



## C A P Í T U L O 1

# EL ROL DE LAS REDES SOCIALES EN EL CIBERACOSO: ANÁLISIS EN MENORES Y UNIVERSITARIOS

**Luis Enrique Colmenares-Guillén**

Benemérita Universidad Autónoma de Puebla Facultad de Ciencias de la Computación

**Ximena Arenas Toxte**

Benemérita Universidad Autónoma de Puebla, Facultad de Medicina,  
Licenciatura en Ciencia Forense

**Mariano Larios Gómez**

Benemérita Universidad Autónoma de Puebla Facultad de Ciencias de la Computación

**RESUMEN:** El objetivo de esta investigación fue analizar las acciones de menores de edad y universitarios en redes sociales e identificar los riesgos que existen al navegar y que pueden estar vulnerables a víctimas de ciberacoso. Además, se comparan resultados con el Módulo sobre Ciberacoso (MOCIBA) con relación a las medidas de seguridad utilizadas con mayor frecuencia. Se utiliza el enfoque cuantitativo, porque se adapta a las características y necesidades de la investigación. Los resultados revelaron que el ciberacoso, con relación a los menores de edad, el 55.1% conoce el término de ciberacoso, mientras que en el caso de universitarios el 56% también conoce el término. Esto refleja que es una problemática común, y que actualmente existe confusión con dicho término. Por otro lado, los resultados demostraron que WhatsApp es la red social que más usuarios, han bloqueado a otros usuarios. Esta investigación enfatiza la importancia de comprender las dinámicas del ciberacoso en diferentes grupos demográficos, al hacer un análisis entre menores de edad y universitarios.

**PALABRAS CLAVE:** ciberacoso, redes sociales, medidas de seguridad.

## 1. INTRODUCCIÓN

Las redes sociales han transformado radicalmente como se comunica y se interactúa; estas plataformas ofrecen herramientas que facilitan la conexión con amigos y familiares, además de ser parte del entretenimiento para muchas personas, por el impacto y la facilidad de acceso a una red social. No todo es positivo con las

redes sociales, ya que existen riesgos al navegar en ellas dando paso a ser víctima de ciberacoso por estos medios: mensajes de textos recibidos en el móvil, acoso vía llamadas, mails denigratorios o con amenazas, páginas web creadas o utilizadas para difamar, por mencionar algunos (Marín Cortés y Linne, 2021).

En 2015, el Instituto Nacional de Estadística y Geografía (INEGI) atiende un problema generado por la constante actualización de la tecnología y medios electrónicos enfocándose en el acoso que se genera por medio de estos. Por ello, se implementa el Módulo sobre Ciberacoso (MOCIBA). En un principio fue agregado como módulo experimental a la Encuesta Nacional sobre Disponibilidad y Uso de las TIC en Hogares (ENDUTIH, 2015), principalmente para tener un panorama acerca de los métodos de captación a utilizar y así obtener los datos requeridos. El objetivo se enfocó en la obtención de información estadística para saber la magnitud de los incidentes de acoso en medios electrónicos, mejor conocido como ciberacoso. Al observar que el instrumento arrojó datos que servirían para la erradicación de esta problemática, se volvió de carácter anual obteniendo datos hasta el año 2022, sin considerar el año 2018.

La estructura del Módulo sobre Ciberacoso (MOCIBA) se basa en antecedentes, Objetivos específicos, Periodicidad, Diseño conceptual, Cobertura geográfica, Desglose geográfico, Diseño estadístico y Periodo de levantamiento (MOCIBA, 2015).

El Instrumento del Módulo sobre Ciberacoso (MOCIBA) busca obtener información a nivel nacional y estatal, en población de 12 años o más, usuaria de internet o celular que vivió alguna situación de ciberacoso por sexo, según grupos de edad, los medios a través de los cuales se realiza, la frecuencia con que se da, la identidad del acosador, las acciones tomadas por las víctimas, así como conocer si tienen conocimiento sobre la prevención del ciberacoso y de las autoridades u organizaciones que puedan brindar apoyo (MOCIBA, 2017).

El Fondo de las Naciones Unidas para la Infancia (UNICEF) define al Ciberacoso como acoso o intimidación por medio de las tecnologías digitales. Puede ocurrir en las redes sociales, las plataformas de mensajería, las plataformas de juegos y los teléfonos móviles (UNICEF, 2024), sin embargo, para algunos el ciberacoso sigue siendo un término nuevo y es un problema que día a día va en crecimiento. En México, 8 de cada 10 mayores de seis años utilizan internet y, en promedio, los internautas pasan cuatro horas y media navegando en plataformas o redes sociales (García, 2023). Es por ello población puede ser vulnerable a ciberacoso, aunque la que engloba a universitarios y menores es la más expuesta a redes sociales y medios digitales por lo que son más vulnerables de ser víctimas de ciberacoso; porque no conocen las medidas de seguridad para proteger las acciones que realizan y los identifica en internet, esto se conoce como identidad digital (López, 2022), por ende, desconocen cómo aplicarlas correctamente.

En la presente investigación se comprendió que la población es consciente de los riesgos que existen al navegar en internet y redes sociales, como son la creación de perfiles falsos en redes sociales, propagación de rumores en foros o redes sociales, envío de mensajes amenazantes y publicación de fotos reales o fotomontajes (Aguilar Torres, 2023); riesgos enfocados al ciberacoso y al mismo tiempo identificar qué medidas de seguridad se usan con mayor regularidad, por ejemplo; proteger los dispositivos con un firewall o poner contraseñas fuertes con más de 8 caracteres, combinar letras, números y símbolos (Cruz Lucas, 2022), para identificar que acciones son las más recomendables para no ser víctima de ciberacoso. Para ello, se aplicó una encuesta a una población de 99 personas de 12-27 años, para analizar y comparar con los datos obtenidos del Instrumento del Módulo sobre Ciberacoso (MOCIBA).

El trabajo de investigación consiste en las siguientes secciones. En la sección 2 se describen algunas preliminares útiles para entender este trabajo; la sección 3 se muestran los detalles de la metodología aplicada para diseñar la encuesta y la población seleccionada, la sección 4 se muestran los resultados y análisis de la encuesta y en la sección 5 las conclusiones.

## 2. PRELIMINARES

### 2.1 Medidas de Seguridad de la muestra de la población encuestada

Este proyecto consistió en conocer las medidas de seguridad que realizan menores y universitarios en redes sociales, por lo que se aplicó una encuesta en la que se consideraron varios tipos de medidas de seguridad considerando como referencia la encuesta que realiza el INEGI conocido como MOCIBA para posteriormente hacer una comparativa. La encuesta tuvo el mismo formato tanto para menores y universitarios, consta de 28 preguntas divididas en las siguientes dimensiones: Medidas de Seguridad, Acciones realizadas en internet, Acciones en redes sociales y Ciberacoso.

Es importante mencionar que de cada dimensión solo se consideraron las preguntas que obtuvieron respuestas relevantes para la realización del análisis con el instrumento del MOCIBA.

## 3. METODOLOGÍA

La investigación fue diseñada bajo el planteamiento metodológico del enfoque cuantitativo, ya que se adapta a las características y necesidades de la investigación. El enfoque cuantitativo “utiliza la recolección de datos para probar hipótesis con base en la medición numérica y el análisis estadístico, con el fin de establecer pautas de comportamiento y probar teorías” (Hernández et al., 2014, p.4).

La población para el estudio la conformaron 99 personas, de 12-27 años, divididas en dos sectores: el primero de niñas y niños de 12-16 años que cursan la secundaria y el segundo fue a universitarios de 17-27 años considerando las cuatro áreas académicas (Económico-Administrativa, Ingeniería y Ciencias Exactas, Ciencias Sociales y Humanidades y Ciencias Naturales y de la Salud) de la Benemérita Universidad Autónoma de Puebla. Las técnicas de recolección de datos son procedimientos y actividades que permiten comprobar el problema planteado de la variable estudiada en la investigación, por lo tanto, el tipo de investigación determinará la técnica a emplear (Useche et al., 2019, p.30).

La encuesta sirvió para recoger datos necesarios para la investigación, razón por la que se aplicó a una muestra piloto a 10 personas, usando la técnica de muestreo por conveniencia; método que permite seleccionar aquellos casos accesibles que acepten ser incluidos. Esto, fundamentado en la conveniente accesibilidad y proximidad de los sujetos para la investigación (Otzen & Manterola, 2017).

El instrumento utilizado para la investigación fue el cuestionario considerando la escala de Likert, quedando de la siguiente manera para la investigación: 5. Muy frecuentemente, 4. Frecuentemente, 3. Ocasionalmente, 2. Raramente y 1. Nunca. La escala de Likert sirve para medir opiniones, actitudes y grados de conformismo y, a la vez, capta la intensidad de los sentimientos hacia la afirmación, enfatizando para Ospina et al. (2005). “Cada elemento de la escala proporciona información sobre la actitud de la persona y que tanto la acumulación de información como la suma de respuestas, permite decidir la posición que una persona ocupa en el eje de la actitud que se busca medir” (Machuca Yaguana et al., 2023).

Con base en las situaciones de ciberacoso planteadas en el Módulo sobre Ciberacoso (MOCIBA, 2022), la investigación se enfocó en las siguientes situaciones: Publicación de información personal; Críticas o burlas por apariencia o clase social; Recibir contenido sexual; Insinuaciones o propuestas sexuales.

## 4. RESULTADOS Y ANÁLISIS DE LA ENCUESTA

El Análisis comparativo de menores con mayores de edad, se realizó a 99 personas utilizando una encuesta, con edad de 12-27 años. Esta se dividió en dos; una específicamente para personas de 12-16 años, es decir, adolescentes de secundaria, y la segunda se aplicó a las cuatro áreas académicas de la Benemérita Universidad Autónoma de Puebla, universitarios de 17-27 años. Como parte del análisis de las dos encuestas realizadas los resultados obtenidos fueron los siguientes:

La dimensión de Medidas de Seguridad fueron las siguientes preguntas: en la primera pregunta fue, ¿Realiza alguna medida de seguridad para proteger su celular?, los universitarios se preocupan más por la seguridad de sus teléfonos, a

diferencia de los adolescentes. Se refleja que el 40 % de los universitarios marcaron la opción de frecuentemente; mientras que los menores solo el 22.4 % selecciono esta opción. Esto se justifica, que para los universitarios su teléfono es indispensable durante esta etapa de formación académica en su respectiva área.

En la siguiente pregunta: ¿Realiza alguna medida de seguridad para proteger su computadora/laptop?, los universitarios son los que más protegen sus equipos, quizás por ser su herramienta de trabajo más importante, a diferencia de los menores. Por otra parte, la opción nunca ha realizado esa medida de seguridad correspondiente a un 26.5% en menores de edad, y en mayores esta opción equivale a un 8%, lo que refleja la vulnerabilidad en los menores de edad en sus equipos de cómputo pues la opción nunca es la de mayor porcentaje.

La siguiente pregunta que fue, ¿Realiza alguna medida de seguridad para proteger sus cuentas de redes sociales?, los menores de edad se preocupan más por la seguridad en sus cuentas de redes sociales, mientras que los universitarios lo hacen en un menor porcentaje. En el caso de los menores de edad destacaron las opciones de, muy frecuentemente con un 26.5% y frecuentemente con un 36.7%. Por otro lado, en los universitarios se obtuvo la opción muy frecuentemente con un 24% y la opción frecuentemente con un 28%.

Siguiendo con la dimensión de Medidas de Seguridad, a continuación, se exponen acciones comunes en torno de las medidas de seguridad que realizan menores de edad y universitarios:

En la siguiente pregunta que fue, Crear y poner contraseñas (claves, huella digital, patrón, PIN, reconocimiento facial), para ambos casos la respuesta que destaca corresponde, a la opción muy frecuentemente con 58% en universitarios y 40.8% en menores de edad; esta medida de seguridad es de fácil acceso, ya que es fácil de realizar, aunque con una gran efectividad para proteger cualquier cuenta de internet o dispositivo móvil.

La siguiente pregunta fue, cambiar periódicamente las contraseñas, los universitarios marcaron en mayor porcentaje la opción raramente con un 42%, mientras que en el caso de los menores se obtuvo un 40.8% con ocasionalmente; lo que indicaría un foco rojo para el robo de sus datos, debido a que no se está realizando una de las medidas de prevención básicas para evitar ser víctima de ciberdelitos pudiendo ser vulnerables a sufrir ciberacoso.

En la siguiente pregunta fue Poner en privado mis cuentas de redes sociales, los menores de edad que realizan esta acción corresponden al 49%, mientras que los universitarios, el 68%. En ese sentido los universitarios consideran más importante esta medida de seguridad.

La última pregunta planteada fue, Instalar o actualizar programas antivirus, cortafuegos o anti-espías, en los menores de edad, la opción nunca es el segundo porcentaje con mayor valor, correspondiente a un 27.5 %; mientras que en universitarios la opción raramente es 22%, ambos casos corresponden a valores negativos. Ahora bien, si se compara la opción frecuentemente, los menores de edad realizan esta medida de seguridad con 2.3% más con respecto a los universitarios.

En la segunda dimensión correspondiente a Acciones realizadas en internet, en la pregunta de, Compartir mis datos personales en sitios web (para obtener información sobre algún producto, un servicio, un empleo o alguna institución académica), el 36% de los universitarios marcaron la opción raramente, mientras que en los menores de edad el 57.1% seleccionó la opción nunca.

Tercera dimensión correspondiente a Acciones en redes sociales se consideraron las siguientes preguntas: ¿En cuál red social has bloqueado a algún usuario?, en ambos casos se obtuvo como respuesta predominante que la red social en la que han bloqueado a algún usuario corresponde a WhatsApp. Para los universitarios el 80% de la población ha bloqueado a algún usuario, mientras que los menores de edad el 65.3% lo ha realizado.

En la pregunta, ¿En cuál red social has reportado a algún usuario?, en ambos casos se encontró que Facebook fue la red social que predominó; en los universitarios con un 62%, mientras que los menores de edad un 38.8%.

La dimensión de Ciberacoso se consideró la siguiente pregunta. En su opinión, ¿Qué es el ciberacoso?, los menores y los universitarios marcaron la respuesta correcta referente a lo que es el ciberacoso; obteniendo un 56% en los universitarios y 55.1% correspondiente a los menores. Por otra parte, no es el resultado esperado, enfatizando que en el caso de los universitarios se esperaba un mejor resultado. Esto nos indica que para algunos el ciberacoso sigue siendo un término nuevo.

En la siguiente pregunta, ¿Considera el ciberacoso como un delito?, tanto los menores como los universitarios consideran el ciberacoso como un delito; obteniendo que el 64% de universitarios y el 55.1% de menores marcaron la opción frecuentemente. Aunque se puede ver opiniones divididas en los menores de edad ya que esto justifica que estos términos como el ciberacoso como delito pueden ser nuevos para ellos o llegar a confundirlos con otros términos.

La siguiente pregunta, ¿Quién tiene mayor riesgo de ser víctima de ciberacoso?, la opción que predomina en ambos casos corresponde a adolescentes de 13 a 17 años; el 69.4% de menores marcaron esta opción, mientras que el 74% de los universitarios coinciden con esta opción marcándole de igual manera. Considerando a los menores de edad; saben que son vulnerables al ciberacoso en redes sociales, por la facilidad de información que se tiene hoy en día en los medios digitales.

En la pregunta, Con lo que realiza, pública o comparte en internet (redes sociales y páginas web) ¿Podría sufrir ciberacoso?, en el caso de los universitarios son más cuidadosos en lo que realizan, publican y comparten debido a que la opción, raramente tiene un 40%, mientras que en el caso de los menores predominaron las opciones ocasionalmente con un 32.7% y raramente con un 22.4%, es decir, que aún no prestan la suficiente atención a sus acciones realizadas en redes sociales y páginas web.

Esta pregunta fue de respuesta múltiple, ¿En qué red social ha sido víctima de ciberacoso?, destaca que los universitarios con un 56% y los menores de edad con un 63.3% no han sido víctimas de ciberacoso en redes sociales. No obstante, Facebook fue la segunda opción con mayor porcentaje marcada, con un 30% por parte de universitarios y un 28.6% por parte de menores; es un número significativo en ambos casos, lo que indica que parte de la población encuestada ha sufrido ciberacoso.

La siguiente pregunta, Se ha informado sobre el procedimiento para realizar una denuncia por ciberacoso, tanto los universitarios como menores de edad no están informados sobre cómo realizar una denuncia por ciberacoso, destacando la opción, nunca con un 34% en universitarios y 26.5% en menores.

La última pregunta que se consideró fue: ¿En qué dependencia gubernamental ha hecho una denuncia por ciberacoso?, en ambos casos nunca han denunciado por ciberacoso en alguna dependencia gubernamental, con un 80% de universitarios y un 61.2% de menores de edad. Se muestra que una minoría ha denunciado llamando al 088 Policía Cibernética y Reportando a la secretaría de Seguridad y Protección Ciudadana, esto nos indica que se desconocen las instancias que ayudan, al estar en una situación de ciberacoso.

#### **4.1 Comparación y discusión de los resultados de la encuesta con el Módulo sobre Ciberacoso (MOCIBA)**

Para realizar la comparación de resultados, se consideró la pregunta número 2, de la encuesta realizada por el Instituto Nacional de Estadística y Geografía (INEGI), y Módulo sobre Ciberacoso (MOCIBA) 2022.

¿Qué medidas de seguridad realiza? Y sus 7 opciones de respuesta: Crear o poner contraseñas (claves, huella digital, patrón, etcétera); instalar o actualizar programas antivirus, cortafuegos y anti-espías; bloquear ventanas emergentes del navegador; cambiar periódicamente las contraseñas; no abrir ni guardar archivos que envían personas desconocidas; no publicar mi correo o número telefónico en redes sociales; y no ingresar a sitios web inseguros o desconocidos.

Para la investigación se eliminó la opción de bloquear ventanas emergentes del navegador que fue considerada por MOCIBA, por lo tanto, las preguntas de la encuesta fueron 6, en comparación con MOCIBA: Crear y poner contraseñas (claves, huella digital, patrón, PIN, reconocimiento facial); cambiar periódicamente las contraseñas; instalar o actualizar programas antivirus, cortafuegos y anti espías; publicar mi correo o número telefónico en redes sociales; ingresar a sitios web inseguros o páginas desconocidas; abrir o guardar archivos que envían personas desconocidas.

La población presentada por MOCIBA fue de 65 188 personas de 12 años o más que usan internet en cualquier dispositivo, mientras que para la investigación fueron 99 personas de 12-27 años, divididas en dos sectores: el primero de niñas y niños de 12-16 años que cursan secundaria y el segundo a universitarios de las cuatro áreas académicas de la Benemérita Universidad Autónoma de Puebla de 17-27 años.

La proporción de las preguntas se obtuvo que las 6 preguntas consideradas para la encuesta, equivale al 86% en comparación con las 7 preguntas de MOCIBA que representa el 100%.

En crear y poner contraseñas (claves, huella digital, patrón, PIN, reconocimiento facial), solo el 84% de los universitarios realiza esta acción. Mientras que, para el caso de los menores de edad el 77.5% la realiza. El resultado final de las personas encuestadas, el 80.80% crean y ponen contraseñas.

En instalar o actualizar programas antivirus, cortafuegos o anti-espías, solo el 44% de los universitarios realiza esta acción. Mientras que, para el caso de los menores de edad el 20.4% la realiza. El resultado final de las personas encuestadas, el 32.32% instalan o actualizan programas antivirus, cortafuegos o anti-espías.

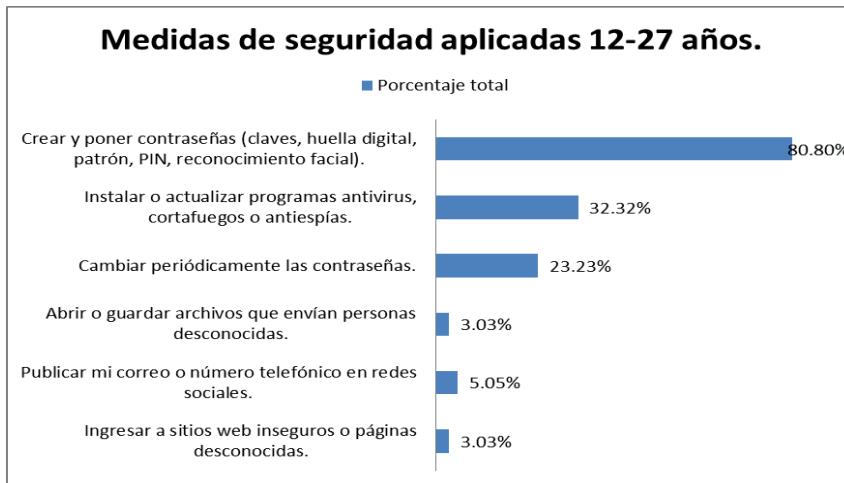
Para cambiar periódicamente las contraseñas, solo el 18% de los universitarios realiza esta acción. Mientras que, para el caso de los menores de edad el 28.6% la realiza. El resultado final de las personas encuestadas, el 23.23% cambian periódicamente las contraseñas.

Para abrir o guardar archivos que envían personas desconocidas, solo el 4% de los universitarios realiza esta acción. Mientras que, para el caso de los menores de edad, el 2% la realiza. El resultado final de las personas encuestadas, el 3.03% abren o guardan archivos que envían desconocidos.

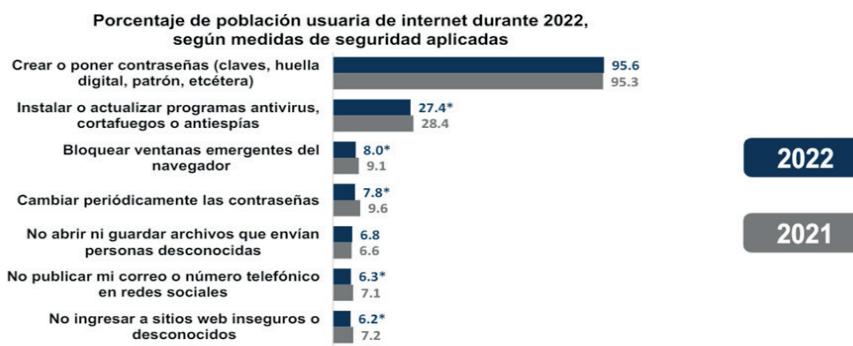
En publicar su correo o número telefónico en redes sociales, solo el 10% de los universitarios realiza esta acción. Mientras que, para el caso de los menores de edad, se obtuvo un cero %. El resultado final de las personas encuestadas, el 5.05% publican su correo o número telefónico en redes sociales.

En ingresar a sitios web inseguros o páginas desconocidas, solo el 4% de los universitarios realiza esta acción. Mientras que, para el caso de los menores de edad solo el 2% la realiza. El resultado final de las personas encuestadas, el 3.03% ingresan a sitios web inseguros o páginas desconocidas.

Para analizar y comparar los resultados que reportó MOCIBA con los nuestros, se obtuvo la figura 1, con los porcentajes finales de cada medida de seguridad, obteniendo lo siguiente:



**Fig 1.** Resultados finales de medidas de seguridad de nuestra encuesta. Fuente: elaboración propia.



**Fig 2.** Porcentajes de medidas de seguridad por usuarios considerando únicamente datos de 2022 de MOCIBA. Fuente: INEGI,2022.

Los resultados de MOCIBA, ver la figura 2, que reportó en 2022, el 95.6% de la población optó por crear y poner contraseñas, mientras que los resultados de la encuesta aplicada muestran que el 80.80% realiza esta medida de seguridad. En ambas encuestas, esta opción predomina con el porcentaje más alto, por lo que es la medida de seguridad más utilizada por la población, debido a la facilidad para crear y poner contraseñas en sus dispositivos y, por lo general, la sociedad conoce esta medida de seguridad como primera opción para sus dispositivos.

Por otro lado, los resultados de MOCIBA, muestran que el 27.4% de su población, usa como medida de seguridad el Instalar o actualizar programas antivirus, cortafuegos o anti-espías, mientras que los resultados de esta investigación muestran que el 32.32% optó por esta medida de seguridad. El resultado es positivo, ya que se nota un aumento del 5% por el avance y uso de la tecnología; ya que actualmente hay muchos programas antivirus y el uso de estos programas es indispensable para proteger dispositivos y datos personales ante amenazas informáticas.

Los datos de MOCIBA reportan que el 7.8% de la población usa como medida de seguridad cambiar periódicamente las contraseñas, mientras que el 23.23 % de la población para esta investigación opta por esta medida de seguridad. En comparación con MOCIBA de 2022, los resultados muestran un porcentaje más alto, hoy en día, cambiar las contraseñas de los dispositivos y cuentas de internet es importante para la población, ya que con el avance de la tecnología también se presentan amenazas, es por ello, que algunas páginas de internet solicitan contraseñas más complejas y un cambio de contraseña con regularidad para mantener protegidas las cuentas y datos personales.

Con base en los resultados obtenidos, se observa que MOCIBA tiene un 6,8 % de su población que no abre ni guarda archivos que envían desconocidos, mientras que los resultados de esta investigación obtuvieron el 3%. Considerando ambas encuestas, hay resultados proporcionales, porque representa una mínima población que actúa, aunque se considera positivo que la población joven y adulta sean conscientes del riesgo que existe al abrir archivos desconocidos, lo que puede poner en peligro sus dispositivos y su información personal.

De acuerdo con los datos de MOCIBA, el 6.3% de la población usa la acción de, no publicar mi correo o número telefónico en redes sociales, mientras que el 5.05% de la población de esta investigación opta por esta medida de seguridad. De igual forma, se obtienen resultados similares, ya que esta acción se realiza con un porcentaje mínimo de usuarios, lo que se refleja en los números mostrados. Sin embargo, esta población conoce los riesgos que conlleva el compartir datos personales y poner en riesgo su privacidad y en algunos casos, su seguridad.

Finalmente, MOCIBA reportó que el 6.3% de su población no ingresa sitios web inseguros o páginas desconocidas, mientras que los resultados de esta investigación obtuvieron el 3.03% de la población. De igual modo, los resultados son similares porque se mantiene con un porcentaje mínimo en usuarios que optan por esta acción. Actualmente los usuarios de internet tienen más conocimiento de redes sociales y páginas web, y están conscientes de la existencia de sitios web desconocidos y pueden exponerse a riesgos en cuanto a la privacidad de los datos personales.

## 5. CONCLUSIONES

Gran parte de la población tiene acceso a dispositivos electrónicos, a la creación de redes sociales y a la navegación por internet; así que se revelaron conclusiones importantes a lo largo de la investigación.

En la primera dimensión Medidas de seguridad, en este apartado se hizo una comparación con el instrumento del módulo sobre Ciberacoso y hubo una medida de seguridad que destaco tanto en la investigación como en los resultados que arrojó el instrumento del MOCIBA, la cual es; crear y poner contraseñas (claves, huella digital, patrón, PIN, reconocimiento facial). Los resultados de la investigación muestran que el 80.80% de la población usa esta medida de seguridad, mientras que MOCIBA arroja un 95,6 %; esto se debe a la facilidad para crear y poner contraseñas en sus dispositivos y, en general, la sociedad conoce esta medida de seguridad como primera opción.

La segunda dimensión corresponde a Acciones realizadas en internet, se obtuvo que 36% de los universitarios raramente comparten sus datos personales en sitios web y los menores de edad, el 57.1% nunca comparten sus datos, este resultado es positivo porque nos demuestra que son conscientes de los riesgos que esta acción conlleva.

En la tercera dimensión que es Acciones en redes sociales, WhatsApp destaca como la red social en la que más usuarios han bloqueado a alguien, obteniendo 80% en universitarios y 65.3% en menores de edad. Mientras que Facebook destaca en ser la red social en donde más usuarios han reportado a alguien, con un 62% en universitarios y 38.8% en menores de edad.

La cuarta dimensión que es Ciberacoso, más de la mitad de la población encuestada para la investigación no ha sido víctima de ciberacoso en redes sociales, obteniendo un 56% en universitarios y 63.3% en menores de edad, sin embargo, Facebook destaca como la red social donde parte de la población ha recibido ataques de ciberacoso con un 30% en universitarios y 28.6% en menores de edad. Por otro lado, los menores de edad, el 55.1 % conoce el término de ciberacoso, mientras que los universitarios solo el 56 % lo conoce.

Para concluir, se demuestra que el ciberacoso es un tema que día con día va en aumento y que, a pesar de contar con diversas medidas de seguridad, parte de la población sigue sin estar familiarizada con ella y de igual manera con el término, originando que se vuelvan población vulnerable para ser víctimas de ciberacoso.

## REFERENCIAS

- Aguilar Torres, G., Delgado Vargas, K. A., de Abiega L'Eglisse, A., López Hernández, L., & Gallegos García, G. (2023). Principales riesgos en el uso de tecnologías de la información en adolescentes. *Revista Transdigital*, 5(2) <https://www.revista-transdigital.org/index.php/transdigital/article/view/218/340#info>
- Cruz Lucas, G. I. (2022). Riesgos de seguridad de los datos en la web. *Journal TechInnovation*, 1(2), 43–49. <https://revistas.unesum.edu.ec/JTI/index.php/JTI/article/view/18/32>
- García, A. (2023). Violencia digital en México afecta más a mujeres y genera mayor conciencia entre ellas. *El economista* .<https://www.eleconomista.com.mx/arteseideas/Violencia-digital-en-Mexico-afecta-mas-a-mujeres-y-genera-mayor-consciencia-entre-ellas-20230829-0036.html>
- Hernández, R., Fernández, C., & Baptista. M. (2014). *Metodología de la investigación*. (6.ª ed.). <https://uniclanet.unicla.edu.mx/assets/contenidos/292420240103233754.pdf>
- INEGI. (2015). *Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH) 2015*. <https://www.inegi.org.mx/programas/dutih/2015/>
- INEGI. (2015). *Módulo sobre Ciberacoso (MOCIBA) 2015*. <https://www.inegi.org.mx/programas/mociba/2015/>
- INEGI. (2017). *Módulo sobre Ciberacoso (MOCIBA) 2017*. <https://www.inegi.org.mx/programas/mociba/2017/>
- INEGI. (2022). *Módulo sobre Ciberacoso (MOCIBA) 2022*. <https://www.inegi.org.mx/programas/mociba/2022/>
- López, J. (2022, marzo 18). Identidad Digital, ¿qué es y por qué es tan importante? *Forbes México* <https://www.forbes.com.mx/identidad-digital-que-es-y-por-que-es-tan-importante/>
- Machuca Yaguana, J. M., Maldonado Machuca, M. E., & Vinces Vinces, F. V. (2023). Tratamiento y representación de datos provenientes de escalas tipo Likert. *Ciencia Latina Revista Científica Multidisciplinaria*, 7(4), 736-747. <https://ciencialatina.org/index.php/ciencialatina/article/view/218/340#info>

cienciala/article/view/6905/10505

Marín Cortés, A., & Linne, J. (2021). Una tipología del ciberacoso en jóvenes. *Revista Mexicana de Sociología*. 2021, vol.83, n.2, pp.331-356.: [https://www.scielo.org.mx/scielo.php?script=sci\\_arttext&pid=S0188-25032021000200331](https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0188-25032021000200331)

Ospina Rave, B. E., Sandoval, J. D., Aristizábal Botero, C. A., & Ramírez Gómez, M. C. (2005). La escala de Likert en la valoración de los conocimientos y las actitudes de los profesionales de enfermería en el cuidado de la salud. Antioquia, 2003. *Investigación y Educación en Enfermería*, XXIII (1), 14-29.

Otzen, T. & Manterola, C. (2017). Técnicas de Muestreo sobre una Población a Estudio. *International Journal of Morphology* vol.35 no.1: [https://www.scielo.cl/scielo.php?script=sci\\_arttext&pid=S0717-95022017000100037](https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0717-95022017000100037)

UNICEF. (2024). Ciberacoso: qué es y cómo detenerlo. <https://www.unicef.org/es/end-violence/ciberacoso-que-es-y-como-detenerlo>

Useche, M. C., Artigas, W., Queipo, B., & Perozo, E. (2019). Técnicas e instrumentos de recolección de datos cuali-cuantitativos. *Repositorio Institucional Uniguajira*. <https://repositoryinst.uniguajira.edu.co/bitstream/handle/uniguajira/467/88.%20Tecnicas%20e%20instrumentos%20recolecci%C3%B3n%20de%20datos.pdf?sequence=1>