A. Gordillo, E. Barra, P. Garaizar and S. López-Pernas, "Use of a Simulated Social Network as an Educational Tool to Enhance Teacher Digital Competence" in IEEE-RITA, vol. 16, no. 1, pp. 107-114, FEB. 2021. doi: 10.1109/RITA.2021.3052686

Uso de una Red Social Simulada como Herramienta Educativa para Mejorar la Competencia Digital Docente

Aldo Gordillo, Enrique Barra, Pablo Garaizar, Sonsoles López-Pernas, *Member, IEEE*

***Title*— Use of a Simulated Social Network as an Educational Tool to Enhance Teacher Digital Competence.**

***Abstract*— There is a worrying gap between the digital competence that teachers must have to effectively develop their students' digital competence and the one they actually have, especially in the area related to the safe and responsible use of technology. Further investigation is needed on the use of training activities, methods and tools aimed at enhancing this competence. This article examines, in the context of an online course in MOOC format, the usefulness of Social Lab, a simulated social network, as an educational tool to improve the digital competence of teachers in the area of safe and responsible use of technology.**

***Index Terms*— Digital competence, e-Safety, educational technology, social engineering, social network, teacher education.**

I. Introducción

La competencia digital, entendida como aquella que "implica el uso creativo, crítico y seguro de las tecnologías de la información y la comunicación para alcanzar los objetivos relacionados con el trabajo, la empleabilidad, el aprendizaje, el uso del tiempo libre, la inclusión y la participación en la sociedad" [1], constituye una competencia básica fundamental que todo estudiante debe haber adquirido tras terminar la enseñanza obligatoria a fin de desarrollarse como persona e integrarse adecuadamente en la sociedad [2].

Recientemente, la Comisión Europea ha establecido como una prioridad la formación de la ciudadanía para desarrollar su competencia digital, de modo que los ciudadanos puedan aprovechar las oportunidades que la transformación digital conlleva, así como afrontar sus desafíos y riesgos [3]. El "Marco Europeo de Competencias Digitales para los Ciudadanos (DigComp)" [4], elaborado por la Comisión Europea, tiene por objetivo ayudar a los Estados miembro a mejorar la competencia digital de sus ciudadanos a través de la educación.

A. Gordillo, Universidad Politécnica de Madrid, Madrid, España.
E. Barra, Universidad Politécnica de Madrid, Madrid, España.
P. Garaizar, Universidad de Deusto, Bilbao, España.
S. López-Pernas, Universidad Politécnica de Madrid, Madrid, España.

Pese a las acciones realizadas por diferentes organismos con el objetivo final de mejorar la competencia digital de los ciudadanos, ésta sigue siendo deficiente, lo cual provoca el riesgo de una nueva brecha digital, no originada por la falta de acceso a la tecnología, sino debida a un nivel insuficiente de competencia digital [5], [6]. Diversos estudios publicados en los últimos años han puesto de manifiesto que la competencia digital no se adquiere de forma inherente simplemente por utilizar la tecnología de manera habitual, sino que es imprescindible una formación específica para ello [6]–[8]. Por este motivo, si no se aborda el problema a través de acciones formativas efectivas, la brecha digital anteriormente mencionada podría afectar, no solamente a los adultos, sino también a los más jóvenes. Prueba de esto son los estudios que indican que los considerados "nativos digitales", a pesar de hacer un uso intensivo de la tecnología, presentan un nivel insuficiente de competencia digital [6], [9].

En vista de los hechos anteriores, resulta evidente la necesidad de formar a los alumnos para que estos adquieran la competencia digital de la que adolecen. Sin embargo, para que esta adquisición se convierta en una realidad, resulta imprescindible que los docentes tengan un nivel adecuado de competencia digital. Al utilizar los docentes las tecnologías de una forma específica y distinta al resto de áreas [10], ha surgido el término "competencia digital docente" para referenciar, de manera específica, al "conjunto de capacidades, conocimientos, habilidades, destrezas y actitudes en relación al uso crítico, seguro y creativo de las tecnologías de la información y comunicación en la docencia" [11]. Existen diferentes iniciativas destinadas a facilitar el desarrollo de la competencia digital docente [12]–[15]. Entre estas iniciativas cabe destacar, en el ámbito europeo, el "Marco Europeo para la competencia digital del profesorado (DigCompEdu)" [14] elaborado por la Comisión Europea, el cual define la competencia digital docente que deben tener los profesores a fin de lograr que los alumnos sean digitalmente competentes, así como, en el ámbito nacional español, el "Marco Común de Competencia Digital Docente" [15] publicado por el INTEF (Instituto Nacional de Tecnologías Educativas y de Formación del Profesorado).

A pesar de las diversas iniciativas que se han desarrollado en diferentes ámbitos a lo largo de los últimos años, existe una preocupante diferencia entre la competencia digital docente

que tienen actualmente los educadores y la que deberían tener para poder desarrollar de forma efectiva la competencia digital en sus estudiantes [7], [8], [16]–[21]. Este hecho evidencia la existencia de una necesidad apremiante de formación inicial y continua del profesorado en competencia digital docente.

Entre las diferentes áreas que engloba la competencia digital docente [13]–[15], la falta de formación del profesorado resulta particularmente relevante en el área relativa al uso seguro y responsable de la tecnología. Esta falta de formación ha sido puesta de manifiesto por diversos estudios [7], [17], [21]–[26], los cuales han reportado carencias de formación sobre diversos temas, incluyendo gestión de la privacidad, identidad digital, uso de redes sociales, riesgos de Internet para menores y normas de comportamiento en la red. Si además de estos datos tenemos en cuenta que los menores carecen de los conocimientos necesarios para hacer un uso seguro y responsable de la tecnología [27]–[30] y que no son plenamente conscientes de todos los riesgos asociados al uso de Internet [28], [29], podemos considerar esta deficiencia formativa del profesorado como un grave problema que debe ser abordado urgentemente. Además, como indica [21], para la adquisición de la competencia asociada al área de seguridad de la competencia digital docente, el papel del profesor cobra un especial protagonismo, ya que su figura es modelo y guía que cuida, orienta y forma a los alumnos sobre cómo hacer un uso seguro y responsable en la navegación, comunicación y compartición de información en Internet.

Un tema de los englobados por el uso seguro y responsable de la tecnología al que debe dedicarse especial atención son las redes sociales, ya que su uso entraña riesgos de privacidad y seguridad, así como riesgos emocionales [31]. La conveniencia de esta atención se vuelve todavía más clara si tenemos en consideración que, por término medio, el 45% de los menores tiene al menos un perfil en una red social, ascendiendo este porcentaje al 83% entre los adolescentes más mayores [32]. Además, los controles de privacidad para redes sociales son poco utilizados en la práctica a pesar de su importancia [33] y, en ocasiones, éstos no permiten a los usuarios reflejar fielmente sus relaciones sociales reales [34].

Con el objetivo de formar a los docentes para que desarrollen su competencia digital de forma efectiva, se deben emprender nuevas acciones formativas, así como utilizar nuevos recursos y herramientas educativas que puedan ser útiles para esta labor. Actualmente, no existen muchos estudios en la literatura que hayan reportado experiencias, métodos o herramientas destinadas a la mejora de la competencia digital docente del profesorado en el área relativa al uso seguro y responsable de la tecnología. Uno de estos estudios [35] analizó tres cursos en línea con formato MOOC (Massive Open Online Course) y concluyó que este tipo de cursos constituyen una forma efectiva de formar al profesorado en el uso seguro y responsable de las tecnologías de la información y la comunicación. Otro estudio similar [36], que también arrojó resultados positivos, analizó un curso semipresencial sobre seguridad en Internet para profesores en el que éstos combinaron clases de expertos en la materia con sesiones prácticas en las que utilizaron una herramienta de autor para crear unidades didácticas. Asimismo, [37] reporta una experiencia en la que se utilizó con éxito la metodología de aula invertida para desarrollar en profesores en formación la competencia digital docente en materias como el uso de redes sociales y la elaboración de materiales digitales. En la experiencia reportada por [26], un grupo de futuros profesores realizaron, como parte de su formación académica presencial, actividades para desarrollar sus conocimientos sobre uso seguro de las tecnologías de la información y la comunicación, así como sobre derechos de autor, obteniendo resultados muy positivos en cuanto al aumento de la concienciación. Por otro lado, [38] presentó una evaluación muy positiva de dos recursos educativos digitales que habían sido utilizados por profesores en un curso en línea para aprender a identificar, respectivamente, sitios web fraudulentos y noticias falsas.

Una tendencia creciente en la enseñanza acerca del uso seguro y responsable de la tecnología es el aprendizaje basado en actividades gamificadas. Fatima y otros [39] reportaron una experiencia exitosa en la que se utilizó un juego de mesa para enseñar a estudiantes universitarios sobre *phishing* y los peligros asociados con la divulgación excesiva de contenidos en Internet. En [40] se utilizó con éxito una escape room educativa para crear conciencia acerca de la seguridad informática y de los peligros de Internet entre estudiantes de distintos niveles y profesionales de diversos ámbitos. En otro estudio [41], se comparó la efectividad instruccional en alumnos universitarios de un videojuego y de un video de concienciación sobre la seguridad de la información, concluyendo que jugar al videojuego no sólo resultaba en un mayor grado de aprendizaje, sino también en un nivel de satisfacción más elevado. Resultados consistentes con este estudio fueron obtenidos en educación primaria por [42], quienes encontraron que los alumnos aprendieron conceptos de ciberseguridad de forma más efectiva mediante juegos que mediante la lectura de materiales tradicionales o la interacción con un tutorial digital con preguntas de autoevaluación. Los autores de [43] también alcanzaron conclusiones similares al comprobar que jugar a un juego sobre suplantación de identidad y otros peligros de Internet era, entre usuarios no expertos, más efectivo que otro tipo de estrategias de aprendizaje como la lectura de material educativo o la realización de tutoriales. Adicionalmente, en el estudio realizado por [44], se analizaron seis juegos serios de distintos géneros para enseñar varios aspectos avanzados de la seguridad de la información a estudiantes universitarios, concluyendo que los juegos desarrollados fueron efectivos para este propósito. En esta misma línea, [45] describe un juego serio para concienciar a los usuarios más jóvenes acerca de la privacidad en Facebook. Para aprender acerca de los riesgos de privacidad que entraña el uso de redes sociales, los autores de [46] desarrollaron una versión simplificada de la red social Facebook y evaluaron su uso por parte de cientos de alumnos de secundaria durante varios años, concluyendo que

el uso de esta plataforma incrementó su sensibilización acerca de la importancia de la privacidad y la seguridad en la red. De manera similar, [47] evaluaron el uso de una aplicación web llamada Social4School que simula la dinámica de la propagación de la información en las redes sociales, consiguiendo concienciar con éxito a alumnos de primaria sobre la importancia de una correcta configuración de privacidad. Los estudios citados en este párrafo reportan experiencias de aprendizaje, basadas en juegos u otro tipo de actividades gamificadas, que abordan algún tema relacionado con el uso seguro y responsable de la tecnología. Cabe destacar que en ninguno de estos estudios se ha evaluado la efectividad de la actividad para la formación docente, sino su efectividad para alumnos o usuarios inexpertos en general.

En base a todos los hechos expuestos anteriormente, queda manifiestamente claro que se necesita más investigación sobre el uso de acciones formativas, métodos y herramientas para mejorar la competencia digital de los docentes relacionada con la seguridad y el uso responsable de la tecnología.

Este estudio examina la utilización, en un curso en línea con formato MOOC, de una red social simulada llamada “Social Lab” como herramienta educativa para mejorar la competencia digital docente de los profesores en el área de uso seguro y responsable de la tecnología. Aunque estudios anteriores describen como Social Lab ha sido utilizado para ofrecer un juego de guerra de ingeniería social para aprender sobre privacidad [48]–[50], este es el primer estudio en el que se reporta una evaluación de la utilidad de Social Lab como herramienta educativa.

El resto del artículo se estructura de la siguiente forma. La siguiente sección proporciona una descripción general de Social Lab, la red social simulada evaluada en este estudio, incluyendo información sobre cómo esta herramienta puede ser utilizada con fines educativos. La sección 3 describe el método de la investigación. La sección 4 presenta los resultados de la evaluación realizada. Finalmente, la última sección discute los resultados, resume las conclusiones del estudio y sugiere algunas líneas futuras de investigación.

II. SOCIAL LAB

A. *Descripción general*

Social Lab es un sistema software de código abierto, gratuito y basado en web que simula una red social [49]. Desde el punto de vista de un usuario o jugador, Social Lab replica las funcionalidades de una red social básica para proporcionar un "cajón de arena” social, un lugar acotado y seguro donde experimentar. Una vez dados de alta, los usuarios pueden hacer uso de un amplio número de funcionalidades tales como modificar su información de perfil (nombre, apellidos, género, cumpleaños, localización, información académica, etc.), actualizar su estado en su muro, escribir en el muro de sus amigos, gestionar solicitudes de amistad, escribir y recibir mensajes privados, compartir fotos y etiquetar a amigos en ellas, crear páginas de intereses y hacerse fan de páginas existentes, o visualizar perfiles de otros usuarios (en función de sus configuraciones de privacidad). Todos los usuarios que estén en un mismo servidor de Social Lab podrán interactuar y relacionarse entre ellos de todas las formas descritas anteriormente.

Sin embargo, lo realmente interesante de Social Lab no son sus funcionalidades de red social sino la presencia de “bots sociales”. En Social Lab, los bots sociales son cuentas de usuario normales que tienen asociadas tareas programadas. Gracias a ellos es posible, para los administradores del servidor, tanto crear una cuenta de usuario que puede ser gestionada automáticamente a través de un programa, como simultanear acciones manuales y automáticas desde una misma cuenta. El comportamiento de los bots sociales se define a través de una secuencia de pasos, que pueden ser de dos tipos: acciones y comprobaciones. Las acciones (por ejemplo: mandar mensaje, aceptar amistad, etc.) se ejecutan en el orden que tienen asignado y siempre pasan a la siguiente acción definida en el comportamiento del bot social al finalizar. Las comprobaciones (por ejemplo, comprobar si alguien es amigo de dos de mis amigos o si algún dato del perfil de dos usuarios coincide), por contra, se evalúan en el orden que tienen asignado, pero no permiten pasar al siguiente paso a no ser que se haya cumplido su condición asociada. Gracias a ambos tipos de acciones, podemos definir una interacción social simulada entre bots sociales y usuarios reales de manera sencilla. Los bots sociales guardan el estado de cada interacción con cada usuario. Así, pueden estar ejecutando el paso 1 de su comportamiento programado con un usuario A y al mismo tiempo ejecutar el paso 3 con un usuario B. Cuando un bot haya ejecutado todos los pasos de su comportamiento para una interacción con un usuario dado, esta interacción finalizará. Sin embargo, las interacciones con otros usuarios seguirán su curso en el estado en el que estuvieran.

La siguiente sección describe como Social Lab puede ser utilizado como herramienta educativa para mejorar el aprendizaje en temas como gestión de la privacidad, identidad digital y prevención de riesgos derivados del uso de Internet. Información sobre cómo Social Lab puede ser utilizado con fines de investigación en relación al uso de redes sociales puede encontrarse en [48], [49].

B. *Adaptación como herramienta educativa*

Gracias a las funcionalidades de Social Lab (descritas en la sección anterior), se ha diseñado y desplegado un *wargame* de ingeniería social dentro de esta red social simulada. Un *wargame*, en el contexto de la informática, es un juego relacionado con la seguridad informática en el que es necesario ir resolviendo una sucesión escalonada de desafíos que requieren emplear técnicas de hacking para superarlos. En este sentido, Social Lab exige desplegar diferentes técnicas de ingeniería social para superar una serie de retos propuestos a los usuarios. Cuando hablamos de ingeniería social, nos referimos al “arte de influir en las personas para que divulguen información sensible o confidencial” y cuando utilizamos el término “ataque de ingeniería social” nos referimos a cualquier proceso realizado con este fin [51].

Son varias las razones que motivaron abordar el problema de la alfabetización en privacidad en redes sociales desde una perspectiva tan rompedora. En primer lugar, reconocemos que enseñar privacidad es una tarea difícil puesto que va en contra de la experiencia de usuario en una plataforma social. Todas las medidas encaminadas a preservar la privacidad del usuario suponen una merma en la funcionalidad de la red social y por lo tanto son percibidas como aburridas o molestas por los usuarios [52]. En segundo lugar, los materiales que enfocan esta alfabetización desde un punto de vista lúdico y práctico son escasos, y generalmente no están diseñados o no son apropiados para docentes. Estas son las razones que propiciaron el desarrollo del *wargame* de Social Lab a fin de ofrecer un juego práctico, interactivo y social en el que sus jugadores puedan conocer en primera persona qué técnicas de ingeniería social se pueden emplear para ganarse la confianza de otros usuarios. De esta forma, al igual que ocurre en los cursos de formación sobre hacking ético, será más fácil que estos usuarios identifiquen las situaciones en las que usuarios malintencionados usen esas mismas técnicas sobre ellos en redes sociales reales. El objetivo final de este uso educativo de Social Lab es múltiple. Por un lado, mostrar de manera práctica a los usuarios diferentes técnicas de ingeniería social utilizadas por hackers, de modo que estos usuarios sean capaces en un futuro de prevenir este tipo de ataques en redes sociales reales. Por otro lado, aumentar la concienciación sobre la importancia de prestar atención y dedicar tiempo a una adecuada configuración de la privacidad en las aplicaciones y servicios que utilizamos en Internet, especialmente en redes sociales. De este modo, los profesores que utilicen Social Lab estarán mejor preparados para enfrentar riesgos derivados del uso de Internet tales como la suplantación de identidad, la pérdida de privacidad, el *grooming*, el *sexting*, el ciberacoso y la sobreexposición de información personal, así como para formar a sus estudiantes en estas materias.

Para participar en el *wargame* ofrecido por Social Lab es necesario crear una cuenta de usuario en el servidor de Social Lab. Una vez hecho esto, basta con recordar nuestro nombre de usuario y contraseña para poder continuar el juego en el estado en el que lo dejamos la última vez tantas veces como sea necesario y desde el dispositivo que deseemos. Tras rellenar cierta información básica en nuestro perfil (que no tiene por qué ser real), podremos utilizar todas las funcionalidades de Social Lab. El primer mensaje privado que un jugador recibe al crearse una cuenta proviene de la propia red Social Lab e indica cuál es el primer reto de hacking social al que tendrá que hacer frente. De la misma forma, tras resolver cada uno de los retos, la propia red Social Lab irá indicando los siguientes objetivos, además de incluir un consejo sobre cómo aprovechar lo aprendido en el último reto resuelto en el uso de redes sociales reales por parte del jugador, ya que éste es el objetivo final del juego.

Para superar cada uno de los retos, el jugador deberá conseguir hacerse amigo de un usuario concreto de la red Social Lab. Cada uno de estos usuarios asociados a un reto está controlado por un bot social. Por ejemplo, el primer reto consiste en conseguir que Alice Johnson nos acepte como amigos en la red social. Este perfil está controlado por un bot social que siempre acepta a todo el mundo por lo que resulta muy fácil lograrlo. En el segundo desafío, la interacción es un poco más complicada ya que requiere que modifiquemos la información de nuestro perfil para hacernos pasar por alguien que vive en el mismo lugar que la persona a la que queremos convencer de que acepte nuestra amistad. Como vemos, el primer reto sirve para enseñar a los participantes que no tienen que aceptar todas las solicitudes de amistad en redes sociales, mientras que el segundo reto va un poco más allá al sugerir que debemos ser selectivos incluso con perfiles que puedan resultarnos cercanos porque viven en nuestra misma localidad o comparten una afición con nosotros.

El *wargame* de Social Lab proporciona un total de 10 retos, que deben resolverse en orden secuencial y que están dispuestos en un orden creciente de dificultad. Para superar todos los retos, los jugadores deberán ponerse en la piel de un hacker social y ejecutar las fases que componen un ataque de ingeniería social hasta el establecimiento de la relación con los diferentes usuarios de la red social controlados por bots. Un ataque de ingeniería social está compuesto por las siguientes fases: formulación del ataque, recolección de información de la víctima, preparación del ataque, desarrollo de la relación, explotación de la relación y recapitulación [53]. En el *wargame* de Social Lab, los jugadores ejecutan todas las fases a excepción de las dos últimas, dejando fuera la explotación de la relación, fase en la cual el hacker social sacaría partido de la relación establecida para obtener información sensible o confidencial.

La utilización de Social Lab como herramienta educativa en un curso en línea con formato MOOC requirió de la realización de varias tareas. La primera de estas tareas consistió en modificar la aplicación Social Lab para hacer posible su incorporación en cursos como una tarea evaluable. Esta modificación fue posible gracias a que Social Lab es software libre y su código fuente se encuentra disponible en https://github.com/txipi/Social-Lab. La versión adaptada de Social Lab que hemos desarrollado también es software libre y su código fuente se encuentra publicado en el siguiente repositorio: https://github.com/ging/Social-Lab. En esta nueva versión de Social Lab, cuando un jugador supera un reto del *wargame*, además de recibir un consejo sobre cómo aprovechar lo aprendido durante este reto en redes sociales reales, también recibe un mensaje privado con un código personalizado. De esta manera, se puede crear una actividad evaluable en el entorno virtual de aprendizaje utilizado en el curso, la cual reciba como dato de entrada este código y dé como resultado una calificación para el jugador. La idea es que cada participante del curso introduzca en esta actividad evaluable el código correspondiente al reto más avanzado al que haya llegado. De este modo, se le puede conceder una calificación diferente a los participantes en función del nivel

de Social Lab que han conseguido superar. En la experiencia reportada en este estudio, utilizamos la plataforma Moodle como entorno virtual de aprendizaje y su módulo "Tarea" para incorporar Social Lab como actividad evaluable. Además de modificar Social Lab para proporcionar códigos personalizados a los jugadores cuando superan retos, también se realizaron cambios en la interfaz gráfica y en la información proporcionada por el portal web para mejorar la integración visual de la herramienta y facilitar su uso por parte de los participantes del curso. La Fig. 1 muestra la página de amigos de un usuario en la nueva versión de Social Lab.

La segunda tarea fue desplegar una instancia autónoma de la nueva versión de Social Lab en un servidor dedicado (disponible en http://sociallab.dit.upm.es de forma pública) y dotar a dicha instancia de las características técnicas necesarias para soportar una gran cantidad de interacciones simultáneas de tal modo que ésta pudiese ser utilizada en cursos con formato MOOC, los cuales pueden y suelen tener un número de alumnos inscritos muy elevado.

Por último, para utilizar Social Lab como herramienta educativa en un curso en línea con formato MOOC, se debe incluir la descripción e instrucciones de la actividad en el entorno virtual de aprendizaje. Además, aunque Social Lab proporciona a los jugadores algunas pistas de forma automática, creemos que resulta conveniente, en un entorno no presencial y sin orientación personalizada como son los cursos con formato MOOC, proporcionar a los jugadores un mecanismo de soporte para esta actividad. En la experiencia que reportamos en este artículo, la descripción e instrucciones de la actividad fueron proporcionadas mediante una lección de Moodle y, como soporte adicional, utilizamos el foro virtual del curso, habilitando un hilo concreto donde los participantes se ayudaron entre sí y en el que, ocasionalmente, también participaron los dinamizadores del curso. En la siguiente sección se incluye más información acerca del uso que hicimos de Social Lab en esta experiencia.

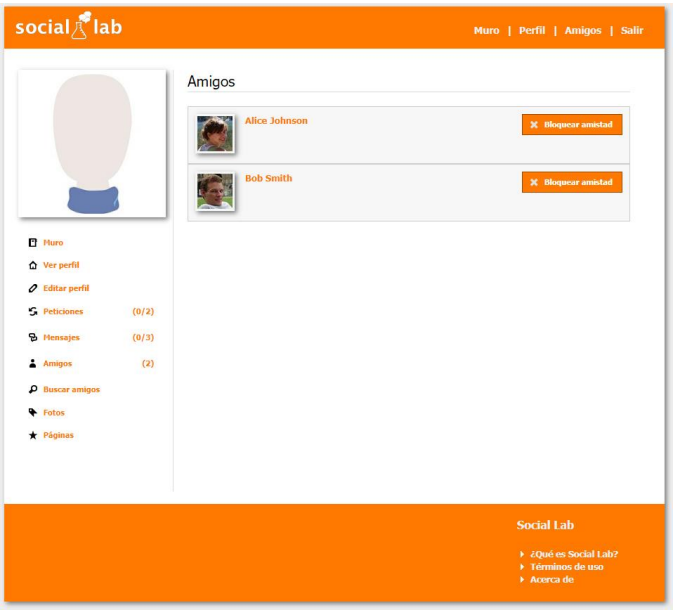

Fig. 1. Interfaz de la herramienta Social Lab (Página de amigos).

III. MÉTODO DE LA INVESTIGACIÓN

El objetivo de este estudio es examinar la utilidad de la red social simulada Social Lab como herramienta educativa para mejorar la competencia digital docente de los profesores en el área de uso seguro y responsable de la tecnología. De este modo, el estudio pretende esclarecer si este tipo de herramientas pueden resultar de ayuda para paliar la actual carencia de formación del profesorado en esta área de la competencia digital docente. Concretamente, el estudio pretende examinar si Social Lab es útil para permitir a los docentes mejorar sus conocimientos sobre ingeniería social y aumentar su preparación para prevenir ataques en redes sociales, así como para hacerles más conscientes de los riesgos asociados al uso de Internet.

En este estudio se ha utilizado una metodología de carácter cuantitativo basada en la aplicación y análisis de un cuestionario anónimo elaborado *ad hoc* para la investigación. El cuestionario estaba formado por preguntas para recopilar datos demográficos (edad y sexo), una pregunta sobre el nivel de competencia digital del encuestado, 11 preguntas tipo Likert con cinco opciones de respuesta (1 totalmente en desacuerdo – 5 totalmente de acuerdo), una pregunta cerrada en la que se pedía a los participantes que indicasen si recomendarían la herramienta Social Lab y, por último, una pregunta abierta en la que los encuestados pudieron indicar libremente comentarios y sugerencias de mejora. Las preguntas tipo Likert se incluyen en la sección IV. La fiabilidad de este cuestionario se evaluó mediante el cálculo del alfa de Cronbach [54], obteniendo un valor de α=0,97, lo cual indica una consistencia interna muy alta y aceptable. El cuestionario fue completado por un total de 70 profesores de primaria y secundaria inscritos en un curso en línea con formato MOOC sobre seguridad, privacidad e identidad digital en el entorno escolar. De estos 70 profesores, de entre 24 y 59 años de edad (M=42,6; DE=7,9), 22 (31,4 %) eran hombres y 48 (68,6 %) mujeres. Cuando fueron preguntados por su nivel de competencia digital, en torno a un 61% declaró tener un nivel alto o medio-alto, un 31% un nivel moderado y un 7% un nivel bajo o muy bajo.

El curso en el que estaban matriculados los profesores participantes en este estudio era un curso de carácter oficial organizado por la Consejería de Educación de la comunidad autónoma española de Castilla y León. Las principales características del curso se resumen en la Tabla 1. Los contenidos del curso están basados en el área de seguridad del "Marco Común de Competencia Digital Docente" [15] elaborado por el INTEF y abarcan temas como protección de dispositivos y contenidos digitales, privacidad, protección de datos personales, identidad digital, prevención de riesgos relacionados con el uso de la tecnología, buenas prácticas para el uso de redes sociales, netiqueta (normas de comportamiento en Internet) y protección de la salud y el bienestar. La impartición del curso se llevó a cabo a través de un entorno virtual de aprendizaje utilizando la plataforma Moodle.

TABLA I
CARACTERÍSTICAS DEL CURSO CON FORMATO MOOC

Perfil de los participantes	Docentes de centros sostenidos con fondos públicos de enseñanza no universitaria de la Comunidad de Castilla y León
Fecha de inicio	Febrero 2020
Duración	10 semanas
Dedicación estimada	30 horas
Certificación	3 créditos
Participantes inscritos	176
Tasa de finalización	61% (107 participantes)

La herramienta Social Lab fue utilizada en el curso para el desarrollo de una actividad de tipo "role-playing" (juego de roles), en la que los participantes tuvieron que superar diferentes retos tras ponerse en la piel de un hacker social, es decir, en la piel de una persona que tenía por objetivo conseguir datos personales de terceros (usuarios ficticios de Social Lab controlados por bots) empleando técnicas de ingeniería social. Esta actividad tenía carácter obligatorio, aunque para completar el curso los participantes solo debían superar los primeros retos, es decir, los de menor dificultad. Para la realización de la actividad, los participantes primero se registraron en la instancia de Social Lab habilitada para el curso disponible en http://sociallab.dit.upm.es (pudiendo utilizar datos falsos para este registro). Después, los participantes fueron completando retos en Social Lab hasta superarlos todos o, como mínimo, hasta superar los retos correspondientes a los primeros niveles. Por último, cada participante introdujo en la tarea de Moodle asociada a la actividad el código correspondiente al nivel más alto al que había llegado y, de este modo, obtuvo la calificación correspondiente. El cuestionario utilizado como instrumento de recolección de datos en este estudio fue completado por cada participante tras la utilización de la herramienta Social Lab y la finalización de la actividad del curso correspondiente.

IV. RESULTADOS

La Tabla 2 muestra los resultados del cuestionario sobre Social Lab completado por 70 profesores que finalizaron el curso con formato MOOC en el que se usó esta herramienta.

La opinión general sobre Social Lab alcanzó una valoración de media de 3,7 en una escala de 1 a 5, indicando que, en general, los profesores estuvieron satisfechos con el uso de Social Lab como herramienta educativa y que ésta tuvo un grado de aceptación satisfactorio. Otra muestra de este elevado grado de aceptación es que un 84% de los profesores encuestados indicó que recomendaría Social Lab a otras personas a fin de mejorar su competencia digital.

En cuanto a la usabilidad de Social Lab desde el punto de vista de los usuarios finales, la inmensa mayoría de profesores (entorno a un 90%) indicaron que esta herramienta fue fácil de utilizar (M=3,7; DE=1,1). No obstante, si bien la dificultad de los primeros retos fue considerada, en general, asequible (M=3,5; DE=1,1), el consenso fue notablemente menor con respecto a la dificultad de los últimos retos (M=3,1; DE=1,2). Prueba de ello es que solamente 54 (77%) de los profesores encuestados afirmó haber completado estos retos, y que en torno a 1 de cada 4 de ellos indicó que éstos eran demasiado complicados. Los comentarios facilitados en la pregunta abierta del cuestionario ratificaron la percepción de esta dificultad por parte de los participantes. Estos datos indican que para utilizar Social Lab como herramienta educativa en entornos donde los estudiantes reciben poca orientación, como es el caso de los cursos en línea con formato MOOC, resulta recomendable proporcionar ayuda adicional a fin de permitir a los participantes superar todos los retos. En el curso objeto de este estudio, se utilizó el foro como mecanismo de ayuda y resolución de dudas. No obstante, los datos obtenidos indican que resultaría recomendable incrementar, para los últimos niveles, las ayudas y consejos proporcionados a los usuarios automáticamente por Social Lab.

TABLA II
RESULTADOS DEL CUESTIONARIO SOBRE SOCIAL LAB

	N	M	DE
Mi opinión general sobre Social Lab es positiva	70	3,7	1,0
Social Lab es fácil de utilizar	70	3,7	1,1
Utilizar Social Lab ha sido divertido	70	3,7	1,1
Social Lab me ha permitido mejorar mis conocimientos sobre ingeniería social	70	3,7	1,2
Social Lab me ha permitido estar mejor preparado para prevenir ataques de ingeniería social en redes sociales	70	3,6	1,2
Social Lab me ha hecho más consciente de los riesgos de Internet	70	3,7	1,3
En general, Social Lab me ha permitido mejorar mi competencia digital	70	3,5	1,2
La dificultad de los primeros niveles (1-5) es asequible	70	3,5	1,1
La dificultad de los últimos niveles (del 6 en adelante) es asequible	54	3,1	1,2
Me gustaría que mis alumnos utilizaran Social Lab para desarrollar su competencia digital	70	3,7	1,2
Me gustaría que Social Lab formase parte de los planes de estudios como herramienta educativa	70	3,6	1,4
¿Recomendaría la herramienta Social Lab a otras personas?	N	Si	No
	70	84%	16%

En cuanto a la efectividad instruccional de la herramienta Social Lab, los profesores encuestados indicaron, en términos generales, que Social Lab les permitió mejorar su competencia digital (M=3,5; DE=1,2), concretamente permitiéndoles mejorar sus conocimientos sobre ingeniería social (M=3,7; DE=1,2), su preparación para prevenir ataques de ingeniería social en redes sociales reales (M=3,6; DE=1,2) y su entendimiento de los diferentes riesgos asociados al uso de Internet (M=3,7; DE=1,3). Además de considerar Social Lab una herramienta útil para la formación en el área de uso seguro y responsable de la tecnología de la competencia digital docente, los profesores que utilizaron Social Lab indicaron que el aprendizaje mediante esta herramienta fue divertido (M=3,7; DE=1,1).

Por último, los profesores que participaron en este estudio manifestaron mayoritariamente, a través del cuestionario, que

les gustaría que Social Lab fuese empleado por sus alumnos para que éstos desarrollasen su competencia digital (M=3,7; DE=1,2), así como que les gustaría que esta herramienta formase parte de los planes de estudios de educación primaria y secundaria (M=3,6; DE=1,4).

En relación a los comentarios proporcionados por los profesores a través de la encuesta, la sugerencia de mejora más recurrente fue la de que Social Lab proporcionase pistas adicionales a los jugadores cuando éstos se atascasen en un reto, algo que ocurre con relativa frecuencia, especialmente en los últimos, los cuales tienen una dificultad elevada para un porcentaje significativo de usuarios. Algún participante sugirió también que las respuestas a las solicitudes de amistad de los contactos ficticios de Social Lab fuesen inmediatas, aun a costa de una pérdida de realismo en el entorno simulado.

Al comparar los resultados proporcionados por los profesores con un mayor nivel declarado de competencia digital con aquellos proporcionados por el resto de participantes, se encontraron diferencias estadísticamente significativas (p-valor < 0.05) con un tamaño de efecto medio de acuerdo a Cohen [55] (con valores de la d de Cohen de 0,5 y 0,6) en el ítem de opinión general sobre Social Lab y en los dos ítems relacionados con la dificultad. Estos datos revelan que aquellos usuarios con menor competencia digital tuvieron más dificultades para superar los distintos retos propuestos por Social Lab y que la opinión general de estos usuarios acerca de la herramienta fue algo menos positiva que la del resto (M=3,4; DE=1,0 versus M=3,9; DE=1,0). Por último, cabe destacar que no hay diferencias estadísticamente significativas en el resto de los ítems del cuestionario, lo que implica que Social Lab fue percibido como fácil de usar, divertido y beneficioso para la formación en el área de seguridad de la competencia digital docente por todos los participantes, con independencia de su nivel de competencia digital.

V. DISCUSIÓN Y CONCLUSIONES

Los resultados obtenidos en este estudio muestran que la red social simulada Social Lab es una herramienta útil para la mejora de la competencia digital docente de los profesores en el área de la seguridad y el uso responsable de la tecnología. En base a estos resultados, resulta posible aseverar que Social Lab puede ser utilizado como herramienta educativa en diferentes entornos educativos, incluso en aquellos en los que los participantes no reciben una orientación personalizada como los cursos en línea con formato MOOC, a fin de contribuir a paliar la preocupante falta de conocimientos del profesorado en el área de la competencia digital asociada al uso seguro y responsable de la tecnología. Concretamente, este estudio proporciona evidencia de que Social Lab es percibida por los docentes como una herramienta entretenida, fácil de usar y útil para aprender sobre ingeniería social, prevenir ataques de ingeniería social en redes sociales e incrementar los conocimientos respecto a los diferentes riesgos existentes asociados al uso de Internet.

Los cursos en línea con formato MOOC tienen unas características propicias para posibilitar una solución para la formación inicial y continua de todos los docentes en competencia digital que sea efectiva, económica y fácilmente viable. Una investigación reciente ha proporcionado una fuerte evidencia de que este tipo de cursos constituyen una forma efectiva de formar al profesorado en el uso seguro y responsable de la tecnología [35]. Este estudio complementa los resultados de esta investigación, aportando evidencia de que el uso de herramientas educativas como Social Lab en estos cursos resulta beneficioso para el aprendizaje de los participantes en temas como privacidad, ingeniería social, riesgos de Internet y uso adecuado de redes sociales, los cuales son temas abarcados por el área de seguridad y uso responsable de la tecnología de la competencia digital docente.

Los resultados obtenidos en este estudio también indican que existe margen de mejora en Social Lab en cuanto a su uso como herramienta educativa, específicamente en la calidad de la ayuda proporcionada de manera automática a los jugadores. Si bien es cierto que los resultados indican que la dificultad de los primeros retos es, en general, percibida como asequible por la mayoría de jugadores, las pistas proporcionadas por Social Lab para resolver los últimos retos pueden resultar insuficientes para un porcentaje significativo de ellos. Esto puede provocar, en ciertas ocasiones, que el jugador se atasque con un determinado reto, lo cual puede conducir, en algunos casos, a que éste se frustre y a que incluso termine abandonando la actividad. A fin de solventar este problema y mejorar Social Lab, tenemos planeado incorporar un sistema de solicitud automática de pistas basado en el uso de cuestionarios, el cual hemos aplicado previamente con éxito en escape rooms educativas [56], [57], otro tipo de actividades gamificadas. Básicamente, al utilizar este mecanismo de gestión de pistas, todo participante puede solicitar una nueva pista para el reto en el que se ha quedado atascado. Para conseguir la pista, el participante deberá superar un breve cuestionario de preguntas sobre la temática de la actividad (en el caso de Social Lab, serán preguntas sobre uso seguro y responsable de redes sociales, privacidad, ingeniería social y riesgos derivados del uso de redes sociales).

Una limitación de la investigación presentada en este artículo es que la evaluación de utilidad de Social Lab se basó exclusivamente en medidas reportadas por los propios participantes. Otra limitación es que no se comparó esta utilidad con la de formas alternativas de aprendizaje. Trabajos futuros podrían evitar estas limitaciones empleando diferentes métodos de investigación, por ejemplo, mediante experimentos de tipo prueba controlada aleatorizada que utilizaran pre-tests y post-tests.

En este estudio se ha analizado la utilidad de Social Lab como herramienta educativa para mejorar la competencia digital docente en el área de la seguridad y el uso responsable de la tecnología. De los resultados queda claro que la mayoría de los profesores son favorables a la utilización de Social Lab por parte de sus alumnos, así como a incorporar esta

herramienta en los planes de estudios. Por tanto, un trabajo futuro interesante y complementario a esta investigación sería la evaluación de la utilidad de Social Lab como herramienta educativa para mejorar, no ya la competencia digital de los profesores, sino la competencia digital de los alumnos.

AGRADECIMIENTOS

Este trabajo ha contado con el apoyo del Departamento de Ingeniería de Sistemas Telemáticos de la Universidad Politécnica de Madrid (España) y de la empresa Orange Espagne S.A. (España), a través del proyecto EducaInternet.

REFERENCIAS

[1] Ministerio de Educación Cultura y Deporte, "Orden ECD/65/2015." 2015.

[2] Diario Oficial de la Unión Europea, "Recomendación del Parlamento Europeo y del Consejo de 18 de diciembre de 2006 sobre las competencias clave para el aprendizaje permanente (2006/962/CE)." 2006.

[3] Comisión Europea, "Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre el Plan de Acción de Educación Digital." 2018.

[4] R. Vuorikari, Y. Punie, S. Carretero, and L. Van den Brande, "DigComp 2.0: The Digital Competence Framework for Citizens. Update Phase 1: The Conceptual Reference Model," *European Commission*. 2016, doi: 10.2791/11517.

[5] A. Van Deursen and J. Van Dijk, "Internet skills and the digital divide," *New Media Soc.*, vol. 13, no. 6, pp. 893–911, 2011, doi: 10.1177/1461444810386774.

[6] A. Pérez-Escoda, A. Castro-Zubizarreta, and M. Fandos-Igado, "Digital skills in the Z generation: Key questions for a curricular introduction in Primary School. [La competencia digital de la Generación Z: Claves para su introducción curricular en la Educación Primaria]," *Comunicar*, vol. 24, no. 49, pp. 71–79, 2016, doi: 10.3916/c49-2016-07.

[7] M. Napal, A. Peñalva-Vélez, and A. M. Mendióroz, "Development of Digital Competence in Secondary Education Teachers' Training," *Educ. Sci.*, vol. 8, no. 3, 2018, doi: 10.3390/educsci8030104.

[8] F.-J. Fernández-Cruz and M.-J. Fernández-Díaz, "Generation Z's teachers and their digital skills. [Los docentes de la generación Z y sus competencias digitales]," *Comunicar*, vol. 24, no. 46, pp. 97–105, 2016, doi: 10.3916/C46-2016-10.

[9] L. Johnson *et al.*, "Horizon Report Europe: 2014 Schools Edition," 2014.

[10] F. M. Røkenes and R. J. Krumsvik, "Development of Student Teachers' Digital Competence in Teacher Education - A Literature Review," *Nord. J. Digit. Lit.*, vol. 9, no. 4, pp. 250–280, 2014.

[11] INTEF, "Cinco años de evolución de la competencia digital docente." 2017.

[12] ISTE (International Society for Technology in Education), "NETS for Teachers: National Educational Technology Standards for Teachers," 2008. [Online]. Available: https://id.iste.org/docs/pdfs/nets-for-teachers-2008_spanish.pdf.

[13] UNESCO, "UNESCO ICT Competency Framework for Teachers." 2011.

[14] C. Redecker and Y. Punie, "European Framework for the Digital Competence of Educators: DigCompEdu." 2017, doi: 10.2760/159770.

[15] INTEF, "Marco Común de Competencia Digital Docente." 2017.

[16] G. Almerich, J. Suárez, J. Jornet, and M. Orellana, "Las competencias y el uso de las Tecnologías de Información y Comunicación (TIC) por el profesorado: estructura dimensional," *Rev. Electrónica Investig. Educ.*, vol. 13, no. 1, pp. 28–42, 2011.

[17] J. M. Falcó, "Evaluación de la competencia digital docente en la Comunidad Autónoma de Aragón," *Rev. electrónica Investig. Educ.*, vol. 19, no. 4, pp. 73–83, 2017, doi: 10.24320/redie.2017.19.4.1359.

[18] F.-J. Fernández-Cruz, M.-J. Fernández-Díaz, and J.-M. Rodríguez-Mantilla, "El proceso de integración y uso pedagógico de las TIC en los centros educativos madrileños," *Educ. XX1*, vol. 21, no. 2, pp. 395–416, 2018, doi: 10.5944/educXX1.17907.

[19] M.-T. Kaarakainen, O. Kivinen, and T. Vainio, "Performance-based testing for ICT skills assessing: a case study of students and teachers' ICT skills in Finnish schools," *Univers. Access Inf. Soc.*, vol. 17, no. 2, pp. 349–360, 2018, doi: 10.1007/s10209-017-0553-9.

[20] J. M. Suárez-Rodríguez, G. Almerich, I. Díaz-García, and R. Fernández-Piqueras, "Competencias del profesorado en las TIC. Influencia de factores personales y contextuales," *Univ. Psychol.*, vol. 11, no. 1, pp. 293–309, 2012.

[21] M.-J. Gallego Arrufat, N. Torres-Hernández, and T. Pessoa, "Competence of future teachers in the digital security area. [Competencia de futuros docentes en el área de seguridad digital]," *Comunicar*, vol. 27, no. 61, pp. 53–62, 2019, doi: 10.3916/C61-2019-05.

[22] B. De los Arcos *et al.*, "OER Data Report 2013-2015: Building Understanding of Open Education." 2015.

[23] I. Govender and B. Skea, "Teachers' understanding of E-safety: An exploratory case in KZN South Africa," *Electron. J. Inf. Syst. Dev. Ctries.*, vol. 70, no. 1, pp. 1–17, 2015, doi: 10.1002/j.1681-4835.2015.tb00505.x.

[24] L. Mannila, L.-Å. Nordén, and A. Pears, "Digital Competence, Teacher Self-Efficacy and Training Needs," in *Proceedings of the 2018 ACM Conference on International Computing Education Research (ICER '18)*, 2018, pp. 78–85, doi: 10.1145/3230977.3230993.

[25] P. Pusey and W. A. Sadera, "Cyberethics, Cybersafety, and Cybersecurity: Preservice Teacher Knowledge, Preparedness, and the Need for Teacher Education to Make a Difference," *J. Digit. Learn. Teach. Educ.*, vol. 28, no. 2, pp. 82–85, 2011, doi: 10.1080/21532974.2011.10784684.

[26] S.-K. Shin, "Teaching Critical, Ethical and Safe Use of ICT in Pre-Service Teacher Education," *Lang. Learn. Technol.*, vol. 19, no. 1, pp. 181–197, 2015, doi: 10125/44408.

[27] M. Sharples, R. Graber, C. Harrison, and K. Logan, "E-safety and Web 2.0 for children aged 11-16," *J. Comput. Assist. Learn.*, vol. 25, no. 1, pp. 70–84, 2009, doi: 10.1111/j.1365-2729.2008.00304.x.

[28] L.-A. Ey and C. G. Cupit, "Exploring young children's understanding of risks associated with internet usage and their concepts of management strategies," *J. Early Child. Res.*, vol. 9, no. 1, pp. 53–65, 2011, doi: 10.1177/1476718X10367471.

[29] R. Gamito, M. P. Aristizabal, M. T. Vizcarra, and A. Tresserras, "La relevancia de trabajar el uso crítico y seguro de Internet en el ámbito escolar como clave para fortalecer la competencia digital," *Fonseca, J. Commun.*, vol. 15, pp. 11–25, 2017, doi: 10.14201/fjc2017151125.

[30] P. Colás-Bravo, J. Conde-Jiménez, and T. González-Ramírez, "Spanish teachers' perception of their own and their students' digital competencies," in *Beliefs and Behaviours in Education and Culture: Cultural Determinants and Education*, M.-M. Crișan and R.-A. Toma, Eds. Editura Pro Universitaria, 2016, pp. 42–53.

[31] S. Livingstone and D. R. Brake, "On the rapid rise of social networking sites: New findings and policy implications," *Child. Soc.*, vol. 24, no. 1, pp. 75–83, 2009, doi: 10.1111/j.1099-0860.2009.00243.x.

[32] M. Garmendia, E. Jiménez, M. Á. Casado, and G. Marcheroni, "Net Children Go Mobile: Riesgos y oportunidades en internet y uso de dispositivos móviles entre menores españoles (2010-2015)." 2016.

[33] Y. Liu, K. P. Gummadi, B. Krishnamurthy, and A. Mislove, "Analyzing facebook privacy settings: User expectations vs. reality," in *Proceedings of the ACM SIGCOMM Internet Measurement Conference*, 2011, pp. 61–70, doi: 10.1145/2068816.2068823.

[34] G. Misra and J. M. Such, "How socially aware are social media privacy controls?," *IEEE Comput.*, vol. 49, no. 3, pp. 96–99, 2016, doi: 10.1109/MC.2016.83.

[35] A. Gordillo, S. López-Pernas, and E. Barra, "Effectiveness of MOOCs for teachers in safe ICT use training. [Efectividad de los MOOC para docentes en el uso seguro de las TIC]," *Comunicar*, vol. 27, no. 61, pp. 98–107, 2019, doi: 10.3916/C61-2019-09.

[36] A. Gordillo, E. Barra, and J. Quemada, "Learning by doing: an experience with a novel e-learning platform and a learning object authoring tool in a teachers' course about e-Safety," in *Proceedings of the 8th International Conference on Education and New Learning Technologies (EDULEARN 2016)*, 2016, pp. 4165–4175.

[37] M. J. Sosa and R. F. Palau, "Flipped classroom para adquirir la competencia digital docente: una experiencia didáctica en la Educación Superior," *Pixel-Bit. Rev. Medios y Educ.*, vol. 52, pp. 37–54, 2018, doi: 10.12795/pixelbit.2018.i52.03.

[38] A. Gordillo, S. López-Pernas, and E. Barra, "RESCORM: A boilerplate for creating SCORM-compliant React applications," in *Proceedings of the 11th International Conference of Education, Research and Innovation (ICERI 2018)*, 2018, pp. 8843–8853, doi: 10.21125/iceri.2018.0632.

[39] R. Fatima, A. Yasin, L. Liu, and J. Wang, "How persuasive is a phishing email? A phishing game for phishing awareness," *J. Comput. Secur.*, vol. 27, no. 6, pp. 581–612, 2019, doi: 10.3233/JCS-181253.

[40] E. Beguin *et al.*, "Computer-security-oriented escape room," *IEEE Secur. Priv.*, vol. 17, no. 4, pp. 78–83, 2019, doi: 10.1109/MSEC.2019.2912700.

[41] J. Jones, X. Yuan, E. Carr, and H. Yu, "A comparative study of CyberCIEGE game and department of defense information assurance awareness video," in *Proceedings of the IEEE SoutheastCon 2010*, 2010, pp. 176–180, doi: 10.1109/SECON.2010.5453895.

[42] B. T. Zahed, G. White, and J. Quarles, "Play it safe: An educational cyber safety game for children in elementary school," in *Proceedings of the 11th International Conference on Virtual Worlds and Games for Serious Applications (VS-Games)*, 2019, doi: 10.1109/VS-Games.2019.8864594.

[43] S. Sheng *et al.*, "Anti-Phishing Phil: The design and evaluation of a game that teaches people not to fall for phish," in *Proceedings of the 3rd Symposium on Usable Privacy and Security (SOUPS 2007)*, 2007, pp. 88–99, doi: 10.1145/1280680.1280692.

[44] M. Mostafa and O. S. Faragallah, "Development of Serious Games for Teaching Information Security Courses," *IEEE Access*, vol. 7, pp. 169293–169305, 2019, doi: 10.1109/ACCESS.2019.2955639.

[45] A. Cetto *et al.*, "Friend Inspector : A Serious Game to Enhance Privacy Awareness in Social Networks," in *Proceedings of the 2nd International Workshop on Intelligent Digital Games for Empowerment and Inclusion (IDGEI 2014)*, 2014.

[46] M. Zinkus, O. Curry, M. Moore, Z. Peterson, and Z. J. Wood, "Fakesbook A social networking platform for teaching security and privacy concepts to secondary school students," in *Proceedings of the 50th ACM Technical Symposium on Computer Science Education (SIGCSE 2019)*, 2019, pp. 892–898, doi: 10.1145/3287324.3287486.

[47] L. Bioglio, S. Capecchi, F. Peiretti, D. Sayed, A. Torasso, and R. G. Pensa, "A Social Network Simulation Game to Raise Awareness of Privacy among School Children," *IEEE Trans. Learn. Technol.*, vol. 12, no. 4, pp. 456–469, 2019, doi: 10.1109/TLT.2018.2881193.

[48] U. Reips and P. Garaizar, "Social Lab: An 'Open Source Facebook,'" in *The SAGE Handbook of Social Media Research Methods*, 2016, pp. 473–483.

[49] P. Garaizar and U. D. Reips, "Build your own social network laboratory with Social Lab: A tool for research in social media," *Behav. Res. Methods*, vol. 46, no. 2, pp. 430–438, 2014, doi: 10.3758/s13428-013-0385-3.

[50] J. Núñez, P. Garaizar, and U. Reips, "Online Workshop on Privacy using Social Lab, A Social Engineering Wargame," in *Proceedings of the 7th International Technology, Education and Development Conference (INTED 2013)*, 2013.

[51] F. Moutonab, L. Leenena, and H. S. Venterb, "Social engineering attack examples, templates and scenarios," *Comput. Secur.*, vol. 59, no. 186–209, 2016, doi: 10.1016/j.cose.2016.03.004.

[52] O. Edbrooke and M. L. Ambrose, "Teaching Privacy in the Twenty-First Century," *Soc. Educ.*, vol. 76, no. 4, pp. 217–220, 2012.

[53] F. Mouton, M. M. Malan, L. Leenen, and H. S. Venter, "Social engineering attack framework," in *Proceedings of the 2014 Information Security for South Africa Conference*, 2014, doi: 10.1109/ISSA.2014.6950510.

[54] L. J. Cronbach, "Coefficient alpha and the internal structure of tests," *Psychometrika*, vol. 16, no. 3, pp. 297–334, 1951, doi: 10.1007/BF02310555.

[55] J. Cohen, "A power primer," *Psychol. Bull.*, vol. 112, no. 1, pp. 155–159, 1992, doi: 10.1037/0033-2909.112.1.155.

[56] S. López-Pernas, A. Gordillo, E. Barra, and J. Quemada, "Examining the use of an educational escape room for teaching programming in a higher education setting," *IEEE Access*, vol. 7, pp. 31723–31737, 2019, doi: 10.1109/ACCESS.2019.2902976.

[57] S. Lopez-Pernas, A. Gordillo, E. Barra, and J. Quemada, "Analyzing Learning Effectiveness and Students' Perceptions of an Educational Escape Room in a Programming Course in Higher Education," *IEEE Access*, vol. 7, pp. 184221–184234, 2019, doi: 10.1109/ACCESS.2019.2960312.

Aldo Gordillo es Doctor en Ingeniería Telemática (2017) e Ingeniero de Telecomunicación (2012) por la Universidad Politécnica de Madrid (UPM). Ha trabajado como ingeniero de investigación y desarrollo en el Departamento de Ingeniería de Sistemas Telemáticos de la UPM (2012-2019). Actualmente trabaja como Profesor Ayudante Doctor en el Departamento de Sistemas Informáticos de la UPM. Sus intereses de investigación están en el campo del aprendizaje potenciado por la tecnología, con especial interés en creación, evaluación y distribución de objetos de aprendizaje, educación en ciencias de la computación, aprendizaje basado en juegos y sistemas de e-Learning.

Enrique Barra es Doctor en Ingeniería Telemática (2014) e Ingeniero de Telecomunicación (2006) por la UPM. Actualmente trabaja como Profesor Ayudante Doctor en el Departamento de Ingeniería de Sistemas Telemáticos de la UPM y está involucrado en varios proyectos contribuyendo al uso seguro y responsable de la tecnología. Sus intereses de investigación incluyen generación y distribución de contenidos educativos, juegos educativos, videoconferencia y redes sociales.

Pablo Garaizar es Doctor en Ingeniería Informática por la Universidad de Deusto y Licenciado en Psicología por la U.N.E.D. Trabaja como profesor-investigador en el Departamento de Tecnologías Informáticas, Electrónicas y de la Comunicación en la Facultad de Ingeniería de la Universidad de Deusto investigando sobre el desarrollo del Pensamiento Computacional dentro del Deusto LearningLab. Ha contribuido al desarrollo de apps educativas como Social Lab, Kodetu, Make World o Lempel y es autor de juegos de mesa educativos como Moon o Arqueras de Nand.

Sonsoles López-Pernas obtuvo el Grado en Ingeniería de Tecnologías y Servicios de Telecomunicación (2016) y el Máster Universitario en Ingeniería de Telecomunicación (2018) en la UPM. Actualmente, cursa sus estudios de doctorado en Ingeniería Telemática en la misma institución. Desde 2015 trabaja como investigadora en el Departamento de Ingeniería de Sistemas Telemáticos. Sus intereses de investigación incluyen el e-Learning y las analíticas en tiempo real, con especial énfasis en herramientas de autor, minería de datos en educación y escape rooms educativas.