RECOMENDACIONES DE SEGURIDAD EN EXÁMENES: ANTES, DURANTE Y DESPUÉS

TEST SECURITY RECOMMENDATIONS: BEFORE, DURING AND AFTER

Autor:
Enrique de la Hoz de la Hoz. Universidad de Alcalá, Departamento de Automática.
enrique.delahoz@uah.es

Resumen:
Este artículo presenta un análisis de los posibles fraudes la realización de exámenes, con especial énfasis en aquellos tipos de fraude que empleen algún mecanismo basado en la tecnología y propone un conjunto de recomendaciones para la mejorar de la seguridad de los mismos. El trabajo se centra en los fraudes relacionados con los exámenes tradicionales. No se abordan las amenazas específicas contra exámenes realizados mediante ordenador o en plataformas online, aunque algunas de las medidas propuestas también suponen mejoras para dichos entornos.

Abstract:
This article presents an analysis of the potential frauds related to test realization, focusing on technology-based frauds and establishes a set of recommendations and good practices to improve test security. This work deals with ‘pen and paper’ tests. The specific threats against compute-based or online tests are out of the scope of this work; they could benefit from the application of some of the recommendations outlined here, though

Palabras clave:
Seguridad en exámenes; Buenas prácticas; Universidad
Keywords:
Test security; Good practices; University

Antecedentes

En este apartado se revisan algunos de los incidentes relacionados con fraudes en exámenes en universidad españolas. Esta misma problemática también se ha plantado en universidades de todo el mundo. Así, por ejemplo, Harvard expulsó a más de 60 estudiantes en 2013 (Toro 2013). También es interesante señalar que se trata de un fenómeno que se está detectando en enseñanzas medias. Como muestra, cabe señalar el incidente de robo y venta de exámenes en un instituto de La Rioja en 2016 (Ruiz 2016).

Este trabajo no constituye una revisión exhaustiva pero sí lo suficiente extensa como para poder apreciar la extensión y complejidad del problema. Para su elaboración, se ha empleado únicamente información procedente de noticias publicadas en las versiones digitales de diarios en Internet.

En esta apartado simplemente se realiza una recopilación de incidentes y de las medidas que se tomaron a continuación. Para un análisis desde el punto de vista legal, se recomienda consultar (Chaves 2014).

Los primeros incidentes

En este trabajo nos vamos a centrar en los incidentes de los últimos años. Mercé Molist en su libro ‘Hackstory.es’ sobre la historia del movimiento hacker en España comenta los incidentes de seguridad en la Universitat Rovira i Virgili en 1996 (Molist 2014). En 1997 se produjo la detención de dos estudiantes acusados del robo de un fichero con contraseñas de más de 2.000 alumnos y de entre 100 y 200 profesores. Los detenidos emplearon esta información para acceder a cuentas de profesores y obtener enunciados de exámenes.

Unos años más tarde, en 2002 un hacker consigue acceder a los sistemas de la Universidad de Alcalá que gestionan los expedientes académicos del alumnado y como prueba de su logro, crea un expediente con todas las asignaturas con calificación 10 en la titulación de Ingeniería de Telecomunicación (Becerra 2002a) El suplemento ‘Campus’ del diario El Mundo informaba que estas acciones tenían

únicamente un carácter reivindicativo, en una entrevista con el supuesto hacker (Becerra 2002b).

2007. Robo de datos en la Universidad de Granada

El 8 de noviembre de 2007 el diario *Ideal de Granada* (Cabrero 2007) informa del descubrimiento de un incidente de seguridad informática en la Escuela Técnica Superior de Ingeniería Informática y Telecomunicaciones que había provocado la pérdida de datos personales y la modificación no autorizada de la página web de la escuela. Como parte de este ataque, el atacante consiguió obtener las credenciales de dos profesores lo que le permitió acceder a calificaciones y a soluciones de exámenes de años anteriores, que custodiaban las víctimas del ataque. De acuerdo con fuentes de los servicios informáticos de la Universidad de Granada (UGR) que se citan en el artículo, el ataque pudo realizarse mediante herramientas de captura de tráfico por parte de algún estudiante de la Escuela.

2008. Robo de exámenes en la Universidad de Las Palmas de Gran Canaria

En el año 2008, el diario *'canarias7.es'* (Arencibia 2008) informa que "se investiga un robo informático que afecta a la evaluación de una asignatura de tercero de medicina en la Universidad de las Palmas de Gran Canaria (ULPGC). El acta se mantiene en suspenso. Se trata de un hecho sin precedentes que podría afectar a unos 80 alumnos. El material robado pone en cuestión los exámenes de las convocatorias de junio y de septiembre" (Arencibia 2008). Ya en ese momento, el entonces decano de la Facultad de Ciencias de la Salud, Juan Cabrera, afirmaba que conocía otros casos similares en facultades de la península e incluso en el examen MIR y denunciaba que "la comunidad universitaria peca de candidez en lo referente a la seguridad de las comunicaciones informáticas". Además, proponía que se repitiera el examen.

2010. Robo de Contraseñas en Universidad de Zaragoza

El *Periódico de Aragón* del 15 de abril de 2010 (Europa Press 2010) informa de la detención de un estudiante de Ingeniería Informática de la Universidad de Zaragoza (UNIZAR) por el robo de credenciales de estudiantes y profesores. Para ello, el

estudiante había creado una página que imitaba la apariencia de la página de autenticación para el acceso a la red inalámbrica. Mediante el empleo de técnicas del tipo de hombre en el medio ('man-in-the-middle') el atacante era capaz de interceptar el tráfico legítimo de los usuarios y obtener sus credenciales.

2010. Robo de exámenes en la Universidad de Córdoba

Según informa el *Diario de Córdoba* del 23 de Septiembre de 2012 (R. Arjona 2012), tres alumnos allanan la Facultad de Medicina de la Universidad de Córdoba (UCO) y roban los exámenes, que estaban almacenados en un equipo informático ubicado en la Facultad, y días más tarde obtienen un 9,5 en el examen. Según la noticia, los tres estudiantes se colaron de noche en la Facultad, para introducirse en el departamento de Farmacología, donde se hicieron con más de tres mil preguntas y respuestas que estaban guardadas en el disco duro de un ordenador. La extrañeza del profesor ante las calificaciones de los estudiantes provocó el inicio de una investigación. Se abrió un expediente sancionador contra los estudiantes que terminó con la expulsión de dos de los tres estudiantes.

2012. Modificación de calificaciones en la Universidad de Málaga

En 2012, el diario *ABC* informa (D. Almoguera 2012) que tres estudiantes fueron detenidos por un ataque informático a la Universidad de Málaga (UMA) con el que lograron apoderarse de claves de acceso restringidas para cambiar las notas de los expedientes académicos. La Escuela Superior Politécnica e Ingeniería Industrial de Málaga detectó a la hora de certificar las modificaciones de actas de notas de alumnos, que una de esas actas contenía un número de aprobados mayor que el real. Los detenidos habían accedido a los usuarios y contraseñas tanto de profesores como de personal de la secretaría y posteriormente habían modificado hasta diez notas para poner aprobado donde había un suspenso, y no sólo en sus propios expedientes académicos sino también en los de otros alumnos elegidos de forma aleatoria para evitar ser identificados. Para conseguir las claves, se había instalado un software de registro de contraseñas en el ordenador de las víctimas (programa 'Caín y Abel'). Los detenidos y un cuarto imputado fueron acusados de

delitos de daños, intrusismo informático, descubrimiento de secretos, falsedad documental y estafa.

En 2016 se dictó sentencia sobre el caso anterior, en la que se absuelve a los acusados, aunque la sentencia establece como hechos probados que se produjo la modificación de las calificaciones. El diario *SUR* del 21 de Octubre de 2016 informa sobre la sentencia (Cano 2016). La sentencia acredita que "*entre el 7 y el 20 de febrero alguien se conectó a la red wifi de la secretaría de la Politécnica desde la cuenta de este mismo alumno y la tarjeta de red del ordenador portátil de un profesor, que había sido 'hackeada'. A partir de ahí, usó las cuentas de correo de tres funcionarias de la secretaría para modificar notas de los tres acusados y de un amigo, al que desde el principio se consideró ajeno a la intrusión. A este último sólo le subió la nota del 7,5 al 8, mientras que el resto pasó del no presentado o el suspenso al aprobado en varias asignaturas"* (Cano 2016). Sin embargo, la sentencia no considera probado que esto fuera realizado por los acusados. La universidad mantuvo la calificación de suspenso para los estudiantes y decidió no apelar la sentencia, al considerarse hecho probado que el cambio de las calificaciones se había realizado.

Según la sentencia, se procedió a instalar el programa 'Caín y Abel' en un ordenador del aula de laboratorio docente del Departamento de Matemáticas Aplicadas de la Escuela Politécnica Superior e Ingeniería Industrial de la UMA. Tras esto *"puso a trabajar el ordenador de manera que, tras varios días funcionando sin ser detectado, fue descubriendo y recopilando las contraseñas de los profesores"* (Cano 2016) . Estas contraseñas fueron las que se utilizaron posteriormente los cambios de notas.

2013. Suplantación de identidades en la Universidad de Málaga

La edición digital del diario *El Mundo* del 31 de marzo de 2013 reproduce una nota de la Agencia EFE donde se informa que *"Una estudiante universitaria de 26 años ha sido detenida por la Policía Nacional en Málaga por suplantar la identidad de una compañera de estudios para hacer cinco exámenes de una asignatura con el fin de*

conocer de antemano las preguntas para poder sacar buena nota en sus propios ejercicios".

La estudiante fue detenida como supuesta autora de delitos de daños, usurpación de estado civil y descubrimiento y revelación de secretos. La detenida estaba matriculada en la misma asignatura que la víctima y presuntamente utilizaba la contraseña de la víctima para conocer las preguntas de los exámenes online de la asignatura con antelación a acceder con las suyas propias. Presuntamente empleó este procedimiento en cinco exámenes. La detenida presuntamente se valió de su cercanía con la víctima para descubrir sus claves, que después presuntamente utilizaba.

2014. Tráfico de exámenes en la Universidad Pablo Olavide

El *Diario de Sevilla* en su edición del 11 de Octubre de 2015 (Muñoz 2015b) informa que dos profesoras del Departamento de Economía Financiera y Contabilidad de la UPO, Concepción Álvarez-Dardet y Carolina Ramírez denunciaron la filtración de los exámenes finales de la asignatura 'Contabilidad de Gestión', de las convocatorias de junio de 2014 y 2015, lo que permitió a decenas de alumnos disponer del examen el día de antes de la prueba. Una vez más, lo que disparó las sospechas fue la disparidad entre el comportamiento de los alumnos en clase y su resultado en el examen. Las profesoras comprobaron que un grupo de alumnos obtuvo una media cercana al sobresaliente, algo "poco frecuente" en la asignatura de 'Contabilidad de Gestión'. Incluso advirtieron que algunos alumnos que *"no había dado muestras de dominio de la asignatura en las numerosas preguntas que se realizan en el transcurso de las clases mantuvieron la clasificación de sobresaliente"* (Muñoz 2015b) e incluso respondieron correctamente a las preguntas más difíciles. Los estudiantes respondieron a las preguntas *"con las mismas palabras y formatos de esquemas y tablas, fuera del explicado en clase y que se pedía en el examen";* además *"cometían los mismos errores" y realizaban cálculos que sólo se encontraban en un archivo de Excel utilizado por los docentes pero que, debido a su complejidad, no fueron solicitados en el enunciado definitivo, sino que se dieron como un dato directamente"* (Muñoz 2015b).

En la investigación, un estudiante declaró que ”*se trataba de algo que se llevaba haciendo desde hace tiempo. Por los interiores de la Universidad y por fuera se producen intercambios de contraseñas y usuarios y negociaciones monetarias a cambio de obtener el examen final. No sólo en este curso y en esta carrera sino en cualquier curso y carrera. De hecho, muchos alumnos tenían en su poder el examen final y las diferentes pruebas que se han ido realizando a lo largo del semestre*” (Muñoz 2015b). También referían que no se trataba de algo aislado para esa asignatura, sino que era generalizado en el Grado de Administración y Dirección de Empresas.

Se inició una investigación y en septiembre de 2014 se estableció que *“parece ser que una serie de alumnos pertenecientes a la UPO han accedido reiteradamente a correos electrónicos, tanto personales como profesionales, además del servicio que ofrece Dropbox, todo al objeto de aprobar varias asignaturas del departamento de Economía Financiera y Contabilidad”.* Fuentes de la UPO citadas por *ABC* (Moguer, 2015) afirman que los atacantes se hicieron con las contraseñas de las profesoras gracias al uso de un programa de registro de pulsaciones de teclado (k*eylogger).*

En junio de 2015, y pese a que las profesoras habían adoptado precauciones tales como intercambiarse el examen en papel o mediante pendrive en lugar de usar el correo electrónico o Dropbox, vuelven a detectar patrones extraños de comportamiento en el examen y en las respuestas. Según la noticia, *“21 alumnos tenían "errores ilógicos exactamente iguales" y otros 33 mostraban procedimientos "idénticos, casi calcados" que no se habían desarrollado en la asignatura”*. Algunos estudiantes confirman que tenían preparado un grupo de whatsapp con un profesor de una academia privada que recibiría una fotografía del enunciado del examen e iría proporcionando la solución mediante fotografías que llegarían a los teléfonos móviles de los estudiantes. Un correo de un estudiante menciona que hasta un total de 40 estudiantes tuvieron acceso al examen por este procedimiento.

La denuncia se extendió a 7 estudiantes de los cuales 4 fueron imputados.

El *Diario de Sevilla* también informa (Muñoz 2015a) de que "*Las docentes decidieron denunciar después de un alumno le mostrara a una de ellas la foto de un familiar suyo, un menor de edad, que había sido extraída de su ordenador personal*".

En la denuncia de las profesoras, se incluye el testimonio de una estudiante que indicaba que "la sustracción de los exámenes mediante el robo de las claves de los profesores es una *"práctica habitual y conocida entre los alumnos, en todas las carreras y facultades"* y alertaba que "quienes realizan los robos "están sumamente preparados y nunca se les va a pillar porque no dejan rastro" en las direcciones IP desde las que acceden".

En octubre de 2015, el juez decide archivar la causa porque los cuatro alumnos imputados tenían el examen previamente pero *"no existen pruebas de que fuesen ellos mismos quienes lo robaran de los correos de las profesoras y del servicio de almacenamiento Dropbox"* (*«El juez archiva por falta de pruebas el robo de exámenes en la Olavide»* 2015).

2012-2014. Copia en exámenes mediante radiotransmisores ("pinganillos") en la Universidad de León

En el curso 2012/2013 se detectó en la Universidad de León (ULE) la existencia de una trama orienta a facilitar la copia en exámenes de la Facultad de Derecho mediante el método del "pinganillo" (Vega 2014) . Este método consiste en un dispositivo de muy pequeño tamaño que se introduce en el oído y que puede recibir las comunicaciones de alguien en el exterior. En la Figura 1 se muestra uno de los dispositivos que se usaron en la Universidad de León. El estudiante previamente debe transmitir las preguntas al exterior para posteriormente recibir las respuestas. La transmisión puede realizarse enviando una foto, dictándolas haciendo uso de un micrófono ultrasensible o a partir de una filtración anterior del examen.

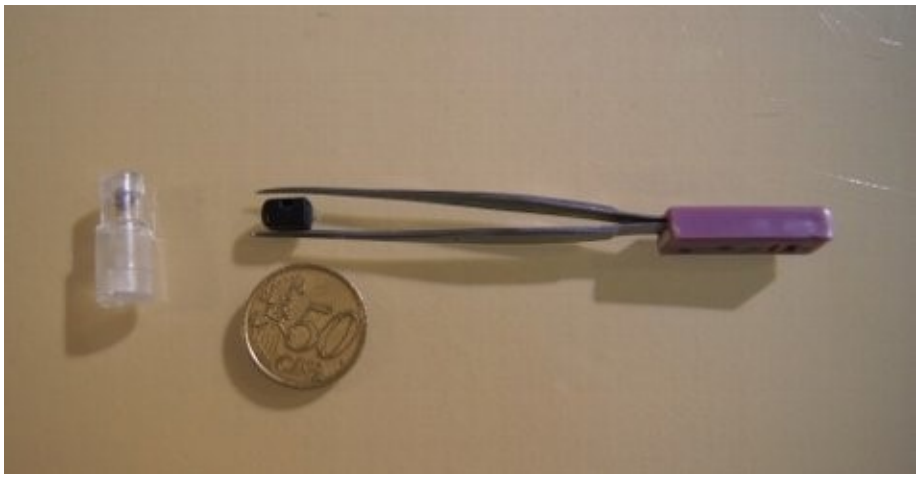

Figura 1. 'Pinganillo' usado en la ULE (Vega 2014)

El sistema completo se muestra en la Figura 2.

Figura 2. "Pinganillo" junto con la conexión al móvil (Vega 2014)

A finales del curso 2012/2013 se conoció que en la Facultad de Derecho existía una trama organizada que se lucraba alquilando los equipos de pinganillos. Para luchar contra la utilización de estos sistemas, la Universidad de León decidió la instalación de inhibidores de frecuencias.

Con respecto a los inhibidores de frecuencias, es importante señalar que existen dudas sobre su legalidad. El Diario *La Nueva España* en su edición del 6 de Junio de 2012 informaba de que la Escuela Politécnica de Ingeniería de Gijón de la Universidad de Oviedo había instalado unos dispositivos inhibidores de frecuencia para luchar contra los pinganillos. En 2014, el gobierno central ordenó a la Universidad de Oviedo retirar los inhibidores de frecuencia (M. 2014), algo que ya había hecho con varias universidades de la Comunidad Valenciana.

En 2016, la Universidad de Almería anunció que implantaría inspecciones aleatorias para la detección de "pinganillos" tras la detección por parte de la Inspección de Servicios de la Universidad de Almería de *"varios episodios de copia organizada y masiva de exámenes"* mediante estos métodos *en "varios centros de la Universidad"* (Europa Press 2016).

2013. Copiar con Whatsapp en la Universidad Politécnica de Catalunya

La Universidad Politécnica de Catalunya (UPC) denunció en 2013 a la Academia Sol en relación con la filtración de las respuestas de un examen de la asignatura 'Electromagnetismo' de segundo curso de la Escuela Técnica Superior de Ingenieros Industriales de Barcelona. De acuerdo con la investigación interna de la universidad, dos estudiantes ajenos a la UPC accedieron al aula donde se hacía la prueba, recogieron el examen y se marcharon de inmediato. Se trataba de un examen tipo test, que respondieron desde fuera con ayuda de la academia (presuntamente). A continuación distribuyeron las respuestas al grupo de alumnos de la academia, con el que estaban conectados vía whatsapp (Playá 2013a).

Los estudiantes que sacaron la prueba no eran alumnos de la asignatura ni siquiera del centro. La alerta dada por algunos alumnos junto con el sorprendente acierto de un grupo de alumnos de la asignatura en el test disparó las alarmas en los profesores de la asignatura.

De acuerdo con la noticia de *La Vanguardia* (Playá 2013a), no se trata del primer incidente de este tipo en la universidad. Hace dos cursos, una academia se hizo con

una copia de un examen y convocó a sus alumnos para distribuirles el ejercicio. Parece que el origen de esa filtración estaba en un control inadecuado de las copias de un examen, por lo que se recomendó que se extremara el control sobre las copias.

A raíz de este incidente, la UPC decidió endurecer la normativa de utilización de dispositivos electrónicos y móviles (Playá 2013b). Entre otras cosas, la normativa establece:

- Para impedir que se saque del aula el enunciado, los estudiantes que salgan antes de la finalización del examen deberán entregarlo al profesor (hasta ahora podían salir veinte minutos antes de su finalización). En todo caso, no podrán salir del aula donde se hace la prueba antes de media hora del inicio y aun así dejarán toda la documentación en la mesa.
- Los estudiantes no podrán tener a su alcance ningún teléfono móvil ni dispositivo de comunicación durante la realización del examen, aunque estén apagados. Estos, juntamente con el material no necesario para la realización del examen, se depositarán en el espacio indicado por el profesor, aunque eso no supondrá ninguna responsabilidad de custodia
- Si a un alumno le suena el móvil en el aula, el profesor podrá suspenderlo.

Por último, la UPC se plantea la adquisición de dispositivos de detección de móviles, que tienen un coste aproximado de 90 €.

2015. Suplantación de identidad en la Universidad de León

El *Diario de León* en su edición del día 7 de Junio de 2015 informa que la Universidad de León ha detectado una decena de suplantaciones de identidad en la realización de exámenes a través de la plataforma online Moodle (Calvo 2015). El vicerrector de Campus y profesor de Industriales, Luis Panizo, informaba que es práctica habitual en su universidad el realizar pruebas de evaluación sobre la plataforma online Moodle. Estas pruebas se realizan desde ordenadores situados en un aula bajo la supervisión de un profesor. Aparentemente, algunos estudiantes facilitaban sus contraseñas a terceras personas que desde fuera del aula y haciendo

uso de documentación y ayuda externa realizaban el examen suplantando su identidad. Estas prácticas se habrían detectado en las Facultades de Derecho, Económicas y Agrícolas.

Para responder ante esta situación, desde el curso 2015/2016 la universidad obliga a los estudiantes a firmar un impreso ('Declaración de honradez académica') en el que declararán su compromiso con la honradez académica durante sus estudios (Universidad de León 2015).

2016. Robo de Datos en la Universidad de Las Palmas de Gran Canaria

Un delincuente informático sustrajo datos personales de 16.000 personas relacionadas con la Universidad de Las Palmas de Gran Canaria (ULPGC) (Cadena SER 2016). Para construir su ataque, empleó las credenciales de un profesor fallecido en el año 2013. Los datos robados pertenecían a estudiantes, profesores y proveedores.

Junto con los datos personales, el atacante había conseguido la sustracción de las contraseñas de muchos de los usuarios del sistema, empleando vulnerabilidades del sistema que le habrían permitido ejecutar un *script* en el servidor de *login* que mandaba las contraseñas de los usuarios cuando estos la introducían a un servidor controlado por el intruso, sustrayendo sus credenciales.

Este es un ejemplo de cómo sustraer de forma masiva credenciales de un sistema que podrán ser empleadas a continuación para robo de exámenes, acceso a sistemas de introducción de calificaciones, aulas virtuales, etc.

2016. Robo de Exámenes en la Universidad de Barcelona

La edición de Cataluña del diario El País del 3 de Agosto de 2016 (Congostrina y Mouzo Quintans 2016) informaba de la imputación de cuatro estudiantes de la Universidad de Barcelona (UB) por robar y vender un examen del grado de Administración y Dirección de Empresas (ADE). Los hechos se remontaban al día 5 de Julio de 2016 cuando se celebró la recuperación del examen de 'Fundamentos de

la Fiscalidad'. Al día siguiente, las profesoras de la asignatura recibieron un correo electrónico anónimo donde se les informaba que el examen había sido robado y vendido a los estudiantes antes de la prueba. Las profesoras dieron verosimilitud a esta denuncia anónima al comprobar que la mayoría de los estudiantes habían cometido un mismo error, error que estaba en uno de los primeros borradores del examen que se intercambiaron por correo electrónico.

La investigación reveló que alguien había accedido, de forma ilegal, a la cuenta de correo electrónico de uno de los profesores y se había apoderado de una primera versión de la prueba final, donde figuraban las preguntas y respuestas del examen. Esta versión contenía el error que después se encontró de forma mayoritaria en los exámenes de los estudiantes.

Tras ser robado, el examen se distribuyó entre el resto de estudiantes por un precio que osciló entre los 20 y los 300 € e incluso horas antes del examen las preguntas circularon por grupos de Whatsapp. Los Mossos estiman que el beneficio que obtuvo cada uno de los imputados fue cercano a los 2.000 € (Redacción 2016).

Ante esta situación, la Universidad de Barcelona (UB) decidió repetir el examen a los 354 alumnos matriculados en la asignatura. Con respecto a la reacción de la UB ante el robo, la universidad manifestó la dificultad de responder antes incidentes de este tipo con el código de rige los derechos y deberes de los estudiantes, que data de 1954, e indicó que junto con las acciones penales que ya ha iniciado, se reservaba el derecho de aplicar sanciones, que serían distintas para los responsables de la sustracción del examen y para los beneficiarios del robo.

Análisis de las Amenazas

En (Foster 2010), se realiza un análisis de las distintas amenazas relacionadas con hacer trampa durante la realización de la prueba y en un robo del contenido de la prueba. Se resumen estas amenazas en la Tabla 1 y Tabla 2.

AMENAZA	AMENAZA
Conocer el contenido del test antes de su aplicación	La persona evaluada obtiene preguntas del test de una fuente de confianza antes de que le sea aplicado
Recibir ayuda de expertos cuando está respondiendo al test	La persona evaluada recibe ayuda del profesor o de otra persona durante el test
Uso de ayudas no autorizadas	La persona evaluada usa ayudas no autorizadas, como chuletas, teléfonos móviles, auriculares, calculadoras programables, etc.
Un suplantador hace el test por la persona evaluada	La persona evaluada se vale de un servicio que proporciona suplantadores o pide a un amigo o colega que haga el test en su lugar.
Manipulación de las hojas de respuestas o de los resultados almacenados	Hecho el test, una persona (por ejemplo, un profesor) puede alterar las hojas de respuesta, cambiando las respuestas erróneas por correctas, o puede cambiar directamente la puntuación asignada al evaluado.
Copia de las respuestas de otra persona	La persona evaluada copia las respuestas de otra persona que está también respondiendo al test.

Tabla 1. Tipos de Amenazas relacionadas con hacer Trampas
(Fuente: International Test Commission 2014)

AMENAZA	AMENAZA
Robo de los archivos que contienen el test o los cuadernillos	El contenido del examen es especialmente vulnerable al robo en algunas etapas de la distribución del test (por ejemplo, cuando los archivos se almacenan en el servidor o los cuadernillos están guardados en un despacho o almacén). Los ladrones pueden conseguir todo el contenido del test y las respuestas correctas si los controles del acceso son inadecuados
Robo de las preguntas del test mediante fotografía digital o dispositivos de copia	Las preguntas del examen se pueden conseguir durante la aplicación del test. Un ladrón puede utilizar una cámara digital oculta e indetectable u otros dispositivos de copia (por ejemplo, bolígrafos que escanean).
Robo de las preguntas mediante la grabación electrónica del contenido de la prueba	En el caso de los tests informatizados, se puede grabar una sesión completa de la aplicación del test, incluyendo todas las preguntas de la prueba, con un procedimiento de registro digital conectado a uno de los puertos de salida del ordenador
Memorización del contenido de la prueba	La persona evaluada memoriza preguntas que son recordadas y grabadas en un momento posterior. Dado que hace falta un esfuerzo colectivo organizado para memorizar todas las preguntas, a este tipo de robo se le denomina "robo organizado".
Transcripción verbal de las preguntas	El contenido oral o escrito puede obtenerse durante la aplicación del test utilizando aparatos de grabación de audio o de texto, como teléfonos móviles, radios bidireccionales o tomando notas con un dispositivo electrónico o en papel.
La obtención de material del test a partir de alguien que trabaja para el programa	Un empleado o responsable de elaborar un programa de evaluación con tests puede robar el contenido de la prueba durante su desarrollo, publicación o distribución

Tabla 2. Tipos de amenazas relacionadas con el robo del contenido
(Fuente: International Test Commission 2014)

En (International Test Commission 2014) se realiza la siguiente valoración del impacto de los distintos tipos de amenazas.

"Que una persona sola, con sus propios medios, haga trampas al responder al test es probable e incluso frecuente en cualquier programa de evaluación con tests. El daño ocasionado generalmente se limita a una sola decisión errónea pues solo hay una puntuación incorrecta. Por otro lado, un cuadernillo robado y distribuido online puede aumentar indebidamente las puntuaciones de miles o decenas de miles de personas evaluadas. Este evento es menos probable, pero produce un daño mucho mayor"

Por tanto, y tal como se recomienda en (International Test Commission 2014), cada organización debe decidir cómo repartir los recursos existentes para responder a las amenazas relacionadas con la realización de trampas de forma individual y a aquellas que vienen de una filtración y distribución de los enunciados de las pruebas.

En (Olson y Fremer 2013), y en el ámbito de la prevención de fraude en exámenes, se identifican los principales riesgos y se clasifican por su ventana de oportunidad, tal y como se muestra en la Tabla 3. La Tabla 3 refleja también si los riesgos afectan a exámenes convencionales (P&P, 'Pen and Paper'), a exámenes realizados mediante ordenador (CBT, *Computer-Based Tests*, y CAT, *Computer-Assisted Tests*)

RISK OF VARIOUS TYPES OF TEST SECURITY BREACHES

BEFORE, DURING, AND AFTER	P&P	CBT	CAT
Lost or stolen booklets	*		
Obtaining unauthorized access to secure exam materials	*	*	*
Educators logging into tests to view questions or change responses		*	*
Hacking into computers		*	*
BEFORE			
Educators or students engaging others to take an exam on a student's behalf	*	*	*
DURING			
Students giving or receiving unauthorized assistance from other students during an examination	*	*	*
Teachers providing answers to students during testing	*	*	*
Students accessing non-allowable resources (notes, textbooks, the Internet)	*	*	*
Use of actual exam questions or answers during the test	*	*	*
Accommodations being used inappropriately to cheat	*	*	*
Keystroke logging		*	*
AFTER			
Altering exam scores	*	*	*
Reconstructing exam materials through memorization	*	*	*
Memorized test items or answers being posted online	*	*	*
Printing, emailing, or storing test information in a computer outside the test delivery system		*	*
Accessing test materials or scores during the transfer of data	*	*	*

Tabla 3. Riesgo de distintos tipos de amenazas de seguridad en exámenes. (Fuente: Olson y Fremer 2013)

En el repaso de los incidentes de seguridad en exámenes en universidades españolas, se muestra como parte de los problemas están directamente relacionados con la posibilidad de que los estudiantes tengan acceso directo o indirecto a móviles u otros dispositivos con capacidad de conectarse a Internet. La experiencia de la UPC muestra que no es suficiente con hacer que los estudiantes guarden sus teléfonos móviles, sino que es necesario establecer una política más estricta. Esto está relacionado con la extraordinaria habilidad que muestran los estudiantes en el manejo de los dispositivos móviles, que les permite enviar, recibir mensajes o manipular el dispositivo sin ni siquiera mirarlos. Es necesario tener esta habilidad de los estudiantes actuales en cuenta a la hora de realizar este análisis de riesgos.

En el apartado siguiente, se establece un conjunto de recomendaciones a partir de las amenazas determinadas en este apartado y las identificadas tras el análisis de los incidentes de seguridad en otras universidades.

Recomendaciones

A partir del análisis de los incidentes anteriores y de las buenas prácticas por distintos organismos, propongo a continuación un conjunto de recomendaciones orientadas a la custodia y protección de exámenes para evitar su filtración o acceso no autorizado. Están orientadas al contexto de la Universidad de Alcalá pero su extensión a otros centros sería muy sencilla.

Elaboración del examen

La protección del contenido de las pruebas comienza en el instante en que se inicia la confección del examen o prueba. Por tanto, las medidas de protección deben comenzar por los medios informáticos que se empleen para la edición del examen.

Como recomendaciones genéricas se establecen las siguientes:

1. Se recomienda no emplear equipos compartidos o públicos y, en general, todos aquellos equipos cuyas medidas de protección se desconozcan.
2. Se recomienda que el equipo cuente con las siguientes medidas de seguridad:
    a. Software actualizado, tanto sistema operativo como aplicaciones, especialmente en lo referente a las actualizaciones de seguridad
    b. Deberá disponer, al menos, de software antivirus siendo recomendable que además tenga instalado software de tipo cortafuegos.
    c. El acceso al equipo deberá realizar con unas credenciales (usuario y contraseña) de uso exclusivo para el docente. La contraseña deberá ser lo suficientemente larga y compleja como para que no pueda ser adivinada por un intruso.

d. Se recomienda que el equipo tenga activadas las funcionalidades de cifrado de disco duro, para disponer de protección frente al extravío o robo del equipo.

3. La carpeta o carpetas donde se almacene el fichero deberán ser preferiblemente locales. Si no es imprescindible, evite el almacenamiento del examen en servicios de almacenamiento en la nube

La mayor parte de las filtraciones de contenido de pruebas están relacionadas con los mecanismos y medios empleados para el envío y compartición de las mismas. A continuación, ponemos algunos ejemplos de errores o descuidos que pueden llevar a la filtración de la prueba:

1. Se guarda una copia del examen en un pendrive y el pendrive se extravía. Si el fichero no está protegido por contraseña, el contenido de la prueba puede hacerse público.
2. El profesor almacena el contenido de la prueba en un disco duro USB que emplea para otros usos como, por ejemplo, para recoger prácticas de los estudiantes de los puestos de laboratorio. El profesor pincha el disco USB en un equipo del alumno y el estudiante guarda una copia del contenido del disco, con la prueba incluida.
3. El profesor envía un borrador de la prueba a sus compañeros de asignatura por correo electrónico e incluye por error a un destinatario no deseado. Resultado: la prueba se ha filtrado.
4. El profesor reenvía por error el correo que contiene la prueba a un destinatario no deseado. Resultado: la prueba se ha filtrado
5. El profesor comparte el fichero con sus compañeros empleando Dropbox y por error incluye a un destinatario no deseado o usa una carpeta pre-existente que está compartidas por destinatarios no autorizados para acceder a esta información

RECOMENDACIÓN:
El fichero o ficheros que contengan la prueba se deben almacenar cifrados o protegidos por contraseña.

La contraseña para la protección del documento debe tener al menos 8 caracteres, no debe ser predecible (no incluya el nombre de la asignatura, de los profesores implicados, de la universidad…) y no debe comunicarse empleando el mismo medio que se emplee para intercambiar el documento protegido. Se recomienda distribuir la contraseña por teléfono o comunicándola en persona.

Si por algún motivo debe transmitir la prueba por medios electrónicos (correo electrónico), almacenarla en un servicio en la nube (Dropbox, Google Drive…) o transportarla en un medio de almacenamiento externo (disco duro USB), los ficheros que contengan la prueba deben estar protegidos por contraseña.

Cómo proteger un fichero Word con contraseña **(Windows)**
Cómo proteger un fichero Word con contraseña **(Mac)**
Proteger contenido en Libreoffice **(Distintas plataformas)**
Proteger un fichero comprimido con contraseña usando 7-zip **(Windows)**

Comunicación e intercambio de la prueba

Utilización del correo electrónico

Si necesita intercambiar el fichero o ficheros de la prueba por correo electrónico, se recomienda que emplee el correo electrónico de la universidad. La universidad de Alcalá ha establecido unos mecanismos de seguridad y control de acceso que aseguran un nivel de protección suficiente ante intrusos. Sin embargo, no podemos determinar ni influir en las medidas que tenga implantadas un proveedor externo.

El mayor de los riesgos está relacionado con la protección de las contraseñas en los proveedores externos. Es muy probable que usted o alguno de sus compañeros esté empleando una contraseña débil o predecible o que se haya filtrado en Internet, tal y como veremos más adelante.

Si usted está reenviando su correo de la universidad a un proveedor externo, como Gmail, el problema es exactamente el mismo, dado que un intruso que tenga acceso a su Gmail, tendría acceso también a sus correos.

RECOMENDACIÓN:
Se recomienda **no consultar su correo electrónico desde un equipo público, compartido o desde un puesto de laboratorio**, dado que esos equipos podrían tener software que registre su actividad y almacene su correo electrónico o incluso su contraseña.

Si se ve obligado a hacerlo, no olvide cerrar su sesión, borrar los datos almacenados y los ficheros que haya podido descargar, incluyendo su eliminación de la papelera de reciclaje. Puede ser recomendable también cambiar su contraseña.

RECOMENDACIÓN:
Si intercambia ficheros con el contenido de las pruebas por correo electrónico, debería **proteger esos ficheros con contraseña**.

Para su protección personal, se recomienda activar la verificación en dos pasos en sus cuentas de Gmail, Outlook o Yahoo:

Verificación en dos pasos en Google
Verificación en dos pasos en Outlook
Verificación en dos pasos en Yahoo

Utilización del Servicio de Almacenamiento Online

Cada vez es más frecuente la utilización de servicios de almacenamiento online como Dropbox o Google Drive para guardar nuestros propios ficheros o especialmente para guardar aquellos ficheros que deseamos compartir con otros. Debemos ser especialmente cautelosos en el uso de Dropbox y Google Drive.

La Universidad de Alcalá pone el servicio de toda la comunidad el servicio OneDrive para la Empresa. En caso de necesitar un servicio de almacenamiento online, se recomienda emplear este servicio frente a otros como Dropbox o Google Drive, sobre los que la universidad no tiene ningún control ni mecanismo de auditoría. Los problemas de usar servicios como Dropbox o Google Drive son los siguientes:

1. No tenemos ningún control sobre las contraseñas usadas para el acceso a estos servicios. Es posible que algunos de los usuarios con los que compartamos la información tengan contraseñas débiles o incluso que se hayan filtrado en Internet

2.

NOTICIA:
'Filtradas 68 Millones de Contraseñas de Dropbox. ¿Está la tuya entre ellas? (Septiembre 2016)

3. Muchos usuarios reutilizan su contraseña en muchos servicios. Esto es un riesgo porque si se filtra su contraseña en uno de los servicios, un atacante podría emplearla para acceder a otros servicios. Por tanto, podemos ser vulnerables sin saberlo.

WEB:
Esta web permite comprobar si tu contraseña se ha filtrado:

4. En caso de un incidente, no es posible obtener desde la universidad la información de quién ha accedido a los ficheros almacenados y desde dónde, lo que dificulta la posterior investigación de un problema de filtración.
5. Se trata de servicios abiertos, por lo que cualquier persona puede crear una cuenta, y con políticas de seguridad que no están controladas por la universidad.

RECOMENDACIÓN:
Si necesita compartir la prueba con otros profesores, **se recomienda que utilice el servicio corporativo OneDrive para la Empresa**.

Los servicios Microsoft Office 365 y han sido auditados y encontrados conforme con las exigencias del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, para el máximo nivel que define la normativa (nivel alto). Esta normativa define los requisitos de seguridad que la administración ha definido para los servicios que las administraciones públicas proporcionan por medios electrónicos. Junto a esta obligación legal, esta plataforma cumple con otras muchas como puede comprobarse aquí: https://www.microsoft.com/online/legal/v2/es-es/MOS_PTC_Security_Audit.htm .

Figura 3. Sello de Conformidad con el ENS

Cómo compartir un fichero en OneDrive para la Empresa
Compartir archivos o carpetas en Office365

RECOMENDACIÓN:
Se recomienda **no intercambiar directamente los ficheros por correo electrónico**. En lugar de adjuntar directamente los ficheros, haga **referencia a los enlaces o carpetas almacenados en OneDrive para la Empresa**. De este modo, evitamos los riesgos de filtraciones del correo o envíos por descuido.

Impresión del examen

Una vez que se ha terminado la preparación del examen, pasamos a la fase de impresión del examen. Esta es una fase crítica que debemos proteger para evitar la filtración del examen. En esta fase, tenemos que vigilar que no hay filtraciones ni de la copia física ni de la versión electrónica del examen.

RECOMENDACIÓN:
La impresión sólo debe realizar en sistema de impresión de confianza y controlados y gestionados por la Universidad de Alcalá. No imprima el examen en servicios externos tales como reprografías externas o servicios ajenos a la Universidad de Alcalá.

Si se decide imprimir el examen en los medios del departamento, es importante vigilar que no se produzca ninguna filtración o pérdida de alguna de las copias. Dado que en muchas ocasiones la impresora se encuentra en una ubicación distinta a la del equipo desde el que se lanza la impresión, puede existir un lapso de tiempo en el que las copias impresas están desatendidas.

RECOMENDACIÓN:
Idealmente, **la impresora deberá estar en una sala de acceso restringido al personal del departamento.**

RECOMENDACIÓN:
Para evitar esto, se recomienda el uso de los **servicios de impresión protegida o de impresión desde dispositivo USB**.

La utilización de estos servicios dependerá del modelo de impresora utilizada. Queda fuera del ámbito de este documento, pero es muy importante también aplicar las medidas de seguridad apropiadas a la impresora o dispositivo multifunción, dado que es otra posible fuente de incidentes de seguridad.

RECOMENDACIÓN:
Opcionalmente, puede imprimir una copia del examen en una impresora local y **generar las copias a partir de esa primera copia mediante la función de fotocopiadora**.

RECOMENDACIÓN:
Es importante **verificar que el número de copias que se recogen de la impresora coincide con el número de copias solicitadas.**

Si esto no sucede, podemos estar ante un posible caso de sustracción de la prueba y debería actuarse informando de este hecho.

Durante el examen

Los alumnos deberán identificarse antes de acceder al aula del examen con su DNI o pasaporte. No se deberá permitir el acceso al aula a aquellos estudiantes no identificados o que no figuren en la lista de convocatoria del examen.

RECOMENDACIÓN:
Establecer una política de **prohibición de uso de dispositivos electrónicos en el examen**. Esto incluye ordenadores, *tablets*, relojes inteligentes y en general cualquier dispositivo con capacidad de comunicación inalámbrica.

RECOMENDACIÓN:
Se recomienda que los alumnos depositen todas sus pertenencias, salvo las estrictamente necesarias para realizar el examen, en sus taquillas o en la tarima del aula.

Si el profesor detecta comportamientos extraños de alguno de los estudiantes durante el examen conviene anotar esos comportamientos, junto con la ubicación del estudiante para su posterior análisis.

Después del examen

En este apartado, no vamos a entrar en consideraciones relativas a la protección de las pruebas escritas, sino que sólo nos centraremos en cómo evitar los riesgos relacionados con las tecnologías de la información.

Simplemente comentaremos aquí, que la presencia de patrones extraños de respuestas (e.g., fallos en las preguntas sencillas y aciertos en las complejas), la aparición repetida del mismo error en el examen de muchos estudiantes o una coincidencia elevada con la solución que haya preparado el profesor con antelación al examen, puede estar relacionada con la existencia de alguna irregularidad en el examen, tal y como hemos visto en los casos de incidentes de seguridad en exámenes en universidades. En ese caso, ponga el caso en conocimiento de la universidad.

RECOMENDACIÓN:
Si se emplea una **hoja de cálculo para almacenar las puntuaciones** de cada una de las partes del examen, **esta hoja de cálculo deberá estar almacenada en un equipo seguro y protegida mediante contraseña**.

RECOMENDACIÓN:
No intercambiar la hoja de cálculo con los resultados por correo electrónico.

RECOMENDACIÓN:
Es conveniente **registrar las ediciones sobre dicha hoja de cálculo** para poder identificar y detectar modificaciones no autorizadas.

Si se almacena la hoja de cálculo en OneDrive para la Empresa, se dispone de un servicio donde quedan reflejadas las sucesivas versiones del documento, lo que puede ayudar para este fin.

Una vez que se dispone de todas las calificaciones, el siguiente paso es proceder a su publicación en Aula Virtual o en Portal.

RECOMENDACIÓN:
La publicación de notas deberá realizarse desde un sistema seguro y desde una red de confianza, preferiblemente desde la red de la UAH. **Si se accede desde fuera de la red de la UAH, se recomienda emplear el servicio de acceso mediante VPN**, para evitar intercepciones de las comunicaciones.

RECOMENDACIÓN:
Se recomienda realizar una **comprobación adicional antes de cerrar el acta para comprobar que las notas que se publican coinciden con las notas que figuran en la hoja de cálculo o sistema de registro de notas.**

Conclusiones

Este documento presenta una aproximación al problema de la seguridad de los exámenes en universidades, con orientación hacia la protección de todo el proceso de los exámenes tradicionales, desde la elaboración a la evaluación de los mismos.

Durante años, la universidad ha desarrollado y aplicado procedimientos para garantizar la integridad de los procesos de evaluación. La incorporación de las tecnologías de la información en el proceso de elaboración, corrección y evaluación de los exámenes obliga a adoptar un conjunto de medidas adicionales para asegurar la integridad del proceso, protegiendo el contenido de las pruebas y garantizando que no se producen modificaciones no autorizadas en las calificaciones de las mismas. Además, el propio acto del examen debe adoptar medidas adicionales orientadas a dificultar la comisión de fraude en el proceso mediante distintos mecanismos como la utilización de dispositivos de radiofrecuencia o la asistencia remota no autorizada. Por último, incidir en la necesidad de fortalecer los procesos de identificación y autenticación en línea, por su criticidad, para evitar el robo de credenciales y la suplantación de identidades, que están detrás de la mayoría de las amenazas expuestas.

Para concluir, indicar que este documento sólo presenta una visión parcial y que deberá integrarse con el resto de procesos de seguridad que existan definidos en la organización y complementarse con otros aspectos de seguridad en pruebas, en concreto para las pruebas realizadas en línea.

Referencias

- ALMOGUERA, Pablo D. (2012/04/04). Detenidos tres estudiantes por cambiar notas de la Universidad. En *ABCdesevilla.* Disponible en http://sevilla.abc.es/20120329/andalucia/sevp-detenidos-tres-estudiantes-cambiar-20120329.html

- ARENCIBIA, Ángeles. (2008/10/07). La ULPGC investiga el robo de un examen en medicina. En *Canarias7.es.* Disponible en http://www.canarias7.es/articulo.cfm?id=111277

- ARJONA, Araceli R. (2012/09/23) Roban exámenes y no pasa nada. En *Diario de Córdoba.* Disponible en http://www.diariocordoba.com/noticias/cordobalocal/roban-examenes-no-pasa-nada_747745.html?inicio=10&id=747745

- BECERRA, Juanjo.
  - **a** (2002/02/27). Un hacker se cuela en Alcalá. En *Campus. El Mundo*. Disponible en http://www.elmundo.es/campus/2002/02/27/actualidad/CAM204181_1.html
  - **b** (2002/03/05). El hacker de Alcalá entierra el hacha de guerra. En *Campus. El Mundo.* Disponible en http://www.elmundo.es/campus/2002/03/05/actualidad/CAM218489_1_impresora.html

- CABRERO, José E. (2007/08/11). Un “hacker” burla la seguridad informática en la facultad y roba datos de alumnos y profesores. En *Ideal.es.* Disponible en http://www.ideal.es/granada/20071108/granada/hacker-burla-seguridad-informatica-20071108.html

- CADENA SER. (2016/03/31). Un alumno de la ULPGC robó 16.000 datos de usuarios del centro universitario. En *SER Canarias.* Disponible en http://cadenaser.com/emisora/2016/03/31/ser_las_palmas/1459424849_529168.html

- CALVO, A. (2015/06/07). La Universidad detecta una docena de suplantaciones de identidad en exámenes. En *Diario de León.es.* Disponible en http://www.diariodeleon.es/noticias/leon/universidad-detecta-docena-suplantaciones-identidad-examenes_984898.html

- CANO, Juan. (2016/12/21). Absuelven a tres alumnos de la UMA acusados de "hackear" un ordenador para aprobar. En *Sur.es.* Disponible en http://www.diariosur.es/malaga-capital/201610/21/absuelven-tres-alumnos-acusados-20161020223532.html

- CHAVES, J.R. (2014/12/26). Fraude en la Universidad: copiar impunemente con los smartphone. En *delajusticia.com.* Disponible en https://delajusticia.com/2014/12/26/fraude-en-la-universidad-copiar-impunemente-con-los-smartphone

- CONGOSTRINA, Alfonso L.; MOUZO QUINTANS, Jessica. (2016/08/03). Imputados cuatro alumnos de la UB por robar y vender un examen. En *El País.* Disponible en http://ccaa.elpais.com/ccaa/2016/08/02/catalunya/1470167114_416118.html

- EL ESPAÑOL. (2016/08/02). Roban un examen de ADE y lo venden por 300 euros. En *Crónica Global Vida. El Español.* Disponible en http://cronicaglobal.elespanol.com/vida/roban-un-examen-de-ade-y-lo-venden-por-300-euros_43883_102.html

- E. M. (2014/01/10). Varios centros tuvieron que retirar inhibidores de frecuencia por orden del Gobierno central. En *La Nueva España.* Disponible en http://www.lne.es/asturias/2014/01/10/centros-tuvieron-retirar-inhibidores-frecuencia/1525475.html

- EUROPA PRESS.
  - (2010/04/15). Detenido un "hacker" tras vulnerar los sistemas informáticos de la universidad. En *El Periódico de Aragón.* Disponible en http://www.elperiodicodearagon.com/noticias/aragon/detenido-hacker-vulnerar-sistemas-informaticos-universidad_574446.html
  - (2016/06/01). La UAL detecta "copias organizadas" en exámenes con pinganillos y móviles. En *La Voz de Almería.* Disponible en http://www.lavozdealmeria.es/Noticias/107616/2/La-UAL-detecta

- FOSTER, D. F. Worldwide Testing and Test Security Issues: Ethical Challenges and Solutions. En *Ethics & Behavior,* 20 (3-4), 2010, p. 207-228. DOI:10.1080/10508421003798943.

- INTERNATIONAL TEST COMMISSION. *The ITC Guidelines on the Security of Tests, Examinations, and Other Assessments*. International Test Commission, 2014.

- MOGUER, Manuel. (2015/02/26). La universidad Pablo de Olavide investiga una supuesta red de tráfico de exámenes. En *ABCdesevilla*. Disponible en http://sevilla.abc.es/sevilla/20150225/sevi-olavide-investigacion-201502241041.html

- MOLIST, Mercé. (2013/07/24). Cap. 6. Paranoia.com». En *Hackstory.es*. Disponible en http://hackstory.net/Ataque_Universitat_Rovira_i_Virgili

- MUÑOZ, Jorge.
  - **a** (2015/10/11) Las profesoras se sintieron como "marionetas" de los alumnos. En *Diario de Sevilla.* Disponible en http://www.diariodesevilla.es/sevilla/profesoras-sintieron-marionetas-alumnos_0_961404215.html
  - **b** (2015/10/11) Tráfico de Exámenes en la Olavide. En *Diario de Sevilla.* Disponible en http://www.diariodesevilla.es/sevilla/Trafico-examenes-Olavide_0_961404343.html

- OLSON, John F.; FREMER. John. 2013. *TILSA Test Security Guidebook.* 2013

- PLAYÁ, Josep.
  - **a** (2013/03/06). La UPC denuncia ante la fiscalía a una academia por filtrar un examen. En *La Vanguardia.* Disponible en http://www.lavanguardia.com/vida/20130306/54369022886/upc-denuncia-fiscalia-academia-filtrar-examen.html
  - **b** (2013/04/05). La UPC endurece la normativa para evitar que los alumnos copien con los móviles. En *La Vanguardia.* Disponible en http://www.lavanguardia.com/vida/20130405/54372009958/la-upc-endurece-la-normativa-para-evitar-que-los-alumnos-copien-con-los-moviles.html

- RUIZ, Luis J. (2016/05/22). Marianistas sanciona a cuatro alumnos de Bachillerato por robar y vender exámenes. En *La Rioja.com.* Disponible en http://www.larioja.com/la-rioja/201605/20/marianistas-sanciona-cuatro-alumnos-20160520013416-v.html.

- SEVILLA DIRECTO. (2015/10/15). El juez archiva por falta de pruebas el robo de exámenes en la Olavide. En *Sevilla Directo.* Disponible en http://www.sevilladirecto.com/el-juez-archiva-por-falta-de-pruebas-el-robo-de-preguntas-de-examenes-en-la-olavide

- TORO, Victoria. (2013/03/12). Harvard expulsa a 60 alumnos por copiar en los exámenes. En *La Voz de Galicia*. Disponible en http://www.lavozdegalicia.es/noticia/sociedad/2013/03/12/harvard-expulsa-60-alumnos-copiar-examenes/0003_201303G12P29991.htm

- UNIVERSIDAD DE LEÓN. *Pautas de actuación en los supuestos de plagio, copia o fraude en exámenes o pruebas de evaluación.* 2015. Disponible en http://centros.unileon.es/cienciasdeltrabajo/files/2013/07/pautas-de-actuaci%C3%B3n-en-los-supuestos-de-plagio-copio-o-fraude-en-ex%C3%A1menes-o-pruebas-de-evaluaci%C3%B3n.pdf

- VEGA, A. (2014/02/18). “La trama del pinganillo”, tecnología contra ética en la Universidad de León. En *ileón.com.* Disponible en http://www.ileon.com/universidad/037309/la-trama-del-pinganillo-tecnologia-contra-etica-en-la-universidad-de-leon