



EL MUNDO DE LAS REDES SOCIALES Y LA CIBERSEGURIDAD EN AMÉRICA LATINA

THE WORLD OF SOCIAL NETWORKS AND CYBERSECURITY IN LATINO AMERICA

¹Kevin Daniel Barrera Quintero

²Carol Natalia Cortes Gutierrez

³Betsy Melisa Gil Reyes

RESUMEN

El presente estudio analiza la estrategia de ciberseguridad y su implementación en la navegación de redes sociales en América Latina durante los últimos cuatro años. Se empleó una metodología descriptiva, basada en el análisis de 35 fuentes, entre ellas revistas científicas, libros, noticias y documentos gubernamentales que abordan temas relacionados con redes sociales, ciberseguridad y confiabilidad de los usuarios. Los resultados evidencian los principales riesgos y políticas de ciberdelincuencia en redes sociales, así como los objetivos de los distintos tipos de ataques y las tendencias asociadas al uso masivo de tecnologías en la región. Asimismo, se identifican buenas prácticas para una navegación segura, destacando la importancia de fortalecer la conciencia del usuario, proteger la información personal y garantizar la supervisión de menores. Todo ello con el fin de reducir la incidencia de estafas, abusos y otras formas de vulneración derivadas del desconocimiento y la falta de prevención.

PALABRAS CLAVE: ciberdelincuentes, ciberataques, malware, ransomware, phishing.

ABSTRACT

This study analyzes cybersecurity strategies and their implementation in social media navigation in Latin America over the past four years. A descriptive methodology was used, based on the analysis of 35 sources, including scientific journals, books, news articles, and government documents addressing topics related to social media, cybersecurity, and user reliability. The results reveal the main risks and cybercrime policies on social media, as well as the objectives of different types of attacks and the trends associated with the widespread use of technology in the region. Additionally, best practices for safe

¹Tecnólogo en Desarrollo de Software, Corporación Tecnológica Industrial Colombiana, estudiante Ingeniería de sistemas, Bogotá, Colombia, 1073526051@teinco.edu.co

²Tecnólogo en Análisis y Desarrollo de Sistemas de Información, Corporación Tecnológica Industrial Colombiana, estudiante Ingeniería de sistemas, Bogotá, Colombia, 1024589669@teinco.edu.co

³Tecnólogo en Informática, Corporación Tecnológica Industrial Colombiana, estudiante Ingeniería de sistemas, Bogotá, Colombia, 1010190304@teinco.edu.co

navigation are identified, highlighting the importance of strengthening user awareness, protecting personal information, and ensuring the supervision of minors. All of this aims to reduce the incidence of scams, abuse, and other forms of harm resulting from lack of knowledge and insufficient preventive measures.

KEYWORDS: cybercriminals, cyberattacks, malware, ransomware, phishing.

INTRODUCCIÓN

Actualmente, los avances tecnológicos vinculados a la globalización en diversas disciplinas del conocimiento han generado un impacto significativo en la sociedad y en las formas de comunicación utilizadas durante años. Un ejemplo claro de ello es el uso de las redes sociales, las cuales, desde su aparición, se han convertido en uno de los principales medios de comunicación, reemplazando métodos tradicionales como las llamadas telefónicas, las conversaciones presenciales prolongadas o la interacción directa con familiares y amigos sin la mediación de dispositivos tecnológicos. De esta manera, los métodos convencionales de comunicación han ido transformándose y la sociedad ha incursionado en el auge de las tendencias tecnológicas y el uso intensivo de redes sociales (Rahman et al., 2016).

En este contexto, puede afirmarse que las nuevas formas de comunicación han evolucionado y que la experiencia en el uso de redes sociales ha incrementado el número de usuarios activos. Martínez y Ávila (2021) sostienen que “la introducción de Facebook, Twitter, YouTube, LinkedIn e Instagram constituye, sin lugar a dudas, una de las formas más novedosas de comunicación” (p. 212).

Más allá de funcionar como un medio de comunicación, las redes sociales se han consolidado como herramientas de trabajo y como una fuente importante de ingresos para muchas personas. Esto incluye quienes promocionan sus emprendimientos o negocios y quienes se desempeñan como *influencers*, entendidos como “una persona que posee cierta credibilidad sobre un tema concreto y cuya presencia e influencia en las redes sociales la convierte en un prescriptor idóneo de una marca determinada” (Gómez, 2018, p. 149).

No obstante, el uso de redes sociales también requiere precaución, pues implica riesgos como ataques cibernéticos, vulneración de la información personal y la necesidad de implementar mecanismos de seguridad adecuados. En Latinoamérica, la ciberseguridad y la navegación en redes sociales han experimentado transformaciones significativas, debido a que dichas plataformas se han convertido en canales esenciales de comunicación y operación. El creciente uso diario de la tecnología y de la información que esta contiene ha incrementado la exposición de los usuarios a ataques perpetrados por ciberdelincuentes.

El presente trabajo tiene como propósito analizar la problemática relacionada con el limitado conocimiento que poseen los usuarios frecuentes de redes sociales sobre los riesgos a los que están expuestos, así como las estrategias para prevenir ataques o brechas que faciliten las acciones de los ciberdelincuentes. En particular, el artículo se enfoca en el análisis de estrategias de ciberseguridad y su implementación en la navegación de redes sociales en países latinoamericanos durante el período comprendido entre 2019 y 2022.

Según Carreño (2021), las tácticas más comunes empleadas por los ciberdelincuentes incluyen ataques mediante *malware*, definido como “un software que interfiere con el propósito de dañar al usuario del ordenador. El objetivo es robar datos personales, financieros y/o comerciales” (Oracle, 2022, párr. 1), y *ransomware*, entendido como software malicioso que secuestra archivos y exige un pago para su recuperación (Avast, 2022). Asimismo, se identifican riesgos como la violación de datos personales, el hurto por medios informáticos y la manipulación de la opinión pública a través de redes sociales.

El uso inadecuado de estas plataformas puede poner en riesgo la integridad de los usuarios si no se adoptan medidas de seguridad apropiadas.

Es relevante señalar que el 72 % de los latinoamericanos utiliza redes sociales (véase tabla1). Durante el primer año de confinamiento por la pandemia, a medida que aumentaba la conectividad, también se incrementaba la vulnerabilidad ante estafas de ingeniería social. Una de las modalidades más comunes es el *phishing*, consistente en obtener información sensible del usuario —como números de tarjetas de crédito— para utilizarla de manera fraudulenta. El estafador, conocido como *phisher*, emplea técnicas de ingeniería social haciéndose pasar por una persona o empresa de confianza y contactando al usuario mediante un formato electrónico, generalmente un correo idéntico al enviado por fuentes legítimas (Acens Technologies, s.f.). Esta modalidad suele manifestarse en correos desconocidos que contienen información llamativa para el receptor y que incluyen un enlace que, al ser activado, permite al ciberdelincuente acceder a información personal, contraseñas y otros datos sensibles, facilitando la comisión de actos delictivos.

Tabla 1. Usabilidad de redes sociales en Latinoamérica

PAÍS	PORCENTAJE
Brasil	15.37%
Ecuador	13.36%
Panamá	12.60%
Chile	11.90%
Colombia	11.90%
Perú	10.30%
Guatemala	10.21%
México	9.41%
Argentina	9.17%
Costa Rica	7.64%

Nota. Elaboración propia. Adaptado de Díaz, H. (2021). *Las redes sociales son utilizadas por el 72% de los latinoamericanos como fuente de información*. Kaspersky. <https://latam.kaspersky.com/blog/las-redes-sociales-son-utilizadas-por-el-72-de-los-latinoamericanos-como-fuente-de-informacion-segun-estudio-de-kaspersky/23038/>

La información presentada corresponde a un periodo de un año, comprendido entre marzo de 2021 y marzo de 2022. Durante este tiempo, el *phishing* se ha consolidado como una de las tácticas más utilizadas para atacar redes sociales. Garzón (2021) afirma que:

En América Latina y el Caribe, el 51 % de los niños entre 3 y 17 años tiene acceso a internet en casa, según un estudio de UNICEF. Esto significa que alrededor de 77 millones de niños podrían acceder a cualquier tipo de contenido, desde información para clases escolares hasta sitios web maliciosos y posibles ataques cibernéticos (párr. 1).

Estos datos evidencian que navegar en internet o interactuar en redes sociales ya no es completamente seguro. El riesgo de que la información personal sea vulnerada es elevado, y la probabilidad de sufrir algún ataque cibernético se ha incrementado notablemente. Actualmente, los ciberataques se intensifican conforme aumenta la cantidad de información disponible en redes sociales, incluyendo datos personales, ubicaciones, propiedades y fotografías. Esta situación hace que los usuarios sean más susceptibles a suplantaciones, amenazas o estafas por parte de ciberdelincuentes.

Un caso particularmente preocupante es el *child grooming*, en el cual un adulto oculta su identidad y establece una relación de confianza con un menor de edad, ejerciendo control emocional con el propósito de abusar física o psicológicamente del menor.

Finalmente, Sack (2021) destaca la evolución de las amenazas de ciberseguridad en Latinoamérica desde el inicio del confinamiento por la pandemia. Durante este periodo, se implementaron modalidades de trabajo remoto y educación virtual, además del surgimiento de nuevas redes sociales, lo que produjo un aumento masivo de usuarios registrados y activos. A su vez, los cibercriminales continúan desarrollando métodos y estrategias para ejecutar ataques dirigidos a estafar, robar información y causar daños a los usuarios.

METODOLOGÍA

Para el desarrollo de este artículo de reflexión, se realizó un análisis documental y exploratorio, entendido como una metodología que permite investigar un tema que no ha sido abordado en profundidad o que no ha recibido suficiente atención dentro del ámbito académico. En el caso de esta investigación, si bien se reconoce la existencia de los ataques cibernéticos, no se ha profundizado de manera precisa en estrategias efectivas para abordar esta problemática (Baptista & Sampieri, 2014).

Asimismo, el estudio se desarrolló con un enfoque cualitativo, definido por Toro (s.f.) como “cualquier tipo de investigación que produce hallazgos a los que no se llega por medio de procedimientos estadísticos u otros medios de cuantificación” (como se cita en Ortega & Traverso, 2021, p. 160). Bajo este enfoque, se llevó a cabo una búsqueda y revisión de diversas fuentes de información, incluyendo revistas científicas, libros, artículos periodísticos y documentos publicados en páginas gubernamentales.

La recopilación de información se realizó tomando como referencia una ventana temporal de seis años, seleccionando documentos que abordaran temáticas relacionadas con redes sociales, ciberseguridad y la confiabilidad de los usuarios.

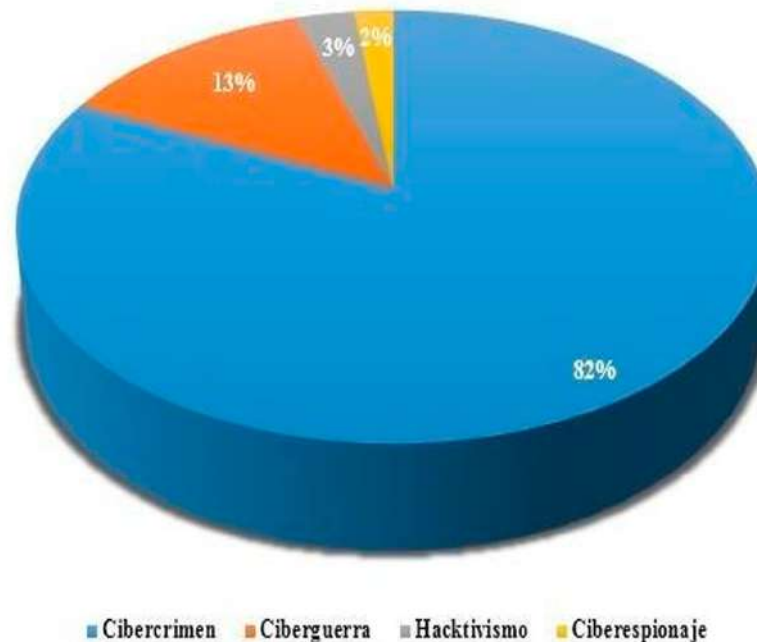
Riesgos y políticas de ciberseguridad en américa latina en el uso de las redes sociales

En lo que respecta a las políticas de ciberseguridad, estas han representado un gran desafío debido a la constante evolución y transformación de las tecnologías digitales. Sin embargo, es importante resaltar el trabajo desarrollado por la Organización de los Estados Americanos (OEA), que formuló una estrategia de alcance internacional orientada a fortalecer la seguridad cibernética en la región. Adicionalmente, Cornaglia y Vercelli (2017) señalan que algunos países de América Latina han logrado consolidar “una política de ciberseguridad, que forma parte de una tendencia creciente de la importancia del tema en la región” (como se cita en Aguilar, 2019, p. 25).

A pesar de estos avances, la rápida evolución tecnológica ha incrementado la frecuencia y complejidad de los ataques cibernéticos, convirtiéndolos en una amenaza significativa para la sociedad y para los usuarios habituales de redes sociales e internet. De acuerdo con Aguilar (2019), los ciberdelincuentes orientan sus objetivos tanto hacia entidades públicas y

privadas como hacia usuarios individuales. Entre las amenazas más comunes se encuentran los ataques de *watering-hole*, *spear-phishing*, malware y troyanos, los cuales son empleados principalmente para cometer fraudes contra entidades financieras, evidenciando una tendencia global en el panorama de la ciberdelincuencia (véase figura 1).

Figura 1. Motivaciones cibernéticas a nivel global



Nota. Elaboración propia. Adaptado de Aguilar, J. (2019). *Hechos ciberfísicos: Una propuesta de análisis para ciberamenazas en las Estrategias Nacionales de Ciberseguridad*. <https://doi.org/10.17141/urvio.25.2019.4007>

Es importante mencionar que los diferentes tipos de riesgos y ciberataques más frecuentes en América Latina tienen como objetivo principal el robo de información sensible y confidencial. Esto se refleja en la gráfica, la cual indica, de menor a mayor, el porcentaje de ataques según su impacto y facilita su identificación. Además, el 82 % de los ataques corresponden a delitos cibernéticos vinculados a “instituciones públicas o gubernamentales, como el ciberespionaje o hacktivismo” (Pessiri, 2019, como se cita en Aguilar, 2019, p. 26). Sin embargo, Aguilar (2019) aclara que hasta el momento no se ha reportado en América Latina ningún ataque cibernético de gran relevancia que involucre a entidades de alto perfil.

Por otra parte, las redes sociales fueron creadas para interactuar y establecer relaciones con personas conocidas, como familiares, compañeros de trabajo o amigos, así como con desconocidos registrados en la misma plataforma. Esto ha llevado a un intercambio constante de mensajes e información, incrementando el número de usuarios activos. No obstante, toda la información compartida está expuesta a numerosos riesgos, por lo que es fundamental que los usuarios conozcan las políticas de seguridad, los riesgos existentes y las buenas prácticas para proteger su información personal.

Duarte (2019) indica que países latinoamericanos como Colombia, Brasil, México y Argentina destacan por el tiempo de navegación diaria en redes sociales, con un rango promedio de 190 a 225 minutos. Por su parte, López (2018) señala que, según la Secretaría de Economía, más de 258 millones de personas en la región están expuestas a vulnerabilidades y riesgos de seguridad, principalmente mediante estafas basadas en ingeniería social. En respuesta, la Asociación de Informática de Argentina ha reforzado la seguridad de sus servidores y desarrollado estrategias para exponer métodos de robo de información y prevenir que otros usuarios caigan en estas trampas.

Pons (2017) destaca que, debido al avance tecnológico en Latinoamérica, se han registrado 40.864 incidentes de ciberataques, siendo las redes sociales el principal objetivo de los delincuentes para sustraer información de los usuarios. Rodríguez (2017) señala que los ciberataques entre estados se han convertido en un fenómeno recurrente, y la implementación de tecnologías como drones ha transformado la ciberseguridad. Organizaciones como la OTAN han desarrollado planes de contingencia para proteger sus servidores y evitar la transmisión masiva de información con virus provenientes de ciberdelincuentes internacionales.

Asimismo, Jurado, Yarad y Carrión (2020) destacan que la relación entre empresas y redes sociales implica un riesgo significativo. La mayoría de las organizaciones gestionan cuentas corporativas con numerosos seguidores, interactuando con clientes y ofreciendo servicios. Esto requiere la implementación de equipos de seguridad que monitoreen las cuentas, dado que se han reportado ataques a perfiles empresariales que afectan la reputación de la organización y pueden perjudicar a sus clientes (BBC News Mundo, 2019).

El Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC, 2020) ha propuesto diez recomendaciones para prevenir riesgos en el entorno digital, basadas en estadísticas y protocolos de protección de los usuarios. Asimismo, establece procesos de control y seguimiento que garantizan la integridad y privacidad de la información. Sánchez (2020) señala que los países latinoamericanos han implementado procesos para prevenir ataques, gestionar incidentes y proteger la privacidad de los datos de los usuarios. Además, la conectividad en zonas rurales ha aumentado, ampliando el acceso a internet y contribuyendo a la inclusión digital.

Peligros en el uso de las redes sociales

El principal riesgo en las redes sociales es el acceso no autorizado a cuentas y perfiles, cuyo objetivo es robar información y utilizarla para perjudicar, engañar o suplantar a cualquier persona. Cuando ocurre una falla de seguridad, se genera una brecha que permite a los ciberdelincuentes acceder a información confidencial, como conversaciones, fotografías, contraseñas guardadas y la posibilidad de modificar datos del usuario.

Según la Cámara de Valencia (s.f.), las redes sociales han transformado completamente la relación entre empresas y usuarios. El estudio Digital 2021 de HootSuite y We Are Social indica que existen más de 4.033 millones de usuarios de redes sociales en todo el mundo, lo que representa un aumento del 13,7 % respecto a 2020 (párr. 8). Este crecimiento exponencial ha incrementado la exposición diaria de los usuarios a diversos tipos de ciberataques, tanto dentro de las plataformas como en su vida cotidiana. Por ello, se recomienda desconfiar de sistemas y mensajes desconocidos en correos electrónicos o smartphones, leer cuidadosamente enlaces o anuncios antes de interactuar con ellos y no proporcionar información confidencial que pueda ser utilizada para cometer fraudes.

Las plataformas de redes sociales aplican políticas de restricción de edad para proteger a los menores, evitando responsabilidad legal y minimizando riesgos de abuso, estafas, suplantaciones o exposición a contenido inapropiado. Sin embargo, muchos menores ingresan proporcionando información falsa, lo que les permite interactuar con cualquier persona y, en algunos casos, utilizar estas plataformas para fines ilícitos, como la trata de personas o la venta de órganos. Esto evidencia que los menores son especialmente vulnerables, ya que aún no tienen la capacidad de dimensionar los riesgos a los que están expuestos. Por ello, es esencial que los padres se mantengan informados sobre actualizaciones de las plataformas y supervisen el uso de la tecnología por parte de sus hijos.

Rojas y Yepes (2022) identifican diversos tipos de ciberataques en redes sociales, describiendo su modo de operación y el daño que pueden causar. Entre los más frecuentes se encuentran: ciberacoso, ciberadicción, ciberdelitos, *fake news*,

grooming, nomofobia, phishing, phubbing, pornografía, secuestro de información, sexting, sextorsión, síndrome de selfie y síndrome FOMO. Es fundamental que los usuarios sean conscientes de estas amenazas para protegerse y evitar convertirse en víctimas.

Según Aenolastname (2022), el 99 % de los ataques se concentró en países como Brasil, Ecuador, Colombia y Argentina, mientras que Perú y México registraron inicialmente un alto número de ataques de *ransomware* en 2021. La identificación de estas amenazas ha sido clave para que cada país diseñe esquemas de seguridad y planes de prevención que reduzcan el riesgo de futuros incidentes.

Ospina (2018) advierte que el riesgo también depende del propio usuario, dado que la información disponible en internet puede transformarse en noticias falsas y generar desinformación. Por ello, es necesario promover un uso responsable de las redes sociales, verificando la información en fuentes confiables antes de publicar o compartir contenidos en plataformas como Twitter, Facebook, Instagram o WhatsApp, con el fin de reducir los riesgos asociados a la desinformación.

Finalmente, los ataques en redes sociales han modificado profundamente la manera en que las empresas y los usuarios interactúan. Como se mencionó, el estudio *Digital 2021* de HootSuite y We Are Social reporta más de 4.033 millones de usuarios en el mundo, con un aumento del 13,7 % respecto a 2020 (párr. 8), evidenciando la magnitud y relevancia de los riesgos cibernéticos asociados a estas plataformas.

Política de buenas prácticas en redes sociales

De acuerdo con Astorga y Schmidt (2019), algunas redes sociales cuentan con políticas de seguridad, privacidad y condiciones de uso que los usuarios pueden configurar según el tipo de información que deseen mantener oculta o visible para amigos y otros usuarios.

En relación con el riesgo asociado a las contraseñas, una práctica recomendable consiste en asignar claves de acceso seguras para cuentas de redes sociales, correos electrónicos, tarjetas y otros servicios. Los usuarios deben ser creativos al establecer sus contraseñas, considerando los parámetros de seguridad establecidos por las políticas de privacidad. Se sugiere evitar información fácilmente identificable, como nombres, apellidos, nombres de mascotas, fechas de nacimiento o números de identificación, ya que estos datos pueden ser utilizados para descifrar la contraseña y comprometer la privacidad y seguridad de la cuenta, aumentando la probabilidad de sufrir un ciberataque.

Arab y Díaz (2015) indican una serie de recomendaciones para mejorar la seguridad y la calidad de vida de los usuarios de redes sociales, tanto adolescentes como adultos, que pueden aplicarse en la rutina diaria:

1. Utilizar correctamente las herramientas que ofrece internet.
2. En familias con menores de edad, definir un tiempo estimado de uso y supervisar las páginas que consultan.
3. Mantener conversaciones con los hijos sobre los riesgos asociados al uso de redes sociales e internet, enseñándoles buenas prácticas de uso.
4. Configurar los dispositivos móviles con aplicaciones que filtren contenido y controlen la información accesible en internet.
5. Desconectar la conexión Wi-Fi durante la noche.

6. Proteger la identidad en el ciberespacio.
7. No proporcionar la ubicación a personas desconocidas.
8. No compartir información personal, como correos electrónicos o números de teléfono.
9. Verificar la veracidad de las noticias o publicaciones antes de compartirlas, para evitar difundir información falsa.
10. Evitar aceptar solicitudes de amistad o seguimiento de personas desconocidas.
11. Crear contraseñas fuertes y seguras que contengan caracteres especiales, mayúsculas, minúsculas y números, y que solo sean conocidas por el propietario de la cuenta.
12. Bloquear sitios o usuarios que generen desconfianza.

Asimismo, la aplicación WhatsApp establece una serie de pautas o prácticas recomendadas (véase tabla 2) para su uso adecuado, con el fin de proteger la identidad, resguardar la información privada y prevenir estafas o ataques cibernéticos.

Tabla 2. Prácticas para el uso de WhatsApp

PRÁCTICAS RECOMENDADAS	PRÁCTICAS QUE SE DEBEN EVITAR
Comunícate con contactos conocidos.	Mensajes no deseados.
Pide permiso y respeta los límites.	Mensajes automáticos o masivos.
Usa los controles de los grupos.	Uso de listas de contactos que no conoces.
Piénsalo dos veces antes de reenviar información.	Uso excesivo de las listas de difusión.
	Extracción de información persona.
	Violación de las condiciones del servicio.

Nota. Elaboración propia.

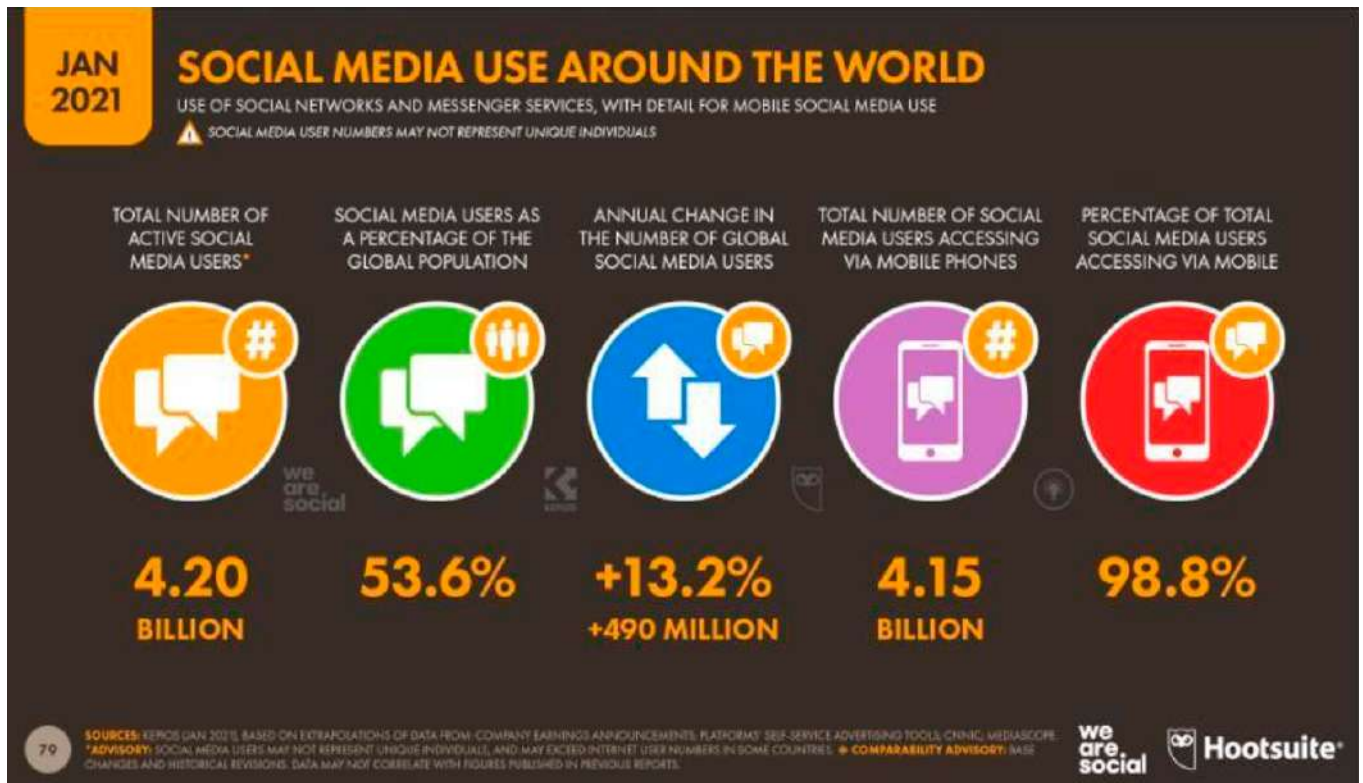
Un póster elaborado por Anchía (2021) ilustra los peligros asociados al uso de las redes sociales, dirigido tanto a niños como a adultos. Esta investigación presenta de manera gráfica tres plataformas que pueden exponer información personal sin el conocimiento de los usuarios: Instagram, Snapchat y WhatsApp. Los resultados evidenciaron que, aunque muchos padres conversan con sus hijos sobre el uso de redes sociales, pocos supervisan y controlan de manera efectiva su interacción en estas plataformas. Además, se identificaron tres riesgos principales y más frecuentes: ciberacoso, acoso sexual y pornografía infantil.

En relación con esta problemática, Osorio y Millán (2020) explican el comportamiento de los jóvenes en redes sociales. Según los autores, la falta de supervisión convierte a los adolescentes en víctimas vulnerables, lo que facilita que los delincuentes aprovechen la información personal de las víctimas para influenciarlas, amenazarlas o manipularlas.

Tendencias digitales según informes a nivel mundial sobre redes sociales y su evolución

Según el Digital Report 2021: Informe sobre tendencias digitales, redes sociales y mobile, durante los últimos 12 meses de 2021 se registró un aumento significativo en el uso de internet y redes sociales. En este periodo, más del 53 % de la población mundial utilizó redes sociales, sumándose aproximadamente 490 millones de nuevos usuarios, lo que generó un crecimiento sostenido en el consumo de dispositivos inteligentes (Álvarez, 2021). Lo anterior se observa en la figura 2.

Figura 2. Estadística uso redes sociales



Nota. Tomado de Álvarez, J. (2021, 27 de enero). *Digital report 2021: El informe sobre las tendencias digitales, redes sociales y mobile.*

Según el Digital Report 2021: Informe sobre tendencias digitales, redes sociales y mobile, el número de usuarios de internet y redes sociales ha mostrado un crecimiento constante. Durante los últimos 12 meses de 2021, más del 53 % de la población mundial utilizó redes sociales, sumándose aproximadamente 490 millones de nuevos usuarios, lo que provocó un aumento masivo en el consumo de dispositivos inteligentes (Álvarez, 2021). El informe también indica que las personas se encuentran en un rango de edad entre 16 y 64 años, dedicando alrededor de siete horas diarias a la navegación en internet a través de distintos dispositivos. Las plataformas más utilizadas incluyen Facebook, YouTube, WhatsApp y Twitter, debido a su flexibilidad para fines laborales, como marketing y publicidad, así como para la comunicación y el consumo de información de marcas y noticias.

Durante 2019, la plataforma Twitter sufrió ataques en varios países de Latinoamérica. Inicialmente, se detectaron incidentes en México, donde se secuestraron cuentas públicas y de funcionarios, modificando perfiles y publicando mensajes de hackeo. Posteriormente, Argentina, Panamá, Guatemala y El Salvador también se vieron afectados. Cada país realizó investigaciones para identificar a los responsables y restaurar las contraseñas comprometidas (Semana, 2019).

En 2021, se reportaron dos ataques significativos en Latinoamérica (Vera, 2022). El primero ocurrió en México, en un sistema de lotería, donde se extrajeron 2,9 GB de datos publicados en la web oscura. El segundo tuvo lugar en Brasil, afectando el sistema de vacunación contra COVID-19, donde se secuestraron 50 TB de información, provocando un colapso temporal del sistema y retrasos en la recuperación de los datos.

A nivel internacional, en Estados Unidos, BBC News Mundo (2021) informó sobre un ciberataque a la mayor red de oleoductos del país, que interrumpió operaciones y permitió el robo de 100 GB de información. El gobierno declaró el estado de emergencia, identificando al grupo de hackers "Dark Side" como responsable.

De acuerdo con IBM Security (A., 2022), el phishing fue el ataque más frecuente en 2021, principalmente mediante el robo de credenciales. En Latinoamérica, se registró un incremento del 4 % en ciberataques, afectando principalmente a Brasil, México y Perú. En la industria manufacturera, los ataques aumentaron un 22 %, aprovechando la posición de los empleados para exigir rescates y obtener beneficios económicos.

En marzo de 2022, Tavella reportó la campaña de espionaje denominada "Operación Discordia", que distribuyó malware njRAT en empresas y entidades gubernamentales de Latinoamérica, con mayor impacto en Colombia. Este malware permitía controlar remotamente computadoras, acceder a archivos, imágenes, cámaras y micrófonos sin ser detectado, con el objetivo de obtener información sin fines de lucro.

La plataforma WhatsApp ha sido utilizada frecuentemente por ciberdelincuentes para estafas. Según Harán (2022), los principales métodos incluyen:

- Mensajes de marcas: Suplantación de marcas reconocidas ofreciendo promociones o premios para propagar el ataque.
- Mensajes de ayudas económicas: Información falsa sobre bonos o subsidios que redirige a sitios con malware.
- Mensajes de suplantación de identidad: Simulación de conocidos para solicitar dinero o información confidencial.
- Aplicaciones externas: Apps como WhatsApp Plus que permiten espiar mensajes sin autorización.
- Mensajes para apoderarse de cuentas: Solicitan códigos de seguridad enviados al teléfono de la víctima.
- Mensajes con malware: Cadenas que al compartirse instalan software malicioso en los dispositivos.

Finalmente, Europa Press (2022) reportó un caso de abuso en el que un adulto fue condenado a cinco años de prisión por solicitar fotos íntimas a una menor de nueve años mediante redes sociales. Este hecho evidencia la necesidad de restringir el acceso de menores y promover la supervisión adecuada por parte de adultos responsables.

CONCLUSIONES

Con base en la presente investigación, se evidencia la alta usabilidad que los latinoamericanos otorgan a las redes sociales, así como la importancia de la ciberseguridad y la manera en que los ciberdelincuentes operan con sus víctimas.

Se recopiló información con el propósito de brindar conocimiento a los lectores sobre los ataques que actualmente ocurren y su forma de ejecución en estas plataformas. Esto permite comprender los riesgos a los que se enfrentan los usuarios

cuando hacen un uso inadecuado de las redes sociales, dado que continúan reportándose casos de estafas, abusos, robo de información y otros delitos cibernéticos.

Al señalar la vulnerabilidad de los usuarios ante distintos tipos de ataques, que afectan tanto a adultos como a menores, este artículo propone la implementación de políticas de buenas prácticas en redes sociales. Se destacan puntos clave para su aplicación en la vida cotidiana de los adultos, así como la necesidad de supervisión y acompañamiento de los menores en el uso de la tecnología y de las redes sociales.

Finalmente, se resalta la evolución constante de las redes sociales y el incremento del número de usuarios que acceden diariamente a estas plataformas. Esto evidencia que, a medida que las redes evolucionan, también surgen nuevos tipos de ataques dirigidos a perjudicar o abusar de los usuarios. Por ello, es fundamental que las personas se mantengan informadas sobre los cambios en las redes sociales, comprendan los objetivos de los ataques y adopten una actitud prudente en el manejo de su información personal, con el fin de reducir el riesgo de ciberataques.



REFERENCIAS



- Acens Technologies. (s.f.). *Qué es el phishing y cómo protegerse*. <https://www.acens.com/wp-content/images/2014/10/wp-phising-acens.pdf>
- Aenolastname, A. (2022). *Los ciberataques que acechan a Latinoamérica y qué países están más afectados*. AméricaEconomía. <https://www.americaeconomia.com/articulos/los-ciberataques-que-acechan-latinoamerica-y-que-paises-estan-mas-afectados>
- Aguilar, J. (2019). *Hechos ciberfísicos: Una propuesta de análisis para ciberamenazas en las Estrategias Nacionales de Ciberseguridad*. URVIO, Revista Latinoamericana de Estudios de Seguridad, 25, 24–40. <https://doi.org/10.17141/urvio.25.2019.4007>
- Álvarez, J. (2021, 27 de enero). *Digital report 2021: El informe sobre las tendencias digitales, redes sociales y mobile*. <https://wearesocial.com/es/blog/2021/01/digital-report-2021-el-informe-sobre-las-tendencias-digitales-redes-sociales-y-mobile/>
- Anchía, L. R. (2021). *Peligro de las redes sociales: Educando en ciberseguridad*. Universidad Nacional de Costa Rica. <https://repositorio.una.ac.cr/handle/11056/19261>
- Arab, L. E., & Díaz, A. (2015). Impacto de las redes sociales e internet en la adolescencia: Aspectos positivos y negativos. *Revista Médica Clínica Las Condes*, 26(1), 7–13. <https://doi.org/10.1016/j.rmcl.2014.12.001>
- Astorga, C., & Schmidt, I. (2019). Social networks dangers: How to educate our children in cybersecurity. *Revista Electrónica Educare*, 23(3), 339–362. <https://dx.doi.org/10.15359/ree.23-3.17>
- Baptista, L., & Sampieri, R. (2014). *Metodología de la investigación*. McGraw Hill Education.
- BBC News Mundo. (2019). *Cómo las redes sociales pueden arruinar tu negocio (y qué hacer al respecto)*. <https://www.bbc.com/mundo/noticias-48991621>
- BBC News Mundo. (2021). *EE. UU. declara estado de emergencia tras un ciberataque a la mayor red de oleoductos del país*. <https://www.bbc.com/mundo/noticias-internacional-57033536>
- Cámara de Valencia. (s.f.). *Los riesgos de ciberseguridad en el uso de redes sociales*. <https://ticnegocios.camaravalencia.com/servicios/tendencias/los-riesgos-de-ciberseguridad-en-el-uso-de-redes-sociales/>



REFERENCIAS



- Díaz, H. (2021, 7 de octubre). *Las redes sociales son utilizadas por el 72% de los latinoamericanos como fuente de información*. <https://latam.kaspersky.com/blog/las-redes-sociales-son-utilizadas-por-el-72-de-los-latinoamericanos-como-fuente-de-informacion-segun-estudio-de-kaspersky/23038/>
- Duarte, F. (2019, 9 de septiembre). *Los países en los que la gente pasa más tiempo en las redes sociales (y los líderes en América Latina)*. <https://www.bbc.com/mundo/noticias-49634612>
- Europa Press. (2022). *Condenado a cinco años de cárcel por pedir fotos íntimas a una menor y compartirlas en redes sociales*. El Periódico. <https://www.elperiodico.com/es/sucesos/20220420/condenado-cinco-anos-carcel-pedir-fotos-intimas-menores-13542803>
- Garzón, K. (2021, 7 de abril). *El 51% de los niños latinoamericanos tiene acceso a Internet y a ciberataques*. <https://bit.ly/3yORQ5A>
- Gómez, B. (2018). El influencer: Herramienta clave en el contexto digital de la publicidad engañosa. *Methaodos Revista de Ciencias Sociales*, 6(1), 149–156. <http://dx.doi.org/10.17502/m.rcs.v6i1.212>
- Harán, J. (2022). *Estafas por WhatsApp: Modalidades de engaño más comunes*. WeLiveSecurity. <https://www.welivesecurity.com/la-es/2022/05/04/estafas-por-whatsapp-modalidades-engano-comunes/>
- Jurado-Pruna, F., Yarad-Jeada, P.V., & Carrión-Jumbo, J.L. (2020). *Análisis de las características del sector microempresarial en Latinoamérica y sus limitantes en la adopción de tecnologías para la seguridad de la información*. Revista Científica ECOCIENCIA. <https://revistas.ecotec.edu.ec/index.php/ecociencia/article/view/303>
- López, A. (2018). *Ciberseguridad en los países del MINT*. Revista de Tecnologías de la Información, 2(3), 155–167. https://www.ecorfan.org/bolivia/researchjournals/Tecnologias_de_la_Informacion/vol2num3/Tecnologias_de_la_Informacion_V2_N3_3.pdf
- Martínez, W., & Ávila, D. (2021). *Ciberseguridad en las redes sociales: Una revisión teórica*. Uniandes Episteme, 8(2), 211–234. <http://45.238.216.13/ojs/index.php/EPISTEME/article/view/2089/1659>
- Ministerio de Tecnologías de la Información y las Comunicaciones. (2020). *Cómo prevenir los riesgos en el entorno digital: 10 recomendaciones en el Día del Internet Seguro*. MINTIC Colombia. <https://mintic.gov.co/porta/inicio/Sala-de-prensa/Noticias/125836:Como-prevenir-los-riesgos-en-el-entorno-digital-10-recomendaciones-en-el-Dia-del-Internet-Seguro>



REFERENCIAS



- Oracle. (2022). *¿Qué es el malware?* <https://www.oracle.com/es/database/security/que-es-el-malware.html#:~:text=Malware%20es%20un%20t%C3%A9rmino%20gen%C3%A9rico,contenido%20activo%20y%20otro%20software>
- Ortega-Aguilar, P., & Traverso-Macias, D. (2021). *Reflexiones para avanzar: Experiencias en la investigación educativa. Márgenes*, Revista de Educación de la Universidad de Málaga, 2(2), 157–172. <http://dx.doi.org/10.24310/mgnmar.v2i2.10900>
- Osorio-Tamayo, D., & Millán-Otero, K. (2020). *Adolescentes en Internet, la mediación entre riesgos y oportunidades*. Revista Colombiana de Ciencias Sociales, 11(1), 153–180. <https://doi.org/10.21501/22161201.2979>
- Ospina-Valencia, J. (2018). *Las redes sociales: El riesgo lo aumentamos nosotros*. DW.com. <https://www.dw.com/es/las-redes-sociales-el-riesgo-lo-aumentamos-nosotros/a-43058048>
- Pons, V. (2017). *Internet, la nueva era del delito: Cibercriminología, ciberterrorismo, legislación y ciberseguridad*. URVIO, Revista Latinoamericana de Estudios de Seguridad, 20, 80–93. <http://dx.doi.org/10.17141/urvio.20.2017.2563>
- Rahman, S., Huang, T. K., Madhyastha, H. V., & Faloutsos, M. (2016). *Detecting malicious Facebook applications*. IEEE/ACM Transactions on Networking, 24(2), 773–787. <https://ieeexplore.ieee.org/abstract/document/7024188>
- Rodríguez, P. (2017). *¿Qué seguridad? Riesgos y amenazas de Internet en la seguridad humana*. Araucaria. Revista Iberoamericana de Filosofía, Política y Humanidades, 18(36), 391–415. <http://dx.doi.org/10.12795/araucaria.2016.i36.17>
- Rojas-Díaz, J. S., & Yepes-Londoño, J. J. (2022). *Panorama de riesgos por el uso de la tecnología en América Latina*. Trilogía Ciencia Tecnología Sociedad, 14(26), e2020. <https://doi.org/10.22430/21457778.2020>
- Sack, S. (2021). *Las evolutivas amenazas de ciberseguridad en América Latina*. Technocio. <https://technocio.com/las-evolutivas-amenazas-de-ciberseguridad-en-america-latina/>
- Sánchez, K. (2020). *Reporte OEA y BID: América Latina avanza en ciberseguridad, pero con temas pendientes*. Voz de América. https://www.vozdeamerica.com/a/tecnologia-ciencia_reporte-oea-bid-ciberseguridad-america-latina-caribe/6066175.html



REFERENCIAS



- Semana. (2019). *Twitter sufre ataque a cuentas oficiales en distintos países de América Latina*. <https://www.semana.com/tecnologia/articulo/twitter-sufre-ataque-a-cuentas-oficiales-en-distintos-paises-de-america-latina/79987/>
- Tavella, F. (2022). *Campaña de espionaje distribuyó el malware njRAT en organizaciones de Colombia*. WeLiveSecurity. <https://www.welivesecurity.com/la-es/2022/05/20/campana-espionaje-malware-njrat-organizaciones-colombia/>
- Vera, G. (2022). *La ciberdefensa en América Latina, entre el peligro y la indiferencia*. El Tiempo. <https://www.eltiempo.com/tecnosfera/novedades-tecnologia/ciberataques-america-latina-muy-vulnerable-por-indiferencia-de-gobiernos-662478>
- Whatsapp. (s.f.). *Cómo usar WhatsApp de manera responsable*. https://faq.whatsapp.com/general/security-and-privacy/how-to-use-whatsapp-responsibly/?lang=es_pe

