Revista Logos Ciencia & Tecnología, 16 (2) 95-117 | Mayo-agosto, 2024
https://revistalogos.policia.edu.co:8443/index.php/rlct

Estudio de caso

Revista Logos Ciencia & Tecnología
ISSN 2422-4200 (en línea)

Gamificación: Estrategia preventiva de ciberseguridad para *sexting* y *grooming*

Gamification: Preventive cybersecurity strategy for sexting and grooming

Gamificação: estratégia preventiva de cibersegurança para *sexting* e *grooming*

Héctor Fernando Vargas Montoya [a,*] | Félix Alexander Usma Guzmán [b]

a https://orcid.org/0000-0002-0861-2883 Instituto Tecnológico Metropolitano (ITM), Medellín, Colombia

b https://orcid.org/0000-0003-2725-8653 Instituto Tecnológico Metropolitano (ITM), Medellín, Colombia

- Fecha de recepción: 2024-02-05
- Fecha concepto de evaluación: 2024-05-21
- Fecha de aprobación: 2024-05-30
https://doi.org/10.22335/rlct.v16i2.1919

Para citar este artículo/To reference this article/Para citar este artigo: Vargas Montoya H. F. & Usme Guzmán, F. A. (2024). Gamificación: Estrategia preventiva de ciberseguridad para sexting y grooming. *Revista Logos Ciencia & Tecnología, 16*(2), 95-117. https://doi.org/10.22335/rlct.v16i2.1919

RESUMEN

Las redes sociales se van expandiendo, captando más suscriptores, y con ello, los menores de edad consumen estos servicios con muy poco control que les permiten una interacción con individuos desconocidos en cualquier parte del mundo. Esto es aprovechado por los delincuentes cibernéticos que utilizan técnicas como el *sexting* y el *grooming*. Este artículo tiene como objetivo proponer una estrategia de ciberseguridad basada en gamificación que apoye a la población adolescente, con base en un punto de prevención asociado al *sexting* y *grooming* para reducir diferentes niveles de riesgos. Para ello, el método utilizado fue el uso de procesos para la identificación de problemas de ciberseguridad en Internet, a través de diferentes controles y aplicándolos en una estrategia educativa de ciberseguridad a estudiantes de una institución de educación primaria en la ciudad de Medellín, Colombia. En la prueba diagnóstica se encontró que solo el 31.2% de los estudiantes respondieron positivamente el cuestionario y, una vez aplicada la estrategia de ciberseguridad, se realizó el cálculo estadístico de la prueba de los signos como una prueba no paramétrica, y fue evidente que la estrategia de ciberseguridad que usa gamificación logró aumentar el nivel de conciencia, con el resultado de que el 93.7% de los estudiantes mejoró notablemente sus respuestas. Se concluye que la estrategia de prevención de riesgos en Internet en contra de los adolescentes es fundamental con la aplicación de mecanismos alternos que generen controles como la toma de conciencia y la gamificación.

Palabras clave: Adolescente, cibercrimen, gamificación[1], *grooming*[2], *sexting*[3].

1 Palabras clave del autor, sin traducción reconocida al español (RAE).
2 Palabras clave del autor, sin traducción reconocida al español (RAE).
3 Palabras clave del autor, sin traducción reconocida al español (RAE).

* Autor de correspondencia. Correo electrónico: hectorvargas@itm.edu.co

ABSTRACT

Social networks are expanding more and more, attracting more subscribers and adolescents consume these services in a poorly controlled manner, allowing an interaction with strangers from anywhere in the world. This has allowed cybercriminals to abuse their victims with mechanisms such as sexting and grooming, especially affecting the adolescent population. This article aims to propose a cybersecurity strategy that supports the adolescent population based on gamification, giving a point of prevention associated with sexting and grooming to reduce different levels of risk. The method used was to make use of processes for the identification of cybersecurity problems on the Internet, through different controls and applying them in a cybersecurity educational strategy to students from a primary education institution in the city of Medellín, Colombia. As a result, in the diagnostic test it was found that only 31.2% of the students responded positively to the questionnaire and once the strategy using gamification was applied, it was found that 93.7% of the students significantly improved their answers. With the application of the non-parametric test using the statistical method for the calculation of the sign test, it was found that the cybersecurity strategies using gamification managed to increase the level of awareness. It is concluded that for the identification and prevention of risks on the Internet that go against adolescents the application of mechanisms that manage to generate controls such as awareness through gamification becomes essential.

Keywords*:* Adolescents, cybersecurity, gamification, grooming, sexting.

RESUMO

As redes sociais estão se expandindo e atraindo mais seguidores. Com isso, os menores consomem esses serviços com pouquíssimo controle, o que lhes permite interagir com indivíduos desconhecidos em qualquer lugar do mundo. Isso é aproveitado por cibercriminosos que usam técnicas como *sexting* e *grooming*. Este artigo tem como objetivo propor uma estratégia de cibersegurança fundamentada na gamificação que apoie a população adolescente, com base num ponto de prevenção associado ao *sexting* e ao *grooming* para reduzir diferentes níveis de riscos. Para tanto, o método utilizado foi a utilização de processos de identificação de problemas de segurança cibernética na internet, por meio de diversos controles e aplicação deles em uma estratégia educacional de segurança cibernética a estudantes de uma instituição de ensino fundamental da cidade de Medellín, Colômbia. No teste de diagnóstico, constatou-se que apenas 31,2% dos estudantes responderam positivamente ao questionário e, uma vez aplicada a estratégia de cibersegurança, o cálculo estatístico do teste de sinais foi realizado como um teste não paramétrico, e ficou evidente que a estratégia de cibersegurança que recorre à gamificação conseguiu aumentar o nível de conscientização, tendo como resultado que 93,7% dos estudantes melhoraram significativamente as suas respostas. Conclui-se que a estratégia de prevenção de riscos da internet contra adolescentes é essencial com a aplicação de mecanismos alternativos que gerem controles como conscientização e gamificação.

Palavras-chave: adolescente, cibercrime, gamificação, *grooming*, *sexting*.

Introducción

Entender las redes sociales, la Internet y la era digital supone un esfuerzo importante para cualquier persona. Los jóvenes vienen reflejando un comportamiento excesivo en el uso de la tecnología, considerando la cantidad de horas por día que dedican, principalmente, a sus *smartphones*, lo que genera una gran dependencia individuo-tecnología. Por ello, los delincuentes digitales o ciberatacantes, aprovechan el aumento de personas en las redes para capturar incautos en este mundo y obtener sus propios beneficios, con lo cual, el problema a tratar, desde las estrategias de gamificación, es lograr reducir los niveles de riesgos entre los estudiantes asociados al *sexting* y *grooming*.

El término "*sexting*" es una palabra que se ha integrado completamente en la literatura hispanoparlante y se refiere al intercambio de mensajes y fotografías con contenido sexual explícito en dispositivos como teléfonos móviles y tabletas, y a través de Internet. La característica distintiva de esta práctica es que, en muchos de los casos, estas imágenes se comparten de manera inmediata y sin restricciones en las redes sociales. El *sexting*, por lo tanto, involucra la distribución de videos, imágenes o elementos multimedia en general con contenido sexual que viaja por las redes sociales, con o sin consentimiento de los propietarios. Esta difusión de contenido es instantánea y conlleva graves consecuencias para los niños, niñas y jóvenes que participan en ella (Mejía-Soto, 2014).

En esa línea, se han indicado diferentes modalidades que toman el concepto de *sexting* para hacer fraudes en Internet, como es el caso de Industrialización del fraude manipulado por la intimidad (IMFI, por su sigla en inglés, *Intimacy Manipulated Fraud Industrialization*), el cual consiste en hacer creer a las personas que han adquirido un servicio para adulto, pero a través de la interfaz de software puede ser cualquier otra persona en el chat que se hace pasar por un hombre o mujer (Wang & Topalli, 2024; Fangzhou, 2024). Así mismo, hay una asociación sobre los problemas mentales acontecidos con el envío consentido o no de imágenes sexuales, en donde la angustia sicológica genera una afectación en los hombres cuando reciben datos que no han solicitado y que son objeto de visualización sin un precedente claro del destinatario (Wright & Wachs, 2024) y diferentes personas se ven coaccionadas e intimidadas para enviar contenido personal por redes, lo que genera una alta angustia principalmente en adolescentes que generan más cibervictimización por medio del uso de sus celulares y de Internet (Holfel et al., 2024).

Por otro lado, el *grooming* es una serie de actividades que una persona adulta ejecuta a través de Internet con el fin de ganarse la confianza de un niño o niña, y con ello, obtener acceso de índole sexual (Kamar et al., 2022). La ciberseguridad, según la empresa experta en tecnología y seguridad, Cisco System (2023), hace referencia a la protección de los diferentes elementos tecnológicos que están interconectados en el ciberespacio y que son susceptibles de ciberataques que puedan afectar la integridad, disponibilidad o la confidencialidad de los datos. Se trata entonces de la gestión coherente de las amenazas y cómo estas pueden afectar los activos conectados, normalmente a Internet. Así, es posible reconocer el valor diferencial del riesgo al cual se enfrentan tanto los elementos tecnológicos como las personas.

En cuanto a las problemáticas en Internet por causa de un uso indebido de las redes, a través de la Inteligencia Artificial (IA), se han desarrollado diferentes plataformas que permiten la creación de imágenes de cualquier tipo, esto incluye semidesnudos y desnudos completos, lo que puede aumentar los engaños en Internet. La creación de los avatares o personalización de las imágenes corporales en una caricatura o similar, permite que a través de la IA se generen perfiles falsos que van en busca del engaño a los niños, niñas y adolescentes, esto combinado con un lenguaje atractivo de acuerdo a la edad (Chawki, 2024), por ello, los atacantes tienen más herramientas que les permiten captar la atención de más menores de edad cuando se envían imágenes no consensadas y, en consecuencia, más personas pueden caer en redes que usan el *sexting* y el *grooming* como mecanismos de interacción, lo que generan diferentes problemas, de una parte, los mismos problemas sicológicos en los menores, y por otra, posible pérdida de sueño que se hace usual para cualquier generación, con más intensificación en niñas y mujeres, generando una pérdida potencial de sueño promedio (Kyle et al., 2024).

La exposición de material sexual explícito con fines extorsivos ha aumentado en las últimas décadas, sumado al incremento del uso de la Internet, los menores de edad se ven enfrentados a un sinnúmero de situaciones que afectan directamente su personalidad. Desde los estamentos políticos y culturales han generado diferentes alertas, pero el consumo de recursos sin control en la web permite obtener fácilmente información de los menores que pueden ser tomadas y ajustadas para posibles abusos sexuales (Katrin & Jörg, 2024). Del mismo modo, Sani et al. (2024) indican sobre los problemas legales y sicológicos que se generan en los niños por el uso intensivo de dispositivos móviles y la baja supervisión de los padres, lo que genera una necesidad latente de buscar mecanismos de prevención de los riesgos que generan un aumento sustancial de impactos en los niños, adolescentes y en la sociedad.

De igual forma, el alto impacto que genera la pornografía en menores de edad ha suscitado un sinnúmero de reacciones de las personas adultas, en los que se han considerado los diferentes aspectos por los cuales los menores de edad generan, comparten y consumen pornografía. Parte de ello toma relevancia en los hombres más que en las mujeres, haciendo uso de esta para otros propósitos, no solo el entretenimiento, por esta razón, una educación que fomenta lo preventivo es fundamental (Frank et al., 2024). Del mismo modo, un estudio generado entre 106 adolescentes acerca de

la relación entre el *grooming* y otras maneras de victimización en línea, mostró una relación directa entre el *sexting* y el acoso sexual consentido, considerando que esta práctica se pudo agudizar un poco más en la pandemia dado el acceso casi sin restricción en el tiempo de los medios digital y en línea (Almeida, 2024).

Ahora bien, la gamificación es un término de origen anglosajón que se ha incorporado ampliamente en la literatura en español. Se refiere al empleo de elementos propios de los juegos con propósitos distintos a la simple diversión. Una manera de lograr este objetivo es adaptar métodos tradicionales de enseñanza a las nuevas teorías pedagógicas, además de aplicar tácticas digitales usando las tecnologías más recientes disponibles, como Internet, multimedia, y en particular, las redes sociales y los videojuegos, que han experimentado un notorio crecimiento en los últimos años (Prieto-Andreu et al., 2022).

Así mismo, tres (3) de cada diez (10) adolescentes en Antioquia y Chocó (Colombia) admitieron haber enviado, recibido o reenviado videos o fotos con contenido sexual o erótico, lo que establece una clara línea asociada al *sexting*, de igual forma, 12.8% se sintieron avergonzados por tal situación, el 11.4% pidieron favores sexuales para no publicar las imágenes en su poder (lo que constituye un ciberdelito), el 11.2% publicó o constató que lo que se envió de forma privada fue publicado a un rango más amplio de personas y el 10.8% fue amenazado con publicar cualquier contenido en poder de un tercero o extorsión dirigida (Morillo et al., 2022). Esto establece cómo el uso de la tecnología por parte de los adolescentes no tiene un control, socialización o plan de conciencia claro frente al tema, lo que genera una problemática en el ciberespacio cada vez mayor y crea una necesidad importante de reducir posibles impactos asociados con la ciberseguridad.

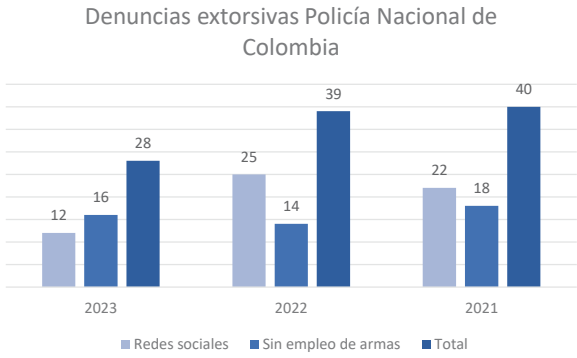
Es oportuno indicar que se hizo una revisión de los hábitos y comportamientos de los menores de edad asociados con las nuevas tecnologías. Este estudio reveló que el 90% de los niños de 7 y los 11 años cuando hacen uso de Internet a redes como YouTube, TikTok, WhatsApp, entre otras, tienen como objetivo la investigación, entretenimiento y/o realización de tareas, mientras el 10% tienden a hacer un uso abusivo de las redes que trae posibles influencias negativas para él y su entorno. Dicha investigación demostró la alta vulneración que se puede presentar, considerando que, alrededor del 32% de los niños tienen una foto real en su perfil, el 17.5% de los niños muestra su identidad, el 1.25% de las niñas y el 3.75% de los niños muestra el número telefónico personal, lo que genera una alta preocupación, aunque, si bien, los porcentajes suelen ser bajos, esa es la ventana que requiere un atacante para contactar a las personas y ser exitoso (Tejada-Garitano et al., 2023).

Siguiendo esta línea, al analizar las estadísticas proporcionadas por la Policía Nacional de Colombia a través de su Centro de Atención Inmediata - CAI Virtual en el año 2023, se observa una disminución en los delitos sexuales cometidos a través de Internet. Hasta octubre del 2020, se reportaron 205 denuncias por pornografía infantil en la ciudad de Medellín, y en todo el departamento de Antioquia se registraron 986 denuncias por delitos sexuales sin el uso de armas o de carácter virtual. En comparación con el año 2019, a la misma fecha, Antioquia tenía 1,165 denuncias, lo que sugiere una tendencia a la baja en estos delitos.

Para el 2021, las denuncias extorsivas a menores de edad en Colombia (Figura 1) usando tanto las "redes sociales" y "sin el empleo de armas" asciende a un total de 40 denuncias, con una leve disminución en el 2020 (39 en total), y hasta julio de 2023, en el mismo portal de la Policía Nacional de Colombia, había un total de 28, lo que puede sugerir una proyección más alta que los años anteriores hasta fin de año. El aumento tanto de las extorsiones como de las denuncias genera gran preocupación en la comunidad, sumados a los problemas de ciberseguridad como *phishing* y el acoso cibernético que no alcanzan a ser reportados, en consecuencia, aquello que no se visualiza no podría ser investigado, teniendo como impacto que las adolescentes y familias en general están generando acciones por su propia cuenta (Policía Nacional de Colombia, 2023b).

Figura 1

Estadísticas de las denuncias extorsivas en Colombia



Nota. Se consideran los últimos tres (3) años y filtrado por aplicabilidad a menores de edad. Consolidación propia a partir de los datos estadísticos del portal de la Policía Nacional de Colombia (2023).

Por lo anterior, se han concentrado diferentes esfuerzos para reducir los niveles de visualización de elementos pornográficos por parte de niños y adolescentes en Colombia; en este sentido, el Ministerio de las TIC y el Instituto de Bienestar Familiar (ICBF), dando cumplimiento a la Ley 679 de 2001 "para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores" han generado una estrategia para que los proveedores de servicio puedan bloquear el mayor número de sitios Web con contenido para adultos en donde se mezclan imágenes y videos de menores de edad (Ministerio de las TIC, 2022), con ello, se espera que la proliferación de amenazas cibernéticas como el *sexting* y el *grooming* (haciendo uso de IA) se reduzca considerablemente.

Ahora bien, el uso de métodos estadísticos para realizar pruebas comparadas entre grupos de estudiantes se ha convertido en una herramienta importante para la resolución de problemas característicos de las muestras poblacionales, obteniendo resultados óptimos y precisos, así es como el uso de la prueba t de Student o test-T permite aceptar o rechazar hipótesis nulas cuyos eventos siguen una distribución normal (Prieto-Andreu et al., 2022), sin embargo, para el caso de los estudiantes que usan la tecnología y deben ser medidos con un proceso, debe usarse algún método como prueba no paramétrica. Es necesario entonces validar la cantidad de eventos y muestra poblacional, de allí que para el caso del artículo, la más indicada es el cálculo de la prueba de los signos, ideal para dos eventos y una población menor a 25 estudiantes. Esta prueba hace una comparación de las medianas y usa la probabilidad binomial (Álvarez, 1995).

Las pruebas estadísticas no paramétricas son esenciales en el análisis de datos en muchas áreas, especialmente cuando los datos no cumplen con los supuestos necesarios para las pruebas paramétricas (no obedecen a una distribución normal). Su capacidad para manejar distribuciones no normales, su resistencia a *outliers* y su aplicabilidad a muestras pequeñas y datos ordinales o nominales las convierten en herramientas valiosas en el arsenal del estadístico (Ramírez & Polack, 2020). Esto resulta una ventaja cuando se requiere obtener comparaciones o definir si una hipótesis nula es la adecuada frente a los datos analizados.

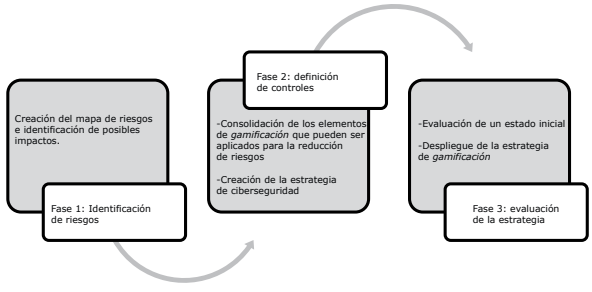
La revolución tecnológica, los cambios generacionales y la amplia disponibilidad de recursos informáticos han exacerbado un problema preexistente: la victimización. Debemos comprender que esta problemática ha evolucionado y se ha camuflado en el mundo virtual. La cibervictimización es un desafío que las organizaciones deben monitorear de cerca y para el cual deben fortalecer y actualizar sus mecanismos y recursos de defensa.

Método

Para la obtención de los resultados, se ejecutaron tres fases (Figura 2), que validan de forma experimental los impactos e incidentes de las amenazas cibernéticas.

Figura 2

Consolidación de fases para el logro de los resultados



Nota. Se inicia con la identificación de riesgos, seguidamente, una definición de controles basada en gamificación y, finalmente, una evaluación de un grupo de estudiantes.

Fase 1: Identificación de riesgos

En esta fase se utilizó la norma internacional ISO 27005:2022 (International Organization for Standardization [ISO], 2022) para la gestión de riesgos. Esta norma establece el proceso para la identificación, valoración y gestión de riesgos de seguridad, entregando como resultado si un proceso u organización puede estar sometido a altos impactos que deben ser tratados de manera inmediata, o generar un plan de tratamiento a corto, mediano o largo plazo. En concordancia, la norma fue usada como mecanismo para la identificación, consolidación y generación de riesgos cibernéticos asociados al *sexting* y *grooming,* con el uso de las siguientes actividades globales:

- *Identificación de las fuentes de riesgos.* En esta actividad se tuvieron en cuenta fuentes organizacionales como el Instituto Colombiano de Bienestar Familiar (ICBF), DQ Institute, la Policía Nacional de Colombia, Asociación Colombiana de Ingenieros de Sistemas (ACIS), entre otras, en las cuales se buscó el uso y consumo de internet por parte de menores de edad, y el análisis de la información documental sobre el tipo de comportamientos que se pudiesen derivar de los excesos en estos accesos.

- *Amenazas y vulnerabilidades.* Mediante un acercamiento a los diferentes mecanismos que un atacante puede ejecutar, así como las vulnerabilidades o debilidades que pueden ser explotadas por atacantes, con una discriminación de lo que acontece con el sexting y grooming. Esta diferenciación es fundamental para entender cada uno de los riesgos que se pueden presentar en los adolescentes, permitiendo establecer una estrategia que combine la toma de conciencia de manera asertiva; o en su defecto, dar a conocer los riesgos a la comunidad, en la espera de ofrecer respuestas futuras en la reducción de posibles impactos.

- *Identificación de posibles impactos:* luego de revisar las fuentes, amenazas y vulnerabilidades que pueden ser usadas, se hace una descripción de los impactos que se pueden generar cuando no existe un control preventivo, periódico y sobre una población objetivo predeterminada. Los impactos pueden ir desde la deserción escolar hasta los problemas judiciales por el abuso físico.

Fase 2

En esta fase, se establecen diferentes mecanismos de *gamificación* que pueden servir como controles a los riesgos identificados, contemplando la reducción de posibles impactos los cuales se espera que sean efectivos una vez se realice una implementación. Los diferentes controles propuestos se centran de manera independiente para el *sexting* y *grooming*, con ello, la propuesta de control para la reducción de riesgos es a través de un software en línea, permitiendo que la comunidad, a través de lo interactivo y uso del Internet, pueda contar con un proceso de toma de conciencia, conocimiento de riesgos y aplicación en otras personas que estén expuestos a los mismos flagelos.

Cada uno de los controles propuestos son definidos validando los riesgos que podría mitigar; así, la estrategia a ser implementada permite identificar de manera más precisa la intervención sobre las problemáticas y la forma de actuar dependiendo de la posible amenaza. Estos mecanismos de reducción de riesgos establecen la forma en que, a partir de los elementos específicos en cada afectación, se toma uno o varios controles que logren reducir en buena parte la problemática, y esto, supeditado a que la implementación sea adecuada, consistente y periódica. Esto implica que profesores y padres de familia establezcan una línea de actuación fuerte, consistente e insistente, dado que en que Internet tiene diferentes amenazas para combatir.

En las diferentes actividades se realizaron consultas en portales especializados en ciberseguridad, delitos informáticos y de protección de menores, como lo es la Policía Nacional de Colombia, Unicef, INCIBE, entre otros, de donde se extrajo información relevante y aportante para la reducción de la problemática y que se puede implementar en diferentes ambientes. Para lograr la propuesta de estrategia de ciberseguridad, se ejecuta una ruta de cumplimiento (Figura 3) que permitió de una forma acertada lograr el objetivo. Esta ruta se inicia con la consecución y definición de los tipos de

gamificación que pueden ser oportunos para la problemática exhibida, que lleva a caracterizar cómo, a partir del acceso en línea, los adolescentes podrían interactuar de una forma didáctica conociendo los riesgos y planteando salidas a eventos que se puedan presentar.

Seguidamente, se hace una definición de controles que utilizan las mismas características de los juegos en línea, toda vez que esto va a permitir que se consoliden los mecanismos en el día a día. En cada control se usa una definición con el fin de entender qué es, para qué sirve y qué riesgos cubre; y finalmente, se desarrolla una propuesta de estrategia de ciberseguridad que logre abarcar los riesgos identificados y sirva como mecanismo proactivo entre los adolescentes (Figura 3).

Fase 3

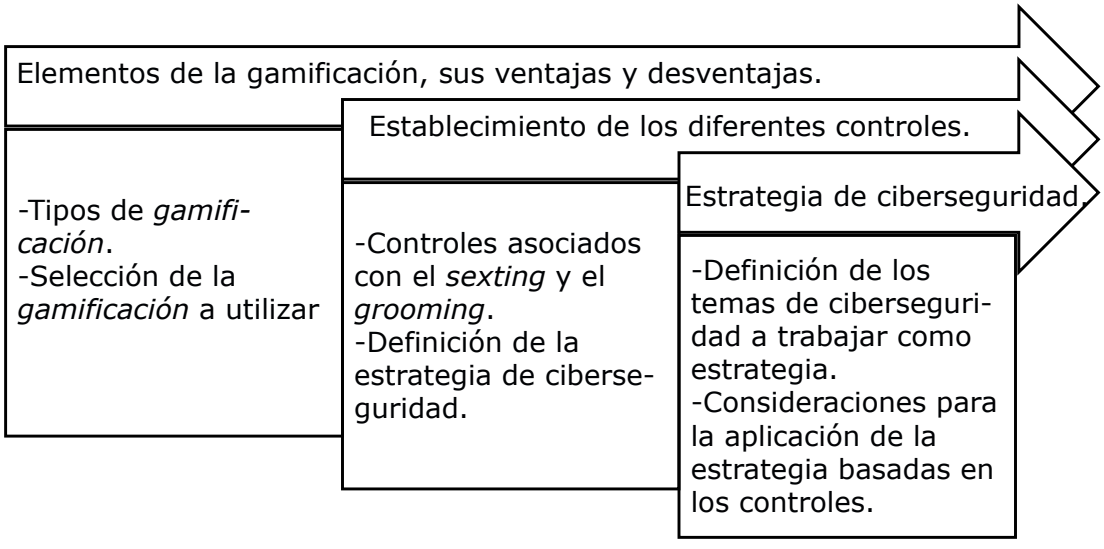
En esta etapa se ejecutaron tres actividades: la primera fue la definición de la estrategia de ciberseguridad a usar con base en riesgos y controles; la segunda está asociada con la prueba diagnóstica inicial para conocer qué tanto los estudiantes se acercan a los conceptos de ciberseguridad y riesgos en Internet, y una tercera actividad que busca desplegar la estrategia creada como propuesta de intervención.

Para validar la estrategia de seguridad informática, se llevó a cabo un estudio de caso en una institución educativa en la ciudad de Medellín, Colombia. Este centro educativo fue seleccionado por su relevancia y para proporcionar una visión práctica de la implementación de la estrategia. En este contexto, se proporciona información básica sobre el centro, incluyendo su perfil demográfico y aspectos clave relacionados con la población estudiantil.

Es necesario precisar que, debido a que dentro del caso de estudio se encuentran menores de edad, se gestionaron los permisos y autorizaciones necesarias, estas, dadas por el señor rector de la institución educativa y con el acompañamiento permanente del coordinador disciplinario y de un profesor de la institución. En ese sentido, no hay registro fílmico ni imágenes, las evidencias para el análisis se basan en la discusión y conclusiones que se toman desde el sitio web en donde se realizaron las pruebas de forma anónima.

Figura 3

Ruta de cumplimiento para llegar a la estrategia de ciberseguridad



Nota. Para el cumplimiento de la estrategia se consolida en tres pasos que reúnen todos los procedimientos necesarios para el logro de los resultados.

Una vez definido el centro educativo para el caso de estudio, se procedió a realizar una evaluación inicial de su infraestructura y de sus prácticas de seguridad informática. Es importante destacar que este proceso se llevó a cabo con la autorización de los directivos de la institución, quienes permitieron aplicar la evaluación y llevar a cabo la ejecución de las acciones correspondientes a la validación de la estrategia de seguridad.

La valoración se desarrolló en varias fases (Figura 4), se inició con una descripción de la institución, una evaluación inicial y otra al final. En la primera fase se ejecutó una prueba diagnóstica para entender el nivel de comprensión de los adolescentes con el fin de desplegar la estrategia, para el estado final se realizó un comparativo con la prueba diagnóstica y generaron las recomendaciones respectivas.

Por lo tanto, como primer paso en la implementación de los temas de ciberseguridad, se procedió a desarrollarla en una de las clases de la Institución Educativa Sebastián de Belalcázar. Esta institución tiene una historia de 41 años y está localizada en el barrio Belalcázar, al noroccidente (comuna 5) de la ciudad de Medellín, Colombia. Está cerca de la Feria de Ganado de Medellín (sitio emblemático y representativo). La institución cuenta con dos sedes, una para preescolar y primaria, y otra para secundaria. En total, alberga cerca de 520 estudiantes, cuenta con 21 docentes, un coordinador y un rector, y ofrece clases en las jornadas de mañana y tarde.

Es importante destacar que diferentes estudiantes provienen de familias que migraron desde subregiones de Antioquia, como Segovia y Tarazá, así como de la costa norte de Colombia y otras áreas del departamento de Chocó. Esta diversidad de orígenes culturales y geográficos agrega un aspecto adicional de relevancia a la implementación de la estrategia de seguridad informática en la institución. Es de resaltar que, los estudiantes tienen una mezcla cultural importante y el acceso a la tecnología y el conocimiento de la misma varía dependiendo de la región de origen y la estrategia que tiene la institución educativa para implementar los modelos pedagógicos.

Los estudiantes que participaron en el conjunto de pruebas tienen edades entre los 9 y los 15 años, y es importante destacar que ninguno de ellos presenta dificultades significativas en el aprendizaje.

La ubicación geográfica de la institución en Medellín, Colombia, se puede observar en la Figura 5.

Figura 5

Ubicación geográfica de la institución en Medellín, Colombia

Nota: la institución de educación está ubicada en el norte de la ciudad de Medellín, Colombia.

Fuente: Google (s. f.).

Figura 4

Ruta para la validación de la estrategia de ciberseguridad

Nota. La estrategia consta de cinco pasos e inicia con la definición del caso a estudiar y finaliza con el análisis de resultados.

Se inició con una sesión informativa para todos los estudiantes, en la que se les explicó en qué consistiría la prueba. Se les informó que se llevaría a cabo una encuesta inicial que incluiría preguntas fundamentales relacionadas con la tecnología y el uso de términos como *sexting* y *grooming*. Además, se proporcionó una pequeña definición de estos términos, enfatizando sus riesgos asociados. Posteriormente, se aplicó la prueba que contenía preguntas formuladas a partir de la información previamente proporcionada sobre estos riesgos.

El sistema de medición está asociado con una muestra de estudiantes a los cuales se les realizó la prueba diagnóstica para conocer sus perspectivas frente al tema y las problemáticas del entorno, de ello se generó una valoración en porcentaje que representa el nivel de entendimiento inicial (de 0% a 100%, siendo 100% el porcentaje mayor en la prueba). Se considera superada la prueba cuando se da respuesta acertada a más del 50% de las preguntas. Luego se socializan los conceptos y se pone en marcha la estrategia de ciberseguridad mediante la gamificación, luego se hace una medición final, y con la diferencia entre la medición 1 y la 2 (final) da el peso de cómo avanzar en mecanismos que influyen en la percepción, conocimiento y reducción de impactos y el quehacer diario de los adolescentes frente a los problemas de Internet.

Para la obtención del resultado sobre si la intervención a través de la socialización y la estrategia de ciberseguridad fue positiva, se consideró la prueba no paramétrica de los signos para dos muestras (medición inicial y medición final). Esta prueba consiste en contrastar dos grupos iguales medidos en dos momentos diferentes, haciendo uso de la distribución binomial para hipótesis unilaterales. Para ello, se han definido el siguiente procedimiento, variables, así como estas hipótesis:

- *Ho (hipótesis nula)*: el plan de capacitación y estrategia preventiva en ciberseguridad a través de la gamificación no aumenta los niveles de toma de conciencia sobre el *sexting* y el *grooming* en los adolescentes.
- *H1 (hipótesis alternativa)*: el plan de capacitación y estrategia preventiva en ciberseguridad a través de la gamificación aumenta los niveles de toma de conciencia sobre el *sexting* y el *grooming* en los adolescentes.
- *Nivel de confianza:* 95%, con nivel de significación (α) en 0.05. Lo que indica que la probabilidad de que la población está dentro de los límites es el 95%.
- *Fórmula*: la fórmula (a) para muestras pequeñas (binomial), aquellas que tienen menos de 25 eventos o elementos:

$$p(x) = \left(\frac{N}{x}\right) \qquad \text{(a)}$$

  - » Donde *N* es el número de casos que tuvo diferencias
  - » Donde *x* hace referencia al número menor de signos.

El procedimiento para el cálculo y obtención de los valores para la fórmula es el siguiente:

- Si el valor de la primera medición es mayor a la segunda, se fija en el signo (+).
- Si el valor de la primera medición es menor a la segunda, se fija en el signo (-).
- Si los valores de ambas mediciones son iguales, se fija en (0).
- Para obtener (x) se contabiliza el número menor de signos.
- Para obtener (N), se contabilizan los signos con diferencia o (+).

La hipótesis nula Ho será válida, si el valor p(x) es mayor que 0.05 que es el nivel de significación, de lo contrario, debe rechazarse y será válida la hipótesis alternativa (Ruiz & Martín, 2005).

Para la realización de la prueba diagnóstica, se hizo uso de la herramienta en línea *Is 4k Internet* Segura *for Kids* del Instituto Nacional de Ciberseguridad del gobierno de España (INCIBE). Esta herramienta (Figura 6) permite establecer a qué riesgos se enfrentan los adolescentes y niños en Internet, así como los conceptos de ciberseguridad, la cual se puede consultar en línea en https://www.is4k.es/de-utilidad/test

Figura 6

Enlace para la encuesta inicial desarrollada por INCIBE

Nota. La figura muestra cómo desde el portal de INCIBE se puede iniciar la encuesta a los menores de edad. Las preguntas se enfocan en descubrir el nivel de conocimiento sobre los diferentes riesgos en Internet.

Fuente: https://www.is4k.es/de-utilidad/test

Las preguntas realizadas para entender el contexto inicial son:

a. Sobre el *ciberbullying* o ciberacoso escolar ¿Cuáles son las principales características?

b. ¿Cuál es menos grave, el ciberbullying o el tradicional acoso escolar?

c. ¿Conoce qué es la identidad digital?

d. ¿Es lo mismo control parental que mediación parental?

e. ¿Piensas que la adicción a las drogas tiene el mismo efecto que la adición a las nuevas tecnologías?

f. ¿Qué es el *grooming*?

g. ¿Cuál cree que es el principal riesgo que tiene el *sexting*? Siendo el *sexting* cuando los jóvenes ejecutan acciones en las redes sociales para llamar la atención.

h. ¿Considera que el software antivirus reduce las infecciones?

Finalmente, en la creación de la estrategia de ciberseguridad se tuvieron en cuenta tanto los riesgos encontrados en la fase 1 como los resultados de la prueba diagnóstico. Así se generan una serie de controles luego del análisis de los resultados que permiten hacer una intervención para reducir los niveles de exposición frente al *sexting* y *grooming*. En esta actividad se tuvieron en cuenta tanto los riesgos administrativos como los técnicos.

Resultados

Después de definir la metodología, en cada fase se obtienen una serie de resultados que conllevan a que la estrategia de seguridad sea posible.

Fase 1. Identificación de riesgos

El índice de seguridad infantil en línea presentado por DQ Institute (2022) considera aquellos países que tienen diferentes estrategias para la protección de niños y niñas en Internet. Algunos de los factores que se analizan son las competencias desarrolladas por los menores como apoyo familiar, políticas y regulaciones. Así mismo, en el 2022 (Figura 7), Inglaterra fue el país con mejores oportunidades para los menores con un puntaje de 81.3, seguido de Japón, mientras que Burundi (África) ocupa el último lugar. Así mismo, Colombia ocupa el puesto 12 del ranking, lo que sugiere que los mecanismos usados prevalecen y apoyan la protección de los menores, aunque falta por desarrollar e implementar.

En esa misma línea, en una consulta más particular para Colombia (Figura 8) se evidencia que, aunque se tienen diferentes aspectos mejorados, es necesario mejorar aquellos que hace falta trabajar como fuentes de riesgos. Es el caso de la infraestructura de ciberseguridad a nivel país que permita la identificación, revisión y control de diferentes contenidos en línea que puedan llegar a menores de edad y que su acceso permita cualquier abuso (DQ Institute, 2022). En ese sentido, la escala de medición establece una escala baja (indicador izquierdo), media (indicador centro), o alta (indicador derecho) de acuerdo con las políticas, inversiones y estrategias en los países; para los factores relevantes como la protección en línea de "política y regulación", la "educación escolar" y la ciberseguridad en "infraestructura tecnológica", se tiene una valoración alta, esto es, el país cuenta con los recursos, estrategias y mantenimiento necesarios para fortalecer la reducción de riesgos en Internet. Otros factores están por mejorar como las competencias digitales de los niños, la privacidad, seguridad y el acceso a Internet desde las escuelas y hogares.

Figura 7

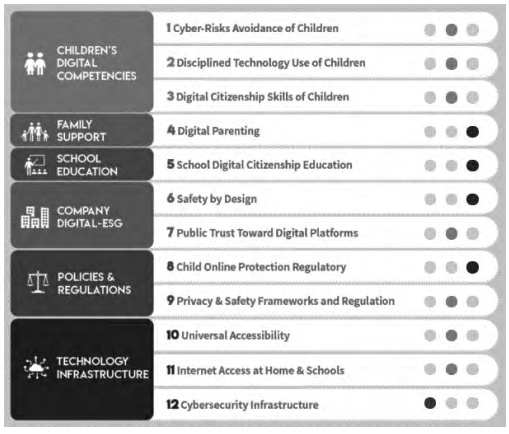
Ranking de países que tienen mecanismos de protección de menores frente a los accesos en línea

RANK	COUNTRY	COSI SCORE
1	United Kingdom	81.3
2	Japan	80.4
3	India	79.9
4	Australia	73.5
5	China	72.1
6	Italy	71.5
7	Singapore	70.8
8	Germany	70.2
9	Republic of Korea	69.6
10	United States of America	67.6
11	Peru	67.2
12	Colombia	67.0
13	Spain	66.7
14	Philippines	66.1
15	Canada	65.2

Nota. La figura establece las diferencias entre los países que tienen o procuran la protección de los menores. La lista está encabezada por Inglaterra y Colombia ocupa el puesto 12 por encima de España y Canadá (DQ Institute, 2022).

Figura 8

Particularidades de Colombia frente el acceso y protección de menores en línea



Nota. La figura establece una medición del estado de diferentes características analizadas en estamentos de la sociedad como los procesos judiciales, el estado de la educación y la tecnología (DQ Institute, 2022).

De acuerdo con la Asociación Colombiana de Ingenieros de Sistemas (ACIS, 2021), se determinó que el 15% de los niños en Latinoamérica pasan más de cuatro horas conectados a internet mediante un dispositivo móvil, y quienes llevan la delantera al respecto son los menores argentinos con 24%, seguidos por chilenos (21%) y brasileños (18%). Más atrás se ubican colombianos (12%), peruanos (7%) y mexicanos (7%). Esta exposición y uso de la red global establecen un alto índice en su probabilidad que, durante esas horas de navegación haya posibles abusadores cibernéticos que utilicen sus estrategias con los menores.

Se destaca que los adolescentes latinos pasan en promedio entre 6.5 y 7.5 horas al día frente a una pantalla de entretenimiento. Esta cifra ilustra ilustra la importante cantidad de tiempo que pasan interactuando con medios digitales y resalta la importancia de comprender y abordar los posibles impactos que esta exposición constante puede tener en su desarrollo y comportamiento. Finalmente, el 71% de los padres de niños más pequeños tienen una preocupación importante por el uso no medido de las redes y servicios en línea (Brooke et al., 2020) y para el 2023 con el auge y aumento de la era digital, la preocupación debe ser mayor.

Según el ICBF (2021), el desconocimiento o la falta de compromiso de padres, familiares e instituciones, a menudo se traduce en una supervisión insuficiente y una gestión deficiente de las actividades y comportamientos de menores de edad en su uso de las redes e Internet. Al analizar el patrón de consumo de redes sociales, se observa que está directamente relacionado con la presencia de jóvenes y adolescentes que tienen perfiles o cuentas en estas plataformas. Además, se evidencia que aquellos encuestados que tienen acceso y utilizan estas redes comparten contenido y suben o publican información en ellas. Es fundamental reconocer la importancia de la supervisión y la orientación por parte de los adultos y las instituciones para guiar a los jóvenes en su interacción en línea para asegurar que utilicen estas herramientas de manera segura y responsable.

Partiendo de este análisis, hay diferentes amenazas y vulnerabilidades que rodean los riesgos hacia los adolescentes, en la consolidación de las fuentes. En la Tabla 1 se tienen diferentes

situaciones que ejecutadas podrían generar la victimización por *grooming* (con un alto impacto en las personas).

Por otro lado, para los temas de *sexting*, en la Tabla 2 se presentan diferentes situaciones que pueden consolidar e impactar a los adolescentes.

Tabla 1

Riesgos, vulnerabilidades y amenazas por Grooming

Riesgo	Amenaza	Vulnerabilidad
Grooming	Abuso infantil	Demasiado tiempo de exposición en redes sociales
		Permitir solicitudes de desconocidos
		Difundir información personal sin control
		Permitir chantaje y extorsiones
	Ciberacoso	Generar relaciones próximas con personas de otras edades
		No hacer la denuncia oportuna
		Poca o nula supervisión de padres o adultos responsables
	Sexting	Recibir dinero u otro incentivo para acceder a algo
		Enviar y recibir contenido sexual
		Enviar y recibir datos personales

Nota: debido al uso no controlado de las redes sociales, los adolescentes tienden a ser vulnerables frente a diferentes amenazas, lo que permite evidenciar las actividades de atacantes que finalizan en la explotación del riesgo de *grooming*.

Tabla 2

Establecimiento de amenazas, riesgos y vulnerabilidad por sexting

Riesgo	Amenaza	Vulnerabilidad
Sexting	Robo de información, contenidos y fotos	Cuentas en redes sin control de seguridad.
		Contraseñas poco seguras o genéricas.
		Usar redes públicas de parques, centros comerciales o colegios.
		Compartir contenidos personales y explícitos en redes sociales.
		Falta de capacitación en el manejo de redes e Internet.
	Distribución o publicación de fotos privadas o de contenido explícito	Guardar fotos, medios o contenidos explícitos y privados en cualquier repositorio.
		Compartir fotos del cuerpo con poca ropa.
		Establecer relaciones vía web en las cuales se considere la transferencia de contenidos sexuales.
	Sextorsión	Participar de la práctica de sexting.
		Acceder a pretensiones de desconocidos.
		No denunciar ante las autoridades correspondientes.
	Ataques físicos	Confiar plenamente en la discreción del destinatario.
		Sentir presión de algún grupo que lleve a ganar notoriedad y aceptación en el contexto digital.
		Temor a pérdida reputacional.

Nota: son cuatro las amenazas principales que pueden desencadenar diferentes vulnerabilidades en los adolescentes que tienen contacto diario con la tecnología sin el acompañamiento necesario (Usma, 2022).

Se puede apreciar (Tablas 1 y 2) que se identificaron tres amenazas y diez vulnerabilidades relacionadas con el *grooming*, y en el caso del *sexting* se encontraron cuatro amenazas principales y quince vulnerabilidades. Esto sugiere un riesgo significativo para los menores de edad que están constantemente en contacto con la tecnología o recursos digitales sin una adecuada capacitación o supervisión. Es fundamental abordar estas amenazas y vulnerabilidades a través de la educación y la concienciación para garantizar que los jóvenes puedan utilizar la tecnología de manera segura y responsable. Así mismo, de acuerdo con las fuentes de riesgos, los diferentes atacantes tienen muchas posibilidades de llegar a los adolescentes, considerando el uso de las TIC y el aumento de personas en las redes sociales e Internet.

De esta manera, son diferentes los impactos que pueden generarse a partir de la consolidación de los riesgos. Lamentablemente, ser víctima de *sexting* y *grooming* no conlleva impactos positivos evidentes, aparte de las lecciones que se pueden extraer de estas experiencias. Los impactos que traen estas vulnerabilidades varían ampliamente, desde advertencias leves hasta consecuencias legales con efectos físicos y emocionales significativos. Es fundamental destacar que estas situaciones pueden tener repercusiones graves en la vida de las personas afectadas, subrayando la importancia de la prevención y la educación en el uso responsable de la tecnología para evitar estos riesgos. Dentro de estos se encuentran (Ledesma, 2023; Kaspersky, 2016; Instituto Colombiano de Bienestar Familiar, 2021; Agencia de la Unión Europea para la Cooperación Policial [Europol], 2022; Policía Nacional de Colombia, 2020):

- *Pérdida reputacional*: cuando las imágenes llegan a internet, ya no se tiene control de esto, por lo tanto, podrían terminar en sitios de pornografía.
- *Sextorsión*: cuando una o varias personas hacen uso de las imágenes para pedir dinero u otro recurso por devolverlas.
- *Prostitución*: se ha encontrado casos de personas que, al caer en sextorsión, le dan continuidad a través de actividades como prostitución o *webcam*.
- *Problemas psicológicos*: es claro que, ante la divulgación de datos personales cuando se vuelven de escrutinio público, se provoca una afectación en la persona.
- *Problemas económicos*: cuando se trata de chantaje derivado del *sexting*, las pérdidas económicas pueden ser grandes.
- *Abuso sexual*: ante el *grooming*, la consolidación y el objetivo final de este riesgo es que un menor de edad puede ser perpetrado sexualmente.

Otro grupo de riesgos de índole tecnológico son los asociados con los códigos maliciosos o *malware;* estos pueden ejecutarse en los sistemas de búsqueda de imágenes o videos y enviarlos a Internet.

Fase 2. definición de controles

Para definir los diferentes controles, es preciso establecer los tipos de gamificación:

- **Gamificación educativa:** entender el conocimiento a partir del juego es una estrategias que tiene los mejores resultados entre los niños, niñas y adolescentes, lo que permite un cambio dentro del aula (Baldeón et al., 2017).
- **Gamificación empresarial:** las empresas tienen un potencial para sus empleados, con ello, el proceso de capacitación a través de la gamificación puede aumentar ese espíritu empresarial y de pertenencia (Cortés et al., 2020).
- **Gamificación en redes sociales:** un escenario perfecto para masificar las estrategias con diferentes públicos y puede establecer elementos diferenciadores sin importar las distancias físicas (Tortosa et al., 2017).

Tomando en cuenta los tipos de estrategias, y para el objetivo de este artículo, la gamificación educativa es la indicada; un estudiante o grupo de estudiantes puede generar un proceso diferenciador con respecto al proceso de aprendizaje, por ello, es la estrategia más usada para reducir los niveles de exposición de los riesgos. Ahora bien, diferentes controles pueden ser aplicados para la reducción de

riesgos (ver Tabla 3), y de ellos se pueden resaltar temas como las contraseñas seguras, reconocer las situaciones y tomar conciencia, así como hacer la respectiva denuncia.

Fase 3. Evaluación de la estrategia

La estrategia de ciberseguridad comprende, entre otras:

- La definición del público objetivo que puede intervenirse a partir de la identificación de fuentes de riesgos.
- Validación de los ciberriesgos identificados, con el fin de comprobar la existencia de vulnerabilidades en la población y los posibles impactos que se pueden generar.
- Aplicación de la estrategia de controles, asociados al *sexting* y el *grooming*, considerando el mismo proceso de sensibilización que debe hacerse a través de la gamificación.
- La socialización debe darse en aras de que, los adolescentes en sus aulas de clase comprendan los riesgos a los que están expuestos y que dichos riesgos vienen con la tecnología, lo que genera probabilidades dentro y fuera del aula.
- Revisión de resultados y retroalimentación del sistema, esto implica establecer líneas de acción para las mejoras que deben hacerse en las escuelas.

Actividad de validación inicial. Acorde con la definición metodológica, se aplicó la encuesta a un grupo de adolescentes de la Institución Educativa ya relacionada. En la Figura 9 se observan los diferentes resultados, tomados como la prueba diagnóstica.

Tabla 3

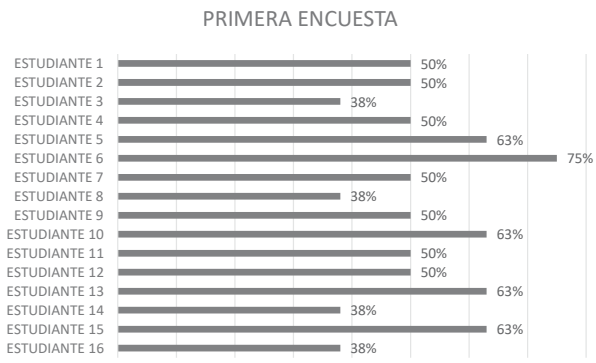
Controles para la reducción de riesgos de sexting y grooming que pueden ser implementados

Riesgo	Control	Estrategia de gamificación
Sexting	Mejorar el uso de las redes sociales.	• Juegos de superación de retos y trivias como complemento del conocimiento. • Videos ilustrativos. • Juegos que simulan la denuncia y el rechazo a los atacantes.
	Aplicar el concepto de contraseñas seguras.	
	Conocer sobre las redes públicas.	
	Concientización sobre qué publicar en Internet.	
	Capacitación en el manejo de medios digitales y validación de a quién se acepta como "amigo" en las redes.	
	Entregar información sobre lo que es *sexting* como riesgo.	
	Recomendaciones sobre las relaciones virtuales.	
	Instruir sobre el proceso de hacer la denuncia.	
Grooming	Estrategias para reconocer quién puede estar al otro lado de la red.	• Video y prueba acerca del uso de Internet. • Juegos que permiten construir desde el hacer. • Juegos para conocer el engaño en Internet.
	Reconocerse como persona y los signos generados a partir de la información que se solicita al otro lado de la red.	
	Capacitar con respecto al *grooming*.	
	Mecanismos para denunciar cualquier situación de acoso.	
	Mantener los equipos de cómputo actualizados y con un sistema antivirus.	

Nota: en el *sexting* se pueden tener ocho controles y para el *grooming* son cinco controles, todos consolidados con diferentes estrategias de gamificación.

Figura 9

Resultados obtenidos con la aplicación de la encuesta inicial



Nota. Al finalizar la prueba, con 8 preguntas para 16 estudiantes, el sistema arroja un resultado entregado en porcentajes por cada estudiante.

Sobre los resultados obtenidos en la prueba diagnóstica, se observa que entre el 38% y el 50% de los estudiantes respondieron correctamente a la mitad o más de las preguntas, mientras que por encima del 60% restante respondió a menos de la mitad de las preguntas de manera adecuada. Este indicador no es satisfactorio, por lo que enfatiza en que hay poco conocimiento por parte de los estudiantes en cuanto a los conceptos básicos de seguridad, *sexting* y *grooming*. Esta carencia de comprensión subraya la necesidad de implementar una educación más efectiva sobre seguridad en línea y promover la concienciación entre los estudiantes para abordar estos importantes temas y reducir los riesgos asociados. Luego de los resultados preliminares, se inició el proceso de sensibilización, tomando como base los riesgos obtenidos, el estado del conocimiento de los estudiantes y la estrategia de gamificación apropiada.

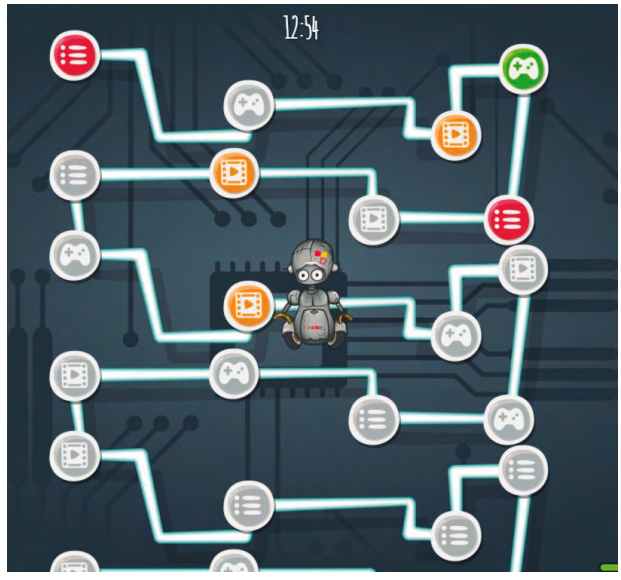
Utilizando todos los elementos de gamificación seleccionados y aplicando los controles previamente establecidos en relación con el *sexting* y el *grooming*, se procedió a implementar la estrategia de seguridad informática. Esta estrategia considera las salvaguardias previamente documentadas para abordar los riesgos asociados con el *sexting* y al *grooming*. En la planeación de esta estrategia, se utilizó la aplicación pública y gratuita disponible en https://cyberscouts.osi.es/ (INCIBE, 2022).

A los estudiantes seleccionados se les pidió que jugaran durante 40 minutos en cada uno de los elementos que ofrece la plataforma, completando todos los desafíos, pruebas breves y cuestionarios interactivos de manera didáctica. Además, se les permitió repetir la actividad en niveles de dificultad más altos si lograban completar todos los desafíos en el nivel inicial. Es importante mencionar que la plataforma proporciona opciones de dificultad que incluyen Fácil, Medio y Alto para adaptarse al nivel de competencia de los estudiantes (Figura 10).

La plataforma consta de tres elementos diferentes a través de los cuales los estudiantes navegan de manera educativa. Durante la selección de uno de estos elementos, se les proporciona información relevante sobre los riesgos asociados al sexting y al grooming. Además, en paralelo con esta información, se implementaron los controles que se proponen para abordar estos riesgos.

Figura 10

Mapa del sitio de juego cyberscouts



Nota. A cada estudiante se le pidió navegar de manera ordenada por cada una de las opciones para conocer los posibles riesgos y estrategias que se frente a los impactos generados.

Fuente: https://cyberscouts.osi.es/

En la misma línea de acción, se llevó a cabo una segunda aplicación de la encuesta utilizando los mismos elementos que se emplearon en la prueba diagnóstica inicial para evaluar el conocimiento de los estudiantes. Esta segunda encuesta se realizó después de haber implementado la estrategia gamificada que incluyó

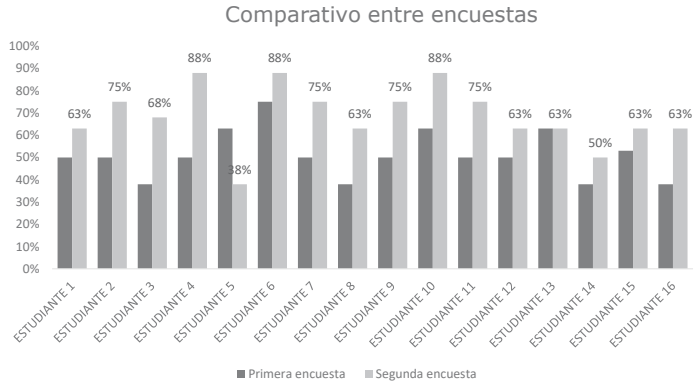
reuniones con los estudiantes, explicación de los riesgos de ciberseguridad y las posibles repercusiones de sus acciones en línea.

Se procedió a realizar un análisis cuantitativo del estado de la población después de la implementación de las actividades y los controles de la estrategia. Esta revisión se realizó con la misma población y la aplicación del mismo cuestionario que se empleó en la etapa inicial, con las mismas ocho preguntas, con el objetivo de recrear un escenario similar al de la primera encuesta y evaluar la efectividad de la estrategia en la mejora del conocimiento y la concienciación de los estudiantes sobre los riesgos en línea (Figura 11).

En las líneas de tendencia de la cuarta columna se puede observar un comportamiento ascendente, lo que refleja el estado inicial de las respuestas de los estudiantes. Sin embargo, otro resultado igualmente importante es el caso del estudiante número 5, quien representa una desviación en la muestra. Ahora bien, para responder a las hipótesis antes planteadas, se ejecutó el procedimiento estadístico de la prueba de los Signos con base en la tabla binomial (Tabla 4), para ello, se han tabulado los resultados de las dos pruebas ejecutadas (Figuras 9 y 11):

Figura 11

Evaluación del estado final y tendencia, comparado con el estado inicial



Nota: se puede evidenciar una notable mejoría en el proceso con respecto a la medición inicial.

Tabla 4

Controles para la reducción de riesgos de sexting y grooming que pueden ser implementados

Test inicial	Test final	Valor	Test inicial	Test final	Valor
38%	63%	-	38%	75%	-
63%	75%	-	50%	88%	-
38%	68%	-	75%	75%	0
63%	88%	-	63%	63%	0
50%	38%	+	5%	63%	-
50%	88%	-	38%	50%	-
63%	75%	-	50%	63%	-
50%	63%	-	50%	63%	-

Nota: elaborado por los autores a partir de los resultados obtenidos por la herramienta de gamificación. De acuerdo con el procedimiento en la columna 3, si la primera medición es mayor a la segunda, se fija el signo (+), si es menor va el signo (-) y si es igual el valor es (0).

Ahora bien, para dar solución a la prueba no paramétrica:

x = 1, el número menor de signos fue el (+)

N = 13, número total de diferencias

En ese sentido, se tiene:

$$p(x) = \left(\frac{N}{x}\right) = \frac{13}{1} = 13 \quad \text{(b)}$$

Se hace la búsqueda de los valores en la tabla binomial (Tabla 5), con un valor n=1 y N=13 se obtiene el valor de 0.002, que comparado con un α = 0.05 es menor, por lo cual y de acuerdo con lo ya definido, se debe rechazar la hipótesis nula H0 y aceptar la hipótesis alternativa H1 que indica que el plan de capacitación y estrategia preventiva en ciberseguridad a través de la gamificación, aumenta los niveles de toma de conciencia sobre el *sexting* y el *grooming* en los adolescentes, esto, con base en los resultados.

Tabla 5

Tabla binomial para la búsqueda de valores calculados

	0	1	2	3	4	5	6
5	0.031	0.388	0.500	0.812	0.987		
6	0.010	0.109	0.344	0.056	0.801	0.984	
7	0.008	0.062	0.227	0.050	0.773	0.938	0.992
8	0.004	0.035	0.145	0.363	0.637	0.855	0.965
9	0.002	0.020	0.090	0.254	0.500	0.740	0.910
10	0.001	0.011	0.055	0.172	0.377	0.623	0.828
11		0.006	0.033	0.113	0.274	0.500	0.720
12		0.003	0.019	0.073	0.104	0.387	0.613
13		0.002	0.011	0.046	0.133	0.291	0.500
14		0.001	0.008	0.029	0.090	0.212	0.395

Nota. Para efectos prácticos, se ha extraído parte de tabla binomial (Walker & Lev, 1953) para la validación de los valores calculados (x) y (N).

El proceso reveló una notable mejora en los resultados de la mayoría de los estudiantes, lo que sugiere que los conocimientos adquiridos con la implementación de la estrategia contribuyeron a comprender los riesgos asociados con el *sexting y al grooming*.

Discusión

Entender el sentido del acoso por Internet es clave para que lo profesores y padres de familia, establezcan una línea de actuación para los adolescentes que tienen a su cargo; por ello, se espera que las estrategias de ciberseguridad en el uso coherente, sano y responsable de la tecnología, de acuerdo con aquello que se pretenda reducir como riesgo. Según los autores Agustina & Gómez-Durán (2016) en un estudio sobre la posibilidad de que el *sexting* impacte a los universitarios, se comprueba que efectivamente la tasa de prevalencia sobre dicha conducta es alta, a pesar de que la mayoría de los estudiantes están por encima de los 18 años, considerando que las personas a través de las redes hacen o dicen cosas que normalmente no harían en ámbitos netamente físicos (reuniones y eventos sociales).

Así mismo, la gamificación en las aulas de clase permite potencializar y reconocer que los menores de edad crecieron con la tecnología, lo que genera una ventaja a la hora de fortalecer los procesos de aprendizaje. Esto conlleva a que los estudiantes que usan la gamificación como mecanismo de obtener conocimientos, tienen mejores resultados en las diferentes pruebas (Alarcón et al., 2020), por esto, la aplicabilidad de las diferentes técnicas para el reconocimiento y control de amenazas cibernéticas con base en los resultados obtenidos con 16 estudiantes, se supone un logro a la hora de reducir los diferentes riesgos.

Por otro lado, para los casos de *grooming,* la recomendación, una vez identificado el posible evento, es denunciar ante las autoridades los hechos que conllevarían a la posible violación de los derechos de los niños, niñas y adolescentes, así como emprender un proceso de socialización y sensibilización frente al tema. Esto debe ser coherente con la fortaleza que supone dejar la vergüenza de tener que informar sobre el tema, lo que genera que los atacantes aprovechen cada vez más la situación y puedan llegar a su cometido (Instituto Nacional de las Tecnologías de Comunicación [Inteco], s. f.). En esa línea, la gamificación planteada como opción, es una alternativa que puede funcionar en

diferentes escenarios y países, solo se requiere un nivel de conciencia de las directivas de los colegios o de los mismos padres de familia para llevar a cabo las actividades.

Cuando se realiza la primera medición, los estudiantes establecen una relación con el sistema en línea y buscan dar solución a diferentes situaciones que son desconocidas y que no llevarían a respuestas concretas o que hayan establecido en el mismo proceso escolar, esto supone un primer reto para superar barreras de ese conocimiento particular. Esto se evidencia por los porcentajes bajos en la medición, en donde, si bien, los estudiantes tienen un contacto continuo con la tecnología, los riesgos de esta actividad son ignorados o no se conocen.

Así mismo, el porcentaje inicial puede dar cuenta del mismo conocimiento que puede o debe ser impartido desde el centro escolar, por tanto, es un llamado a los docentes y directivos para que se apropien de ese conocimiento y establezcan mecanismos de atención como lo indica la Ley 1620 de 2013, la cual establece que las entidades escolares deben generar los mecanismos, rutas de atención y respuesta para la "Educación para la Sexualidad y la Prevención y Mitigación de la Violencia Escolar". De esta manera, la educación de los niños y niñas se genera desde diferentes perspectivas, como complemento de los procesos de enseñanza y aprendizaje y fortalecimiento de los controles frente a las diferentes amenazas en Internet.

Aunque la población objetivo tiene una relevancia para el centro de educación, considerando la cantidad de estudiantes de la prueba de concepto, es claro que esto no se acerca a un dimensionamiento para todas las instituciones. Dicha muestra poblacional solo tiene en cuenta las problemáticas alrededor de las aulas de clase, instituciones y personas menores de edad que hacen uso de las redes digitales, sin las consideraciones suficientes y necesarias para la identificación de riesgos asociados y cómo prevenirlos o corregirlos. En ese sentido, se requiere establecer una línea de acción más amplia en diferentes colegios a través de estrategias que le permitan al cuerpo docente entender, comprender, apropiarse y aplicar la ley y las recomendaciones que existen en la era digital, máxime que cada vez son más estudiantes los que tienen acceso casi sin restricciones a redes como Internet.

A partir de diferentes roles y estrategias, la gamificación permite establecer y fortalecer diferentes conceptos de la ciberseguridad, permitiendo que las personas sin conocimiento previo en las temáticas puedan acercarse a las que más riesgos generan cuando se tiene un acceso en línea y se desconoce quiénes están al otro lado de la red (Álvarez, 2021). Estos procesos de enseñanza y aprendizaje pueden ser útiles cuando los padres de familia y profesores reconocen los riesgos cibernéticos y pueden instruir de primera mano a los menores sobre diferentes aspectos.

Del mismo modo, con la segunda medición, se identifican varios elementos relevantes, el primero es la necesidad de acercar el conocimiento de los riesgos cibernéticos a las aulas de clase, lo que sugiere un proceso de capacitación inicial para los profesores, considerando una planeación obligatoria en los planes de trabajo y con ello, replicar el conocimiento a los estudiantes en sus aulas a través de algún mecanismo que permite llegar a un gran público. Un segundo elemento es la disposición de los estudiantes para recibir y practicar los controles a los riesgos identificados, esto conlleva a que las directivas y docentes generen un plan de monitoreo o auditoria (seguimiento) en la aplicabilidad del concepto, considerando las familias en ese campo de acción y, un tercer elemento fundamental, poder replicar el modelo en otras instituciones con el fin de que sean incorporados los diferentes conceptos en el aula de clase.

En relación con los resultados, una de las fortalezas del estudio fue la posibilidad de contar con la apertura de un colegio de la ciudad, lo que proporciona una perspectiva muy positiva tanto de la investigación como de las autoridades del plantel, y da la posibilidad de generar conciencia en el aula de clase. Así se posiciona una visión amplia sobre la disposición de querer medir y validar formas para dar cumplimiento a la ley y así mismo fortalecer el autocuidado y autoprotección de los estudiantes. Si bien, el estudio permitió medir un grupo de estudiantes, es clara la limitación que esto supone, dado que solo es un modelo aplicado en un aula de clase, lo que genera un punto de vista importante, pero no definitivo.

Los siguientes retos de investigación pueden estar asociados con la ampliación en la vali-

dación del conocimiento entre un público más diverso (más edades y más personas), así como a diferentes instituciones tanto del ámbito público como privado. Así mismo, establecer algunos parámetros que permita medir esa capacidad de conocimiento en áreas rurales, revisando con antelación cuál es el nivel de conectividad en los colegios y el de los estudiantes por fuera de los salones de clase. Esto permitirá contar con unos resultados más contundentes que generen propuestas más acertadas de las directivas de los centros de educación y aplicarlas en las aulas con procesos de monitoreo permanente.

Finalmente, se podría tener un reto asociado con la búsqueda de otros riesgos cibernéticos, según el uso de la tecnología, como es el caso del *Cyberbullying* o matoneo por internet. Esto en conjunto con el *sexting* y el *grooming* generarían un panorama más completo de los riesgos que enfrentan los estudiantes de las escuelas y colegios, lo que puede ser un punto de partida para otras investigaciones desde las áreas sociales como el relacionamiento, la sicología, sociología, entre otras, considerando los impactos en el rendimiento escolar, deserción y otros problemas escolares a partir de las situaciones derivadas del mal uso de las redes sociales e Internet.

Conclusiones

Las estrategias de ciberseguridad basadas en mecanismos gamificados han demostrado tener un impacto positivo y una respuesta efectiva en relación con los fines perseguidos en las fases. Estas estrategias han logrado reducir los posibles niveles de riesgo y el impacto en niños, niñas y jóvenes de edades comprendidas entre los 9 y 15 años en instituciones de educación básica y media.

El proceso de ciberseguridad implementado, que utiliza un enfoque diferenciado para la entrega de información, ha demostrado ser eficaz para mejorar la percepción, conciencia y capacidad de la toma de decisiones de los estudiantes cuando se enfrentan a riesgos en Internet. En consecuencia, se ha evidenciado que explicar el *sexting* y *grooming* desde sus orígenes, riesgos e impactos es estratégico para que el proceso de ciberseguridad se adapte a los riesgos que sufren los estudiantes de educación básica y media en Colombia.

A través de la lúdica se ha demostrado que la educación puede llevarse a otros niveles, en el ejercicio, en temas de ciberseguridad y el uso coherente de la tecnología, lo que genera nuevos mecanismos de protección frente a las amenazas constantes. Este nuevo estado de la información la convierte en un activo valioso cuando es evaluada.

Los resultados de la evaluación fruto de la aplicación del proceso estadístico de pruebas de signos bajo la tabla bimodal, se vuelven útiles para desarrollar estrategias efectivas en la prevención de ciberataques y comportamientos que puedan dar lugar a la cibervictimización. En otras palabras, el análisis y la comprensión de los resultados de la evaluación se convierten en una herramienta valiosa para diseñar medidas preventivas que puedan proteger a las personas de posibles amenazas en línea y reducir la posibilidad de convertirse en víctimas de delitos cibernéticos.

Referencias

Agencia de la Unión Europea para la Cooperación Policial [Europol] (2022, enero 5). *Online sexual coercion and extortion is a crime*. https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/online-sexual-coercion-and-extortion-crime

Agustina, J. R. & Gómez-Durán, E. L. (2016). Factores de riesgo asociados al *sexting* como umbral de diversas formas de victimización. Estudio de factores correlacionados con el *sexting* en una muestra universitaria. *IDP - Revista de Internet, Derecho y Política*, *22*(1), pp. 21-47. https://www.redalyc.org/pdf/788/78846481004.pdf

Alarcón-Diaz, M. A., Alarcón-Diaz, H. H., Rodríguez-Baca, L. S., & Alcas-Zapata, N. (2020). Intervención educativa basada en la gamificación: experiencia en el contexto universitario. *Revista Eleuthera*, *22*(2), 117-131. https://doi.org/10.17151/eleu.2020.22.2.8

Álvarez Cáceres, R. (1995). *Estadística multivariante y no paramétrica con SPSS.* Ediciones Diaz Díaz de Santos.

Álvarez Oria, L. (2021). *Desarrollo de una herramienta para plan de conciencia en ciberseguridad basada en gamificación* [Trabajo de grado, Escuela Técnica Superior de Ingeniería y Sistemas de Telecomunicación] https://oa.upm.es/70726/1/TFG_LUIS_ALVAREZ_ORIA.pdf

Almeida, T. C., & Barreiros, I. (2024). Online grooming among Portuguese adolescents and the COVID-19 lockdown: Relationship with other types of victimization. *Children and Youth Services Review, 156*, 107370. https://doi.org/10.1016/j.childyouth.2023.107370

Asociación Colombiana de Ingenieros de Sistemas [ACIS] (2021, noviembre 19). *Niños de Latinoamérica y uso de redes Sociales*. https://www.acis.org.co/portal/content/noticiasdelsector/redes-sociales-el-45-de-los-ni%C3%B1os-en-colombia-tiene-perfil-y-el-15-de-los-padres-desconoce

Baldeón, J., Rodríguez, I., Puig, A., & López-Sánchez, M. (2017). Evaluación y rediseño de una experiencia de gamificación en el aula basada en estilos de aprendizaje y tipos de jugador. En R. S. Contreras Espinosa, y J. L. Eguia (eds.), *Experiencias de gamificación en las aulas* (pp. 95-112). Universidad Autónoma de Barcelona.

Brooke, A., Anderson, M., Perrin, A., & Turner, E. (2020). *Parenting children in the age of screens*. Pew Research Center. https://www.pewresearch.org/internet/2020/07/28/parenting-children-in-the-age-of-screens/

Chawki, M. (2024). *Navigating legal challenges of deepfakes in the American context: a call to action.* Cogent Engineering, *11*(1). https://doi.org/10.1080/23311916.2024.2320971

Cisco System. (2023). *¿Qué es la ciberseguridad?* https://www.cisco.com/c/es_mx/products/security/what-is-cybersecurity.html

Cortés, C., Lajara, M., Úbeda García, M., García Lillo, F., Rienda García, L., Zaragoza Sáez, P. C., Andreu Guerrero, R., Manresa Marhuenda, E., Seva Larrosa, P., Ruiz Fernández, L., Sánchez García, E., Poveda Pareja, E., & Martínez Falcó, J. (2020). El uso de la gamificación en Dirección Estratégica de la Empresa (1er ed., pp. 1034-1043). Octaedro. https://dialnet.unirioja.es/servlet/articulo?codigo=7668022

DQ Institute (2022). Child Online Safety Index Score (COSI) (2022). Best Countries for Child Online Safety. *DQ Institute.* https://www.dqinstitute.org/impact-measure-2022/

Google. (s. f.). Institución Educativa Sebastián de Belalcázar. 15 de diciembre de 2023. https://goo.gl/maps/d5sZujirv3PxZKwm8. Todos los derechos reservados 2023 por Google. [Adaptado con permiso del autor].

Holfeld, B., Mishna, F., Craig, W., & Zuberi, S. (2024). A latent profile analysis of the consensual and non-consensual sexting experiences among Canadian adolescents. *Youth & Society, 56*(4), 713-733. https://doi.org/10.1177/0044118X231202814

INCIBE (2022) *Cyberscouts*, *INCIBE*. https://cyberscouts.osi.es/.

Instituto Colombiano de Bienestar Familiar [ICBF], (2021, 15 de febrero). *Del sexting al ciberbullying y la sextorsión.* https://www.icbf.gov.co/mis-manos-te-ensenan/del-sexting-al-ciberbullying-y-la-sextorsion

Instituto Nacional de las Tecnologías de Comunicación [Inteco] – España, (s. f*.). Guía S. O. S. contra el Grooming. Padres y educadores.* https://www.adolescenciasema.org/usuario/documentos/sos_grooming.pdf

International Organization for Standardization [ISO], (2022). *Information security, cybersecurity and privacy protection — Guidance on managing information security risks*. (ISO/IEC Standard No. 27005:2022). https://www.iso.org/standard/80585.html

Kamar, E., Maimon, D., Weisburd, D., & Shabat, D. (2022). Parental guardianship and online sexual grooming of teenagers: A honeypot experiment. *Computers in Human Behavior*, 137(2022), 1-7. https://doi.org/10.1016/j.chb.2022.107386

Kaspersky Labs. (2016, 2 de agosto). *Las consecuencias del sexting.* https://www.kaspersky.es/blog/sexting-y-sus-consecuencias/7692/

Katrin, C. & Jörg, M. F. (2024). Victims of technology-assisted child sexual abuse. *A Scoping Review*, *25*(2), 1335-1348. https://doi.org/10.1177/15248380231178754

Kyle, T. G., Carolyn, O., Jason M. N., Alexander, T., Dylan B. J., Nelson, P., & Faye, M. (2024). Associations between receiving non-consensual image and video sexts and average sleep duration among adolescents and young adults. *Sexual Health 21*, SH23202. https://doi.org/10.1071/SH23202

Ledesma, S. (2023, 25 de marzo). *Sexting en menores.* https://bedigitalbereal.com/sexting-en-menores/

Ley 1620 de 2013. (2013, 15 de marzo). Por la cual se crea el Sistema Nacional de Convivencia Escolar y Formación para el Ejercicio de los Derechos Humanos, la Educación para la Sexualidad y la Prevención y Mitigación de la Violencia Escolar. Congreso de la República. *Diario Oficial* No. 48733. https://www.mineducacion.gov.co/1759/articles-327397_archivo_pdf_proyecto_decreto.pdf

Mejía-Soto, G. (2014). *Sexting*: una modalidad cada vez más extendida de violencia sexual entre jóvenes. *Perinatología y Reproducción Humana*, *28*(4), 217-221. http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0187-53372014000400007&lng=es&tlng=es.

Ministerio de las TIC Colombia (2022, 4 de octubre). *MinTIC capacitó a los PRST sobre los mecanismos de protección a menores de edad en entornos digitales.* https://mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/243732:MinTIC-capacito-a-los-PRST-sobre-los-mecanismos-de-proteccion-a-menores-de-edad-en-entornos-digitales

Morillo Puente, E., Ríos Hernández, I. N., & Henao López, G. C. (2022). Evaluación empírica del *sexting* y las actividades rutinarias de los adolescentes en Colombia. *OBETS Revista de Ciencias Sociales*, *17*(2), 285-304. https://doi.org/10.14198/OBETS2022.17.2.07

Policía Nacional de Colombia (2023). *Estadística delictiva para el 2023.* https://www.policia.gov.co/estadistica-delictiva?page=3

Paulus, F. W., Nouri, F., Ohmann, S., Möhler, E., & Popow, C. (2024). The impact of Internet pornography on children and adolescents: A systematic review. *L'Encéphale*. https://doi.org/10.1016/j.encep.2023.12.004

Prieto-Andreu, J. M., Gómez-Escalonilla-Torrijos, J. D., y & Said-Hung, E. (2022). Gamificación, motivación y rendimiento en educación: una revisión sistemática. *Revista Electrónica Educare*, *26*(1), 251-273. https://dx.doi.org/10.15359/ree.26-1.14

Ramírez Ríos, A., & Polack Peña, A. M. (2020). Estadística inferencial. Elección de una prueba estadística no paramétrica en investigación científica. *Horizonte de La Ciencia*, *10*(19), 191-208. https://doi.org/10.26490/uncp.horizonteciencia.2020.19.597

Sani, A. I., Vara, M., & Pimenta Dinis, M. A. (2024). Online Sexual Grooming of Children: Psychological and Legal Perspectives for Prevention and Risk Management. In G. Borges, A. Guerreiro, & M. Pina (Eds.), *Modern Insights and Strategies in Victimology* (pp. 25-55). IGI Global. https://doi.org/10.4018/979-8-3693-2201-7.ch002

Tejada-Garitano, E., Arce-Alonso, A., Bilbao-Quintana, N., & López de la Serna, A. (2023). Internet, smartphone y redes sociales: entre el uso y abuso, previo a la adicción. *Alteridad*, *18*(1), 14-22. https://doi.org/10.17163/alt.v18n1.2023.01

Tortosa, A. J., Sánchez, M. A., Bernal, M. J., & Gracia, V. B. (2017). Gamificación y aprendizaje cooperativo en la didáctica de las ciencias sociales#CCAFYDExpress. En A. R. Fernández Parada, M. Fernández Parada & G. A. Gutiérrez Montoya. Editorial Universidad Don Bosco. http://hdl.handle.net/11268/8223

Usma Guzmán, F. A. (2022). *Estrategia de seguridad informática basada en gamificación, para la enseñanza en la prevención de abusos de ciber victimización por sexting y grooming para adolescentes de educación básica y/o media en Medellín* [Trabajo de maestría, Instituto Tecnológico Metropolitano]. http://hdl.handle.net/20.500.12622/5841

Walker, H., & Lev, J. (1953). *Inferencia estadística, anexo 9 tabla para prueba binomial*. http://www-eio.upc.edu/teaching/estad/MC/taules/com-usar-taules.pdf

Wang, F., & Topalli, V. (2024). The cyber-industrialization of catfishing and romance fraud. *Computers in Human Behavior*, 154, 108133. https://doi.org/10.1016/j.chb.2023.108133

Wright, M. F., & Wachs, S. (2024). Longitudinal associations between different types of sexting, adolescent mental health, and sexual risk behaviors: Moderating effects of gender, ethnicity, disability status, and sexual minority status. *Arch Sex Behav*, *53*, 1115-1128. https://doi.org/10.1007/s10508-023-02764-7