Seguridad Digital Para Todos: experiencia de implementación de un NOOC de alcance internacional

Francisco Javier Rocha Estrada
Instituto Tecnológico y de Estudios Superiores de Monterrey
fcojvr25@gmail.com

Carlos Enrique George Reyes
Instituto Tecnológico y de Estudios Superiores de Monterrey
cgeorge@tec.mx

Leonardo David Glasserman Morales
Instituto Tecnológico y de Estudios Superiores de Monterrey
glasserman@tec.mx

Área temática: Tecnologías de la información y comunicación (TIC) en educación
Línea temática: Avances de las TIC en educación: cursos en línea masivos y abiertos
Tipo de ponencia: Reporte parciales o final de investigación

Resumen

Hoy en día, actividades como la educación, el trabajo y el entretenimiento se han trasladado a entornos virtuales gracias a los beneficios que ofrecen las nuevas tecnologías. Sin embargo, cada oportunidad también puede conllevar algunos riesgos, por lo que la seguridad digital se vuelve una alfabetización imprescindible para cualquiera que quiera participar de forma segura en la era digital. Luego de la pandemia del COVID-19, las modalidades virtuales surgieron como una alternativa para continuar con el proceso de aprendizaje, y aunque la crisis mundial ha pasado, las opciones en línea siguen vigentes. Una de estas alternativas son los NOOC, cursos en línea, gratuitos, abiertos para cualquier persona con una conexión a internet y de corta duración. Esta propuesta implementó una estrategia para fortalecer competencias en seguridad digital a través de un NOOC, que incluye temas de ciudadanía digital, construcción de conocimiento, identidad digital, privacidad, *sexting,* ciberacoso y protección de datos. El diseño instruccional del curso siguió el modelo ADDIE, una metodología ampliamente utilizada para desarrollar material educativo para entornos presenciales o virtuales que integra las etapas de análisis, diseño, desarrollo, implementación y evaluación. Ocho meses después de su lanzamiento, el curso ha alcanzado los 3000 alumnos matriculados de 47 países y tiene una valoración de 4.67/5.00, por lo que se considera una alternativa confiable para capacitarse en temas de seguridad digital.

Palabras clave: MOOC, NOOC, Seguridad digital, Tecnología.

Introducción

Las políticas de distanciamiento social anunciadas por la Organización Mundial de la Salud (OMS) e implementadas por los gobiernos locales como medida para frenar la propagación del COVID-19, cambiaron la forma de relacionarse para todas las personas (Adedoyin y Soykan, 2020), muestra de lo anterior es que actividades de trabajo, estudio y recreación tuvieron que trasladarse a escenarios no presenciales (Valle Martínez y Basilio Rivera, 2020). Pero, así como las tecnologías brindan nuevas oportunidades, también pueden presentarse acompañadas de algunos riesgos, por lo que es necesario adquirir conocimientos básicos de seguridad digital para poder participar en estos escenarios de forma segura (Mikelic Preradovic et al., 2016). Por esta razón, la promoción de la seguridad digital se ha convertido en un foco de atención en años recientes (Lin, 2020).

Hoy en día las personas no solo enfrentan el reto de utilizar las nuevas herramientas tecnológicas, sino que además deben evitar exponerse a los peligros de internet (Vitak et al., 2018). Las estadísticas muestran un aumento en el volumen y la complejidad de las nuevas amenazas digitales, enfatizando la importancia de desarrollar una conciencia de la seguridad digital (Koyuncu y Pusatli, 2019). La seguridad constituye uno de los aspectos de mayor preocupación para el diseño de las políticas de protección para los usuarios en el entorno actual (García-Valcárcel et al., 2019), por lo que promover la seguridad digital es clave para garantizar un uso crítico, responsable y seguro de las tecnologías (Gamito et al., 2017). Con estos conocimientos, los usuarios tendrán mayor oportunidad de ser conscientes de los peligros a los que están expuestos en la red y así, asumir precauciones y comportamientos seguros (Ibarra-Rius et al., 2018).

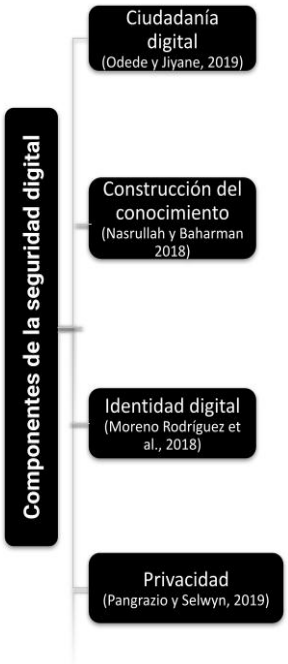
Cuando las personas tienen más habilidades y son conscientes de la seguridad digital presentan un riesgo bajo de convertirse en víctimas de delitos cibernéticos (Nalaka y Diunugala, 2020). Inclusive, en caso de enfrentar las amenazas digitales serán capaces de tener una mejor respuesta ante los problemas de seguridad (Gratian et al., 2018). Mientras que, por el contrario, aquellos que no están familiarizados con la seguridad digital, al desconocer muchas opciones críticas de seguridad pueden experimentar graves consecuencias (Watson y Zheng, 2017), puesto que los usuarios que no comprenden adecuadamente cómo funciona la tecnología son las más propensos a las situaciones de riesgo (Tomczyk, 2019).

La seguridad digital se define como la capacidad de gestionar, inspeccionar y detectar amenazas como el acoso, la seducción, la radicalización, el desprecio y los contenidos prohibidos (Na-Nan et al., 2019). Esta disciplina permite la protección de activos de información digitales, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas que se encuentran interconectados,

está orientada tanto a los sistemas de información como a los usuarios (Ghafir et al, 2018). Entre las principales problemáticas a la seguridad se encuentran la difusión de las noticias falsas, la vulneración de la privacidad de los datos, el ciberacoso, el *sexting*, el *grooming* y la visualización de contenidos explícitos como violencia y pornografía (Gamito et al., 2017). Ante tales riesgos, las medidas de prevención están orientadas hacia la alfabetización en seguridad digital, puesto que, si se ofrece una buena educación y formación en el futuro, las personas desarrollarán los conocimientos necesarios para evitar los peligros (Yan et al., 2018).

La seguridad digital implica comprender cómo se desarrollan los comportamientos seguros o de riesgo, así como cuáles elementos la van integrando (Lohnes Watulak 2016). Para entender esta alfabetización es necesario abordarla desde sus elementos básicos (Figura 1); la ciudadanía digital implica normas de comportamiento en los entornos virtuales a través del uso competente, seguro, responsable y ético de las tecnologías (Odede y Jiyane, 2019); la construcción del conocimiento permite cumplir los objetivos de aprendizaje en los nuevos escenarios educativos a través del uso de herramientas tecnológicas (Nasrullah y Baharman, 2018); la identidad digital se construye por medio de las interacciones que realizas en la red, es independiente de tu identidad en el mundo real, aunque puede afectarla y es posible tener varias identidades de acuerdo a los perfiles que manejas en distintas plataformas (Moreno Rodríguez et al., 2018); la privacidad se refiere al uso autorizado que se le da a tu información y puedes gestionarla de acuerdo a las políticas de cada sitio o aplicación que utilizas (Pangrazio y Selwyn, 2019).

Figura 1. *Componentes de la seguridad digital*



Para promover la seguridad digital se han implementado diversas estrategias, algunas están relacionados con restricciones de uso, sin embargo, han sido criticadas por perpetuar prácticas conservadoras y adversas, al mismo tiempo que limitan las oportunidades de aprendizaje y comunicación (Hope, 2013), muestra de ello es el control parental, los filtros y demás alternativas que no abonan a la seguridad digital (Plichta, 2017). En contraste con los enfoques que intentan promover la seguridad limitando el acceso a dispositivos y herramientas, el concepto de seguridad digital es mucho más complejo e implica la articulación de una serie de mecanismos dentro y fuera del entorno de los usuarios. (Pangrazio y Cardozo-Gaibisso, 2020). Por tanto, los expertos apuestan por la formación en seguridad digital como una herramienta de prevención con el objetivo de incrementar las competencias de las personas a fin de que logren afrontar los riesgos de la red de forma segura (Rodríguez de Dios y Igartua, 2018).

Uno de los desafíos del contexto actual es diseñar programas de formación enfocados en los temas emergentes de seguridad (Tomczyk, 2019). Se debe educar sobre los riesgos que representan las amenazas digitales, así como alentar a los usuarios a comportarse con cautela, responsabilidad y cuidado al acceder a este medio (Na-Nan et al., 2019). Las instituciones educativas juegan un papel importante en el desarrollo de la seguridad digital de la comunidad, debido a que son el principal medio por el cual una sociedad puede abordar las problemáticas actuales dentro de un entorno de aprendizaje estructurado (Livingstone et al., 2013). Tan es así, que la universidad es considerada el espacio más relevante para capacitar a las personas en conocimientos profesionales y de formación para la vida (Cabrales y Díaz, 2017).

A pesar de lo anterior, aun cuando varias instituciones ya han introducido diversas alfabetizaciones en sus planes de estudios de forma obligatoria, la educación en seguridad digital sigue siendo un curso optativo para muchas otras (Ndiege y Okello, 2018). Además, pareciera que los temas de seguridad digital solo están enfocados a ciertas carreras y dado que las tecnologías han penetrado en diversas profesiones, deben extenderse sus contenidos para todos los estudiantes (Wang y Zhou, 2017). Sin embargo, el tema de seguridad digital no ha recibido suficiente atención en la literatura (Tomczyk, 2019), por lo tanto, son necesarias investigaciones que aporten datos sobre está problemática y propuestas de intervención para promover la seguridad digital.

Desarrollo

Un movimiento que ha llamado la atención como una alternativa de formación en el contexto actual son los cursos en línea masivos y abiertos (MOOC, por las siglas en inglés de *Massive Open Online Courses*). De acuerdo con Siemens (2013), se definen como cursos porque plantean una estructura enfocada a la enseñanza y a la superación de pruebas; abiertos porque sus contenidos están a libre disposición de cualquier estudiante, que puede compartirlos e incluso modificarlos; en línea porque se accede a ellos a través de internet y masivos porque están enfocados a una demanda de millones de personas. Hoy en día, los MOOC continúan

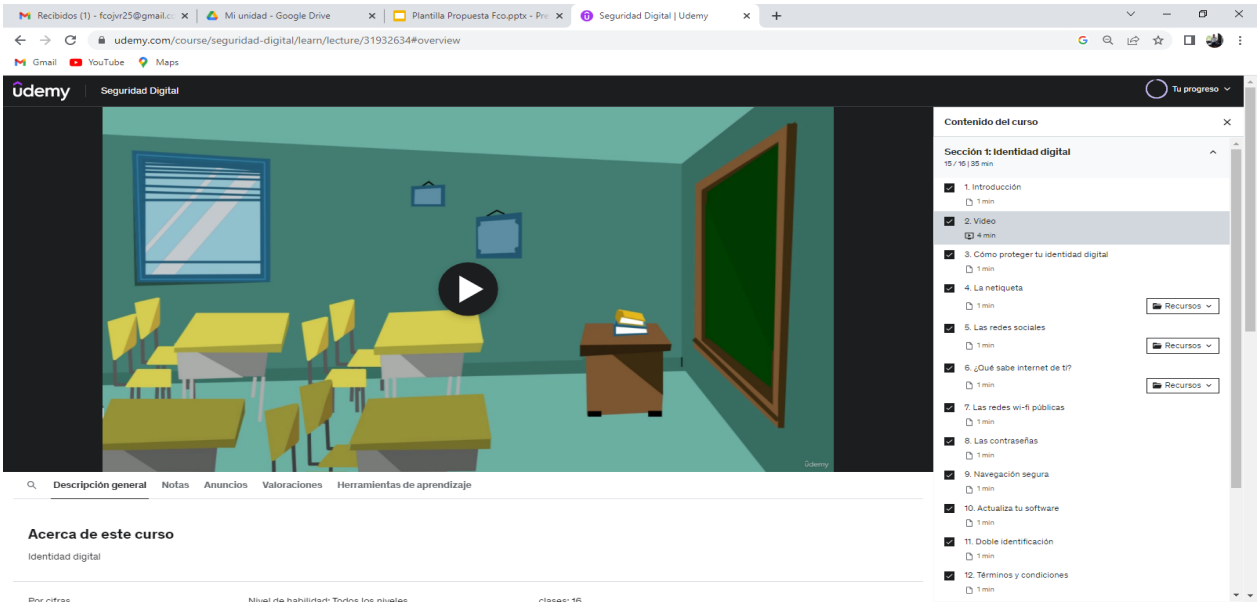
siendo un referente de la formación a través de internet, inclusive, su demanda ha aumentado a partir de la pandemia, por lo que instituciones educativas han buscado mantenerse vigentes elaborando nuevos contenidos para sus estudiantes y para aquellas personas que los utilizan como formación a lo largo de la vida (La Tríada, 2021).

Existen diversas clasificaciones para los MOOC (Daniel, 2012), en un origen existían los CMOOC, que eran entornos de aprendizaje virtual donde los participantes tienen un rol activo en la construcción del conocimiento, estaban basados en el conectivismo y las actividades se realizaban en la red, mientras que en los xMOOC el conocimiento se centraba en los expertos, utilizaban una pedagogía conductista-constructivista y las actividades se realizaban dentro de una plataforma (Bartolomé y Steffens, 2015). En la actualidad continúan surgiendo variantes de cursos y aunque las diferencias son mínimas con relación a las características de los MOOC, es importante distinguirlos para decidir qué opción se adapta mejor a cada estilo de aprendizaje, tales como los SPOC (*Small Private Online Course*), que son desarrollados para grupos pequeños y con características muy definidas en sus participantes; los NOOC (*Nano Open Online Course*), que son mucho más cortos y están basados en el uso de videos; y los SPOOC (*Self-Placed Open Online Course*), donde no existen fechas establecidas de cierre del curso y los estudiantes pueden avanzar a su ritmo (Dolores Castrillo et al., 2018).

Entre estas opciones, destacan los NOOC, cuya diferencia principal con los MOOC es la cantidad de tiempo estimado para completar el curso. Mientras que en los MOOC el tiempo de trabajo puede llegar hasta las 72 horas distribuido en varias semanas, los NOOC son más compactos, requiriendo desde una hasta veinte horas de dedicación (Lozano et al., 2019). Estos cursos representan una estrategia que facilita el aprendizaje al desarrollarlo desde videos cortos, con recursos de información concretos y actividades bien definidas, que además no necesitan mucho tiempo de parte de los estudiantes y permiten realizarlos en cualquier momento (Sánchez et al., 2017). Entre sus ventajas destacan que no hay límite de participantes, fomentan el aprendizaje autónomo, tienen una estructura flexible, los contenidos están sintetizados y los materiales son de acceso abierto (Jurado Mendoza, 2021).

Esta investigación reporta los hallazgos en la implementación de un módulo de prueba en formato NOOC, con el propósito de validar esta experiencia de aprendizaje como una alternativa de formación y explorar su viabilidad a gran escala (Figura 2). Para ello se elaboró una versión piloto con el diseño de un módulo del tema identidad digital, con un tiempo de aproximadamente 30 minutos para completarlo.

Figura 2. *Módulo de identidad digital*



El curso estuvo disponible en la plataforma *Udemy* e incluyó videos, archivos descargables, foros y enlaces externos, al finalizar, un grupo de diez participantes fue invitado a responder una encuesta para compartir su experiencia. El 90% de los alumnos consideró que la organización de los temas era adecuada y el 80% estuvo conforme con los recursos incluidos. En las preguntas abiertas, los estudiantes expresaron no haber tenido problemas con el funcionamiento de la plataforma y se mostraron interesados por temas como la confidencialidad, la ingeniería social y las redes sociales, estos contenidos estuvieron contemplados para ser abordados en la versión final del curso. Además, dos participantes expresaron comentarios:

> Siento que presentas información muy concreta pero muy útil y que todos deberían conocer. Por ejemplo, el cuidar el tipo de fotografías que subes a redes sociales, porque puede crear una idea de quién eres como persona. El último video también tiene información importante sobre la seguridad sobre todo con permitir el uso del micrófono y cámara. La tecnología tiene muchísimos beneficios, pero desafortunadamente se ha ido utilizando para mal, como todo en la vida, y por ello tenemos que cuidarnos también dentro de estos medios digitales. Gracias por este curso, te felicito [E1]
>
> Me encantó. Debería de saberse más sobre esto [E2]

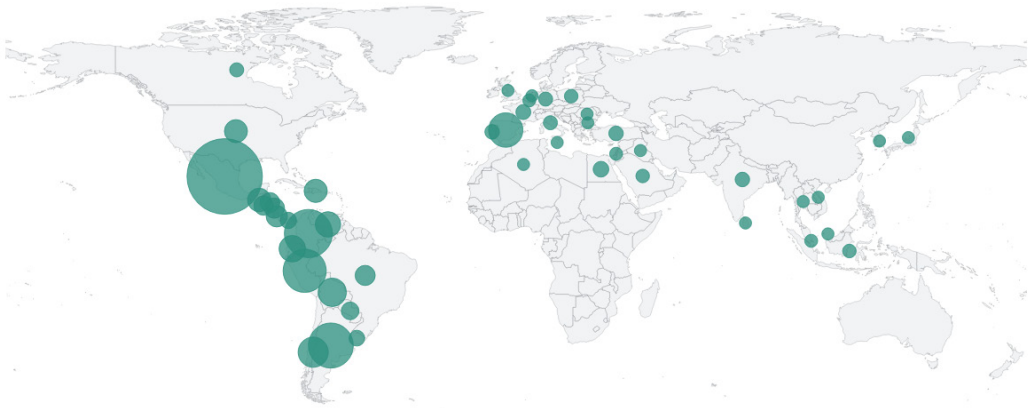
Tras una amplia aceptación y buena valoración del curso se diseñó una experiencia de aprendizaje denominada *Seguridad Digital Para Todos*. La modalidad de impartición fue a través de un NOOC, seleccionado por ser un formato de corta duración basado en videos y

donde los estudiantes pueden avanzar a su propio ritmo (Lozano et al., 2019), el cual se alojó en la plataforma de cursos en línea *Udemy* (Figura 3). El diseño instruccional del curso siguió el modelo ADDIE, una metodología ampliamente utilizada para desarrollar material educativo para entornos presenciales o virtuales, la cual se integra de las etapas de análisis, diseño, desarrollo, implementación y evaluación (Castellanos Altamirano y Rocha Trejo, 2020).

Figura 3. *Página de inicio del curso seguridad digital para todos*

El curso tiene una duración aproximada de tres horas y está dividido en los módulos de ciudadanía digital, construcción del conocimiento, identidad digital, privacidad, *sexting,* ciberacoso y protección de datos. Es gratuito, está abierto al público en general, fomenta el aprendizaje autónomo, además de que no tiene un límite de participantes, se accede a través de internet y no cuenta con requisitos previos de conocimiento. Se han registrado participantes provenientes de 47 países hablantes de catorce idiomas (Figura 3).

Figura 4. *Procedencia de los participantes del curso seguridad digital para todos*



Después de ocho meses de estar disponible, alcanzó las 3,000 inscripciones y cuenta con una valoración de 4.67/5.00. A continuación, se presentan algunos comentarios de las personas tras finalizar el curso:

> Es una bonita experiencia de aprendizaje. El curso es sencillo, pero explica claramente los contenidos abordados. Si, con este curso he ampliado mis conocimientos sobre Seguridad Digital [C-fahp]
>
> Fue muy bueno, realmente estaba muy desinformada en muchos aspectos, creo que con toda la información, seré más cuidadosa en lo que respecta a las redes sociales.
>
> Un curso dirigido a todas las personas, por lo cual, es asimilable para todo mundo, y de contenido [C-od]
>
> Creo que, para mí, ha sido de gran utilidad ya que aunque sabemos cierta información, con este curso realmente se toma conciencia de muchas cosas. Por ejemplo, el hecho de que muchas veces solo damos aceptar a los términos y condiciones de las páginas web o aplicaciones, sin leerlos detenidamente [C-mbfv]
>
> Mi experiencia personal es que el curso nos hace conscientes de lo vulnerables que somos ante la falta de cuidado para mantener. Distancia entre las publicaciones y opiniones que damos a través de la red. Y lo que presentamos en el mundo de carne y hueso. Ser cuidadosos, ordenados, precavidos y discretos. Es una buena forma de no sufrir problemas de acoso o robo de identidad. Por citar solo dos eventos desagradables que con cuidado podemos evitarnos [C-a]

Conclusiones

En los últimos años, la incorporación masiva de las tecnologías a la vida cotidiana de las personas ha facilitado muchos procesos, sin embargo, algunas personas mal intencionadas se han aprovechado de esta dependencia tecnológica y las vulnerabilidades de la red para perjudicar a otras (Lin, 2020). Es por eso que la seguridad digital ha cobrado relevancia a nivel mundial, ya que brinda las herramientas necesarias para prevenir y afrontar las amenazas digitales (Rodríguez de Dios y Igartua, 2018).

A pesar de lo anterior y aunque las instituciones académicas son consideradas el lugar ideal de formación, no existe un espacio donde todas las personas puedan adquirir estos conocimientos ya que la universidad ha enfocado sus esfuerzos hacia las carreras de informática y para el resto de áreas lo ha dejado como cursos optativos (Cabrales y Díaz, 2017; Ndiege y Okello, 2018). Es por eso que se requieren nuevas alternativas de formación confiables que brinden los conocimientos necesarios para protegerse frente a las amenazas digitales.

La experiencia de aprendizaje en formato NOOC seguridad digital para todos, ha demostrado ser una alternativa aceptada por los estudiantes para capacitarse en temas de seguridad digital,

además, el diseño de esta experiencia de aprendizaje está respaldado por una metodología sólida y sus contenidos son de acceso abierto, por lo que cualquier persona con acceso a internet puede acceder a ellos.

Un siguiente paso en esta investigación sería evaluar los niveles de seguridad digital de los estudiantes, para determinar si este tipo de intervenciones además de ser aceptadas por los participantes también son efectivas para mejorar las competencias en seguridad digital de los estudiantes. Futuros estudios podrían abordar los componentes de la seguridad digital propuestos en esta investigación con relación a nuevas amenazas digitales, implementar talleres en formato presencial para contrastar sus hallazgos con el formato virtual y desarrollar otras alternativas de formación como juegos o aplicaciones.

Referencias

Adedoyin, O. B., y Soykan, E. (2020). Covid-19 pandemic and online learning: the challenges and opportunities. *Interactive Learning Environments*, 1-13. https://doi.org/10.1080/10494820.2020.1813180

Bartolomé, A., y Steffens, K. (2015). ¿Son los MOOC una alternativa de aprendizaje? *Comunicar 27*(44), 91-99. http://digital.casalini.it/3011436

Cabrales, O., y Díaz, V. (2017). El aprendizaje autónomo en los nativos digitales. *Conhecimento y Diversidade*, *9*(17), 12-32. http://dx.doi.org/10.18316/rcd.v9i17.3473

Castellanos Altamirano, H., y Rocha Trejo, E. H. (2020). Aplicación de ADDIE en el proceso de construcción de una herramienta educativa distribuida b-learning. *Revista Iberoamericana de Tecnología en Educación y Educación en Tecnología,* (26), 10-19. https://doi.org/10.24215/18509959.26.e1

Daniel, J., (2012). Making Sense of MOOCs: Musings in a Maze of Myth, Paradox and Possibility. Journal of Interactive Media in Education, 18, 1-20. https://www-jime.open.ac.uk/articles/10.5334/2012-18/

Dolores Castrillo, M., Martín-Monje, E., y Vásquez-Cano, E. (2018). *Guía práctica para el diseño y tutorización de MOOC*. Miríadax.

Gamito, R., Aristizabal, P., y Olasolo, M. (2017). La necesidad de trabajar los riesgos de internet en el aula. *Profesorado. Revista de Currículum y Formación de Profesorado*, *21*(3), 409-426. https://www.redalyc.org/pdf/567/56752489020.pdf

Ghafir, I., Saleem, J., Hammoudeh, M., Faour, H., Prenosil, V., Jaf, S., Jabbar, S., y Baker, T. (2018). *Security threats to critical infrastructure: the human factor. The Journal of Supercomputing, 74*(10), 4986-5002. https://doi.org/10.1007/ s11227-018-2337-2

Gratian, M., Bandi, S., Cukier, M., Dykstra, J., y Ginther, A. (2018). Correlating human traits and cyber security behavior intentions. *Computers y Security, 73*, 345-358. https://doi.org/10.1016/j.cose.2017.11.015

Hope, A. (2013). The politics of online risk and the discursive construction of e-safety. En K. Facer y N. Selwyn (Eds.), The Politics of Education and Technology: Conflicts, controversies and connections (pp. 83-98). Palgrave/Macmillan. https://doi.org/10.1057/9781137031983_5

Ibarra-Rius, N., Ballester Roca, J., y Marín, F. (2018). Encrucijadas de la competencia mediática y la ciudadanía: uso y consumo de aplicaciones educativas. *Prisma Social*, (20), 92-113. https://revistaprismasocial.es/article/view/2311

Koyuncu, M., y Pusatli, T. (2019). Security Awareness Level of Smartphone Users: An Exploratory Case Study. *Hindawi Mobile Information Systems*, *2019*, 786913. https://doi.org/10.1155/2019/2786913

Jurado Mendoza, T. L. (2021). *Los Nooc como estrategia tecno-pedagógica para la formación de competencias digitales en docentes de la unidad educativa fiscomisional.* (Tesis de maestría). La Inmaculada, Otavalo. http://repositorio.utn.edu.ec/handle/123456789/11852

La Tríada. (2021). La Tríada en Coursera. https://latriada.tec.mx/es/innovacion-educativa/la-triada-en-coursera

Lin, K. Y. (2020). Application of a Blended Assessment Strategy to Enhance Student Interest and Effectiveness in Learning: Case Study With Information Security Literacy. *CIN: Computers, Informatics, Nursing*, *38*(10), 508-514. https://doi.org/10.1097/CIN.0000000000000665

Livingstone, S., Kalmus, V., y Talves, K. (2013). Girls' and boys' experiences of online risk and safety. The routledge companion to media y gender, 190-200. https://sisu.ut.ee/sites/default/files/genire/files/livingstone_etal_media_and_gender_companion.pdf

Lohnes Watulak, S. (2016). Reflection in action: Using inquiry groups to explore critical digital literacy with pre-service teachers. *Educational Action Research, 24*(4), 503–518. https://doi.org/10.1080/09650792.2015.1106957

Lozano, P. G. B., Monllor, J. F., Fernández, F. B., Ramírez, M. G., Ávalos, S. H., Prados, A. H., ... y Roca, J. J. R. (2019). Experiencia de un NOOC de Física. En *Redes de Investigación e Innovación en Docencia Universitaria: Volumen 2019* (pp. 555-563). Instituto de Ciencias de la Educación, Universidad de Alicante. http://rua.ua.es/dspace/handle/10045/98732

Mikelic Preradovic, N., Lešin, G., y Šagud, M. (2016). Investigating Parents' Attitudes towards Digital Technology Use in Early Childhood: A Case Study from Croatia. *Informatics in education*, *15*(1), 127-146. https://doi.org/10.15388/infedu.2016.07

Moreno Rodríguez, M. D., Gabarda Méndez, V., y Rodríguez Martín, A. M. (2018). Alfabetización informacional y competencia digital en estudiantes de magisterio. *Profesorado, Revista de currículum y formación del profesorado*, *22*(3), 253-270. https://doi.org/10.30827/profesorado.v22i3.8001

Na-Nan, K., Roopleam, T., y Wongsuwan, N. (2019). Validation of a digital intelligence quotient questionnaire for employee of small and medium-sized Thai enterprises using exploratory and confirmatory factor analysis. *Kybernetes, 49*(5), 1465-1483. https://doi.org/10.1108/K-01-2019-0053

Nalaka, S., y Diunugala, H. (2020). Factors Associating with Social Media related Crime Victimization: Evidence from the Undergraduates at a Public University in Sri Lanka. *International Journal of Cyber Criminology*, *14*(1), 174- 184. https://doi.org/174-184.10.5281/zenodo.3748685

Nasrullah y Baharman (2018). Exploring Practical Responses of M3LC for Learning Literacy. *Journal of Physics Conference Series, 954*(1). htts://doi.org/10.1088/1742-6596/954/1/012007

Ndiege, J. R., y Okello, G. (2018). Information security awareness amongst students joining higher academic institutions in developing countries: Evidence from Kenya. *The African Journal of Information Systems, 10*(3), 204-221. https://www.researchgate.net/publication/325442591

Odede, I. R., y Jiyane, G. V. (2019). Exploring dimensional constructs of digital literacy skills for higher education. https://digitalcommons.unl.edu/libphilprac/2806

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

Pangrazio, L., y Selwyn, N. (2019). 'Personal data literacies': A critical literacies approach to enhancing understandings of personal digital data. *New Media y Society*, *21*(2), 419-437. https://doi.org/10.1177/1461444818799523

Plichta, P. (2017). Socialization and Education of Children and Adolescents with Intellectual Disabilities in the Digital Age. *Toruń: Wydaw. Adam Marszałek*. https://www.repozytorium.uni.wroc.pl/dlibra/publication/127975/edition/117557

Rodríguez de Dios, I., y Igartua, J. J. (2018). Skills of digital literacy to address the risks of interactive communication. En *Information and Technology Literacy: Concepts, Methodologies, Tools, and Applications*, *9*(1), 621-632. http://doi.org/10.4018/JITR.2016010104

Sánchez, L. P., de la Torre, M. J., y Martín-Cuadrado, A. M. (2017). Los NOOC para la formación en competencias digitales del docente universitario. Una experiencia piloto de la Universidad Nacional de Educación a Distancia (UNED). *Revista De Educación a Distancia (RED)*, *17*(55). https://revistas.um.es/red/article/view/315281

Siemens, G. (2013). Massive Open Online Courses: Innovation in Education? In R. McGreal, W. Kinuthia y S. Marshall (Eds.), Open Educational Resources: Innovation, Research and Practice (pp. 5-15). Commonwealth of Learning. https://www.oerknowledgecloud.org/archive/pub_PS_OER-IRP_CH1.pdf

Tomczyk, L. (2019). What do teachers know about digital safety? *Computers in the Schools*. *36*(3), 167-187. https://doi.org/10.1080/07380569.2019.1642728

Valle Martínez, M. D., y Basilio Rivera, R. (2020). La experiencia de la Escuela Nacional Preparatoria frente a la pandemia de COVID-19. *Revista mexicana de bachillerato a distancia*, *24*(12), 28. http://dx.doi.org/10.22201/cuaed.20074751e.2020.24.76820

Vitak, J., Liao, Y., Subramaniam, M., y Kumar, P. (2018). 'I Knew It Was Too Good to Be True" The Challenges Economically Disadvantaged Internet Users Face in Assessing Trustworthiness, Avoiding Scams,

and Developing Self-Efficacy Online. *Proceedings of the ACM on Human-Computer Interaction*, *2*(CSCW), 1-25. https://doi.org/10.1145/3274445

Wang, J., y Zhou, H. (2017). Embedding Information Security Literacy in College Education. En *2017 International Conference on Social science, Education and Humanities Research (ICSEHR 2017),* 48-51. Atlantis Press. https://doi.org/10.2991/icsehr-17.2017.12

Watson, B., y Zheng, J. (2017). On the User Awareness of Mobile Security Recommendations. *ACM SE*, 13-15. https://doi.org/10.1145/3077286.3077563

Yan, Z., Robertson, T., Yan, R., Park, S. Y., Bordoff, S., Chen, Q., y Sprissler, E. (2018). Finding the weakest links in the weakest link: How well do undergraduate students make cybersecurity judgment?. *Computers in Human Behavior*, *84*, 375-382. https://doi.org/10.1016/j.chb.2018.02.019