CIBERATAQUES QUE PUEDEN SUFRIR LOS JÓVENES EN REDES SOCIALES.

C. Ruiz Hernández[1], L. C. Sánchez Villada[1] y S. Quiceno Castañeda[1]

[1] Semillero de investigación SIPI, Centro de Servicios y Gestión Empresarial, Servicio Nacional de Aprendizaje SENA. Medellín, Colombia.

pimaheco@hotmail.com; laurasv546@gmail.com; sarayquiceno9002@gmail.com

Palabras clave: ciberataques, redes sociales, seguridad informática, educación.

RESUMEN

Con la llegada de la pandemia generada por el Covid 19, el uso de las redes sociales ha aumentado de forma considerable, especialmente en los jóvenes, lo cual ha provocado un incremento constante de ataques haciendo uso de estos espacios virtuales. Las consecuencias de los acosos en línea son nefastas, toda vez que existe una baja cultura de prevención en estos contextos y, además, hay un desconocimiento en la individualización de estas conductas. En este artículo de investigación documental, se caracterizan los principales ataques en redes sociales, como sextorsión, grooming, doxing, happy slapping, trolling, flaming y ciberstalkeo, y se hace referencia a las principales prácticas empleadas para minimizar estos riesgos en las redes sociales por parte de los jóvenes, como principales víctimas de este flagelo. La investigación se soporta en diferentes artículos de revistas especializadas e informes de entidades oficiales, tanto de índole nacional como internacional.

01 INTRODUCCIÓN

El Covid 19 provocó un crecimiento acelerado de la digitalización. Las actividades cotidianas en el ámbito laboral, académico, social e incluso familiar, debieron migrar a escenarios virtuales. Estos nuevos contextos trajeron consigo, ventajas importantes en materia de transformación digital, de adaptación a herramientas tecnológicas y de alfabetización informática, sin embargo, se permitieron visibilizar una serie de problemáticas como las relacionadas con la seguridad digital.

Respecto al sector educativo, especialmente en lo relacionado con los procesos formativos de niños y adolescentes, algunos estudios afirman que, desde el inicio de sus clases en modalidad virtual debido a la pandemia, se incrementó el acoso en línea en un 70%, lo cual se soporta, en parte, por el aumento del tiempo digital de ocio, el incremento de usuarios en línea y el estrés generalizado que provoca comportamientos más hostiles [1]. Esos acosos virtuales, se deben en parte, a que existe un considerable acceso al ámbito de la tecnología, un dominio respecto al uso de redes sociales, y a ello, se le suma que el agresor puede conservar su anonimato [2].

En ese contexto, se hace necesario que la comunidad académica identifique las principales conductas que configuran el ciberbullying, entendido este como el ataque o intimidación en la red [3], ya que este fenómeno trae consigo una cantidad de consecuencias emocionales para su población escolar, sea en su rol de víctima o victimario y se entiende que, una intervención adecuada a tiempo, tiene el potencial de frenar las consecuencias negativas que se desprenden de estos eventos.

Las emociones dependen de la internalización de la víctima, indicando que, si se auto responsabilizan, pueden llegar a sentir angustia, culpa y pánico, mientras que, si responsabilizan a otros, pueden sentir ira y ánimo de venganza. Las víctimas pueden, además, sufrir depresión y síntomas postraumáticos, como miedo debido a la exposición digital permanente, ya que saben que muchos agresores se mantienen en el anonimato, y escasa vez reciben condenas ejemplares y, en algunos casos, el ciberacoso puede también provocar traumas e ideas suicidas [4].

Es así como esta investigación documental pretende en un primer momento, generar una caracterización de las principales modalidades del ciberacoso, buscando su comprensión por parte de la comunidad educativa y, finalmente, se establecen sugerencias de adopción de conductas preventivas, tomando en consideración el referente de las buenas prácticas propuestas por entidades de control e implementadas por algunas entidades educativas del orden nacional e internacional.

02 METODOLOGÍA

Este artículo obedece a la revisión de 20 referencias documentales, las cuales abordan la temática del acoso cibernético o ciberataques desde diferentes perspectivas, siendo preponderantes los artículos de reflexión en materia educativa, seguidos de los informes expedidos por entidades públicas, hasta llegar a los textos con tintes legales y psicológicos, que nutren la presente investigación cualitativa. Estos textos se extraen de diferentes fuentes digitales, especialmente de bases de datos de artículos académicos, haciendo búsqueda de los textos más recientes, privilegiando los publicados desde el año 2019 hasta lo corrido del año 2021. Sin embargo, se consideran 4 referencias publicadas con anterioridad por la pertinencia con la investigación.

Se hace lectura de los 20 documentos recuperados y se selecciona la información adecuada al propio objeto de investigación, el cual versa sobre los diferentes ataques cibernéticos y las medidas preventivas de cada uno de ellos. Es de anotar que las referencias consultadas pertenecen, tanto al ámbito colombiano como internacional, pues el fenómeno de investigación no tiene fronteras, al estar intermediado por el internet.

03 RESULTADOS Y DISCUSIONES

El ciberbullying significa ataque o intimidación en la red, y ha estado presente de manera progresiva conforme avanza la tecnología, trayendo consigo efectos lamentables desde lo social, lo emocional, familiar y personal. Los ciberacosadores hacen uso de mensajes de texto, de redes sociales y chats, sin que sea necesario estar de manera sincrónica en alguno de estos recursos [3]. En ese caso, se hace más prudente prevenir este flagelo, que entrar a corregir las consecuencias emocionales ocurridas, así que es necesario caracterizar algunos de estos ciberataques y establecer algunas pautas preventivas.

3.1 CIBERATAQUES EN REDES SOCIALES

A continuación, se describen algunos ciberataques, los cuales son solo una muestra del gran abanico de posibilidades que existen para hostigar en las redes sociales, pues cada día se crean nuevas modalidades y estas se van popularizando rápidamente debido, en gran parte, a que hacen uso de las redes sociales, que sirven de vehículo efectivo para su propagación. Para permanecer en conexión con los demás, los jóvenes y adolescentes, hacen uso permanente de redes sociales, como Facebook, LinkedIn, Twitter, Instagram y otras, las cuales ofrecen una opción económica, ubicua, masiva y de fácil acceso para la población referenciada. [5]

Tabla 1 en la página 127.

La anterior relación de ciberdelitos, evidencia que el común denominador es el desconocimiento respecto al adecuado manejo y aprovechamiento de los medios sociales, en los cuales la confianza excesiva y la escasa precaución en la salvaguarda de la información personal, pueden provocar desenlaces poco alentadores para los usuarios, quienes de manera ingenua comparten su intimidad con personas poco confiables que manipulan las emociones de la víctima de una manera casi imperceptible, logrando acceder a su esfera personal, escenario ideal para perpetrar estos delitos. Así mismo, se evidencia una insuficiente cultura digital, la cual debería iniciar desde el núcleo familiar, llegando a las instituciones educativas y a la sociedad en general.

3.2 BUENAS PRÁCTICAS PARA MINIMIZAR LOS RIESGOS EN REDES SOCIALES

- Generar el hábito de conocer las condiciones de uso, las reglas y las políticas antes de acceder a crear un perfil en cualquier red social.
- Procurar identificar las políticas de la red social relacionadas con el uso de contenidos, ya sea información o imágenes que se suban a la plataforma.
- Las instituciones educativas deben generar políticas respecto al uso de redes sociales en dispositivos pertenecientes a la entidad con miras a blindar de manera segura la información institucional.
- Seguir los parámetros que exijan las redes sociales respecto a la configuración correcta de los perfiles.
- Prestar la debida atención a la asignación y al uso de usuarios y contraseñas.
- Si la red social permite, hacer uso de un segundo factor de autenticación y del protocolo https para navegación.
- Los dispositivos pertenecientes a entidades educativas deberían contar con herramientas *anti-spam y firewall* con la finalidad de optimizar la seguridad del sistema y protegerlo ante eventuales riesgos.
- Sensibilizar respecto a la importancia de no compartir contraseñas de redes sociales y solo acceder con el usuario y contraseña propios.
- Enfatizar en la importancia de no utilizar la misma contraseña de la red social en otros sitios de internet, en otras redes sociales o aplicaciones.
- Enseñar sobre la creación de contraseñas difíciles de adivinar y encontrar, evitando el uso de nombres o palabras comunes. Las claves deben ser fuertes y complejas.
- En la medida de los posible evitar acceder a redes sociales desde computadores públicos.
- Invitar a la instalación de apps antirrobo, las cuales permitan ubicar el dispositivo en caso de pérdida o robo, pudiendo incluso bloquearlo o borrar datos de la memoria de manera remota.
- Educar sobre el uso de redes WIFI públicas, haciendo énfasis en la evitación de manejar información confidencial y sensible cuando se usen.
- Reiterar la importancia de mantener actualizadas las versiones del sistema operativo.
- Procurar la utilización directamente del navegador cuando se desconozca el enlace al que se va a acceder, puntualizando que este debe aparecer con las letras HTTPS, lo cual sirve para indicar que hay un protocolo de seguridad válido.
-Evitar compartir demasiada información en las redes sociales.

Tabla I. Ciberdelitos y su prevención

CIBERDELITO	¿EN QUÉ CONSISTE?	¿CÓMO PREVENIRLO?
SEXTORSIÓN	Es una utilización en el despojo de una persona que cumple con una amenaza de hacer pública sus fotos sin permiso de ella [6]. Puede iniciar con el envío voluntario de mensajes o imágenes con contenido sexual explícito (sexting), pero puede llegar a convertirse en sextorsión cuando una de las partes amenaza con publicar o compartir ese material enviado en la esfera íntima [7]. ESET, empresa de seguridad digital, indica que los criminales usan dos técnicas online para obtener información sensible o imágenes comprometedoras de sus potenciales víctimas, con las que posteriormente comienzan sus extorsiones: Acciones basadas en la confianza: aprovechando el anonimato que permite internet, los delincuentes logran generar la confianza de la víctima para luego engañarlas y solicitarles información e imágenes sensibles. Acciones basadas en malware: aquí se utilizan programas malignos que pueden encender la cámara web de los dispositivos de la víctima, quien entrega imágenes sin siquiera darse cuenta. La víctima descarga aplicaciones inocentemente que llegan en mensajes de WhatsApp o de correo electrónico, bajo la promesa de recibir algún premio o recompensa. [8]	Es por lo que se propone que los jóvenes en edad escolar sean desconfiados con quienes conocen en la red y con las aplicaciones que descargan, debiendo ser cuidadosos también con revelar información sensible o compartir imágenes. Es ideal que los jóvenes solo generen relaciones en red con personas que sean de su mismo círculo social o que, al menos, se permitan identificar con claridad sus lazos con ellos. Además, deben evitar caer en trampas, siendo muy cuidadosos con las recompensas ofrecidas y con el material que descargan, guardan o divulgan en sus redes sociales.
GROOMING	El Grooming significa acoso sexual en línea. Este se presenta cuando una persona adulta, que de aquí en adelante llamaremos groomer, establece una relación con una niña, niño o adolescente con la intención de atraerlo, manipularlo, invitarlo a participar en actividades sexuales. Los agresores del grooming pueden iniciar y establecer esta relación en el escenario real o a través de redes sociales. Una vez que el groomer logra esa relación «ideal» de amigos, empieza a manipular las emociones de la NNA (Niña, niño y adolescente) y, le propone que le envíe fotos, o videos grabados por él mismo o le propone grabarlos a través de una webcam. El principal objetivo del grooming es captar menores de edad, engancharlos para acceder sexualmente a estos, tanto física como mentalmente, y luego tomar fotos o grabar videos y obtener beneficios monetarios por el material que este obtiene, y las víctimas, al no querer, los empieza a extorsionar o amenazar con quitarle la vida a él y a su familia. Pasos para llevar a cabo la práctica de grooming: Se hace un análisis del perfil de su víctima y así lograr ser aceptado (reclutamiento); posteriormente, se empieza a verificar qué es lo que la NNA sube a las redes sociales, y luego de encontrar sus puntos más débiles, les ofrecen su apoyo incondicional y así lograr ganarse la cercanía que se necesita (Lealtad). Empieza a mandarle fotos o mensajes para que el otro también lo haga y vea esto de manera graciosa y sin que nadie se dé cuenta de lo que realmente sucede (Encanto) y, finalmente, al ya tener todo lo que buscaba, lo empieza a amenazar para que lo siga haciendo y se muestra tal cual como es realmente (Descaro). [9]	El 30% de menores de edad encuestados en un estudio colombiano, manifestaron que habían conocido personas por internet, y un 17% de ellos, los habían conocido posteriormente cara a cara [10], lo cual sin duda se convierte en un riesgo latente para iniciar esta clase de delitos, pues se demuestra que los menores son confiados, entonces pueden caer fácilmente en un ciberataque como el grooming. Se recomienda evitar el envío de material visual de contenido erótico o sexual o subirlos a las redes sociales, y si ya fueron enviados, es necesario evitar ceder ante el chantaje y preferir hablar con adultos de confianza y denunciar el caso ante las autoridades. [11]

CIBERDELITO	¿EN QUÉ CONSISTE?	¿CÓMO PREVENIRLO?
DOXING	El doxing es una forma actual de acosar a las personas en internet, que consiste en investigar a las personas para después comenzar a amenazar y extorsionar a estos individuos; generalmente, los seres humanos que están en riesgo de sufrir esta forma de acoso son los adolescentes, puesto que en esta etapa de su vida, ellos buscan la manera de ser aceptados, y al estar afectados por esta forma de acoso generan que se sientan inseguros en su propio entorno. El doxing se genera por un comentario o una foto en cualquier red social, a partir de ese momento, una persona se encarga de realizar un seguimiento y comienza a investigar la vida de esta persona que realizó la publicación, ocasionando que este hacker se aproveche de esto y comience a extorsionar a la persona, ya que si llega a realizar una publicación comprometedora, la persona se perjudica, utilizando esto en forma de chantaje. La manera más segura de defendernos de este acoso es mantener un perfil limpio en las redes, para que así estas personas no encuentren ninguna información que les sirva y acabar con este fenómeno que daña mucho a la sociedad [12].	En algunos sitios web o aplicaciones, está la opción de iniciar sesión a través de Facebook o Google, esta práctica se debe evitar, pues mientras más sitios accedan con las mismas credenciales, más información personal puede recopilarse. Adicionalmente, se recomienda mantener los perfiles de redes sociales como privados y revisar las opciones de configuración de privacidad en cada una de ellas. Finalmente, si se participa en foros en línea, es ideal usar pseudónimos [13].
HAPPY SLAPPING	Happy slapping, traducida al español como bofetada feliz, es un término que nace en el 2004 en Lewisham, Londres para mirar la cara que ponían las personas cuando las golpeaban. Son las agresiones físicas que se le realizan a compañeros de estudio y que son publicadas en internet, específicamente, en redes sociales, ya que se pretende hacerlos virales. Estas conductas de violencia física son realizadas por adolescentes, normalmente conformados en grupos. Los agresores no conocen a la persona contra quien van a atentar físicamente, y su objetivo es publicar estas agresiones para mostrar sus logros. Lo que estas personas ignoran es que, al conseguir que estos videos se hagan conocidos, es que pueden ser reconocidos por las autoridades y esto en muchos países es considerado un delito [14].	Es importante que los jóvenes no promuevan estas conductas, mediante el rechazo a participar en ellas. Se invita a no unirse a grupos donde se comparta esta clase de videos o fotografías y si llega en otro medio, es necesario que no la compartan y es indispensable que hablen con un adulto responsable quien denunciará ante las respectivas autoridades.
TROLLING O TROLL EN INTERNET	Esto hace referencia al uso que hace el individuo en las redes sociales para realizar comentarios inapropiados, y por medio de estos, destacarse e incomodar a las personas, crear oposición y fomentar el enfrentamiento entre otros usuarios. El objetivo del Troll en internet es impulsar y poner en pie el enfrentamiento y persuadir la atención al resto de los usuarios. [15]	Lo más importante es no hacer parte del troleo, evitando estar en comunidades de troleo, evitando compartir comentarios o información referente, y en la medida de lo posible, eliminar y bloquear a quienes lo hagan, para no quedar envueltos en una red perjudicial que incluso puede llegar a consecuencias legales.

CIBERDELITO	¿EN QUÉ CONSISTE?	¿CÓMO PREVENIRLO?
FLAMING	Flaming o flamear, es cuando se ataca a otra persona de manera verbal haciendo uso de internet. Es muy frecuente cuando se hace alusión a temas religiosos, políticos, ambientales, como por ejemplo el cambio climático, entre otros, que generen controversia. Es importante anotar que incluso puede surgir son alguna clase de provocación [16].	Es necesario que el usuario de redes sociales se abstenga de revelar información o de comentar publicaciones de contenido religioso, político o de cualquier tema sensible, pues una postura determinada puede provocar un ataque con consecuencias lamentables. En caso de hacerlo, deben ser respetuosos de la expresión ajena y evitar el uso de palabras groseras, vulgares o despectivas. Se recomienda no tener dentro de los contactos en las redes sociales personajes con esta marcada tendencia, ya que eso hace parte de un apoyo indirecto, y en caso de tenerlos, evitar participar en sus publicaciones o de compartirlas.
CIBER STALKEO	El stalkeo es una conducta reiterada y con marcada intención en la que una persona denominada stalker, hace un seguimiento a otra, denominada víctima, en contra de su voluntad, creando una sensación de aprehensión, la cual provoca un miedo razonable [17]. La palabra stalkear se convirtió en un verbo que básicamente quiere decir rastrear a alguien, así que quien lo hace, recibe la denominación de stalker, que en inglés se traduce como acosador. [18] En ese orden de ideas, cuando se habla de ciberstalkeo, se refiere a un acoso realizado en la red, en la cual los perpetradores espían a sus víctimas haciendo uso de diversas herramientas, utilizando generalmente la información que se extrae para fines delictivos. Un ejemplo del referido delito de ciberstalkeo, es la suplantación de identidad, el cual se da cuando el acosador lanza una página web o genera un perfil social bajo el nombre de la víctima [19].	Es necesario mantener los perfiles en redes sociales bajo estricta privacidad y compartir poca información e imágenes, evitando revelar datos personales y sensibles. Es importante no indicar lugar de ubicación, nombres de entidades a las que se pertenece, fechas relevantes o relacionar parentesco.

04 CONCLUSIONES

Se deben hacer sensibilizaciones periódicas a aquellos usuarios de las redes sociales, especialmente a los niños y jóvenes en edad escolar, para que tengan presente que, el no hacer un buen uso de estos medios sociales, puede traer consecuencias fatales como el acoso online, extorsiones, violencia física y mental, incluso suicidio, afectando tanto al victimario como a la misma víctima y a su contexto familiar y social.

Debido a que es muy frecuente ver en las redes todo tipo de información de personas que no protegen bien sus cuentas, es prudente no aceptar a cualquiera, así tengan familiares o amigos en común, es mejor prevenir que lamentar, verificar que a las páginas que se vaya a acceder si tengan la protección de los datos. Antes de subir cualquier tipo de información se debe pensar dos veces si es necesario o no hacerlo. Es importante, además, no compartir información personal o laboral que los puedan poner en riesgo.

Se puede evidenciar que las víctimas de estos ataques generalmente son jóvenes, por lo tanto, es indispensable que se implemente una campaña educativa sobre los riesgos que tienen las redes sociales y cómo se deben manejar para evitar que sufran estos ciberataques.

Por último, también es fundamental que se refuercen la seguridad en las redes sociales para así reducir, en mayor medida, estas agresiones cibernéticas que ocasionan daños en muchas personas.

05 AGRADECIMIENTOS

Agradecemos a Dios y al semillero de investigación SIPI por brindarnos la oportunidad de participar en la elaboración de este artículo.

06 REFERENCIAS

[1] Delgado, P. 2019. Aumenta número de ciberataques a alumnos, ¿cómo pueden prepararse? México. https://observatorio.tec.mx/edu-news/ciberataques-universidades
[2] Cedillo-Ramirez, L.P. 2020. Acoso escolar cibernético en el contexto de la pandemia por COVID-19. Rev cubana med vol.59 no.4 Ciudad de la Habana oct.-dic. 2020 Epub 15-Nov-2020
[3] Astorga-Aguilar, C., & Schmidt-Fonseca, I. (2019). Social Networks Dangers: How to educate our childs in cibersecurity. Revista Electrónica Educare, 23(3), 9. https://doi.org/10.15359/ree.23-3.17
[4] Marín-Cortés, A., & Linne, J. (2020). Una revisión sobre emociones asociadas al ciberacoso en jóvenes adultos. Psicoperspectivas, 19(3), 1-16. https://www.psicoperspectivas.cl/index.php/psicoperspectivas/article/view/1824#:~:text=Los%20resultados%20indican%20que%20las,insomnio%2C%20depresi%C3%B3n%20e%20ideaciones%20suicidas.
[5] Sánchez, M.A. y Pinochet Sánchez, G. El rol de las redes sociales virtuales en la difusión de información y conocimiento: estudio de casos. Universidad & Empresa, vol. 19, núm. 32, 2017. https://revistas.urosario.edu.co/xml/1872/187247578006/index.html
[6] CHS Alternativo, 2020, Sextorsión, chantaje sexual en línea, Lima, Perú, página 4.https://drive.google.com/file/d/151KQnxc2LhdVlmHdRSFHGTqVIFoof_9D/view
[7] Ramírez, H. 2021. Ciberbullying o Ciberacoso ¿Qué es y cómo prevenirlo?. España. https://protecciondatos-lopd.com/empresas/ciberbullying-ciberacoso/
[8] MINTIC, 2017. ¿Cómo evitar que sus hijos caigan en sextorsiones? Colombia. https://www.enticconfio.gov.co/como-evitar-sextorsion
[9] Capital Humano y Social Alternativo, 2020, Grooming captación en línea. Primera edición, Lima Perú. Página 4-14. https://drive.google.com/file/d/1qF7fu3rxvVWskZdUJFWuQdYeb59k1PhJ/view
[10] ICBF, 2021. ¿Cómo evitar ser víctima del grooming y proteger a los menores de edad? Colombia. https://www.icbf.gov.co/mis-manos-te-ensenan/como-evitar-ser-victima-del-grooming-y-proteger-los-menores-de-edad
[11] Centro cibernético policial, 2016. ¿Cómo evitar el grooming?. Colombia. https://caivirtual.policia.gov.co/sites/default/files/boletin_grooming03_0.pdf
[12] Camprubí, I.B. enero, 2020.Doxing una forma de acoso por internet de largo alcance. España, Página 1-2, http://www.feuso.es/images/docs/informa/FEUSOSALUDLABORAL533.pdf

[13] Latto, N. 2020. ¿Qué es el doxxing y cómo puede evitarlo?. https://www.avast.com/es-es/c-what-is-doxxing
[14] Derecho de la red, 2019. ¿Qué es el 'Happy Slapping'? https://derechodelared.com/happy-slapping/
[15] Ramírez, H. 2021. Trolls en Internet: los tipos de trolling que encontrarás en la red. España. https://protecciondatos-lopd.com/empresas/trolls-internet-tipos-trolling/
[16] González, Y. 2020. ¿Qué es el flaming en Internet?. España. https://protecciondatos-lopd.com/empresas/flaming/
[17] Estiarte, C.V. (2009). stalking y derecho penal, relevancia jurídico-penal de una nueva forma de acoso Iustel.
[18] Ibarra, Y. 2018. ¿Qué significa ser un «stalker»? TreceBits. https://www.trecebits.com/2018/01/05/que-significa-ser-un-stalker/
[19] González, Y. ¿Qué son los stalkers de internet? España. https://protecciondatos-lopd.com/empresas/stalkers-que-son/
[20] Guzmán, C.A. 2019. Seguridad aplicada en la utilización de redes sociales. Universidad Piloto de Colombia.