

Percepciones y comportamientos de los estudiantes hacia el engaño en educación en línea

M. Elena Rodríguez, Ana-Elena Guerrero-Roldán, David Baneres, Ingrid Noguera

Title— Students' perceptions and behaviors toward cheating in online education

Abstract— Online education is pushing universities to search for technologies that can support e-assessment. Opinions and behaviors of stakeholders are required in order to develop such technologies. This paper underlines the need for mechanisms to prevent cheating and increase security, by analyzing the differences between students' perceptions of cheating and the acts of academic dishonesty they commit, contributing to fill a gap in the literature on cheating behaviors in online education. The research questions are: RQ1) Are students aware of what constitutes cheating in online education? RQ2) Do students believe that an e-authentication system may increase their security and prevent cheating? RQ3) Would the use of an e-authentication system for assessment increase students' trust? RQ4) What are students' real cheating behaviors? 154 students taking an online course from the Computer Engineering and Telecommunications degree consented to participate in the study. The research instruments were two surveys, and two tools of the course (an intelligent tutoring system and an image plagiarism detection tool). Results show that the fact students know an e-authentication and authoring system is used may prevent cheating and make students feel more confident. The findings have significant implications for institutions interested in e-assessment secure systems.

Index Terms— cheating, e-authentication, e-assessment, students' perceptions, students' behavior

I. INTRODUCCIÓN

La educación en línea constituye una solución prometedora para proporcionar flexibilidad y personalizar el proceso de enseñanza-aprendizaje, así como la evaluación. Algunos de los beneficios de la evaluación en línea (e-evaluación o *e-assessment*, por su término en inglés) son la flexibilidad que ofrece (en espacio y tiempo), la posibilidad de proporcionar retroalimentación (en inglés, *feedback*) inmediata, el hecho que puede estar

centrada en el estudiante y en un aprendizaje auténtico, y la fiabilidad [1]–[4]. Sin embargo, algunos aspectos negativos predecibles, como serían el aumento del fraude académico y los problemas de accesibilidad están bajo discusión [5]–[14]. Con independencia de las evidencias que las investigaciones muestran con respecto a la relación entre la educación en línea y la deshonestidad académica, el personal docente y los estudiantes aún creen que es más probable que ocurra en la educación en línea que en las formas de educación más tradicionales [15]–[18]. En consecuencia, la percepción de las posibilidades de engaño e incluso la concepción de lo que significa cometer actos de deshonestidad académica en el contexto digital también están afectando la educación universitaria en línea. Dada esta situación de desconfianza e inseguridad, el proyecto TeSLA (*An Adaptive Trust-Based e-Assessment System for Learning*), financiado por la Comisión Europea bajo el programa H2020) ha aprovechado el potencial de la tecnología para desarrollar un sistema adaptativo (llamado como el proyecto, TeSLA) basado en la confianza que incorpora mecanismos de seguridad para facilitar la evaluación en línea. El principal objetivo del proyecto ha sido desarrollar un sistema que permita verificar la identidad del estudiante y la autoría de las actividades de aprendizaje en línea. En otras palabras, que el o la estudiante que está detrás de la pantalla es quien dice ser, y que la actividad de aprendizaje que ha realizado, la ha hecho él o ella. Por lo tanto, el sistema creado permite verificar la autoría y la autenticación en entornos mixtos, a distancia y completamente en línea (o virtuales). El proyecto ha contado con la participación de 7 universidades (incluyendo universidades en línea y semipresenciales), 3 empresas, 4 centros de investigación especializados en técnicas de reconocimiento biométrico y 3 agencias de calidad. Durante el proyecto el sistema ha sido testeado en los 7 entornos de aprendizaje reales a través de diferentes pilotos en los que han participado estudiantes y profesores [19]–[21]. Este artículo se centra en los resultados obtenidos en una de las universidades participantes en el proyecto en el primero de los pilotos realizados, que justamente es una universidad totalmente virtual, tal y como se describe más adelante en la Sección III. Los mecanismos o instrumentos testeados han sido: reconocimiento facial (RF), reconocimiento de voz (RV), reconocimiento de patrones de teclado o *keystroke* (RPT), análisis forense o reconocimiento del estilo de escritura (AF) y plagio (PL). Para cada estudiante, se crea un modelo biométrico a partir de las denominadas

This work is supported by the European Union (H2020-ICT-2015) through the TeSLA project (An adaptive Trust-based e-assessment System for Learning). Number 688520.

M.E. Rodríguez, A.E. Guerrero-Roldán, D. Baneres are with the Faculty of Computer Science, Multimedia and Telecommunication, Universitat Oberta de Catalunya, Rambla del Poblenou 156, Barcelona 08018, España (mrodriguez, aguerrero, dbaneres}@uoc.edu)

I. Noguera is with the eLearn Center, Universitat Oberta de Catalunya, Rambla del Poblenou 156, Barcelona 08018, España (inoguerafr@uoc.edu).

actividades de registro (actividades con fines no evaluativos que sirven como registro de usuario) y que se utilizan como referencia en *actividades reales* (actividades de evaluación, es decir, tareas o trabajos en los que se aplican los mecanismos de seguridad para autenticar al estudiante y certificar que es el autor legítimo de la actividad). Los mecanismos de RF, RV y RPT se utilizan, respectivamente, para autenticar a los estudiantes al capturar imágenes de su rostro, muestras de su voz (audio) y sus patrones de teclado (es decir, el ritmo de escritura que sigue el estudiante cuando usa el teclado). Por otro lado, los mecanismos de AF y PL se utilizan para verificar la autoría al comparar el estilo de escritura y detectar similitudes entre los documentos de texto, respectivamente. El mecanismo de AF también se puede utilizar con fines de autenticación. Como los datos recopilados son confidenciales y altamente sensibles, todos los estudiantes que han aceptado participar en los pilotos han firmado un documento de consentimiento que les informaba sobre la protección de datos.

El objetivo de este trabajo es analizar las percepciones y comportamientos de los estudiantes hacia los actos de engaño cuando se utiliza un sistema de autenticación electrónica para facilitar la evaluación en la educación en línea. Las preguntas de investigación que este trabajo pretende responder son las siguientes:

- P1. ¿Son conscientes los estudiantes de lo que constituye cometer actos de engaño en la educación en línea?
- P2. ¿Creen los estudiantes que un sistema de autenticación en línea puede aumentar la seguridad y evitar cometer actos de engaño?
- P3. ¿El uso de un sistema de autenticación en línea para la evaluación aumentaría la confianza de los estudiantes?
- P4. ¿Cuáles son los comportamientos de engaño reales de los estudiantes?

Las tres primeras preguntas de investigación se refieren a las percepciones de los estudiantes sobre la realización de actos de engaño durante el proceso de evaluación, mientras que la cuarta pregunta de investigación aborda el comportamiento real de los estudiantes con respecto a dichos actos de engaño que atentan contra la integridad académica.

Este trabajo se organiza de la siguiente manera: el trabajo relacionado se presenta en la Sección II, mientras que la metodología seguida para realizar el estudio se describe en la Sección III. A continuación, los principales resultados para cada una de las preguntas de investigación formuladas se presentan en la Sección IV, y esos resultados se discuten en la Sección V. Seguidamente, las limitaciones del estudio y las conclusiones principales (así como las posibles líneas de trabajo futuro) se presentan en la Sección VI y la Sección VII, respectivamente.

II. TRABAJO RELACIONADO

El rápido crecimiento de la educación en línea plantea retos en los procesos de evaluación y especialmente, en la educación superior. La mayoría de iniciativas se centran en la virtualización de los exámenes, aunque la realización de pruebas de evaluación en línea es aún una práctica poco

frecuente en la educación universitaria en línea [22], [23]. La perpetuación de los exámenes tradicionales (realizados en papel) está íntimamente relacionada con la preocupación que existe acerca de la integridad académica de la educación en línea [24]–[27]. Para abordar este reto, un corpus creciente de literatura está explorando el uso de herramientas para identificar (es decir, autenticar) los estudiantes y demostrar la autoría de los trabajos que estos realizan. En el presente trabajo el término engaño se utiliza como un sinónimo de *deshonestidad académica*. Esto puede incluir, por ejemplo, cualquier intento deliberado de suplantar la identidad de una persona, falsificar datos, obtener ayuda no autorizada durante la realización de actividades de evaluación en línea, o plagiar (es decir, usar el trabajo, ideas o palabras de otros sin citarlos). En la literatura existen múltiples ejemplos de trabajos centrados en el engaño académico [32]–[37]. Una primera estrategia para abordar estos comportamientos ilegítimos es la utilización de mecanismos de seguridad como el análisis forense y las herramientas de detección de plagio. Una segunda estrategia, ampliamente usada en Europa [38], consiste en la realización de exámenes dentro de entornos controlados (es decir, supervisados) combinados con el uso de mecanismos biométricos. Trabajos recientes demuestran que estas estrategias pueden ayudar en la detección de conductas no deseadas [39]–[43]. Por otro lado, trabajos anteriores muestran que la realización de test de evaluación en línea en entornos no supervisados son más propensos al engaño que los test realizados en entornos controlados [27], [44], [45]. A este respecto, cuestionarios realizados a estudiantes de grado y máster revelan que los estudiantes consideran que el engaño es más sencillo en cursos en línea, puesto que no existe supervisión, y pueden, por ejemplo, tener acceso a múltiples recursos [46]. Sin embargo, en otro estudio, más de la mitad de los estudiantes consultados consideran que las situaciones de engaño ocurren con la misma frecuencia en la educación en línea y en la educación presencial. Asimismo, la mitad de ellos creen que ocurre con la misma frecuencia en exámenes supervisados y no supervisados [45]. A pesar de los presumibles beneficios de los exámenes supervisados, en la educación en línea se consideran bastante invasivos desde el punto de vista de la privacidad. Aunque el uso de mecanismos de seguridad y la creación de entornos supervisados puede ayudar a prevenir y detectar situaciones de engaño, la literatura sugiere una tercera estrategia que consiste en modificar las actitudes de los estudiantes hacia este tipo de comportamiento ilegítimo. Entre otras, estas estrategias incluyen informar a los estudiantes o exigir un acuerdo con respecto a un código de honor. Por ejemplo, en [47] se propone una intervención orientada a crear conciencia sobre aspectos relativos a la integridad académica. Como resultado, se observó una mejora en el conocimiento y un cambio en las actitudes de los estudiantes en relación a esta materia. En [48] los autores investigaron los efectos de los códigos de honor y el uso de avisos para reducir la tasa de engaño. Sus resultados sugieren que el uso de avisos pueden disuadir los actos de engaño en entornos de aprendizaje en línea. Estas iniciativas son relevantes porque existe una gran variabilidad en la comprensión de qué constituye un acto de engaño en cursos

en línea, lo cual puede desembocar en la comisión de actos de engaño de forma inconsciente. En un estudio previo [49] se discute que, de hecho, la frontera entre comportamientos adecuados y de engaño puede no estar clara o ser difusa, pudiéndose crear malentendidos. A modo de ejemplo, únicamente una minoría de los encuestados identificaron el auto plagio (reutilizar trabajo propio) como un comportamiento potencialmente punible. Evidencias más recientes [50] muestran que los estudiantes consideraron poco ético usar recursos externos cuando están realizando un examen final en línea, aunque consideraron aceptable y ético el uso de dichos recursos cuando estaban completando otras actividades de evaluación propuestas durante el curso. Los hallazgos presentados en [51] revelan que cerca del 27 % de los estudiantes (sobre una muestra de 300 estudiantes) no sabían que combinar diferentes fuentes de información de Internet para una actividad de evaluación sin citar a los autores de dichas fuentes era un acto de plagio. Además de los problemas de comprensión sobre qué constituye un acto de plagio, es poco frecuente que los estudiantes admitan haber engañado. Por ejemplo, en un estudio realizado por [52] en el que participaron 1.153 estudiantes, solo una minoría de estudiantes admitieron haber cometido prácticas de deshonestidad en entornos de aprendizaje en línea (en inglés, *e-dishonesty*). A pesar del volumen de participantes en dichos estudios, ninguno de ellos recoge el testeado de un sistema que contenga todos los instrumentos definidos anteriormente. En este trabajo se analizan las diferencias entre las percepciones de los estudiantes con respecto al engaño cuando se utiliza un sistema de autenticación y autoría como TeSLA en educación universitaria en línea, y los actos de deshonestidad académica que estos cometen.

III. METODOLOGÍA

Los participantes en el primer piloto del proyecto TeSLA en el caso de la Universitat Oberta de Catalunya (UOC) fueron estudiantes matriculados en la asignatura *Fundamentos de computadores*. Se trata de una asignatura obligatoria que se cursa en el primer curso académico, tanto en el Grado de Ingeniería Informática como en el Grado de Tecnologías de la Telecomunicación. La asignatura tiene como objetivo capacitar a los estudiantes para analizar y sintetizar circuitos digitales, y comprender la arquitectura informática subyacente. Destacar que la asignatura tradicionalmente tiene un número elevado de estudiantes matriculados y una tasa de rendimiento académico baja. Para muchos estudiantes, la asignatura es su primer contacto, no solo con los fundamentos teóricos de la educación en ingeniería, sino también con la educación en línea. Estas dos circunstancias típicamente causan una tasa de abandono alta (aproximadamente de un 49 %). El número de estudiantes matriculados en la asignatura en el semestre en el que el piloto tuvo lugar (curso académico 2016/2017) fue de 543 estudiantes. La muestra total de estudiantes que voluntariamente consintieron participar en el piloto fue de 154 estudiantes (11.4 % mujeres, 88.6 % hombres; edad media 34 años). El desequilibrio de género de la muestra es consistente con la presencia minoritaria de mujeres en los campos de Ciencia, Tecnología, Ingeniería y Matemáticas

(más conocidos por su acrónimo equivalente en inglés, STEM) [53], [54]. Por requisitos específicos del propio proyecto los estudiantes debían participar de forma voluntaria en el piloto. En otras palabras, en ningún caso era obligatorio formar parte del estudio, por diferentes motivos. En primer lugar, por cuestiones éticas para la investigación que tienen como objetivo evitar que los estudiantes sufran desigualdades dependiendo de su participación en el piloto. En segundo lugar, porque las normativas académicas aún no están preparadas para este tipo de sistemas, y por lo tanto, la globalidad de las sanciones académicas derivadas (por ejemplo, en el caso de aplicar RF, RV o RPT) no están definidas. En tercer lugar, el sistema TeSLA estaba en fase de desarrollo y, en consecuencia, no se trataba de un producto software acabado, hecho que podía ocasionar un sobreesfuerzo en su utilización por parte de los estudiantes. A nivel global del proyecto, en el primer piloto participaron 637 estudiantes de las 7 universidades, siendo la UOC una de las más numerosas en cuanto a participantes.

Como muestra la Figura 1, el piloto consistió en la realización de las actividades de registro que sirvieron para construir un perfil biométrico de cada estudiante para los instrumentos (RF, RV y RPT) en una instancia estándar de Moodle. El piloto también incluyó la realización de tres actividades de evaluación en línea auténticas (o reales) que incluyeron un vídeo corto donde se habilitaron los instrumentos de RF y RV, y un test de Moodle con el instrumento de RPT. Las actividades fueron las propias de la asignatura, pero se incorporaron estos instrumentos. Es decir, los estudiantes realizaron las actividades de evaluación habituales, pero con los instrumentos citados habilitados para la recolección de los datos biométricos.

Las percepciones y comportamientos de los estudiantes hacia el engaño fueron recogidos a través de dos cuestionarios (uno previo al inicio del piloto, o pre-cuestionario, y otro a la finalización del piloto, o post-cuestionario). Las preguntas incluidas en el pre-cuestionario tenían como objetivo recoger las experiencias previas de aprendizaje en línea de los estudiantes, mientras que el post-cuestionario recogió la experiencia adquirida durante el piloto. Los cuestionarios se diseñaron bajo la premisa de que las preguntas incluidas en ambos cuestionarios deberían estar correlacionadas para permitir la comparación de las percepciones de los estudiantes antes y después de su participación en el piloto. Sin embargo, algunas preguntas se incluyeron simplemente en uno de los dos cuestionarios considerando que: a) solo tenía sentido recopilar cierta información en uno de los cuestionarios (por ejemplo, las opiniones sobre el uso del sistema TeSLA solo se podían recoger después de utilizar el sistema); y b) no se esperaba

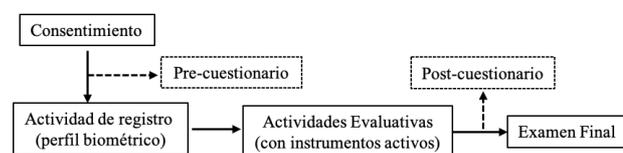


Figura 1. Pasos del piloto

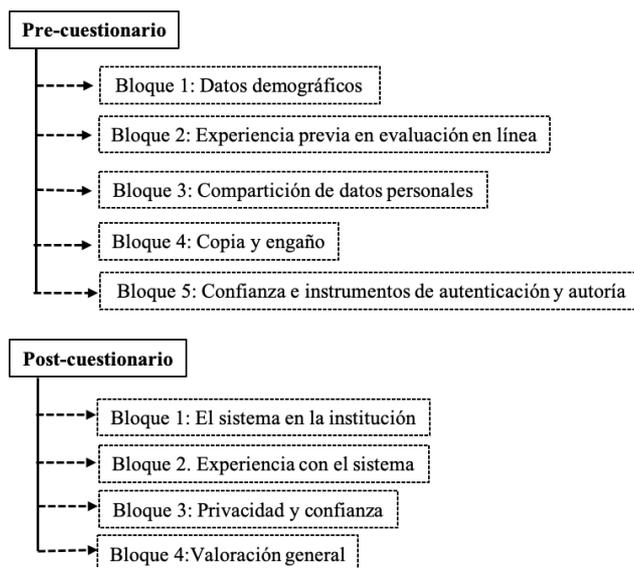


Figura 2. Bloques de preguntas de los cuestionarios

que algunas opiniones cambiaran debido a la participación en el piloto (por ejemplo, la noción del estudiante acerca del engaño probablemente no cambiaría porque no se realizaron durante el piloto acciones específicas al respecto para contribuir a tal transformación).

Los cuestionarios, organizados en diferentes secciones o bloques (véase la Figura 2), incluyeron una variedad de áreas de interés para el proyecto (por ejemplo, experiencias previas de aprendizaje y evaluación en línea, percepciones sobre la compartición de datos personales, confianza en la evaluación en línea, experiencias y dificultades de estudiantes con necesidades educativas especiales en relación a la evaluación en línea, entre otras). Teniendo en cuenta el objetivo del presente trabajo, solo se han considerado las preguntas que tratan con las conductas de engaño y la seguridad que potencialmente brinda el sistema TeSLA. La mayoría de estas preguntas fueron adaptadas de estudios previos ([2], [14], [27], [38], [47], [51], [55], [56]), aunque algunas preguntas fueron creadas teniendo en cuenta las características distintivas del proyecto. Las preguntas consideran los instrumentos utilizados en el piloto (autenticación y autoría) disponibles en el sistema TeSLA. Como el cuestionario comprendía varias secciones y era necesario mantener una longitud adecuada del mismo, las preguntas que se referían a conductas de engaño tenían que ser limitadas y equilibradas con respecto al número de preguntas relativas a otras secciones. Los borradores de los cuestionarios fueron refinados para adaptarse a los contextos de las 7 instituciones participantes en el proyecto. Los cuestionarios se completaron en línea y de forma anónima. Aunque los cuestionarios se utilizaron en las 7 universidades participantes en el proyecto, este trabajo solo presenta los resultados obtenidos en la UOC. Esta decisión se tomó después de aplicar los siguientes criterios: a) explotar datos del contexto educativo en línea, ya que es donde hay una brecha en la literatura sobre conductas de engaño, b) usar datos de una muestra suficiente de estudiantes. Como resultado de este filtrado, de las tres universidades en línea participantes (la Open University del Reino Unido, la Open Universiteit de los Países Bajos y la UOC), únicamente se

obtuvo una tasa de respuesta a los cuestionarios aceptable en el caso de los estudiantes de la UOC.

La participación en el pre-cuestionario fue de 130 estudiantes, mientras que 48 estudiantes respondieron el post-cuestionario. En global, hubo una tasa de respuesta razonable: el 100 % de los estudiantes del piloto respondieron el pre-cuestionario, mientras que la tasa de participación en el post-cuestionario fue de 36.9 %.

Como el sistema TeSLA estaba bajo desarrollo en el primer piloto, los resultados de los instrumentos de autenticación no se podían usar para verificar el comportamiento real de los estudiantes con respecto a diferentes actos de engaño. De hecho, los datos biométricos de los estudiantes recopilados por el sistema durante la actividad de registro y las actividades de evaluación en línea posteriores que activaron los instrumentos de RF, RV y RPT, sirvieron como una primera prueba de recogida, almacenamiento y consolidación de datos en una sola base de datos. Esto permitió al equipo técnico involucrado en el proyecto probar y ajustar los instrumentos para pilotos posteriores. Por estas razones, y para complementar el análisis de los resultados del piloto, se adoptaron las herramientas (así como los datos que dichas herramientas proporcionan) disponibles en la asignatura. Estas herramientas se aplican sobre las actividades (tanto de evaluación como de aprendizaje) realizadas por todos los estudiantes matriculados en la asignatura. Las herramientas se orientan a detectar casos de plagio, y el plan (o guía) docente de la asignatura advierte de su uso y de las consecuencias académicas en caso de detección de plagio en las actividades de evaluación. En concreto, se trata de un tutor inteligente [57] y una herramienta de detección de plagio de imágenes. El tutor inteligente asiste a los estudiantes en el aprendizaje del diseño de circuitos digitales a través de la propuesta de diferentes actividades de aprendizaje no evaluativas, y también permite validar la corrección de las actividades de evaluación en línea antes de enviar el documento en formato de texto que contiene la solución a las actividades de evaluación propuestas en la asignatura. Esta herramienta emplea la firma digital, la marca de tiempo y el tiempo invertido en la actividad para rastrear qué envíos se han compartido entre los estudiantes (a lo largo de este trabajo, el uso del término compartido se utiliza para referirse a casos de plagio no verificados, una vez estos han sido verificados se denominan como plagio). Esas actividades de evaluación en línea compartidas entre los estudiantes contienen los metadatos antes descritos para todos los estudiantes involucrados. La herramienta analiza estos metadatos para detectar el plagio en las actividades de evaluación en línea (es decir, no es necesario comparar el contenido de los documentos). Además, también hay disponible una herramienta de detección de plagio de imágenes. Esta herramienta extrae las imágenes del documento de texto con la solución a las actividades de evaluación en línea propuestas que cada estudiante entrega. Estos documentos contienen imágenes de los circuitos digitales que los estudiantes han diseñado y máquinas de estados finitos de circuitos secuenciales. La herramienta de detección de plagio de imágenes se basa en una técnica de dispersión de percepción (en inglés, *perceptual hashing*)

[58]. La comparación de *perceptual hashing* consiste en

TABLA I

CONOCIMIENTO DE LOS ESTUDIANTES SOBRE ACTOS DE ENGAÑO

Pregunta	Cue.*	Valores (%)		
		TA	N	TD
Creo que estoy informado/a sobre que se considera engañar en la asignatura en que me he matriculado	Pre	89.2	8.5	2.2
	Post	77.1	16.7	6.2
Entiendo las implicaciones de cometer actos de engaño en la asignatura en que me he matriculado	Pre	94.6	3.9	1.5
	Post	83.3	10.4	6.3
El uso de mecanismos de autenticación en la evaluación evita comportamientos ilegítimos	Pre	86.2	11.5	2.3
	Post	66.7	29.2	4.1
Ayudar o trabajar con un compañero de clase y después presentar trabajos individuales que son similares o idénticos al plagio	Pre	54.6	28.2	16.9
	Post	-	-	-
Copiar y pegar información de un sitio web en mi trabajo sin citar la fuente original es un tipo de engaño	Pre	89.2	6.2	4.6
	Post	-	-	-
Enviar mi trabajo a un compañero de clase antes de enviarlo para su evaluación, es un tipo de engaño	Pre	83.1	9.2	7.7
	Post	-	-	-
Leer el trabajo de un compañero de clase antes de enviarlo para su evaluación, es un tipo de engaño	Pre	67.8	23.8	8.4
	Post	-	-	-

Respuestas Totales: Pre-cuestionario: 130 Post-cuestionario: 48

* Cue. - Cuestionario, TA - Totalmente De Acuerdo - De Acuerdo, N - Neutral, TD - Totalmente En Desacuerdo - En Desacuerdo

reducir las imágenes a un ancho y alto idénticos, decolorar a una escala de grises y crear una función de hash basada en la variación de la intensidad de los colores de los píxeles. A continuación, la distancia de Hamming entre los hash determina la similitud entre las imágenes. Para una información más detallada acerca de estas herramientas de plagio, véase [59].

IV. RESULTADOS

A continuación se describen los principales resultados obtenidos del análisis de los datos recogidos durante el piloto. En primer lugar se analizan las respuestas de los estudiantes a los cuestionarios realizados en el piloto (pre y post cuestionarios). En segundo lugar se analizan los comportamientos de engaño reales de los estudiantes durante el piloto que se derivan de la aplicación de las herramientas de detección de plagio disponibles en la asignatura. Mientras que para el análisis de los resultados de los cuestionarios únicamente se tiene en cuenta a los estudiantes que participaron voluntariamente en el piloto (154 estudiantes), para los comportamientos de engaño reales de los estudiantes se tiene en cuenta el total de estudiantes matriculados en la asignatura en la que tuvo

lugar el piloto (543 estudiantes).

Los resultados se presentan tomando como hilo conductor las preguntas de investigación que aborda este trabajo. Más concretamente las secciones IV-A, IV-B y IV-C presentan, respectivamente, los datos recogidos sobre el conocimiento de los estudiantes en torno a actos de engaño durante el proceso de evaluación (pregunta de investigación P1), sus creencias sobre el uso de un sistema de autenticación en línea para aumentar la seguridad en la evaluación y evitar el engaño (pregunta de investigación P2), y la confianza de los estudiantes en la institución, los profesores y los compañeros de clase si se implementa un sistema de autenticación en línea (pregunta de investigación P3). Finalmente, la sección IV-D analiza los comportamientos reales de los estudiantes en relación a actos de engaño (pregunta de investigación P4).

IV-A. Conocimiento de los estudiantes sobre actos de engaño (P1)

La Tabla I resume las respuestas de los estudiantes que han probado el sistema TeSLA, con respecto a su percepción sobre posibles actos de engaño que atentan contra la integridad académica durante el proceso de

evaluación. Antes del piloto, casi todos los estudiantes declararon sentirse informados acerca de tales actos de engaño (89.2 %), y afirmaron que entendían las consecuencias de dichos actos en las asignaturas en las que estaban matriculados (94.6 %). Hay que tener en cuenta que, el propio plan (o guía) docente de todas las asignaturas de la UOC incluye una sección institucional específica dedicada a tal efecto, y se indica también cuáles son las consecuencias académicas que se aplican cuando ocurre esta situación. Los estudiantes consideraron que el uso de mecanismos de autenticación para la evaluación evita comportamientos ilegítimos (86.2 %). En el caso del post-cuestionario se obtuvieron resultados similares para las mismas preguntas discutidas previamente. El 77.1 % de los encuestados se sintió informado acerca de actos de engaño, y el 83.3 % entendió las consecuencias de tales actos. El 66.7 % de los encuestados afirmaron que los mecanismos de autenticación para fines de evaluación utilizados en el curso impidieron los actos de engaño. Sin embargo, la concepción de lo que constituye un comportamiento ilegítimo varía entre ellos:

- El 54.6 % de los estudiantes encuestados consideraron que ayudara un compañero o trabajar de forma conjunta en la resolución de actividades (o trabajos) individuales, y entregar trabajos similares o idénticos, constituye un acto de plagio.
- La mayoría de encuestados (89.2 %) consideraron que la acción de copiar y pegar información desde una página web, e incluir dicha información en una actividad constituye un acto de engaño.
- La mayoría de encuestados (83.1 %) estuvieron de acuerdo en que compartir su trabajo con otros compañeros antes de que este sea enviado a evaluar es un acto de engaño.
- Un 67.8 % de los encuestados creen que leer el trabajo de un compañero antes de su entrega, constituye un

acto de engaño.

TABLA II

CREENCIAS DE LOS ESTUDIANTES SOBRE LA SEGURIDAD CUANDO SE UTILIZA UN SISTEMA DE AUTENTICACIÓN Y AUTORÍA PARA LA EVALUACIÓN EN LÍNEA

Pregunta	Cue.*	Valores (%)		
		TA	N	TD
Creo que la evaluación en línea puede ser tan segura como la evaluación presencial	Pre	76.2	18.4	5.4
	Post	81.3	18.7	0
El sistema TeSLA ayudará a controlar mejor los casos de engaño y el plagio	Pre	-	-	-
	Post	81.3	12.5	6.2
El sistema TeSLA representará una mejora en mi universidad con respecto a la autenticación y la autoría en la evaluación	Pre	-	-	-
	Post	81.3	12.5	6.2

Respuestas Totales: Pre-cuestionario: 130 Post-cuestionario: 48

* Cue. - Cuestionario, TA - Totalmente De Acuerdo - De Acuerdo, N - Neutral, TD - Totalmente En Desacuerdo - En Desacuerdo

IV-B. Creencias de los estudiantes sobre el uso de un sistema de autenticación en línea para aumentar la seguridad en la evaluación y evitar el engaño (P2)

La Tabla II muestra que, antes del piloto, el 76.2 % de los estudiantes encuestados creen que un sistema de evaluación en línea puede ser tan seguro y fiable como un proceso de evaluación presencial. Después del piloto, esta valoración se elevó hasta el 81.3 % de los encuestados. Además, después de experimentar la evaluación en línea, la mayoría de los encuestados mostraron una percepción positiva de las ventajas que supone utilizar un sistema como TeSLA en relación a los comportamientos de engaño:

- El 81.3 % de los encuestados afirmaron que el sistema TeSLA mejorará el control de los actos de engaño (incluyendo el plagio).
- El 81.3 % de los encuestados consideraron que el sistema TeSLA representará una mejora en la autenticación y autoría en la evaluación en línea de la UOC.

IV-C. Confianza de los estudiantes en la institución, los profesores y los compañeros de clase si se implementa un sistema de autenticación en línea (P3)

Considerando las respuestas a los cuestionarios (Tabla III), la confianza de los estudiantes en la institución, los profesores y el sistema TeSLA fue alta antes y después del piloto, sin diferencias notables derivadas de su participación en el piloto. Sin embargo, en una de las preguntas abiertas, los estudiantes declararon que su participación en el piloto tuvo un efecto muy positivo, y que su nivel de confianza en los profesores de la asignatura y la propia institución se incrementó. En relación a las respuestas de los estudiantes, destacar:

- La mayoría de los encuestados confían en un sistema completamente en línea para evaluar a los estudiantes (88.5 % y 87.5 % en el pre y post cuestionario, respectivamente), y creen que el uso de un sistema

TABLA III
CONFIANZA DE LOS ESTUDIANTES EN UN SISTEMA DE AUTENTICACIÓN Y AUTORÍA EN LÍNEA PARA AUMENTAR LA SEGURIDAD

Pregunta	Cue.*	Valores (%)		
		TA	N	TD
Confío en un sistema que evalúe a los estudiantes completamente en línea (sin interacción presencial)	Pre	88.5	8.4	3.1
	Post	87.5	10.4	2.1
El uso de un sistema de autenticación como TeSLA hará que la evaluación en línea sea tan fiable como la evaluación presencial	Pre	-	-	-
	Post	91.7	6.3	2.0
Creo que mi universidad confía en mí, aunque utilice un sistema de autenticación durante la evaluación	Pre	82.3	9.2	8.5
	Post	-	-	-
Confiare' más en los procesos de evaluación de mi universidad si se utiliza el sistema TeSLA	Pre	-	-	-
	Post	56.3	41.7	2.0
Confío en mis compañeros/as de clase; no plagiarán mis actividades de evaluación	Pre	51.6	36.1	12.3
	Post	58.4	35.3	6.3
Mi profesor/a me protegerá si mis compañeros copian mi trabajo	Pre	58.5	30.8	10.7
	Post	-	-	-

Respuestas Totales: Pre-cuestionario: 130 Post-cuestionario: 48

* Cue. - Cuestionario, TA - Totalmente De Acuerdo - De Acuerdo, N - Neutral, TD - Totalmente En Desacuerdo - En Desacuerdo

como TeSLA hará que la evaluación en línea sea tan fiable como la evaluación presencial (91.7 %).

- Casi todos los encuestados consideran que la universidad confía en ellos, aunque use un sistema de autenticación con finalidades evaluativas (82.3 %). A pesar de ello, poco más de mitad de los encuestados (56,3 %) confiaría más en los procesos de evaluación de la UOC si utilizara el sistema TeSLA. La interpretación de este hecho es que los estudiantes confían en el proceso de evaluación que actualmente efectúa la universidad, independientemente de si la institución adopta o no el sistema TeSLA en el futuro.
- Solo la mitad de los encuestados (51.6 % y 58.4 % en el pre y post cuestionario, respectivamente) confía en que sus compañeros de clase no plagiarán su trabajo, y el 58.5 % cree que sus profesores los protegerán de ellos, en el caso de que alguien haya plagiado su trabajo.

IV-D. Comportamientos de engaño reales de los estudiantes (P4)

TABLA IV
COMPORTAMIENTO REAL DE LOS ESTUDIANTES EN RELACIÓN AL PLAGIO

	Participantes TeSLA	No Participantes TeSLA Núm. Estudiantes	Total Asignatura Núm. Estudiantes	%
AE1 TI	8	18	26	4.8
AE1 detector imágenes	3	6	9	1.7
AE1 TI	5	10	15	2.8
AE1 detector imágenes	1	2	3	0.6
AE1 TI	7	11	18	3.3
AE1 detector únicos	5	8	13	2.4
TI en AE (estudiantes únicos)	13	33	46	8.4
Detector de únicos en AE (estudiantes únicos)	9	14	23	4.2
TI en AnE (estudiantes únicos)	22	44	66	12.1

Total de Estudiantes: Participantes TeSLA: 154 No Participantes TeSLA: 389 Matriculados: 543

* AE. – actividad de evaluación en línea, AnE. - otras actividades no evaluables, TI - tutor inteligente

La Tabla IV muestra los resultados del análisis proporcionado por las herramientas de detección de plagio de la asignatura, el tutor inteligente (TI) y la herramienta de detección de plagio de imágenes, para todos los estudiantes matriculados, y distinguiendo entre participantes y no participantes en el piloto TeSLA. Para cada herramienta y actividad de evaluación en línea (AE) de la asignatura (3 AE) se muestra el número de estudiantes que han incurrido en copia (véanse las 6 primeras filas de la Tabla IV). Destacar que un mismo estudiante puede haber copiado en más de una actividad de evaluación. Por lo tanto, un mismo estudiante puede estar contado en más de una ocasión. Por ello, las tres últimas filas de la Tabla IV muestran, respectivamente, el número de estudiantes (ahora cada estudiante se cuenta una única vez) que han plagiado en las actividades de evaluación y en otras actividades no evaluables (AnE). Recuérdese que en la asignatura se proponen actividades no evaluables orientadas a que los estudiantes, asistidos por el tutor inteligente, adquieran las competencias. La herramienta ha detectado un porcentaje relativamente bajo de casos de plagio (12.2 % de estudiantes matriculados), y cuando se restringe a las actividades de evaluación, el plagio disminuye a 8.4 %. En su mayoría, los estudiantes compartieron actividades no evaluables porque el plagio no tenía consecuencias correctivas (en todo caso, los estudiantes incurrían en auto engaño). Sin embargo, algunos estudiantes continuaron copiando en las actividades de evaluación en línea que validaron dentro del tutor inteligente (4.8 % en AE1, 2.8 % en AE2 y 3.3 % en AE3). La herramienta de detección de imágenes encontró plagio adicional en los documentos de texto enviados, en su mayoría por estudiantes que no utilizaron el tutor inteligente (su uso es opcional). Un resultado interesante es que la mayoría de los estudiantes (en la mayoría de los casos más del doble) que copiaron no participaron en el piloto. Se infiere que estos estudiantes pensaron que no participar en el piloto implicaba que no se analizaban sus actividades.

El análisis detallado de los casos detectados de plagio, arroja los siguientes patrones de comportamiento:

- Los estudiantes que mayoritariamente habían copiado en las actividades no evaluables a ser resueltas con el tutor inteligente, continuaron haciéndolo con el tutor inteligente en las actividades de evaluación en línea.
- Los estudiantes que copiaron en las actividades de evaluación en línea usando el tutor inteligente, después de validar el diseño del circuito digital, modificaron intencionalmente el esquema del circuito (es decir, movieron la posición de los componentes digitales).

Por lo tanto, la herramienta de detección de plagio de imágenes no detectó la copia.

- Algunos estudiantes que no usaron el tutor inteligente, obtuvieron la solución correcta validada por el tutor inteligente de otros estudiantes, y agregaron la imagen correspondiente a su documento de solución. Por lo tanto, el detector de plagio de imágenes fue capaz de identificar el engaño.
- Los ejercicios que no se podían validar en el tutor inteligente (los relativos a máquina de estados finitos) fueron los más comúnmente compartidos por los estudiantes y detectado por el detector de plagio de imágenes, y principalmente por los estudiantes que no participaron en el piloto.

V. DISCUSIÓN

Los resultados obtenidos en este trabajo coinciden con estudios previos disponibles en la literatura, a la vez que proporcionan evidencias adicionales para comprender las percepciones y comportamientos de los estudiantes cuando estos cometen actos de engaño en la educación en línea. De forma similar a [49], se han encontrado malentendidos sobre qué se considera engañar, y cómo el engaño afecta especialmente a las prácticas de plagio. Según los resultados, se puede considerar que los estudiantes son conscientes de lo que es engañar, pero su comprensión varía en función del tipo de engaño y del contexto de situación. Por ejemplo, solo la mitad de los estudiantes creía que ayudar a un compañero o trabajar de forma conjunta con un compañero de clase en una actividad individual constituye un engaño. Esto puede explicar los resultados obtenidos con respecto a los actos reales de engaño de los estudiantes que colaboraron en la realización de actividades de aprendizaje no evaluables. Los estudiantes trabajaron con sus compañeros para resolver las actividades, incluso cuando debían ser realizadas individualmente, sin saber que estaban cometiendo plagio ya que sus productos finales eran similares o idénticos, como detectó el tutor inteligente.

Los resultados obtenidos en los casos de engaño en las actividades de evaluación en línea sugieren que los estudiantes que intencionalmente querían copiar intentaron encontrar una manera de evitar las herramientas de detección de plagio de la asignatura. Además, los estudiantes que no querían engañar mayoritariamente participaron en el piloto. Es más, el piloto podría haber desalentado a algunos estudiantes a realizar actos de engaño

debido al mayor nivel de vigilancia. En consecuencia, aquellos estudiantes que participaron en el piloto, afirmaron que los mecanismos de autenticación y autoría utilizados en el curso mejoraron el control respecto la comisión de actos de engaño (como el plagio) y que, en consecuencia, evitaron que tuviesen lugar. Dichos resultados confirman evidencias previas que afirman que las herramientas biométricas y de antiplagio pueden ayudar a contrarrestar los actos de deshonestidad académica por parte de los estudiantes [38]–[43].

En cuanto a las percepciones de los estudiantes sobre las posibilidades de engaño en la educación en línea, los resultados revelan que la confianza de los estudiantes en la seguridad de la evaluación en línea aumentó como consecuencia de su participación en el piloto. Los encuestados creyeron que el uso de un sistema como TeSLA mejoraría la autenticación y la autoría en los procesos de evaluación, haciendo que la evaluación en línea sea tan confiable como la evaluación presencial. Estos resultados son consistentes con estudios previos, donde los estudiantes no percibieron diferencias entre las posibilidades de engañar en la educación en línea y presencial [45]. Es necesario destacar, que solo la mitad de los encuestados creyó que sus compañeros no copiarían, y que sus profesores los protegerían de los que sí lo hacían. Este resultado enfatiza la posible sensación de desconfianza de los estudiantes hacia sus propios compañeros, y lo desprotegidos que se sentían antes de usar un sistema de autenticación y autoría para la evaluación en línea.

La observación más sorprendente que surge es que, el simple hecho de que los estudiantes sepan que se está utilizando un sistema de autenticación y autoría en línea para la evaluación, puede evitar el engaño, y puede hacer que los estudiantes se sientan más seguros y confiados para realizar el proceso de evaluación en línea.

VI. LIMITACIONES

El análisis de los datos ha sido limitado por varias razones. Primero, en el piloto existe un sesgo de autoselección puesto que la participación es voluntaria. El motivo se relaciona con los estándares éticos para la investigación, que tienen como objetivo evitar que los estudiantes sufran desigualdades dependiendo de su participación en el piloto (es decir, que se beneficien del uso de los mecanismos de seguridad con finalidad evaluativa). En segundo lugar, debido al sesgo de selección, tal y como se ha demostrado, fueron los estudiantes que habitualmente no comenten actos de engaño los que consintieron en participar en el piloto. Esto puede haber afectado los resultados obtenidos a través de los instrumentos de investigación utilizados en este trabajo. En tercer lugar, en cuanto al sesgo de supervivencia, la pérdida de participantes durante el piloto es principalmente debida a la tasa de abandono del curso en sí y, por lo tanto, no está vinculada al diseño y la ejecución del piloto. Sin embargo, el presente estudio es limitado dadas las diferencias en el número de participantes en el pre y post cuestionario. Estas diferencias pueden haber afectado el análisis sobre el impacto del sistema TeSLA en las percepciones de los estudiantes. Finalmente, con respecto a la validez de constructo, y tal y

como se ha explicado en secciones previas, durante el piloto se interactuó con otras herramientas de plagio disponibles en la asignatura donde tuvo lugar la experiencia. Aún así, los instrumentos de investigación permitieron recopilar toda la información acerca de las percepciones del uso del sistema TeSLA.

VII. CONCLUSIONES Y TRABAJO FUTURO

Los resultados de este trabajo proporcionan más evidencias para comprender la percepción y el comportamiento de los estudiantes en torno a lo que significa engañar, contribuyendo así a llenar un vacío existente en la literatura, más específicamente en el caso de la educación en línea.

Los resultados muestran que el simple hecho de que los estudiantes sepan que se utiliza un sistema de autenticación y autoría en línea en los procesos de evaluación puede evitar comportamientos deshonestos, y a su vez, hace que se sientan más seguros durante la evaluación en línea. Por lo tanto, esta investigación destaca la importancia de utilizar herramientas o sistemas de autenticación y de autoría en línea para incrementar la percepción de seguridad y confianza en la educación en línea, haciendo que el proceso de evaluación sea tan fiable como en las instituciones presenciales. Sin embargo, el estudio realizado también revela malentendidos entre los estudiantes sobre qué se considera engaño, tanto durante el proceso de aprendizaje como de evaluación, especialmente en relación a las prácticas de plagio, y cómo esto puede afectar a su proceso de aprendizaje. En consecuencia, la tecnología debe ir acompañada de estrategias y procedimientos orientados a modificar las actitudes de los estudiantes hacia dichos comportamientos no deseados, mejorando así la integridad académica.

Una de las principales limitaciones de esta investigación ha sido el tamaño de la muestra. Por lo tanto, y como línea futura, para una realizar una investigación más completa, se deberían realizar más pruebas piloto en diferentes asignaturas e involucrando a un mayor número de estudiantes para obtener muestras más amplias, e incluso de disciplinas diferenciadas. De esta manera se obtendrá una visión más amplia de las percepciones y comportamientos de los estudiantes sobre el engaño al usar el sistema TeSLA.

AGRADECIMIENTOS

Este artículo ha sido financiado por el proyecto H2020 TeSLA (ref. 688520) y por el proyecto New Goals 2018NG001 "LIS: Learning Intelligent System" del eLearn Center (UOC).

REFERENCIAS

- [1] G. Crisp, "Towards authentic e-assessment tasks," in Proceedings of EdMedia: World Conference on Educational Media and Technology 2009, G. Siemens and C. Fulford, Eds. Honolulu, HI, USA: Association for the Advancement of Computing in Education (AACE), June 2009, pp. 1585–1590.
- [2] J. Dermo, "E-assessment and the student learning experience: A survey of student perceptions of e-assessment," British Journal of Educational Technology, vol. 40, no. 2, pp. 203–214, 2008.

- [3] P. Marriott and A. Lau, "The use of on-line summative assessment in an undergraduate financial accounting course," *Journal of Accounting Education*, vol. 26, no. 2, pp. 73 – 90, 2008.
- [4] A. Rastgoo, Y. Namvar, and A. Iran, "Assessment Approach in virtual learning," *Turkish Online Journal of Distance Education*, vol. 11, no. 1, pp. 42–48, 2010.
- [5] M. Heberling, "Maintaining academic integrity in on-line education," *Online Journal of Distance Learning Administration*, vol. 5, no. 1, 2002.
- [6] M. Hersh and B. Leporini, "Accessibility and usability of educational gaming environments for disabled students," in 2012 IEEE 12th International Conference on Advanced Learning Technologies, 2012, pp. 752–753.
- [7] K. Kennedy, S. Nowak, R. Raghuraman, J. Thomas, and S. F. Davis, "Academic dishonesty and distance learning: Student and faculty views," *College Student Journal*, vol. 34, no. 2, pp. 309–315, 2000.
- [8] M. Kent, "Disability and elearning: Opportunities and barriers," *Disability Studies Quarterly*, vol. 35, no. 1, 2015. [Online]. Available: <http://dx.doi.org/10.18061/dsq.v35i1.3815>
- [9] M. M. Lanier, "Academic integrity and distance learning," *Journal of criminal justice education*, vol. 17, no. 2, pp. 244–261, 2006.
- [10] D. McManus, R. Dryer, and M. Henning, "Barriers to learning online experienced by students with a mental health disability," *Distance Education*, vol. 38, no. 3, pp. 336–352, 2017.
- [11] G. G. Ravasco, "Technology-aided cheating in open and distance e-learning," *Asian journal of distance education*, vol. 10, no. 2, pp. 71–77, 2012.
- [12] N. C. Rowe, "Cheating in online student assessment: Beyond plagiarism," *Online journal of Distance Learning Administration*, 2004. [Online]. Available: <https://calhoun.nps.edu/handle/10945/36015>
- [13] M. Vilchez and M. O. Thirunarayanan, "Cheating in online courses: A qualitative study," *International Journal of Instructional Technology and Distance Learning*, vol. 8, no. 1, 2011. [Online]. Available: <http://itdl.org/Journal/jan11/article05.htm>
- [14] Y.-W. Wang, "University student online plagiarism," *International Journal on ELearning*, vol. 7, no. 4, pp. 743–758, 2008.
- [15] B. Dietz-Uhler, "Academic dishonesty in online courses. Proceedings of the ASCUE Summer Conference, 2011." [Online]. Available: <https://www.ascue.org/files/proceedings/2011-final.pdf>
- [16] T. Grijalva, J. Kerkvliet, and C. Nowell, "Academic honesty and online courses," *College Student Journal*, vol. 40, pp. 180–186, 2006.
- [17] D. J. Hancock, "Faculty beliefs regarding online academic dishonesty and the measures taken to address academic dishonesty in Georgia, ph.d. dissertation," Ph.D. dissertation, Georgia Southern University, Georgia, USA, 2012. [Online]. Available: <http://dspaceprod.georgiasouthern.edu:8080/xmlui/handle/10518/3490>
- [18] D. Stuber-McEwen, P. Wiseley, and S. Hoggatt, "Point, click, and cheat: Frequency and type of academic dishonesty in the virtual classroom," *Online Journal of Distance Learning Administration*, vol. 12, no. 3, 2009. [Online]. Available: <http://www.westga.edu/~distance/ojdla/fall123/stuber123.html>
- [19] I. Noguera, A.-E. Guerrero-Roldán, and M. E. Rodríguez, "Assuring authorship and authentication across the e-assessment process," in *Technology Enhanced Assessment*. Springer International Publishing, 2017, pp. 86–92.
- [20] M. E. Rodríguez, D. Baneres, M. Ivanova, and M. Durcheva, "Case study analysis on blended and online institutions by using a trustworthy system," in *Technology Enhanced Assessment*, Barcelona, Spain, Oct. 2017.
- [21] R. Peytcheva-Forsyth, B. Yovkova, and T. Ladonlahti, "The potential of the TeSLA authentication system to support access to e-assessment for students with special educational needs and disabilities (sofia university experience)," in *ICERI2017 Proceedings*, ser. 10th annual International Conference of Education, Research and Innovation. IATED, 16-18 November, 2017 2017, pp. 4593–4602.
- [22] R. James, "Tertiary student attitudes to invigilated, online summative examinations," *International Journal of Educational Technology in Higher Education*, vol. 13, no. 1, p. 19, Mar 2016. [Online]. Available: <https://doi.org/10.1186/s41239-016-0015-0>
- [23] P. Marriott, "Students' evaluation of the use of online summative assessment on an undergraduate financial accounting module," *British Journal of Educational Technology*, vol. 40, no. 2, pp. 237–254, 2009.
- [24] A. Khare and H. Lam, "Assessing student achievement and progress with online examinations: Some pedagogical and technical issues," *International Journal on Elearning*, vol. 7, no. 3, pp. 383–402, 2008.
- [25] S. C. Shaffer, "Distance education assessment infrastructure and process design based on international standard 23988." *Online Journal of Distance Learning Administration*, vol. 15, no. 2, 2012.
- [26] R. W. Yates and B. Beaudrie, "The impact of online assessment on grades in community college distance education mathematics courses," *The American Journal of Distance Education*, vol. 23, no. 2, pp. 62–70, 2009.
- [27] G. R. Watson and J. Sottile, "Cheating in the digital age: Do students cheat more in online courses?" *Online Journal of Distance Learning Administration*, vol. 13, no. 1, 2010. [Online]. Available: <https://www.westga.edu/~distance/ojdla/spring131/watson131.html>
- [28] S. Asha and C. Chellappan, "Authentication of e-learners using multimodal biometric technology," in *International Symposium on Biometrics and Security Technologies*, 2008. ISBAST 2008. IEEE, 2008, pp. 1–6.
- [29] D. Foster, N. Mattoon, and R. Shearer, "Using multiple online security measure to deliver secure course exams to distance education students: A white paper," Kryterion Inc, Tech. Rep., 2008. [Online]. Available: <https://www.ou.nl/Docs/Campagnes/ICDE2009/Papers/Final Paper 101Walker>
- [30] G. Kambourakis and D. Damopoulos, "A competent post-authentication and non-repudiation biometric-based scheme for m-learning," in *Proceedings of the 10th IASTED International Conference on Web-based Education (WBE 2013)*, 2013, pp. 821–827.
- [31] K. Rabuzin, M. Baca, and M. Sajko, "E-learning: Biometrics as a security factor," in 2006 International Multi-Conference on Computing in the Global Information Technology - (ICCGI'06), 2006, pp. 64–64.
- [32] O. H. Graven and L. M. MacKinnon, "A consideration of the use of plagiarism tools for automated student assessment," *IEEE Transactions on Education*, vol. 51, no. 2, pp. 212–219, 2008.
- [33] I. Y. Jung and H. Y. Yeom, "Enhanced security for online exams using group cryptography," *IEEE Transactions on Education*, vol. 52, no. 3, pp. 340–349, 2009.
- [34] S. Manoharan, "Personalized assessment as a means to mitigate plagiarism," *IEEE Transactions on Education*, vol. 60, no. 2, pp. 112–119, 2017.
- [35] A. H. Osman, N. Salim, and A. Abuobieda, "Survey of text plagiarism detection," *Computer Engineering and Applications Journal (ComEngApp)*, vol. 1, no. 1, pp. 37–45, 2012.
- [36] Simon, B. Cook, J. Sheard, A. Carbone, and C. Johnson, "Academic integrity: Differences between computing assessments and essays," in *Proceedings of the 13th Koli Calling International Conference on Computing Education Research*, ser. Koli Calling '13. ACM, 2013, pp. 23–32.
- [37] E. Stamatas, "A survey of modern authorship attribution methods," *Journal of the American Society for Information Science and Technology*, vol. 60, no. 3, pp. 538–556, 2009.
- [38] I. Glendinning, "Responses to student plagiarism in higher education across europe," *International Journal for Educational Integrity*, vol. 10, no. 1, pp. 4–20, 2014.
- [39] D. W. Bedford, J. R. Gregg, and M. S. Clinton, "Preventing online cheating with technology: A pilot study of remote proctor and an update of its use," *Journal of Higher Education Theory and Practice*, vol. 11, no. 2, pp. 41–59, 2011.
- [40] R. Caldarola and T. MacNeil, "Dishonesty deterrence and detection: How technology can ensure distance learning test security and validity," in *Proceedings of the 8th European Conference on E-Learning, ECEL 2009*, 2009, pp. 108–115.
- [41] N. Chiesel, "Pragmatic methods to reduce dishonesty in web-based courses," *Quarterly Review of Distance Education*, vol. 8, no. 3, pp. 203–211, 2007.
- [42] K. Hylton, Y. Levy, and L. P. Dringus, "Utilizing webcam-based proctoring to deter misconduct in online exams," *Computers and Education*, vol. 92, pp. 53–63, 2016.
- [43] S. Trenholm, "A review of cheating in fully asynchronous online courses: A math or fact-based course perspective," *Journal of Educational Technology Systems*, vol. 35, no. 3, pp. 281–300, 2007.
- [44] I. J. Arnold, "Cheating on online formative tests: Does it pay off?" *The Internet and Higher Education*, vol. 29, pp. 98 – 106, 2016.
- [45] O. R. Harmon, J. Lambrinos, and J. Buffolino, "Assessment design and cheating risk in online instruction." *Online Journal of Distance Learning Administration*, vol. 13, no. 3, 2010. [Online]. Available: <https://www.westga.edu/~distance/ojdla/Fall133/harmonlambrinosbuffolino133.html>

- [46] M. T. Cole and L. B. Swartz, "Understanding academic integrity in the online learning environment: A survey of graduate and undergraduate business students," *ASBBS Proceedings*, vol. 20, no. 1, pp. 738–746, 2013.
- [47] I. R. A. Chertok, E. R. Barnes, and D. Gilleland, "Academic integrity in the online learning environment for health sciences students," *Nurse education today*, vol. 34, no. 10, pp. 1324–1329, 2014.
- [48] H. Corrigan-Gibbs, N. Gupta, C. Northcutt, E. Cutrell, and W. Thies, "Deterring cheating in online environments," *ACM Transactions on Computer-Human Interaction*, vol. 22, no. 6, pp. 1–23, 2015. [Online]. Available: <http://doi.acm.org/10.1145/2810239>
- [49] M. Joy, G. Cosma, J. Y. K. Yau, and J. Sinclair, "Source code plagiarism from a student perspective," *IEEE Transactions on Education*, vol. 54, no. 1, pp. 125–132, 2011.
- [50] D. M. Douglas, K. Poullet, and A. Chawdhry, "Student perspectives of cheating in online classes." *Issues in Information Systems*, vol. 16, no. 4, pp. 215–223, 2015.
- [51] H. Shariff and R. Ahamed, "Academic dishonesty on the internet and suggested strategies to be used by academic staff to minimize the trend," *International Journal of Information Systems and Engineering*, vol. 2, no. 1, pp. 32–40, 2014.
- [52] S. Sendag, M. Duran, and M. R. Fraser, "Surveying the extent of involvement in online academic dishonesty (e-dishonesty) related practices among university students and the rationale students provide: One university's experience," *Computers in Human Behavior*, vol. 28, no. 3, pp. 849 – 860, 2012.
- [53] H. Fényes, "Gender differences in higher education efficiency and the effect of horizontal segregation by gender," *Journal of Social Research & Policy*, vol. 6, no. 2, pp. 83–103, 2015.
- [54] UNESCO, "Cracking the code: Girls' and women's education in science, technology, engineering and mathematics (stem)," Online, 2007. [Online]. Available: <http://unesdoc.unesco.org/images/0025/002534/253479E.pdf>
- [55] D. McCabe, "Academic integrity survey," <http://academic-integrity.rutgers.edu/rutgers.asp>, 2008.
- [56] J. M. Stephens, M. F. Young, and T. Calabrese, "Does moral judgment go offline when students are online? a comparative analysis of undergraduates' beliefs and behaviors related to conventional and digital cheating," *Ethics & Behavior*, vol. 17, pp. 233–254, 09/2007 2007.
- [57] D. Baneres, R. Clarisó, J. Jorba, and M. Serra, "Experiences in digital circuit design courses: A self-study platform for learning support," *IEEE Transactions on Learning Technologies*, vol. 7, no. 4, pp. 360–374, 2014.
- [58] A. Buldas, A. Kroonmaa, and R. Laanoja, "Keyless signatures' infrastructure: How to build global distributed hash-trees," in *Secure IT Systems*, H. Riis Nielson and D. Gollmann, Eds. Springer Berlin Heidelberg, 2013, pp. 313–320.
- [59] D. Baneres, I. Noguera, M. E. Rodríguez, and A. E. Guerrero-Roldán, "Using an intelligent tutoring system with plagiarism detection to enhance e-assessment," in *Advances in Intelligent Networking and Collaborative Systems. The 10th International Conference on Intelligent Networking and Collaborative Systems (INCoS-2018)*, F. Xhafa, L. Barolli, and M. Gregus, Eds. Springer International Publishing, September 2018, pp. 363–372.



M. Elena Rodríguez received her BSc and PhD in computer science from the Universitat Politècnica de Catalunya Barcelona Tech and the University of Alcalá, respectively. Since 2001, she has been a full-time lecturer at the Universitat Oberta de Catalunya (Open University of Catalonia, UOC) and member of the TEKING research group. Her current research interests include the development of innovative e-learning systems, as well as the analysis of the data that these systems collect. The development of knowledge-based systems and their integration into e-learning systems are also an object of interest.



Ana-Elena Guerrero-Roldán is a Bachelor of pedagogy from Ramon Llull University and specialist in online education. She has a Master's in information and knowledge society, and a PhD in e-learning and technology from the Universitat Oberta de Catalunya (UOC). Since 2003, she is an associate professor at the UOC. She focuses her research on the design of technology-enhanced systems for online education, focusing on e-assessment. IP of TEKING research group, she has participated in several national and international research projects. She is the coordinator of the TeSLA EU project (H2020. Ref. EC: 688520).



David Baneres received a BSc in computer science (2001) and a PhD in computer science (2008) from the the Universitat Politècnica de Catalunya BarcelonaTech. He is currently a full-time lecturer at the Universitat Oberta de Catalunya (Open University of Catalonia, UOC). He has also been a part-time associate professor at the Universitat Autònoma de Barcelona (2010-2012). His research interests include optimization techniques on logic synthesis domain, formal methods and innovative e-learning systems.



Ingrid Noguera received her BA in pedagogy in 2006 and her PhD in educational multimedia in 2011 from the University of Barcelona. She is currently a postdoctoral researcher at the Universitat Oberta de Catalunya (Open University of Catalonia, UOC). She has also been a part-time associate professor at the University of Barcelona (2010-2014). Her research interests include technology-enhanced learning, computer-supported collaborative learning and e-learning.