Congreso In-Red 2022
UPV, 6 - 8 de julio de 2022
Doi: https://doi.org/10.4995/INRED2022.2022.15855

Ciberseguridad y educación. Variables de sensibilidad y cambio en la formación del profesorado.

Cybersecurity and education. Sensibility and change variables in teaching training educators.

Javier Herrero-Martín[a], Cristina Rodríguez-Merino[b], Rosario Valdivielso Alba[c], Daniel Amo-*Filva*[c]

[a]Departamento de Educación Infantil y Primaria. Facultad de Educación. Centro Superior de Estudios Universitarios La Salle (Universidad Autónoma de Madrid). Madrid, Spain. j.herrero@lasallecampus.es[a] ,: r.valdivielso@lasallecampus.es[c] CALPA La Salle. Facultad de Educación. Centro Superior Universitario La Salle (Universidad Autónoma de Madrid). crodriguez@lasallecampus.es[b] Departamento de Ingeniería. GRETEL-Group of Research on Technology Enhanded Learning. La Salle/Universidad Ramón Llull. Barcelona, Spain. daniel.amo@salle.url.edu[d] .

How to cite: Javier Herrero-Martín, Cristina Rodríguez-Merino, Rosario Valdivielso Alba, Daniel Amo-*Filva*. 2022. Ciberseguridad y educación. Variables de sensibilidad y cambio en la formación del profesorado. En libro de actas: *VIII Congreso de Innovación Educativa y Docencia en Red.* Valencia, 6 - 8 de julio de 2022. https://doi.org/10.4995/INRED2022.2022.15855

Abstract

The present study is aimed to analyze the change in university teacher training based on emergent needs to consider cybersecurity as a specific and complementary content. The study involved first course students of the Teacher Training degrees in Early Childhood Education and Primary Education. The research design followed a mixed sequential and concurrent model, using a GLM-RM procedure for the quantitative data-analysis, by means of pre-post contrast during the training; also, a semantic network analysis was used for quantitative data. The results point to two fundamental clues. On the one hand, an increase in sensitivity to risk perception as a consequence of specific training in cybersecurity and, second, the identification of two contrasting groups of perception of change.

Keywords: *cybersecurity, education, risk, digital awareness, magisterial.*

Resumen

Se presenta un estudio de análisis del cambio en la formación del profesorado universitario a partir de la necesidad de considerar la ciberseguridad como un contenido específico y complementario. En el estudio participaron estudiantes de primer curso de las enseñanzas de Magisterio en Educación Infantil y Educación Primaria. El diseño de investigación siguió un modelo mixto secuencial y concurrente, utilizando para el analisis cuantitativo de los datos un procedimiento MLG-MR, mediante contraste pre-post durante la formación y en la capa cualitativa mediante un análisis de redes semánticas. Los resultados apuntan a dos

claves fundamentales. Por un lado, un aumento de la sensibilidad en la percepción del riesgo como consecuencia de la formación específica en ciberseguridad y, por otro, la identificación de dos grupos contrastados de percepción al cambio.

1. Introducción

La era digital ha traído una nueva forma de reconocer el mundo (Verhoef et al., 2021). La vida, proyectada a nivel meta representacional sobre lo cotidiano, se transforma en un continuo mixto, entre lo real y físico y lo virtual e imaginable, sobre el que el ser humano ha de desenvolverse, más o menos adaptativamente.

Que los dispositivos digitales y la tecnología aportan este valor, no es nada nuevo. El problema, sin embargo, emerge en el momento en que se considera el papel de la tecnología en el desarrollo humano, el aprendizaje y la manifestación de la conducta (Gonzalez-Sanmamed et al., 2020), individual o colectiva. Es entonces donde el sentido de garantía sobre el *uso* y sus consecuencias negativas, el *abuso*, se manifiestan de manera relevante (García-Umaña & Tirado-Morueta, 2018; Rahayu et al., 2020)).

La manera en que los humanos hacen uso de los soportes digitales delimita el marco de relación en un ecosistema social de aprendizaje, hasta el punto de trascender su conciencia mental para proyectarla sobre entornos virtuales inmersivos (Dzardanova et al., 2018) e, incluso, adictivos (Bağci, 2019). Es entonces cuando el desdoblamiento representacional concede rangos de libertad de pensamiento y acción paralelos y compatibles entre sí.

Es en este contexto donde se producen, o se pueden producir, transgresiones de los límites en virtud de múltiples causas y orígenes (Tayouri, 2015). La seguridad en el uso de los dispositivos tecnológicos y los desarrollos digitales se condiciona, entonces, a la forma canónica en que los sujetos deberían hacer un uso racional y socialmente aceptable (además de normativo y prescriptivo), para alcanzar algún tipo de beneficio individual o colectivo (Alzighaibi, 2021).

En educación, una pieza clave respecto al uso del contenido y del soporte digital es la modelización del patrón de interacción entre la persona y la máquina (HCI, human-computer interaction) (Richardson et al., 2020). En el discurso pedagógico, se hace necesaria la observación constante sobre los límites y los riesgos, tanto presentes como potenciales, desde muy temprano, que relacionan la función social y comunicativa de las redes y los soportes digitales con la contextualización ética y oral derivada de un adecuado modelo de interacción (Pangrazio & Cardozo-Gaibisso, 2020). Así, dado que el avance tecnológico sigue un curso vertiginoso, el aseguramiento constante de las garantías de uso se convierte en una constante permanente.

El profesorado es un colectivo de especial interés en este encuadre (Gallego-Arrufat et al., 2019), dado su papel mediador fundamental en la construcción del perfil adecuado a la representación social positiva del uso tecnológico (Tomczyk, 2019). En la actualidad, sin embargo, los planes de estudio formales en la formación de profesores, independientemente de la etapa, no cuentan con formación específica relativa a la relación entre ciberseguridad y educación. Estudios previos han puesto de manifiesto la transformación en la percepción de los riesgos cuando se establece un contexto de reflexión alrededor de los usos tecnológicos (Wolf et al., 2020), incluso, a pesar de la disposición de una cierta conciencia del riesgo (Zwilling et al., 2022; Amankwa, 2021).

2. Objetivos

- Posibilitar el acceso a la consideración del uso digital como instrumento educativo.
- Fomentar un uso responsable y seguro de las redes sociales, que permita balancear adecuadamente ocio, conocimiento y privaciad.

La actual investigación se centra en la percepción que tienen los estudiantes de Magisterio en formación tanto de la conciencia de uso como de los riesgos derivados de las prácticas digitales en internet (sociales, informativas, comerciales, etc.). Este planteamiento está en línea con la consideración de que una ciudadanía digital adecuada se corresponde con un uso tecnológico digital, que incorpora elementos propios y definitorios, como *huella*, *privacidad* o *identidad* digitales (Martin et al., 2019), más aún cuando la *vigilancia de datos* se ha convertido en objeto de atención fundamental en el contexto educativo (Alier et al., 2021). Considerando como tal, que la formación de este tipo de perfiles deber aunar, al mismo tiempo, la reflexión sobre la cuestión curricular, en sí misma, para la inclusión de contenidos sobre ciberseguridad, y la modelización de la conducta, en cuanto a la visibilizarían del perfil mediador y referente del educador para con los niños y jóvenes en las primeras etapas de escolarización.

3. Desarrollo de la innovación

El Nuevo Contexto de Aprendizaje (NCA) es una propuesta global de transformación metodológica, desarrollada en el seno de la Institución La Salle, a nivel estatal (Herrero-Martín et al., 2020). Su horizonte abarca el desarrollo y despliegue del nuevo modelo pedagógico en todas las etapas educativas, incluyendo la universidad (Herrero-Martín et al., 2020). Su base metodológica gira en torno a cinco ámbitos didácticos, denominados *acogidas*, *seminarios*, *talleres*, *proyectos* y *cierres*. Para cada etapa educativa, estos cinco elementos interactúan de manera particular, proyectando características específicas que otorgan identidad metodológica propia a cada etapa. Así, por ejemplo, el NCA incorpora la noción de *entorno de aprendizaje* en educación infantil, para integrar conceptualmente el taller y proyecto, algo que en Primaria permanece con identidades diferentes y definidas o que en educación secundaria se relaciona con los conceptos didácticos de *narrativa* e *Inter narrativa*. Tal es el caso que la definición conceptual incorporada desde el diseño, a la acción metodológica y didáctica determina las condiciones propias de cada ecosistema de aprendizaje.

En la universidad, más concretamente en los estudios de formación de maestros de educación infantil y primaria, este hecho adquiere una singularidad propia alrededor de la metodología ABPI © (Aprendizaje Basado en Proyectos Integrados), basada en el diseño y desarrollo de propuestas de conocimiento globales e interconectadas. El diseño se inició en el año 2018 y su despliegue ha sido paulatino y escalable, a lo largo de cuatro cursos académicos, a lo largo de los cuales, se han introducido de manera progresiva elementos propios de la base metodológica del NCA. Este es el caso de los seminarios y talleres. Su objetivo pedagógico fundamental considera la necesidad de dotar a los estudiantes en formación de recursos personales y conocimiento complementarios para hacer frente a los retos singulares del tiempo en que vivimos. A su vez, tanto el conocimiento como los recursos alimentan el desarrollo de los proyectos integrados a realizar.

Desde un punto de vista conceptual, el taller, como ámbito didáctico, concentra en la propuesta integral de innovación en NCA el propósito educativo que focaliza la construcción personal. Ello significa que su

contenido y procedimiento didáctico ha de orientarse a cubrir necesidades de desarrollo humano que preparen a los estudiantes par su inclusión social en la comunidad. En la etapa universitaria, esta intencionalidad ha de alinearse, además, con las necesidades propias del perfil profesional en formación. En el caso de la formación de maestras y maestros, esta conexión con el mundo ha de actuar como elemento clave que posibilite la mediación entra la construcción del ser personal del educador y la referencia para la construcción del educando. Es ahí donde la ciberseguridad cobra un especial interés, pues su centro de interés pedagógico reside en la necesidad de adecuar el desarrollo individual al contexto social de uso y disfrute de lo colectivo, digital e interactivo, desde la consideración moral y socialmente positiva del uso de las tecnologías y redes digitales de conocimiento.

3.1. Método.

Con objeto de posibilitar el desarrollo de las bases instrumentales para el cambio en la percepción de la seguridad en el uso digital, se diseñó una propuesta de formación constituida por un seminario conjunto, para todos los estudiantes de primer curso de los Grados de Educación Infantil y Educación Primaria de la facultad de educación del Campus La Salle y un taller posterior, a través del uso de computadores, en grupos reducidos y convocatorias sucesivas, a lo largo del segundo semestre del curso académico.

3.1.1. Diseño.

El diseño se enmarca en el paradigma mixto de investigación evaluativa. (Herreras, 2003), sigue una propuesta de desarrollo cuasiexperimental, con dos líneas concurrentes (Sahin & ztrk, 2019), consistentes en un cuestionario tipo Likert (escala de 10 puntos) sobre la autopercepción del uso y riesgo en las redes, y una entrevista semiestructurada, de cumplimentación telemática, acerca de la satisfacción personal por la formación recibida. El tratamiento de los datos resultantes de la escala fue realizado siguiendo un procedimiento pre-post, mediante análisis de varianza (MR, SPSS IBM v27), para lo cual se establecieron dos grupos, test, de realización de la intervención y control, tomando datos de un grupo diferente de estudiantes de primer curso de la facultad de educación.

En cuanto a la línea de análisis cualitativa, se empleó el software de investigación y análisis cualitativo ATLAS.TI para la organización y agrupamiento de códigos (Sabariego-Puig et al., 2014). A partir de ello, se consolidó la correspondiente red semántica asociada al cambio en la representación subjetiva de los participantes, una vez concluida la actividad formativa.

3.1.2. Participantes y muestra.

Un total de 83 personas participaron en la formación, todos ellos estudiantes de primer curso de los grados de magisterio de Educación Infantil y Educación Primaria en el CSEU La Salle de Madrid. La selección muestral se realizó siguiendo un muestreo incidental y procedimiento de saturación completa, de manera que todos los posibles participantes fueron invitados a la actividad. El promedio de edad fue de 18,87 años (desv. típica, 1,96), con 14 varones y 69 mujeres.

3.1.3. Materiales.

Se diseñó un instrumento mixto de recogida de datos, utilizando Microsoft Forms, en el que se incluyeron módulos de inscripción, certificación e investigación. En el primer momento (PRE), los cuestionarios se utilizaron para el registro, tanto en la acción formativa como para determinar el id de cada caso, y el el segundo (POST) los datos sirvieron para la sincronización de casos y la certificación de la actividad.

3.1.4. Procedimiento.

La realización de la investigación siguió un transcurso longitudinal en el tiempo, a lo largo del segundo trimestre del presente curso académico. Consta de varias fases en su desarrollo, siendo esta que aquí se presenta la primera. El procedimiento utilizado en el diseño tiene un carácter secuencial, mixto y concurrente, de configuración pre-post, con un desarrollo de formación de 6 horas, dos de seminario colectivo y dos de taller, en grupos de 35 personas aproximadamente, con interacción frente al ordenador. Se utilizó un cuestionario online, bajo soporte de Microsoft Forms, para la recogida de datos, tanto de carácter personal como de la investigación. . El intervalo total de la intervención en la fase fue de 60 días.

La estructura del cuestionario se diseñó en dos cuerpos diferentes y fue integrado, en el inicio, junto con el documento de inscripción a la jornada, y al fonal, junto con la solicitud de certificación de la formación. Todo ello de manera digital. El módulo cuantitativo del documento contenía cinco cuestiones que referían, secuencialmente, a relevancia en la vida de la seguridad, conciencia de manipulación, dependencia de la conexión digital y número de horas de conexión. Todos los ítems se puntuaban de 1 a 10 puntos (menor a mayor implicación/conciencia/dependencia/uso). El segundo cuerpo consistía en una pregrunta abierta y semiestructurada, acerca de los elementos de significado en la vida, relacionados con la seguridad digital, tanto antes como después de haber recibido la formación. Esta condición estaba contenida en la formulación de la pregunta en la fase post de la aplicación.

La formación consistió en un seminarios general de tres horas de duración, al que asistieron todos los participantes acerca del uso seguro de las redes digitales y su implicación en los procesos educativos. Para su impartición se seleccionó un perfil misto acreditado en ciberseguridad y protección de datos y educación, con formación especializada en ambos campos a nivel universitario (grado y postgrado) y post-universitario. Por su parte, al seminario se siguó un taller práctico de tres horas sobre el uso de las redes, centrado de manera particular en la *Deep Web*, su utilidad, riesgos y contextos de uso. El taller fue repetido en varias ocasiones, de manera que todos los asistentes al seminario hubieron pasado por él.

4. Resultados

En primer lugar, se procedió a realizar un contraste pre-post entre los dos momentos de recogida de datos, al inicio y finalización de la actividad formativa. El cuestionario contenía cuatro escalas, tres ordinales (0-10), cuyas variables se relacionaron con la importancia subjetiva concedida a la seguridad en el uso de internet, la conciencia de manipulación, la conciencia de dependencia digital, y una cuarta sobre el número de horas destinado al uso digital (variable numérica). Además, el cuestionario incorporó una pregunta abierta, relativa a las condiciones de cambio respecto a la situación actual, una vez concluida la actividad de formación.

En el análisis de los datos recogidos en las variables ordinales se utilizó el programa estadístico SPSS (v26), y se aplicó un modelo lineal general, con medidas repetidas, comparando los posibles efectos diferenciales entre el momento previo y el posterior a la formación. Los resultados devolvieron una significación particular en la variable relativa al sentimiento de manipulación a través del uso de las redes. Estos efectos particulares no se observaron significativos para el resto de las variables observadas.

Tabla 1. Resultados del análisis factorial. Efectos pre-post para sensibilidad al cambio (conciencia de manipulación)

Pruebas multivariantes

Efecto		Valor	F	Sig.	Parámetro de no centralidad	Potencia observada c
factor1	Traza de Pillai	,124	,012	6,814	,725	,012
	Lambda de Wilks	,876	,012	6,814	,725	,012
	Traza de Hotelling	,142	,012	6,814	,725	,012
	Raíz mayor de Roy	,142	,012	6,814	,725	,012

a. Diseño : Intersección

Diseño intra-sujetos: FACT_CONCMANIP

b. Estadístico exacto

c. Se ha calculado utilizando alpha = ,05

Como puede verse en la tabla 1, los participantes en la actividad de formación incrementaron su sensibilidad ante la ciberseguridad en las redes de manera significativa (p=0,012, PRE, media 5,633; POST, media 6,673) de algo más de un punto, lo que señala un claro efecto de la formación específica sobre ciberseguridad y educación sobre la conciencia percibida del riesgo y manipulación personal.

Con el objetivo de determinar, a partir de estos datos iniciales, las condiciones cualitativas asociadas al patrón de representación subjetiva una vez finalizado el proceso de formación, se procedió al análisis de las categorías (códigos y relaciones semánticos) asociados a la percepción del cambio, mediante la utilización de ATLAS.TI (v8). La figura 1 ilustra el resultado de la red semántica asociada a las respuestas ofrecidas por los participantes en la formación.

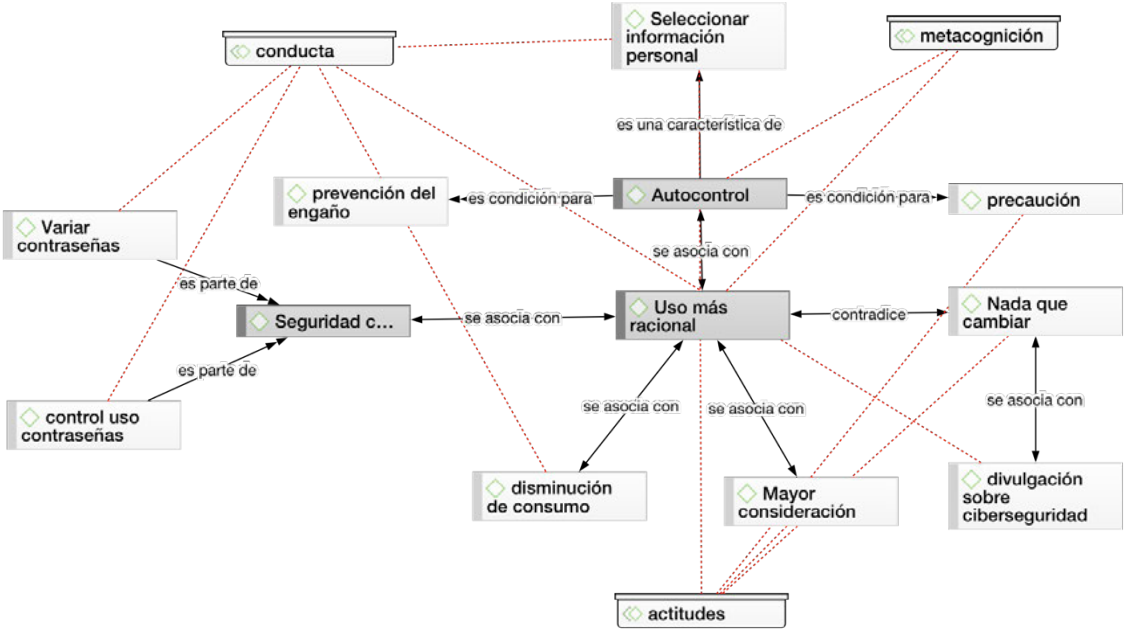

Fig. 1 Red semántica asociada al cambio en la práctica de uso.

De la interpretación de la red semántica se derivan algunas condiciones particulares. Por un lado, la existencia de tres elementos (señalados en trama gris) que actúan como nodos de agrupamiento de códigos, en la unidad hermenéutica definida. Así, se identificaron tres núcleos de significado definidos como "uso más racional de la tecnología digital", "autocontrol", entendida como capacidad para prevenir y anticipar riesgos, proyectada sobre la regulación de mecanismos de selección de la información y procedimientos de uso, y "seguridad contraseñas", que definió de manera particular la identificación de un foco de riesgo situado en la falta de seguridad percibida respecto a la protección de los datos de carácter personal. A partir de los vínculos y relaciones observados, se añadieron tres familias o grupos de códigos, de manera que el resultado final fuese más comprensivo, etiquetados como "actitudes", que expresaban la preocupación por el desarrollo de condicionas estables de percepción de la realidad, "metacognición", que definió la percepción de un cambio en la reflexión previa y durante el uso de los dispositivos digitales, y "conducta", que expresaba la condición relativa a las prácticas de uso directo.

Los datos generales contrastaron con un grupo particular de códigos asociados a la percepción de que no es necesario el cambio, mostrando un perfil general de significado diferente respecto al comportamiento de respuestas del grupo sensible al cambio, conectando, a lo sumo, con un cierto deseo de ofrecer apoyo en la divulgación sobre ciberseguridad a otras personas.

5. Conclusiones y discusión

Los resultados preliminares del estudio mostraron un incremento de la sensibilidad sobre el riesgo en el uso de los soportes digitales. Sin embargo, este cambio en la autopercepción no pareció acompañarse de cambios equivalentes en las dinámicas de uso o de conducta de seguridad. La forma en que las personas reflexionan a partir de la información presentada en la formación sobre seguridad facilita los procesos de

toma de conciencia racional y reflexiva y posibilita la conciencia del uso regulado, aunque no parece ser suficiente para que ese cambio sea transferible al uso, a la seguridad y al tiempo de dedicación. Por último, cabe señalar la relevancia de dos perfiles diferenciados de respuesta. Junto con aquellos que inicialmente muestran una mayor afinidad a la sensibilidad y al cambio, otros participantes consideraron que no había nada que cambiar. Este hallazgo sugiere la necesidad de continuar en la línea de prospección de las condiciones particulares de este perfil.

En el mundo actual, se hace necesario reforzar las políticas educativas que consoliden la formación en el uso de las redes, no solo por mitigar efectos antagonistas derivados de la llamada ingeniería social (Aldawood & Skinner, 2019) sino también por lo que respecta a la mediación educativa que garantice la prevención y salvaguarde las condiciones de seguridad en la escuela (Richardson et al., 2020). En línea con la investigación actual, nuestro estudio sugiere la importancia de velar en la formación de los futuros profesionales de la educación por la consolidación de hábitos competenciales que diferencien aspectos vinculados a las amenazas potenciales, a la conciencia digital y a la conducta adecuada en el mundo digital (Herath et al., 2022). No obstante, si bien los hallazgos muestran que la formación aumenta la conciencia general sobre la ciberseguridad en el uso digital y se encuentran en línea con estudios previos (Bhatnagar & Pry, 2020), se hace necesaria una consideración instrumental de la representación que vaya más allá de la mera sensibilización y que permita proyectar, de manera efectiva, el cambio, sobre las prácticcas de uso y seguridad digital de las personas.

6. Referencias

Aldawood, H., & Skinner, G. (2019). Reviewing Cyber Security Social Engineering Training and Awareness Programs—Pitfalls and Ongoing Issues. *Future Internet*. https://doi.org/10.3390/FI11030073

Alier, M., Casañ Guerrero, M. J., Amo, D., Severance, C., & Fonseca, D. (2021). Privacy and E-Learning: A Pending Task. *Sustainability, 13*(16), 9206. https://doi.org/10.3390/su13169206

Alzighaibi, A. R. (2021). Cybersecurity Attacks on Academic Data and Personal Information and the Mediating Role of Education and Employment. *Journal of Computer and Communications*, *9*(11), 77-90. https://doi.org/10.4236/jcc.2021.911006

Amankwa, E. (2021). Relevance of Cybersecurity Education at Pedagogy Levels in Schools. *Journal of Information Security*, *12*(4), 233-249. https://doi.org/10.4236/jis.2021.124013

Bağci, H. (2019). Analyzing the Digital Addiction of University Students through Diverse Variables: Example of Vocational School. *International Journal of Contemporary Educational Research*, *6*(1), 100-109. https://doi.org/10.33200/ijcer.546326

Bhatnagar, N., & Pry, M. (2020). Student Attitudes, Awareness, and Perceptions of Personal Privacy and Cybersecurity in the Use of Social Media: An Initial Study. *Undefined*. https://iapp.org/media/pdf/resource_center/student_attitudes_awareness_security_social_media.pdf

Dzardanova, E., Kasapakis, V., & Gavalas, D. (2018). On the Effect of Social Context in Virtual Reality: An Examination of the Determinants of Human Behavior in Shared Immersive Virtual Environments. *IEEE Consumer Electronics Magazine*, *7*(4), 44-52. https://doi.org/10.1109/MCE.2018.2816204

García-Umaña, A., & Tirado-Morueta, R. (2018). Digital Media Behavior of School Students: Abusive Use of the Internet. *Journal of New Approaches in Educational Research*, *7*(2), 140-147. https://doi.org/10.7821/naer.2018.7.284

Gallego-Arrufat, M.-J., Torres-Hernández, N., & Pessoa, T. (2019). Competencia de futuros docentes en el área de seguridad digital. *Comunicar: Revista Científica de Comunicación y Educación*, *27*(61), 57-67. https://doi.org/10.3916/C61-2019-05

Gonzalez-Sanmamed, M., Sangrà, A., Souto-Seijo, A., & Blanco, I. E. (2020). Learning ecologies in the digital era: Challenges for higher education. *PUBLICACIONES*, *50*(1), 83-102. https://doi.org/10.30827/publicaciones.v50i1.15671

Herath, T. B. G., Khanna, P., & Ahmed, M. (2022). Cybersecurity Practices for Social Media Users: A Systematic Literature Review. *Journal of Cybersecurity and Privacy*. https://doi.org/10.3390/jcp2010001

Herreras, E. B. (2003). Metodología de la Investigación Evaluativa: Modelo CIPP1. *Revista Complutense de Educación*, *14*(2), 361-376. https://revistas.ucm.es/index.php/RCED/article/view/RCED0303220361A

Herrero-Martín, J., Canaleta, X., Fonseca, D., Rodríguez-Merino, C., Kinnear, L., & Amo, D. (2020). Designing a multi-scale and multi-dimensional assessment for a new national educational context. *Eight International Conference on Technological Ecosystems for Enhancing Multiculturality*, 791-796. https://doi.org/10.1145/3434780.3436567

Martin, F., Gezer, T., & Wang, C. (2019). Educators' Perceptions of Student Digital Citizenship Practices. *Computers in the Schools*, *36*(4), 238-254. https://doi.org/10.1080/07380569.2019.1674621

Pangrazio, L., & Cardozo-Gaibisso, L. (2020). Beyond cybersafety: The need to develop social media literacies in pre-teens. *Digital Education Review*, *37*, 49-63. https://doi.org/10.1344/der.2020.37.49-63

Rahayu, F. S., Nugroho, L. E., Ferdiana, R., & Setyohadi, D. B. (2020). Research Trend on the Use of IT in Digital Addiction: An Investigation Using a Systematic Literature Review. *Future Internet*, *12*(10), 174. https://doi.org/10.3390/fi12100174

Richardson, M. D., Lemoine, P. A., Stephens, W. E., & Waller, R. E. (2020). Planning for Cyber Security in Schools: The Human Factor. *Educational Planning*, *27*(2), 23-39. https://eric.ed.gov/?id=EJ1252710

Sabariego-Puig, M., Vilà-Baños, R. y Sandín-Esteban, M. P. (2014). El análisis cualitativo de datos con ATLAS.ti. [En línea] REIRE, Revista d'Innovació i Recerca en Educació, 7 (2), 119-133. Accesible en: http://www.ub.edu/ice/reire.htm

Sahin, M. D., & Öztürk, G. (2019). Mixed Method Research: Theoretical Foundations, Designs and Its Use in Educational Research. *International Journal of Contemporary Educational Research*, *6*(2), 301-310. https://eric.ed.gov/?id=EJ1239419

Tayouri, D. (2015). The Human Factor in the Social Media Security – Combining Education and Technology to Reduce Social Engineering Risks and Damages. *Procedia Manufacturing*, *3*, 1096-1100. https://doi.org/10.1016/j.promfg.2015.07.181

Tomczyk, Ł. (2019). What Do Teachers Know About Digital Safety? *Computers in the Schools*, *36*(3), 167-187. https://doi.org/10.1080/07380569.2019.1642728

Verhoef, P. C., Broekhuizen, T., Bart, Y., Bhattacharya, A., Qi Dong, J., Fabian, N., & Haenlein, M. (2021). Digital transformation: A multidisciplinary reflection and research agenda. *Journal of Business Research*, *122*, 889-901. https://doi.org/10.1016/j.jbusres.2019.09.022

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), 353. https://doi.org/10.3390/educsci10120353

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. *Journal of Computer Information Systems*, *62*(1), 82-97. https://doi.org/10.1080/08874417.2020.1712269