ANÁLISIS DE LA PRIVACIDAD Y SEGURIDAD EN LAS REDES SOCIALES EN UN MUNDO DE CIBERDELITOS

(Un enfoque desde la cibercriminología y la ciberseguridad)

TRABAJO DE FIN DE GRADO

Grado: Criminología

Autora: Dña. Estefania Varela Campos

Profesor-Tutor: Don. Mikel Rufián Albarrán

Madrid, 2024

Resumen

El actual proyecto se enfoca en analizar la percepción de las personas respecto a la privacidad y seguridad en las redes sociales, considerando la evolución tecnológica y los riesgos en un uso inadecuado de las plataformas sociales. La metodología se basa en una revisión bibliográfica que da lugar a un marco teórico amplio, abordando cuatro aspectos relevantes, como son la ciberseguridad, la cibercriminología, ciberespacio y los ciberdelitos destacando su impacto en el contexto de las redes sociales. Dentro del marco teórico, se analiza la naturaleza cambiante de las tecnologías de la información y comunicación, y su influencia en la forma en que las personas interactúan entre sí. Se identifica la exposición a diversas amenazas, como puede ser el robo de identidad, la difusión de información falsa o la violación de la privacidad personas. Además, se estudia la importancia de la protección de datos personales y la necesidad de concienciación y educación en la sociedad sobre la materia a tratar. De manera específica, para abordar el objetivo principal del estudio, se diseñó y se aplicó una encuesta dirigida a los usuarios de redes sociales, con el fin de evaluar su percepción hacia la protección de su privacidad y seguridad en línea. Los resultados se relacionan con el marco teórico, permitiendo una comprensión más profunda sobre las percepciones y preocupaciones de los usuarios en relación con este tema crucial en la era digital. Dando lugar a una metodología mixta, tanto cualitativa como cuantitativa.

Palabras clave: *ciberseguridad, cibercriminología, ciberespacio, ciberdelitos, redes sociales, privacidad, seguridad.*

Abstract

The current proyect focuses on analyzing individuals' perception regarding privacy and security on social networks, considering technological evolution and risks associated with inappropriate use of social platforms. The methodology is based on a literature review that leads to a comprehensive theoretical framework, addressing four relevant aspects: cbersecurity, cybercriminology, cyberspace, and cybercrimes, highlighting their impact within the context of social networks. Within the theoretical framework, the changing nature of information and communication technologies and their influence on how people interact with each other are analyzed. Exposure to various threats, such as identity theft, dissemination of false information, or violation of personal privacy, is identified. Additionally, the importance of personal data protection and the need for awareness and education in society on the subject are studied. Specifically, to address the main objective of the study, a survey was designed and administered to social media users to evaluate their perception towards the protection of their privacy and security online. The results are linked to the theoretical framework, allowing for a deeper understanding of users' perceptions and concerns regarding this crucial topic in the digital age, resulting in a mixed methodology, encompassing both qualitative and quantitative approaches.

Keywords: cybersecurity, cybercriminology, cyberspace, cybercrimes, social networks, privacy, security.

ÍNDICE

1 INTRODUCCIÓN

1.1 Justificación

La elección del tema para el Trabajo de Fin de Grado se fundamenta en la necesidad de abordar los desafíos relacionados con la privacidad y seguridad en las redes sociales. Esta decisión surge ante el reconocimiento de la creciente importancia que las plataformas de redes sociales han adquirido en la vida cotidiana de las personas a nivel global. Sin embargo, junto con su popularidad, también han surgido una serie de preocupaciones en torno a la gestión y protección de la información personal de los usuarios.

El panorama de las redes sociales presenta una constante evolución tecnológica, la cual lleva a la aparición de amenazas y con ello a una serie de riesgos que puede suponer un problema para la privacidad y seguridad de los usuarios. Desde el robo de identidad, y suplantación de cuentas hasta la difusión de noticias falsas y el ciberacoso, las redes sociales se han convertido en un terreno fértil para una variedad de vulnerabilidades que pueden tener consecuencias adversas tanto a nivel individual como general.

Es evidente que el manejo inadecuado de la privacidad y seguridad en las redes sociales puede tener impactos significativos en la sociedad en su conjunto. La difusión de información falsa y la violación de privacidad, puede deteriorar la confianza en las instituciones, alterar la percepción pública y dañar la credibilidad dentro de un sistema democrático. Por tanto, es esencial comprender y abordar estos problemas de manera efectiva para salvaguardar los derechos y la seguridad de los usuarios en el entorno digital.

Desde una perspectiva académica y profesional, el estudio de la privacidad y seguridad en las redes sociales es de gran relevancia y utilidad. Hoy en día, existe una gran demanda creciente de investigaciones que contribuyen al desarrollo de políticas más rigurosas y herramientas eficaces para proteger la privacidad y seguridad dentro de las plataformas sociales. El Tfg representa, por tanto, una gran oportunidad para explorar en profundidad estos aspectos críticos y poder contribuir al avance del conocimiento en este campo en constante evolución.

El estudio y análisis detallado de la privacidad y seguridad en las redes sociales según las percepciones de los usuarios, ayudará a su comprensión y proporcionará una base sólida para abordar estos desafíos de manera efectiva y promover un uso seguro y responsable de las plataformas en línea, a través de la mejora de las estrategias que han sido creadas para su protección.

1.2 Objetivos

1.2.1 Objetivo general

Evaluación de la percepción de los usuarios de redes sociales sobre la privacidad y seguridad en línea.

1.2.2 Objetivos específicos

- Analizar las distintas amenazas de seguridad, así como las oportunidades que existen hoy en día para violar el uso de la privacidad de los usuarios dentro de las plataformas de redes sociales desde una perspectiva de la cibercriminología.
- Evaluar las diversas medidas y estrategias de ciberseguridad dentro del entorno Social Media para disminuir los riesgos asociados con la cibercriminalidad.
- Investigar el nivel de conciencia y comportamiento de los usuarios dentro de las redes sociales y el impacto que ha tenido.

1.3 Hipótesis

- Cuanto más conectados estemos a las redes sociales mayor será el riesgo de amenazas y ataques en el ciberespacio.
- Las medidas y estrategias de protección no serán efectivas por la poca conciencia y educación que reciben y tienen los usuarios.
- La evolución constante de las herramientas de ciberseguridad creadas por los organismos sociales, suponen un impacto positivo para la reducción de los ataques dentro del ciberespacio.

2 MARCO TEÓRICO

2.1 Contextualización

Hace ya unos años, la creación de las redes sociales supuso un "boom" en la historia de nuestro planeta abriendo puertas hacia un abanico amplio de posibilidades a la hora de relacionarse y de comunicarse las personas. Empezó siendo algo desconocido, y, hoy en día, se ha vuelto algo imprescindible para la mayoría de la gente.

La gran cantidad de personas conectadas a las redes sociales ha supuesto que diversos **ciberdelincuentes** hayan tomado camino para la comisión de los delitos. Han encontrado en las redes sociales un campo fértil para llevar a cabo sus acciones delictivas, aprovechando la vulnerabilidad de los usuarios y la ingenuidad de muchos frente a los riesgos asociados con la privacidad y seguridad en línea.

Es por ello, por lo que muchos organismos e instituciones, tanto nacionales como internacionales, luchan por crear herramientas que ayuden a salvaguardar la privacidad de las personas dentro de las plataformas y canales de comunicación sociales. A través de la **ciberseguridad**, equipos de profesionales protegen todo tipo de redes, aplicaciones de software, datos electrónicos, etc.

Pero no todo vale, porque al igual que la **ciberseguridad** se ha ido especializando en el ámbito de la **cibercriminalidad**, el cibercrimen también ha evolucionado, lo que ha supuesto que sus principales protagonistas, es decir, los **ciberdelincuentes**, estudien y trabajen en obtener sus mejores resultados, y con ello mejores técnicas de ejecución para la comisión de sus delitos.

Por otro lado, cabe destacar la importancia del papel de la **cibercriminología** dentro del amplio tema, ya que gracias a la misma nos ayuda a entender la naturaleza del problema, lo que piensa, y la manera en la que puede actuar un ciberdelincuente. Nos guía hacia la elaboración de las estrategias y medidas para hacer frente a los comportamientos cibercriminales.

En esta perspectiva, surge la necesidad de abordar el complejo de factores que influyen en la seguridad y privacidad en las redes sociales desde una perspectiva multidisciplinaria. ¿Cómo afecta la actividad delictiva en línea a la privacidad y seguridad de los usuarios de redes sociales? ¿Cuál es el papel de la **ciberseguridad** y la **cibercriminología** en la protección contra estos riesgos emergentes? ¿Qué estrategias y medidas pueden implementarse para mitigar eficazmente los riesgos asociados con la

actividad delictiva en línea en el contexto de las redes sociales? Siendo algunas de las preguntas de investigación que guiarán el análisis en este estudio.

2.2 Ciberespacio

En la actualidad el concepto de **ciberespacio** ha dejado de ser una mera especulación de la ciencia ficción para convertirse en una realidad tangible. Es un universo que permite la comunicación, interacción y comprensión entre personas en un entorno y espacio virtual. Gracias al avance de la tecnología y a la capacidad del ser humano, dentro de este mundo digital la información fluye sin restricción, desafiando los límites del espacio y el tiempo.

El nacimiento del **ciberespacio** surge con la novela que escribió William Gibson (1984) "El **ciberespacio**. Una alucinación consensual experimentada diariamente por billones de legítimos operadores, en todas las naciones, por niños a quienes se enseña altos conceptos matemáticos… Una representación gráfica de la información abstraída de los bancos de todos los ordenadores del sistema humano. Una complejidad inimaginable. Líneas de luz clasificadas en el no-espacio de la mente, conglomerados y constelaciones de información. Como las luces de una ciudad que se aleja…". Una novela ficticia, que empezó siendo algo imaginario, algo lejano de la realidad y que acabó formando parte de la sociedad.

En el ámbito físico tangible, la evolución y expansión mundial a lo largo de los años de las redes de comunicación a través de las tecnologías, ha permitido la creación de un espacio de interacción humana, el **ciberespacio**, con el poder de influir en la sociedad desde una perspectiva económica, social, política y cultural. Su desarrollo constante está ligado a una evolución continua de las telecomunicaciones y tecnologías de la información que se inician en la primera mitad del siglo XIX. A lo largo de la historia, el correo postal fue el principal medio para enviar mensajes a distancia. Sin embargo, este método se vio desafiado con los avances científicos que permitieron la integración de la electricidad en las telecomunicaciones. Esto marcó un hito significativo al posibilitar la transmisión de mensajes más allá de los límites visuales, no solo físicamente si no de manera virtual (Gómez, 2013).

A diferencia de otros tipos de espacios, que tienen una función específica y pueden realizar otro tipo de funciones, el **ciberespacio** surge como un espacio racional, un

espacio que no es real. Dos personas pueden encontrarse en un espacio físico y empezar algún tipo de relación y luego despedirse, pero el espacio físico donde se reúnen va a seguir estando ahí cuando esa relación se termine. Sin embargo, el **ciberespacio** existe solamente como relacional, su realidad se construye a través del intercambio de información, siendo a la vez espacio y medio virtual. Una red sin interacción entre sus miembros deja de ser una red, su existencia depende de las relaciones entre sus integrantes (Aguirre Romero, 2004).

En la actualidad esa red de información mundial se denomina "Internet", concepto que se remonta desde 1957, durante la Guerra Fría, Estados Unidos y la Unión Soviética estaban inmersos en un enfrentamiento que abarcaba diversos ámbitos, como lo eran los ideológicos, económicos, políticos, militares y, por supuesto, tecnológicos. En este contexto, Estados Unidos sentía la necesidad de proteger su información y comunicaciones en caso de un ataque nuclear por parte de la Unión Soviética. Como resultado, surgieron innovaciones dirigidas a resolver este problema, las cuales dieron lugar a lo que hoy se conoce como Internet (Forero, 2019).

Desde los orígenes, han aumentado las actividades sociales hacia el **ciberespacio** y una mayor dependencia de las tecnologías digitales. La pandemia de COVID-19 marcó un punto de inflexión en esta tendencia, llevando consigo una rápida transición de servicios, interacciones y relaciones hacia el mundo virtual, algo que antes parecía impensable. En la actualidad, la gran parte de la vida social de las personas, como negocios, transacciones financieras, educación, compras y relaciones personales se encuentran dentro de la esfera digital (Sánchez Vera et al., 2022).

Esta expansión acelerada del **ciberespacio** ha sido fascinante por las nuevas oportunidades y servicios que ha desarrollado, pero a su vez preocupante, debido a los riesgos y amenazas que ha generado. La seguridad en el **ciberespacio** está lejos de ser una garantía absoluta, y el desarrollo de actividades en este nuevo entorno ha ido de la mano con un aumento de los **ciberdelitos**. En este sentido, es evidente que el **ciberespacio** ha dado lugar a una nueva forma de criminalidad. Los **ciberdelincuentes**, ya sea de manera individual o en grupos organizados, pueden ejecutar ataques desde cualquier lugar con recursos mínimos y causar un impacto significativo en sus víctimas, ya sean personas, empresas, entidades públicas o incluso países. Este aumento del ciberdelito se debe tanto a las características tecnológicas como a factores socioculturales (Sánchez et al., 2022).

2.2.1 Cifras generales del ministerio del interior de Cibercriminalidad

Desde hace décadas, la criminalidad en España ha sido objeto de una atención prioritaria por parte de los gobiernos, siendo considerada un factor de riesgo que repercute de forma directa en la seguridad y bienestar de la población, además de influir en la evaluación de la efectividad de las políticas gubernamentales en materia de seguridad ciudadana. A pesar de esto, la criminalidad no se ha frenado y la sociedad ha ido avanzando, la aparición de nuevas tecnologías y su desarrollo han propiciado el nacimiento de nuevos delitos y delincuentes especializados en el ámbito de la **cibercriminalidad**.

Datos estadísticos del Ministerio del Interior (2023) muestran como en el tercer trimestre del año 2023 se reúne el progreso de Criminalidad en España recogido por las Fuerzas y Seguridad del Estado. Entre enero y septiembre de 2023, hubo un aumento del 5,0% en la criminalidad total comunicada por la policía en España en comparación con el mismo periodo del año anterior. El incremento marca un cambio en la tendencia, dado que el crecimiento en el primer trimestre de 2023 fue del 7,2% y del 5,8% en el primer semestre, lo que indica una disminución en la brecha con respecto a 2022.

Durante ese periodo se registró un total de 1.826.911 infracciones penales. De estas, 1.489.660 se clasifican como delitos convencionales, abarcando todas las formas de delincuencia que no están relacionadas con el **ciberespacio**. Se destacan "los delitos contra la libertad sexual" que incrementan un 12,0% con respecto a 2022, las personas toman conciencia sobre la problemática y se reduce la tolerancia, por lo que las víctimas adoptan mayor iniciativa a denunciar su caso. El tráfico de drogas aumenta un 8,9%, de 14.462 hechos registrados en los primeros nueve meses de 2022 a 15.750 en 2023. Quedan registrados mayores hechos delictivos en 2023 con la efectividad de las distintas actuaciones de las Fuerzas y Cuerpos de Seguridad en el marco de ejecución de planes específicos.

Por otro lado, la evolución y el aumento del uso de Internet que se muestra desde 2016, supone la aparición de la **cibercriminalidad**, en tanto que, de toda la suma de infracciones penales registradas, esta presenta un 18,5% del total, 337.251 de delitos cometidos a través de sistemas informáticos, incremento del 21,5% sobre 2022. Las estafas son uno de los tipos delictivos más ejecutados dentro de la clasificación con un total de 304.819 infracciones cometidas, lo que representa un 90,4% de la

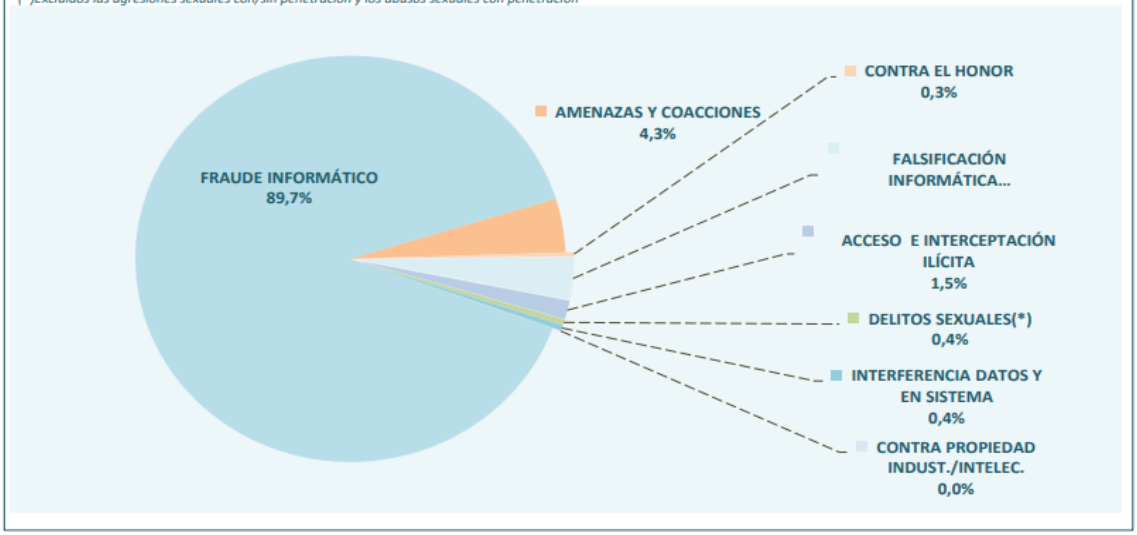
cibercriminalidad y el 16,7% de la delincuencia total, experimentando un aumento del 22,8% en comparación con 2022.

De manera más específica y para una mejora de su comprensión, el Ministerio del Interior (2022) realiza un análisis donde se puede ver la representación de distintos **ciberdelitos** cometidos por diversos **ciberdelincuentes**. Entre ellos se observa de manera significativa que el fraude informático es el delito que más veces se comete con un 89,7% del total de los hechos conocidos, seguido de amenazas y coacciones con un 4,3%.

Imagen 1: Evolución de hechos conocidos por categorías delictivas (Datos estadísticos de **cibercriminalidad** 2022).

HECHOS CONOCIDOS	2018	2019	2020	2021	2022
ACCESO E INTERCEPTACIÓN ILÍCITA	3.384	4.004	4.653	5.342	5.578
AMENAZAS Y COACCIONES	12.800	12.782	14.066	17.319	15.982
CONTRA EL HONOR	1.448	1.422	1.550	1.426	1.191
CONTRA PROPIEDAD INDUST./INTELEC.	232	197	125	137	114
DELITOS SEXUALES(*)	1.581	1.774	1.783	1.628	1.646
FALSIFICACIÓN INFORMÁTICA	3.436	4.275	6.289	10.476	12.569
FRAUDE INFORMÁTICO	136.656	192.375	257.907	267.011	335.995
INTERFERENCIA DATOS Y EN SISTEMA	1.192	1.473	1.590	2.138	1.662
Total HECHOS CONOCIDOS	**160.729**	**218.302**	**287.963**	**305.477**	**374.737**

(*)Excluidos las agresiones sexuales con/sin penetración y los abusos sexuales con penetración



Fuente: Sistema estadístico de Criminalidad realizado por el Ministerio del Interior

2.3 Privacidad en línea y Ciberseguridad

2.3.1 Normativa general de protección de datos

Según el Ministerio de hacienda (s.f.) "el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, (Reglamento general de protección de datos, RGPD) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), establecen el marco legal de referencia que desarrolla el derecho fundamental a la protección de datos personales.

Queda derogada la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, sin perjuicio de lo previsto en la disposición adicional decimocuarta de la LOPDGDD, y siguen vigentes las disposiciones de su Reglamento, aprobado por Real Decreto 1720/2007, de 21 de diciembre, que no contradigan, se opongan, o resulten incompatibles con lo dispuesto en el RGPD y la LOPDGDD.

Para el tratamiento de datos personales relativos a condenas e infracciones penales, la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales constituye la norma de referencia por la que se rige el tratamiento de este tipo de datos. Dicha Ley Orgánica traspone a nuestro ordenamiento jurídico la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 relativa a esta misma materia.

En materia de seguridad del tratamiento, resulta de aplicación, en virtud de la disposición adicional primera de la LOPDGDD, el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad y, en el ámbito ministerial, la Política de Seguridad de la Información aprobada por la Orden HFP/873/2021, de 29 de julio"

El Reglamento General de Protección de Datos (RGPD), implementado en mayo de 2016 y obligatorio para todas las empresas de la Unión Europea desde el 25 de mayo de 2018, resulta ser significativo en la protección de la información personal en el ámbito digital. Este reglamento otorga a los ciudadanos un mayor control y seguridad sobre sus datos personales, y otorga a cada individuo el derecho a decidir sobre su uso por parte de entidades públicas o privadas, así como a gestionar el acceso a ellos y eliminarlos cuando quieran.

Muchas empresas aún no han tomado medidas significativas para adaptarse a esta nueva normativa. Muchas otras, a pesar de los desafíos que representa el cumplimiento del RGPD, están adoptando una perspectiva proactiva y buscando convertirlo en una ventaja competitiva. Reconocen que el conocimiento profundo de los datos proporcionados por sus clientes actuales y potenciales puede ser valioso en su estrategia comercial. En este sentido, están buscando asesoramiento y recursos para aprovechar el RGPD como un aspecto diferenciador y una oportunidad para prestar la mejor gama de servicios (Ekon, s.f.)

Un factor clave dentro del RGPD, es el rol del Delegado de Protección de Datos (DPD), que debe ser seleccionado en función de sus competencias profesionales, con unos conocimientos especializados en derecho y práctica en protección de datos. No se requiere ninguna titulación específica ni un certificado para ocupar este cargo. El DPD opera de manera independiente y se dedica a informar y asesorar al responsable o encargado del tratamiento de datos, así como supervisar el cumplimiento del RGPD. Es importante destacar que el DPD puede ser un miembro interno o externo de la organización, tanto una persona física como una jurídica (Agencia Española Protección Datos, s. f.).

Por otra parte, La Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD) tiene como objetivo principal salvaguardar la intimidad, privacidad e integridad de los individuos, al mismo tiempo que regula las obligaciones relacionadas con la transferencia de datos para asegurar un intercambio seguro de información (Pdatos, s.f.).

La modificación de esta ley se ha vuelto indispensable para adaptarse al avance de las nuevas tecnologías y enfocarse en un nuevo propósito: proteger los datos personales en el ámbito de Internet. Es por ello, por lo que hoy en día, la mayoría de los sitios web solicitan el consentimiento para aceptar cookies o marcar las casillas legales, permitiendo a los usuarios aceptar o rechazar la utilización de sus datos. Este derecho fundamental garantiza que terceros no puedan utilizar los datos personales de otros individuos, protegiendo así la intimidad de estas personas. La Agencia Española de Protección de Datos (AEPD), es la encargada de velar por el cumplimiento de esta ley (Pdatos, s.f.).

2.3.2 Importancia de la privacidad en redes sociales

La privacidad en las redes sociales es fundamental para proteger la integridad personal y la seguridad de los usuarios, con muchos los **ciberdelitos** que ocurren continuamente en el **ciberespacio**. Al mantener cierto nivel de privacidad, se reduce el riesgo de exposición a información sensible o datos personales que podrían ser utilizados de manera indebida o para cometer actos delictivos, como el robo de identidad o ciberacoso. Además, la privacidad en las redes sociales permite a los usuarios controlar quién tiene acceso a su contenido y con quién comparten su información, lo que contribuye a mantener relaciones digitales más seguras y confiables.

Los usuarios han de investigar y comprender las diversas opciones de configuración de privacidad que ofrecen las redes sociales. Esto permite a cada individuo decidir que información desea compartir o publicar en su perfil, siempre y cuando no incumplan las políticas de la plataforma. Además, al crear cualquier tipo de cuenta que requiera datos personales es fundamental conocer las políticas y condiciones de la plataforma, por lo que los usuarios tendrán que estar informados sobre las limitaciones y normativas bajo las cuales están utilizando los servicios. Es importante que los usuarios sean discretos al publicar cualquier tipo de información en línea, independientemente de la configuración de privacidad de la plataforma. Esto ayuda a proteger la privacidad y seguridad de los usuarios en un entorno digital cada vez más complejo (Polo Calvo, s.f.).

La política de cookies es un documento legal que debe estar presente en todas las páginas web que utilicen cookies, es decir, que almacenen pequeños archivos de texto en el navegador de los usuarios para registrar diversos tipos de datos mientras navegan por el sitio y, en algunos casos, incluso fuera de él. En España, el uso y la política de cookies están regulados tanto por la Ley de Servicios de la Sociedad de la Información y el Comercio Electrónico (LSSI-CE) como por la normativa de protección de datos, incluyendo el Reglamento General de Protección de Datos (RGPD) y la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD). Esto se debe a que las cookies recopilan información personal de los usuarios (Atico34, s.f.).

Dado que la presencia de las cookies en una página web son inevitables y universales en la actualidad, aparecerán en todo momento mientras se navega por Internet. Incluso se puede encontrar avisos de cookies en las Smart TV, ya que estas se conectan a Internet y los servicios de transmisión en línea también utilizan cookies, por lo que están sujetos a las mismas regulaciones que los sitios web (Atico34, s.f.).

2.3.3 Rol que tiene la Ciberseguridad en la protección de la privacidad

Más de 40 años atrás, “Creeper” fue el primer virus informático de la historia creado por Robert H. Thomas en 1970, no causaba daños más allá de crear un simple mensaje, pero aun asi fue considerado el origen de los actuales virus informáticos. Después de esto, han ido surgiendo numerosos virus y ciberataques con destacada relevancia mediática como la crisis de WannaCry (programa dañino), y desde entonces, la preocupación por la seguridad y privacidad de los usuarios ha ido aumentando. La **ciberseguridad** ha ocupado un papel fundamental dentro de toda esta preocupación, es un problema que afecta a los gobiernos, empresas y usuarios de redes en todo el mundo debido a las características únicas del **ciberespacio** que lo hacen propenso a la ocurrencia de ciberataques (Hernández, 2017).

La **ciberseguridad** desempeña un papel fundamental dentro de la privacidad, dedicada a salvaguardar la integridad personal de los usuarios en las plataformas sociales. Según Firma-e (2014) la confidencialidad, la integridad y la disponibilidad son los tres pilares básicos en los que se centra para poder asegurar la protección necesaria de los navegantes de redes.

La integridad mantiene la información en su forma original, sin ningún tipo de alteración ni manipulación en el sistema informático. Asegura que cualquier dato o archivo virtual conserva todas sus partes sin cambios no autorizados. La firma digital es una herramienta clave para garantizar esta integridad al verificar la autenticidad del usuario, es fundamental para asegurar que solo las personas autorizadas puedan acceder a los documentos mediante controles de acceso adecuados, con cualquier tipo de cifrado o contraseña.

La confidencialidad por su parte implica la protección de la información. Se pierde cuando no se siguen las medidas de seguridad apropiadas, como compartir contraseñas, dejar las sesiones abiertas sin supervisión o se tiran archivos sin borrar antes sus datos.

A su vez, la disponibilidad refiere la capacidad de acceder a la información cuando sea necesario, siguiendo los procedimientos correctos. Garantizar la disponibilidad puede entrar en conflicto con el término anterior, a través de las medidas estrictas de seguridad que dificultan el acceso.

Para lograr sistemas seguros que garanticen la confidencialidad, integridad y disponibilidad de los datos, se han propuesto diversos métodos de evaluación de

amenazas cibernéticas, así como prácticas y herramientas para el desarrollo seguro de software y hardware. A pesar de estos avances, el constante desarrollo de las Tecnologías de la Información y las Comunicaciones (TIC), junto con la aparición de nuevas vulnerabilidades y ataques de día cero, requiere un esfuerzo continuo en **ciberseguridad** para disminuir los riesgos y protegerse contra cibercriminales y softwares malicioso (Camilo et al., 2018).

Además, la **ciberseguridad** se apoya en la ciencia de la criminología que aporta numerosos métodos desde una perspectiva de la investigación, encargada de analizar los factores que contribuyen al riesgo y a la protección. Se centra en el delito, el delincuente y la víctima, que son cruciales en el estudio de la dinámica criminal, principios que se aplican de manera efectiva a la seguridad en línea. La **ciberseguridad** desarrolla los perfiles criminales ayudando al control sobre los **ciberdelincuentes**, rastreando, evitando el intercambio de información ilícita o cerrando sitios web que promueven actividades ilegales. Existe la necesidad de que los criminólogos se adapten y se preparen para un mundo en un ámbito tecnológico, adquiriendo conocimientos necesarios para comprender un mundo digital sin descuidar sus principios y teorías fundamentales. Esto permite una integración equilibrada que podría denominarse Criminología del **ciberespacio** o **cibercriminología** (Ara, 2022).

2.4 Cibercriminología

A lo largo de la historia, los delincuentes han aprovechado la tecnología para innovar en sus métodos delictivos, utilizando herramientas y recursos tecnológicos para alcanzar sus objetivos. La rapidez de las comunicaciones a distancia, la capacidad para realizar acciones y la posibilidad de mantener el anonimato son tres características clave de las nuevas tecnologías que, potencian la comisión de delitos. Anteriormente, un estafador tenía que planificar cuidadosamente su engaño, interactuar con la víctima y persuadirla para llevar a cabo la estafa, sin embargo, en el contexto de las estafas electrónicas, estos pasos se reducen de manera significante. Con el uso de herramientas tecnológicas, los delincuentes pueden llevar a cabo estafas desde cualquier lugar con acceso a Internet, alcanzando a múltiples víctimas a la vez y enviando diversos correos de manera inmediata. Además, pueden utilizar técnicas para ocultar su identidad y dificultar su rastreo o identificación.

Esta conexión entre la tecnología y el crimen ha dado lugar a la necesidad de crear un nuevo campo de estudio conocido como **cibercriminología**. Se atribuye su creación a Jaishankar, considerado el pionero de esta disciplina, quien lo define como el estudio de las causas de los delitos que tienen lugar en el **ciberespacio** y su repercusión en el mundo físico. La **cibercriminología** analiza el comportamiento criminal y la victimización en el **ciberespacio** desde una perspectiva teórica y criminológica. Según este autor, el uso del término se justifica por dos razones: para distinguir el estudio de los delitos informáticos de la investigación forense en este ámbito; y para establecer una disciplina independiente dedicada a explorar y entender los **ciberdelitos** desde una perspectiva de las ciencias sociales (Cámara Arroyo, 2020).

Su creación fue una extensión especializada de la Criminología, ciencia interdisciplinaria y multidisciplinaria holística que estudia de manera integral el fenómeno criminal. Cuando se habla de un conocimiento holístico en una ciencia, se hace referencia a la aspiración de comprender cada aspecto relacionado con el crimen, el delincuente, la víctima, así como su prevención, control y tratamiento, considerando estos factores conectados entre sí, como un conjunto que va más allá de la simple suma de sus partes. (Cámara Arroyo, 2020).

Así pues, la **cibercriminología** surgió como una extensión especializada de la Criminología para atender de forma específica los **ciberdelitos** que se realizan dentro de las plataformas sociales y las herramientas tecnológicas asociadas con ellos.

2.4.1 Conceptos fundamentales (ciberdelincuencia/cibercrimen/ciberdelito)

En la era digital actual, la **ciberdelincuencia** se ha convertido en un fenómeno de alcance global que plantea desafíos significativos para la seguridad tanto en el ámbito individual como en el colectivo. La evolución de las tecnologías y el crecimiento de los usuarios en las plataformas sociales han creado un escenario para la perpetración de delitos Informáticos, que abarcan desde el robo de identidad y el fraude financiero hasta el ciberacoso. En este contexto, la **cibercriminología** surge como una disciplina esencial para entender la naturaleza cambiante de la delincuencia en el **ciberespacio**. Al centrarse en el estudio científico de los **ciberdelitos**, sus causas, patrones y consecuencias, proporciona un marco teórico y metodológico para analizar y combatir eficazmente la **ciberdelincuencia**. Además, combina elementos de la criminología, la informática

forense, la psicología y la sociología, entre otros, que permiten una comprensión de los factores que impulsan los delitos en las redes, así como el desarrollo de estrategias de prevención y respuestas efectivas por parte de las autoridades y la sociedad en general.

Son muchos los autores que mencionan la "**cibercriminalidad**" en sus explicaciones sobre **ciberdelincuencia**, pero la cuestión reside en si realmente significarían lo mismo. En primer lugar, como gran diferencia entre esta última y la **ciberdelincuencia**, encontramos lo relativo a la organización del delito. Es decir, cuando se refiere a delitos informáticos, delincuencia informática o **ciberdelincuencia**, se hace alusión a aquellos delitos que ocurren a diario, tipificados penalmente, pero que ocurren de forma independiente, o individual. Por ejemplo, un caso de acceso indebido a una cuenta de correo electrónico, realizado por una persona a su expareja. O bien, cuando un empleado en una empresa borra información importante sin autorización (ERREIUS, 2018).

En cambio, cuando se habla de **cibercriminalidad** se refiere a una serie de cibercrímenes que ocurren de una forma más profesional, organizada, donde la principal motivación es la económica, los **ciberdelincuentes** buscan elevar sus ganancias a través del perfeccionamiento de distintas técnicas delictivas. Trabajan organizados en bandas, con una clara distribución de tareas. Un ejemplo de Cibercrimen puede ser el ransomware, un tipo de malware, que tiene como objetivo bloquear cifrando, el acceso a toda o parte de la información que contiene el equipo, para después poder pedir un rescate a cambio de su liberación. En estos casos los **ciberdelincuentes** no están interesados en el objetivo o en la víctima, sino que se busca el pago por el rescate. Es un negocio organizado, donde las bandas suelen estar compuestas por personas que se dedican a desarrollar el malware, otras a infectar sistemas, otras a la atención al cliente para indicar cuánto y cómo se debe pagar el rescate, entre otras, además muchas de ellas están compuestas por líderes. (Anónimo, 2018).

La realidad demuestra como el fenómeno de la **ciberdelincuencia** pese a ser una amenaza silenciosa puede llegar a causar mucho daño en la sociedad. Los hábitos de vida se trasladan al **ciberespacio**, que resulta ser la principal cuestión de la transformación digital, un gran reto para el Derecho Penal. Los actuales sistemas de justicia observan varios inconvenientes, los **ciberdelincuentes** son muy hábiles y no son fáciles de encontrar, entre tanto las actividades ilícitas a través de internet pueden llegar a alcanzar un impacto económico de un billón de euros al año en el mundo, según estimaciones del

Instituto Nacional de **ciberseguridad** (Incibe), cifra equivalente al PIB de un país como España. Fuentes policiales aseguran que esta actividad supera al narcotráfico en lucro. En cambio, las inversiones en **ciberseguridad** en el planeta se estima que alcanzan los 70.000 millones de euros (Lapuerta, 2017).

Por el contrario, los gobiernos encuentran en las TICs (Tecnologías de la Información y la Comunicación), otro camino para llevar a cabo la actividad criminal de forma más fácil, segura y eficaz. La existencia de estos instrumentos tecnológicos ha modificado las técnicas de investigación criminal. Ofrecen ventajas para la investigación de comportamientos delictivos, no solamente aquellos relacionados con las nuevas tecnologías como pueden ser la distribución de pornografía infantil, el phising o el child grooming sino también respecto a comportamientos delictivos más tradicionales en los que la geolocalización de un teléfono móvil o la determinación de la dirección IP, puede contribuir a la explicación del hecho delictivo (Lapuerta Irigoyen, 2017).

2.4.2 Tipos de Ciberdelitos

Dentro del campo del Cibercrimen, se destacan diversas categorías que abarcan desde ataques individuales hasta amenazas contra los gobiernos como señala el artículo de PandaSecurity (2023). Además, se distinguen diversos tipos de Cibercrímenes y técnicas que según el método que se utilice, o el nivel de dificultad pertenecerán a una categoría u otra.

- **Ataques DDoS:** Se utilizan para hacer que un servicio en línea no esté disponible y para que la red se caiga con el tráfico de diversas fuentes. Las grandes redes de dispositivos infectados, conocidas como Botnets, se crean introduciendo malware en los ordenadores de los usuarios. Una vez que la red está caída, el pirata informático hackea el sistema.
- **Botnets:** Los botnets son redes de ordenadores infectados, controlados de forma externa por hackers remoto. Estos envían spam o atacan a otros ordenadores a través de esos botnets. También pueden utilizarse para actuar como malware y realizar tareas maliciosas.

- **Robo de identidad:** Este ciberdelito se produce cuando un delincuente accede a datos personales de un usuario para robar fondos, acceder a información confidencial o participar en un fraude fiscal o contra un seguro médico. También pueden abrir una cuenta de teléfono/internet en su nombre, utilizar su identidad para planificar una actividad delictiva o reclamar subvenciones gubernamentales en su nombre. Pueden hacerlo averiguando las contraseñas de los usuarios a través de hackeos, recuperando información personal de las redes sociales o enviando correos electrónicos de phishing.

- **Ciberacoso:** Este tipo de ciberdelito implica un acoso en línea en el que el usuario es sometido a una variedad de mensajes y correos electrónicos. Los ciberacosadores suelen utilizar las redes sociales o los sitios web para intimidar al usuario. Normalmente, el ciberacosador conoce a su víctima y le hace sentir miedo o preocupación por su seguridad. El ciberbullying y el child grooming o ciberacoso sexual a menores son algunos de los ejemplos de Ciberacoso.

- **Ingeniería social:** La ingeniería social implica que los delincuentes se pongan en contacto directo con la víctima, normalmente por teléfono o correo electrónico. Buscan ganarse su confianza y suelen hacerse pasar por un agente de atención al cliente para conseguir la información que necesitan: a menudo se trata de una contraseña, la empresa para la que trabaja o datos bancarios. En otros casos, los **ciberdelincuentes** averiguarán todo lo que puedan sobre la víctima en Internet y luego intentarán añadirla como contacto en las cuentas sociales. Una vez que acceden a una cuenta, pueden vender su información o asegurar cuentas en su nombre.

- **Phishing:** Este tipo de ciberataques consiste en que los piratas informáticos envían archivos adjuntos de correo electrónico o URLs a los usuarios para acceder a sus cuentas o a su equipo. Los **ciberdelincuentes** que usan este método están cada vez más consolidados y muchos de estos correos electrónicos esquivan los filtros antispam. Los usuarios son manipulados con correos electrónicos en los que se afirma que deben cambiar su contraseña o actualizar sus datos.

- **PUPs:** Los PUPS o Programas Potencialmente No Deseados (Potentially Unwanted Programs) son una amenaza menos grave que otros **ciberdelitos**, pero no dejan de ser un tipo de malware. Desinstalan el software necesario en el

sistema, incluidos los motores de búsqueda y las aplicaciones predefinidas. Se debe de instalar un software antivirus para evitar descargas maliciosas.

- **Contenido prohibido/ilegal:** Este ciberdelito consiste en que los delincuentes comparten y distribuyen contenidos inapropiados que pueden considerarse ofensivos y susceptibles para las personas. Los contenidos ofensivos pueden incluir, entre otros, actividad sexual, vídeos con violencia intensa o de actividades delictivas. Los contenidos ilegales incluyen materiales como el terrorismo y material de explotación infantil, como la pornografía infantil.
- **Estafas online:** Suelen presentarse en forma de anuncios o correos electrónicos de spam, que incluyen promesas de recompensas u ofertas, con cantidades de dinero poco realistas. Las estafas incluyen ofertas tentadoras, que son demasiado buenas para ser verdad y que, al hacer clic en ellas, pueden provocar la instalación de malware.
- **Kits de exploits:** Los kits de exploits necesitan una vulnerabilidad (un error en el código de un software) para obtener el control del ordenador de un usuario. Se trata de herramientas ya preparadas que los delincuentes pueden comprar en línea y utilizar contra cualquiera que tenga un ordenador. Los kits de exploits se actualizan regularmente de forma similar al software normal y están disponibles en los foros de hacking de la web oscura.

Entre todos ellos, los más comunes dentro del entorno de las redes sociales, destacan el fraude, el chantaje, el phishing, los virus informáticos y la publicidad engañosa, suplantando la identidad de los usuarios, difundiendo información falsa, utilizando libremente sus datos personales, estafando, etc.

2.5 Redes sociales

En la antigüedad, los humanos se comunicaban principalmente a través de métodos básicos, como el habla, los gestos o la escritura, y los distintos lugares físicos donde se llevaba a cabo esta comunicación. Estos medios limitaban la velocidad y el alcance de la comunicación, dando lugar a interacciones cara a cara. Sin embargo, en el mundo contemporáneo, la comunicación ha evolucionado experimentando un gran cambio gracias a la llegada de las redes sociales. Estas plataformas han redefinido la forma en la que hoy en día se relaciona la gente, la manera de interactuar y de transmitir información.

Las redes sociales, surgieron como plataformas para facilitar la comunicación y el intercambio de información entre individuos de diferentes lugares geográficos. Surgieron en 1978 con la creación del Computerized Bulletin Board System (CBBS) por Ward Christensen y Randy Suess, dos amigos incomunicados crearon en cuatro semanas un programa informático que les permitían comunicarse por una vía telefónica de transmisión de datos (Alto nivel, 2013). Más adelante, a finales del año 1997, fue diseñada en Internet, la primera red social SixDegrees (SeisGrados). Fue creada por Andrew Winreich y desarrollada por la empresa Macroview, dentro de esta aplicación se daba la oportunidad de generar un perfil y crear una lista de amigos, además de poder intercambiar mensajes entre ellos. Desde entonces, se han ido diseñando y generando distinto tipos de plataformas sociales y gracias al avance tecnológico siguen evolucionando constantemente. (Andrade Alarcón, 2021).

2.5.1 Tipos de redes sociales

Según Ureña et al. (2011) dentro de las redes sociales se pueden identificar dos categorías distintas basadas en la forma en la que los usuarios interactúan entre sí: las redes sociales de comunicación directa y las redes de comunicación indirecta.

Redes sociales directas: "Son redes sociales directas aquellas cuyos servicios prestados a través de Internet en los que existe una colaboración entre grupos de personas que comparten intereses en común y que, interactuando entre sí en igualdad de condiciones, pueden controlar la información que comparten. Los usuarios de este tipo de redes sociales crean perfiles a través de los cuales gestionan su información personal y la relación con otros usuarios. El acceso a la información contenida en los perfiles suele estar condicionada por el grado de privacidad que dichos usuarios establezcan para los mismos" (Ureña et al., 2011, p.13).

Redes sociales indirectas: "Son redes sociales indirectas aquellas cuyos servicios prestados a través de Internet cuentan con usuarios que no suelen disponer de un perfil visible para todos existiendo un individuo o grupo que controla y dirige la información o las discusiones en torno a un tema concreto. Resulta especialmente relevante aclarar que este tipo concreto de redes sociales son las precursoras de las más recientes redes sociales directas desarrolladas dentro del nuevo marco de la Red 2.0**"** (Ureña et al., 2011, p.16).

Este tipo de distinción permite comprender de una mejor manera la dinámica de las redes sociales y como los usuarios se relacionan dentro de ellas. Del mismo modo, nos permite entender el riesgo que puede suponer una mala gestión de comunicación entre los usuarios, y la importancia que tiene una buena aplicación de la privacidad, seguridad y la relación de construcción virtual que se genera entre los navegantes.

Asi mismo, se puede elaborar una distinción de las redes sociales más utilizadas y relacionarlas con la clasificación de plataformas según la forma de comunicación de los usuarios que se ha realizado anteriormente. Estas redes permiten a los usuarios interactuar entre sí de manera inmediata y sin intermediarios, a través de funciones como comentarios, mensajes directos o chats grupales. Hay cuatro plataformas, que destacan notablemente dentro de la categoría de "redes sociales directas".

Tabla1: "Redes sociales directas"

Red social	Función	Usuarios mensuales activos (2023)
WhatsApp	Mensajería instantánea que permite a los usuarios mandar texto, imágenes, videos, documentos, etc.	2.900 millones
Instagram	Intercambio de fotos y videos, creación de perfiles, y envío de mensajes directos entre usuarios.	1.336 millones
Facebook	Creación de perfiles, conexión con amigos y familiares, seguimiento de empresas y organizaciones, transmisión en vivo, etc.	2.960 millones
Twitter	Publicación de mensajes cortos de hasta 280 caracteres denominados "tweets".	354 millones

Fuente: Tabla de elaboración propia a través de datos de Google

Por otro lado, existen diversas plataformas sociales, que destacan dentro de la categoría de "redes sociales indirectas". La comunicación entre los usuarios tiende a ser más estructurada y mediada por la plataforma. Dentro de este tipo de plataformas se pueden clasificar en foros y blogs.

Tabla 2: “Redes sociales indirectas”

Red social	Función	Usuarios mensuales activos (2023)
Linkedln	Orientada al ámbito profesional y laboral. Los usuarios crean perfiles profesionales sobre su experiencia laboral	746 millones
Blogs	Ofrecen información sobre un tema y opiniones personales.	
Foros	Expertos dentro de un área de conocimientos. Valoraciones y opiniones de expertos que responden a todo tipo de preguntas planteadas por los usuarios.	

Fuente: Tabla de elaboración propia a través de datos de Google

2.5.2 Ventajas y desventajas del uso de redes sociales

Estos tipos de redes sociales han ido abriéndose camino en un mundo de desconocimiento donde la veracidad de la información era a menudo cuestionada por los distintos medios de comunicación que había anteriormente. La desinformación se extendía rápidamente y la percepción de la información era moldeada según la narrativa de la gente. Múltiples perspectivas de opinión podían originar contenido incompleto y engañoso para la ciudadanía. Las redes sociales han venido para quedarse ofreciendo una ventana sin precedentes a la diversidad de opiniones, experiencias y conocimientos que permiten que la información sea veraz. Las redes sociales no solo comparten noticias de lo que ocurre en el día a día, ayudan a comunicarse y permiten establecer un contacto constante con la persona que se quiera.

No obstante, como contaba Gallardo Lobato (2022) ni todo es tan bueno, ni todo es tan malo. Los aspectos positivos de las redes sociales están relacionados con la conectividad que aportan con cualquier parte del mundo, a cualquier hora y en todo momento. Ahora bien, se tiene que hacer un buen uso de estas plataformas, su desventaja está relacionada con la manera en la que se utilizan estas aplicaciones. Lo principal, es tener control, realizar un uso moderado y evitar que absorban la totalidad del tiempo de las personas, pues podrían afectar de manera negativa a la salud mental de las mismas.

Por lo que es necesario explorar los beneficios que aportan como los desafíos que imponen a la sociedad.

Las redes sociales permiten mantener conexión con el mundo entero, eliminando la distancia y facilitando la comunicación con personas sin nunca restricción. Permiten mantener relaciones con conocidos, amigos o familiares que residen en otros países o ciudades, promoviendo la cercanía y continuidad de las relaciones interpersonales. Además, de este modo las personas interactúan y se conocen, una buena forma de hacer nuevos contactos que comparten intereses en común.

Estas plataformas también brindan acceso a una amplia gama de información que de otra manera sería difícil de obtener. A través de ellas, las personas se mantienen informadas sobre noticias, publicaciones de ofertas de trabajo y eventos relevantes tanto a nivel local como global. Además, muchas empresas utilizan las redes sociales como canales de comunicación para proporcionar actualizaciones sobre sus productos o servicios, lo que permite estar al tanto de las últimas novedades en el mercado. Con la creación de comunidades digitales y estrategias de marketing, las empresas pueden llegar a nuevos clientes, aumentar sus ventas y reforzar su presencia en el mercado (Gómez, 2013).

Otro aspecto destacado de las redes sociales es su capacidad para proporcionar entretenimiento y diversión. Desde la visualización de vídeos hasta la participación en concursos, estas plataformas ofrecen una amplia gama de opciones para disfrutar del tiempo libre y compartir momentos de diversión con amigos y seguidores, para todos los gustos y edades, sin necesidad de muchos recursos técnicos, simplemente un dispositivo que tenga acceso a Internet (Mejía Llano 2023).

Además de ser una fuente de entretenimiento, las redes sociales también son una buena herramienta educativa. A través de plataformas virtuales se ofrece apoyo a la docencia con el intento de mejorar la formación de los estudiantes. Favorecen el trabajo en grupo y comunidad, los alumnos pueden acceder a información y recursos educativos, participar en discusiones académicas y aprender nuevas habilidades o conocimientos. Las plataformas de aprendizaje virtual permiten ampliar las competencias de los jóvenes y su desarrollo personal (Muñoz Prieto et al., 2013).

Pero no todo es bueno, los seres humanos cometen errores continuamente en el uso de las redes sociales. Al publicar fotos, pensamientos y datos personales, se corre el

riesgo de comprometer la privacidad de uno mismo y la de los demás contactos, si no se es cuidadoso con la configuración de privacidad y la selección de nuestras conexiones. Además, las redes sociales abren la puerta al ciberacoso y otras formas de **ciberdelitos**, como por ejemplo los fraudes, en los que se aprovechan los "hackers". El anonimato que ofrecen estas plataformas puede ser explotado por individuos malintencionados, que buscan robar y luego descubrir los datos bancarios, contraseñas y números de cuentas de los usuarios para obtener beneficios propios mediante transacciones electrónicas. Lo que puede resultar en experiencias traumáticas y perjudiciales para quienes son víctimas de este tipo de comportamiento (ESPE, s.f.).

2.5.3 Impacto y riesgos producidos en la sociedad

En general las redes sociales han impactado en la sociedad tanto positiva como negativamente, el riesgo principal que supone estar conectado una gran cantidad de tiempo a un dispositivo electrónico, afecta de manera negativa, pudiendo provocar una adicción al uso de las tecnologías junto con una falta de autocontrol, un daño en las relaciones personales y un riesgo en la salud mental de las personas. El mayor impacto se genera en jóvenes de 16 a 24 años, periodo significativo para el desarrollo emocional y psicosocial. Además, han nacido en la época álgida de las tecnologías, no conocen lo que es un mundo sin las mismas.

La obsesión por la aprobación social es un riesgo potencial, constantemente se busca obtener likes, comentarios y compartidos en publicaciones de manera pública. Esta búsqueda de validación puede llevar a una disminución de la autoestima y una dependencia emocional de la retroalimentación positiva de los demás, además de ofrecer la libre circulación de la información ayudando de forma inconsciente a que los **ciberdelincuentes** la obtengan de manera más fácil exponiéndose a posibles estafas, fraudes o robos de identidad, violando la privacidad y realizando un mal uso de su seguridad.

Los riesgos asociados con la privacidad son una gran preocupación significativa de los usuarios en el contexto de redes sociales. La información privada puede ser divulgada y publicada fácilmente. Datos que van desde la ubicación geográfica, edad y dirección, hasta información más delicada como números de tarjetas de crédito, números de teléfono, etc., pueden ser utilizados de manera. El robo de información puede ser

ejecutado por los hackers o usuarios que tengan la intención de suplantar la identidad de otros usuarios haciéndose pasar por ellos. Además, existen riesgos relacionados con ventas fraudulentas, solicitudes de donaciones u ofertas comerciales engañosas. La exposición de contenido íntimo como fotografías de desnudos o mensajes eróticos, que se comparten de manera privada, pueden ser filtrados o vendidos en sitios web de pornografía sin el consentimiento del usuario, quien confiaba en la privacidad de la comunicación directa (Editorial Etecé, 2021).

Organizar una cita con un individuo desconocido o realizar transacciones económicas de manera informal representa una conducta de alto riesgo de seguridad dentro de las plataformas sociales. En el caso de los menores, se encuentran en una situación vulnerable, dado que pueden percibir las redes sociales como espacios donde la supervisión parental es inexistente lo que les expone a formar relaciones con desconocidos o el acceso a contenido ilegal que pueden no estar preparados para manejar de manera adecuada por sí mismos. Además, las redes sociales se encuentran cargadas de amenazas como malware, **ciberdelincuentes** que buscan atentar contra la seguridad del usuario y su falta de preocupación (Editorial Etecé, 2021).

3 ESTRATEGIAS Y MEDIDAS DE PROTECCION DE LA PRIVACIDAD Y SEGURIDAD DE LOS USUARIOS

3.1 Desafíos actuales en la protección de la privacidad en redes sociales

Según un estudio publicado en la Revista Summa (2023) se identificaron cinco desafíos principales que enfrentan los usuarios en las plataformas de redes sociales:

La recopilación y uso de datos personales: Las redes sociales reúnen grandes cifras de datos personales de sus usuarios, incluyendo intereses y actividades. El reto reside en la forma en que los datos son utilizados y compartidos, asi como en garantizar el consentimiento adecuado por parte de los usuarios.

Las configuraciones de privacidad y opciones complejas: Las configuraciones de privacidad en las redes sociales son complejas y las opciones pueden resultar confusas para los usuarios, lo que dificulta su comprensión y control sobre quien puede acceder a su información personal.

Compartir información sin consentimiento: Los usuarios etiquetan o comparten información sobre otras personas sin su consentimiento, comprometiendo su privacidad. Se tiene que saber encontrar un equilibrio entre la libertad de expresión y el respeto a la privacidad de los individuos.

El Ciberacoso y abuso en línea: Las redes sociales han aumentado y facilitado el problema del ciberacoso y el abuso en línea. Los usuarios pueden ser objeto de hostigamiento, intimidación, difamación. Estas acciones afectan la privacidad y seguridad de los usuarios dentro del **ciberespacio**.

Las brechas de seguridad y filtraciones de datos: Las redes sociales son objeto de brechas de seguridad y filtraciones de datos, difundiendo información personal no autorizada. Pues supone un riesgo para la privacidad de los usuarios y consecuencias negativas.

En este contexto, la **ciberseguridad** trabaja hacia soluciones que protejan los datos personales y brinden a los usuarios un mayor control sobre su información, desarrollando medidas de seguridad, creando una gestión de privacidad más accesible y fácil de leer, y buscando la colaboración entre los sectores públicos y privados, de este modo establecer regulaciones efectivas en la protección de datos en línea.

3.2 Medidas utilizadas para la disminución de la Cibercriminalidad

Los gobiernos y empresas trabajan continuamente en un espacio digital cada vez más complejo. Dentro del **ciberespacio** la **cibercriminalidad** representa una amenaza desafiando los conocimientos tradicionales de seguridad. Las redes sociales como fuente de comunicación e interacción se convierten en un campo de batalla desarrollando conflictos de privacidad y seguridad, dando lugar a una serie de desafíos en términos de protección de datos personales, prevención de **ciberdelitos** y conservación de la integridad digital de los usuarios. Los gobiernos, las empresas y la sociedad luchan adoptando una serie de herramientas y medidas con el objetivo de disminuir los riesgos asociados con el uso de las redes sociales, y fomentar un entorno más seguro y confiable.

A pesar de que el rápido desarrollo de las Tecnologías de la información y la Comunicación (TIC) ha impulsado el progreso económico y social, también ha incrementado la dependencia de Internet, lo que conlleva mayores riesgos y vulnerabilidades, asi como nuevas oportunidades para actividades delictivas. Los gobiernos construyen marcos regulatorios eficaces y fomentan la cooperación internacional en materia de **ciberseguridad.** Al mismo tiempo, las empresas de tecnología desarrollan herramientas y políticas de privacidad más estrictas para la protección de los usuarios.

Según INTERPOL (2021) una estrategia de lucha contra la **ciberdelincuencia** se tiene que juntar con otra estrategia de **ciberseguridad** para garantizar la efectividad de las medidas utilizadas. Una estrategia a nivel nacional contra la **ciberdelincuencia** fortalece la capacidad global de su país para disminuir los **ciberdelitos** coordinándose con las prácticas de ejecuciones internacionales.

En diciembre de 2020, la Comisión Europea y el Servicio Europeo de Acción Exterior (SEAE) introdujeron una nueva Estrategia de **ciberseguridad** de la UE con la intención de reforzar la resistencia de Europa ante las amenazas de los **ciberdelincuentes**. Su objetivo es asegurar que todos los ciudadanos y empresas puedan aprovecharse de los servicios y herramientas digitales de manera segura. El 22 de marzo de 2021, el Consejo adoptó unas conclusiones sobre la Estrategia de **ciberseguridad** en las que destacó que la **ciberseguridad** es importante para construir una Europa resistente y digital. Los ministros de la Unión Europea establecen como objetivo principal conseguir una autonomía estratégica, ampliando la capacidad de la toma de decisiones autónomas,

fortaleciendo asi el liderazgo digital y las capacidades estratégicas de la UE (Consejo Europeo, 2024).

En marzo de 2021 el Plan Estratégico contra la **cibercriminalidad** fue aprobado en España por el Ministerio del Interior con el objetivo de reforzar las capacidades de los órganos ministeriales para detectar, prevenir y perseguir actividades delictivas en el ámbito del **ciberespacio**. Este plan busca proporcionar un impulso operativo y técnico efectivo que garantice la protección de los derechos y libertades de los ciudadanos, asi como la seguridad pública.

Según el Ministerio del Interior (2022), el plan estratégico diseñado por la Secretaría de Estado de Seguridad pone el foco "en la prevención; en la cooperación entre las diferentes Fuerzas y Cuerpos de Seguridad del Estado (FCSE) y los operadores jurídicos; en la dotación de capacidades suficientes y adecuadas para articular respuestas adaptadas a las diferentes modalidades delictivas; en la colaboración con la industria y los operadores relevantes en materia de **ciberseguridad** en el sector público y privado; y en el respeto escrupuloso a la libertad, a la privacidad y demás derechos fundamentales".

3.3 Educación y concienciación dentro de la sociedad

No solo son los gobiernos y las empresas los que juegan un papel fundamental dentro de este contexto, es la sociedad la que recibe la educación y concienciación sobre la importancia de la privacidad y la seguridad que supone navegar por las redes sociales y los que tienen la responsabilidad de cumplir o no con las normas. Comprender los riesgos y desafíos protege la información personal de los individuos, por lo tanto, es esencial promover programas educativos que promuevan un pensamiento crítico, una buena responsabilidad y el respeto por la privacidad, asegurándose un entorno virtual más seguro.

Los riesgos y desafíos que invaden la privacidad de los usuarios dañando su seguridad, fomentan una mayor alfabetización digital y conciencia en la sociedad, adquiriendo habilidades que promuevan el buen uso de las redes sociales. La educación y concienciación implican tanto valores éticos como la capacidad para evaluar la veracidad de la información en la red y resistir la manipulación o el abuso de datos personales. Se desarrollan programas educativos adaptados a diferentes grupos de edad y contexto culturales, abordando la privacidad, la detección de fraudes y estafas, y la

promoción de comportamientos responsables en las plataformas sociales (Grupo de Trabajo de Tecnologías del Aprendizaje [GTTA], 2022).

Las personas utilizan continuamente las redes sociales, expandiendo su círculo social, sin comprender el valor que tiene la información difundida ni los posibles riesgos asociados a la privacidad y seguridad en la red. El mal uso de las plataformas y la divulgación de datos privados no autorizados conducen a consecuencias negativas en la vida de las personas, por lo que la educación y concienciación sobre la protección de datos son fundamentales para prevenir todo tipo de ciberataques que se produzcan dentro del **ciberespacio**. No obstante, la percepción de privacidad varía según el tipo de usuario, son muchos los que no muestran preocupación y simplemente se dejan guiar por lo hace el resto, hay estudios que lo afirman "cuantos más amigos con perfil privado tenga un adolescente, mayor será la disponibilidad del adolescente por mantener su propio perfil privado" (Argente et al., 2017).

La educación en **ciberseguridad** es importante para todas las edades, dado que las personas se enfrentan a los riesgos de las redes todos los días. Los adultos necesitan estar enterados de las últimas amenazas del **ciberespacio** y adoptar medidas de seguridad para salvaguardar sus datos personales y financieros. Por otro lado, los jóvenes están inmersos en un mundo digital y necesitan ser educados desde pequeños con el fin de aprender un uso responsable y seguro de las redes sociales. Los usuarios deben entender las consecuencias a largo plazo que pueden tener si difunden cualquier tipo de información indebida. Se debe de educar a los usuarios para que sepan evaluar la confiabilidad de las plataformas sociales, antes de compartir sus datos confidenciales, asi como la manera de evitar las técnicas maliciosas como el phishing o el malware que utilizan los **ciberdelincuentes**, mediante el uso de sofware antivirus (Herrero, 2023).

En cuanto a las políticas de privacidad, los usuarios deben comprender que información recopilan, el objetivo que tienen y como protegen esa información. Cada plataforma en línea establece sus propias reglas sobre el manejo de datos personales, como menciona el Observatorio de la Infancia y El Instituto Nacional de **ciberseguridad** (2019). Además, en ellas se incluyen los procedimientos a seguir para ejercer los derechos del usuario, denominados ARCO "(acceso, rectificación, cancelación y oposición, ampliados con el Reglamento General de Protección de Datos con la limitación del tratamiento, la portabilidad de los datos y el no ser objeto de decisiones individualizadas automatizadas)" que aseguran que el usuario tenga control sobre su información personal.

Por último, es importante que el usuario esté informado y capacitado para enfrentar situaciones como la suplantación de identidad y la publicación de contenido sin su consentimiento. Los usuarios tienen que ser conscientes de sus derechos y saber como proteger su privacidad, fortaleciendo su capacidad para actuar ante cualquier violación digital. Según las recomendaciones de Justizia.eus (2022) en el caso de suplantación de la identidad, el usuario debe de contactar directamente con la plataforma para solicitar la eliminación del perfil falso, y en los casos de publicación no consentida de contenido sensible o violento, se tendrá que utilizar el Canal Prioritario de la AEPD para denunciar de forma rápida y gratuita.

4 METODOLOGÍA

La metodología llevada a cabo en este trabajo de fin de grado ha consistido en la realización de un análisis profundo sobre la percepción y seguridad de los usuarios en su uso de las redes sociales. Su elaboración se ha basado en un enfoque de estudio mixto, de forma tanto cualitativa como cuantitativa.

4.1 Revisión bibliográfica

En primer lugar, como se ha podido observar con anterioridad, se ha realizado una búsqueda bibliográfica profunda sobre los distintos aspectos relevantes sobre la materia a tratar. Para dicha revisión bibliográfica se han consultado diversas fuentes informáticas para llevar a cabo la investigación, asi como numerosos artículos publicados en la red, páginas web, informes, documentos o estudios especializados en la materia a tratar. Se han realizado diversas búsquedas a partir de palabras clave como: "Privacidad y seguridad en la red", "**ciberseguridad**", "**cibercriminología**", "Redes Sociales" entre otras. Como resultado de dicha búsqueda se obtuvieron los diversos títulos del trabajo, que han sido de gran utilidad para la elaboración del marco teórico. La búsqueda, se ha realizado a través de Internet con la herramienta de Google y a partir de las palabras clave mencionadas anteriormente, se han tenido acceso a una gran cantidad de artículos, libros, blogs o páginas webs que hablan sobre el tema. La variedad de información obtenida en las distintas fuentes constata la ide de la importancia de la privacidad y seguridad de los usuarios en el uso de las redes sociales.

En el apartado final de la bibliografía del presente Trabajo Fin de Grado se detallan todas las fuentes de las que se han obtenido la información.

4.2 La encuesta

Teniendo en cuenta toda la bibliografía y el objetivo principal del Tfg, a través de un enfoque cuantitativo se realiza una encuesta como técnica de recogida de datos estadísticos. Mediante la construcción de una serie de preguntas, se ha podido obtener toda la información necesaria acerca de la percepción de las personas sobre su privacidad y seguridad al navegar por las redes sociales.

Para la elaboración de la investigación, se diseñó un cuestionario online estructurado utilizando la plataforma de Google Forms, distribuyéndolo a través de uno de los principales canales de comunicación, en su caso WhatsApp, en el periodo del mes

de marzo de 2024. Para dicha investigación, ha sido de relevancia obtener datos personales como la edad y el sexo de los encuestados, para asi poder cruzar dicha información con el resto de los resultados en las diferentes preguntas y poder realizar su comentario.

Como se observa a continuación en ambas tablas, fueron un total de 67 mujeres las que contestaron a la encuesta y 33 hombres, haciendo un total de la muestra de N=100 encuestados. Entre los cuales se muestra una gran variedad de edades, que van desde los menores de edad, hasta las personas de más de 65 años.

Tabla 1. Sexo de las personas encuestadas

		Recuento	% de N columnas
sexo	Femenino	67	67,0%
	Masculino	33	33,0%

Fuente: Elaboración propia, a través de los datos estadísticos obtenidos en la herramienta del SPSS de la encuesta realizada (Anexo1).

Tabla 2. Edad de las personas encuestadas

			sexo		
			Femenino	Masculino	Total
¿Cuántos años tiene?	Entre 18-25 años	Recuento	9	10	19
		% dentro de sexo	13,4%	30,3%	19,0%
	Entre 26-40 años	Recuento	16	5	21
		% dentro de sexo	23,9%	15,2%	21,0%
	Entre 41-50 años	Recuento	11	4	15
		% dentro de sexo	16,4%	12,1%	15,0%
	entre 51-65 años	Recuento	12	6	18
		% dentro de sexo	17,9%	18,2%	18,0%

	Más de 65 años	Recuento	6	6	12
		% dentro de sexo	9,0%	18,2%	12,0%
	Menor de edad	Recuento	13	2	15
		% dentro de sexo	19,4%	6,1%	15,0%
Total		Recuento	67	33	100
		% dentro de sexo	100,0%	100,0%	100,0%

Fuente: Elaboración propia, a través de los datos estadísticos obtenidos en la herramienta del SPSS de la encuesta realizada (Anexo1).

Los datos de estas dos tablas, junto con el resto de las preguntas del cuestionario, han sido analizados mediante la herramienta IBM SPSS Statistic, a partir de la función de análisis de datos descriptivos, tablas cruzadas personalizadas. Dicha encuesta, recogía un total de 16 preguntas, entre su mayoría cerradas con opción a seleccionar una sola respuesta, excluyendo dos de ellas en las que la persona podía seleccionar más de una opción.

A modo de aclaración e introducción se ha de destacar que, desde el comienzo de la encuesta, se explicó el objetivo de la misma y se informó del anonimato del encuestado. Todas las respuestas se recogieron de forma anónima Conforme a Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, la cual tiene por objeto la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos.

Por tanto, todo el material que se recoge a continuación se ha obtenido mediante las distintas herramientas expuestas que han sido mencionadas anteriormente. De manera coherente y de forma ordenada, se podrá observar cómo toda la información ha quedado clasificada y clarificada. Este enfoque metodológico mixto ha permitido obtener una clara comprensión sobre la percepción que tienen los usuarios sobre su privacidad y seguridad en las redes sociales, asi como la resolución de los objetivos.

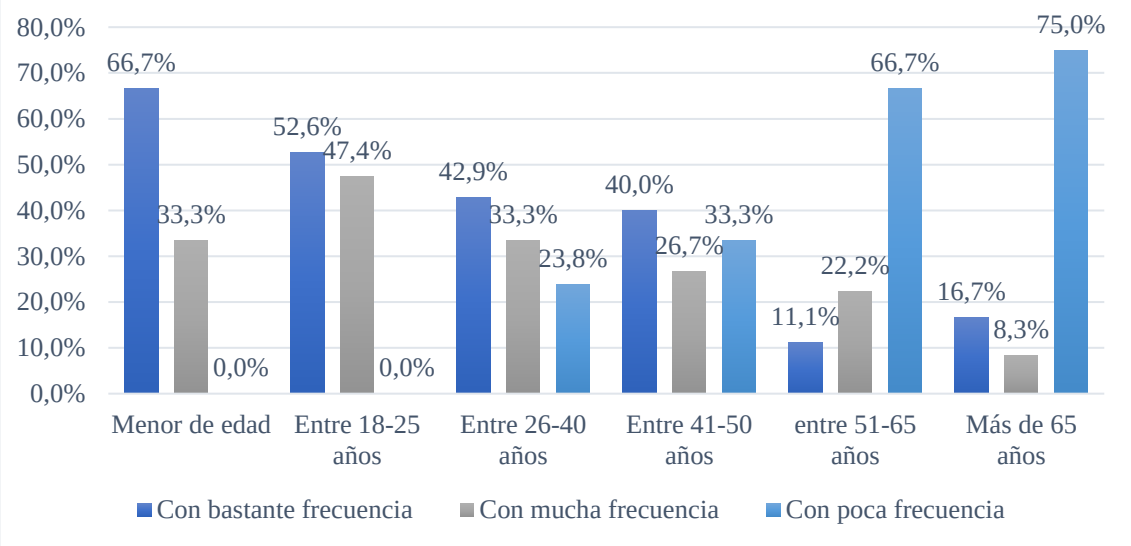
5 ANÁLISIS DE RESULTADOS

5.1 Análisis descriptivo

En la realización de la encuesta se han llevado a cabo distintos tipos de preguntas, en las cuales se han obtenido una seria de respuestas por parte de los encuestados. Los datos obtenidos se han agrupado en diversas tablas, cruzando dos tipos de variables distintas, el sexo y la edad. Las distintas tablas obtenidas, se han representado en diversos gráficos, para asi poder visualizar los resultados de manera gráfica y efectiva. La descripción estadística, aportará información y con ello se podrá establecer la veracidad de las hipótesis acerca de la percepción de la privacidad y seguridad que tienen los usuarios en su uso de las redes sociales.

5.1.1 Gráfico de datos de la pregunta número 1 (Anexo 1)

"¿Con qué frecuencia utiliza las redes sociales?"



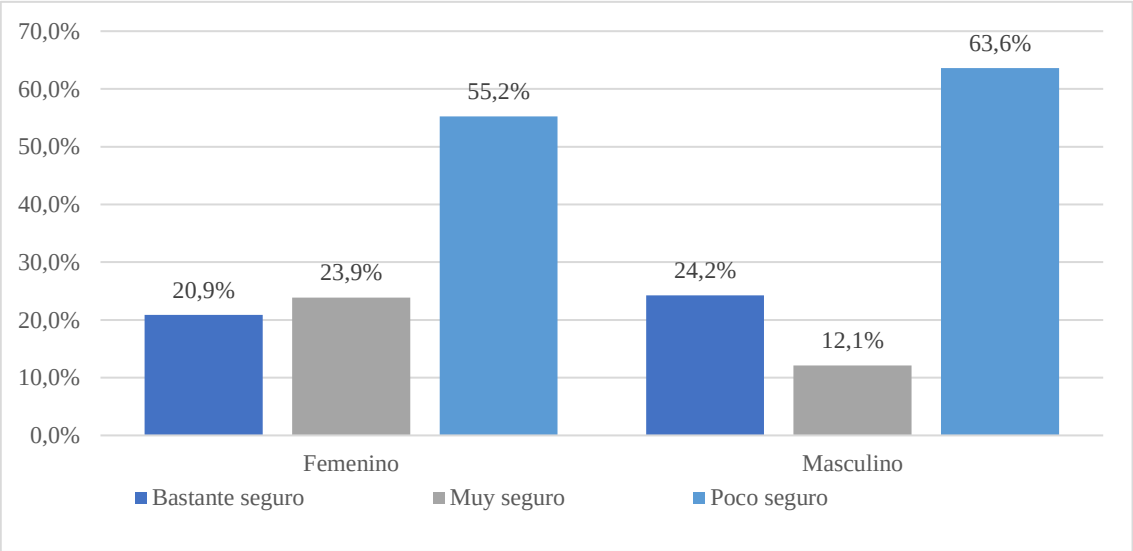
Fuente: Elaboración propia a partir de Tabla cruzada 1 (Anexo 2)

En la gráfica se muestra la frecuencia con la que las personas usan las redes sociales según el grupo de edad. Entre las personas más jóvenes se observa un alto porcentaje de la frecuencia de uso de redes sociales, siendo la opción de "con bastante frecuencia" la más seleccionada, con un 66,7% en los menores de edad, seguido de un 52,6% entre los que tienen 18 y 25 años. Un número menor de los encuestados utiliza las redes con poca frecuencia, entre los que están las personas mayores de 65 años con un 75%, seguidos de las personas que tienen entre 51 y 65 años con un 66,7%.

Con la descripción del gráfico, se afirma como las redes sociales han transformado la comunicación en la edad moderna, y la adaptación positiva que han tenido los ciudadanos ante las nuevas tecnologías, donde las redes sociales permiten una interacción más rápida y globalizada entre los individuos de diferentes partes del mundo, lo que facilita el intercambio de información entre los usuarios y el aumento de uso de estas. Aun asi, las personas jóvenes tienden a utilizar las redes sociales con mayor frecuencia que la gente adulta.

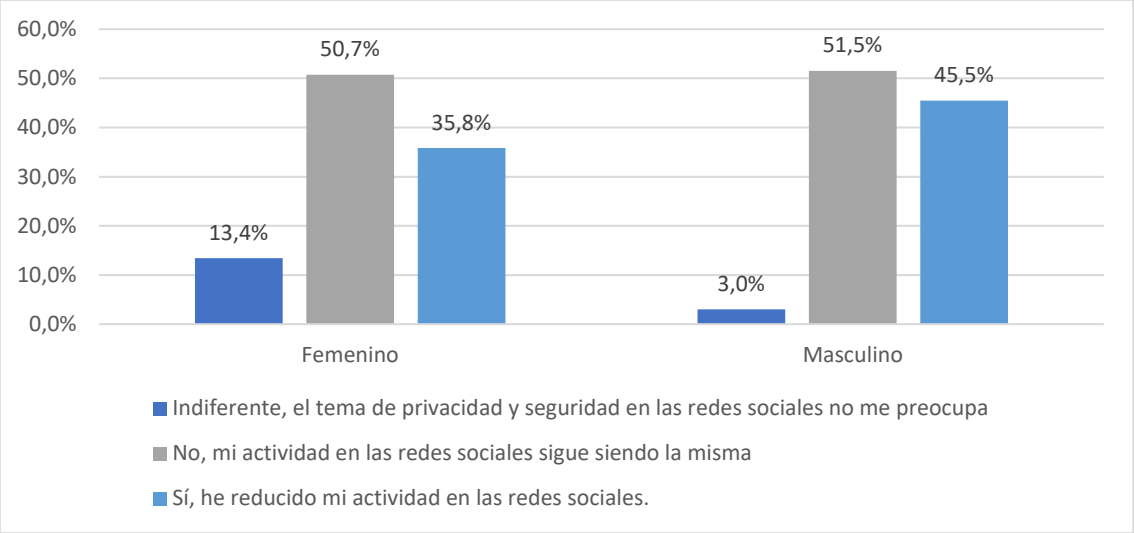
5.1.2 Gráficos de datos de la pregunta número 2 y 11 (Anexo 1)

"¿Como de seguro se siente cuando navegas por las redes sociales?



Fuente: Elaboración propia a partir de Tabla cruzada 2 (Anexo 2)

"¿Ha cambiado sus hábitos de uso de redes sociales debido a preocupaciones sobre privacidad y seguridad?"



Fuente: Elaboración propia a partir de Tabla cruzada 11 (Anexo 2)

Los gráficos tratan sobre la percepción de seguridad en las redes sociales y los cambios en los hábitos de uso de las plataformas debido a preocupaciones sobre la privacidad y seguridad. Comparando ambas tablas se pueden identificar algunas contradicciones.

En el gráfico de la de la *Tabla cruzada 2,* se observa como una parte significativa de los encuestados se sienten poco seguros al navegar por las redes sociales, en concreto un 55,2% de las mujeres y un 63,6% de los hombres. Sin embargo, en el gráfico de la *Tabla cruzada 11,* la mayoría de los encuestados indican que su actividad en las redes sociales sigue siendo la misma, con un porcentaje de 50,7% siendo femenino y un 51,5% siendo masculino. Esto supone una posible discrepancia entre la percepción de seguridad y la respuesta real en términos de cambios de comportamiento.

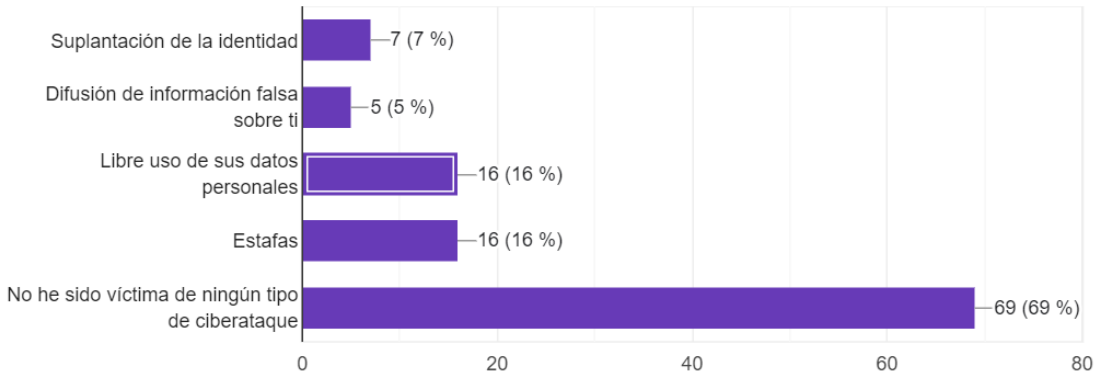
En el gráfico de la *Tabla cruzada 11*, también se observa un mayor porcentaje de hombres con un 45,5% que han reducido su actividad en las redes sociales en comparación con un 35,8% de las mujeres que han seleccionado esta opción. En esta ocasión, los hombres podrían estar más inclinados a tomar medidas concretas en respuesta a estas preocupaciones.

Además, en la *Tabla cruzada 11* se observa como una minoría de los encuestados, de tan solo el 10% indican, lo que contrasta con la percepción generalizada de sentirse poco seguro al navegar por las redes sociales como se muestra en el gráfico de la *Tabla cruzada 2.*

Aunque los usuarios puedan sentirse inseguros, no necesariamente modifican su comportamiento en las redes sociales en respuesta a estas preocupaciones. La **ciberseguridad** destaca la necesidad de medidas de seguridad para salvaguardar la privacidad de los usuarios en las plataformas sociales. Pero, aunque los usuarios puedan ser conscientes de los riesgos que puede suponer, es posible que no se sientan motivados para cambiar sus hábitos de uso de las redes sociales.

5.1.3 Gráfico de datos de la pregunta número 3 (Anexo 1)

"¿Ha sido víctima de alguno de estos ciberdelitos o cualquier otro ataque que haya violado su privacidad en una red social? (Puede seleccionar más de una opción)"



Fuente: Elaboración por Google forms a partir de Pregunta 16 de la encuesta

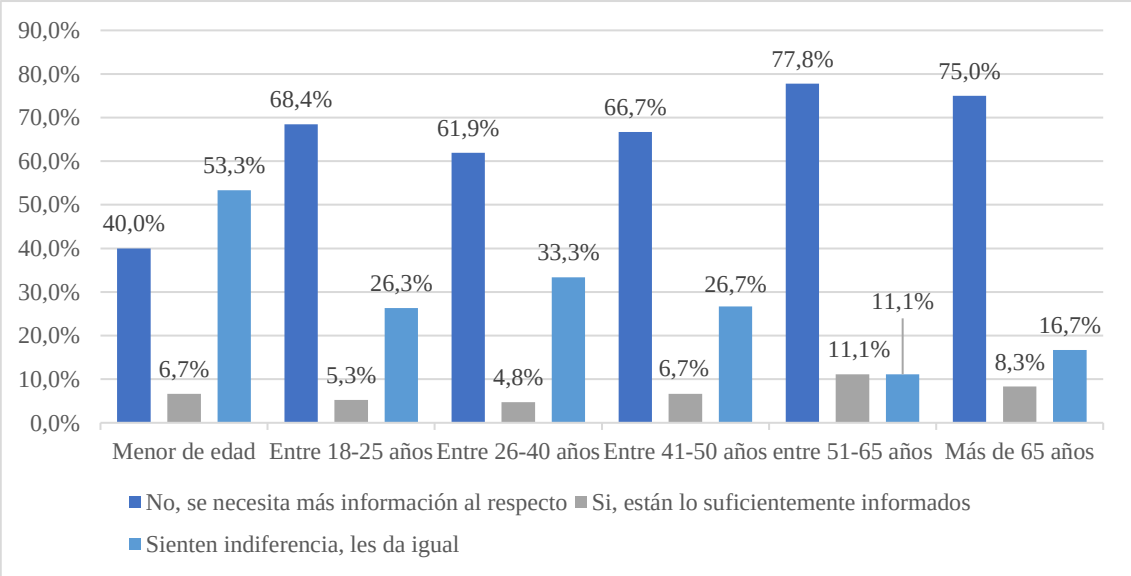
En esta gráfica se ven representados distintos **ciberdelitos** de los que son víctimas las personas. En ella se observa como la mayoría de las personas no han sido víctimas de ningún tipo de ciberataque, lo que resulta bastante confortante para el progreso dentro de la sociedad. Aun asi, las estafas y el libre uso de los datos personales son los dos **ciberdelitos** que más sufren los usuarios con un 16% del total en ambos casos. Seguido de la suplantación de identidad de las cuales7 personas han sido víctimas, y la difusión de información falsa en la que solo 5 personas seleccionaron la opción.

Si se realiza una pequeña comparación con la gráfica del Ministerio del interior mencionada en el marco teórico (Imagen 1). Se puede observar que, tanto en la gráfica del Ministerio, como en esta pregunta llevada a cabo en la encuesta realizada de este proyecto, coincide en ambas la opción de la mayoría de las respuestas seleccionadas, tanto por los **ciberdelincuentes** como por las propias víctimas, ya que en las dos gráficas se observa como el fraude informático es el delito que más se comete y el que más víctimas los sufren.

Con esta descripción se puede destacar la necesidad de incidir en este tipo de delito, para asi poder disminuir la **ciberdelincuencia** y que los usuarios protejan su privacidad y naveguen de forma más segura. A través de herramientas y mecanismos que verifiquen el medio y asi poder confiar en él.

5.1.4 Gráfico de datos de la pregunta número 4 (Anexo 1)

"¿Cree que los usuarios están lo suficientemente informados sobre los riesgos de privacidad y seguridad en las redes sociales?"



Fuente: Elaboración propia a partir de Tabla cruzada 4 (Anexo 2)

En la siguiente gráfica se muestra las opiniones de los encuestados según el rango de edad sobre si creen que están lo suficientemente informados sobre los riesgos de privacidad y seguridad en las redes sociales.

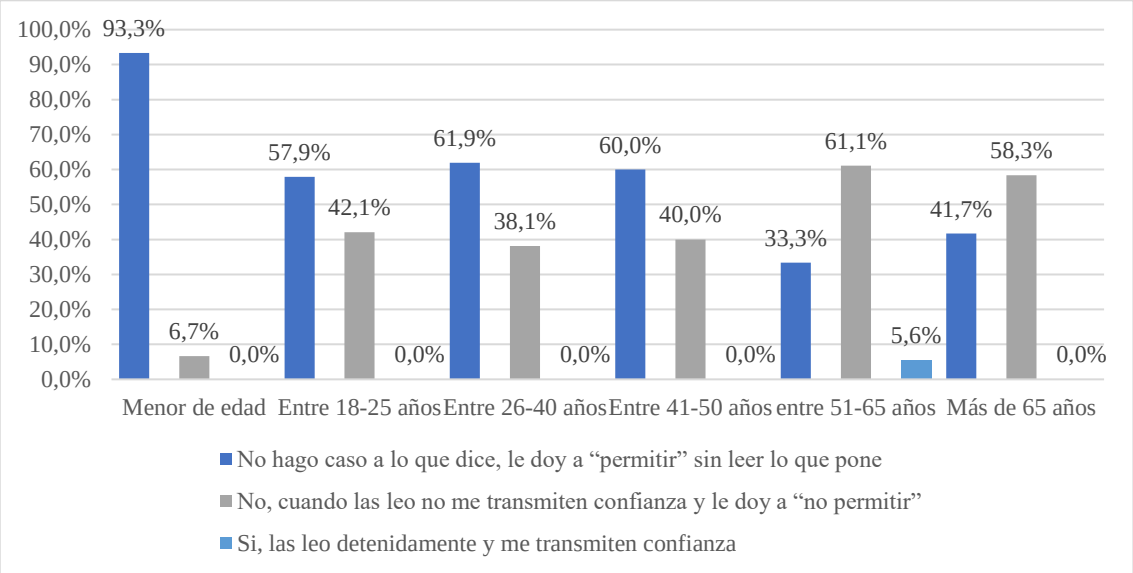
En general, la mayoría de los encuestados independientemente de su rango de edad, con un total de 65 personas, parecen sentir que los usuarios no están lo suficientemente informados sobre los riesgos de privacidad y seguridad en las redes sociales. Aun asi, las personas que más eligieron esta opción son los grupos de más avanzada edad, con porcentajes que van desde el 61,9% hasta el 77,8%.

Por otro lado, se observa, como los porcentajes más elevados en la respuesta de sentir indiferencia se encuentran entre las personas más jóvenes con un 33,3% entre el grupo de 26 y 40 años, hasta un 53,3% en los menores de edad. Solo 7 personas seleccionaron la opción de estar lo suficientemente informados sobre los riesgos.

Esto destaca la necesidad de una mayor conciencia sobre la materia, especialmente entre los usuarios más jóvenes, ya que sienten indiferencia hacia los riesgos expuestos anteriormente.

5.1.5 Gráfico de datos de la pregunta número 6 (Anexo 1)

"¿Las políticas de cookies le transmiten confianza?"



Fuente: Elaboración propia a partir de Tabla cruzada 6 (Anexo 2)

El gráfico relaciona la confianza que les transmite a los diferentes grupos de edad las políticas de cookies. La mayoría de los encuestados han optado por seleccionar la opción de ignorar las políticas de cookies y dar clin en "permitir" sin leerlas, entre ellos destacan los menores de edad con un alto porcentaje del 93,3%, seguido por el grupo de edad que está entre los 26 y 40 años con un 61,9%.

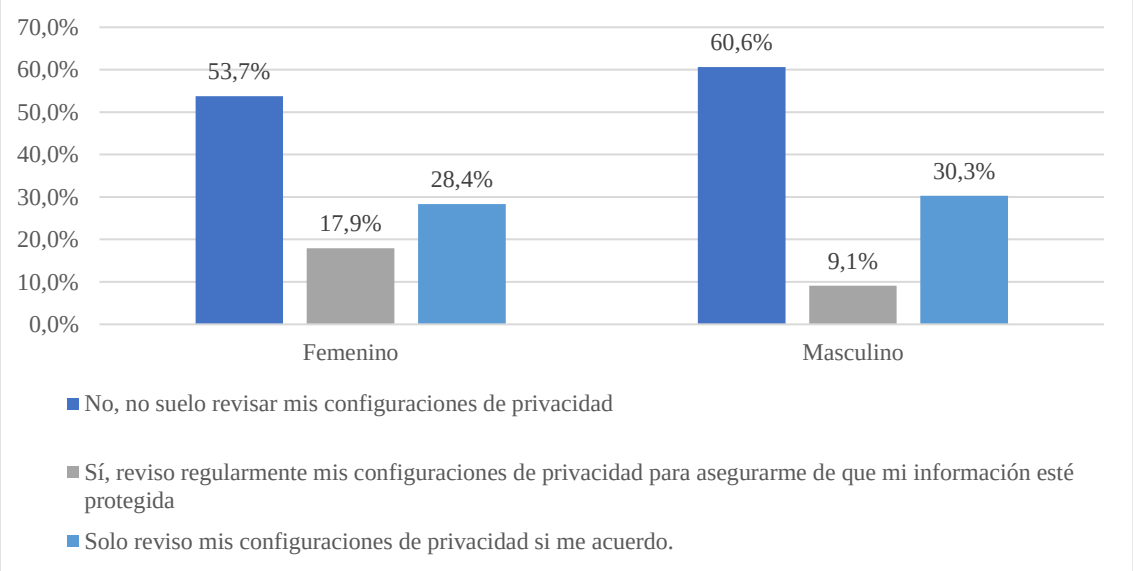
Por otro lado, hay un grupo significativo que, si lee las políticas de cookies, pero no les transmite confianza y optan por no permitirlas. La distribución por grupos de edad muestra que la mayoría de las personas que eligieron esta opción se encuentran entre los 51 y 65 años con un 61,1% seguido por el grupo que tiene entre 26 y 40 años.

Solo una persona indicó que lee detenidamente las políticas de cookies y le transmite confianza, perteneciente al grupo de entre 51 y 65 años con un 5,6%.

Esta gráfica refleja la importancia de la educación sobe la privacidad en línea y la necesidad de que los usuarios estén educados sobre como leer y comprender las políticas de privacidad. El hecho de que la mayoría de los encuestados, especialmente los más jóvenes, tiendan a ignorar las políticas de cookies y simplemente den clic en "permitir" sin leerlas, podría indicar una falta de comprensión sobre la importancia de proteger su información personal en línea.

5.1.6 Gráfico de datos de la pregunta número 7 (Anexo 1)

"¿Con respecto a la pregunta anterior, está al tanto de las configuraciones de privacidad de sus perfiles en redes sociales?"



Fuente: Elaboración propia a partir de Tabla Cruzada 7 (Anexo 2)

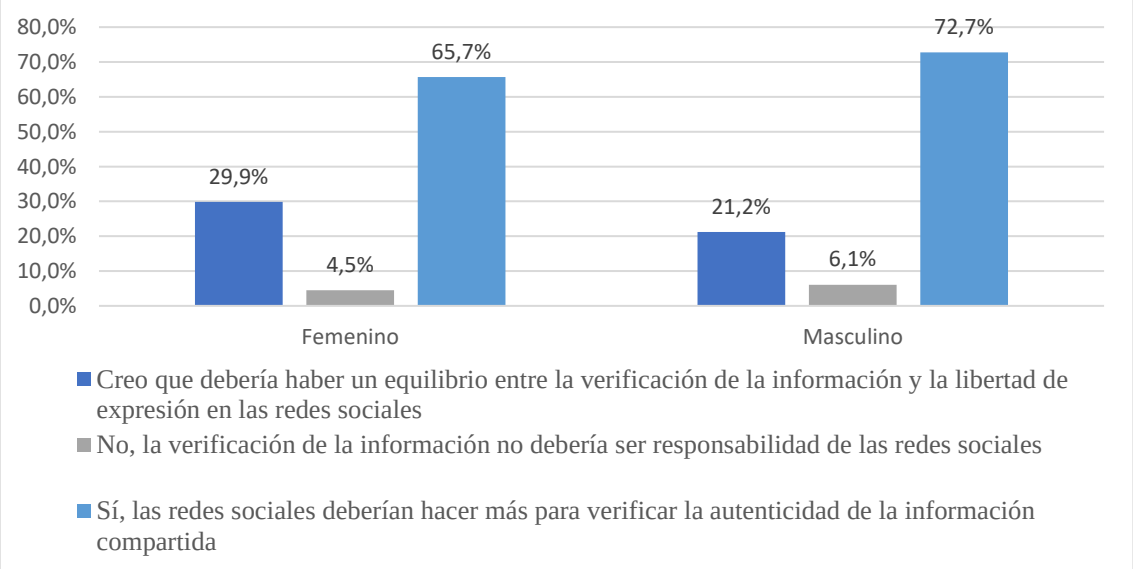
En la siguiente gráfica se observa como de importante es para los usuarios su privacidad en las redes sociales. En general, la mayoría de los encuestados, en concreto 56 personas, con un 53,7% de mujeres y un 60,6% de hombres, han contestado que no suelen revisar sus configuraciones. Esto sugiere, que una gran parte de los usuarios puede no estar al tanto de las configuraciones de privacidad de sus perfiles en las redes sociales, lo que podría dejar su información personal expuesta a riesgos de seguridad.

Por otro lado, resalta la disminución que se observa en cuanto a la respuesta contraria a la anterior, ya que el 17,9% de las mujeres y el 9,1% de los hombres sí que revisan su privacidad para asegurarse de que su privacidad esté protegida.

Además, hay 29 personas, de las cuales un 28,4% son mujeres y un 30,3% mencionan que solo revisan sus configuraciones si se acuerdan. Lo que resulta algo confuso, porque pueden tener conocimiento sobre la importancia que tiene la privacidad, pero no lo mantienen como un hábito continuo de hacerlo.

5.1.7 Gráfico de datos de la pregunta número 9 (Anexo 1)

"¿Cree que las redes sociales deberían tener la responsabilidad de verificar la autenticidad de la información compartida en sus plataformas para combatir la desinformación y las noticias falsas?"



Fuente: Elaboración propia a partir de Tabla Cruzada 9 (Anexo 2)

En la siguiente gráfica se muestra la opinión de los usuarios sobre la importancia de abordar tanto los beneficios como los riesgos asociados al uso de las redes sociales y como estas plataformas pueden tener tanto un impacto positivo como negativo en la vida de los usuarios.

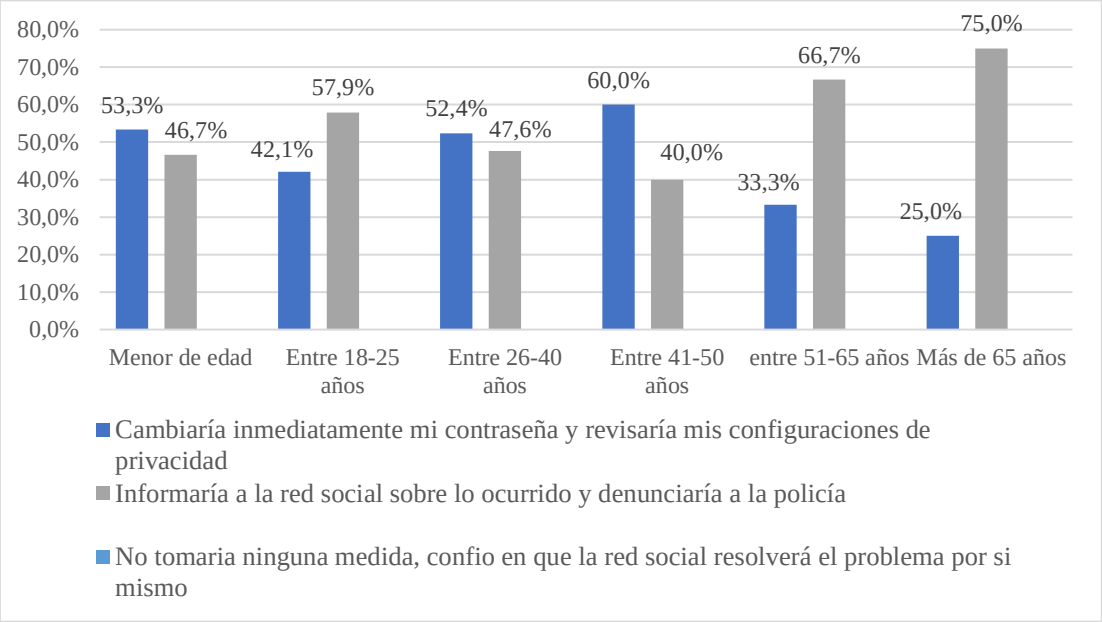
En relación con la pregunta, sobre si las redes sociales deberían de tener la responsabilidad de verificar la autenticidad de la información compartida en sus plataformas para combatir la desinformación, y las noticias falsas relacionada con el sexo, se observa como la mayoría de los encuestados tanto hombre con un 72,7% y mujer con un 65,7% se muestran de acuerdo, con que las redes deberían de hacer más para verificar la autenticidad de la información compartida. Confirmando que, la mayoría de las personas encuestadas no estarían de acuerdo con la respuesta que dice “no, la verificación de la información no debería de ser responsabilidad de las redes sociales”.

A la vez, muchos de ellos, estaban de acuerdo con que debería de haber un equilibrio entre la verificación de la información para combatir la desinformación y la preservación de la libertad de expresión en las redes sociales. Con un porcentaje del 29,9% en las mujeres y un 21,2% en los hombres.

Es importante que las redes sociales ofrezcan entretenimiento y herramientas educativas, pero también presentan riesgos para la sociedad. Los usuarios deberían tomar medidas para protegerse mientras disfrutan de sus beneficios, asi como las redes sociales deberían de encontrar un equilibrio entre proporcionar acceso a información valiosa y proteger la privacidad y seguridad de sus usuarios.

5.1.8 Gráfico de datos de la pregunta número 10 (Anexo 1)

"¿Qué medida tomaría si descubriera que sus datos personales han sido difundidos en una red social?"



Fuente: Elaboración propia a partir de Tabla Cruzada 10 (Anexo 2)

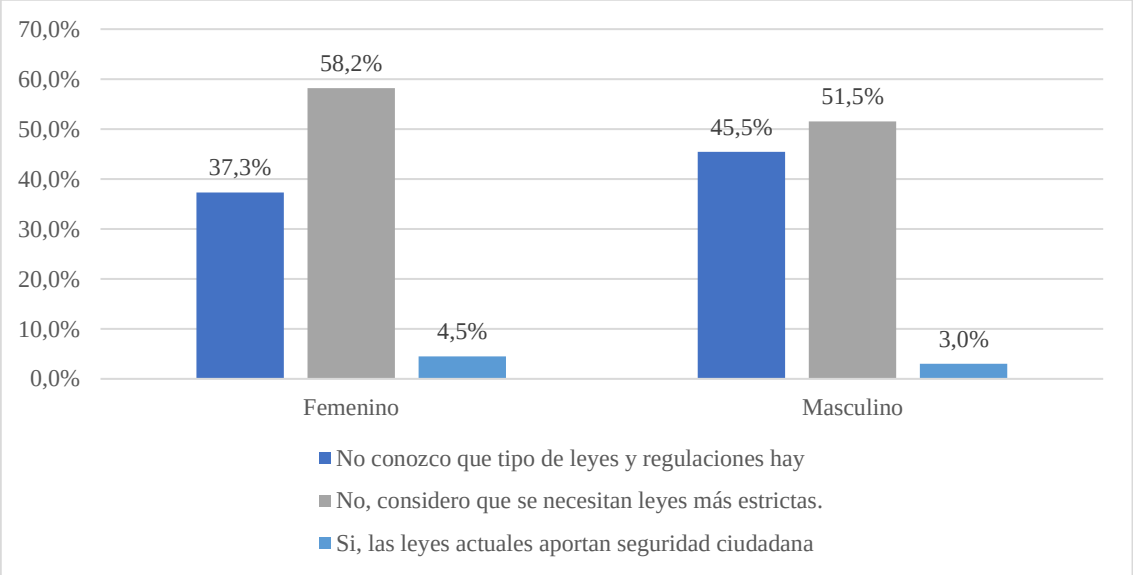
En esta gráfica se representa como los diferentes grupos de edad respondieron a la pregunta sobre qué medidas tomarían si descubrieran que sus datos han sido difundidos en una red social. Un total de 45 encuestados contestaron que cambiarían inmediatamente su contraseña y revisarían sus configuraciones de privacidad. La distribución por grupos de edad muestra que el mayor porcentaje de personas que elegirían esta medida se encuentra en el rango de edad entre 26 y 40 años con un 52,4%, seguido por el grupo menor de edad con un 53,3%, mostrándose entre ellos una distribución más uniforme.

Por consiguiente, se encuentran un total de 55 encuestados que seleccionaron la opción de informar a la red social sobre lo ocurrido y denunciar a la policía. El mayor porcentaje de personas que elegirían esta medida se encuentra en el rango de edad de entre 51 y 65 con un 66,7% seguido por el grupo de más de 65 años con un 75,0%.

En cuanto a la opción de no tomar ninguna medida, no se ve representada en la tabla, ya que ninguno de los encuestados seleccionó esa opción.

5.1.9 Gráfico de datos de la pregunta número 12 (Anexo 1)

"¿Cree que las leyes y regulaciones actuales son suficientes para proteger la privacidad y seguridad en un mundo de redes sociales?"

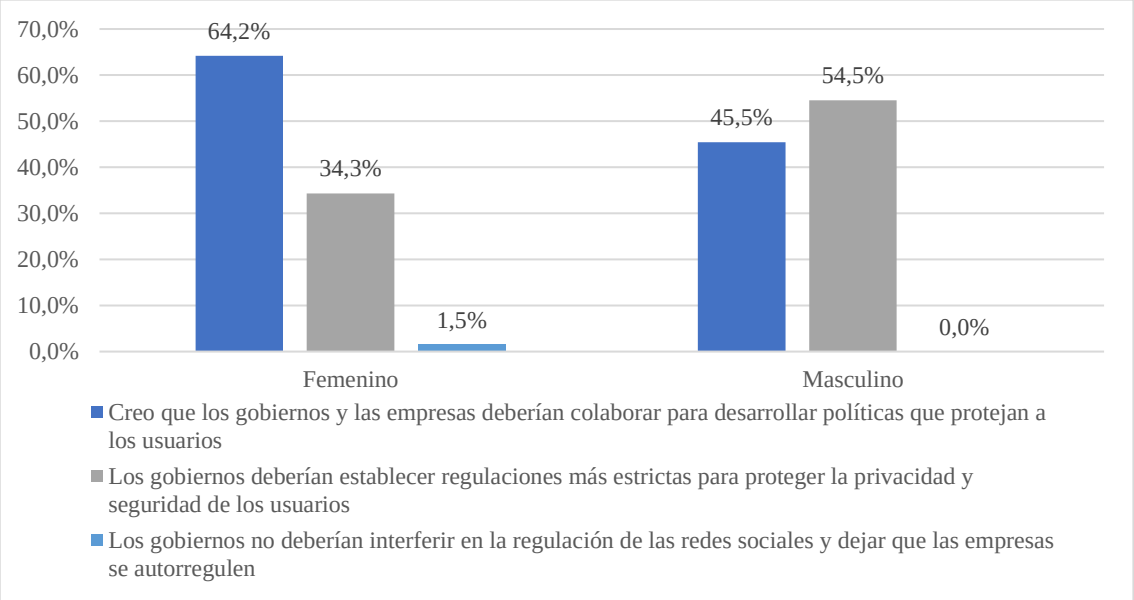


Fuente: Elaboración propia a partir de Tabla Cruzada 12 (Anexo 2)

En el gráfico se muestra la percepción de los encuestados sobre la eficacia de las leyes y regulaciones actuales en la protección de la privacidad y seguridad en un entorno de redes sociales. Los resultados muestran que una proporción significativa de los encuestados, tanto hombres como mujeres, consideran que las leyes y regulaciones actuales no son suficientes para proteger la privacidad y seguridad en un mundo de redes sociales. Específicamente, 40 de los encuestados en total, los cuales el 37,3% son mujeres, y el 45,5% son hombres, responden que no conocen que tipo de leyes y regulaciones existen, mientras que otras 56 personas, con un 58,2% de mujeres y un 51,5% de hombres consideran que se necesitan leyes más estrictas.

Lo que resulta haber una discrepancia entre la percepción de los usuarios sobre las leyes y regulaciones existentes y su eficacia real. Siendo el principal motivo, la falta de información y desconocimiento sobre ello.

5.1.10 Gráfico de datos Gráfico de datos de la pregunta número 14 (Anexo 1) "¿Qué papel cree que deberían desempeñar los gobiernos en la regulación de la privacidad y seguridad en las redes sociales?"



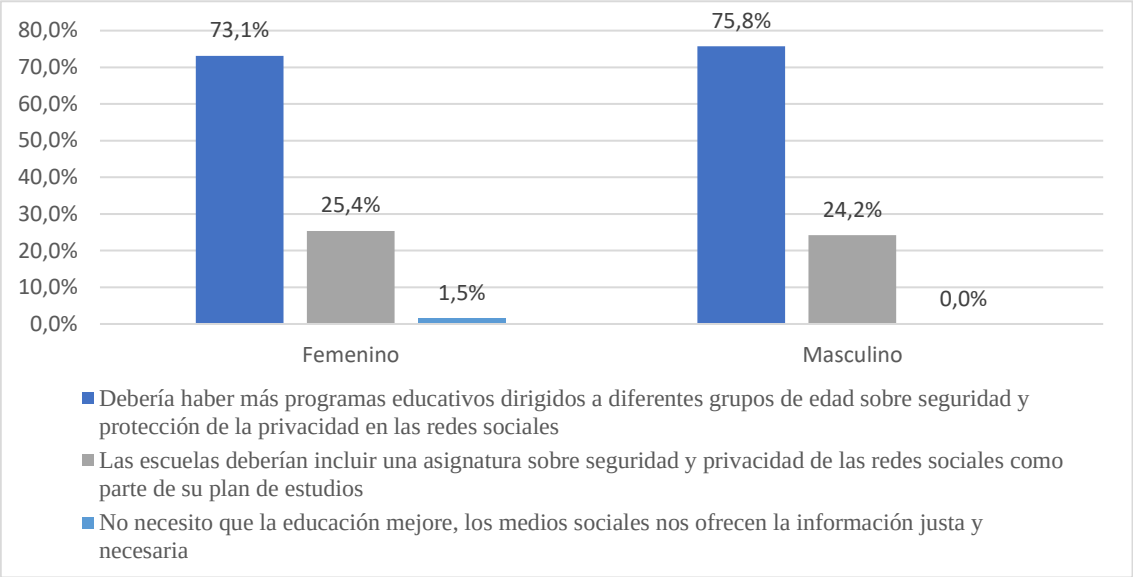
Fuente: Elaboración propia a partir de Tabla Cruzada 14 (Anexo 2)

En la siguiente gráfica se observa la importancia de la colaboración entre gobiernos, empresas y otros actores relevantes para abordar las amenazas de la **cibercriminalidad** y fortalecer la **ciberseguridad** a nivel nacional y europeo, con la elaboración de políticas y regulaciones para la protección de los usuarios.

En general, se observa una división de opiniones sobre el papel que deberían desempeñar los gobiernos en la regulación de la privacidad y seguridad en las redes sociales. La mayoría del sexo femenino con un 64,2% están a favor de una colaboración entre gobiernos y empresas para desarrollar políticas que protejan a los usuarios. Por otro lado, una proporción significativa del sexo masculino con un 54,5% opinan que los gobiernos son los que tendrían que establecer las regulaciones sin ayuda de las empresas. Solo una persona considera que los gobiernos no deberían de interferir en la regulación de las redes sociales, y dejar que las empresas se autorregulen.

5.1.11 Gráfico de datos de la pregunta número 15 (Anexo 1)

"¿Cómo cree que la educación sobre seguridad en línea y privacidad podría mejorar para los usuarios de todas las edades?"



Fuente: Elaboración propia a partir de Tabla Cruzada 15 (Anexo 2)

La gráfica refleja la importancia de la educación en **ciberseguridad** para todas las edades, y como los usuarios creen que puede mejorar la educación sobre la privacidad en línea.

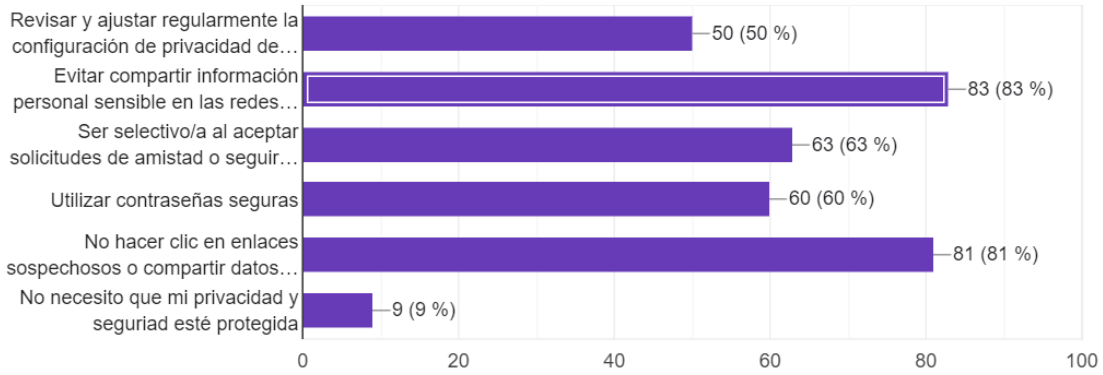
Un total de 74 encuestados, es decir, más de la mitad del total de los encuestados, contestaron que debería de haber más programas educativos dirigidos a diferentes grupos de edad sobre seguridad y protección de la privacidad en las redes sociales. La distribución por sexo muestra con un 73,1% del total de las mujeres y un 75,8% del total de los hombres.

La opción de que las escuelas deberían de incluir una asignatura sobre seguridad y privacidad de las redes sociales como plan de estudio, resultó ser menos seleccionada por los encuestados, solo fueron 25 las personas que la escogieron, el 25,4% del total de las mujeres y con un 24,2% de los hombres.

Solo una persona del sexo femenino no necesita que la educación mejore, ya que cree que los medios sociales ofrecen una información justa y necesaria.

5.1.12 Gráfico de datos de la pregunta número 16 (Anexo 1)

"¿Qué recomendaciones escogería para proteger su privacidad y seguridad en las redes sociales? (Puede seleccionar más de una opción)"



Fuente: Elaboración por Google forms a partir de Pregunta 16 de la encuesta

En la siguiente gráfica se observa la diversidad de soluciones, que los encuestados tomarían para proteger su privacidad y seguridad, en este caso podían seleccionar más de una opción.

Estadísticamente, se muestran dos opciones de respuesta significantes, ya que la mayoría de los encuestados opinan que la recomendación más efectiva sería "evitar compartir información sensible en las redes sociales" con un 83% y "no hacer clic en enlaces sospechosos o compartir datos personales con terceros" con un 81% de respuestas. Seguida la opción de "ser selectivo/a al aceptar solicitudes de amistad o seguir a otras personas" con un 63% y "utilizar contraseñas seguras" con un 60% de respuestas. Solo 9 personas opinaban que no necesitaban que su privacidad y seguridad estuviera protegida.

Lo que muestra de manera significativa las propuestas de los usuarios, para asi la **ciberseguridad** obtenga información sobre las opiniones de los usuarios, y pueda combatir de manera eficaz hacia los desafíos sobre el problema y elaborar medidas útiles.

6 CONCLUSIONES

La investigación realizada en este proyecto ha proporcionado una comprensión profunda acerca de cómo los usuarios perciben la privacidad y seguridad en el contexto de las redes sociales. A través del análisis de los resultados obtenidos de la encuesta y la revisión del marco teórico, se ha observado que existe una preocupación significativa entre los usuarios sobre la efectividad de las medidas que se implantan en estas plataformas.

En primer lugar, las respuestas de la encuesta indican que existe una necesidad crítica de mejorar la educación y concienciación sobre la privacidad y seguridad en línea. Aunque la mayoría de los encuestados estén familiarizados con los aspectos básicos de su seguridad dentro de las plataformas, como puede ser la configuración de privacidad de los perfiles, aún hay una gran multitud de usuarios que no tienen conocimiento sobre las regulaciones actuales ni de las estrategias o herramientas que existen para la protección de su información personal. Esta observación apoya la hipótesis de que las medidas de protección no serán efectivas debido a la poca conciencia y educación recibida por los usuarios.

Por otro lado, en cuanto a la existencia de leyes y regulaciones como el RGPD y la LOPDGDD, los resultados revelan que muchos usuarios perciben que las medidas actuales no son suficientes para la protección de su privacidad, consideran necesario poner en marcha leyes más estrictas y medidas de cumplimiento para garantizar una protección adecuada de los datos personales. Lo que sugiere la necesidad de revisar y fortalecer las políticas de protección para poder abordar los desafíos en un mundo digital en constante evolución. Además, de aportar la confianza necesaria por parte de las plataformas sociales y las entidades gubernamentales para asi poder fomentar un entorno digital seguro.

Asimismo, debido al rápido avance de la tecnología y las continuas amenazas recibidas por los usuarios, por la cantidad de **ciberdelincuentes** que hay dentro del **ciberespacio**, será necesario que las políticas y regulaciones a parte de ser fortalecidas por los gobiernos, se actualicen regularmente para mantenerse al día con los desafíos que surgen continuamente. Lo que también confirma que la exposición y la actividad en las redes sociales aumenta el riesgo de amenazas y ataques en el **ciberespacio**, afirmando la hipótesis de que cuanto más conectados estemos a las redes sociales, mayor será el riesgo de amenazas y ataques del **ciberespacio**.

A pesar de todos estos riesgos, la **ciberseguridad** se crea por los organismos sociales como herramienta fundamental para la creación de estrategias y protección de los datos como elementos fundamentales para salvaguardar la integridad y privacidad de los usuarios, que junto con la **cibercriminología** trabajan para identificar patrones de comportamiento y vulnerabilidades que pueden ser útiles para los atacantes.

La **ciberseguridad**, por tanto, se beneficia de lo que aporta la **cibercriminología**, poder comprender las motivaciones, las técnicas y tácticas de los **ciberdelincuentes** en el campo virtual, para asi poder formular políticas e implementar estrategias efectivas para la protección de los usuarios dentro de las redes sociales.

En resumen, esta investigación subraya la necesidad de un enfoque integral y colaborativo para abordar los desafíos de la privacidad y seguridad en las plataformas sociales. Desde la actualización de las regulaciones hasta la promoción de la educación y concienciación, es importante que se trabaje en conjunto para garantizar un entorno digital seguro y protegido para todos los usuarios de las redes sociales, en un mundo que se encuentra en continua evolución tecnológica y lleno de **ciberdelincuentes**.

7 BIBLIOGRAFÍA

Agencia Española Protección Datos. (s. f.). *¿Qué es un Delegado de Protección de Datos (DPD)?* Aepd. Recuperado 11 de marzo de 2024, de https://www.aepd.es/preguntas-frecuentes/4-dpd/1-delegado-de-proteccion-de-datos

Aguirre Romero, J. M. (2004). ciberespacio y comunicación: nuevas formas de vertebración social en el siglo XXI. *Espéculo. Revista de Estudios Literarios.*, (27). Recuperado 12 de marzo de 2024, de https://biblioteca.org.ar/libros/150717.pdf

Alicia Gil Gil, Roberto Hernández Berlinches (2019). Ciberdelincuencia. Editorial Dykinson, S.L

Alto Nivel. (2013, 18 julio). BBS, el verdadero precursor de las redes sociales. *ALTONIVEL*. Recuperado 15 de marzo de 2024, de https://www.altonivel.com.mx/tecnologia/37059-bbs-el-verdadero-precursor-de-las-redes-sociales/

Andrade Alarcón, L. (2021). Criminología en las redes sociales: *Archivos de Criminología, Seguridad Privada y Criminalística*, *19*(29), 43–74. Recuperado 18 de marzo de 2024, de https://dialnet.unirioja.es/servlet/articulo?codigo=8333919

Anónimo. (2018). *CIBERCRIMEN Y DELITOS INFORMÁTICOS: Los nuevos tipos penales en la era de internet* (1.ª ed.) [Ebook]. ERREIUS. Recuperado 13 de marzo de 2024, de https://www.pensamientopenal.com.ar/system/files/2018/09/doctrina46963.pdf

Ara, R. (2022, 16 febrero). La relación entre Criminología y ciberseguridad. Medium. https://medium.com/@rafael.ara.casanova/la-relaci%C3%B3n-entre-criminolog%C3%ADa-y-ciberseguridad-729f24aadfd8

Argente, E., Vivancos, E., Alemany, J., & García-Fornes, A. (2017). Educando en privacidad en el uso de las redes sociales. *Education in the Knowledge Society*, 18(2), 107-126. https://www.redalyc.org/pdf/5355/535554766007.pdf

Atico 34. (s. f.). *Política de cookies: texto de cookies, plantilla y ejemplos*. Atico34. Recuperado 16 de marzo de 2024, de https://protecciondatos-lopd.com/empresas/politica-de-cookies/#Que_es_la_politica_de_cookies

Balance Trimestral de Criminalidad Tercer Trimestre (Informe del Ministerio Del Interior NIPO 126-20-005-0). (2023). Ministerio del interior. Balance de Criminalidad Tercer Trimestre 2023.pdf

Cámara Arroyo, S. (2020). Estudios criminológicos contemporáneos (IX): La cibercriminología y el perfil del ciberdelincuente. *Derecho y Cambio Social*, *60*, 470-512. Recuperado 18 de marzo de 2024 https://dialnet.unirioja.es/servlet/articulo?codigo=7524987

Camilo Urcuqui, C., García Peña, M., Osorio Quintero, J. L., & Navarro Cadavid. (2018). *ciberseguridad: un enfoque desde la ciencia de datos: Vol. 86 p*. José Ignacio Claros V. https://repository.icesi.edu.co/biblioteca_digital/bitstream/10906/84046/3/navarro_ciberseguridad_ciencia_2018.pdf

Castells, Manuel (1999). La era de la información: economía, sociedad y cultura. Madrid: Alianza

Castells, Manuel (2011). La sociedad red: una visión global. Madrid: Alianza

Editorial Etecé. (2021). Riesgos y peligros de las redes sociales. En *Concepto*. Recuperado 15 de marzo de 2024, de https://concepto.de/riesgos-y-peligros-de-las-redes-sociales/

Ekon. (s. f.). ¿Qué es y cómo afecta el RGPD? *Ekon*. Recuperado 15 de marzo de 2024, de https://www.ekon.es/rgpd

ESPE (s. f.). *Desventajas de las redes sociales*. Roa. Recuperado 17 de marzo de 2024, de https://roa.cedia.edu.ec/webappscode/42/desventajas_de_las_redes_sociales.html

Firma-e. (2014, 14 octubre). Pilares de la seguridad de la información: confidencialidad, integridad y disponibilidad. *ciberseguridad/GRC*. Recuperado 11 de marzo de 2024, de https://www.firma-e.com/blog/pilares-de-la-seguridad-de-la-informacion-confidencialidad-integridad-y-disponibilidad/#:~:text=Pilares%20de%20la%20Seguridad%20de%20la%20Informaci%C3%B3n%3A%20confidencialidad%2C%20integridad%20y%20disponibilidad,-Inicio

Flores Marquéz, E. (2023, 12 julio). Redes sociales y salud mental en adolescentes. *Escola de Salut Sant Joan de Déu*. Recuperado 14 de marzo de 2024, de https://escolasalut.sjdhospitalbarcelona.org/es/consejos-salud/salud-mental/rol-redes-sociales-salud-mental-adolescentes

Forero, T. (2019, 7 agosto). Conoce la historia del Internet desde su nacimiento hasta lo que es hoy. *Rockcontent*. Recuperado 21 de marzo de 2024, de https://rockcontent.com/es/blog/historia-del-internet/

Gallardo Lobato, R. (2022, 24 junio). 10 ventajas y desventajas de las Redes Sociales. *Aprendamos Marketing*. Recuperado 21 de marzo de 2024, de https://aprendamosmarketing.com/ventajas-y-desventajas-de-las-redes-sociales/

Gómez, H. (2013). El ciberespacio y su impacto en el Orden Social: Monografías y ensayos. *Revista de Marina*, 128-135, de https://revistamarina.cl/revistas/2013/2/gomez.pdf

Gomez Rivera, S. (2023, 19 abril). Las 10 ventajas y desventajas de las redes sociales que debes conocer. *Beedigital*. Recuperado 18 de marzo de 2024, de https://www.beedigital.es/redes-sociales-pymes-autonomos/las-10-ventajas-de-las-redes-sociales-que-debes-conocer/

Grupo de Trabajo de Tecnologías del Aprendizaje [GTTA] (Ed.). (2022). *Marco de Referencia de la Competencia Digital Docente* [Pleno de la Conferencia de Educación]. https://intef.es/wp-content/uploads/2022/03/MRCDD_V06B_GTTA.pdf

Observatorio de la Infancia & Instituto Nacional de ciberseguridad [INCIBE]. (2019). *Guía de uso seguro y responsable de Internet para profesionales de servicios de protección a la infancia*. Recuperado 13 de marzo de 2024, de https://observatoriodelainfancia.mdsocialesa2030.gob.es/productos/pdf/Guia_Internet_Accesible_2_Con_cubiertas_alta_resolucion.pdf

Hernández Moreno, A. (2017). ciberseguridad y confianza en el ámbito digital. *ICE*, *897*, 55-65. Recuperado 20 de marzo de 2024, de https://dialnet.unirioja.es/servlet/articulo?codigo=6265462

Herrero, M. (2023, 19 mayo). Educación y conciencia en seguridad cibernética. Escuela de Internet. Recuperado 21 de marzo de 2024, de https://www.escueladeinternet.com/educacion-y-conciencia-en-seguridad-cibernetica/

IBM. (s. f.). *¿Qué es el phishing?* Recuperado 20 de marzo de 2024, de https://www.ibm.com/es-es/topics/phishing

Justizia.eus. (2022, 30 marzo). *¿Cómo actuar si vulneran tus derechos en las redes sociales?* Recuperado 21 de marzo de 2024, de https://www.justizia.eus/noticia/2022/como-actuar-si-vulneran-tus-derechos-en-las-redes-sociales/webjus00-contentgen/es/#:~:text=En%20estos%20casos%2C%20puedes%20utilizar,sensibles%2C%20sexuales%20o%20violentos%E2%80%9D

Lapuerta Irigoyen, C. (2017, septiembre). ~El cibercrimen y el agente encubierto on line~. *Foro FICP*, 460-478. Recuperado 17 de marzo de 2024, de https://ficp.es/wp-content/uploads/2013/06/Foro-FICP-2017-2.pdf

Los desafíos de la privacidad en la era de las redes sociales. (2023, 4 julio). *Revista Summa*. Recuperado 21 de marzo de 2024, de https://revistasumma.com/los-desafios-de-la-privacidad-en-la-era-de-las-redes-sociales/

Maza, P. (s. f.). ¿Cómo se clasifican los delitos informáticos? #5. *Plablo Maza*. Recuperado 13 de marzo de 2024, de https://pablomazaabogado.es/ufaq/como-se-clasifican-los-delitos-informaticos

McAffe. (s. f.). *¿Qué es el malware?* McAfee. Recuperado 21 de marzo de 2024, de https://www.mcafee.com/es-es/antivirus/malware.html

Mejía Llano, J. C. (2023, febrero). INTERNET Y LAS REDES SOCIALES: CONOCE SUS BENEFICIOS, RIESGOS Y CÓMO PROTEGERTE. *Marketing Digital*. Recuperado 21 de marzo de 2024, de https://www.juancmejia.com/varios/internet-y-las-redes-sociales-conoce-sus-beneficios-riesgos-y-como-protegerte/

Ministerio de Hacienda. (s. f.). *Normativa sobre datos personales*. Recuperado 22 de marzo de 2024, de https://www.hacienda.gob.es/es-ES/El%20Ministerio/Paginas/DPD/Normativa_PD.aspx

Muniesa Tomás, P., Herrera Sánchez, D., Herrera Sánchez, J., Mártinez Moreno, F., Rubio García, M., Gil Pérez, V., Santiago Orozco, A. M., & Gómez Martín, M. Á. (2022*). INFORME SOBRE LA CIBERCRIMINALIDAD EN ESPAÑA* (Informe del Ministerio Del Interior NIPO 126-20-021-2). Ministerio del interior. Informe cibercriminalidad 2022 (1).pdf

Muñoz Prieto, M. del M., Fragueiro Barreiro, M. S., & Ayuso Manso, M. J. (2013). La importancia de las redes sociales en el ámbito educativo. *Escuela Abierta*, *16*, 91-104. Recuperado 20 de marzo de 2024, de https://ea.ceuandalucia.es/index.php/EA/article/view/159

Panda Security. (2023, 22 marzo). *Tipos de cibercrimen*. Pandasecurity. Recuperado 10 de marzo de 2024, de https://www.pandasecurity.com/es/mediacenter/tipos-de-cibercrimen

Pdatos. (s. f.). ¿Qué es la Ley de Protección de Datos o LOPDGDD? *Diccionario RGPD*. Recuperado 16 de marzo de 2024, de https://www.pdatos.com/blog/que-es-la-ley-de-proteccion-de-datos-o-lopdgdd

Polo Calvo, C. (s. f.). Privacidad en redes sociales. *Euroinnova*. Recuperado 20 de marzo de 2024, de https://www.euroinnova.edu.es/blog/privacidad-en-redes-sociales#de-que-trata-la-privacidad-en-redes-sociales%20

REDES SOCIALES: UNA VENTANA AL MUNDO ¿OPORTUNIDAD O PELIGRO? (II). (s. f.). Psicoworks. https://www.psicoworks.eu/redes-sociales-oportunidad-o-peligro-ii/

Sánchez Vera, F., Martínez Guirao, J. E., & Téllez Infantes, A. (2022). La seguridad en el ciberespacio desde una perspectiva sociocultural Security in cyberspace from a sociocultural perspective. Methaodos, 10(2), 243-258. Recuperado 21 de marzo de 2024, de Dialnet-LaSeguridadEnElciberespacioDesdeUnaPerspectivaSoci-8634381.pdf

Stalman, Andy (2016). Humanoffon: ¿Está internet cambiándonos como seres humanos? Deusto.

Stock, J. (2021). Guía sobre la Estrategia Nacional contra la ciberdelincuencia. *INTERPOL*, 1-38. Recuperado 15 de marzo de 2024, de https://www.interpol.int/es/Pagina-de-busqueda?search=Gu%C3%ADa+sobre+la+Estrategia+Nacional+contra+la+Ciberdelincuencia

Suplantación y robo de identidad en las redes sociales, un riesgo para las empresas. (2023, 4 abril). *INCIBE*. Recuperado 12 de marzo de 2024, de https://www.incibe.es/empresas/blog/suplantacion-y-robo-identidad-las-redes-sociales-riesgo-las-empresas

Ureña, A., Ferrari, A., Blanco, D., & Valdecasa, E. (2011). *Las Redes Sociales en Internet* (Informe del observatorio nacional de las telecomunicaciones y de la SI). Recuperado 18 de marzo de 2024, de https://www.ontsi.es/sites/ontsi/files/redes_sociales-documento_0.pdf

VV.AA. (2016). Media and information literacy: reinforcing human rights, countering radicalization and extremism. UNESCO. https://unesdoc.unesco.org/ark:/48223/pf0000246371

ANEXO 1

Encuesta: Privacidad y Seguridad en Redes Sociales

Estimado/a

participante,

Mi nombre es Estefania Varela Campos estudiante de quinto curso de Criminología y Trabajo Social.

El propósito de esta investigación es analizar las percepciones y experiencias de los usuarios en relación con la protección de su privacidad y su seguridad al navegar por las Redes Sociales

Las respuestas serán tratadas de manera confidencial y se utilizarán únicamente con fines académicos. La participación es voluntaria y la realización de este cuestionario está diseñado para que le tome alrededor de 10 minutos.

Le agradezco de antemano por dedicar unos minutos a compartir su opinión. Su participación contribuirá de manera significativa al proyecto académico de TFG.

Conforme a Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, la cual tiene por objeto la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos.

Sexo

- Femenino
- Masculino
- Prefiero no especificar

¿Cuántos años tiene?

- Menor de edad
- Entre 18-25 años
- Entre 26-40 años
- Entre 41-50 años

- Entre 51-65 años
- Más de 65 años

1. **¿Con qué frecuencia utiliza las redes sociales?**
    - Con poca frecuencia
    - Con mucha frecuencia
    - Con bastante frecuencia
2. **¿Como de seguro se siente cuando navegas por las redes sociales?**
    - Poco seguro
    - Muy seguro
    - Bastante seguro
3. **¿Ha sido víctima de alguno de estos ciberdelitos o cualquier otro ataque que haya violado su privacidad en una red social? (Puede seleccionar más de una opción)**
    - Suplantación de la identidad
    - Difusión de información falsa sobre ti
    - Libre uso de sus datos personales
    - Estafas
    - No he sido víctima de ningún tipo de ciberataque
    - Otro…
4. **¿Cree que los usuarios están lo suficientemente informados sobre los riesgos de privacidad y seguridad en las redes sociales?**
    - Si, están lo suficientemente informados.
    - No, se necesita más información al respecto.
    - Sienten indiferencia, les da igual.

5. **¿Qué opina sobre la recopilación de datos por parte de las redes sociales con fines publicitarios o de análisis de comportamiento?**

    - Estoy de acuerdo con la recopilación de datos si es para mejorar la experiencia del usuario.
    - No estoy de acuerdo con la recopilación de datos sin el consentimiento explícito del usuario.
    - Creo que los usuarios deberían tener más control sobre qué datos se recopilan y cómo se utilizan.

6. **¿Las políticas de cookies le transmiten confianza?**

    - Si, las leo detenidamente y me transmiten confianza.
    - No, cuando las leo no me transmiten confianza y le doy a "no permitir".
    - No hago caso a lo que dice, le doy a "permitir" sin leer lo que pone.

7. **¿Con respecto a la pregunta anterior, está al tanto de las configuraciones de privacidad de sus perfiles en redes sociales?**

    - Sí, reviso regularmente mis configuraciones de privacidad para asegurarme de que mi información esté protegida.
    - No, no suelo revisar mis configuraciones de privacidad.
    - Solo reviso mis configuraciones de privacidad si me acuerdo.

8. **¿Cuándo ha compartido información personal sensible en las redes sociales (por ejemplo, su dirección, número de teléfono, etc.) se ha sentido seguro?**

    - Sí, he compartido información personal sensible y me he sentido seguro con la plataforma.
    - Sí, he compartido información sensible pero no me he sentido seguro con la plataforma.
    - No, nunca comparto información personal sensible en las redes sociales.

9. **¿Cree que las redes sociales deberían tener la responsabilidad de verificar la autenticidad de la información compartida en sus plataformas para combatir la desinformación y las noticias falsas?**

    - Sí, las redes sociales deberían hacer más para verificar la autenticidad de la información compartida.
    - No, la verificación de la información no debería ser responsabilidad de las redes sociales.
    - Creo que debería haber un equilibrio entre la verificación de la información y la libertad de expresión en las redes sociales.

10. **¿Qué medida tomaría si descubriera que sus datos personales han sido difundidos en una red social?**

    - Cambiaría inmediatamente mi contraseña y revisaría mis configuraciones de privacidad.
    - Informaría a la red social sobre lo ocurrido y denunciaría a la policía.
    - No tomaría ninguna medida, confío en que la red social resolverá el problema por sí mismo.

11. **¿Ha cambiado sus hábitos de uso de redes sociales debido a preocupaciones sobre privacidad y seguridad?**

    - Sí, he reducido mi actividad en las redes sociales.
    - No, mi actividad en las redes sociales sigue siendo la misma.
    - Indiferente, el tema de privacidad y seguridad en las redes sociales no me preocupa.

12. **¿Cree que las leyes y regulaciones actuales son suficientes para proteger la privacidad y seguridad en un mundo de redes sociales?**

    - Si, las leyes actuales aportan seguridad ciudadana.
    - No, considero que se necesitan leyes más estrictas.
    - No conozco que tipo de leyes y regulaciones hay.

13. **¿Qué medidas cree que deberían tomar las plataformas de redes sociales para garantizar la privacidad y seguridad de sus usuarios?**

    - Mejorar las políticas de privacidad y términos de servicio.
    - Proporcionar herramientas más claras para controlar la privacidad.
    - Educación sobre seguridad en las redes sociales para los usuarios.
    - Implementar medidas más estrictas para verificar la autenticidad de las cuentas.

14. **¿Qué papel cree que deberían desempeñar los gobiernos en la regulación de la privacidad y seguridad en las redes sociales?**

    - Los gobiernos deberían establecer regulaciones más estrictas para proteger la privacidad y seguridad de los usuarios.
    - Los gobiernos no deberían interferir en la regulación de las redes sociales y dejar que las empresas se autorregulen.
    - Creo que los gobiernos y las empresas deberían colaborar para desarrollar políticas que protejan a los usuarios.

15. **¿Cómo cree que la educación sobre seguridad en línea y privacidad podría mejorar para los usuarios de todas las edades?**

    - Debería haber más programas educativos dirigidos a diferentes grupos de edad sobre seguridad y protección de la privacidad en las redes sociales.
    - Las escuelas deberían incluir una asignatura sobre seguridad y privacidad de las redes sociales como parte de su plan de estudios.
    - No necesito que la educación mejore, los medios sociales nos ofrecen la información justa y necesaria.

16. **¿Qué recomendaciones escogería para proteger su privacidad y seguridad en las redes sociales? (puede seleccionar más de una)**

- Revisar y ajustar regularmente la configuración de privacidad de su cuenta.
- Evitar compartir información personal sensible en las redes sociales.
- Ser selectivo/a al aceptar solicitudes de amistad o seguir a otras personas.
- Utilizar contraseñas seguras.
- No hacer clic en enlaces sospechosos o compartir datos personales con terceros.
- No necesito que mi privacidad y seguridad esté protegida
- Otro…

ANEXO 2

Tabla cruzada 1

Tabla cruzada 1. ¿Con qué frecuencia utiliza las redes sociales?*¿Cuántos años tiene?

			¿Cuántos años tiene?						
			Entre 18-25 años	Entre 26-40 años	Entre 41-50 años	entre 51-65 años	Más de 65 años	Menor de edad	Total
1. ¿Con qué frecuencia utiliza las redes sociales?	Con bastante frecuencia	Recuento	10	9	6	2	2	10	39
		% dentro de ¿Cuántos años tiene?	52,6%	42,9%	40,0%	11,1%	16,7%	66,7%	39,0%
	Con mucha frecuencia	Recuento	9	7	4	4	1	5	30
		% dentro de ¿Cuántos años tiene?	47,4%	33,3%	26,7%	22,2%	8,3%	33,3%	30,0%
	Con poca frecuencia	Recuento	0	5	5	12	9	0	31
		% dentro de ¿Cuántos años tiene?	0,0%	23,8%	33,3%	66,7%	75,0%	0,0%	31,0%
Total		Recuento	19	21	15	18	12	15	100
		% dentro de ¿Cuántos años tiene?	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%

Fuente: Elaboración propia, a través de los datos estadísticos obtenidos en la herramienta del SPSS de la encuesta realizada.

Tabla cruzada 2

Tabla cruzada 2. ¿Como de seguro se siente cuando navegas por las redes sociales?*sexo

			sexo		
			Femenino	Masculino	Total
2. ¿Como de seguro se siente cuando navegas por las redes sociales?	Batante seguro	Recuento	14	8	22
		% dentro de sexo	20,9%	24,2%	22,0%
	Muy seguro	Recuento	16	4	20
		% dentro de sexo	23,9%	12,1%	20,0%
	Poco seguro	Recuento	37	21	58
		% dentro de sexo	55,2%	63,6%	58,0%
Total		Recuento	67	33	100
		% dentro de sexo	100,0%	100,0%	100,0%

Fuente: Elaboración propia, a través de los datos estadísticos obtenidos en la herramienta del SPSS de la encuesta realizada.

Tabla cruzada 4

Tabla cruzada 4. ¿Cree que los usuarios están lo suficientemente informados sobre los riesgos de privacidad y seguridad en las redes sociales?*¿Cuántos años tiene?

			¿Cuántos años tiene?						
			Entre 18-25 años	Entre 26-40 años	Entre 41-50 años	entre 51-65 años	Más de 65 años	Menor de edad	Total
4. ¿Cree que los usuarios están lo suficientemente informados sobre los riesgos de privacidad y seguridad en las redes sociales?	No, se necesita más información al respecto	Recuento	13	13	10	14	9	6	65
		% dentro de ¿Cuántos años tiene?	68,4%	61,9%	66,7%	77,8%	75,0%	40,0%	65,0%
	Si, están lo suficientemente informados	Recuento	1	1	1	2	1	1	7
		% dentro de ¿Cuántos años tiene?	5,3%	4,8%	6,7%	11,1%	8,3%	6,7%	7,0%
	Sienten indiferencia, les da igual	Recuento	5	7	4	2	2	8	28
		% dentro de ¿Cuántos años tiene?	26,3%	33,3%	26,7%	11,1%	16,7%	53,3%	28,0%
Total		Recuento	19	21	15	18	12	15	100
		% dentro de ¿Cuántos años tiene?	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%

Fuente: Elaboración propia, a través de los datos estadísticos obtenidos en la herramienta del SPSS de la encuesta realizada.

Tabla cruzada 6

Tabla cruzada 6. ¿Las políticas de cookies le transmiten confianza?*¿Cuántos años tiene?

			¿Cuántos años tiene?						
			Entre 18-25 años	Entre 26-40 años	Entre 41-50 años	entre 51-65 años	Más de 65 años	Menor de edad	Total
6. ¿Las políticas de cookies le transmiten confianza?	No hago caso a lo que dice, le doy a "permitir" sin leer lo que pone	Recuento	11	13	9	6	5	14	58
		% dentro de ¿Cuántos años tiene?	57,9%	61,9%	60,0%	33,3%	41,7%	93,3%	58,0%
	No, cuando las leo no me transmiten confianza y le doy a "no permitir"	Recuento	8	8	6	11	7	1	41
		% dentro de ¿Cuántos años tiene?	42,1%	38,1%	40,0%	61,1%	58,3%	6,7%	41,0%
	Si, las leo detenidamente y me transmiten confianza	Recuento	0	0	0	1	0	0	1
		% dentro de ¿Cuántos años tiene?	0,0%	0,0%	0,0%	5,6%	0,0%	0,0%	1,0%
Total		Recuento	19	21	15	18	12	15	100
		% dentro de ¿Cuántos años tiene?	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%

Fuente: Elaboración propia, a través de los datos estadísticos obtenidos en la herramienta del SPSS de la encuesta realizada.

Tabla cruzada 7

Tabla cruzada 7. ¿Con respecto a la pregunta anterior, está al tanto de las configuraciones de privacidad de sus perfiles en redes sociales?*sexo

			sexo		
			Femenino	Masculino	Total
7. ¿Con respecto a la pregunta anterior, está al tanto de las configuraciones de privacidad de sus perfiles en redes sociales?	No, no suelo revisar mis configuraciones de privacidad	Recuento	36	20	56
		% dentro de sexo	53,7%	60,6%	56,0%
	Sí, reviso regularmente mis configuraciones de privacidad para asegurarme de que mi información esté protegida	Recuento	12	3	15
		% dentro de sexo	17,9%	9,1%	15,0%
	Solo reviso mis configuraciones de privacidad si me acuerdo.	Recuento	19	10	29
		% dentro de sexo	28,4%	30,3%	29,0%
Total		Recuento	67	33	100
		% dentro de sexo	100,0%	100,0%	100,0%

Fuente: Elaboración propia, a través de los datos estadísticos obtenidos en la herramienta del SPSS de la encuesta realizada.

Tabla cruzada 9

Tabla cruzada 9. ¿Cree que las redes sociales deberían tener la responsabilidad de verificar la autenticidad de la información compartida en sus plataformas para combatir la desinformación y las noticias falsas?*sexo

			sexo		
			Femenino	Masculino	Total
9. ¿Cree que las redes sociales deberían tener la responsabilidad de verificar la autenticidad de la información compartida en sus plataformas para combatir la desinformación y las noticias falsas?	Creo que debería haber un equilibrio entre la verificación de la información y la libertad de expresión en las redes sociales	Recuento	20	7	27
		% dentro de sexo	29,9%	21,2%	27,0%
	No, la verificación de la información no debería ser responsabilidad de las redes sociales	Recuento	3	2	5
		% dentro de sexo	4,5%	6,1%	5,0%
	Sí, las redes sociales deberían hacer más para verificar la autenticidad de la información compartida	Recuento	44	24	68
		% dentro de sexo	65,7%	72,7%	68,0%
Total		Recuento	67	33	100
		% dentro de sexo	100,0%	100,0%	100,0%

Fuente: Elaboración propia, a través de los datos estadísticos obtenidos en la herramienta del SPSS de la encuesta realizada.

Tabla cruzada 10

Tabla cruzada 10. ¿Qué medida tomaría si descubriera que sus datos personales han sido difundidos en una red social?*¿Cuántos años tiene?

			¿Cuántos años tiene?						
			Entre 18-25 años	Entre 26-40 años	Entre 41-50 años	entre 51-65 años	Más de 65 años	Menor de edad	Total
10. ¿Qué medida tomaría si descubriera que sus datos personales han sido difundidos en una red social?	Cambiaría inmediatamente mi contraseña y revisaría mis configuraciones de privacidad	Recuento	8	11	9	6	3	8	45
		% dentro de ¿Cuántos años tiene?	42,1%	52,4%	60,0%	33,3%	25,0%	53,3%	45,0%
	Informaría a la red social sobre lo ocurrido y denunciaría a la policía	Recuento	11	10	6	12	9	7	55
		% dentro de ¿Cuántos años tiene?	57,9%	47,6%	40,0%	66,7%	75,0%	46,7%	55,0%
Total		Recuento	19	21	15	18	12	15	100
		% dentro de ¿Cuántos años tiene?	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%

Fuente: Elaboración propia, a través de los datos estadísticos obtenidos en la herramienta del SPSS de la encuesta realizada.

Tabla cruzada 11

Tabla cruzada 11. ¿Ha cambiado sus hábitos de uso de redes sociales debido a preocupaciones sobre privacidad y seguridad?*sexo

			sexo		
			Femenino	Masculino	Total
11. ¿Ha cambiado sus hábitos de uso de redes sociales debido a preocupaciones sobre privacidad y seguridad?	Indiferente, el tema de privacidad y seguridad en las redes sociales no me preocupa	Recuento	9	1	10
		% dentro de sexo	13,4%	3,0%	10,0%
	No, mi actividad en las redes sociales sigue siendo la misma	Recuento	34	17	51
		% dentro de sexo	50,7%	51,5%	51,0%
	Sí, he reducido mi actividad en las redes sociales.	Recuento	24	15	39
		% dentro de sexo	35,8%	45,5%	39,0%
Total		Recuento	67	33	100
		% dentro de sexo	100,0%	100,0%	100,0%

Fuente: Elaboración propia, a través de los datos estadísticos obtenidos en la herramienta del SPSS de la encuesta realizada.

Tabla cruzada 12

Tabla cruzada 12. ¿Cree que las leyes y regulaciones actuales son suficientes para proteger la privacidad y seguridad en un mundo de redes sociales?*sexo

			sexo		
			Femenino	Masculino	Total
12. ¿Cree que las leyes y regulaciones actuales son suficientes para proteger la privacidad y seguridad en un mundo de redes sociales?	No conozco que tipo de leyes y regulaciones hay	Recuento	25	15	40
		% dentro de sexo	37,3%	45,5%	40,0%
	No, considero que se necesitan leyes más estrictas.	Recuento	39	17	56
		% dentro de sexo	58,2%	51,5%	56,0%
	Si, las leyes actuales aportan seguridad ciudadana	Recuento	3	1	4
		% dentro de sexo	4,5%	3,0%	4,0%
Total		Recuento	67	33	100
		% dentro de sexo	100,0%	100,0%	100,0%

Fuente: Elaboración propia, a través de los datos estadísticos obtenidos en la herramienta del SPSS de la encuesta realizada.

Tabla cruzada 14

Tabla cruzada 14. ¿Qué papel cree que deberían desempeñar los gobiernos en la regulación de la privacidad y seguridad en las redes sociales?*sexo

			sexo		
			Femenino	Masculino	Total
14. ¿Qué papel cree que deberían desempeñar los gobiernos en la regulación de la privacidad y seguridad en las redes sociales?	Creo que los gobiernos y las empresas deberían colaborar para desarrollar políticas que protejan a los usuarios	Recuento	43	15	58
		% dentro de sexo	64,2%	45,5%	58,0%
	Los gobiernos deberían establecer regulaciones más estrictas para proteger la privacidad y seguridad de los usuarios	Recuento	23	18	41
		% dentro de sexo	34,3%	54,5%	41,0%
	Los gobiernos no deberían interferir en la regulación de las redes sociales y dejar que las empresas se autorregulen	Recuento	1	0	1
		% dentro de sexo	1,5%	0,0%	1,0%
Total		Recuento	67	33	100
		% dentro de sexo	100,0%	100,0%	100,0%

Fuente: Elaboración propia, a través de los datos estadísticos obtenidos en la herramienta del SPSS de la encuesta realizada.

Tabla cruzada 15

Tabla cruzada 15. ¿Cómo cree que la educación sobre seguridad en línea y privacidad podría mejorar para los usuarios de todas las edades?*sexo

			sexo		
			Femenino	Masculino	Total
15. ¿Cómo cree que la educación sobre seguridad en línea y privacidad podría mejorar para los usuarios de todas las edades?	Debería haber más programas educativos dirigidos a diferentes grupos de edad sobre seguridad y protección de la privacidad en las redes sociales	Recuento	49	25	74
		% dentro de sexo	73,1%	75,8%	74,0%
	Las escuelas deberían incluir una asignatura sobre seguridad y privacidad de las redes sociales como parte de su plan de estudios	Recuento	17	8	25
		% dentro de sexo	25,4%	24,2%	25,0%
	No necesito que la educación mejore, los medios sociales nos ofrecen la información justa y necesaria	Recuento	1	0	1
		% dentro de sexo	1,5%	0,0%	1,0%
Total		Recuento	67	33	100
		% dentro de sexo	100,0%	100,0%	100,0%

Fuente: Elaboración propia, a través de los datos estadísticos obtenidos en la herramienta del SPSS de la encuesta realizada.