Artículo

Análisis del Uso de Datos Personales en Redes Sociales: Privacidad y Seguridad

Hernandez-Uribe Citlaly [1], Hernández Najera Erick[2], Cristales Bonilla Saulo Gregorio[3], Chávez Cruz Adrián[4], Lartundo Gutierrez Fatima[5], *

[2-4]Afiliación 1; Tecnológico Nacional de México /ITS Huichapan. Ingeniería en Sistemas Computacionales/Docentes
[1, 5]Afiliación 2; Tecnológico Nacional de México /ITS Huichapan. Ingeniería en Sistemas Computacionales/Estudiantes
* Correspondencia: achavez@iteshu.edu.mx, Sgcristales@iteshu.edu.mx, Ehernandez@iteshu.edu.mx, a22021057@iteshu.edu.mx, a22021528@iteshu.edu.mx.

Resumen:

El artículo analizó el uso de datos personales en redes sociales, su impacto en la privacidad y seguridad de los usuarios. Para ello, el estudio buscó comprender las prácticas de manejo de información personal en plataformas como Facebook, WhatsApp e Instagram, destacando la vulnerabilidad de estos datos. Se empleó una metodología mixta, combinando enfoques cualitativos y cuantitativos, con encuestas y análisis documental de perfiles de usuarios. Se encontró que, aunque las configuraciones de privacidad permitían personalizar la experiencia del usuario, a menudo eran insuficientes, y los usuarios no siempre eran conscientes de los riesgos asociados. La investigación destacó la necesidad de mejorar las medidas de protección y concientizar a los usuarios sobre la gestión de su información personal para prevenir el mal uso y robo de datos.

Keywords: redes sociales; usuarios; datos personales; privacidad; seguridad.

Chávez-Cruz Adrián.; Cristales-Bonilla Saulo Gregorio; Hernández-Najera Erik; Hernandez-Uribe Citlaly; Lartundo-Gutierrez Fatima. Análisis del Uso de Datos Personales en Redes Sociales: Privacidad y Seguridad. ***REIA*** 2024, 8, (2), 11-25.

Recibido: 16/09/2024
Aceptado: 15/11/2024
Publicado: 29/11/24

1. Introducción

La modernización y el avance de la Sociedad de la Información (SI) establecen nuevos requisitos para las tecnologías de la información y la comunicación (TIC) contemporáneas abordando diversos desafíos como la globalización [1], el acceso remoto a los recursos de información y la computación en la nube [2], la información distribuida, servicios y entornos virtuales [3] y determinación de una política adecuada de seguridad de la información en las empresas [4]. Las redes sociales también deberían incluirse en este ámbito, ya que las TIC contemporáneas permiten ampliar las relaciones sociales y consolidar el campo de la "informática social" relacionado con la construcción de redes de sitios web (Facebook, Twitter, Instagram, WhatsApp, LinkedIn, etc.) [5].

En este contexto, el término 'redes sociales' describe un conjunto de diversas tecnologías móviles y basadas en la web que transforman la comunicación en una conversación interactiva y permiten compartir imágenes, información de audio y video, experiencias, etc. [6] Estas plataformas garantizan el acceso de usuarios a recursos de la red para crear, editar y complementar contenido, por lo que no son simplemente consumidores pasivos de información en estas plataformas, sino que también pueden realizar diferentes formas de comunicación directa, incluidas interacciones con empresas y otros usuarios. Las

nuevas TIC y los entornos distribuidos permiten que los usuarios creen su propio perfil con datos personales y publiquen información personal, la cual está disponible para otros usuarios a través de la red global.

Estas características son fundamentales en el contexto de las redes sociales, cuyo origen teórico-sociológico fue propuesto por Frigyes Karinthy (1929) con la teoría de los "seis grados de separación ", la cual establece que cualquier persona puede conectarse e interactuar con cualquier otra persona del planeta con sólo seis enlaces (conexiones). Este concepto, respaldado por Duncan J. Watts (2004), está basado en la idea de que el número de conocidos crece exponencialmente con el número de enlaces en la cadena, y sólo un pequeño número de enlaces son necesarios para que el conjunto de conocidos se convierta en toda la población humana [7].

Este concepto es complementado por Kietzmann, J. H & Hermkens, K (2011) [8] identificando siete bloques funcionales del marco de las redes sociales: identidad (sobre el alcance de la divulgación de información en un entorno de redes sociales); conversaciones (sobre el alcance de las comunicaciones entre usuarios en una red social); compartir (sobre el alcance del intercambio, distribución y recepción de contenidos por parte de los usuarios); presencia (sobre hasta qué punto los usuarios pueden saber si otros usuarios son accesibles); relaciones (representa el grado en que los usuarios pueden estar relacionados con otros usuarios); reputación (representa el grado en que los usuarios pueden identificar la posición de los demás, incluidos ellos mismos, en un entorno de redes sociales); grupos (representa el grado en que los usuarios pueden formar comunidades y subcomunidades). Estas funcionalidades permiten a cada usuario regular su identidad, relaciones y reputación sobre la base de elementos básicos.

En el ámbito de la privacidad de la información, según Santiago Gutiérrez, profesor de la Facultad de Comunicación, las redes sociales utilizan los datos personales para "entender" mejor a cada usuario. Esta segmentación de las audiencias les permite a las redes sociales conocer más a sus públicos, saber qué les gusta más para saber qué tipo de contenidos producir y cómo fomentar una interacción. "Los usos entrañan, sobre todo, condiciones publicitarias. Se conoce la información de valor acerca de los usuarios y, con base en ello, las redes sociales cuentan con un algoritmo que retribuye y circula (lo llaman feed) datos de cada persona. Después, poco a poco, se envía información consecuente con las decisiones que en el pasado ha tomado la persona en la red social, es decir, se le muestra un contenido cada vez más centrado en los gustos que ya el usuario ha suministrado, sin ser consciente de ello", afirma el profesor Gutiérrez [9].

Las redes sociales ofrecen información y opciones para definir y especificar el nivel de acceso o difusión de la información, es decir, el grado de privacidad. Sin embargo, en general, estas opciones vienen configuradas por defecto en el nivel más bajo de privacidad, siendo el propio usuario quien debe ajustarlas según sus preferencias. Muchos usuarios, sobre todo los más vulnerables, desconocen estas posibilidades y los riesgos que implica no establecer ciertas restricciones sobre la información compartida [10].

Esto adquiere mayor relevancia en un contexto marcado por diversos incidentes que desde principios de la década de 2010 han afectado la seguridad de plataformas sociales y digitales. En junio de 2012, LinkedIn sufrió un ataque de piratas informáticos rusos que comprometió cerca de 6.5 millones de contraseñas, afectando al 5% de sus usuarios [11]. En marzo de 2018, se reveló que Cambridge Analytica adquirió ilegalmente datos de al menos 87 millones de usuarios de Facebook a través de una aplicación de cuestionarios, vendiendo la información a la campaña de Donald Trump [12].

Polar, una app de fitness usada por personal militar y de seguridad, también sufrió una brecha de seguridad en 2018 que expuso datos de más de 6,460 miembros. Facebook enfrentó críticas en 2019 por almacenar contraseñas de usuarios de Instagram en texto plano y en julio de 2020 Twitter vio caer sus acciones después de que piratas informáticos tomaran el control de cuentas de alto perfil para estafar bitcoins [13]. Estos incidentes exponen la continua vulnerabilidad de las plataformas digitales y la necesidad urgente de mejorar la seguridad y protección de datos.

Por lo cual, esta investigación se centra precisamente en esta vulnerabilidad de la información de los usuarios en redes sociales, susceptible de ser explotada con diversos propósitos, como la publicidad dirigida y el robo de identidad. Este problema subraya la necesidad urgente de comprender cómo se maneja la información de los usuarios en este entorno digital y asegurar efectivamente su privacidad y seguridad. En la actualidad, dado el impacto creciente de las redes sociales en la vida cotidiana de millones de personas, es crucial entender cómo se emplean estos datos y qué medidas se implementan para proteger la privacidad de los usuarios.

Es así, que las plataformas han implementado diversas medidas de seguridad, como la encriptación de datos y la autenticación en dos pasos. Sin embargo, también han surgido nuevos desafíos, como el rastreo de usuarios a través de múltiples dispositivos y el uso de algoritmos avanzados para personalizar contenidos y publicidad. Estos avances tecnológicos han aumentado la capacidad de las redes sociales para recopilar y analizar datos, incrementando las preocupaciones sobre cómo se utiliza y se protege esta información.

El objetivo de esta investigación es analizar y explicar el uso de la información en la privacidad y seguridad de los usuarios en redes sociales, identificar sus principales amenazas y vulnerabilidades, y evaluar las medidas de protección vigentes. Este trabajo se propone explorar en detalle los desafíos y oportunidades relacionados con el manejo de la información, con la meta de contribuir al desarrollo de estrategias y políticas más efectivas en esta área crucial de la sociedad digital actual.

2. Materiales y Métodos

MATERIALES

El estudio se enfocó en la recolección y análisis de datos descriptivos sobre el uso de la información en la privacidad y seguridad de usuarios en redes sociales, se utilizaron las siguientes plataformas de redes sociales: Facebook, WhatsApp e Instagram. Estas plataformas fueron seleccionadas por su amplia base de usuarios y sus diversas características que impactan la privacidad y seguridad de los usuarios.

METODOLOGÍA

- Naturaleza de la Investigación: Se empleó un enfoque mixto combinando tanto enfoques cualitativos como cuantitativos. El enfoque cualitativo permitió obtener una comprensión profunda de las políticas y prácticas de privacidad y seguridad en redes sociales, mientras que el enfoque cuantitativo proporcionó datos empíricos y medibles para analizar el comportamiento y las percepciones de los usuarios.

- Tipo de Investigación: Se utilizó un enfoque descriptivo, lo que permitió explorar detalladamente las políticas y prácticas de privacidad y seguridad en redes sociales. El estudio se enfocó en recopilar información precisa sobre las prácticas

de privacidad y seguridad, proporcionando una visión clara de cómo estas fueron implementadas y percibidas por los usuarios de redes sociales.

- Diseño de la Investigación: El diseño utilizado fue no experimental y transversal, en el que los datos fueron recolectados en un único momento. Las encuestas aplicadas permitieron entender cómo los usuarios interactúan con las políticas de privacidad, perciben la seguridad de sus datos y responden a situaciones específicas en redes sociales. Además, se complementó con entrevistas y análisis documental para obtener una visión integral.

- Análisis de Datos: Se emplearon estadísticas descriptivas para resumir y presentar los datos obtenidos. Los resultados se presentaron gráficamente, describiendo las configuraciones de privacidad utilizadas por los usuarios en las distintas plataformas de redes sociales.

MÉTODO

Procedimiento

1. **Definición de la población:**
    - La población objetivo del estudio fue constituida por usuarios activos de redes sociales como Facebook, WhatsApp e Instagram, residentes del Municipio de Huichapan, y comunidades próximas, en el Estado de Hidalgo, México. Estos usuarios representan una variedad de características demográficas, incluyendo diferentes rangos de edad, géneros, niveles educativos y ubicaciones geográficas dentro de la región mencionada. Además, la población comprende usuarios que utilizan estas plataformas de manera habitual, permitiendo un análisis de sus comportamientos en relación con la privacidad y la seguridad en línea.

2. **Selección de la Muestra**:
    - Se seleccionaron 200 usuarios de la población, utilizando el método de muestreo probabilístico aleatorio simple, asegurando tanto la representatividad como la profundidad en la investigación.
    - El marco muestral estuvo conformado por usuarios activos de redes sociales residentes en el Municipio de Huichapan,Hgo., México y comunidades próximas.

3. **Recolección de Datos**:
    - Se recopilaron datos sobre las configuraciones de privacidad y seguridad de los usuarios, así como sus patrones de uso de las plataformas.
    - La recolección de datos se realizó a través de encuestas realizadas en Google Forms (https://forms.gle/cQiZokrd6Pc8RYwZ7) y análisis de perfiles de usuarios, así como análisis de documentación.

4. **Análisis Descriptivo de los Datos**:
    - **Evaluación de Configuraciones de Privacidad**:
      Se analizó cómo las configuraciones de privacidad afectan la visibilidad de la información del usuario en las redes sociales.

    - **Análisis de Autenticación y Encriptación**:
      Se evaluaron los métodos de autenticación utilizados por las redes sociales y las técnicas de encriptación empleadas para proteger los datos de los usuarios.

5. **Interpretación de Resultados**:
    - Los resultados obtenidos se interpretaron en función de la eficacia de las configuraciones de privacidad y seguridad para proteger la información del usuario.
    - Se analizaron las tendencias en el uso de configuraciones de privacidad y seguridad entre los diferentes grupos de usuarios.

3. Resultados

El uso de las redes sociales continúa creciendo rápidamente, y la cantidad de personas que utilizan la plataforma principal en cada país ha aumentado en casi 1 millón de nuevos usuarios cada día durante los últimos 12 meses. Más de 3 mil millones de personas en todo el mundo utilizan las redes sociales cada mes, y 9 de cada 10 de esos usuarios acceden a las plataformas elegidas a través de dispositivos móviles [14].

De acuerdo con los resultados obtenidos de las personas encuestadas en Huichapan, Hgo. México, la red social más utilizada es WhatsApp, un 61.5% de los usuarios la eligen de plataforma principal, seguida de Facebook, con el 50.5% de los usuarios e Instagram con un 37% de preferencia, (Figura 1). Estos datos revelan una clara preferencia de estas aplicaciones de mensajería y redes sociales, siendo herramientas esenciales para la comunicación y la interacción social.

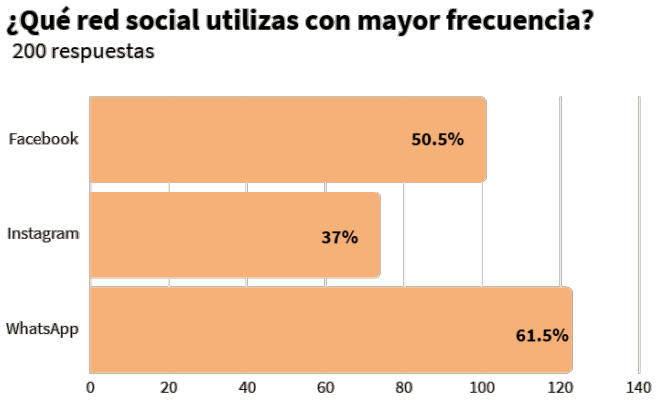

Figura 1. Red social más utilizada en Huichapan, Hgo., México. [Fuente: Propia]

Estos hallazgos se alinean con los resultados del Estudio sobre los Hábitos de Usuarios de Internet en México 2023 (Figura 2); donde WhatsApp también se destaca como la plataforma de redes sociales más utilizada a nivel nacional, con un 95.60% de usuarios, seguida de un 84.90% de usuarios en la plataforma Facebook e Instagram el tercero con un 76.20%. También muestra una alta adopción: YouTube y Twitter, con 59.30% y 55.80% respectivamente. LinkedIn, TikTok y Telegram siguen en la lista con participaciones del 49.60%, 44.20% y 41.90% respectivamente, mientras que Pinterest cierra con un 33.50% de usuarios. Estos datos reflejan una preferencia marcada por aplicaciones de mensajería instantánea y redes sociales visuales entre los usuarios de internet en México [15].

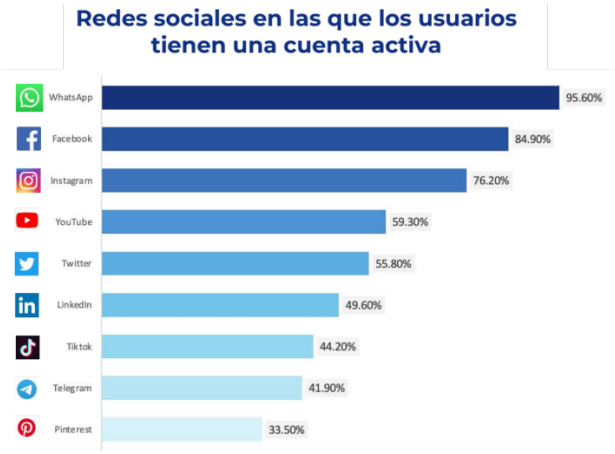

Figura 2. Redes sociales en las que los usuarios tienen una cuenta activa en México. [15]

En términos de conexión a redes sociales en Huichapan, Hgo. México (Figura 3); el 39% de los encuestados dedican entre 1 y 2 horas al día a las redes sociales. El 29.5% de las personas pasan entre 2 y 4 horas, mientras que el 20% pasan más de 4 horas al día en estas plataformas. Finalmente, el 11.5% dedica menos de una hora diaria a estas plataformas. Estos patrones de uso indican que una parte significativa de la población invierte una cantidad considerable de tiempo en redes sociales, lo que refuerza la importancia de estas plataformas en la vida cotidiana de los habitantes.

Figura 3. Tiempo promedio de conexión a redes sociales, Huichapan, Hgo., México [Fuente: Propia]

Comparando estos datos con el contexto nacional (Figura 4), el tiempo promedio de conexión a internet en México muestra que el 27.10% reporta estar conectados más de 9 horas al día. Un 23.20% se conecta de 3 a 5 horas diarias, mientras que el 22.00% lo hace entre 5 y 7 horas. Un 15.60% se conecta de 7 a 9 horas, y solo el 12.2% de los encuestados afirma tener un tiempo de conexión de al menos 1 a 3 horas. Estos datos indican que una parte significativa de la población pasa una considerable cantidad de tiempo en línea diariamente, con un 42.7% de los encuestados conectados entre 7 y más de 9 horas al día [15]. De las cuales, según el estudio "Cómo utilizan los mexicanos las redes sociales" realizado por Luis Ángel Hurtado Razo, académico de la Facultad de Ciencias Políticas y Sociales de la UNAM, aproximadamente seis horas se destinan al entretenimiento en redes sociales, lo que indica que la mayoría de los mexicanos destinan una cuarta parte del día a su uso [16].

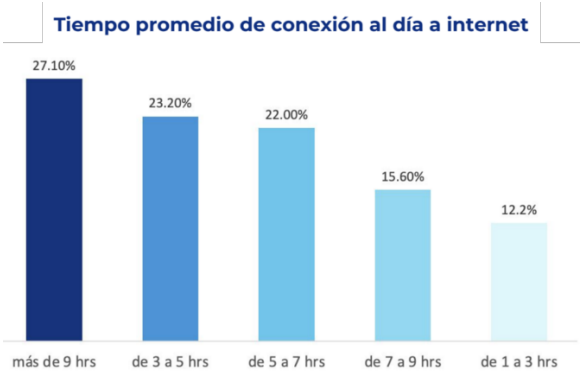

Figura 4. Tiempo promedio de conexión al día en internet en México. [15]

La comparación entre ambos estudios destaca diferencias significativas en los hábitos de conexión y uso de internet a nivel nacional versus local. A nivel nacional, una gran proporción de usuarios (42.7%) pasa más de 7 horas al día en internet, lo que sugiere una fuerte dependencia y uso intensivo de la red. En contraste, la encuesta local en Huichapan, Hgo., México muestra que la mayoría de los encuestados (68.5%) pasa entre 1 y 4 horas al día en redes sociales, indicando un uso más moderado de internet para este propósito específico.

Este uso prolongado aumenta la cantidad de información personal que los usuarios comparten en estas plataformas. Por lo que, en cuanto a la información compartida en redes sociales (Figura 5), la mayoría de los encuestados (65.5%) comparte fotos y videos personales, destacando una fuerte inclinación hacia la publicación de contenido visual de sus vidas. Un 61.5% divulgan su fecha de nacimiento, mientras que el 50.5% revela su nombre completo, demostrando una disposición a compartir detalles básicos de identidad. Sin embargo, solo un 34.5% comparte su número de teléfono, lo que plantea preocupaciones sobre la privacidad y la seguridad. El 25% comparte su dirección de correo electrónico, facilitando el contacto, pero aumentando el riesgo de spam o phishing. Menos común es la publicación de historial académico (15%) y perfiles familiares (6.5%), indicando una cautela creciente en la revelación de información más detallada. Solo un pequeño porcentaje revela su dirección física (5.5%), reflejando una mayor prudencia. Categorías como entretenimiento, actividades grupales y frases de superación tienen una participación mínima (0.5%), al igual que aquellos que eligen no utilizar información personal en redes sociales (0.5%). Apenas un 5% afirma no compartir ninguna información personal en redes sociales, mientras que solo el 1% comparte información sobre eventos institucionales, datos bancarios y/o compras. Reflexiones y fotografías representan también un 1% de las publicaciones.

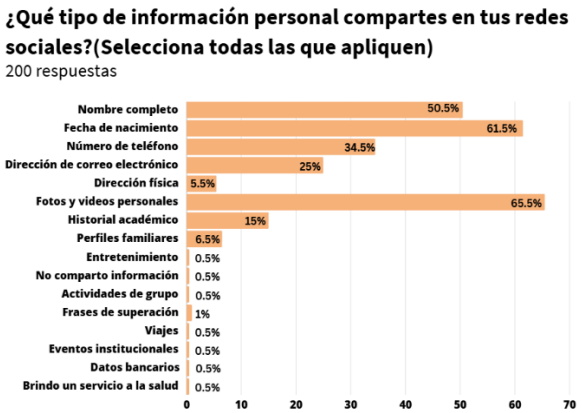

Figura 5. Información personal compartida por los usuarios, Huichapan, Hgo., México [Fuente: Propia]

En relación con estos datos, los usuarios muestran una tendencia a compartir principalmente contenido visual y detalles básicos de identidad, pero ejercen mayor cautela al compartir información sensible como direcciones físicas y datos financieros.

Este patrón refleja lo publicado en el estudio del artículo: "Sabes qué información compartes en las redes sociales" de la Universidad de Veracruz, donde menciona que los usuarios de redes sociales comparten diversos tipos de información personal y privada, incluyendo:

1. **Datos personales**: Muchos usuarios comparten información como direcciones, números de teléfono, cumpleaños y planes de vacaciones, lo que puede ser utilizado por cibercriminales para robar identidades o cometer fraudes financieros.
2. **Información sensible**: Casi un tercio de los usuarios comparten información sensible como fotos de niños sin permiso, detalles de viajes o información financiera.
3. **Mensajes y reservas**: Casi un tercio de los usuarios comparte sus mensajes y reservaciones con todos los que están en línea, no solo con sus amigos.
4. **Permisos de aplicaciones**: Las redes sociales permiten que aplicaciones de terceros accedan a información personal del usuario.
5. **Confianza en amigos**: Un cuarto de los usuarios hace clic en enlaces enviados por amigos sin verificar su contenido, lo que puede exponer su información [17].

Estas prácticas de compartir información personal se vinculan con los principales usos que se les dan a las redes sociales (Figura 6); los cuales se centran en tres tipos de actividades: acceso a la información, contacto social y económica. En el primer caso, predomina la búsqueda de información (77%) y el consumo de contenidos de entretenimiento (62.60%). En el segundo caso, destacan el contacto con familiares y amigos (76.80%), y con colegas del trabajo (44.70%). En el tercer caso, el uso de redes está orientado a buscar recomendaciones de productos (35.60%), comprar artículos (33.50%), ofrecer y recibir servicios profesionales (26.40% y 22.50%, respectivamente), y buscar empleo (16%) [15].

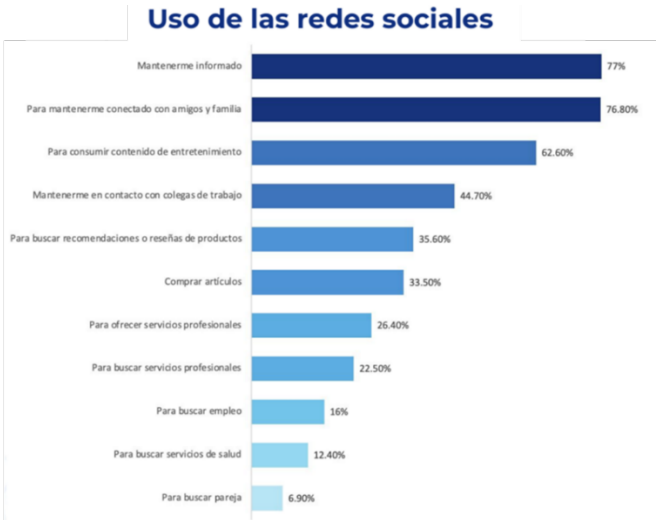

Figura 6. Uso de las redes sociales en México [15]

En México, de los 97 millones de usuarios de internet, el 81.50% identifican el robo de datos personales como el principal riesgo de navegación. Mientras que el 58% de cibernautas menciona la invasión de la privacidad entre las principales vulneraciones de ciberseguridad en México, de acuerdo con la Asociación de Internet MX (AIMX). Prácticamente el 40% de incidencias reportadas en 2023 lo fue por suplantación de identidad y 13% experimentó fuga de información sensible. Ambas situaciones,

relacionadas con los datos personales [18]. Estos incidentes han aumentado significativamente, con los casos reportados pasando de 505 en 2022 a mil 607 en 2023 de los cuales el 62% se debió a hackeo de redes sociales, según datos del Consejo Ciudadano [19].

En la (Figura 7), se muestran los principales riesgos que preocupan a los usuarios en el ámbito digital. El robo de datos personales es la mayor preocupación, afectando al 81.50% de los usuarios. Le siguen el miedo a recibir virus en el dispositivo (58.40%) y la invasión a la privacidad (57.60%). Otros riesgos importantes incluyen el fraude (52.30%), las noticias falsas (26.50%), recibir contenidos desagradables o inadecuados (24.60%) y el ciberacoso (21%).

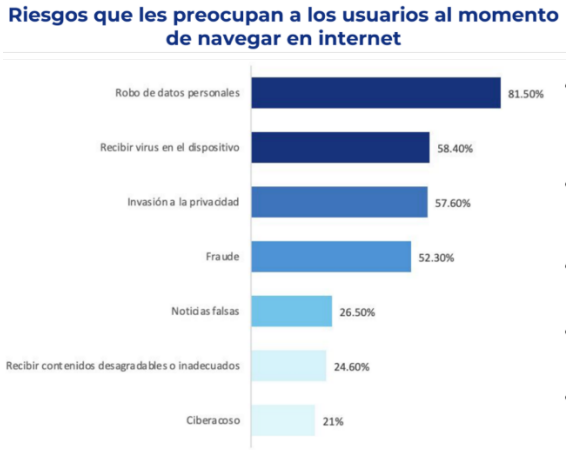

Figura 7. Riesgos que le preocupan a los usuarios al navegar online en México [15]

Respecto a experiencias personales de violaciones de privacidad en redes sociales en usuarios de Huichapan, Hgo., México (Figura 8); el 86.5% de los encuestados indicó no haber experimentado ninguna violación de privacidad, mientras que el 13.5% afirmó haber sufrido alguna forma de violación. Entre las violaciones reportadas se encuentran la suplantación de identidad, el hackeo de cuentas, el uso indebido de fotos de Instagram para crear cuentas falsas y estafar a amigos, el robo de cuentas y de identidad, intentos de ingreso ajeno en cuentas personales, el uso de información personal para otros fines y acoso.

Figura 8. Porcentaje de casos de violación de privacidad en usuarios, Huichapan,Hgo, México [Fuente: Propia]

En ambas graficas se observa la preocupación por los riesgos al navegar por internet y las experiencias reales de violaciones de privacidad en redes sociales. En la primera gráfica destaca las principales preocupaciones de los usuarios a nivel nacional, centrándose en el

robo de datos personales como el riesgo más significativo, mientras que la segunda gráfica ofrece una perspectiva más concreta sobre las violaciones de privacidad experimentadas por los usuarios en la localidad de Huichapan, Hidalgo, México. Aunque los usuarios están altamente preocupados por ciertos riesgos, no todos han experimentado estos problemas directamente en sus interacciones diarias en redes sociales, pasando por desapercibido el uso o robo de su información.

4. Discusión

Los hallazgos muestran que las redes sociales manejan una vasta cantidad de datos personales, y la adherencia a regulaciones como el Reglamento General de Protección de Datos (GDPR) es crucial para garantizar la protección de la privacidad del usuario [21]. Las plataformas deben implementar medidas claras para el manejo y protección de estos datos, asegurando el cumplimiento de normativas internacionales o nacionales sobre el manejo y protección de información.

Por otro lado, los resultados muestran que los algoritmos de personalización impactan la privacidad del usuario porque recolectan y analizan datos para determinar preferencias y comportamientos. Esto tiene relación con lo que dice Newberry (2024) que describe cómo los algoritmos en redes sociales personalizan y distribuyen contenido basado en la probabilidad de interacción del usuario [22]. Esto subraya la importancia de entender y gestionar los algoritmos para proteger la privacidad de los usuarios.

Un dato significativo observado en las encuestas está relacionado al nivel de preocupación de los usuarios sobre la privacidad de sus datos personales compartidos en las redes sociales. La (Figura 9), muestra el nivel de preocupación en una escala del 1 al 5, donde 1 es "No me preocupa" y 5 es "Muy preocupado". Se observa que 44 personas se encuentran en el nivel 5 de preocupación, mientras que 39 están en el nivel 4, lo que indica una gran inquietud por la privacidad de sus datos personales. Sin embargo, 57 usuarios son indiferentes al manejo y la privacidad de su información, ubicándose en el nivel 3. Los niveles 2 y 1, con 37 y 23 usuarios respectivamente, representan a aquellos que menos se preocupan por estos aspectos, teniendo una menor representación.

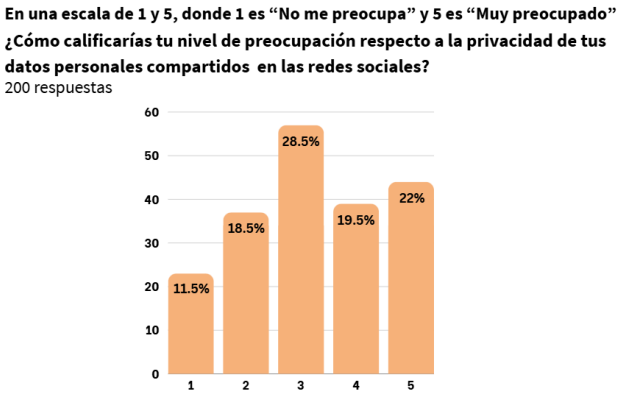

Figura 9. Nivel de preocupación respecto a la privacidad de los datos personales en redes sociales, Huichapan, Hgo. México [Fuente: Propia]

Este dato es crucial porque muestra que la mayoría de los usuarios están conscientes y preocupados por cómo se manejan sus datos personales en las redes sociales (44 más 39 usuarios).

Por otra parte, se destaca en la Figura 10, que un porcentaje considerable de los encuestados no leen las políticas de seguridad y privacidad (22%), un 58% solo las leen ocasionalmente, lo que genera una brecha del 80% en el desconocimiento real de estas políticas, poniendo en desventaja al usuario final. Una posible área de oportunidad es sintetizar o mostrar de forma puntual las características relevantes de las políticas de privacidad y seguridad; independientemente del contenido estos documentos legales regulan la recolección, uso y protección de datos personales (Grupo Adaptalia, 2024) [23]. Por lo tanto, deben de ser claras y accesibles sobre el manejo de los datos de los usuarios, ya que esto permitirá construir confianza y garantizar la seguridad de la información personal.

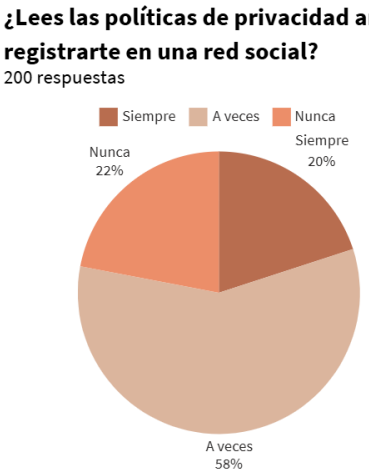

Figura 10. Porcentaje de personas que leen las políticas de privacidad y seguridad, Huichapan, Hgo. México [Fuente: Propia]

Además de la preocupación por la privacidad, también se evaluó el nivel de satisfacción de los usuarios con las políticas de privacidad y medidas de seguridad implementadas por las redes sociales que utilizan (Figura 11). Un 62.5% de los encuestados se sienten insatisfechos con las políticas actuales, un 23.5% manifiestan estar poco satisfechos, un 8% se declaran satisfechos y solo un 6% indican estar muy satisfechos.

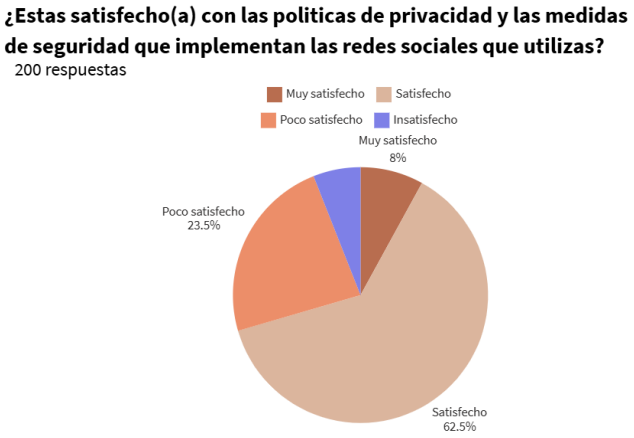

Figura 11. Porcentaje de satisfacción con respecto a las políticas de privacidad y seguridad, Huichapan, Hgo. México [Fuente: Propia]

Frente a las estadísticas preocupantes sobre el uso o robo de información personal de los usuarios, el Estudio de Consumo de Medios y Dispositivos entre Internautas Mexicanos 2021 (Figura 12); revela que el 59% de los internautas consideran que necesitan verificar y aumentar las medidas de seguridad en internet. Un 26% cree que su información está 100% segura en internet, mientras que el 15% considera que su información está altamente

vulnerable. Para proteger su información, el 69% verifica que el sitio cuente con certificado de seguridad, un 56% asegura utilizar una red segura, y un 36% verifica en otras fuentes la información que les parece dudosa. Además, el 28% reporta mensajes o correos electrónicos no confiables. Sin embargo, un 6% no tiene conocimiento de cómo proteger su información, y un 1% nunca verifica la información. Estos datos reflejan una preocupación significativa entre los usuarios por la seguridad de su información en línea y la necesidad de adoptar medidas proactivas para protegerla [24].

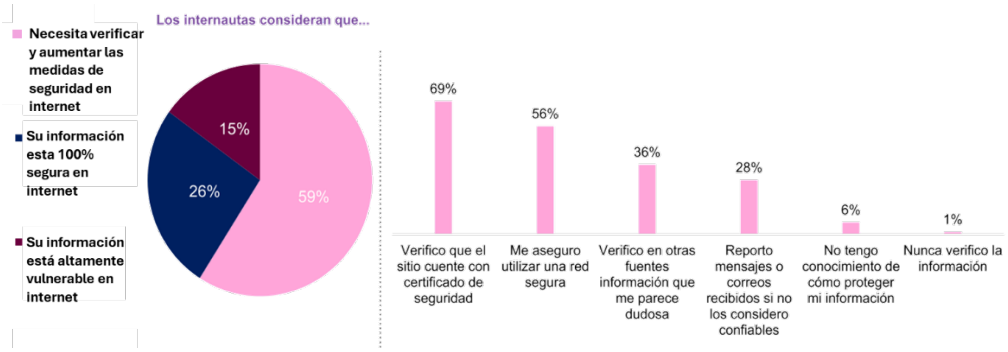

Figura 12. Acciones tomadas para proteger la información personal en redes sociales en México [20]

De acuerdo con el estudio de los usuarios en Huichapan, Hgo. México (Figura 13), un 80% de los encuestados mencionan que utilizan contraseñas fuertes para proteger su información personal en las redes sociales. Además, el 67% de los usuarios indica que limitan la cantidad de información personal que comparten. Un 54.5% no acepta solicitudes de amistad de desconocidos, mientras que el 41.5% habilita la autenticación de dos factores para mayor seguridad. Asimismo, el 39% revisa y ajusta regularmente su configuración de privacidad. Finalmente, un 0.5% de los encuestados aplica el uso de cambios constantes de contraseñas.

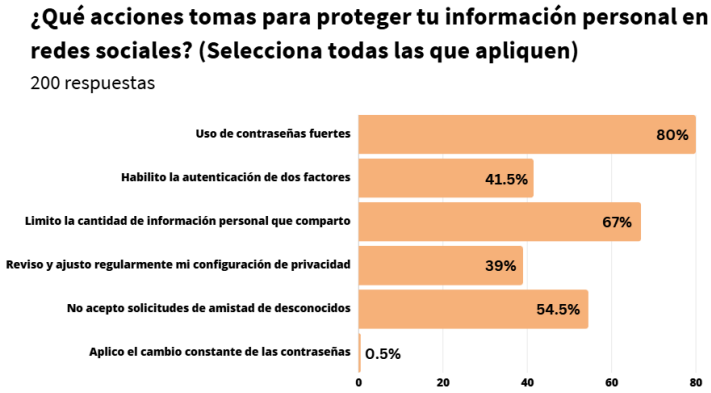

Figura 13. Acciones tomadas para proteger información personal en redes sociales, Huichapan, Hgo. México [Fuente: Propia]

Estos estudios reflejan una conciencia significativa entre los usuarios mexicanos sobre la importancia de proteger su información personal en línea. Sin embargo, mientras que el estudio nacional sugiere una preocupación más amplia y generalizada con respecto a la seguridad en internet, el estudio local muestra prácticas más específicas y detalladas que los usuarios implementan para protegerse. Esto indica que, aunque existe una preocupación generalizada, las prácticas concretas de seguridad varían según el contexto local y las prácticas individuales de los usuarios.

Estos resultados también destacan la importancia crucial de implementar métodos de autenticación robustos y encriptación de datos para proteger la información personal de los usuarios en las redes sociales. En concordancia con Cloudflare (2024), es esencial enfatizar la relevancia de la autenticación y la encriptación para garantizar la seguridad de la información. Igualmente, es crucial gestionar adecuadamente la identidad digital para salvaguardar la privacidad y seguridad del usuario [25-26].

5. Conclusiones y limitaciones

"El conocimiento es poder" (Francis Bacon, 1597) Hoy en día, internet es la mayor fuente de información que tenemos disponible, al alcance no solo de cualquier persona, sino de grandes empresas y organizaciones que cuentan con las herramientas para analizar y procesar este inmenso volumen de información [27]. En este sentido, en el mundo de la información digital, si no estás pagando por un producto, eres el producto. Si las empresas continúan incrementando la cantidad de datos que almacenan sobre los individuos, los datos en sí se convierten en un producto a la venta y, si los individuos no protegen la información que divulgan, corren el riesgo de que sus datos se vendan al mejor postor.

Los datos recolectados en esta investigación muestran el creciente protagonismo de las redes sociales en la vida cotidiana, tanto a nivel local como nacional. Plataformas como WhatsApp, Facebook e Instagram se destacan como las más utilizadas, con una inversión significativa de tiempo por parte de los usuarios. Esto resalta la importancia de estas herramientas para la comunicación y el entretenimiento. Sin embargo, también emergen preocupaciones sobre la privacidad y la seguridad de la información personal compartida en estas plataformas. Aunque la mayoría de los usuarios están dispuestos a compartir contenido visual y datos básicos, muestran mayor cautela al divulgar información sensible, como números de teléfono y direcciones. Esta actitud refleja una creciente conciencia sobre los riesgos asociados a la seguridad en línea. A pesar de ello, persiste una brecha considerable en el conocimiento y comprensión de las políticas de privacidad, lo que deja a muchos usuarios expuestos a vulnerabilidades.

Los resultados también revelan que, aunque muchos usuarios se sienten insatisfechos con las políticas de seguridad actuales, la mayoría ha adoptado medidas preventivas básicas, como el uso de contraseñas fuertes y la limitación de la información personal que comparten. No obstante, la implementación de medidas de seguridad más avanzadas, como la autenticación de dos factores, aún no es ampliamente utilizada. En conjunto, estos hallazgos destacan la necesidad de que tanto las plataformas como los usuarios incrementen sus esfuerzos por proteger la privacidad de los datos personales. Es crucial que las empresas gestionen de manera transparente los datos y los algoritmos que emplean, garantizando la seguridad y fomentando un entorno digital más confiable para los usuarios.

La investigación también sugiere áreas para estudios futuros, incluyendo temas como:

- Impacto de la personalización de contenido en el comportamiento de los usuarios.
- Impacto de las violaciones de datos en la confianza de los usuarios.
- Uso de las principales plataformas de redes sociales en menores de edad.
- Riesgos y consecuencias del robo de identidad en redes sociales y plataformas.
- Generación de mecanismos o herramientas de encriptación y algoritmos para la seguridad de información.

Contribución: Todos los autores participaron en la lectura y aprobación de la versión final del manuscrito. La autoría se limita a aquellos que contribuyeron sustancialmente al trabajo reportado.

Financiamiento: Esta investigación no recibió financiamiento externo.

Conflicto de interés: Los autores declaran no tener conflictos de interés que puedan influir en la representación o interpretación de los resultados de investigación presentados.

Referencias

1. Subramanian, A., Kessler, M. The Hyperglobalization of Trade and its Future. Global Citizen Foundation, June, 2013, 76 p. (http://www.gcf.ch/wp-content/uploads/2013/06/GCF_Subramanian-working-paper-3_-6.17.13.pdf)
2. Simoens, P., De Turck, F., Dhoedt, B., Demeester, P. Remote Display Solution for Mobile Cloud Com-puting. Computer, August, 2011, pp.46-53.
3. Garber, L. The Challenges of Securing the Virtualized Environment. Computer, January, 2012, pp.17-23.
4. European Commission – Eurostat. ICT Security in Enterprises. International Journal on Information Technologies and Security (ijits-bg.com), 2 (vol. 3), 2011, pp.45-54.
5. Lampe, C., Ellison, N. Understanding Facebook: Social Computing isn't 'Just' Social. Computer, September, 2012, pp.98-100.
6. Lam, S. K., Riedl, J. Are Our Online „Friend" Really Friends? Computer, January, 2012, pp.91-93.
7. Frigyes Karinthy "Chains" 1929; Teoría reafirmada actualmente por el sociólogo Duncan J. Watts en "Six Degrees: The Science of a Connected Age" Ed. Norton, 2004
8. Kietzmann, J. H., Hermkens, K. Social Media? Get Serious! Understanding the Functional Building Blocks of Social Media. Business Horizons, vol. 54, 2011,pp.241-251
9. Edu.co ¿Qué hacen las redes sociales con los datos de sus usuarios?. Disponible en: https://www.unisabana.edu.co/portaldenoticias/al-dia/que-hacen-las-redes-sociales-con-mis-datos/
10. FAN, L.; LI, B. (2008). «VisoLink: A User-Centric Social Relationship Mining». En: G. WANG [et al.] (eds.). Lecture Notes in Artificial Intelligence. N.º 5009, pág. 668-675.
11. Silicon Technology Powering Business . (19 de Mayo de 2016). El robo de datos de LinkedIn en 2012 alcanza ahora a 100 millones de usuarios. Disponible en: El robo de datos de LinkedIn en 2012 alcanza ahora a 100 millones de usuarios | Silicon
12. FastCompany. (13 de Diciembre de 2018). How our data got hacked, scandalized and abused in 2018. Disponible en: How our data got hacked, scandalized, and abused in 2018 - Fast Company
13. The Verge. (18 de Abril de 2019). Facebook stored millions of Instagram passwords in plain text. Disponible en: El robo de datos de LinkedIn en 2012 alcanza ahora a 100 millones de usuarios | Silicon (theverge.com)
14. We are social. (30 de Enero de 2018). DIGITAL IN 2018: WORLD'S INTERNET USERS PASS THE 4 BILLION MARK. Disponible en: Facebook stored millions of Instagram passwords in plain text - The Verge (wearesocial.com).
15. Asociación de Internet MX (2023). 19° Estudio sobre los hábitos de usuarios de internet en México 2023. Disponible en: Estudios de Hábitos de Internet en México | AIMX (asociaciondeinternet.mx)
16. Staff F.(30 de Junio de 2023). Mexicanos destinan 6 horas del día en entretenimiento en redes sociales: experto. Disponible en: Mexicanos destinan 6 horas del día en entretenimiento en redes sociales: experto (forbes.com.mx)
17. Gutiérrez Amaya C. (2024) Conocimientos generales: Sabes qué información compartes en las redes sociales. Disponible en: Conocimientos generales: Sabes qué información compartes en las redes sociales – Seguridad de la información (uv.mx)
18. Padua, M. (2024, abril 18). Protección de datos: lo que las organizaciones deben saber. IT Masters Mag. Disponible en: https://www.itmastersmag.com/ciberseguridad/proteccion-de-datos-personales-en-mexico/
19. Consejo Ciudadano Para La Seguridad y Justicia de La Ciudad de México. SUBEN 218% REPORTES POR ROBO DE IDENTIDAD. Disponible en: https://consejociudadanomx.org/contenido/suben-218-reportes-por-robo-de-identidad
20. Morales, J. A. y Barroso, J (2012). LAS REDES SOCIALES EN EL AMBITO UNIVERSITARIO. Redes Educativas: La Educación en la Sociedad del Conocimiento.
21. Your Europe (7 de Junio de 2022). Protección de datos conforme al reglamento RGPD. Disponible en: Protección de Datos conforme al reglamento RGPD - Your Europe (europa.eu)
22. Newberry, C. (22 de Abril de 2024). Algoritmos de las redes sociales: la guía para todas las redes en 2024. Disponible en: https://blog.hootsuite.com/es/algoritmos-de-las-redes-sociales/
23. Grupo Adaptalia. (28 de Mayo de 2024). Política de privacidad. Disponible en: https://grupoadaptalia.es/blog/que-es-y-como-funciona-la-politica-de-privacidad/
24. México, I. A. B. (2021, septiembre 28). Estudio de Consumo de Medios y Dispositivos entre Internautas Mexicanos 2021. IAB México - El Interactive Advertising Bureau (IAB) es la asociación que agrupa a las empresas de la publicidad interactiva de

los principales mercados del mundo. Disponible en: https://www.iabmexico.com/estudios/estudio-de-consumo-de-medios-y-dispositivos-entre-internautas-mexicanos-2021/

25. CLOUDFLARE. (2024). ¿Qué es la Autenticación? Disponible en: https://www.cloudflare.com/es-es/learning/access-management/what-is-authentication/
26. CLOUDFLARE. (2024). ¿Qué es la encriptación? Disponible en: https://www.cloudflare.com/es-es/learning/ssl/what-is-encryption/
27. Itbacking, S.L. (20 de abril de 2020). ¿Qué es el Business Intelligence? Definición y beneficios. Disponible en: https://www.itbacking.com/que-es-bussines-intelligence-y-como-puede-beneficiar-a-tu-negocio/