Métodos y efectos de la educación en ciberseguridad: una revisión sistemática

Alberto Beltran[1]; Manuel G. Jiménez-Torres[2] & Sara Sampayo[3]

[1] *Escuela Internacional de Posgrado, Universidad de Granada*

[2] *Departamento de Personalidad, Evaluación y Tratamiento Psicológico, Universidad de Granada*

[3] *Centro de investigación CRIMINA, Universidad Miguel Hernández de Elche*

Beltrán, Alberto; Jiménez-Torres, Manuel G. y Sampayo, Sara. (2023). Métodos y efectos de la educación en ciberseguridad: Una revisión sistemática. *Revista Electrónica de Criminología, 14-07*. 1-19

RESUMEN: Este estudio tiene como objetivo analizar las técnicas educativas en el área de ciberseguridad y ciberdelincuencia, concretamente, las dirigidas a población no-técnica. Se llevó a cabo una revisión sistemática de la literatura científica empleando las bases de datos Scopus, Web of Science y Proquest. Tras analizar 79 artículos, se encontró que la gamificación, el entrenamiento, la simulación, el multimétodo y los medios audiovisuales son las técnicas más habituales y con mejores resultados de efectividad. También se encontró que los estudios se centran más en la ciberseguridad y las herramientas de protección que en educar en las ciberamenazas y concienciar. Por otra parte, se halló un reparto equitativo de los estudios siguiendo el criterio edad, con la excepción de la educación dirigida a la tercera edad, que resultó ser escasa. Finalmente, se encontró que existe fuerte predominancia de las ciencias STEAM, como ciencias computacionales e informática, frente a las ciencias sociales (psicología, criminología o ciencias de la educación), existiendo una grave falta de interdisciplinariedad en el área de estudio.

PALABRAS CLAVE: Educación, ciberseguridad, ciberdelito, revisión sistemática, población no-técnica.

METHODS AND EFFECTS OF CYBERSECURITY EDUCATION: A SYSTEMATIC REVIEW.

ABSTRACT: The aim of this study was to analyze educational techniques in the area of cybersecurity and cybercrime, specifically those aimed at non-technical population. A systematic review of the scientific literature was carried out using the Scopus, Web of Science and Proquest databases. After analyzing 79 articles, it was found that gamification, training, simulation, multimethod and audiovisual media are the most common techniques with the best results in terms of effectiveness. It was also found that studies focus more on cybersecurity and protection tools than on educating on cyber threats and awareness. On the other hand, we found an even distribution of studies according to the age criterion, with the exception of education aimed at the elderly, which was found to be scarce. Finally, it was found that there is a strong predominance of STEAM sciences, such as computer science and informatics, as opposed to social sciences (psychology, criminology or educational sciences), with a serious lack of interdisciplinarity in the area of study.

KEYWORDS: Education, cybersecurity, cybercrime, literature Reviews, non-technical population.

FECHA DE RECEPCIÓN EN REC: 18/04/23
FECHA DE PUBLICACIÓN EN REC: 30/12/23
AUTOR/A DE CORRESPONDENCIA: Alberto Beltrán, albertobeltran@correo.ugr.es

1. Introducción

La ciberdelincuencia es una problemática que va en aumento, y en el caso de España, las cifras son muy preocupantes. En el "Estudio sobre percepción y nivel de confianza en España" (ONTSI, 2022) se encontró que, en tan solo un año, del 2019 al 2020, la ciberdelincuencia aumentó un 31,9% llegando a los 287.963 hechos conocidos. Directamente relacionado con esta cuestión, en el mismo estudio se afirma que "*las costumbres online determinan en gran medida la exposición a los ataques*" (ONTSI, 2022). Los factores de comportamiento humano son la clave para combatir el ciberdelito (Hadlington & Chivers, 2018). Por lo tanto, a la hora de prevenir la ciberdelincuencia, se debe incidir en la educación para poder cambiar dichos comportamientos. Dentro de la educación, son de especial importancia las técnicas educativas y su relación con la vulnerabilidad y capacidad de los usuarios no-técnicos (Choi, 2008). Estas se pueden dividir en dos objetivos distintos y compatibles: la educación en ciberseguridad, dirigida a formar en herramientas y capacidades para protegerse, y la educación en ciberdelincuencia, orientada a conocer las ciberamenazas y formas que toma el ciberdelito. Actualmente se están investigando distintas formas de educar, técnicas, metodologías, estrategias, etc., por lo que también se han realizado distintas revisiones sobre aspectos concretos dentro del ámbito.

En Coenraad et al. (2020), se realizó una revisión sistemática de los juegos digitales relacionados con la ciberseguridad. Identificaron 181 juegos y tras probarlos 1 hora cada uno, expusieron sus características. En Svabensky et al. (2020) examinaron 71 documentos centrándose en la educación en ciberseguridad. Discuten cursos, herramientas, ejercicios y enfoques de enseñanza y evaluaron las percepciones subjetivas de los estudiantes a través de cuestionarios. En cuanto a Zhang-Kennedy & Chiasson (2021), realizaron una revisión que cubría publicaciones académicas y productos de la industria relacionados con la educación en ciberseguridad dirigidas a usuarios finales no expertos. Identificaron 119 herramientas que catalogan en cinco categorías. También exploraron las tendencias actuales, evaluaron su uso y revisaron la evidencia empírica de la efectividad de las herramientas.

En Mendivil et al. (2022), se elaboró una revisión sistemática con el objetivo de explorar el uso de modelos de competencias para la elaboración de programas de formación y concienciación en ciberseguridad. Aldawood & Skinner (2018), consiguieron identificar algunas amenazas de ciberseguridad relacionadas con la ingeniería social en diversos entornos. Detallaron cómo los programas innovadores de educación en seguridad de la información pueden aumentar de manera efectiva la conciencia de los usuarios/empleados y, en última instancia, reducir los incidentes de seguridad cibernética. También se centra en empleados de organizaciones Jampen (2020), quien analiza la formación y entrenamiento en antiphishing y su eficacia. Al-Daeef et al. (2017), revisan el enfoque de capacitación de los usuarios como una solución no-técnica para mitigar las amenazas de seguridad en general y el problema de phishing en particular. Estudian factores como la atención de los usuarios, la concienciación y la retención de los conocimientos adquiridos durante más tiempo. Encuentran que las actividades de capacitación deben considerar los aspectos de adquisición, retención y transferencia de conocimientos.

Existe un amplio repertorio de técnicas y herramientas que presentan diversos resultados (Coenraad et al., 2020; Zhang-Kennedy & Chiasson, 2021) y que, en general, consiguen mejorar los conocimientos y la concienciación ante formas concretas de ciberdelitos (Aldawood & Skinner, 2018; Al-Daeef et al., 2017). Por lo tanto, es de especial relevancia analizar los beneficios que muestra cada una de esas técnicas en la población. Este estudio permitiría saber con más precisión cuáles de ellas son más adecuadas y efectivas. A esto se añade la importancia de conocer cuáles son los perfiles específicos a los que se dirige y las diferencias que hay en las técnicas empleadas. Es por todo ello que, un análisis de los resultados de las técnicas educativas puede ser de gran utilidad para seleccionar las más adecuadas en cada caso. También es de especial interés saber si se educa sobre las distintas formas de ciberdelito o si solo se educa en las medidas para protegerse.

Otro punto relevante es analizar cuál es la disciplina de trabajo de los autores implicados en los estudios, para así conocer el peso de las aportaciones desde distintas áreas (Ingenierías, Ciencias Sociales, etc.) y valorar si se está produciendo una desproporción, tal y como señalan algunos autores (Thackray et al., 2016). Por último, se busca determinar si se incluye la educación en ciberdelincuencia en la educación en ciberseguridad, ya que permite concienciar sobre las amenazas y riesgos del ciberespacio. Actualmente, no hay disponible una revisión sistemática y/o metaanálisis reciente que evalúe todas estas cuestiones presentadas. En el caso de este estudio, la relevancia reside en poder seleccionar las mejores técnicas de educación en ciberseguridad a la hora de proteger a población no-técnica. Con todo ello, la educación se podría optimizar y también los recursos necesarios que implica.
En la siguiente sección, se explicará la metodología del trabajo, que consiste en una revisión sistemática, las bases de datos empleadas, la estrategia de búsqueda, el proceso de selección y codificación. En la tercera sección, se describirán los resultados sobre las técnicas encontradas, su efectividad comparada, perfiles diana y áreas de estudio. En la cuarta sección, se discutirán los resultados y sus implicaciones, además de su relación con la literatura científica. En la última, resumiremos los contenidos y expondremos las principales conclusiones.

2. Método

El método empleado para este estudio ha sido la revisión sistemática, consultando las bases de datos SCOPUS, Web of Science y Proquest. Las revisiones sistemáticas de la evidencia científica son estudios que sintetizan la evidencia científica disponible, de forma eficiente (Tricco et al., 2015). Usan métodos explícitos y rigurosos para identificar, seleccionar, evaluar, analizar y sintetizar los estudios empíricos que permitirán responder a cuestiones específicas (Perestelo-Pérez, 2013). Permiten analizar áreas emergentes y son útiles

para responder preguntas de investigación (Sucharew & Macaluso, 2019). Mediante este procedimiento, se han seleccionado 79 artículos relacionados con la educación en ciberseguridad dirigida a población no-técnica. Estos artículos se eligen de revistas de referencia, altamente citadas y revisadas por pares. Además, en todo momento se ha seguido el protocolo PRISMA (Liberati et al., 2009; Hutton et al., 2016) para revisiones sistemáticas, con criterios de inclusión y exclusión de los artículos, y sus fases de identificación, selección, elegibilidad e inclusión.

La pregunta, claramente definida, sigue el formato PICOS: descripción de los participantes (P), las intervenciones (I), las comparaciones (C) y las medidas de resultado de la revisión sistemática (O), así como el tipo de estudio (S). Además, este tipo de técnicas son cada vez más empleadas para facilitar la toma de decisiones (Bosch-Capblanch et al., 2012). Se hace necesario enfocar cuidadosamente la pregunta y usar estrategias de búsqueda (Grant & Booth, 2009). En cuanto a la Pregunta de investigación que se plantea en este estudio es la siguiente: ¿Cuáles son los efectos de las distintas técnicas y herramientas utilizadas en educación en ciberseguridad/ciberdelincuencia orientada a usuarios no-técnicos?

A partir de dicha pregunta de investigación se determinan los siguientes objetivos de investigación:

- Objetivo 1: Identificar cuáles son las principales técnicas y herramientas para educar en ciberseguridad/ciberdelincuencia.
- Objetivo 2: Comparar los efectos de las diferentes técnicas y herramientas utilizadas en la educación en ciberseguridad/ciberdelincuencia sobre usuarios no-técnicos.
- Objetivo 3: Averiguar si la educación se centra únicamente en la educación en ciberseguridad o, por lo contrario, también incluye nociones de ciberdelincuencia y sus amenazas.
- Objetivo 4: Estudiar cuáles son las poblaciones específicas a las que se dirige esta educación.
- Objetivo 5: Identificar los perfiles científicos o áreas de estudio de los/as autores/as en dichas investigaciones.

2.1 Protocolo PICO

Se ha aplicado el protocolo PICO para la delimitación del estudio. Se utiliza el acrónimo PICO para la construcción de la pregunta (Villasís-Keever et al., 2020), en la cual se incluyen los cuatro componentes principales: población de estudio; intervención por evaluar; comparación de la intervención; outcome measures (efectos). Una vez finalizado, se ha procedido a codificar y analizar los artículos resultantes para la elaboración del análisis de resultados. En nuestro estudio los componentes son los siguientes:

(P) Población: La población objetivo del estudio es la población general, entendiendo esta como usuarios no-técnicos. Se excluye del estudio aquella educación dirigida a la siguiente población: Personas que por su rol o función tengan encomendadas tareas de ciberseguridad; profesionales de ciberseguridad; personas de tecnologías de la información en organizaciones y empresas; alumnos de titulaciones vinculadas a la ciberseguridad; Trabajadores públicos relacionados con la ciberseguridad o la ciberdelincuencia.

(I) Intervención: Recibir educación en el área de la ciberseguridad y/o sobre la ciberdelincuencia en sus distintas modalidades.

(C) Comparativo: Se comparan las distintas técnicas educativas en ciberseguridad/ciberdelincuencia sobre la población objetivo (usuarios no-técnicos).

(O) Resultados: Los efectos de la educación sobre la población objeto de estudio.

2.2 Estrategia de búsqueda

Para las búsquedas se han utilizado los términos «educación», «ciberseguridad», «ciberdelincuencia» junto con términos referentes a las consecuencias y efectos de dicha educación. Además, se han añadido términos relacionados con la población objetivo (población no técnica), se emplearon términos equivalentes y los conectores lógicos «Y» y «O» de acuerdo con la búsqueda booleana. Se seleccionaron únicamente artículos en lengua inglesa. Se han delimitado el tipo de literatura a aquellos que sean: artículos o artículos de conferencias.

El análisis de las bases de datos se llevó a cabo el 3 de junio del año 2022. Después de un examen de las bases de datos existentes, se seleccionaron como fuentes de búsqueda de datos primarios Web of Science, SCOPUS y Proquest.

2.3 Fórmula de búsqueda

TITLE-ABS-KEY (cybersecurity OR cyber-security OR cybercrime OR phishing) AND TITLE-ABS-KEY (educat* OR pedagog* OR teach* OR train* OR intervention OR gamification OR simulation) AND TITLE-ABS-KEY (result* OR benefit* OR capabilit* OR effect* OR skill* OR knowledge* OR victimisation OR victimization OR awareness) AND TITLE-ABS-KEY (non-tech* OR "non technical" OR "high school" OR high-school OR teen* OR teenage* OR child* OR youth OR k-12 OR "young people" OR citizenship OR elderly OR "elder population" OR user*)

2.4 Proceso de selección de los artículos

En primer lugar, los estudios recuperados se revisaron por título, keywords y resumen. Solo aquellos estudios preseleccionados en esta primera criba (teniendo en cuenta los criterios de inclusión/exclusión) pasaron a revisarse a texto completo. Fueron dos los revisores que procedieron a seleccionar las referencias relevantes de forma independiente. Para realizar un procedimiento exhaustivo se ha empleado el protocolo PRISMA (Liberati et al., 2009). La Figura 1, muestra el diagrama de flujo del proceso de búsqueda y selección según viene establecido en PRISMA y cuya finalidad es garantizar trasparencia y claridad.
En cuanto a los criterios de inclusión, fueron los siguientes:

a) Estudios primarios relativos a la educación en ciberseguridad y/o educación en cibercrimen y sus efectos en población no-técnica: beneficios, conocimientos, concienciación, habilidades, y reducción de la victimización.

b) Artículos de revistas y artículos de conferencias.

c) Revisión por pares (peer review).

d) Estudios observacionales: Diferencias en los resultados de capacitación/vulnerabilidad frente a ciberdelitos y ciberamenazas en función de haber recibido las técnicas de educación en ciberseguridad.

e) Estudios quasi y experimentales: Diferencias pre y post en los resultados de test, simulaciones o pruebas de capacitación y/o vulnerabilidad ante ciberamenazas, según hayan recibido educación en ciberseguridad y/o ciberdelincuencia.

Los criterios de exclusión:

a) Artículos duplicados.

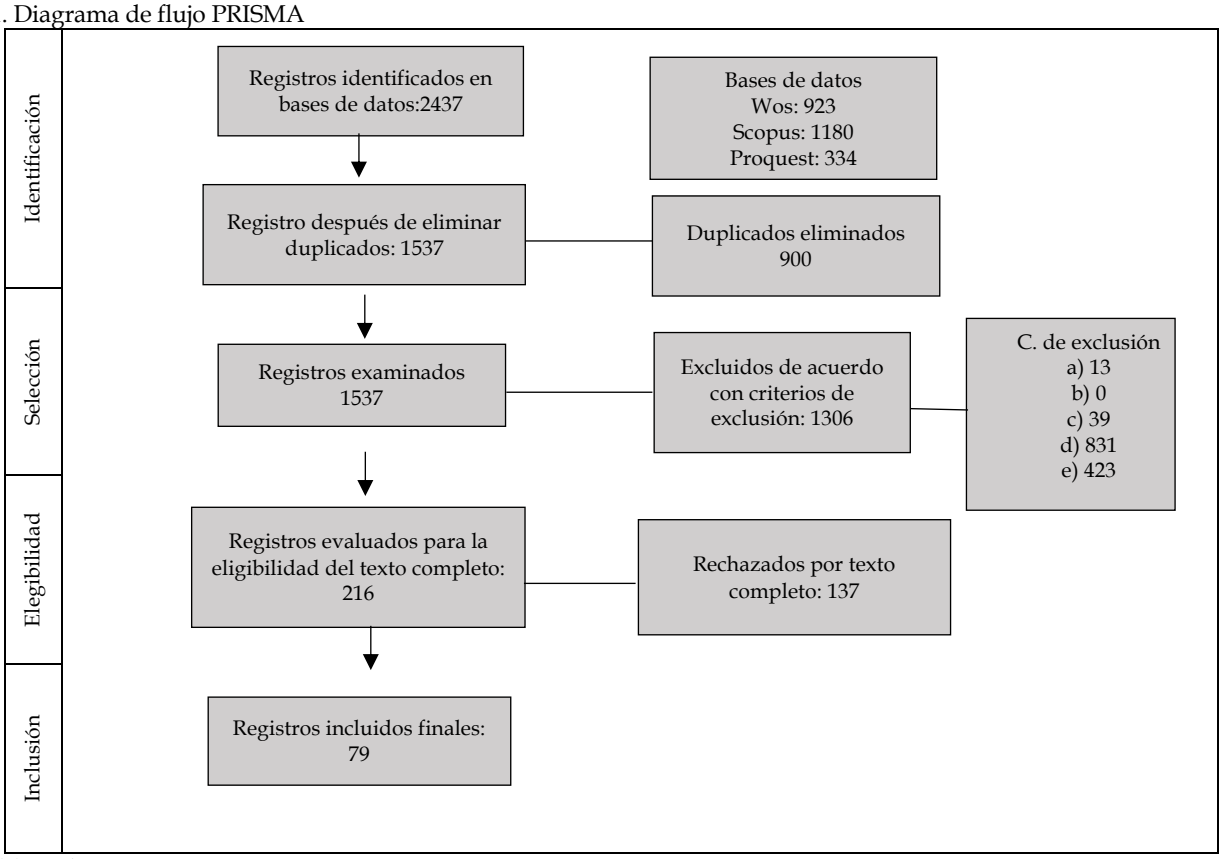
b) Literatura gris como blogs y noticias.

c) Revisiones sistemáticas y metaanálisis.

d) Artículos cuya población a la que se dirige la educación quede fuera del objeto de estudio: Personas que por su rol o función tengan encomendadas tareas de ciberseguridad; profesionales de ciberseguridad; personas TI de organizaciones y empresas; alumnos de titulaciones vinculadas a la ciberseguridad; Trabajadores públicos relacionados con la ciberseguridad o la ciberdelincuencia.

e) Artículos fuera de objeto de estudio; artículos sobre cuestiones relacionadas, pero no tengan intervención.

Figura 1. Diagrama de flujo PRISMA



Fuente: Elaboración propia

Tabla 1. Artículos incluidos en fase final

Ar.	1° AUTOR Y AÑO	Ar.	1° AUTOR Y AÑO	Ar.	1° AUTOR Y AÑO	Ar.	1° AUTOR Y AÑO
1	Giannakas, F. 2019	21	Shen, L.W. et al. 2021	41	Moreno-Fernández, M. 2017	61	Gokul, C.J. et al. 2018
2	Reid, R. 2015	22	Giannakas, F. et al. 2015	42	Herzberg, A. et al. 2011	62	Newbould, M. et al. 2009
3	Decusatis, C. 2022	23	Qusa, H. et al. 2021	43	Jin, G. et al. 2018	63	Visoottiviseth, V. et al. 2018
4	Cornel, C. 2016	24	Amo, L.C. et al. 2019	44	Scholefield, S. 2019	64	Kumaraguru, P. et al. 2007
5	Yett, B. 2020	25	Veneruso, S.V. et al. 2020	45	Kumaraguru, P. et al. 2007	65	Neo, H.F. et al. 2021
6	Al-Hamar, Y. 2020	26	Huynh, D. et al. 2017	46	Chen, T. et al. 2020	66	Kaabi, L.A. et al. 2022
7	Chattopadhyay, A. 2019	27	Alqahtani, H. et al. 2020	47	Beckers, K. et al. 2016	67	Kovačević, A. et al. 2020
8	Tsokkis, P. 2018	28	Septiana, R. et al. 2020	48	Alwanain, M. 2021	68	Kumaraguru, P. et al. 2009
9	Saito, T. et al. 2019	29	Lim, I. et al. et al. 2016	49	Lastdrager, E. et al. 2019	69	Giannakas, F. et al. 2016
10	De Bona, M. et al. 2020	30	Maqsood, S. et al. 2021	50	Cuchta, T. et al. 2019	70	Olano, M. et al. 2014
11	Mugayitoglu, B. 2021	31	Mikka-Muntuumo, J. et al. 2021	51	Rastenis, J. et al. 2020	70	Ganesh, A. et al. 2022
12	Burris, J. et al. 2018	32	Volkamer, M. et al. 2018	52	Baillon, A. et al. 2019	72	Baslyman, M. et al. 2016
13	Plachkinova, M. et al. 2019	33	Sercombe, A.A. et al. 2012	53	Wolf, S. et al. 2020	73	Reid, R. 2014
14	Reinheimer, B. 2020	34	Sookhanaphibarn, K. et al. 2020	54	Davinson, N. et al. 2010	74	Quinkert, F. et al. 2021
15	Pittman, J.M. et al. 2016	35	Tschakert, K.F. et al. 2019	55	Kumaraguru, P. et al. 2008	75	Zhang-Kennedy, L. 2 et al. 016
16	Sheng, S. et al. 2007	36	Sun, J.C. et al. 2016	56	Kunz, A. et al. 2016	76	Weaver, B.W. et al. 2021
17	Alencar, G.D. et al. 2013	37	Dodge, R. et al. 2012	57	Zielinska, O.A. et al. 2014	77	Silic, M. et al. 2020
18	Wang, Y.J. et al. 2018	38	Salazar, M. et al. 2013	58	Peker, Y.K. et al. 2018	78	Wen, Z.A. et al. 2019
19	Wolf, S. et al. 2020	39	Streiff, J. et al. 2019	59	Schoebel, S. et al. 2021	79	Wash, R. et al. 2018
20	Kolb, C. et al. 2022	40	Althobaiti, K. et al. 2018	60	Alwanain, M. 2020		

Fuente: Elaboración propia

2.5 Codificación

Posteriormente, se procedió a la codificación de los 79 estudios que fueron finalmente incluidos en la revisión sistemática (Tabla 1) y se evaluó su calidad metodológica y/o riesgo de sesgo (González et al., 2012). Todo el proceso de selección de los estudios se realizó por pares, resolviendo las posibles discrepancias por consenso y con la intervención de una tercera autora. Las tablas de codificación se han incluido en el anexo. En ellas se encuentra toda la información completa empleada para el estudio. Durante la codificación de los estudios, se extrajo de cada uno de ellos los siguientes datos:

a) Publicación: cita completa, año, revista y país.

b) Tipo de técnicas empleadas.

c) Tipo de educación incluida: Ciberseguridad; ciberdelincuencia+ciberseguridad; ciberdelincuencia.

d) Población diana.

e) Área/disciplina de los/as autor/es

f) Resultados: Efectos de la educación en la población objeto de estudio. Mejora, disminución o ausencia de cambios sobre la vulnerabilidad/capacitación frente a la ciberdelincuencia.

- Ef.1: La mejora de la capacidad para protegerse en el ciberespacio/ disminución de la vulnerabilidad;
- Ef.2: La mejora de la capacidad para protegerse en el ciberespacio/ disminución de la vulnerabilidad frente a un grupo control;
- Ef.3: Disminución de la capacidad / aumento de la vulnerabilidad;
- Ef.4: Disminución de la capacidad / aumento de la vulnerabilidad frente a un grupo control;
- Ef.5: Ausencia de cambios o cambios no significativos.
- Ef.6: Ausencia de cambios / resultados idénticos al grupo contro

3. Resultados

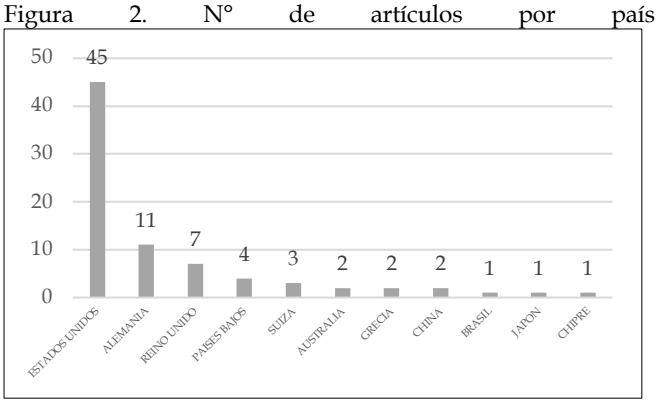
Los resultados se han dividido en un primer apartado de variables geográficas con el análisis por países. Un segundo apartado con los tipos de educación y las técnicas empleadas en donde se exponen los efectos de la educación y se comparan las técnicas. Por último, un apartado con las poblaciones diana y las áreas de estudio de los autores.

3.1 Países

Tal y como se puede observar en la Figura 2, la predominancia de Estados Unidos es clara, con un total de 45 artículos de los 79 incluidos en el estudio. La mayor parte de las revistas de ciberseguridad en las que se publicaron los artículos de esta revisión, tienen su origen en los Estados Unidos. Le siguen muy de lejos Alemania con 11 artículos y Reino Unido con 7. Los demás países

aportan entre 1 y 4 de esta revisión. En cuanto a España, ninguno de los 79 artículos procede de dicho país.

Figura 2. N° de artículos por país



Fuente: Scopus y Web of Science

3.2 Tipos de educación y de técnicas empleadas

En la Tabla 2 se muestra el listado resultante de las técnicas encontradas en los 79 artículos. Se ha incluido en la primera columna el listado de técnicas y en la segunda columna el número de artículos de cada una. En la tercera se muestra el porcentaje de los artículos con relación al total (79). Entre las tres primeras técnicas están: Gamificación (31; 39,24%), Entrenamiento (14; 17,72%) y Multimétodo (10; 12,65%). Suman el 70% del total de las técnicas. El resto son menos frecuentes, encabezadas por la Simulación (6,33%) y los Medios audiovisuales (5,6%). También están presentes los campamentos de ciberseguridad o Cybercamp, robots, clases prácticas, escape room, e-learning, juego de cartas, talleres colaborativos, mapas conceptuales, comics y lectura de consejos y relatos.

A continuación, se han expuesto las distintas posibilidades planteadas de los efectos tras recibir educación en ciberseguridad/ciberdelincuencia. En los casos del Ef. 3 y Ef. 4 no hay ningún registro ya que no se encontraron estudios en los que los resultados post-tratamiento fuesen peores que los pre-tratamiento. Son ampliamente mayoritarios los que tuvieron Ef. 1 (La mejora de la capacidad) y Ef. 2 (Mejora frente al grupo control). En cuanto a los que presentaron los efectos Ef.5 (Ausencia de cambios) y Ef.6 (Ausencia de cambios frente a grupo control) son minoritarios, únicamente 5 artículos del total de 79.

Tabla 2. Técnicas educativas, n° de artículos y % de mejora tras la intervención.

Técnica	N° art.	% del total	Ef. 1	Ef. 2	Ef. 3	Ef. 4	Ef. 5	Ef. 6	% Mejora*
Gamificación	31	39,24%	20	10			1		51,75%
Entrenamiento	14	17,72%	4	8			1	1	29,25%
Multimétodo	10	12,65%	7	3					59,5%
Simulación	5	6,33%	3	1			1		47,16%
Medios audiovisuales	4	5,6%	3	1					67,5%
Cybercamp	3	3,79%	3						49,5%
Robot	2	2,53%	1	1					33%
Clases prácticas	2	2,53%	1					1	-
Escape Room	2	2,53%	2						-
E-Learning	1	1,27%	1						58%
Juego de cartas	1	1,27%	1						
Taller grupal/ colaborativo	1	1,27%	1						82%
Mapas conceptuales	1	1,27%		1					-
Cómic	1	1,27%	1						42%
Lectura de consejos/ relatos	1	1,27%		1					21%

Nota. El % medio de mejora tras recibir educación en ciberseguridad/ciberdelincuencia.

Fuente: Elaboración propia

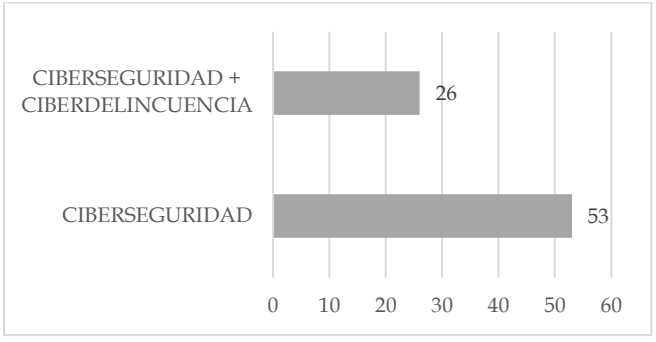
Por último, tras recopilar los datos de los resultados que presentaron los participantes de los estudios y armonizar los datos en % de mejora, se elaboró una tabla (Tabla 3) en donde poder comparar los % de dichos estudios organizados por técnica. Las mejoras en algunos casos se obtuvieron mediante pretest y postest tras la intervención. En otros casos, mediante la comparativa de distintas técnicas en diferentes grupos. En algunos estudios no fue posible obtener esos datos porque, o bien no se mostraba ese dato en el artículo, o bien no fue posible transformar en % de mejora. Una vez realizada la tabla, se procedió a hacer la media total de mejora de todos los estudios de cada técnica empleada. Esa media de % de mejora se muestra en la última columna (% Mejora).

Si ordenamos las técnicas por % de mejora tras la intervención educativa, encontramos entre las 5 primeras: el taller colaborativo (82%) (solamente 1 estudio), seguido de Medios Audiovisuales (67,5%), la técnica Multimétodo (59,5%), E-Learning (58%) y la Gamificación (51,75%). De estas 5 primeras técnicas con

mejor % de mejora, la Gamificación y el Multimétodo se encuentran también entre las 5 primeras en número de artículos totales. Se puede afirmar que estas 2 técnicas, Gamificación y Multimétodo, son las que presentan mejores puntuaciones de aprendizaje siendo las mejores a nivel de respaldo empírico. La técnica de entrenamiento, aunque se encuentra en el segundo puesto en número total de artículos, tiene el penúltimo resultado en % de mejora. Por lo tanto, se muestra como una de las técnicas que menores beneficios proporciona frente a otras técnicas. A esto se añade que, si la comparamos con las otras que tienen mayor respaldo científico en número de artículos, se encuentra en el último puesto a nivel de % de mejora.

En cuanto a los tipos de educación según los contenidos incluidos (ver Figura 3), existe una gran diferencia entre aquellas que se orientan únicamente a la ciberseguridad, frente a las que incluyen también aspectos sobre ciberdelincuencia. Las primeras se centran en las herramientas, medios, capacidades y conocimientos para defenderse de posibles ciberamenazas, mientras que las segundas incluyen nociones sobre cuáles son las ciberamenazas: formas de ciberdelitos, conceptos teóricos y prácticos sobre phishing, malware, grooming, sexting, smishing, rootkit, etc. Tal y como se puede observar en la Figura 3, las que se orientan fundamentalmente a la ciberseguridad (53) son mayores que las que contienen conocimientos también en ciberdelincuencia (26). No se han encontrado artículos que solamente contengan conocimientos sobre las ciberamenazas sin incluir ciberseguridad.

Figura 3. Gráfica de barras de los distintos tipos de educación según sus contenidos



Fuente: Elaboración propia

3.3 Población diana y áreas de estudio

En la Tabla 4 se muestran los datos relacionados con los colectivos objetivo de intervención según su edad. Tal y como se puede observar, siguen una progresión numérica desde la infancia hasta los adultos, con la excepción de la tercera edad en donde hay 1 solo artículo (0,94%). Este dato resalta la falta de investigaciones que estudien la educación en ciberseguridad orientada a la tercera edad. La mayor parte de las intervenciones educativas se centran en adultos (31,13%) y en los jóvenes (26,41%), que juntos suman 57,54% del total. También cabe destacar que parte de los estudios orientados a estos grupos, estaban dirigidos específicamente a empleados de organizaciones, instituciones y empresas. Por último, los niños (18,86%) y los adolescentes (22,64%) acumulan el 41,5% del total de las investigaciones.

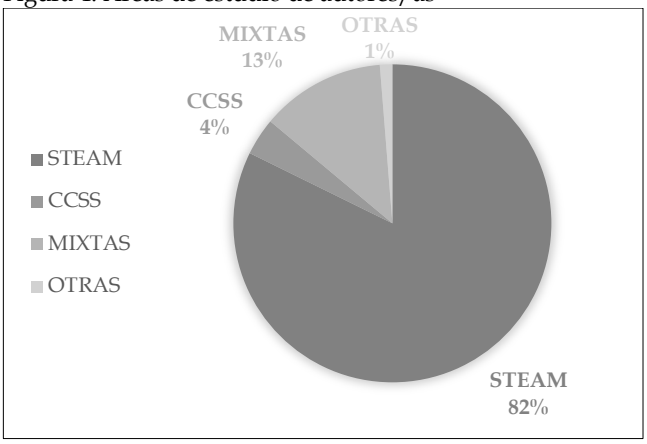
Tabla 3. Tabla de colectivos por edades y área de estudio de autores/as

Colectivo por edad	Rango de edades	N°Artículos	porcentaje
Niños	0-12	20	18,86%
Adolescentes	12-18	24	22,64%
Jóvenes	18-30	28	26,41%
Adultos	30-65	33	31,13%
Ancianos	+65	1	0,94%
Área de Estudio de los/as autores/as		N° de artículos	Porcentaje
STEAM	Ciencias/Tecnologías / Ingenierías/ Artes/ Matemáticas	65	82%
CC.SS.	Ciencias Sociales	3	4%
MIXTAS	STEAM y/o CCSS y/o Otras	10	13%
OTRAS	Áreas no incluidas anteriormente	1	1%

Fuente: Elaboración propia

En cuanto a las áreas de estudio de los autores, los datos son muy claros en la supremacía de las ciencias (STEAM) frene a otras áreas como son las ciencias sociales (ver Figura 4). Los artículos que fueron elaborados exclusivamente por autores/as procedentes de ciencias STEAM forman el 82% del total, mientras que los elaborados en exclusiva por autores/as de ciencias sociales (en adelante CC.SS) apenas alcanzan el 4%. Dentro del área STEAM, predominan las Ciencias Computacionales, ya que un gran número de autores/es pertenecen a esa rama de estudio. Otro dato relevante es la falta de interdisciplinariedad: de todos los estudios, tan solo el 13% estuvieron formados por miembros procedentes de áreas de STEAM y CC. SS conjuntamente.

Figura 4. Áreas de estudio de autores/as



Fuente: Elaboración propia

4. Discusión

Tras los resultados hallados, se puede afirmar que las principales técnicas que se están empleando en el ámbito de la educación en ciberseguridad son la gamificación, el entrenamiento, las técnicas multimétodo, la simulación y los medios audiovisuales. Este conjunto de técnicas va más allá de la educación expositiva tradicional y enfocan la educación como un proceso interactivo en el que la persona participante debe implicarse activamente. Por su parte, la gamificación aplica los conocimientos de la teoría del juego y la teoría del flujo (Deterding et al., 2011; Silic, 2020) a contextos ajenos al juego, con la finalidad de modificar los comportamientos y resultados. Los principios de esta "ludificación" se han mostrado como un enfoque eficaz para mejorar la capacidad de protección (51,75%), la motivación intrínseca, el aprendizaje, las habilidades de afrontamiento y el cumplimiento de las normas de seguridad.

En cuanto al entrenamiento, se considera una estrategia para mejorar la capacidad de discriminación, adecuada para aumentar sensibilidad a las señales visuales de engaño y para producir una mejora de las capacidades discriminativas (Dodge, 2012; Moreno-Fernández, 2017; Lastdrager, 2019). No obstante, tal y como se muestra en los resultados, es de las técnicas que tiene una tasa de mejora más baja frente a las demás (29,25%). De esto se desprende que quizás fuese una buena técnica para combinar con otras dentro del multimétodo. Las tareas multimétodo se refieren al uso mixto de varias técnicas de forma conjunta, aunque habitualmente consisten en la combinación de las técnicas más habituales como la gamificación, el entrenamiento o la simulación (Chattopadhyay, 2019; Mugayitoglu, 2021; Reinheimer, 2020; Pittman, 2016; Alencar, 2013; Wolf, 2020; Tschakert, 2019; Herzberg, 2011; Baillon, 2019; Wen, 2019). El uso mixto de técnicas muestra buenos resultados (59,5% de mejora) y permite beneficiarse de los beneficios que aporta cada una de ellas. El hecho de que en la mayoría de las ocasiones que se emplea el multimétodo se incluya la gamificación, es otra muestra de la versatilidad y efectividad que tiene la misma. De los resultados obtenidos se desprende que esta opción resulta de las mejores a la hora de educar en ciberseguridad.

Los campamentos de ciberseguridad o Cybercamp también muestran buenos resultados (49,5%), siendo un tipo de actividad inmersiva, con un fuerte contenido de socialización y trabajo en equipo (Cornel, 2016; Pittman, 2016; Jin, 2018; Wolf, 2020). Otras técnicas, como el empleo de Robot o Robot Social (Yett, 2020; Althobaiti, 2018) apuestan por dar nuevas aplicaciones (educativas en ciberseguridad) a las tecnologías más innovadoras. Las Clases prácticas son otra herramienta que se muestra eficaz por la implicación y la atención que requiere, mejorando la motivación intrínseca (Amo, 2019; Kolb, 2022). El Escape Room, el tradicional juego que consiste en tratar de escapar de una sala o lugar en un tiempo límite, también se ha conseguido aplicar al ámbito de la educación en ciberseguridad (Decusatis, C. 2022; Streiff, 2019).

Por último, se han encontrado resultados positivos en las técnicas de E-Learning (Peker, 2018), los juego de cartas (Wang, 2018), taller grupal y colaborativo (Kovačević, 2020), mapas conceptuales (Sun, 2016), cómic (Zhang-Kennedy, 2016) y la lectura de consejos y relatos (Wash, 2018). Merece una especial atención los talleres grupales y colaborativos (mejora del 82%) porque permiten socializar, de una forma transversal a todo el proceso educativo, con el grupo de iguales. Hay que señalar que la literatura a este respecto es escasa, ya que solo se ha podido incluir un estudio. En estos talleres, los participantes trabajan en grupo para superar las distintas pruebas y retos educativos.

Basándose en los resultados encontrados, se confirma que son más numerosas las técnicas que se orientan únicamente a la ciberseguridad frente a las que incluyen también aspectos sobre ciberdelincuencia. La relevancia de este hecho radica en que, la ciberseguridad como elemento único, puede no ser suficiente a la hora de prevenir la ciberdelincuencia en la población. Si solamente se da formación en medios y herramientas para poder protegerse, pero no se informa lo suficiente de cuáles son las amenazas reales en el ciberespacio, no estaremos completando totalmente la prevención de los individuos. Esto va en la misma línea que diversos autores, los cuales señalan que la clave de la prevención es la es la concienciación ciberdelito (Aldawood & Skinner, 2018; Hadlington & Chivers, 2018; Huynh, 2017). Otro motivo es que, tal y como señala la literatura (Chadee & Ng Ying, 2013), cuando se informa a la población sobre cuáles son las amenazas existentes, también estamos apelando a una cierta preocupación o miedo moderado. Este motivará al individuo y conseguirá que ponga en marcha esos conocimientos de ciberseguridad.

Los datos arrojan que la educación se dirige de una forma muy equilibrada a los colectivos poblacionales siguiendo el criterio de edad. Se reparten entre niños, adolescentes, jóvenes y adultos en un rango del 18% al 31%. La única excepción es la de la tercera edad (Alwanain, 2020), para la que apenas se han puesto en marcha estudios de cómo adaptar la educación en ciberseguridad. En cuanto a niños y adolescentes, las técnicas empleadas más habituales son las técnicas de gamificación, en algunos casos adaptadas de modo específico para esos colectivos (Giannakas, 2015; Giannakas, 2016; Giannakas, F. 2019; Shen, 2021; Qusa, 2021; Maqsood, 2021; Schoebel, 2021; Neo, 2021; Reid, 2014). El empleo de juegos tiene un componente motivador muy grande en estos colectivos y, sobre todo, consigue un equilibrio necesario entre aprendizaje y entretenimiento.

También son especialmente útiles los materiales audiovisuales (Reid, 2015) y los cybercamps (Cornel, 2016; Pittman, 2016; Jin, 2018; Wolf, 2020). Los materiales audiovisuales fomentan la activación de

distintos sentidos y crean estímulos visuales y auditivos. Estas cualidades permiten mejorar la motivación y la atención en la infancia frente a la exposición oral o los textos. En el caso de los cybercamps, éstos permiten crear un entorno educativo completo con inmersión educativa prolongada y compartida. En cuanto al entrenamiento aplicado a niños, Saito (2019), Alwanain (2021) y Lastdrager (2019), han tenido buenos resultados, con mejoras del 49%, 50% y 14% respectivamente. Esto demuestra que siempre que sean técnicas que requieran una respuesta constante y participativa, será útil y efectiva en los/as niños/as.

En lo que respecta a los jóvenes y adultos, gran parte de las técnicas que se han implementado han seguido la línea de la gamificación (Sheng, 2007; Veneruso, 2020; Huynh, 2017; Alqahtani, 2020; Sercombe, 2012; Sookhanaphibarn, 2020; Salazar, 2013; Scholefield, 2019; Chen, 2020; Beckers, 2016; Cuchta, 2019; Kunz, 2016; Gokul, 2018; Newbould, 2009; Kumaraguru, 2009; Baslyman, 2016; Silic, 2020). La media de mejora conseguida con esta técnica es un 51,75% (Tabla 3), por lo que emplear esta técnica es garante de buenos resultados, aunque un elemento imprescindible a tener en cuenta es procurar adaptar siempre la gamificación a la población diana a la que se dirige.

Siguiendo con el colectivo de jóvenes y adultos, también nos encontramos el entrenamiento (Moreno-Fernández, 2017; Kumaraguru, 2007; Rastenis, 2020; Davinson, 2010; Kumaraguru, 2008; Zielinska, 2014; Quinkert, 2021; Weaver, 2021) y la simulación (De Bona, 2020; Burris, 2018 Septiana, 2020; Lim, 2016) como las grandes apuestas para poder educar y proteger a estos colectivos. El entrenamiento y la simulación van muy unidos, suelen incluir ejemplos de ciberataques ante los que el participante debe protegerse. Mediante ensayo y error y con mensajes de feedback, se van mejorando los conocimientos y la capacidad de defensa. También permiten al usuario/a habituarse al lenguaje del ámbito, al modus operandi de los ciberdelincuentes, identificar y detectar contenidos sospechosos o fraudulentos y aprender a reaccionar ante ellos.

Los resultados muestran claramente la supremacía de los perfiles procedentes de ciencias STEAM, especialmente de ciencias computacionales e informática. Se ha encontrado que son perfiles muy técnicos centrados en cuestiones de programación, diseño y ciberseguridad a un nivel avanzado. Por otra parte, los perfiles procedentes de CC.SS. son escasos, como sería el caso de psicología, criminología, sociología o ciencias de la educación. Esta falta de interdisciplinariedad va en línea con lo que señalan algunos autores (Ghernaouti-Helie, 2009), que apuntan a una falta de diversidad científica en los perfiles dedicados a la educacióne en ciberseguridad. La importancia de lo que está sucediendo reside en que, cuando hablamos de educación en ciberseguridad, deberían estar presentes perfiles con conocimientos en pedagogía y aprendizaje. También son necesarios perfiles relacionados con el comportamiento humano, como psicología o criminología. Cuando se habla de víctimas, delincuentes, heurísticos, factor del miedo, vulnerabilidad, capacitación, ciberresiliencia, error humano, etc. estamos dentro del área de estudio de estas ciencias. En línea de lo que señala la literatura (López et al., 2021), la riqueza de disponer de distintas visiones, metodologías, enfoques y conocimientos permitirá abordar la cuestión de la educación en ciberseguridad orientada a población no-técnica de un modo completo y más adaptado a la realidad. Adicionalmente, es de destacar que ninguno de los 79 artículos proceda de España, lo que pueda ser señal de una falta de inversión, de medios y de revistas de impacto en el área de la ciberseguridad. Se debe tener en cuenta el efecto distorsionador del idioma, ya que el inglés es el idioma predominante, y tanto EE. UU. como Reino Unido son de habla inglesa.

5. Conclusiones

La principal contribución de este estudio es dar una visión global de las técnicas educativas en el área de ciberseguridad y ciberdelincuencia. Se ha encontrado que la gamificación, el entrenamiento, la simulación, el multimétodo y los medios audiovisuales son las técnicas más habituales. De ellas, las que obtienen mejores resultados de eficacia son la gamificación y el multimétodo. Todas estas técnicas consiguen mejorar la protección, los conocimientos en ciberseguridad y en ciberdelincuencia, y sobre todo, defenderse de ciberamenazas como el phishing. En líneas generales, los beneficios de emplear estas técnicas son: la mejora de la motivación intrínseca, asentar los conocimientos, conseguir valoraciones muy positivas de los participantes y mejorar la atención frente a la educación tradicional (expositiva).

En cuanto a los contenidos, se ha hallado que los estudios se enfocan principalmente en las herramientas y medidas para protegerse, frente a aquellos otros que incluyen contenidos para educar sobre la ciberdelincuencia. Estas diferencias son relevantes por la enorme utilidad que tiene aprender cuáles son las ciberamenazas, especialmente de cara a la concienciación y la puesta en marcha de las medidas de autoprotección. También se analizó la literatura científica atendiendo a las poblaciones diana en función de la edad, encontrando un reparto equitativo entre los distintos colectivos con la excepción de la tercera edad. Esta última apenas tiene estudios que la hayan abordado, por lo que sería necesario un mayor trabajo en esta dirección.

Finalmente, se ha encontrado que existe fuerte predominancia de las ciencias STEAM (especialmente ciencias computacionales) frente a las CC.SS. Todo ello a pesar de la importancia que tienen los enfoques interdisciplinares, con la presencia de ciencias del comportamiento como pueden ser la psicología,

criminología, sociología o las ciencias de la educación. En cuanto a las limitaciones, se debe señalar que los porcentajes de mejora se han obtenido de estudios que emplearon distintas muestras. También que la cantidad de artículos de las distintas técnicas fueron distintos, por ejemplo, los de gamificación fueron más numerosos que los de talleres colaborativos. Otra limitación sería las propias de las revisiónes sistemáticas, ya que se han empleado bases de datos como Scopus y Web of Science, sin embargo, existen artículos en la literatura gris o en otras bases de datos que podrían aportar importantes estudios para el análisis.

Las implicaciones de esta investigación pueden ser especialmente relevantes en el ámbito aplicado de la educación en ciberseguridad. El motivo es que existe un gran esfuerzo por parte de las instituciones públicas y entidades privadas en mejorar la protección y conocimientos en la ciudadanía. Se están poniendo en marcha campañas y estrategias para poder empoderar a la población en estas capacidades, así que es de especial transcendencia poder conocer cuáles son las mejores técnicas y qué efectos tienen. Por esta razón, los resultados hallados en este estudio deberían ser tenidos en cuenta a la hora de diseñar los planes educativos en la materia. Para futuras investigaciones, sería interesante profundizar en cuáles han sido los puntos fuertes y débiles de cada una de esas técnicas. También sería enriquecedor el poder ampliar la información de efectos y resultados en algunas técnicas de las que apenas se han realizado estudios, como sería el caso de uso de cómics, talleres colaborativos, lectura de consejos y relatos, etc.

Referencias bibliográficas

Al-Daeef, M.M., Basir, N., & Saudi, M.M. (2017). Security awareness training: A review. Lecture Notes in *Engineering and Computer Science*, 2229, 446–451

Al-Hamar, Y., & Kolivand, H. (2020). A New Email Phishing Training Website. *Proceedings - International Conference on Developments in eSystems Engineering, DeSE*, *2020-December*, 263-268. https://doi.org/10.1109/DeSE51703.2020.9450238

Aldawood, H., & Skinner, G. (2018). Educating and Raising Awareness on Cyber Security Social Engineering: A Literature Review. In Lee, MJW and Nikolic, S and Shen, J and Lei, LCU and Wong, GKW and Venkatarayalu, N (Ed.), *PROCEEDINGS OF 2018 IEEE INTERNATIONAL CONFERENCE ON TALE*, (pp. 62–68).

Alencar, G. D., de Lima, M. F., & Firmo, A. C. A. (2013). Behavioral analysis as a means to prevent social engineering and phishing. *RESI Revista Electronica de Sistemas de Informacao*, *12*(3), 1. Advanced Technologies & Aerospace Collection.

Alqahtani, H., & Kavakli-Thorne, M. (2020). Design and evaluation of an augmented reality game for cybersecurity awareness (CybAR). *Information (Switzerland)*, *11*(2). https://doi.org/10.3390/info11020121

Althobaiti, K., Vaniea, K., & Zheng, S. (2018). Faheem: Explaining URLs to people using a Slack bot. *Proceedings of AISB Annual Convention 2018*, 1-8. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85051426851&partnerID=40&md5=c56d6bb6162bb263e3b69498131e3c8a

Alwanain, M., I. (2020). Phishing Awareness and Elderly Users in Social Media. *International Journal of Computer Science and Network Security*, *20*(9), 114-119. https://doi.org/10.22937/IJCSNS.2020.20.09.14

Alwanain, M., I. (2021). How Do Children Interact with Phishing Attacks? *International Journal of Computer Science and Network Security*, *21*(3), 127-133. https://doi.org/10.22937/IJCSNS.2021.21.3.17

Amo, L. C., Liao, R., Frank, E., Rao, H. R., & Upadhyaya, S. (2019). Cybersecurity Interventions for Teens: Two Time-Based Approaches. *IEEE Transactions on Education*, *62*(2), 134-140. Social Science Premium Collection. https://doi.org/10.1109/TE.2018.2877182

Baillon, A., de Bruin, J., Emirmahmutoglu, A., van de Veer, E., & van Dijk, B. (2019). Informing, simulating experience, or both: A field experiment on phishing risks. *PLOS ONE*, *14*(12). https://doi.org/10.1371/journal.pone.0224216

Baslyman, M., & Chiasson, S. (2016). «smells Phishy?»: An educational game about online phishing scams. *eCrime Researchers Summit, eCrime*, *2016-June*, 91-101. https://doi.org/10.1109/ECRIME.2016.7487946

Beckers, K., Pape, S., & Fries, V. (2016). HATCH: Hack and trick capricious humans – A serious game on social engineering. *Proceedings of the 30th International BCS Human Computer Interaction Conference, HCI 2016*, *2016-July*. https://doi.org/10.14236/ewic/hci2016.94

Bosch-Capblanch X., Lavis, J.N., Lewin, S., Atun, R., Røttingen, J.A., Dröschel D., Beck, L., Abalos, E., El-Jardali, F., Gilson, L., Oliver, S., Wyss, K., Tugwell, P., Kulier, R., Pang, T., & Haines, A. (2012). Guidance for evidence-informed policies about health systems: rationale for and challenges of guidance development. *PLoS Med*, 9(3), e1001185. https://doi.org/10.1371/journal.pmed.1001185

Burris, J., Deneke, W., & Maulding, B. (2018). Activity simulation for experiential learning in cybersecurity workforce development. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *10923 LNCS*, 17-25. https://doi.org/10.1007/978-3-319-91716-0_2

Chadee, D., & Ng Ying, N.K. (2013). Predictors of fear of crime: general fear verses perceived risk. *Journal of Applied Psychology*, 43(1), 1896-1904.

Chattopadhyay, A., Christian, D., Oeder, A., & Budul, I. (2019). A Novel Visual-Privacy Themed Experiential- Learning Tool for Human-Privacy Societal-Security Awareness in Middle-School and High-School Youth. *Proceedings - Frontiers in Education Conference, FIE*, *2019-October*. https://doi.org/10.1109/FIE43999.2019.9028375

Chen, T., Stewart, M., Bai, Z., Chen, E., Dabbish, L., & Hammer, J. (2020). Hacked time: Design and evaluation of a self-efficacy based cybersecurity game. *DIS 2020 - Proceedings of the 2020 ACM Designing Interactive Systems Conference*, 1737-1749. https://doi.org/10.1145/3357236.3395522

Choi, K. (2008). Computer Crime Victimization and Integrated Theory: An Empirical Assessment. *International Journal of Cyber Criminology* 2 (1): 308–333. Recuperado de: https://www.researchgate.net/publication/238621672_C

omputer_Crime_Victimization_and_Integrated_Theory_An_Empirical_Assessment

Coenraad, M., Pellicone, A., Ketelhut, D. J., Cukier, M., Plane, J., & Weintrop, D. (2020). Experiencing Cybersecurity One Game at a Time: A Systematic Review of Cybersecurity Digital Games. *Simulation and Gaming*, 51(5), 586–611. https://doi.org/10.1177/1046878120933312

Cornel, C., Cornel, C. M., Rowe, D. C., & Moses, S. (2016). A cybersecurity camp for girls. *ASEE Annual Conference and Exposition, Conference Proceedings*, *2016-June*. Recuperado de: https://www.scopus.com/inward/record.uri?eid=2-s2.0-84983347749&partnerID=40&md5=bd701a49eabb23972b48d3b95806f211

Cuchta, T., Blackwood, B., Devine, T. R., Niichel, R. J., Daniels, K. M., Lutjens, C. H., Maibach, S., & Stephenson, R. J. (2019). Human risk factors in cybersecurity. *SIGITE 2019 - Proceedings of the 20th Annual Conference on Information Technology Education*, 87-92. https://doi.org/10.1145/3349266.3351407

Davinson, N., & Sillence, E. (2010). It won't happen to me: Promoting secure behaviour among internet users. *Computers in Human Behavior*, *26*(6), 1739-1747. APA PsycInfo. https://doi.org/10.1016/j.chb.2010.06.023

De Bona, M., & Paci, F. (2020). A real world study on employees' susceptibility to phishing attacks. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3407023.3409179

Deterding, S., Dixon, D., Khaled, R., & Nacke, L. (2011). From game design elements to gamefulness: defining gamification. 15th international academic MindTrek conference: Envisioning future media environments. pp. 9-15.

Decusatis, C., Gormanly, B., Alvarico, E., Dirahoui, O., McDonough, J., Sprague, B., Maloney, M., Avitable, D., & Mah, B. (2022). A Cybersecurity Awareness Escape Room using Gamification Design Principles. *2022 IEEE 12th Annual Computing and Communication Workshop and Conference, CCWC 2022*, 765-770. https://doi.org/10.1109/CCWC54503.2022.9720748

Dodge, R., Coronges, K., & Rovira, E. (2012). Empirical benefits of training to phishing susceptibility. *IFIP Advances in Information and Communication Technology*, *376 AICT*, 457-464. https://doi.org/10.1007/978-3-642-30436-1_37

Ganesh, A., Ndulue, C., & Orji, R. (2022). Smartphone Security and Privacy – A Gamified Persuasive Approach with Protection Motivation Theory. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *13213 LNCS*, 89-100. https://doi.org/10.1007/978-3-030-98438-0_7

Ghernaouti-Helie, S. (2009). An Inclusive Information Society Needs a Global Approach of Information Security. *2009 International Conference on Availability, Reliability and Security*, 658-662. DOI: 10.1109/ARES.2009.127

Giannakas, F., Kambourakis, G., & Gritzalis, S. (2015). CyberAware: A mobile game-based app for cybersecurity education and awareness. *Proceedings of 2015 International Conference on Interactive Mobile Communication Technologies and Learning, IMCL 2015*, 54-58. https://doi.org/10.1109/IMCTL.2015.7359553

Giannakas, F., Kambourakis, G., Papasalouros, A., & Gritzalis, S. (2016). Security education and awareness for K-6 going mobile. *International Journal of Interactive Mobile Technologies*, *10*(2), 41-48. https://doi.org/10.3991/ijim.v10i2.5473

Giannakas, F., Papasalouros, A., Kambourakis, G., & Gritzalis, S. (2019). A comprehensive cybersecurity learning platform for elementary education. *Information Security Journal*, *28*(3), 81-106. https://doi.org/10.1080/19393555.2019.1657527

Gokul, C. J., Pandit, S., Vaddepalli, S., Tupsamudre, H., Banahatti, V., & Lodha, S. (2018). Phishy—A serious game to train enterprise users on phishing awareness. *CHI PLAY 2018 - Proceedings of the 2018 Annual Symposium on Computer-Human Interaction in Play Companion Extended Abstracts*, 169-181. https://doi.org/10.1145/3270316.3273042

González, J., Buñuel, J.C., & González, P. (2012). Listas guía de comprobación de estudios observacionales: declaración STROBE. *Evid Pediatr*. 8:65

Grant, M.J., & Booth, A. (2009). A typology of reviews: an analysis of 14 review types and associated methodologies. *Health Information and Libraries Journal*, 26(2), 91-108. https://doi.org/10.1111/j.1471-1842.2009.00848.x

Hadlington, L., & Chivers, S. (2018). Segmentation analysis of susceptibility to cybercrime: Exploring individual differences in information security awareness and personality factors. Policing: *A Journal of Policy and Practice*, April, 1-14.

Herzberg, A., & Margulies, R. (2011). Forcing Johnny to login safely: Long-term user study of forcing and training login mechanisms. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *6879 LNCS*, 452-471. https://doi.org/10.1007/978-3-642-23822-2_25

Hutton, B., Catalá-López, F., & Moher, D. (2016). La extensión de la declaración PRISMA para revisiones sistemáticas que incorporan metaanálisis en red: PRISMA-NMA. *Medicina Clinica*, *147*(6), 262–266. https://doi.org/10.1016/j.medcli.2016.02.025

Huynh, D., Luong, P., Iida, H., & Beuran, R. (2017). Design and evaluation of a cybersecurity awareness training game. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *10507 LNCS*, 183-188. https://doi.org/10.1007/978-3-319-66715-7_19

Jampen, D., Gür, G., Sutter, T., & Tellenbach, B. (2020). Don't click: towards an effective anti-phishing training. A comparative literature review. In *Human-centric Computing and Information Sciences* (Vol. 10, Issue 1). Springer Berlin Heidelberg. https://doi.org/10.1186/s13673-020-00237-7

Jin, G., Tu, M., Kim, T.-H., Heffron, J., & White, J. (2018). Game based cybersecurity training for High School Students. *SIGCSE 2018 - Proceedings of the 49th ACM Technical Symposium on Computer Science Education*, *2018-January*, 68-73. https://doi.org/10.1145/3159450.3159591

Kaabi, L. A., Ketbi, W. A., Khoori, A. A., Shamsi, M. A., & Alrabaee, S. (2022). Safe: Cryptographic Algorithms and Security Principles Gamification. *IEEE Global Engineering Education Conference, EDUCON*, *2022-March*, 1169-1178. https://doi.org/10.1109/EDUCON52537.2022.9766526

Kolb, C., Strouse, J., Palmer, J., Ford, V., & Turygina, V. (2022). Cyber Securing the Future. *AIP Conference Proceedings*, *2425*. https://doi.org/10.1063/5.0081419

Kovačević, A., & Radenković, S. D. (2020). SAWIT—Security Awareness Improvement Tool in the Workplace. *Applied Sciences*, *10*(9), 3065. Advanced Technologies & Aerospace Collection; Earth, Atmospheric & Aquatic Science Collection; ProQuest One Academic; Publicly Available Content Database. https://doi.org/10.3390/app10093065

Kunz, A., Volkamer, M., Stockhardt, S., Palberg, S., Lottermann, T., & Piegert, E. (2016). NoPhish: Evaluation of a web application that teaches people being aware of phishing attacks. *Lecture Notes in Informatics (LNI), Proceedings - Series of the Gesellschaft fur Informatik (GI)*, *P-259*, 509-518. Recuperado de: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85020702971&partnerID=40&md5=4e91989eb224aacf8f160041c1eb053e

Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2007). Protecting people from phishing: The design and evaluation of an embedded training email system. *Conference on Human Factors in Computing Systems - Proceedings*, 905-914. https://doi.org/10.1145/1240624.1240760

Kumaraguru, P., Rhee, Y., Sheng, S., Hasan, S., Acquisti, A., Cranor, L. F., & Hong, J. (2007). Getting users to pay attention to anti-phishing education: Evaluation of retention and transfer. *ACM International Conference Proceeding Series*, *269*, 70-81. https://doi.org/10.1145/1299015.1299022

Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F., & Hong, J. (2008). Lessons from a real world evaluation of anti-phishing training. *eCrime Researchers Summit, eCrime 2008*. https://doi.org/10.1109/ECRIME.2008.4696970

Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., Blair, M. A., & Pham, T. (2009). School of phish: A real-world evaluation of anti-phishing training. *SOUPS 2009 - Proceedings of the 5th Symposium On Usable Privacy and Security*. https://doi.org/10.1145/1572532.1572536

Lastdrager, E., Gallardo, I. C., Hartel, P., & Junger, M. (2019). How effective is anti-phishing training for children? *Proceedings of the 13th Symposium on Usable Privacy and Security, SOUPS 2017*, 229-239. Recuperado de: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85075917140&partnerID=40&md5=c509892b8cff514dd540a70a3f0bffd2

Liberati, A., Altman, D. G., Tetzlaff, J., Mulrow, C., Gotzsche, P. C., Ioannidis, J. P. A., & Moher, D. (2009). The PRISMA statement for reporting systematic reviews and meta-analyses of studies that evaluate healthcare interventions: Explanation and elaboration. *British Medical Journal*, *339*, b2700. doi: https://doi.org/10.1136/bmj. b2700

Lim, I., Park, Y.-G., & Lee, J.-K. (2016). Design of Security Training System for Individual Users. *Wireless Personal Communications*, *90*(3), 1105-1120. Advanced Technologies & Aerospace Collection. https://doi.org/10.1007/s11277-016-3380-z

López, J., Sánchez, F., Herrera, D., Martínez, F., Rubio, M., Gil, V., Santiago, A.M., & Gómez, M.A . (2021). Informe sobre la Cibercriminalidad en España. Dirección General de Coordinación y Estudios Secretaría de Estado de Seguridad . Ministerio del Interior, España. Recuperado de https://www.interior.gob.es/opencms/pdf/archivos-y-documentacion/documentacion-y-publicaciones/publicaciones-descargables/publicaciones-periodicas/informe-sobre-la-cibercriminalidad-en-Espana/Informe_cibercriminalidad_Espana_2021_126200212.pdf

Maqsood, S., & Chiasson, S. (2021). Design, Development, and Evaluation of a Cybersecurity, Privacy, and Digital Literacy Game for Tweens. *ACM Transactions on Privacy and Security*, *24*(4). https://doi.org/10.1145/3469821

Mikka-Muntuumo, J., & Peters, A. N. (2021). Designing an Interactive Game for Preventing Online Abuse in Namibia. *2021 3rd International Multidisciplinary Information Technology and Engineering Conference, IMITEC 2021*. https://doi.org/10.1109/IMITEC52926.2021.9714592

Moreno-Fernández, M. M., Blanco, F., Garaizar, P., & Matute, H. (2017). Fishing for phishers. Improving Internet users' sensitivity to visual deception cues to prevent electronic fraud. *Computers in Human Behavior*, *69*, 421. Advanced Technologies & Aerospace Collection.

Mugayitoglu, B., Borowczak, M., Burrows, A., Carson, A., Person, C., Finch, A., & Kennedy, C. (2021). A university's developmental framework: Creating, implementing, and evaluating a K-12 teacher cybersecurity micro-credential course. *ICSIT 2021 - 12th International Conference on Society and Information Technologies, Proceedings*, 35-40. Recuperado de https://www.scopus.com/inward/record.uri?eid=2-s2.0-85105867054&partnerID=40&md5=4d3140888267c6189eb1d76ae1c896ad

Neo, H.F., Teo, C.C., & Peng, C. L. (2021). Safe Internet: An Edutainment Tool for Teenagers. *Lecture Notes in Electrical Engineering*, *739 LNEE*, 53-70. https://doi.org/10.1007/978-981-33-6385-4_6

Newbould, M., & Furnell, S. (2009). Playing safe: A prototype game for raising awareness of social engineering. *Proceedings of the 7th Australian Information Security Management Conference*, 24-30. https://www.scopus.com/inward/record.uri?eid=2-s2.0-84864552106&partnerID=40&md5=c35c02b54b3c5929bc9cdb6fffd4c843

Olano, M., Sherman, A., Oliva, L., Cox, R., Firestone, D., Kubik, O., Patil, M., Seymour, J., Sohn, I., & Thomas, D. (2014). SecurityEmpire: Development and evaluation of a digital game to promote cybersecurity education. *2014 USENIX Summit on Gaming, Games, and Gamification in Security Education, 3GSE 2014*. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85040226944&partnerID=40&md5=78b3676884e4e3fb2e7c4ecbfe3d4725

ONTSI (Observatorio Nacional de Tecnología y Sociedad). (2022). Cómo se protege a la ciudadanía ante los ciberriesgos. Estudio sobre percepción y nivel de confianza en España. *Observaciber*. Recuperado de https://www.observaciber.es/sites/observaciber/files/media/documents/ciudadaniaciberriesgos_abril2022_1.pdf

Peker, Y. K., Ray, L., da Silva, S., & IEEE. (2018). *Online Cybersecurity Awareness Modules for College and High School Students* (WOS:000463185700004). 24-33. https://doi.org/10.1109/NCS.2018.00009

Perestelo-Pérez, L. (2013). Standards on how to develop and report systematic reviews in Psychology and Health. International Journal of Clinical and Health Psychology, 13, 49–57.

Pittman, J. M., & Pike, R. E. (2016). An Observational Study of Peer Learning for High School Students at a Cybersecurity Camp. *Information Systems Education Journal*, *14*(3), 4-13. ERIC.

Plachkinova, M., & Menard, P. (2019). An Examination of Gain- and Loss-Framed Messaging on Smart Home Security Training

Programs. *Information Systems Frontiers*. https://doi.org/10.1007/s10796-019-09970-6

Quinkert, F., Degeling, M., & Holz, T. (2021). Spotlight on Phishing: A Longitudinal Study on Phishing Awareness Trainings. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *12756 LNCS*, 341-360. https://doi.org/10.1007/978-3-030-80825-9_17

Qusa, H., & Tarazi, J. (2021). Cyber-Hero: A Gamification framework for Cyber Security Awareness for High Schools Students. *2021 IEEE 11th Annual Computing and Communication Workshop and Conference, CCWC 2021*, 677-682. https://doi.org/10.1109/CCWC51732.2021.9375847

Rastenis, J., Ramanauskaitė, S., Janulevičius, J., & Čenys, A. (2020). Impact of information security training on recognition of phishing attacks: A case study of vilnius gediminas technical university. *Communications in Computer and Information Science*, *1243 CCIS*, 311-324. https://doi.org/10.1007/978-3-030-57672-1_23

Reid, R., & Van Niekerk, J. (2014). Snakes and ladders for digital natives: Information security education for the youth. *Information Management & Computer Security*, *22*(2), 179-190. Advanced Technologies & Aerospace Collection; ProQuest One Academic; ProQuest One Business; Social Science Premium Collection. https://doi.org/10.1108/IMCS-09-2013-0063

Reid, R., & Van Niekerk, J. (2015). A cyber security culture fostering campaign through the lens of active audience theory. *Proceedings of the 9th International Symposium on Human Aspects of Information Security and Assurance, HAISA 2015*, 34-44. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85026347994&partnerID=40&md5=90f8bac7ab485818b4265a118ea60ba0

Reinheimer, B., Aldag, L., Mayer, P., Mossano, M., Duezguen, R., Lofthouse, B., von Landesberger, T., & Volkamer, M. (2020). An investigation of phishing awareness and education over time: When and how to best remind users. *Proceedings of the 16th Symposium on Usable Privacy and Security, SOUPS 2020*, 259-284. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85091852889&partnerID=40&md5=6643e561a062c251360023104af547b7

Saito, T., Yashiro, S., Tanabe, K., & Saito, Y. (2019). A Proposal and the Evaluation of a Hands-On Training System for Cyber Security. En Barolli, L and Leu, FY and Enokido, T and Chen, HC (Ed.), *Advances on broadband and wireless computing, communication and applications, BWCCA-2018* (Vol. 25, pp. 339-349). https://doi.org/10.1007/978-3-030-02613-4_30

Salazar, M., Gaviria, J., Laorden, C., & Bringas, P. G. (2013). Enhancing cybersecurity learning through an augmented reality-based serious game. *IEEE Global Engineering Education Conference, EDUCON*, 602-607. https://doi.org/10.1109/EduCon.2013.6530167

Schoebel, S., Roepke, R., & Schroeder, U. (2021). Phishing Academy: Evaluation of a Digital Educational Game on URLs and Phishing. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *13134 LNCS*, 44-53. https://doi.org/10.1007/978-3-030-92182-8_5

Scholefield, S., & Shepherd, L. A. (2019). Gamification Techniques for Raising Cyber Security Awareness. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *11594 LNCS*, 191-203. https://doi.org/10.1007/978-3-030-22351-9_13

Sercombe, A. A., & Papadaki, M. (2012). Education in the «virtual» community: Can beating Malware Man teach users about social networking security? *Proceedings of the 6th International Symposium on Human Aspects of Information Security and Assurance, HAISA 2012*, 33-39. https://www.scopus.com/inward/record.uri?eid=2-s2.0-84926306106&partnerID=40&md5=f1644a3a54a362b2832d3bbb04d16e84

Septiana, R., & Julian, R. K. (2020). Design of Phishing Simulation Dashboard Using Analytic Data Concepts. *Journal of Physics: Conference Series*, *1577*(1). Advanced Technologies & Aerospace Collection; ProQuest One Academic; Publicly Available Content Database. https://doi.org/10.1088/1742-6596/1577/1/012041

Shen, L. W., Mammi, H. K., & Din, M. M. (2021). Cyber Security Awareness Game (CSAG) for Secondary School Students. *2021 International Conference on Data Science and Its Applications, ICoDSA 2021*, 48-53. https://doi.org/10.1109/ICoDSA53588.2021.9617548

Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2007). Anti-Phishing Phil: The design and evaluation of a game that teaches people not to fall for phish. *ACM International Conference Proceeding Series*, *229*, 88-99. https://doi.org/10.1145/1280680.1280692

Silic, M., & Lowry, P. B. (2020). Using Design-Science Based Gamification to Improve Organizational Security Training and Compliance: JMIS. *Journal of Management Information Systems*, *37*(1), 129-161. Advanced Technologies & Aerospace Collection; ProQuest One Academic; ProQuest One Business; Social Science Premium Collection. https://doi.org/10.1080/07421222.2019.1705512

Sookhanaphibarn, K., & Choensawat, W. (2020). Educational games for cybersecurity awareness. *2020 IEEE 9th Global Conference on Consumer Electronics, GCCE 2020*, 424-428. https://doi.org/10.1109/GCCE50665.2020.9291723

Streiff, J., Justice, C., & Camp, J. (2019). Escaping to cybersecurity education: Using manipulative challenges to engage and educate. *Proceedings of the European Conference on Games-based Learning*, *2019-October*, 1046-1050. https://doi.org/10.34190/GBL.19.183

Sucharew, H., & Macaluso, M. (2019). Methods for Research Evidence Synthesis: The Scoping Review Approach. *Journal of Hospital Medicine* 14, 416-418. https://doi.org/10.12788/jhm.3248

Sun, J. C.-Y., & Chen, A. Y.-Z. (2016). Effects of integrating dynamic concept maps with Interactive Response System on elementary school students' motivation and learning outcome: The case of anti-phishing education. *COMPUTERS & EDUCATION*, *102*, 117-127. https://doi.org/10.1016/j.compedu.2016.08.002

Svabensky, V., Vykopal, J., & Celeda, P. (2020). What Are Cybersecurity Education Papers About? A Systematic Literature Review of SIGCSE and ITiCSE Conferences. *SIGCSE 2020 - Proceedings of the 51st ACM Technical Symposium on Computer Science Education*, 2–8. https://doi.org/10.1145/3328778.3366816

Thackray, H., McAlaney, J., Dogan, H., Taylor, J., & Richardson, C. (2016). Social psychology: An under-used tool in cybersecurity. *Proceedings of the 30th International BCS*

Human Computer Interaction Conference, HCI 2016, 2016-July. https://doi.org/10.14236/ewic/HCI2016.64

Tricco, A.C., Antony, J., Zarin, W., Strifler, L., Ghassemi, M., Ivory, J., Perrier, L., Hutton, B., Moher, D., & Straus, S.E. (2015). A scoping review of rapid review methods. *BMC Medicine*, 13(224). Recuperado de: https://bit.ly/2ZT1PUN

Tschakert, K. F., & Ngamsuriyaroj, S. (2019). Effectiveness of and user preferences for security awareness training methodologies. *Heliyon*, *5*(6), 1. MEDLINE. https://doi.org/10.1016/j.heliyon.2019.e02010

Tsokkis, P., & Stavrou, E. (2018). A password generator tool to increase users' awareness on bad password construction strategies. *2018 International Symposium on Networks, Computers and Communications, ISNCC 2018*. https://doi.org/10.1109/ISNCC.2018.8531061

Veneruso, S. V., Ferro, L. S., Marrella, A., Mecella, M., & Catarci, T. (2020). CyberVR: An Interactive Learning Experience in Virtual Reality for Cybersecurity Related Issues. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3399715.3399860

Villasís-Keever, M.A., Rendón-Macías, M.E., García, H., Miranda-Novales., M.G., & Escamilla-Núñez, A. (2020). La revisión sistemática y el metaanálisis como herramienta de apoyo para la clínica y la investigación. Rev Alerg Mex.; 67(1):62-72.

Visoottiviseth, V., Sainont, R., Boonnak, T., & Thammakulkrajang, V. (2018). POMEGA: Security game for building security awareness. *Proceeding of 2018 7th ICT International Student Project Conference, ICT-ISPC 2018*. https://doi.org/10.1109/ICT-ISPC.2018.8523965

Volkamer, M., Renaud, K., Reinheimer, B., Rack, P., Ghiglieri, M., Mayer, P., Kunz, A., & Gerber, N. (2018). Developing and evaluating a five minute phishing awareness video. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 11033 LNCS*, 119-134. https://doi.org/10.1007/978-3-319-98385-1_9

Wang, Y.-J., Tseng, S.-S., Yang, T.-Y., & Weng, J.-F. (2018). Building a frame-based cyber security learning game. *Communications in Computer and Information Science*, *797*, 32-41. https://doi.org/10.1007/978-981-10-7850-7_4

Wash, R., & Cooper, M. M. (2018). Who provides phishing training? Facts, stories, and people like me. *Conference on Human Factors in Computing Systems - Proceedings*, *2018-April*. https://doi.org/10.1145/3173574.3174066

Weaver, B. W., Braly, A. M., & Lane, D. M. (2021). Training Users to Identify Phishing Emails. *Journal of Educational Computing Research*, *59*(6), 1169-1183. https://doi.org/10.1177/0735633121992516

Wen, Z. A., Lin, Z., Chen, R., & Andersen, E. (2019). What.Hack: Engaging Anti-Phishing Training through a Role-playing Phishing Simulation Game. *Conference on Human Factors in Computing Systems - Proceedings*. https://doi.org/10.1145/3290605.3300338

Wolf, S., Burrows, A. C., Borowczak, M., Johnson, M., Cooley, R., & Mogenson, K. (2020). Integrated outreach: Increasing engagement in computer science and cybersecurity. *Education Sciences*, *10*(12), 1-23. https://doi.org/10.3390/educsci10120353

Wolf, S., Cooley, R., Johnson, M., Burrows, A. C., & Borowczak, M. (2020). Constructing and refining engaging computer science outreach. *ASEE Annual Conference and Exposition, Conference Proceedings*, *2020-June*. Recuperado de https://www.scopus.com/inward/record.uri?eid=2-s2.0-85095780473&partnerID=40&md5=05052e69cca875c069c9f7b96122cb68

Yett, B., Hutchins, N., Stein, G., Zare, H., Snyder, C., Biswas, G., Metelko, M., & Ledeczi, A. (2020). A hands-on cybersecurity curriculum using a robotics platform. SIGCSE 2020 - Proceedings of the 51st ACM Technical Symposium on Computer Science Education, 1040-1046. https://doi.org/10.1145/3328778.3366878

Zhang-Kennedy, L., Chiasson, S., & Biddle, R. (2016). The role of instructional design in persuasion: A comics approach for improving cybersecurity. *International Journal of Human-Computer Interaction*, *32*(3), 215-257. APA PsycInfo®. https://doi.org/10.1080/10447318.2016.1136177

Zhang-Kennedy, L., & Chiasson, S. (2021). A Systematic Review of Multimedia Tools for Cybersecurity Awareness and Education. *ACM Computing Surveys*, 54(1), 1–39. https://doi.org/10.1145/3427920

Zielinska, O. A., Tembe, R., Hong, K. W., Ge, X., Murphy-Hill, E., & Mayhorn, C. B. (2014). One phish, two phish, how to avoid the internet phish: Analysis of training strategies to detect phishing emails. *Proceedings of the Human Factors and Ergonomics Society*, *2014-January*, 1466-1470. https://doi.org/10.1177/1541931214581306

ANEXOS

Tabla de codificación con cita completa.

	TITULO	PRIMER AUTOR Y AÑO	REVISTA	PAÍS
1	A comprehensive cybersecurity learning platform for elementary education	Giannakas, F. 2019	Information Security Journal	GRECIA
2	A cyber security culture fostering campaign through the lens of active audience theory	Reid, R. 2015	Proceedings of the 9th International Symposium on Human Aspects of Information Security and Assurance	GRECIA
3	A Cybersecurity Awareness Escape Room using Gamification Design Principles	Decusatis, C. 2022	2022 IEEE 12th Annual Computing and Communication Workshop and Conference	ESTADOS UNIDOS
4	A cybersecurity camp for girls	Cornel, C. 2016	ASEE Annual Conference and Exposition	ESTADOS UNIDOS
5	A hands-on cybersecurity curriculum using a robotics platform	Yett, B. 2020	SIGCSE 2020 - Proceedings of the 51st ACM Technical Symposium on Computer Science Education	ESTADOS UNIDOS
6	A New Email Phishing Training Website	Al-Hamar, Y. 2020	Proceedings - International Conference on Developments in eSystems Engineering	REINO UNIDO
7	A Novel Visual-Privacy Themed Experiential- Learning Tool for Human-Privacy Societal-Security Awareness in Middle-School and High-School Youth	Chattopadhyay, A. 2019	Proceedings - Frontiers in Education Conference	ESTADOS UNIDOS
8	A password generator tool to increase users' awareness on bad password construction strategies	Tsokkis, P. 2018	2018 International Symposium on Networks	CHIPRE
9	A Proposal and the Evaluation of a Hands-On Training System for Cyber Security	Saito, T. 2019	ADVANCES ON BROADBAND AND WIRELESS COMPUTING	JAPON
10	A real world study on employees' susceptibility to phishing attacks	De Bona, M. 2020	ACM International Conference Proceeding Series	ESTADOS UNIDOS
11	"A University's Developmental Framework: Creating, Implementing, and			
12	Evaluating a K-12 Teacher Cybersecurity Micro-credential Course"	Mugayitoglu, B. 2021	implementing	ESTADOS UNIDOS
13	Activity simulation for experiential learning in cybersecurity workforce development	Burris, J. 2018	Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)	ESTADOS UNIDOS
14	An Examination of Gain- and Loss-Framed Messaging on Smart Home Security Training Programs	Plachkinova, M. 2019	Information Systems Frontiers	PAISES BAJOS
15	An investigation of phishing awareness and education over time: When and how to best remind users	Reinheimer, B. 2020	Proceedings of the 16th Symposium on Usable Privacy and Security	AUSTRALIA
16	An Observational Study of Peer Learning for High School Students at a Cybersecurity Camp	Pittman, J.M. 2016	Information Systems Education Journal	ESTADOS UNIDOS
17	Anti-Phishing Phil: The design and evaluation of a game that teaches people not to fall for phish	Sheng, S. 2007	ACM International Conference Proceeding Series	ESTADOS UNIDOS
18	BEHAVIORAL ANALYSIS AS A MEANS TO PREVENT SOCIAL ENGINEERING AND PHISHING	Alencar, G.D. 2013	RESI Revista Electronica de Sistemas de Informacao	BRASIL
19	Building a frame-based cyber security learning game	Wang, Y.-J. 2018	Communications in Computer and Information Science	ALEMANIA
20	Constructing and refining engaging computer science outreach	Wolf, S. 2020	ASEE Annual Conference and Exposition	ESTADOS UNIDOS
21	Cyber Securing the Future	Kolb, C. 2022	AIP Conference Proceedings	ESTADOS UNIDOS
22	Cyber Security Awareness Game (CSAG) for Secondary School Students	Shen, L.W. 2021	2021 International Conference on Data Science and Its Applications	ESTADOS UNIDOS
23	CyberAware: A mobile game-based app for cybersecurity education and awareness	Giannakas, F. 2015	Proceedings of 2015 International Conference on Interactive Mobile Communication Technologies and Learning	ESTADOS UNIDOS
24	Cyber-Hero: A Gamification framework for Cyber Security Awareness for High Schools Students	Qusa, H. 2021	2021 IEEE 11th Annual Computing and Communication Workshop and Conference	ESTADOS UNIDOS

	TITULO	PRIMER AUTOR Y AÑO	REVISTA	PAÍS
25	Cybersecurity Interventions for Teens: Two Time-Based Approaches	Amo, Laura C. 2019	IEEE Transactions on Education	ESTADOS UNIDOS
26	CyberVR: An Interactive Learning Experience in Virtual Reality for Cybersecurity Related Issues	Veneruso, S.V. 2020	ACM International Conference Proceeding Series	ESTADOS UNIDOS
27	Design and evaluation of a cybersecurity awareness training game	Huynh, D. 2017	Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)	ALEMANIA
28	Design and evaluation of an augmented reality game for cybersecurity awareness (CybAR)	Alqahtani, H. 2020	Information (Switzerland)	SUIZA
29	Design of Phishing Simulation Dashboard Using Analytic Data Concepts	Septiana, R. 2020	Journal of Physics: Conference Series	REINO UNIDO
30	Design of Security Training System for Individual Users	Lim, I. 2016	Wireless Personal Communications	PAISES BAJOS
31	Design, Development, and Evaluation of a Cybersecurity, Privacy, and Digital Literacy Game for Tweens	Maqsood, S. 2021	ACM Transactions on Privacy and Security	ESTADOS UNIDOS
32	Designing an Interactive Game for Preventing Online Abuse in Namibia	Mikka-Muntuumo, J. 2021	2021 3rd International Multidisciplinary Information Technology and Engineering Conference	ESTADOS UNIDOS
33	Developing and evaluating a five minute phishing awareness video	Volkamer, M. 2018	Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)	ESTADOS UNIDOS
34	Education in the 'virtual' community: Can beating Malware Man teach users about social networking security?	Sercombe, A.A. 2012	Proceedings of the 6th International Symposium on Human Aspects of Information Security and Assurance	ESTADOS UNIDOS
35	Educational games for cybersecurity awareness	Sookhanaphibarn, K. 2020	2020 IEEE 9th Global Conference on Consumer Electronics	ESTADOS UNIDOS
36	Effectiveness of and user preferences for security awareness training methodologies.	Tschakert, K.F. 2019	Heliyon	PAISES BAJOS
37	Effects of integrating dynamic concept maps with Interactive Response System on elementary school students' motivation and learning outcome: The case of anti-phishing education	Sun, J.C. 2016	COMPUTERS & EDUCATION	REINO UNIDO
38	Empirical benefits of training to phishing susceptibility	Dodge, R. 2012	IFIP Advances in Information and Communication Technology	ESTADOS UNIDOS
39	Enhancing cybersecurity learning through an augmented reality-based serious game	Salazar, M. 2013	IEEE Global Engineering Education Conference	ESTADOS UNIDOS
40	Escaping to cybersecurity education: Using manipulative challenges to engage and educate	Streiff, J. 2019	Proceedings of the European Conference on Games-based Learning	ALEMANIA
41	Faheem: Explaining URLs to people using a Slack bot	Althobaiti, K. 2018	Proceedings of AISB Annual Convention 2018	REINO UNIDO
42	Fishing for phishers. Improving Internet users' sensitivity to visual deception cues to prevent electronic fraud	Moreno-Fernández, M. 2017	Computers in Human Behavior	REINO UNIDO
43	Forcing Johnny to login safely: Long-term user study of forcing and training login mechanisms	Herzberg, A. 2011	Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)	ALEMANIA
44	Game based cybersecurity training for High School Students	Jin, G. 2018	SIGCSE 2018 - Proceedings of the 49th ACM Technical Symposium on Computer Science Education	ESTADOS UNIDOS
45	Gamification Techniques for Raising Cyber Security Awareness	Scholefield, S. 2019	Lecture Notes in Computer Science	ALEMANIA
46	Getting users to pay attention to anti-phishing education: Evaluation of retention and transfer	Kumaraguru, P. 2007	ACM International Conference Proceeding Series	ESTADOS UNIDOS
47	Hacked time: Design and evaluation of a self-efficacy based cybersecurity game	Chen, T. 2020	DIS 2020 - Proceedings of the 2020 ACM Designing Interactive Systems Conference	PAISES BAJOS
48	HATCH: Hack and trick capricious humans – A serious game on social engineering	Beckers, K. 2016	Proceedings of the 30th International BCS Human Computer Interaction Conference	ESTADOS UNIDOS
49	How Do Children Interact with Phishing Attacks?	Alwanain, M. 2021	INTERNATIONAL JOURNAL OF COMPUTER SCIENCE AND NETWORK SECURITY	CHINA
50	How effective is anti-phishing training for children?	Lastdrager, E. 2019	Proceedings of the 13th Symposium on Usable Privacy and Security	ESTADOS UNIDOS

	TITULO	PRIMER AUTOR Y AÑO	REVISTA	PAÍS
51	Human risk factors in cybersecurity	Cuchta, T. 2019	SIGITE 2019 - Proceedings of the 20th Annual Conference on Information Technology Education	ESTADOS UNIDOS
52	Impact of information security training on recognition of phishing attacks: A case study of vilnius gediminas technical university	Rastenis, J. 2020	Communications in Computer and Information Science	ALEMANIA
53	Informing, simulating experience, or both A field experiment on phishing risks	Baillon, A. 2019	PLoS ONE	ESTADOS UNIDOS
54	Integrated outreach: Increasing engagement in computer science and cybersecurity	Wolf, S. 2020	Education Sciences	SUIZA
55	It won't happen to me: Promoting secure behaviour among internet users	Davinson, N. 2010	Computers in Human Behavior	REINO UNIDO
56	Lessons from a real world evaluation of anti-phishing training	Kumaraguru, P. 2008	eCrime Researchers Summit	ESTADOS UNIDOS
57	NoPhish: Evaluation of a web application that teaches people being aware of phishing attacks	Kunz, A. 2016	Lecture Notes in Informatics (LNI)	ALEMANIA
58	One phish, two phish, how to avoid the internet phish Analysis of training strategies to detect phishing emails	Zielinska, O.A. 2014	Proceedings of the human factors and ergonomics Society	ESTADOS UNIDOS
59	Online Cybersecurity Awareness Modules for College and High School Students	Peker, Y.K. 2018	2018 national cyber summit research track	ESTADOS UNIDOS
60	Phishing Academy: Evaluation of a Digital Educational Game on URLs and Phishing	Schoebel, S. 2021	Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)	ALEMANIA
61	Phishing Awareness and Elderly Users in Social Media	Alwanain, M. 2020	INTERNATIONAL JOURNAL OF COMPUTER SCIENCE AND NETWORK SECURITY	CHINA
62	Phishy - A serious game to train enterprise users on phishing awareness	Gokul, C.J. 2018	CHI PLAY 2018 - Proceedings of the 2018 Annual Symposium on Computer-Human Interaction in Play Companion Extended Abstracts	ESTADOS UNIDOS
63	Playing safe: A prototype game for raising awareness of social engineering	Newbould, M. 2009	Proceedings of the 7th Australian Information Security Management Conference	AUSTRALIA
64	POMEGA: Security game for building security awareness	Visoottiviseth, V. 2018	Proceeding of 2018 7th ICT International Student Project Conference	ESTADOS UNIDOS
65	Protecting people from phishing: The design and evaluation of an embedded training email system	Kumaraguru, P. 2007	Conference on Human Factors in Computing Systems - Proceedings	ESTADOS UNIDOS
66	Safe Internet: An Edutainment Tool for Teenagers	Neo, H.F. 2021	Lecture Notes in Electrical Engineering	ALEMANIA
67	Safe: Cryptographic Algorithms and Security Principles Gamification	Kaabi, L.A. 2022	IEEE Global Engineering Education Conference	ESTADOS UNIDOS
68	SAWIT—Security Awareness Improvement Tool in the Workplace	Kovačević, A. 2020	Applied Sciences	SUIZA
69	School of phish: A real-world evaluation of anti-phishing training	Kumaraguru, P. 2009	SOUPS 2009 - Proceedings of the 5th Symposium On Usable Privacy and Security	ESTADOS UNIDOS
70	Security education and awareness for K-6 going mobile	Giannakas, F. 2016	International Journal of Interactive Mobile Technologies	ESTADOS UNIDOS
70	SecurityEmpire: Development and evaluation of a digital game to promote cybersecurity education	Olano, M. 2014	2014 USENIX Summit on Gaming	ESTADOS UNIDOS
72	Smartphone Security and Privacy – A Gamified Persuasive Approach with Protection Motivation Theory	Ganesh, A. 2022	Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)	ALEMANIA
73	Smells Phishy?: An educational game about online phishing scams	Baslyman, M. 2016	eCrime Researchers Summit	ESTADOS UNIDOS
74	Snakes and ladders for digital natives: information security education for the youth	Reid, R. 2014	Information Management & Computer Security	REINO UNIDO
75	Spotlight on Phishing: A Longitudinal Study on Phishing Awareness Trainings	Quinkert, F. 2021	Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)	ALEMANIA
76	The role of instructional design in persuasion: A comics approach for improving cybersecurity	Zhang-Kennedy, L. 2016	International Journal of Human-Computer Interaction	ESTADOS UNIDOS

	TITULO	PRIMER AUTOR Y AÑO	REVISTA	PAÍS
77	Training Users to Identify Phishing Emails	Weaver, B.W. 2021	Journal of Educational Computing Research	ESTADOS UNIDOS
78	Using Design-Science Based Gamification to Improve Organizational Security Training and Compliance: JMIS	Silic, M. 2020	Journal of Management Information Systems	ESTADOS UNIDOS
79	What.Hack: Engaging Anti-Phishing Training through a Role-playing Phishing Simulation Game	Wen, Z.A. 2019	Conference on Human Factors in Computing Systems - Proceedings	ESTADOS UNIDOS

Tabla de clasificación de artículos y efectos conseguidos

	TÉCNICA	EFECTOS	TIPO EDUCACIÓN	POBLACIÓN DIANA/ INTERVALO DE EDAD	ÁREA DE ESTUDIO DE LOS AUTORES
1	GAMIFICACIÓN	2 (81% mejora)	CIBERSEGURIDAD	Niños (Estudiantes de Primaria 9-12)	TIC (Ingeniería de Sistemas)
2	MEDIOS AUDIOVISUALES	2	CIBERSEGURIDAD	Niños	TIC
3	GAMIFICACIÓN / SCAPE ROOM	1	CIBERSEGURIDAD	Jóvenes (Estudiantes preunivesitarios y Universitarios)	TIC
4	CAMPAMENTO DE CIBERSEGURIDAD	1 (44% mejora)	CIBERSEGURIDAD	Niños; Adolescentes (10-14)	TIC
5	PLATAFORMA ROBOTICA	1 (33% mejora)	CIBERSEGURIDAD	Adolescentes (Estudiantes de secundaria)	TIC (Ingeniería de Ciencias Computacionales)
6	MATERIALES AUDIOVISUALES	1 (98% mejora)	CIBERSEGURIDAD	Adultos (Empleados de organizaciones)	TIC (Ciencias Computacionales)
7	MATERIALES AUDIOVISUALES / PRÁCTICAS CON HERRAMIENTA WEB	1	CIBERSEGURIDAD	Niños; Adolescentes. (12- 18)	TIC (Ciencias de la Información y Computación)
8	SIMULADOR	1 (80%)	CIBERSEGURIDAD	Adultos (23-55)	TIC (Ciencias Computacionales)
9	EJERCICIOS PRÁCTICOS DE ENTRENAMIENTO (HERRAMIENTA VIRTUAL)	1 (49%)	CIBERSEGURIDAD	Adolescentes; Estudiantes de Secundaria (12-16)	TIC (Ciencias Computacionales)
10	SIMULACIÓN	5 (1%)	CIBERSEGURIDAD	Adultos; Empleados de organizaciones	TIC (Ciencias Computacionales)
11	MULTIMÉTODO: Sistema de gestión de aprendizaje (LMS): Materiales audiovisuales; Elearning	1	CIBERSEGURIDAD	Adultos (Profesores de Primaria)	Educación ; TIC (Ciencias Computacionales)
12	SIMULACIÓN	2: 54% Simulación frente a 30% Grupo Control (educación tradicional)	CIBERSEGURIDAD / CIBERDELINCUENCIA	Adultos	TIC (Ciencias Computacionales)
13	MATERIALES AUDIOVISUALES	1	CIBERSEGURIDAD	Adultos	TIC (Informática y Gestión de Tecnologías)
14	Multimétodo: material de texto 1,61; material audiovisual 1,8; Herramienta interactiva 1,73;	1	CIBERSEGURIDAD/ CIBERDELINCUENCIA	Adultos	TIC (Informática Aplicada)

	TÉCNICA	EFECTOS	TIPO EDUCACIÓN	POBLACIÓN DIANA/ INTERVALO DE EDAD	ÁREA DE ESTUDIO DE LOS AUTORES
15	CAMPAMENTO DE CIBERSEGURIDAD / APRENDIZAJE ENTRE PARES	1	CIBERSEGURIDAD	Adolescentes; Alumnos de Secundaria	TIC
16	GAMIFICACIÓN	2: 18% mejora pre-post test; Tasa de error del 0,34 a 0,17 sobre 5;	CIBERSEGURIDAD	Jóvenes (18-34)	TIC
17	Multimétodo: Clase expositiva; material audiovisual	2: Phishing en grupo experimental 108 frente a 174 grupo control	CIBERSEGURIDAD / CIBERDELINCUENCIA	Adultos (Trabajadores de empresa)	TIC (Ciencias Computacionales)
18	Juego de Cartas	1	CIBERSEGURIDAD / CIBERDELINCUENCIA	Niños	TIC (Ciencias Computacionales e Ingeniería de la información ; Informática Aplicada y Multimedia)
19	Mixto: Clase expositiva; tallers grupales; laboratorio.	1	CIBERSEGURIDAD	Niños; Adolescentes (12-16)	TIC (Ciencias Computacionales) ; Ciencias de la Educación
20	Clases prácticas	6 Clases prácticas 30% a 87%; Grupo control (solo lectura) 30% a 91%	CIBERSEGURIDAD / CIBERDELINCUENCIA	Adolescentes	TIC
21	GAMIFICACIÓN	1 70%	CIBERSEGURIDAD/ CIBERDELINCUENCIA	Adolescentes	TIC (Ciencias Computacionales; Ingeniería; Matemáticas)
22	GAMIFICACIÓN (Juego para el movil)	1 (15%+33% /2 =24%)	CIBERSEGURIDAD	Niños (9-11)	TIC (Ingeniería de Sistemas de Información y Comunicación)
23	GAMIFICACIÓN	5 (5%)	CIBERSEGURIDAD	Niños; Adolescentes; Jóvenes (9-22)	TIC (Ciencias Computacionales)
24	Taller de aprendizaje práctico (hands-on learning workshop)	1	CIBERSEGURIDAD	Adolescentes; Jóvenes	TIC (Gestión de Sistemas; Ingeniería Computacional)
25	GAMIFICACIÓN	2 Grupo tratamiento (Gamificación) frente a Grupo control	CIBERSEGURIDAD	Jóvenes (24-34)	TIC (Informática; Ciencias Computacionales;
26	GAMIFICACIÓN	1 (76%)	CIBERSEGURIDAD / CIBERDELINCUENCIA	Jóvenes	TIC (Ciencias Computacionales)
27	GAMIFICACIÓN	1 (4/5 = 80%)	CIBERSEGURIDAD / CIBERDELINCUENCIA	Adultos (18-65)	TIC (Ciencias Computacionales)
28	SIMULACIÓN	1 (clics en phishin 43% a 16% = mejora del 27%)	CIBERSEGURIDAD	Adultos (Empleados de organizaciones)	TIC (Ciencias Computacionales)
29	SIMULACIÓN	1 (mejora de entre un 12 y un 14%)	CIBERSEGURIDAD	Adultos	TIC (Ciencias Computacionales)
30	GAMIFICACIÓN	1 (70% - 80%)	CIBERSEGURIDAD	Niños (11 - 13 años)	TIC (Ciencias Computacionales)
31	GAMIFICACIÓN	1 (80%)	CIBERSEGURIDAD	Niños; Jóvenes; Adultos (7 a 35)	TIC (Ciencias Computacionales)
32	MEDIOS AUDIOVISUALES (VÍDEO EDUCATIVO)	1 (37%)	CIBERSEGURIDAD	Adultos (media de edad: 37 años)	TIC (Ciencias Computacionales)
33	GAMIFICACIÓN	2 (Grupo tratamiento 77% ; 55% Grupo control)	CIBERSEGURIDAD	Jóvenes; Adultos. (18-65)	TIC (Ciencias Computacionales)
34	GAMIFICACIÓN	1 (75%)	CIBERSEGURIDAD	Adolescentes; Jóvenes	TIC (Ciencias Computacionales)
35	Mixto: GAMIFICACIÓN; MATERIALES MULTIMEDIA; TEXTO	1 (8%)	CIBERSEGURIDAD	Jóvenes (18-23)	TIC (Información y Comunicación)
36	Mapas conceptuales	"2 grupo de control	CIBERSEGURIDAD	Niños; Adolescentes	Educación

	TÉCNICA	EFECTOS	TIPO EDUCACIÓN	POBLACIÓN DIANA/ INTERVALO DE EDAD	ÁREA DE ESTUDIO DE LOS AUTORES
37	Entrenamiento	2 (18% frente a grupo control)	CIBERSEGURIDAD	No se especifica	TIC (Ciencias Computacionales); Ciencias del comportamiento
38	GAMIFICACIÓN	1 (3,92/5 = 78%)	CIBERSEGURIDAD/ CIBERDELINCUENCIA	Adolescentes; Jóvenes (14-19)	TIC (Ingeniería Informática y Telecomunicaciones;
39	ESCAPE ROOM	1	CIBERSEGURIDAD	Niños; Adolescentes	TIC (Ciencias Computacionales)
40	ROBOT	2 (G intervención M=4.55 G.Control M=2.15)	CIBERSEGURIDAD	Jóvenes; Adultos	TIC (Ciencias Computacionales; Informática)
41	Entrenamiento progresivo	1	CIBERSEGURIDAD	Jóvenes; Adultos (18-66)	Psicología; TIC (Informática)
42	Marcador de inicio de sesión +Imágenes	2 (Grupo tratamiento 82% ; G. Control 20%)	CIBERSEGURIDAD/ CIBERDELINCUENCIA	Estudiantes	TIC (Ciencias Computacionales)
43	Campamento de ciberseguridad	1	CIBERSEGURIDAD	Adolescentes	TIC (Ciencias Computacionales; Informática; Tecnologías de Gráficos por Ordenador)
44	GAMIFICACIÓN	1	CIBERSEGURIDAD / CIBERDELINCUENCIA	Adolescentes; Jóvenes	TIC (Informática)
45	FORMACIÓN INTEGRADA (Embedded training)	2 (G. intervención mejora 67% ; G. control 0%)	CIBERSEGURIDAD	Jóvenes; Adultos (media edad 25)	TIC (Ciencias Computacionales)
46	GAMIFICACIÓN	2	CIBERSEGURIDAD	Jóvenes; Adultos	TIC (Ciencias Computacionales)
47	GAMIFICACIÓN	1 (50% - 100% ; Media 75%)	CIBERSEGURIDAD / CIBERDELINCUENCIA	Empleados (generales) de organizaciones	TIC (Informática) ; Económicas.
48	Entrenamiento	2 (Capacidad de identificar Phishing); 6 (concienciación)	CIBERSEGURIDAD / CIBERDELINCUENCIA	Niños (7-13)	TIC (Ciencias Computacionales)
49	Entrenamiento	2 (14% frente a grupo control)	CIBERSEGURIDAD / CIBERDELINCUENCIA	Niños (8-13)	TIC (Ciencias Computacionales)
50	GAMIFICACIÓN	2	CIBERSEGURIDAD / CIBERDELINCUENCIA	Jóvenes	TIC (Ciencias Computacionales); Matemáticas
51	Entrenamiento	1	CIBERSEGURIDAD / CIBERDELINCUENCIA	Adultos (empleados de organizaciones)	Económicas; TIC (Informática)
52	Educación tradicional (información) ; Simulación	Educación Tradicional: 6 (4 % de mejora frente a grupo control); Simulación: 2 (12% de mejora frente a grupo control)	CIBERSEGURIDAD / CIBERDELINCUENCIA	Jóvenes; Adultos	
53	CAMPAMENTO DE CIBERSEGURIDAD	1 (63%; 47%. Media 55%)	CIBERSEGURIDAD / CIBERDELINCUENCIA	Niños; Adolescentes (10-18)	TIC (Ciencias Computacionales); Educación
54	Entrenamiento	5	CIBERSEGURIDAD	jovenes; Adultos (18-43)	Psicología
55	Entrenamiento integrado	2 (28%)	CIBERSEGURIDAD	Empleados (generales) de organizaciones	TIC (Ciencias Computacionales)
56	GAMIFICACIÓN	1 (20%)	CIBERSEGURIDAD	Jóvenes; Adultos (18-56)	TIC (Ciencias Computacionales)
57	Entrenamiento	6	CIBERSEGURIDAD	Jóvenes; Adultos (19-67)	Psicología; Interación Humana-Computacional
58	E-Learning	1 (58%)	CIBERSEGURIDAD/ CIBERDELINCUENCIA	Adolescentes; Jóvenes; Adultos (13-63)	Psicología; Ciencias Computacionales
59	Gamificación	1 (12%)	CIBERSEGURIDAD	Niños; Adolescentes	TIC (Informática)
60	Entrenamiento	2 (50%)	CIBERSEGURIDAD	Tercera edad (65 - 75)	TIC (Ciencias Computacionales)
61	GAMIFICACIÓN	1 (29%)	CIBERSEGURIDAD	Jóvenes, Adultos	TIC (Ciencias Computacionales)
62	GAMIFICACIÓN	1	CIBERSEGURIDAD	Adolescentes; Jóvenes; Adultos	TIC (Ciencias Computacionales)
63	GAMIFICACIÓN	1	CIBERSEGURIDAD	Adolescentes; Jóvenes (15-23)	TIC (Tecnologías de la Información y Comunicación; Ingeniería Software)

	TÉCNICA	EFECTOS	TIPO EDUCACIÓN	POBLACIÓN DIANA/ INTERVALO DE EDAD	ÁREA DE ESTUDIO DE LOS AUTORES
64	Entrenamiento Integrado	2	CIBERSEGURIDAD	Jóvenes; Adultos	TIC (Ciencias Computacionales)
65	GAMIFICACIÓN	1 (76%)	CIBERSEGURIDAD /CIBERDELINCUENCIA	Niños; Adolescentes. (11-22)	TIC (Ciencias Computacionales)
66	GAMIFICACIÓN	2 (20%)	CIBERSEGURIDAD / CIBERDELINCUENCIA	NO CONSTA	TIC(Sistemas de Información y Seguridad)
67	Aprendizaje colaborativo (Collaborative learning)	1 (82%)	CIBERSEGURIDAD /CIBERDELINCUENCIA	Jóvenes; Adultos. (Empleados de empresas)	TIC (Ingeniería Software; Tecnologías de la Información en Finanzas)
68	GAMIFICACIÓN	2 (27% - 32%)	CIBERSEGURIDAD	Jóvenes; Adultos	TIC (Ciencias Computacionales)
69	GAMIFICACION	1 (24%)	CIBERSEGURIDAD /CIBERDELINCUENCIA	Niños (9-11)	TIC (Ingeniería de Sistemas de Información y Comunicación) ; Matemáticas
70	GAMIFICACION	1	CIBERSEGURIDAD	Adolescentes; Jóvenes	TIC (Ciencias Computacionales)
70	GAMIFICACION	2 (72% grupo tratamiento; 14% G. control)	CIBERSEGURIDAD	no consta	TIC (Ciencias Computacionales)
72	GAMIFICACIÓN	1	CIBERSEGURIDAD / CIBERDELINCUENCIA	Jóvenes (24-44)	TIC (Ciencias Computacionales)
73	GAMIFICACIÓN	1 (35%)	CIBERSEGURIDAD	Niños; Adolescentes (9-14)	TIC (Ciencias Computacionales)
74	SIMULACIÓN (entrenamiento)	1 (9%)	CIBERSEGURIDAD	Jóvenes; Adultos (empleados)	TIC (Ciencias Computacionales)
75	COMIC	1 (42%)	CIBERSEGURIDAD /CIBERDELINCUENCIA	Jóvenes (20-30)	TIC (Ciencias Computacionales)
76	Entrenamiento	2 (28%Grupo tratamiento; 12% g.control)	CIBERSEGURIDAD	Jóvenes (18-23)	Ciencias Sociales (Psicologia)
77	GAMIFICACIÓN	2	CIBERSEGURIDAD	Jóvenes; Adultos (empleados de organizaciones)	TIC (Tecnologías de la Información)
78	GAMIFICACIÓN; SIMULACIÓN ROLE-PLAYING	1 (37%)	CIBERSEGURIDAD	Jóvenes	TIC (Ciencias computacionales)
79	Lectura de Consejos y Relatos	2 (21% frente a grupo control)	CIBERSEGURIDAD /CIBERDELINCUENCIA	Población general	Medios e información; Seguridad de la información