventana para seleccionar la foto.

- Luego de seleccionar la foto desde la ubicación que el usuario indique, el Script aplica el análisis de la imagen y muestra en pantalla a la imagen con los recuadros identificando los “posibles” objetos (Figura 41):

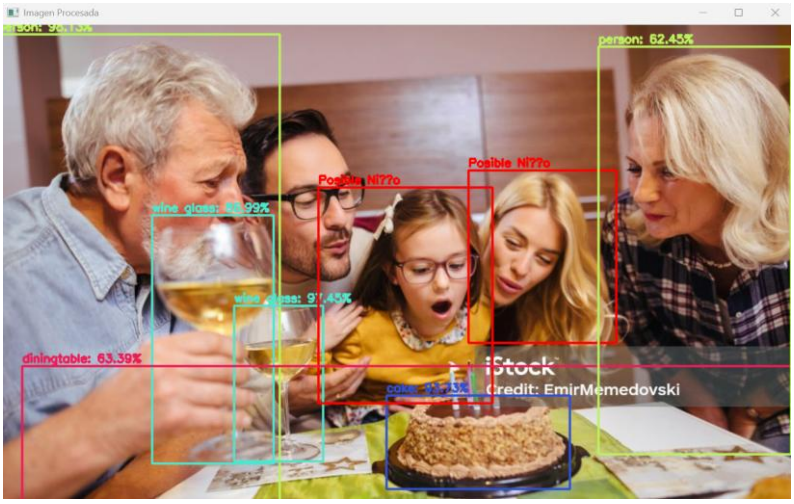


Figura 41. Script para OpenCV – Foto con los objetos identificados remarcados en la imagen.

- Luego de cerrar la ventana con la foto, el Script genera el reporte en un documento de texto (extensión .txt) y crea una foto duplicada conteniendo todos los recuadros con los objetos encontrados. En la captura (Figura 42) del reporte se puede evidenciar que se detecta más cantidad de objetos por categoría. De todos modos, eso tiene que ver con la precisión que maneja la librería. Además, se puede observar que se detectan 4 Factores de Incremento de Exposición y con los mismos se calcula el valor de Exposición del Atributo Familia.

```
Imagen analizada: C:/Users/Administrator/OneDrive/Documentos/Universidad/Tesis EMISI - UTN - RZenobi/
Categoría de la imagen: Familia
Tamaño de la imagen: 1024x682 píxeles

--- Objetos detectados por categoría ---
- wine glass: 7
- Persona: 15
- cake: 4
- diningtable: 2

--- Posibles niños detectados: 2 ---
--- Total de Factores de Incremento de Exposición detectados: 4 ---
--- Factores de Incremento de Exposición detectados: ---
- Cantidad de integrantes y posible parentesco
- Fechas y/o acontecimientos particulares
- Identificación de menores
- Locaciones relacionadas a la familia

--- Valor de Exposición del Atributo Familia (VE_AtributoFamilia): 0.57 ---

--- Lista completa de Factores de Incremento de Exposición Totales ---
- Cantidad de integrantes y posible parentesco
- Identificación de menores
- Fechas y/o acontecimientos particulares (cumpleaños, casamientos, etc.)
- Mascotas de familia
- Vehículos de familia
- Locaciones relacionadas a la familia
- Fechas y/o acontecimientos particulares
--- Fin del Informe ---
```

Figura 42. Script para OpenCV – Informe de Análisis de la foto seleccionada.

En conclusión, se puede mencionar que OpenCV cumple las expectativas iniciales para probar una librería que aplique Inteligencia Artificial para detectar objetos en fotos. Además, es personalizable y permite cambios accesibles para incrementan las funcionalidades y agregar el resto de los Atributos para el análisis.

Capítulo 9: Conclusiones.

Con el desarrollo de este trabajo de tesis, se evidencia la importancia de contar con usuarios responsables frente a los Perfiles Biográficos Digitales en el contexto de la exposición de datos personales en Redes Sociales Digitales. Se necesita trabajar en concientizar sobre el valor de la privacidad considerando que cada aspecto de una exposición puede ser útil para que se abra una filtración de información sensible no deseada. Por lo tanto, crear un perfil biográfico digital y publicar información, conlleva una gran responsabilidad. La misma no sólo recae en el autor del perfil y el cuidado de su privacidad, sino también, y quizás más importante, para cuidar la exposición de personas / contactos relacionados.

En el Capítulo 1 se definieron los conceptos centrales que se relacionan a esta problemática de la exposición, entre ellos el perfil digital como representación de la identidad de cada usuario y la influencia que tiene en su privacidad. Al analizar el crecimiento de las redes sociales y su papel en la vida cotidiana, se identificó que la exposición en estas plataformas genera un impacto directo sobre la privacidad, dada la visibilidad que se otorga a la información personal y el efecto de diseminación que esto produce sobre los usuarios y su entorno. Esta exposición aumenta la vulnerabilidad frente a riesgos como la ingeniería social, donde los atacantes explotan la información compartida en redes sociales digitales para manipular o dañar al usuario.

En el Capítulo 2 se exploraron los antecedentes y casos emblemáticos de ataques a la privacidad, como los incidentes de Cambridge Analytica en Facebook y la filtración de datos en LinkedIn. Estos ejemplos proporcionan un panorama sobre las técnicas empleadas por los atacantes y la facilidad con la que pueden aprovechar la información accesible públicamente en redes sociales para obtener beneficios personales o comerciales. La exposición no se limita a los usuarios individuales, sino que afecta a un nivel más amplio, generando un “efecto dominó” en la red de contactos del usuario expuesto.

El análisis de estos antecedentes demostró que las redes sociales presentan vulnerabilidades que pueden ser explotadas tanto por atacantes internos como externos. Los primeros incluyen a usuarios legítimos de la plataforma que abusan de la confianza de otros para obtener información, mientras que los segundos, los atacantes externos, acceden a datos públicos sin necesidad de estar registrados, aprovechando la exposición que muchos usuarios dejan sin controlar. Este fenómeno evidencia una falta de conocimiento sobre la manera en que los datos compartidos en plataformas digitales pueden ser accedidos y utilizados sin el consentimiento explícito del usuario; una situación que potencia la necesidad de una mayor concientización y educación sobre prácticas de privacidad en redes sociales digitales.

El análisis de políticas de privacidad en el Capítulo 3 reveló que, si bien las plataformas como Facebook, Instagram y LinkedIn ofrecen opciones de configuración de privacidad, éstas suelen ser complejas de entender y ajustar correctamente. Este capítulo mostró cómo las políticas de privacidad generalmente resultan insuficientes para proteger a los usuarios, dado que son extensas y están redactadas en lenguaje técnico y requieren una administración manual detallada por parte del usuario para ajustar su perfil adecuadamente. A pesar de que las plataformas notifican sobre actualizaciones en sus políticas, no siempre es claro para los usuarios el impacto de estos cambios en su exposición personal.

Derivado de lo anterior, se remarca la importancia de que las plataformas simplifiquen y mejoren sus políticas de privacidad, incorporando interfaces más intuitivas y alertas de seguridad que guíen al usuario en cada ajuste de privacidad. Asimismo, se recomienda que las redes sociales adopten prácticas de privacidad predeterminada que reduzcan la visibilidad de los datos personales, contribuyendo a un entorno más seguro para los usuarios.

En el Capítulo 4 se revisaron los tipos de ataques más comunes, como la ingeniería social y el scraping, que explotan las configuraciones de exposición de los perfiles en redes sociales digitales. Estos ataques muestran cómo los atacantes, internos o externos, pueden aprovechar la información compartida para realizar fraudes, extorsiones y otros delitos. Estos ataques se facilitan por la falta de conocimiento de los usuarios sobre las configuraciones de privacidad, evidenciando la necesidad de educación en este ámbito

En dicho capítulo también se describió la metodología OSINT. La misma permite comprender el alcance de la exposición digital a través de la recopilación de datos públicos. En el contexto de esta tesis, OSINT se presenta como una herramienta que facilita el análisis de perfiles y la detección de posibles factores de riesgo. Este enfoque no solo permite identificar las vulnerabilidades en el perfil de un usuario, sino que también puede ser utilizado por los propios usuarios para evaluar y reducir su nivel de exposición, promoviendo un uso más seguro y consciente de sus datos en redes sociales. Además, se puede mencionar que el potencial de OSINT radica en que permite realizar análisis detallados de la información pública en redes sociales digitales, una práctica que puede realizarse manualmente o a través de herramientas informáticas.

En el Capítulo 5, se desarrolló un modelo conceptual que especifica cómo los elementos de un perfil biográfico digital contribuyen a la exposición de un usuario y su entorno. Este modelo conceptual sirve como base para diseñar estrategias de mitigación, dado que permite a los usuarios entender la relación entre los distintos componentes de su perfil y los riesgos que implican. Por eso es fundamental identificar los Factores de Exposición porque son los amplificadores de cada uno de los Tipos de Atributos expuestos y definen al final, el valor total de la exposición para los usuarios y su entorno.

En el Capítulo 6 se presentaron métricas específicas que permiten a los usuarios evaluar su exposición, basándose en la visibilidad y sensibilidad de la información compartida. Estas métricas son una herramienta para que los usuarios comprendan cómo cada elemento del perfil impacta en la privacidad. La implementación de estas métricas permite alertar a los usuarios sobre el riesgo de ciertas publicaciones, contribuyendo a reducir la exposición de sus datos. Para mitigar una exposición inadecuada, estas métricas deben tender a cero, para que la publicación efectuada represente lo que realmente se desea exponer y no más. Como una regla de oro en relación con las Redes Sociales Digitales, cuando un usuario decida crear un perfil y publicar información, en primer lugar, debe saber que ya está ingresando a una plataforma de acceso público. Esto significa que su perfil estará en Internet y la superficie de exposición y posterior ataque será más alta en dicho ambiente.

Durante el Capítulo 7, se propusieron recomendaciones prácticas de mitigación y sanitización de exposición de los usuarios. Además, se mencionó el concepto de capas de seguridad, para aplicar a nivel dispositivos, plataforma de redes sociales y a nivel de uso de las mismas. Estas prácticas, junto con el uso de métricas de exposición, ayudan a los usuarios a comprender su perfil de privacidad y adoptar medidas concretas para reducir su vulnerabilidad en redes sociales. Además, las plataformas deben contribuir activamente con configuraciones predeterminadas seguras y notificaciones claras, mejorando así la capacidad del usuario para gestionar su exposición. Por lo anterior mencionado, la clave está en cómo minimizar la exposición y tomar las medidas adecuadas para que la información compartida en las Redes Sociales Digitales esté protegida y se tenga control sobre la privacidad.

Como primera medida de mitigación, se debe proteger el dispositivo sobre el que se accede al perfil de la red social y el inicio de sesión concreto a la plataforma. Vale considerar que la Seguridad Informática actúa por capas, colocando medidas de seguridad en diferentes niveles, para proteger desde diferentes posiciones, de tal manera que, si un atacante logra superar una barrera, todavía existen otras que se deben superar. En base a lo anterior, el concepto de capas de seguridad aplicará a la protección del acceso a la Red Social para el usuario.

Por otro lado, en segundo lugar, para mitigar la exposición de un perfil, se deben aplicar una serie de prácticas que ayudan a la “limpieza” de la exposición de un perfil en una red social digital. Con estas prácticas, lo que se busca es controlar los factores de exposición que posee el perfil. Este concepto se denomina también “sanitización” y hace referencia a articular las medidas y cambios necesarios para lograr un nivel de exposición adecuado.

Es importante mencionar que la exposición no se puede eliminar completamente y que, una vez que se publica información, ya no se tiene control de su ciclo de vida. En el caso de buscar la “máxima sanitización”

posible, entonces se debería eliminar el Perfil completo de la Red Social. Por lo tanto, considerando un perfil biográfico digital, se deben tener en cuenta las prácticas de sanitización que se presentaron en el Capítulo 7. Esto incluye, de manera resumida, considerar lo siguiente: gestión de contactos evitando no aceptar desconocidos; revisión de perfiles y publicaciones para detectar información sensible; eliminación o modificación de publicaciones riesgosas y que atenten contra la privacidad; búsqueda del propio nombre de los usuarios en redes sociales digitales para identificar menciones, revelando posibles exposiciones no intencionadas de uno mismo o de otros.

Finalmente, en el Capítulo 8, se propuso una herramienta informática de análisis que está prevista para emplear técnicas de Inteligencia Artificial y reconocimiento de imágenes para evaluar la exposición de fotos en redes sociales digitales. Este prototipo se piensa como una extensión del navegador Web que ayuda al usuario a analizar el contenido de sus fotos antes de publicarlas, proporcionando advertencias sobre el nivel de exposición y ofreciendo sugerencias para proteger la privacidad. La implementación de esta herramienta informática busca ofrecer a los usuarios un método práctico para controlar y medir su nivel de exposición. Al detectar los Factores de Incremento de Exposición en las fotos, esta herramienta permite una evaluación de riesgos, haciendo que el usuario tenga una visión más clara de cómo su publicación puede exponer más información sensible de lo que realmente se desea. Además, al permitir al usuario recibir recomendaciones sobre su contenido, esta herramienta fomenta un uso más consciente y seguro de las redes sociales, ayudando a prevenir exposiciones innecesarias.

Líneas de Trabajo Futuras

A continuación, se enumeran las líneas de trabajo futuras para este proyecto:

1. Incorporar un conjunto de restricciones OCL (Object Constraint Language) al modelo conceptual que permitan validar diferentes modelos de instancias, y agregar consultas sobre dichos modelos, por ejemplo, para inferir la existencia de Exposición en cadena en un PBD, o cuando un usuario es un Sujeto Expuesto Pasivo
2. Desarrollar una herramienta que se integre a los navegadores web y permita determinar y alertar a los usuarios de una posible exposición inadecuada cuando está subiendo una foto a un perfil biográfico digital. En un trabajo relacionado, se propuso un modelo conceptual que incorpora los principales aspectos que intervienen en el dominio de una herramienta de tales características.
3. Validar la herramienta como elemento de concientización tanto para uso individual, como por organizaciones. Esto deriva en la creación de un programa de concientización para los usuarios, tomando como base una encuesta a una determinada muestra de ellos para indagar sobre los comportamientos

presentes en las Redes Sociales Digitales. La encuesta deberá indagar sobre el conocimiento de las personas de las Políticas de Privacidad de cada una de las plataformas. Es decir, si conocen de su existencia y si las tienen en cuenta para leer o si se omiten directamente

4. Definir reglas que automaticen la detección de factores de exposición o usuarios expuestos pasivos.
5. Se explorará la posibilidad de emplear tecnologías de reconocimiento de imágenes. A continuación, se muestran una serie de ejemplos de librerías detección de objetos en imágenes sobre los cuales se busca indagar a futuro para la aplicación en este trabajo: Azure AI | Vision Studio[27], Google Cloud - API de Cloud Vision[28], Image Recognize[29] y Astica[30].

Conclusiones finales

Con el desarrollo de este trabajo de tesis, se reafirma la necesidad de una concientización activa sobre la privacidad en el ámbito digital, donde cada acción y publicación contribuye a la configuración de un perfil de exposición. El enfoque basado en OSINT y la propuesta de una herramienta informática de análisis de exposición representan un avance en el camino hacia una mayor protección de los usuarios, permitiendo a estos, tomar el control de su privacidad y cuidando su exposición y la de su entorno.

A medida que las redes sociales digitales se integran cada vez más en la vida cotidiana, es importante que los usuarios estén capacitados para entender y manejar sus niveles de exposición. Este proceso es una responsabilidad compartida entre los usuarios y las plataformas, quienes deben ofrecer configuraciones de privacidad accesibles y claras, y facilitar una comprensión real de cómo sus datos personales pueden ser utilizados.

Este trabajo de tesis contribuye al objetivo de brindar a los usuarios de un conocimiento más profundo sobre su privacidad y los medios necesarios para protegerla, impulsando la gestión responsable de la exposición digital tomando a la concientización como pilar fundamental.

Un factor importante para mencionar es el comportamiento de los usuarios de las redes sociales digitales. Independientemente de las medidas de seguridad que cada plataforma implemente y de las configuraciones de privacidad efectuadas en los perfiles biográficos digitales, en última instancia está el comportamiento del usuario como único dueño de la exposición que desea realizar.

Cada una de las personas dueñas de un perfil biográfico digital, son las propietarias de sus publicaciones y, por ende, son quienes deciden qué y cómo exponer la información. Si bien una herramienta

[27] Azure AI | Vision Studio: https://portal.vision.cognitive.azure.com/demo/generic-object-detection
[28] Google Cloud - API de Cloud Vision: https://cloud.google.com/vision/docs/object-localizer?hl=es-419
[29] Image Recognize: https://imagerecognize.com/
[30] Astica: https://www.astica.org/vision/object-detection/

informática podría ayudar a mostrar qué nivel de exposición tiene una determinada publicación, la decisión final la tendrá cada usuario. Por lo dicho anteriormente, es clave trabajar en un proceso de concientización hacia las personas, relacionado al cuidado de la exposición en las redes sociales digitales y los posibles ataques y consecuencias que un inadecuado uso de la información puede producir en los usuarios y su entorno.

Este trabajo de tesis propone una capa de concientización para los usuarios de redes sociales que permite tener conocimiento del nivel de exposición de sus publicaciones, logrando preservar la privacidad del usuario en el nivel deseado. Para ello se identificaron una serie de atributos de exposición frecuente, los cuales, en conjunto, con las medidas de sanitización propuestas, contribuyen al fortalecimiento de las acciones que posibilitan la protección de los perfiles biográficos digitales.

El ideal es que los usuarios de manera activa opten por preservar su privacidad y cuando decidan publicar información en una Red Social Digital, ya lo hagan aplicando las mitigaciones, atenuando el nivel de exposición y confiando en que mostrarán lo que quieren mostrar con total conocimiento del acto. Claro está que una herramienta que ayude en este proceso será un gran aliado. Sin embargo, no hay que quitar el foco por el cual se desea que las personas incorporen en sus conductas de usuarios de las plataformas de redes sociales, el manejo consciente y seguro de su exposición.

Tal como se mencionó al principio de este trabajo, administrar un perfil de una red social digital por parte de un usuario conlleva una gran responsabilidad. De ello depende que tan vulnerable será su privacidad y la de su entorno. Las plataformas de redes sociales digitales cuentan con las configuraciones para mitigar la exposición, pero el único y verdadero dueño, quien tiene el mando para decidir cómo mostrar su información, es ni más ni menos que el usuario. Ellos tienen el poder absoluto y son responsables plenos de cuidar su exposición y la de sus cercanos. En conclusión, las personas son los principales custodios de su información personal, y, por lo tanto, son las principales interesadas en proteger su privacidad y la de su entorno.

Bibliografía:

1. Stalman, A.: Humanoffon. Ediciones Deusto (2016).
2. Wu He.: A review of social media security risks and mitigation techniques. In: Journal of Systems and InformationTechnology Vol. 14, pp. 171 – 180 (2012).
3. LinkedIn Blog Page, https://blog.linkedin.com/2016/05/18/protecting-our-members, last accessed: 2020/05/23.
4. Infobae Homepage, https://www.infobae.com/america/tecno/2018/03/20/7-datos-para-entender-el-escandalo-de-facebook-y-cambridge-analytica/, last accessed: 2020/05/23.
5. WhatsApp Homepage, https://www.whatsapp.com/unsupportedbrowser?doc=privacy-policy&version=20160825, last accessed: 2020/05/23.
6. AEPD Homepage, https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/la-aepd-sanciona-whatsapp-y-facebook-por-ceder-y-tratar, last accessed: 2020/05/23.
7. Twitter Blog Page, https://blog.twitter.com/en_us/topics/company/2020/an-update-on-our-security-incident.html, last accessed: 2020/06/21.
8. Rosenblum D.: What Anyone Can Know: The Privacy Risks of Social Networking Sites. In: IEEE Security & Privacy, vol. 5, no. 3, pp. 40-49 (2007).
9. Choi, B. C. F., Jiang, Z. (Jack), Xiao, B., & Kim, S. S.: Embarrassing Exposures in Online Social Networks: An Integrated Perspective of Privacy Invasion and Relationship Bonding. In: Information Systems Research, pp. 675–694 (2015).
10. Srivastava A., Geethakumari G.: Measuring privacy leaks in Online Social Networks. In: 2013 International Conference on Advances in Computing, Communications and Informatics (ICACCI), pp. 2095-2100 (2013).
11. F. Company y Meta, https://about.fb.com/news/2023/06/parental-supervision-and-teen-time-management-on-metas-apps/amp/, last accessed 2024/01/27.
12. F. Company y Meta, https://about.fb.com/news/2024/01/teen-protections-age-appropriate-experiences-on-our-apps/, last accessed 2024/01/27.
13. Télam, https://www.lavoz.com.ar/tecnologia/detectaron-una-megafiltracion-de-datos-en-linkedin-twitter-y-otras-redes/, last accessed 2024/01/27.
14. E. Snowden: Vigilancia permanente. Editorial Planeta (2019).
15. A. Groenewald, https://www.cyberghostvpn.com/es_ES/privacyhub/countries-ban-social-media/, last accessed 2024/02/03.

16. Bellamy, R. K. E., & Williams, A. R.: Privacy in the Metaverse: Addressing the Risks of Biometric Data Exposure in Immersive Social Networks. In: Virtual Reality & Intelligent Interaction, pp. 100-115 (2024).
17. Singh, R., & Bhargava, R.: Facial Recognition and Privacy Concerns on Social Media: A Study of Facebook and Instagram. In: Journal of Privacy and Confidentiality, pp. 22-37 (2023).
18. De Wolf, R., & Van der Weij, P.:. Privacy Concerns in Professional Social Networks: An Analysis of LinkedIn Users' Perceptions and Practices. In: Computers in Human Behavior (2023).
19. Rahman, F., & Smith, M.: Artificial Intelligence and Privacy in Social Media: Opportunities and Risks. In: Journal of Artificial Intelligence Research, pp. 123-145 (2024).
20. Nuevo proyecto de Ley de Protección de Datos Personales. (2024). Argentina.gob.ar. https://www.argentina.gob.ar/aaip/datospersonales/proyecto-ley-datos-personales.
21. Balbiano, M., Castillo, N., Karchesky, D., Bircher, F., Bressan, M. & Zenobi, R: Caracterización de los perfiles biográficos digitales en Facebook de adolescentes de Rafaela y Sunchales (2014).
22. Lobrería OpenCV. OpenCV Documentation. (2025). https://docs.opencv.org/.
23. Alexey Bochkovskiy. YOLOv4: Optimal Speed and Accuracy of Object Detection. (2020). https://github.com/AlexeyAB/darknet.