Cibercrimen entre niños y adolescentes en Portugal: un estudio basado en datos del videojuego RAYUELA

Andrea Baños Ramos[1], María Reneses Botija[2], Mario Castro Ponce[1], Farid Bagheri-Gisour Marandyn[1], Constança Brito[3], Filipe Rodrigues[3], Gregorio López López[1]
[1]Instituto de Investigación Tecnológica (IIT), España
Escuela Técnica Superior de Ingeniería (ETSI), Universidad Pontificia Comillas, España
[2]Instituto de Investigación Tecnológica (IIT), España
Facultad de Ciencias Humanas y Sociales (CHS), Universidad Pontificia de Comillas, España
[3]Polícia Judiciária (PJ), Rua Gomes Freire 174, 1150-177 Lisbon, Portugal
abanos@comillas.edu, mreneses@comillas.edu, marioc@iit.comillas.edu, fbagherigisour@comillas.edu, constanca.brito@pj.pt, filipe.rodrigues@pj.pt, gllopez@comillas.edu

***Resumen*—Este estudio presenta un análisis exploratorio de los datos recopilados durante la primera edición de la campaña nacional de prevención Missão Cibersegura (2024–2025) en Portugal, que contó con una muestra de 5852 participantes. El análisis se centra en la prevalencia y los factores de riesgo asociados a cuatro amenazas cibernéticas clave: ciberacoso, phishing, online grooming y la difusión de noticias falsas. La metodología expuesta es innovadora, ya que combina la recopilación de datos con una experiencia interactiva y atractiva basada en un videojuego. El principal objetivo es utilizar estos datos para comprender mejor cómo se producen las distintas formas de victimización digital entre menores, así como identificar los factores psicológicos, conductuales y contextuales que los sitúan en mayor riesgo. Por último, este trabajo pretende sentar las bases para un análisis interdisciplinar integral de las amenazas digitales que afectan a los jóvenes.**

***Index Terms*—Ciberamenazas, factores de riesgo, análisis de prevalencia, victimización, jóvenes, videojuego.**

Tipo de contribución: *Investigación en desarrollo*

I. Introducción

Hoy en día existe una amplia variedad de amenazas cibernéticas que afectan a una gran parte de la población mundial. Diversos grupos dentro de la sociedad siguen sin ser conscientes de estas amenazas y de los riesgos potenciales que conllevan, en particular los adolescentes y menores de entre 10 y 16 años. La identificación de numerosos factores de riesgo puede aumentar la prevalencia de dichas amenazas cibernéticas. Con el fin de examinar estos riesgos, este estudio utiliza un juego serio llamado RAYUELA[1] [www.rayuela-h2020.eu], junto con la recopilación de datos sociodemográficos y cuestionarios relacionados con el apoyo externo y experiencias previas de ciberacoso.

En la era digital contemporánea, los menores están profundamente inmersos en entornos en línea que configuran su socialización, educación e identidad personal. Vectores emergentes, como las plataformas de redes sociales, la denominada "manosfera", las herramientas de inteligencia artificial y los entornos de aprendizaje gamificados, están transformando tanto la forma en que los jóvenes pueden ser captados para actividades delictivas como la manera en que pueden convertirse en víctimas de daños en línea [1], [2], [3]. Si bien estos espacios digitales ofrecen oportunidades sin precedentes para la conexión y el aprendizaje, también exponen a los usuarios jóvenes a amenazas diversas y en rápida evolución. Entre las más prevalentes se encuentran el ciberacoso (CB), el phishing, el online grooming (OG) y la exposición a noticias falsas (FN), que en conjunto constituyen un amplio espectro de amenazas cibernéticas que afectan de manera significativa a niños y a adolescentes.

Uno de los principales objetivos de este trabajo es apoyar el desarrollo de campañas de prevención y concienciación en los centros educativos destinados a mitigar estas amenazas cibernéticas. Iniciativas desarrolladas por el Instituto Nacional de Ciberseguridad de España (INCIBE), proporcionando un servicio a familias, jóvenes y profesores de los centros educativos, como Internet Segura for Kids (IS4K) y la estrategia Europea Better Internet for Kids (BIK), promoviendo la creación de entornos digitales más seguros y conformando Centros de Seguridad en Internet. Además, Safer Internet Centre Spain 4.0 (SIC-SPAIN 4.0) es un proyecto que refuerza estas actuaciones y proporciona cobertura a IS4K.

Muchos menores siguen sin ser conscientes del daño que su comportamiento en línea puede causar a otros compañeros. La educación es, por tanto, un ámbito clave de intervención, fomentando un entorno seguro en las escuelas. Las familias también desempeñan un papel crucial, dado que el comportamiento de los menores en distintos contextos sociales está fuertemente influido por su relación con padres, madres o cuidadores.

Pueden implementarse programas de formación específicos en los centros educativos para ayudar a identificar vulnerabilidades entre los menores y promover una evaluación crítica de los contenidos y las interacciones en línea. Además, estos resultados pueden servir de base para la elaboración de políticas en el ámbito educativo, apoyando la integración de medidas de seguridad infantil, protecciones de la privacidad y sistemas de notificación transparentes, como la iniciativa del Plan Director para la convivencia y mejora de la seguridad en los centros educativos y sus entornos (2023), impulsada por

[1]Se puede descargar el videojuego y visualizar los escenarios en la pestaña RAYUELA GAME, download the game.

la Policía Nacional y la Guardia Civil. En los casos en los que se identifiquen riesgos o daños graves, los agentes de las fuerzas y cuerpos de seguridad pueden intervenir para llevar a cabo las actuaciones oportunas cuando sea necesario.

II. Marco conceptual de las amenazas cibernéticas

El ciberacoso representa una de las formas más prevalentes de victimización en línea y se define como el uso intencional de dispositivos electrónicos para dañar o intimidar a otras personas [4]. A diferencia del acoso tradicional, el ciberacoso trasciende las barreras físicas y temporales, lo que a menudo deriva en daños psicológicos persistentes, como ansiedad, depresión y una disminución de la autoestima [5].

Otra amenaza, cada vez más sofisticada, que afecta a los menores es el phishing, un ciberdelito que emplea mensajes digitales engañosos para obtener información personal sensible. Aunque tradicionalmente se ha asociado a víctimas adultas, investigaciones recientes demuestran que los niños y adolescentes son objetivo de este tipo de ataques debido a su limitada concienciación sobre la seguridad en línea y a su mayor tendencia a confiar en las comunicaciones digitales [6], provocando violaciones directas de la privacidad, robo de identidad y malestar psicológico tras descubrir el engaño.

El online grooming se refiere a un proceso relacional manipulador mediante el cual un agresor cultiva la confianza y la proximidad psicológica y emocional con una persona vulnerable, normalmente un menor o un adulto en situación de riesgo, con el fin de facilitar el abuso o la explotación sexual [7], [8]. En el contexto de este estudio, el online grooming alude a la explotación de plataformas digitales por parte de un adulto que manipula la confianza de un menor para redefinir su percepción de la seguridad y de las interacciones apropiadas, utilizando posteriormente el miedo y la vergüenza como mecanismos de control y secreto.

Por último, la proliferación de las noticias falsas influye de manera significativa en la forma en que los jóvenes usuarios perciben e interpretan la información. Su difusión a través de las redes sociales dificulta la distinción entre contenidos fiables y falsos, haciendo a los jóvenes especialmente vulnerables a la manipulación [9], como la que subyace al grooming o al phishing. Además, las noticias falsas pueden influir en las actitudes de los menores, exacerbar la polarización y debilitar sus habilidades de pensamiento crítico.

En conjunto, estos fenómenos evidencian la complejidad y el impacto del cibercrimen en la vida de los menores. Asimismo, estas amenazas digitales no son estáticas, sino que evolucionan de forma paralela a la innovación tecnológica. Por ello, es esencial definir estrategias de prevención con visión de futuro, que incluyan una educación reforzada, marcos regulatorios sólidos y mecanismos de supervisión proactivos.

II-A. Factores de riesgo comunes a distintas amenazas cibernéticas

Los factores de riesgo son condiciones individuales, sociales y contextuales que incrementan la vulnerabilidad de los menores frente a comportamientos dañinos en línea. Mientras que los factores de protección, engloban las habilidades personales, los recursos sociales y las condiciones ambientales que protegen a los jóvenes frente al daño y fomentan la resiliencia en los entornos digitales. El análisis conjunto de ambos factores proporciona un marco integral para comprender las experiencias en línea de los menores y para diseñar enfoques informados de protección basados en la evidencia.

Estos factores de riesgo ponen de manifiesto que los cuatro fenómenos, ciberacoso, phishing, online grooming y noticias falsas, están interconectados a través de vulnerabilidades estructurales y psicológicas compartidas. En todos los casos, la limitada alfabetización digital, la inmadurez emocional y la supervisión adulta insuficiente emergen como determinantes centrales (ver Tabla I). Asimismo, el diseño de las plataformas en línea, optimizado para maximizar la participación más que para garantizar la seguridad, genera condiciones sistémicas que facilitan la explotación. Una comprensión holística de estos riesgos requiere integrar perspectivas individuales, sociales y tecnológicas, reconociendo que una prevención eficaz debe combinar educación, regulación normativa y responsabilidad de las plataformas.

III. Metodología

III-A. Diseño de la investigación

Con el fin de abordar de manera integral el estudio de los fenómenos de ciberacoso, phishing, online grooming y noticias falsas, se diseñó una serie de ciberaventuras basadas en una extensa investigación preliminar a nivel europeo que combinó cuatro estrategias complementarias de recogida de datos: el análisis de sentencias judiciales [19], entrevistas en profundidad con expertos, agresores y víctimas [15], grupos focales con adolescentes [18], [20] y una encuesta [21]. A partir de estos trabajos, se diseñaron escenarios que permitían medir situaciones y factores de riesgo (ver Tabla II). Además, al inicio del juego se incluyeron tanto cuestionarios validados como preguntas sociodemográficas.

Por razones éticas, la probabilidad de convertirse en agresor solo se midió en dos situaciones concretas: una relacionada con el ciberacoso y otra con el ciberacoso homófobo. La victimización por ciberacoso no se midió directamente dentro del juego, sino a través de cuestionarios validados. En el resto de los fenómenos potencialmente delictivos, la probabilidad de victimización se evaluó mediante situaciones de riesgo específicas. El phishing se midió a través de la acción de hacer clic en un enlace falso. En el caso del online grooming, estas incluyeron la aceptación de solicitudes de amistad de desconocidos y el envío de fotografías. Por su parte, las noticias falsas se evaluaron considerando prácticas inadecuadas para verificar la veracidad de la información. En este sentido, otorgar mayor importancia a la apariencia de exactitud de la información, la presencia de gráficos y estadísticas, o al aspecto profesional del sitio web se consideró menos recomendable y más arriesgado que otras estrategias, como comprobar la fuente de la noticia o realizar búsquedas adicionales en internet para contrastar la información.

Las medidas recogidas dentro del juego fueron validadas mediante validez de constructo [22] y validez de criterio [23]. La primera se refiere a la medición de un factor latente subyacente que no se observa directamente. En este caso, los escenarios del juego buscan medir cada uno de los ciberdelitos analizados. La segunda está relacionada con la capacidad predictiva, examinando en qué medida las variables del juego predicen constructos no observados.

Tabla I: Factores de riesgo identificados en investigaciones previas.

Fenómeno	Factores individuales	Factores sociales / contextuales	Factores tecnológicos / de plataforma
Ciberacoso	Baja autoestima y alta impulsividad [10], género, orientación sexual u origen migrante	Entornos conflictivos, supervisión parental insuficiente, bajo apoyo de pares	El anonimato reduce la empatía y facilita la agresión [11]
Phishing	Menor edad, impulsividad y experiencia digital limitada [12]	Compartición de información personal	Mensajes de *phishing* altamente personalizados a partir de datos en línea [13]
Online grooming	Soledad emocional, baja autoestima, problemas de salud mental o abuso previo [14], género [15]	Supervisión parental insuficiente y búsqueda de validación adolescente [16]	Acceso a datos personales que permite una manipulación adaptada
Noticias falsas / desinformación	Bajo pensamiento crítico y baja alfabetización mediática [9], sesgo de confirmación [17], impulsividad	Alta dependencia de redes sociales como fuente informativa	Diseño atractivo o "científico" que incrementa la credibilidad y la difusión de contenidos falsos [18]

Tabla II: Factores de riesgo medidos (dentro y fuera del juego).

Factores de riesgo	Cuestionarios y registro	Escenarios dentro del juego
Victimización previa por CB	Victimización previa por CB	—
Conducta previa como agresor en CB	Conducta previa como agresor en CB	Conducta previa como agresor en CB
Apoyo / Comunicación familiar	Apoyo familiar	Comunicación familiar
Apoyo social	Apoyo social	—
Autoestima	Autoestima	—
Género	Género	—
Edad	Edad	—
Tiempo en línea	Tiempo en línea	Tiempo en línea
Sociabilidad	Sociabilidad	Sociabilidad
Información personal en línea	—	Información personal en línea
Tipo de centro educativo	Tipo de centro educativo	—

III-B. Tamaño muestral

La muestra inicial estuvo compuesta por 5852 participantes, que se utilizará para otro análisis de tendencias. Sin embargo, este estudio utiliza mayor control y precisión, 1984 individuos fueron retenidos para el análisis tras excluir a aquellos que indicaron tras finalizar el juego, que no habían jugado de la misma forma en que se comportarían en la vida real. Esta muestra final incluyó a 998 chicos, 950 chicas y 7 estudiantes no binarios, con edades comprendidas entre los 10 y los 16 años, en Portugal. Se empleó una estrategia de muestreo no probabilístico por conveniencia, utilizando los centros educativos como puntos de acceso, lo que permitió incluir un gran número de participantes, pero limita la representatividad estadística estricta. La muestra está compuesta predominantemente por estudiantes de centros públicos (aproximadamente el 91 %), con una menor proporción procedente de instituciones privadas (8,4 %) y un número residual de otros tipos de centros. Esta distribución refleja, en cierta medida, el predominio de la educación pública en Portugal, aunque la educación privada está infrarrepresentada en la muestra. Además, el 73 % de los participantes procedía de áreas urbanas y el 27 % de áreas rurales, garantizando la inclusión de contextos territoriales diversos. Los participantes fueron reclutados a través de centros educativos que formaban parte del programa de la Policía Judiciaria "Missão Cibersegura".

Aunque el diseño muestral no permite una generalización inferencial estricta, el gran tamaño de la muestra proporciona un alto nivel de precisión estadística. Bajo supuestos estándar (nivel de confianza del 95 % y máxima variabilidad), el margen de error estimado sería de aproximadamente ±2,2 %. En conjunto, si bien la muestra no puede considerarse plenamente representativa, su tamaño y heterogeneidad respaldan la solidez analítica de los resultados, que deben interpretarse con cautela en términos de generalización.

III-C. Comité de Ética

Se obtuvo la aprobación del comité de ética y todos los participantes (y sus familias, cuando fue necesario) firmaron un consentimiento informado en el que se proporcionaba información completa sobre los objetivos del estudio.

III-D. Procedimiento de recogida de datos

El videojuego se llevó a cabo durante el horario lectivo en las aulas, bajo la supervisión de un docente responsable de su implementación. Se siguió un protocolo previamente establecido que incluía tres fases principales: en primer lugar, la preparación, instalación del juego y la recogida de los formularios de consentimiento; en segundo lugar, la presentación del estudio al alumnado, el registro de los estudiantes y las instrucciones para jugar las seis aventuras; y, finalmente, una serie de preguntas destinadas a una discusión guiada con los estudiantes, que incluían información práctica sobre cómo denunciar incidentes o buscar ayuda en situaciones concretas.

III-E. Análisis de datos

Tras la recogida de los datos, estos fueron exportados y analizados mediante RStudio, versión 2024.09.0-375, un entorno de desarrollo integrado para el lenguaje de programación R. Se realizó un análisis descriptivo de frecuencias simples y un análisis bivariante mediante tablas de contingencia y el test de chi-cuadrado (χ^2), comprobando la significación estadística entre pares de variables a través de los residuos tipificados corregidos. Asimismo, se llevó a cabo un análisis de regresión logística con el fin de evaluar simultáneamente los distintos factores de riesgo, junto con un análisis de colinealidad.

IV. Resultados

IV-A. Ciberacoso

IV-A1. Agresión: Este análisis examinó la probabilidad de convertirse en agresor en contextos de ciberacoso. Dentro del juego se evaluaron dos escenarios: compartir un meme

ofensivo sobre un compañero de clase (N = 1717) y reírse de una broma homófoba dirigida a otra persona (N = 1166).

Ambas situaciones mostraron una prevalencia similar, de un 19,5 % y un 16,3 % respectivamente, incurriendo en conductas agresivas (ver Figura 1). De manera relevante, cuando se pidió a los estudiantes que reflexionaran sobre sus acciones, alrededor del 69,5 % de quienes habían actuado como agresores reconocieron que su comportamiento era incorrecto y muchos lo identificaron explícitamente como una forma de acoso.

La relación entre estas variables es elevada, ya que ambas se midieron dentro del juego, aunque en aventuras distintas relacionadas con el ciberacoso. Esta asociación quedó respaldada por un coeficiente de χ^2 de 50,197 (indicativo de una asociación fuerte) y un valor de $p < 1{,}39 \times 10^{-12}$, lo que refleja una significación estadística muy alta.

IV-A2. Victimización: Aunque la victimización no se midió directamente dentro del juego, esta se estimó mediante un cuestionario sobre victimización previa (N = 1984), el cual mostró una prevalencia del 28,3 % (ver Figura 1).

IV-B. Phishing

Si bien el phishing suele recibir menor atención en los programas de prevención, emergió como el ciberdelito más frecuente entre los participantes (N = 1046), con una prevalencia potencial del 41 % (ver Figura 1).

IV-C. Online Grooming

La exposición al online grooming se evaluó a través de dos escenarios: la aceptación de una solicitud de amistad de un desconocido en una red social (N = 1295) y el envío de fotografías tras recibir una petición de ese mismo desconocido, que se hacía pasar por un fotógrafo y ofrecía la creación de un portafolio de modelaje (N = 1293).

Los resultados revelaron que el 22,5 % de los participantes aceptó la solicitud sin comprobar el perfil del desconocido (ver Figura 1). Además, entre quienes sí revisaron el perfil, el 16,4 % aceptó igualmente la solicitud, ya que la cuenta incluía indicios realistas frecuentemente utilizados por los agresores, como amigos en común, publicaciones antiguas, comentarios y fotografías reales. Finalmente, el 10,4 % de la muestra total aceptó enviar fotografías.

IV-D. Noticias falsas

El riesgo de caer en noticias falsas se evaluó mediante un escenario en el que los jugadores debían decidir las mejores estrategias para comprobar la veracidad de una información relacionada con personas refugiadas (N = 1118). Se consideró que los participantes estaban en riesgo cuando elegían como primera opción confiar en la apariencia de exactitud de la información y en el aspecto profesional del sitio web. Por el contrario, se consideró que no estaban en riesgo cuando optaban por comprobar la fuente de la noticia o realizar búsquedas adicionales en internet para contrastar la información.

Los resultados muestran que aproximadamente dos tercios de los participantes respondieron de forma adecuada para evitar este tipo de engaño. Sin embargo, un tercio decidió que lo más conveniente era confiar en los aspectos más superficiales de la noticia, en lugar de llevar a cabo una verificación más exhaustiva (ver Figura 1).

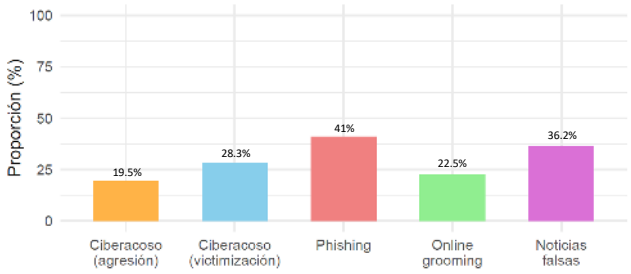


Figura 1: Prevalencia de ciberamenazas. Ciberacoso (agresión) se refiere al escenario de compartir un meme de un compañero de clase en el videojuego, y Online grooming se refiere al escenario de aceptar una invitación de un extraño en una red social.

IV-E. Factores de riesgo comunes a todas las amenazas cibernéticas

Uno de los hallazgos más relevantes es la superposición de factores de riesgo entre las cuatro amenazas cibernéticas analizadas, lo que sugiere que las estrategias de prevención dirigidas a estos factores pueden tener efectos protectores amplios (ver Tabla III).

A partir de estos resultados, se destacan los siguientes factores transversales:

- Género: Los chicos presentaron una mayor probabilidad de convertirse en agresores en contextos de ciberacoso (especialmente en situaciones homófobas), así como de ser víctimas de phishing, noticias falsas y, de forma aún más marcada, de online grooming.
- Divulgación de información personal: En una red social simulada, se pidió a los participantes que decidieran si hacer público su perfil, compartir fotografías personales, publicar su lugar de residencia y elegir una contraseña. Los cuatro comportamientos se asociaron con un mayor riesgo en todas las amenazas cibernéticas analizadas.
- Comunicación familiar: Una comunicación débil en el entorno familiar emergió como un factor común en todas las amenazas. Asimismo, el bajo apoyo familiar, medido mediante un cuestionario validado, mostró asociaciones significativas.
- Tiempo de uso de internet: En línea con observaciones previas, el uso intensivo de internet se confirmó como el segundo factor de riesgo más relevante para la mayoría de amenazas cibernéticas. Este resultado se observó tanto en las respuestas directas de los participantes como en las situaciones evaluadas dentro del juego.

El tiempo dedicado por agresores y víctimas en cada uno de los escenarios de amenazas cibernéticas, en comparación con las personas que no pertenecen a estas categorías, presenta diferencias significativas. Tanto las víctimas (de las diferentes amenazas cibernéticas) como los agresores completaron las aventuras en menos tiempo durante el juego (ver Figura 3).

Por lo tanto, se confirma la hipótesis de que el tiempo necesario para responder a los escenarios del juego varía entre los distintos grupos.

Tabla III: Factores de riesgo a través de las distintas amenazas cibernéticas.

Factor de riesgo	CB agresión*	CB victimización	Phishing	Online grooming	Noticias falsas
Género	Masculino	X	Masculino	Masculino	Masculino
Edad	Mayor	Mayor	X	Mayor	X
Autoestima	Baja	Baja	Baja	X	Baja
Apoyo social y otros apoyos	Bajo	Bajo	X	Bajo	Bajo
Tiempo en línea (en el juego)	Alto	Alto	Alto	Alto	X
Tiempo en línea (registro)	X	Alto	Alto	X	X
Apoyo familiar (en el juego)	Bajo	Bajo	Bajo	Bajo	Bajo
Apoyo familiar (cuestionario)	Bajo	Bajo	Bajo	X	X
Información personal en línea – Perfil	Público	X	Público	Público	Público
Información personal en línea – Lugar	Real	Real	Real	Real	Real
Información personal en línea – Fotos	Real	Real	Real	Real	Real
Información personal en línea – Contraseña	Insegura	X	Insegura	Insegura	Insegura
Rasgo de sociabilidad (en el juego)	Alta	X	X	X	X
Rasgo de sociabilidad (cuestionario)	Alta	X	X	X	X
Tipo de centro educativo (cuestionario)	Público	Público	Público	Público	X

Nota: La descripción (categoría relevante) de los factores de riesgo que afectan a diferentes amenazas cibernéticas están representados en esta tabla. Las casillas representadas con una "X" indican que no existe ningún tipo de relación. * Se evalúa el escenario de compartir un meme ofensivo. Al considerar el escenario de la broma homófoba, resultan relevantes los mismos factores de riesgo, con excepción de la edad, la autoestima y la sociabilidad (medida dentro del juego).

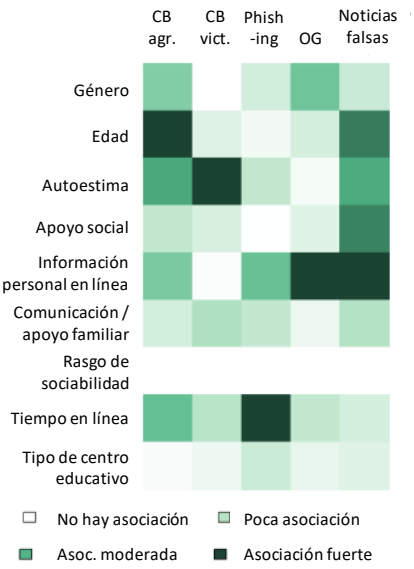
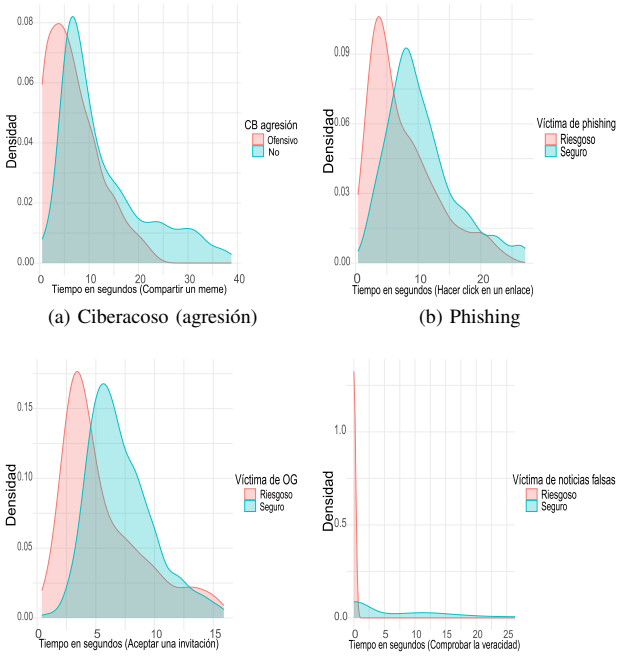


Figura 2: Asociación entre ciberamenazas y factores de riesgo. Las asociaciones de χ^2 comprenden diferentes rangos de valores dependiendo del tipo de ciberamenza: ciberacoso (agresión) $\in [6,2;25,1]$, ciberacoso (victimización) $\in [0,1;129,4]$, phishing $\in [0,3;35,6]$, online grooming $\in [0,4;66,8]$ y noticias falsas $\in [0,7;10,9]$.



(a) Ciberacoso (agresión) (b) Phishing

(c) Online Grooming (aceptar una invitación) (d) Noticias Falsas

Figura 3: Tiempo empleado jugando al videojuego. Las situaciones de victimización medidas dentro del juego ponen de manifiesto conductas de riesgo (ser víctima) o conductas seguras (no ser víctima de la situación de riesgo).

V. Discusión

V-A. *Ciberamenazas*

Se identifican dos hallazgos principales. En primer lugar, las tasas de prevalencia de los distintos ciberdelitos son considerablemente elevadas, lo cual resulta preocupante si se tiene en cuenta que el estudio se desarrolló en una situación relativamente controlada, como es el entorno habitual del aula. En segundo lugar, se observa una superposición entre los factores de riesgo y los distintos tipos de ciberdelitos. En el apartado siguiente se analizan de forma individual cada uno de los ciberdelitos y sus factores de riesgo asociados, para posteriormente ofrecer una discusión conjunta.

V-A1. Ciberacoso: Los resultados relativos al ciberacoso se basan en dos medidas diferentes. La medida de victimiza-

ción previa donde aproximadamente un tercio de los participantes la reportó, lo que constituye una cifra preocupante.

Las cifras relativas a la agresión también resultan alarmantes. Una prevalencia de aproximadamente el 17,9 % de conductas agresivas y, alrededor del 69,5 % de quienes habían actuado como agresores reconocieron que su comportamiento era incorrecto y muchos lo identificaron explícitamente como una forma de acoso.

No obstante, la prevalencia debe interpretarse únicamente en términos de jóvenes en riesgo de convertirse en agresores, y no como agresores reales. A pesar de la elevada validez ecológica del juego, la ausencia de daño real hacia otras personas puede haber incrementado ligeramente las respuestas de los participantes.

V-A2. Phishing: Esta ciberamenaza afectó a casi la mitad de la muestra de participantes. De manera relevante, la edad no resultó ser un factor significativo [12], lo que indica que, incluso en una muestra amplia, los jóvenes no están desarrollando progresivamente las habilidades necesarias para gestionar este riesgo a medida que crecen.

V-A3. Online Grooming: La elevada prevalencia de decisiones de riesgo en los escenarios de online grooming evidencia que las estrategias preventivas tradicionales resultan insuficientes, como "no aceptar solicitudes de desconocidos" o "no enviar fotografías" (más de uno de cada diez participantes estuvo dispuesto a hacerlo). La progresión observada en el juego, desde la aceptación de una solicitud hasta el envío final de fotografías, refleja la escalada gradual característica de los procesos reales de online grooming y muestra cómo los límites de los adolescentes pueden desplazarse rápidamente cuando se establece confianza o curiosidad.

Además, la aceptación de perfiles aparentemente legítimos sugiere que los jóvenes sobreestiman su capacidad para detectar riesgos, lo que subraya la necesidad de campañas educativas centradas en el desarrollo de competencias críticas y realistas para identificar amenazas en entornos digitales.

V-A4. Noticias falsas: En este caso, tampoco se midió la prevalencia directa, sino el riesgo de caer en desinformación a partir de la confianza en criterios de veracidad poco fiables, como la afinidad o confianza en la persona que comparte el contenido, el grado de sofisticación en el diseño de la fuente de información [24], así como el hecho de que el contenido esté patrocinado e incluya datos y estadísticas [25], [18].

V-B. Factores de riesgo

El estudio ilustra la relación entre variables individuales, sociales y contextuales como factores de riesgo y su conexión con distintos ciberdelitos, poniendo de manifiesto que dichos factores son, en gran medida, compartidos entre todos los tipos de cibercriminalidad analizados.

- Divulgación de información personal: Una de las asociaciones más fuertes observadas en la Figura 2 se da entre la información personal compartida en línea y el phishing, el online grooming y las noticias falsas, lo que confirma que niveles elevados de autoexposición digital incrementan significativamente la vulnerabilidad, ya que estos dependen en gran medida de la explotación de información. Conductas como hacer público el perfil, compartir fotografías, publicar el lugar de residencia o el centro educativo y utilizar contraseñas débiles se asociaron con un mayor riesgo. Este resultado respalda investigaciones previas que subrayan la importancia de los ajustes de privacidad y de una autopresentación cautelosa en entornos digitales [26]. Por lo que, las estrategias de prevención deberían priorizar la alfabetización en privacidad y el control de la autopresentación, enseñando a los adolescentes a auditar su huella digital.
- Tiempo de uso de internet: En el marco del estudio, el tiempo pasado en línea se identificó como el segundo factor de riesgo más relevante, mostrando su asociación más fuerte con el phishing. La presencia excesiva en entornos digitales se ha vinculado previamente con comportamientos impulsivos, una menor autorregulación y una mayor exposición a estresores sociales o emocionales [27]. Además, tanto posibles víctimas como agresores dedicaron menos tiempo en responder las preguntas del videojuego, lo que evidencia una tendencia a actuar de forma impulsiva. Por ello, la prevención debería centrarse en el fortalecimiento de la autorregulación, el control de la atención y el establecimiento de rutinas digitales saludables.
- Género: El género muestra una asociación moderada con la perpetración de ciberacoso (CB), el online grooming y, en menor medida, con el phishing y las noticias falsas, en consonancia con los resultados obtenidos y con estudios previos [28]. El mayor riesgo observado en los chicos puede estar influido por normas de género relacionadas con asumir riesgos, la sobreconfianza o la creencia de que las amenazas digitales son mínimas. Este hallazgo subraya la importancia de abordar los roles de género en las estrategias de prevención.
- Edad: Esta variable, como factor de riesgo, mostró un patrón diferenciado según el tipo de ciberdelito. En nuestros datos, la edad se asoció tanto con la agresión como con la victimización por ciberacoso (CB), así como con el online grooming (OG), especialmente en la adolescencia temprana y media, etapas caracterizadas por mayor reactividad emocional y vulnerabilidad social. Estas características del desarrollo pueden intensificar tanto la perpetración (por ejemplo, impulsividad, búsqueda de estatus, menor empatía) como la vulnerabilidad (por ejemplo, deseo de aceptación social, susceptibilidad a la atención en línea) [29], [16]. Sin embargo, la edad no redujo la vulnerabilidad frente al phishing ni a las noticias falsas, lo que indica una escasa adquisición espontánea de competencias protectoras, de modo que el aumento de la edad no se traduce automáticamente en una mejor detección de mensajes fraudulentos o desinformación. En conjunto, estos hallazgos sugieren que los riesgos de ciberacoso y online grooming alcanzan su punto máximo durante las transiciones evolutivas, mientras que los riesgos asociados al phishing y a la desinformación se mantienen elevados a lo largo de toda la adolescencia, lo que subraya la necesidad de una instrucción explícita sobre el engaño digital.
- Comunicación y apoyo familiar: La comunicación y el apoyo familiar débiles actúan como un factor general de vulnerabilidad frente a distintos ciberriesgos analizados. Este resultado coincide con la literatura sobre mediación parental y seguridad digital: aunque los vínculos directos

con el phishing siguen siendo escasos, diversos estudios indican que la baja supervisión familiar y una comunicación deficiente aumentan la exposición a la victimización en línea y a conductas de riesgo [30], [31]. Los hallazgos sugieren que el diálogo abierto dentro de las familias resulta más eficaz que el control o las restricciones, tanto para prevenir como para detectar amenazas digitales. La falta de orientación en las prácticas digitales favorece decisiones impulsivas. Las intervenciones deberían reforzar el diálogo abierto, y no la vigilancia, fomentar el uso compartido de tecnologías y entornos seguros de comunicación. Asimismo, los centros educativos podrían ofrecer talleres dirigidos a familias sobre normas digitales, estafas, señales de grooming y tácticas de phishing.

- Autoestima: Esta variable, como factor de riesgo, muestra una fuerte asociación con la victimización y una relación moderada con el phishing. Aunque la evidencia previa ha vinculado la baja autoestima principalmente con la cibervictimización en general [32], nuestros resultados sugieren que sus efectos psicológicos indirectos, como la necesidad de validación, la vulnerabilidad emocional o la indecisión, también pueden aumentar la susceptibilidad a intentos de phishing. Por ello, la prevención no debería centrarse únicamente en programas de alfabetización digital, sino también en programas de aprendizaje socioemocional. De este modo, resultaría útil educar sobre cómo los delincuentes explotan la inseguridad personal y emplean estrategias de manipulación.
- Apoyo social: Se observa una asociación particularmente fuerte entre bajos niveles de apoyo social y la victimización por ciberacoso, así como una relación destacable con la susceptibilidad a las noticias falsas. Esto sugiere que redes de apoyo más débiles pueden dejar a los adolescentes más expuestos a la manipulación o a la exclusión. El apoyo social actúa como un factor protector, especialmente frente a riesgos de naturaleza emocional. Por lo que, las estrategias de prevención deberían orientarse a fortalecer el sentido de pertenencia y las redes de iguales.
- Tipo de centro educativo: Se ha identificado una asociación moderada entre el tipo de centro (público) y el phishing, lo que refuerza que factores ambientales y estructurales, como una menor alfabetización digital o menos recursos en ciberseguridad, pueden desempeñar un papel relevante. Sobre todo, adolescentes de contextos educativos más desfavorecidos con mayor vulnerabilidad al phishing [33], debido a habilidades cognitivas más débiles o a un menor rendimiento académico. Por ello, la implementación de currículos gratuitos y estandarizados de alfabetización digital en todos los centros educativos es clave para garantizar un acceso equitativo a la educación en ciberseguridad.

V-C. Limitaciones

A pesar de la amplitud y la alta validez ecológica del videojuego, es necesario reconocer varias limitaciones. En primer lugar, aunque el uso de un videojuego inmersivo proporciona un entorno realista para observar los comportamientos en línea de los adolescentes, los escenarios simulados no pueden reproducir perfectamente las presiones emocionales, sociales y contextuales propias de las interacciones digitales reales, dando lugar a una ligera sobreestimación o subestimación de las conductas de riesgo.

En segundo lugar, el diseño se apoya parcialmente en medidas de autoinforme para algunas variables (por ejemplo, victimización previa o apoyo familiar), las cuales están inherentemente influenciadas por sesgos de recuerdo y deseabilidad social. La combinación de ambos tipos de medidas (cuestionarios validados y situaciones dentro del juego) se planteó precisamente para mitigar estos sesgos.

En tercer lugar, a pesar de que el tamaño muestral obtenido en Portugal es considerable, la generalización de los resultados a otras áreas geográficas podría ser limitada.

Por último, aunque se incluyó una amplia variedad de variables, no se contemplaron otros factores estructurales o psicológicos adicionales que podrían enriquecer futuros análisis y ofrecer una comprensión más completa de los riesgos digitales en la adolescencia.

VI. Conclusión

Los resultados de este estudio exploratorio demuestran que el ciberacoso, el phishing, el online grooming y la exposición a noticias falsas constituyen amenazas generalizadas e interconectadas que afectan a los menores. Incluso en un entorno escolar controlado, muchos participantes mostraron conductas de riesgo o vulnerabilidad, lo que indica una falta de preparación en línea y apoyo adecuados. La metodología innovadora basada en el videojuego permitió observar directamente la toma de decisiones en escenarios realistas, aportando información y patrones difícilmente observados en cuestionarios tradicionales.

Uno de los hallazgos centrales del estudio es el solapamiento significativo de los factores de riesgo entre las cuatro amenazas cibernéticas. Variables como el tiempo de uso de Internet, la comunicación familiar deficiente, la baja autoestima, el escaso apoyo social y la divulgación de información personal aparecieron de forma reiterada como predictores de vulnerabilidad. Esta convergencia sugiere que los riesgos en línea comparten mecanismos de carácter evolutivo, emocional y contextual. Además, la impulsividad indicó que los adolescentes tomaron decisiones rápidas sin evaluar las posibles consecuencias. Del mismo modo, la fuerte asociación entre la información personal compartida en línea y tanto el online grooming como el phishing subraya hasta qué punto los agresores explotan la huella digital de los menores.

Otra conclusión relevante se refiere a la edad. Mientras que los riesgos de ciberacoso y online grooming alcanzan su punto máximo durante la adolescencia temprana, la vulnerabilidad frente al phishing y las noticias falsas no disminuye con la edad, lo que indica que estas competencias no se adquieren de forma natural. La persistencia de estas vulnerabilidades a lo largo de las distintas edades refuerza la necesidad de una enseñanza explícita orientada a reconocer señales de diseño manipulativo, estrategias de persuasión emocional y las tácticas engañosas propias del fraude y la desinformación.

Finalmente, los resultados de este trabajo subrayan la necesidad de diseñar programas de prevención que integren competencias emocionales, cognitivas y digitales. Las intervenciones eficaces deben abordar no solo las habilidades técnicas, sino también las necesidades psicológicas y los entornos

sociales que configuran el comportamiento en línea de los adolescentes. El programa "Missão Cibersegura" constituye una base sólida para avanzar en este objetivo, ya que ofrece evidencias que pueden orientar futuras investigaciones, informar el desarrollo de políticas públicas y apoyar la formación de ciudadanos digitales resilientes y con pensamiento crítico.

AGRADECIMIENTOS

Este proyecto de investigación ha sido posible gracias a la concesión de una beca estratégica por parte del Instituto de Investigación Tecnológica (IIT), como parte de la Universidad Pontificia de Comillas. Parte del trabajo también ha sido posible gracias a la financiación recibida por European Anti-Cybercrime Technology Development Association (EACTDA) con fondos del programa Internal Security Fund (ISF) para Tools4LEAs (nº 101136295), a través del proyecto "National plan for the implementation of RAYUELA project in Portugal" y del proyecto PID2022-140217NB-I00, financiado por MCIN/AEI/10.13039/501100011033 y por "ERDF/EU A way of making Europe".

REFERENCIAS

[1] Bokolo, B. G., and Liu, Q.: "Artificial Intelligence in Social Media Forensics: A Comprehensive Survey and Analysis", en *Electronics*, vol. 13, n. 9, pp. 1671, 2024, doi:10.3390/electronics13091671.

[2] Wolbers, H., Cubitt, T., and Cahill, M. J.: "Artificial intelligence and child sexual abuse: A rapid evidence assessment", en *Trends and Issues in Crime and Criminal Justice*, n. 711, pp. 1-18, 2025, doi: 10.3316/informit.T20250130000125016737888879

[3] Franklin-Paddock, B., Platow, M.J. and Ryan, M.K.: "From Privilege to Threat: Unraveling Psychological Pathways to the Manosphere", en *Archives of Sexual Behavior*, vol. 54, n. 4, pp. 1325–1340, 2025, doi: 10.1007/s10508-025-03114-5.

[4] Slonje, R., and Smith, P. K.: "Cyberbullying: Another main type of bullying?", en *Scandinavian journal of psychology*, vol. 49, n. 2, pp. 147-154, 2008, doi: 10.1111/ j.1467-9450.2007.00611.x.

[5] Waasdorp, T. E., and Bradshaw, C. P.: "The overlap between cyberbullying and traditional bullying", en *Journal of Adolescent Health*, vol. 56, n. 5, pp. 483–488, 2015, doi: 10.1016/j.jadohealth.2014.12.002.

[6] Nicholson, J., Javed, Y., Dixon, M., Coventry, L., Ajayi, O. D., and Anderson, P.: "Investigating teenagers' ability to detect phishing messages", en *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pp. 140-149, 2020, September. IEEE.

[7] Craven, S., Brown, S., and Gilchrist, E.: "Sexual grooming of children: Review of literature and theoretical considerations", en *Journal of sexual aggression*, vol. 12, n. 3, pp. 287-299, 2006.

[8] Jeglic, E. L., Winters, G. M., and Johnson, B. N.: "Identification of red flag child sexual grooming behaviors", en *Child Abuse & Neglect*, vol. 136, pp. 105998, 2023.

[9] Molina-Cañabate, J. P., González-Esteban, J. L., and López-Rico, C. M.: "Children and fake news: Media literacy and digital education in the age of disinformation", en *Education Sciences*, vol. 13, n. 8, pp. 763, 2023, doi: 10.3390/educsci13080763.

[10] Kowalski, R. M., Limber, S. P., and McCord, A.: "A developmental approach to cyberbullying: Prevalence, consequences, and risk factors", en *Journal of Youth and Adolescence*, vol. 48, n. 9, pp. 1767–1781, 2019, doi: 10.1007/s10964-019-01099-4.

[11] Runions, K. C., Bak, M., and Shaw, T.: "Cyberbullying perpetration and victimization: The role of social–emotional competence and moral disengagement", en *Aggressive Behavior*, vol. 47, n. 5, pp. 530–541, 2021, doi: 10.1002/ab.21959.

[12] Algarni, A., Xu, Y., and Chan, T.: "An empirical study on the susceptibility to social engineering in social networking sites: The case of phishing", en *Information & Computer Security*, vol. 23, n. 4, pp. 367–388, 2015, doi: 10.1108/ICS-05-2014-0029.

[13] Jagatic, T. N., Johnson, N. A., Jakobsson, M., and Menczer, F.: "Social phishing", en *Communications of the ACM*, vol. 50, n. 10, pp. 94-100, 2007.

[14] Gámez-Guadix, M., De Santisteban, P., and Resett, S.: "Sexting among Spanish adolescents: Prevalence and association with sexual grooming and cyberbullying victimization", en *Computers in Human Behavior*, vol. 120, pp. 106761, 2021, doi: 10.1016/j.chb.2021.106761.

[15] Reneses, M., Riberas-Gutiérrez, M., and Bueno-Guerra, N.: ""He flattered me". A comprehensive look into online grooming risk factors: Merging voices of victims, offenders and experts through in-depth interviews", en *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, vol. 18, n. 4, 2024.

[16] Whittle, H., Hamilton-Giachritsis, C., Beech, A., and Collings, G.: "A review of online grooming: Characteristics and concerns", en *Aggression and Violent Behavior*, vol. 19, n. 1, pp. 62–70, 2014, doi: 10.1016/j.avb.2013.11.007.

[17] Pennycook, G., and Rand, D. G.: "Lazy, not biased: Susceptibility to partisan fake news is better explained by lack of reasoning than by motivated reasoning", en *Cognition*, vol. 188, pp. 39–50, 2019, doi: 10.1016/j.cognition.2018.06.011.

[18] Reneses, M., Riberas-Gutierrez, M., and Bueno-Guerra, N.: "Who shares fake news? The consumption and distribution of information among adolescents and its relationship to hate speech", en *Revista de educación*, n. 406, pp. 265-291, 2024.

[19] Riberas-Gutiérrez, M., Reneses, M., Gómez-Dorado, A., Serranos-Minguela, L., and Bueno-Guerra, N.: "Online grooming: factores de riesgo y modus operandi a partir de un análisis de sentencias españolas", en *Anuario de Psicología Jurídica*, vol. 34, n. 1, pp. 119-131, 2024.

[20] Reneses, M., Riberas-Gutiérrez, M., and Bueno-Guerra, N.: ""It's just a joke": gender, sexuality and trivialisation in adolescent online violence such as cyberhate, cyberbullying, and online grooming", en *Humanities and Social Sciences Communications*, vol. 12, n. 1, pp. 1-14, 2025.

[21] Reneses, M., Parder, M. L., Riberas-Gutiérrez, M., and Bueno-Guerra, N.: "Cyberbullying and cyberhate as an overlapping phenomenon among adolescents in Estonia and Spain: Cross-cultural differences and common risk factors", en *Children and Youth Services Review*, vol. 172, pp. 108285, 2025.

[22] Shrestha, N.: "Factor analysis as a tool for survey analysis", en *American journal of Applied Mathematics and statistics*, vol. 9, n. 1, pp. 4-11, 2021.

[23] Marengo, D., and Settanni, M.: "Examining the postdictive validity of self-report Big Five personality traits with objective recordings of online behaviors: a ten-year retrospective study using Facebook Page Likes", en *Heliyon*, vol. 10, n. 12, 2024.

[24] Herrero-Diz, P., Conde-Jiménez, J., and Reyes de Cózar, S.: "Teens' motivations to spread fake news on WhatsApp", en *Social Media+ Society*, vol. 6, n. 3, pp. 1–14, 2020, doi: 10.1177/2056305120942879.

[25] McGrew, S., Ortega, T., Breakstone, J., and Wineburg, S.: "The Challenge That's Bigger than Fake News: Civic Reasoning in a Social Media Environment", en *American Educator*, vol. 41, n. 3, pp. 4–9, 2017.

[26] Walrave, M., Vanwesenbeeck, I., and Heirman, W.: "Connecting and protecting? Comparing predictors of self-disclosure and privacy settings use between adolescents and adults", en *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, vol. 6, n. 1, 2012.

[27] Ribeiro, L., Guedes, I. S., and Cardoso, C. S.: "Which factors predict susceptibility to phishing? An empirical study", en *Computers & Security*, vol. 136, pp. 103558, 2024.

[28] Kavvadias, A., and Kotsilieris, T.: "Understanding the role of demographic and psychological factors in users' susceptibility to phishing emails: A review", en *Applied Sciences*, vol. 15, n. 4, pp. 2236, 2025.

[29] Kowalski, R. M., Giumetti, G. W., Schroeder, A. N., and Lattanner, M. R.: "Bullying in the digital age: a critical review and meta-analysis of cyberbullying research among youth", en *Psychological bulletin*, vol. 140, n. 4, pp. 1073, 2014.

[30] Akter, M., Godfrey, A. J., Kropczynski, J., Lipford, H. R., and Wisniewski, P. J.: "From parental control to joint family oversight: Can parents and teens manage mobile online safety and privacy as equals?", en *Proceedings of the ACM on Human-Computer Interaction*, vol. 6, n. CSCW1, pp. 1-28, 2022.

[31] Dittus, P. J.: "Parental monitoring and risk behaviors and experiences among high school students—Youth Risk Behavior Survey, United States, 2021", en *MMWR supplements*, vol. 72, 2023.

[32] Álvarez-García, D., García, T., and Betts, L.: "Anxiety and self-esteem as causes and consequences of cyber-victimization in preadolescence: a longitudinal study", en *European Journal of Psychology Applied to Legal Context*, vol. 7, n. 1, pp. 1-9, 2025.

[33] Jerrim, J.: "Who Responds to Phishing Emails? An International Investigation of 15-Year-¡? a3b2 show [nbs]?¿Olds¡? a3b2 show [/nbs]?¿Using PISA Data", en *British Journal of Educational Studies*, vol. 71, n. 6, pp. 701-724, 2023.