



Universidad
Carlos III de Madrid

**Máster en Derecho de Telecomunicaciones, Protección
de Datos, Audiovisual y Sociedad de la Información**

2014-2015

Trabajo Fin de Máster

**“Informe a la UC3M sobre cómo permitir el
uso de ordenadores, *smartphones* y *tablets*
durante exámenes y pruebas académicas”**

Fernando Bueno Sastre

Tutor

Agustín Eugenio de Asís Roig

Madrid, 9 de julio de 2015





Resumen:

El uso de una plataforma de *e-learning*, desarrollada basándose en el principio “*privacy by desing*”, garantiza el respeto de la privacidad y el derecho a la protección de datos de carácter personal de los estudiantes. Esto posibilita la realización de exámenes utilizando dispositivos electrónicos –ordenadores, *smartphones* o *tablets*–, de forma presencial o a distancia, de una forma segura y efectiva, generando pruebas electrónicas válidas de los exámenes y de cuantas conductas llevan a cabo los usuarios durante el ejercicio del mismo.

Palabras clave:

Educación, Universidad, TIC, ordenadores, *smartphones*, *tablets*, dispositivos, exámenes, pruebas académicas, plataforma, *e-learning*, *privacy by desing*, medio de prueba, DNI electrónico, privacidad, protección de datos de carácter personal, interés legítimo, Políticas de Uso.

Agradecimientos:

Quiero mostrar mi gratitud a todas aquellas personas que han colaborado con su ayuda, sus consejos y su asesoramiento, que ha culminado en el desarrollo del presente informe jurídico.

En especial, quiero agradecer el apoyo de todo el equipo de profesionales del despacho Castañeda Abogados, S.L., mención particular para Alexandra Juanas Fabeiro y Santiago Antón Ruiz de la Herrán Pidal.

No quiero olvidarme de mis familiares, amigos y compañeros que me han soportado durante este proceso y, deseo, sigan estando ahí de aquí en adelante, agradeciendo su ayuda y, en particular, la de Juan Manuel.

También deseo dar las gracias a todos los profesores del Máster por la aportación, directa o indirecta, en el presente informe y agradecer a mi tutor, Agustín Eugenio de Asís Roig, su colaboración durante la elaboración del mismo.



ÍNDICE

0. <u>Supuesto de hecho</u>	4
1. <u>Introducción</u>	5
2. <u>Observaciones de la situación previa al informe</u>	7
3. <u>Aspectos a tener en cuenta</u>	10
3.1. Derechos fundamentales afectados.....	10
<i>A. Derecho a la educación</i>	10
<i>B. Derecho a la intimidad</i>	10
<i>C. Protección de datos de carácter personal</i>	12
<i>D. Derecho a la propia imagen</i>	13
<i>E. Derecho al secreto de las comunicaciones</i>	14
<i>F. Derecho a la presunción de inocencia</i>	15
3.2. Interés legítimo.....	17
3.3. Seguridad informática.....	20
3.4. Uso de inhibidores de frecuencia en las aulas.....	20
3.5. Uso de otras aplicaciones tecnológicas.....	22
3.6. Medios de generación de prueba electrónica.....	23
3.7. Requisitos y opciones de la herramienta a utilizar.....	24
4. <u>Universidades que permiten el uso de dispositivos electrónicos para la realización de pruebas académicas</u>	29
4.1. Universidades españolas.....	29
4.2. Universidades europeas.....	30
4.3. Universidades no europeas.....	31
5. <u>Conclusión</u>	33
5.1. Plataforma de <i>e-learning</i>	34
5.2. Desarrollo de las pruebas académicas.....	38
5.3. Dispositivos a utilizar y su titularidad.....	40
5.4. Políticas de Uso de los dispositivos.....	42
6. <u>Trabajo futuro</u>	44



7. <u>Bibliografía</u>	45
8. <u>Anexo documental</u>	46
<u>Anexos</u>	53
Anexo I: Aviso de cookies.....	54
Anexo II: Cláusula informativa.....	55
Anexo III: Normas para el uso de los dispositivos.....	57



0- Supuesto de hecho:

La Universidad Carlos III de Madrid (en lo sucesivo, “el cliente”) ha contactado con nuestro despacho ante las crecientes quejas de algunos alumnos por la escasa transparencia y falta de información en relación con la realización de determinadas pruebas académicas, en las que los profesores han permitido utilizar ordenadores durante el desarrollo de los exámenes.

El cliente, ante la incertidumbre de cómo abordar el problema y adoptar una solución que permita la utilización de ordenadores durante las pruebas universitarias, nos ha solicitado que elaboremos un informe jurídico en relación a las implicaciones legales que pueden derivarse de la utilización de ordenadores, *smartphones* y *tablets* (en adelante, “dispositivos”) en exámenes y pruebas universitarias (en lo sucesivo, “pruebas académicas”) que pueda desarrollar el cliente.

En este sentido, el cliente ha manifestado una especial preocupación por la necesidad de utilizar una herramienta de gestión que garantice el respeto de los derechos de los estudiantes, pero que a su vez sea efectiva contra los intentos de algunos alumnos de copiar durante las pruebas. Por ello, desea asumir unos riesgos mínimos para obtener dichos resultados, implantando una metodología de uso de los dispositivos que no genere grandes vulneraciones en la privacidad y la protección de los datos de carácter personal de los alumnos.

Por lo anterior, el cliente ruega que éste despacho le facilite una valoración jurídica acerca de cuáles son las mejores opciones entre las diferentes metodologías de uso de dispositivos en concordancia con las características educativas de la Universidad Carlos III de Madrid, dando una recomendación final sobre cómo podría permitirse, de una forma segura, la realización de dichas pruebas utilizando dispositivos electrónicos.



1- Introducción:

El mundo evoluciona sin descanso, día a día surgen nuevas herramientas tecnológicas con la finalidad de hacer más productiva la vida del ser humano. Mientras ustedes leen este trabajo, quizás alguien se encuentre desarrollando alguna aplicación, programa o dispositivo que les puede ayudar en un futuro cercano en sus quehaceres diarios, en sus funciones profesionales o, simplemente, les proporcionará entretenimiento.

Diferentes estudios, como el publicado en el año 2007 por profesores de la Universidad Autónoma de Madrid y de la Universidad Pública de Navarra¹ han demostrado que la utilización de las Tecnologías de la Información y la Comunicación (en adelante, las “TIC”) no sólo genera un incremento en la productividad de las personas. Además, las TIC permiten que, organizaciones con una estructura tradicional, se vean inmersas en un proceso de transformación al dotarles de mayor flexibilidad en su ámbito de actuación. Este marco evolutivo no es indiferente para ningún sector socioeconómico, pues todos se ven afectados, en mayor o menor medida, por la implantación de las TIC.

Las sinergias entre la educación y el uso de las TIC en esta área han suscitado varios estudios al respecto, como el artículo publicado por Martin Carnoy², el publicado por Pere Marquès Graells³ o el de Paloma González Pendás⁴. Estas publicaciones destacan el valor añadido que puede generar el uso de las TIC en la educación para fomentar las habilidades digitales y mejorar los procesos de aprendizaje de los alumnos, beneficios que se verán reflejados a largo plazo en la sociedad.

El presente informe jurídico tiene por objeto analizar cómo se pueden implantar el uso de las TIC en la educación y, en particular, la utilización de

¹ BILLÓN CURRÁS, Margarita; LERA LÓPEZ, Fernando; y ORTIZ SERRANO, Salvador. “Evidencias del impacto de las TIC en la productividad de la empresa. ¿Fin de la «paradoja de la productividad»?”. Cuadernos de Economía. Vol. 30, Núm. 82, enero-abril, 2007, págs. 005-036.

² CARNOY, Martin. “ICT in Education: Possibilities and Challenges”. Lección inaugural del curso académico 2004-2005. Disponible en <<http://www.uoc.edu/inaugural04/eng/carnoy1004.pdf>> a 25 de junio de 2015.

³ MARQUÈS GRAELLS, Pere. “Impacto de las TIC en la enseñanza universitaria”, 2000 (revisado en 2007). Disponible en <<http://ddd.uab.cat/pub/dim/16993748n11/16993748n11a5.pdf>> a 25 de junio de 2015..

⁴ GONZÁLEZ PENDÁS, Paloma. “Influencia de las TIC en el crecimiento de las TIC en el crecimiento de la productividad. Un análisis descriptivo”, Revista Economía Industrial (Ministerio de Industria, Energía y Turismo, año 2013, pág. 78. Disponible en <<http://www.minetur.gob.es/Publicaciones/Publicacionesperiodicas/EconomiaIndustrial/RevistaEconomiaIndustrial/390/PALOMA%20GONZALEZ%20PENDAS.pdf>> a 25 de junio de 2015.



ordenadores, *smartphones* y *tablets* para la realización de exámenes y pruebas académicas en la Universidad, prestando especial atención a la condición que tiene la Universidad de fomentar la cultura entre la sociedad a través de la docencia y la investigación y la formación de las personas para su futuro desarrollo profesional.

En primer lugar, se analizarán los derechos de los estudiantes que pueden verse afectados por el uso de dispositivos electrónicos en exámenes y pruebas académicas. Para ello, el informe examinará la normativa aplicable y los pronunciamientos más relevantes que se hayan dictaminado en supuesto similares.

En segundo lugar, se plantearán las posibles recomendaciones aplicables, orientadas a la adecuación de la normativa de la Universidad a todas las exigencias desarrolladas con anterioridad.

Para concluir, el informe aconsejará a la Universidad Carlos III la alternativa a aplicar que este despacho considera más recomendable, en función de las valoraciones que generan las necesidades propias del cliente.



2- Observaciones de la situación previa al informe:

Previa a la realización del presente informe jurídico para la UC3M, este despacho procedió a analizar el marco legal que ampara al cliente, analizando las diferentes normas, reglamentos y códigos de conducta que le son de aplicación.

En este análisis hemos detectado que el cliente carece de un marco jurídico adecuado a sus deseos de permitir el uso de ordenadores, *smartphones* y *tablets* durante la realización de pruebas académicas. En las diferentes normas de la Universidad Carlos III consultadas, sólo se contempla la realización de pruebas académicas por medios electrónicos a aquellos alumnos que se encuentren en cursando sus estudios en situación de un programa de intercambio⁵, pero no es una política de uso o un código de conducta específico para la utilización de dispositivos electrónicos durante un examen.

La otra referencia respecto a los dispositivos electrónicos durante la realización de pruebas académicas se encuentra en la «Guía de buenas prácticas de los estudiantes de la Universidad Carlos III de Madrid»⁶, donde se establecen una serie de indicaciones que, pese a no ser normas como tal, constituyen pautas éticas que ayudan a profesores y estudiantes a conocer cuáles son las conductas adecuadas.

En esta “Guía de buenas prácticas” se fijan una serie de recomendaciones en la realización de exámenes, entre las que se encuentra:

“A. Los estudiantes no pueden acudir a los exámenes o pruebas con medios electrónicos, tales como teléfonos móviles, tablets o cualquier otro, salvo que ‘expresamente’ haya sido autorizado por el profesor. [...]”

Como se puede observar, esta recomendación no habla de la utilización de dispositivos electrónicos durante la prueba académica, si no que trata el asunto de si los alumnos pueden portar dichos dispositivos durante el examen o si deben acceder al aula sin ellos, pero no expresa en ningún caso la posibilidad de que puedan ser utilizados por los alumnos durante el examen.

⁵ Artículos 1 y 2 de la norma en relación a los exámenes en la UC3M “Adaptación de la normativa reguladora de la realización de exámenes por medios electrónicos a los estudiantes de la Universidad Carlos III de Madrid que se encuentren realizando programas oficiales de intercambio, aprobada por el Consejo de Gobierno en sesión de 20 de octubre de 2006, modificada en sesión de 7 de febrero de 2013”.

⁶ Apartado 1 (realización de evaluaciones de conocimientos) de la «Guía de buenas prácticas de los estudiantes de la Universidad Carlos III de Madrid», aprobada por el Consejo de Gobierno en su sesión de 29 de noviembre de 2012.



Este despacho contactó con algunos alumnos de la Universidad Carlos III para conocer la situación real del cliente y, en concreto, si permite el uso de dispositivos durante la realización de pruebas académicas y, en caso de que se autorice dicha utilización, en qué términos se produce.

Una parte de los alumnos encuestados nos informaron que en sus estudios de postgrado –Máster en Derecho de las Telecomunicaciones, Protección de Datos, Audiovisual y Sociedad de la Información– se permitía la utilización de dispositivos tecnológicos con fines de ayuda para consultar la jurisprudencia y normativa que crean conveniente durante la realización de las pruebas académicas. Asimismo, otros alumnos nos informaron de que el cliente, quien dispone de modalidades de titulaciones semipresenciales, en éstas no se prevé la posibilidad de que los alumnos puedan realizar exámenes a distancia, siendo obligatorio su realización de forma presencial.

Por ejemplo, en el Grado de Información y Documentación, en su versión semipresencial, se expresa lo siguiente,

“la normativa de la Universidad Carlos III impide, por el momento, poder realizar los exámenes a distancia (con la única excepción de si el alumno está disfrutando de una beca ERASMUS). Así, para examinarse de las asignaturas matriculadas será necesario acudir presencialmente al Campus en el que se vayan a realizar los exámenes”.

También en otro grado de la Universidad Carlos III, en su versión semipresencial, como el Grado de Humanidades, se establece que la evaluación final será presencial, pero no se fija dicha obligatoriedad para las pruebas académicas de carácter parcial.

En consecuencia, una vez analizada la normativa aplicable al cliente, debemos tener en cuenta que, si bien la normativa no prohíbe el uso de dispositivos tecnológicos, tampoco contempla una política de uso de los mismos, ello puede generar dudas que es necesario resolver. Asimismo, al no estar permitida la realización de exámenes de evaluación final a distancia, salvo en el caso mencionado de alumnos que estén cursando sus estudios en programas de intercambio, se estarían limitando las posibilidades que la tecnología ofrece en la actualidad y que el cliente, al solicitarnos la elaboración del presente informe, desea solventar.

Por todo lo anterior, procederemos a analizar todos los aspectos que se deben tener en cuenta a la hora de informar y recomendar al cliente cuales son los métodos que puede adoptar, ofreciendo unas medidas adecuadas que ofrezcan garantías de calidad educativa y seguridad jurídica, como elementos de excelencia que persigue nuestro cliente, permitiendo que sus alumnos puedan realizar las pruebas académicas



utilizando durante las mismas dispositivos tecnológicos prestados por la Universidad o que sean propios del alumnado, y que estas pruebas puedan desarrollarse dentro del recinto Universitario o fuera del mismo.



3- Aspectos a tener en cuenta:

3.1- Derechos fundamentales afectados:

A. Derecho a la educación:

La educación es un derecho fundamental, como recoge nuestra Constitución en su artículo 27 de la Constitución, que establece

“1. Todos tienen el derecho a la educación. Se reconoce la libertad de enseñanza. [...]”

8. Los poderes públicos inspeccionarán y homologarán el sistema educativo para garantizar el cumplimiento de las leyes. [...]”

10. Se reconoce la autonomía de las Universidades, en los términos que la ley establezca”.

El derecho fundamental a la educación promueve la libertad y la autonomía personal, garantizando el desarrollo de la persona y reduciendo las probabilidades de discriminación y exclusión social, permitiendo que quien se encuentra social y económicamente marginado tenga una oportunidad de salir de la pobreza por su propio esfuerzo y desarrolle su vida en comunidad, según recoge la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO) en su página web.

Como tal, y dentro del marco de la estrategia comunitaria Europa 2020, que busca el impulso de la economía mediante la implantación a nivel europeo de las TIC en los diferentes sectores, nuestro cliente ha solicitado un informe que busque aclarar el marco legal aplicable para permitir, garantizando el respeto de los derechos de los estudiantes, que se puedan utilizar durante las pruebas académicas ordenadores, *smartphones* y *tablets*, siempre con un adecuado control por parte del profesorado para evitar posibles conductas inapropiadas de los alumnos.

B. Derecho a la intimidad:

El artículo 18.1 de la Constitución Española expresa que *“1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen”*. Asimismo, la jurisprudencia asentada⁷ expresa que *“el derecho a la intimidad personal, en cuanto derivación de la dignidad de la persona (art. 10.1 C.E.), implica ‘la existencia de un*

⁷ Tribunal Supremo, Sala Segunda, de lo Penal, Sentencia 311/2015, de 27 mayo. JUR 2015\154238, que hace referencia a lo dispuesto en la STC 207/1996, de 16 de diciembre, Fundamento Jurídico Tercero (apartado B).



ámbito propio y reservado frente a la acción y el conocimiento de los demás, necesario, según las pautas de nuestra cultura, para mantener una calidad mínima de la vida humana' [...]".

El derecho a la intimidad se puede ver afectado en diferentes ámbitos, como podría ser el ámbito laboral o el penitenciario. En estos ámbitos, el derecho a la intimidad de un individuo cederá frente a otros bienes jurídicamente protegidos cuando estén justificados y resulten medidas proporcionales sobre la base de otros derechos o bienes jurídicamente protegidos de interés general, como sería el derecho a la educación y la protección del interés legítimo de la Universidad de garantizar el mismo trato a los alumnos y que algunos estudiantes no utilicen métodos fraudulentos durante los exámenes, lo que implicaría un perjuicio para aquellos alumnos que actúan respetando las reglas fijadas por las Leyes y disposiciones de la Universidad.

En derecho laboral⁸, el ámbito de cobertura del derecho a la intimidad se determina en virtud de las expectativas de privacidad que puede tener un trabajador al utilizar los dispositivos o aplicaciones, como el correo electrónico, según las circunstancias de cada caso concreto. De esta forma, no se entenderá vulnerado el derecho a la intimidad del trabajador si la empresa hubiera establecido ciertas normas o reglas de uso –política de uso de los recursos, por ejemplo– y se las hubiera comunicado de forma fehaciente a los trabajadores. Esta conclusión se alcanzó tras la realización de un juicio de proporcionalidad entre los derechos de los trabajadores y el derecho del empresario, y así lo contempla el artículo 20.3 del Estatuto de los Trabajadores, que establece

"3. El empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad humana y teniendo en cuenta la capacidad real de los trabajadores disminuidos, en su caso".

En consecuencia, hay bases legales y jurisprudenciales –como veremos en el apartado "interés legítimo"– para defender el control por parte de la Universidad del uso los dispositivos que realizan los alumnos durante las pruebas académicas, por analogía con el control empresarial de los trabajadores, siempre que se trate de medidas proporcionales que respeten los derechos de los estudiantes. Por tanto, la Universidad podrá prever medidas proporcionales y no excesivas que garanticen el respeto del derecho a la intimidad de los alumnos, en virtud de lo dispuesto en el Real Decreto 1791/2010, de 30 de diciembre, por el que se aprueba el Estatuto del Estudiante Universitario.

⁸ FERNÁNDEZ DÍEZ, Antonio. *"Límites y garantías del trabajador en el uso del ordenador de la empresa"*. Disponible en <http://portaljuridico.lexnova.es/articulo/JURIDICO/112513/limites-y-garantias-del-trabajador-en-el-uso-del-ordenador-de-la-empresa> a 25 de junio de 2015.



El artículo 13 del Real Decreto 1791/2010, en relación con los deberes de los estudiantes universitarios, establece que:

“1. Los estudiantes universitarios deben asumir el compromiso de tener una presencia activa y corresponsable en la universidad, deben conocer su universidad, respetar sus Estatutos y demás normas de funcionamiento aprobadas por los procedimientos reglamentarios.

2. Entendidos como expresión de ese compromiso, los deberes de los estudiantes universitarios serán los siguientes:

[...]

c) Cuidar y usar debidamente los bienes, equipos, instalaciones o recinto de la universidad o de aquellas entidades colaboradoras con la misma.

d) Abstenerse de la utilización o cooperación en procedimientos fraudulentos en las pruebas de evaluación, en los trabajos que se realicen o en documentos oficiales de la universidad. [...]”.

Asimismo, como consecuencia de la utilización de dispositivos por los alumnos, se está generando jurisprudencia en relación con el acceso a dispositivos tecnológicos por personal de centros educativos y en los que se ha confirmado que no suponen un acceso ilegítimo a los mismos en determinadas circunstancias, como se verá con posterioridad.

C. Protección de datos de carácter personal:

El artículo 18.4 de la Constitución recoge el derecho fundamental a la protección de datos de carácter personal

“4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos”.

Este derecho fundamental se desarrolla en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante, “LOPD”) y en su normativa de desarrollo (Real Decreto 1720/2007) y le reconoce a los ciudadanos la facultad de controlar sus datos personales, teniendo capacidad para disponer y decidir sobre los mismos.



Se entiende por dato de carácter personal *“toda información concerniente a personas físicas identificadas o identificables”*. En este sentido, se entenderán por datos de carácter personal en el marco de la Universidad, a título enunciativo: el nombre y los apellidos del alumno, el DNI, la dirección de correo postal y correo electrónico, fotos o imágenes grabadas, la voz, las calificaciones de las pruebas académicas, las pruebas y exámenes en que pueda identificar al autor, etc.

Por tanto, la Universidad, por la propia actividad que desarrolla, tiene que tener registrados en la Agencia Española de Protección de Datos (AEPD) una serie ficheros, de titularidad pública, como responsable de los datos personales que trata y deberá adoptar las medidas de seguridad adecuadas al nivel de seguridad exigido en función de la normativa española (Real Decreto 1720/2007).

Asimismo, la normativa de protección de datos de carácter personal exige que, cuando se recaben datos personales, el responsable informe a los afectados de forma expresa, y con carácter previo a la recogida de los datos, que éstos van a ser recabados y con qué finalidad, etc. Para recabar estos datos de carácter personal, la Universidad, tras informar expresamente al alumno, debe obtener su consentimiento inequívoco para poder tratar sus datos personales.

D. Derecho a la propia imagen:

El artículo 18.1 de la Constitución garantiza el respeto del derecho a la propia imagen de una persona. Este derecho fundamental se desarrolla en la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.

El derecho fundamental a la propia imagen faculta a la persona a evitar la difusión de su aspecto físico al ser éste el elemento básico de identificación y proyección exterior de toda persona y factor imprescindible para su reconocimiento. En consecuencia, el individuo puede decidir qué aspectos de su personalidad preserva de la difusión para protegerse de injerencias externas, resumiéndose en la frase *«usted tiene derecho a decidir quién y para qué se usa su imagen»*.

En cuanto al debate entre algunos autores en relación a si la voz se puede considerar un derecho fundamental, protegido dentro del marco del derecho a la propia imagen, Francisco de Paula Blasco Gascó⁹ ha expresado que no puede considerarse derecho fundamental como tal, sino que únicamente se podrá entender

⁹ BLASCO GASCÓ, Francisco de Paula. *“Algunas cuestiones del derecho a la propia imagen”*, pág. 38. Disponible en <http://www.derechocivil.net/esp/ALGUNAS%20CUESTIONES%20DEL%20DERECHO%20A%20LA%20PROPIA%20IMAGEN.pdf> a fecha 26 de junio de 2015.



una intromisión ilegítima su uso si atenta contra el honor, la intimidad o la propia imagen de una persona.

Al ser el individuo quien tiene la facultad de preservar la difusión de su imagen, él será el único, como titular del derecho, que puede otorgar su consentimiento expreso para su captación y difusión de la imagen a efectos de permitir que dicha captación no se pueda considerar una intromisión ilegítima, según establece el apartado dos del artículo segundo de la Ley Orgánica 1/1982

“Dos. No se apreciará la existencia de intromisión ilegítima en el ámbito protegido [...] cuando el titular del derecho hubiere otorgado al efecto su consentimiento expreso [...]”.

E. Derecho al secreto de las comunicaciones:

El artículo 18.3 de la Constitución contempla el derecho al secreto de las comunicaciones, sin enumerar una lista cerrada de los medios que están amparados, expresando que

“3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial”.

Este derecho al secreto de las comunicaciones abarca tanto a la propia comunicación –lugar, fecha, hora, identidad de los interlocutores, etc.– como al contenido de la misma¹⁰. Sin embargo este derecho tiene algunos límites, pudiendo ser interceptada la comunicación si así lo autoriza un Juez, o cuando entra en conflicto con otros derechos como podría ser el derecho del empresario a controlar la conducta del trabajador al utilizar los medios puestos a su disposición por la empresa para la realización de las funciones propias de su puesto.

Al igual que en relación con el derecho a la intimidad, para que se pueda realizar un control por parte de la Universidad del uso que realizan los alumnos de los dispositivos durante las pruebas académicas, se deberá regir en todo momento con lo dispuesto en la doctrina jurisprudencial¹¹ relativa al control empresarial, siendo defendible en base a esta jurisprudencia que el personal docente pueda acceder al dispositivos del alumno sin ser considerado un acceso ilegítimo.

Asimismo, existe jurisprudencia sobre el acceso a un terminal móvil de un alumno de un centro educativo por parte de personal docente para la investigación y

¹⁰ NARANJO DE LA CRUZ, Rafael, escritor participante en el. *“Manual de Derecho Constitucional”*, redactando el capítulo XVIII sobre "Derechos fundamentales", págs. 489-491.

¹¹ Tribunal Supremo, Sala Cuarta, de lo Social, Sentencia 6128/2007, Fundamento Jurídico Cuarto.



aplicación de la normativa disciplinaria, permitiéndose dicho acceso sin necesidad de consentimiento del afectado o de sus padres o tutores en base al interés legítimo del centro educativo por preservar otros bienes jurídicos. Esta sentencia a la que ahora nos referimos será estudiada con posterioridad en el apartado “interés legítimo”.

F. Derecho a la presunción de inocencia:

El derecho fundamental a la presunción de inocencia, reconocido en el artículo 24.2 de nuestra Constitución, es un principio jurídico que reconoce el derecho de toda persona imputada en un proceso penal a que sea tratada como si fuese inocente, debiendo ser la parte acusadora quien demuestre su culpabilidad en juicio, ostentando dicha condición de inocente el imputado hasta que recaiga una sentencia firme condenatoria.

Amplia jurisprudencia, como la Sentencia del Tribunal Constitucional 18/1981, de 8 de junio, expresa el hecho de que *“los principios inspiradores del orden penal son de aplicación, con ciertos matices, al derecho administrativo sancionador [...]”*. Para ello es necesario que las sanciones administrativas respeten las garantías procesales que establece el artículo 24 de la Constitución.

Según establece la citada STC 18/1981¹², *“[...] los principios esenciales reflejados en el artículo 24 de la Constitución [...] han de ser aplicables a la actividad sancionadora de la Administración, en la medida necesaria para preservar los valores esenciales [...]”*. En consecuencia, el derecho a la presunción de inocencia en el Derecho Administrativo implica que los administrados no requieren probar su inocencia, pues la carga de la prueba del hecho objeto de sanción le corresponde a la Administración, y el momento en que debe realizarse la comprobación del hecho sancionable es con anterioridad a la iniciación del expediente sancionador.

Este derecho a la presunción de inocencia se puede ver afectado por el principio de presunción de veracidad (presunción de certeza) de algunas autoridades públicas, propio del Derecho Administrativo, y que incluye al profesorado universitario.

Así lo establece el artículo 6 de la Ley 2/2010, de 15 de junio, de Autoridad del Profesor, que trata de la presunción de veracidad

“En el ejercicio de las competencias disciplinarias, los hechos constatados por los directores y demás miembros de los órganos de gobierno, así como por los profesores, gozan de presunción de veracidad, cuando se formalicen por escrito en documento que cuente con los requisitos establecidos reglamentariamente”.

¹² Tribunal Constitucional, Sala Primera, de lo Civil, Sentencia 18/1981 de 8 de junio, Fundamento Jurídico Segundo.



De esta forma, las posibles conductas fraudulentas de un alumno, constatadas por un profesor durante la realización de una prueba académica, pueden ser valoradas como prueba de cargo apta para fundar la sanción, pero en ningún caso se podrá invertir la carga de la prueba, por lo que no será el alumno quien deba demostrar su inocencia.

Además, la Universidad no podrá castigar aquellas conductas que no hubiera tipificado como sancionables, de manera que en virtud del principio de permisión el cliente debe regular de una forma adecuada las conductas que supondrían, en el caso del presente informe, una vulneración de las normas de uso de los dispositivos durante la realización de las pruebas académicas.

El principio de permisión se fundamenta en la expresión «lo no prohibido, está permitido». En virtud de este principio, como metanorma de nuestro ordenamiento jurídico¹³, se justifica que en aquellos vacíos normativos se permitan determinadas conductas que, de estar recogidas en alguna disposición jurídica, sería de aplicación el derecho sancionador.

La permisión contempla las disposiciones jurídicas como elementos que fijan obligaciones y prohibiciones de actuar, de forma que el Estado fija como prohibidas aquellas conductas lesivas que considera que no deben producirse en el ámbito de la comunidad. El resto de conductas, que no han sido expresamente prohibidas por el derecho positivo, estarán permitidas por el principio de permisión.

Sin embargo, este principio de permisión está limitado únicamente al ámbito penal y sancionador, este último que es el correspondiente al presente caso.

Como posible infracción de la normativa de la Universidad, que un alumno aproveche los dispositivos que se ponen a su disposición –ordenadores, *smartphones* y *tablets*– para la realización de pruebas académicas para infringir la «Instrucción informativa sobre régimen jurídico y procedimiento disciplinario de aplicación a los alumnos de la Universidad Carlos III de Madrid», la Universidad debe prever un mecanismo que permita la realización de estas pruebas a través de dichos medios tecnológicos –como una política de uso de esos recursos–.

¹³ ITURRALDE SESMA, Victoria. “Consideración crítica del principio de permisión según el cual «lo no prohibido está permitido»”. *Anuario de Filosofía del Derecho*, Madrid, núm. 15, 1998, págs. 187-218. Disponible en <http://www.google.es/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0COCIQFjAA&url=http%3A%2F%2Fdialognet.unirioja.es%2Fdescarga%2Farticulo%2F142384.pdf&ei=KGSRVaTbL-H-ywOvqrnoDw&usg=AFQjCNGtSb-nByl4Bl11iseVuZ8YJoiY-Q&sig2=hPmS-EZcUpNidZNVhfxHfA&bvm=bv.96783405,d.bGQ> a 26 de junio de 2015.



3.2- Interés legítimo:

Se entiende por interés legítimo, en Derecho Administrativo, a la exigencia de que los actos de la Administración no excedan de sus facultades, extralimitándose de sus competencias dando lugar a abusos discrecionales.

Por ello, en las acciones de la Administración debe demostrarse la concurrencia de interés legítimo y, en caso de que dicho acto chocara con derechos y libertades fundamentales de los ciudadanos, se deberá realizar una ponderación entre los intereses en conflicto¹⁴.

De esta forma, por ejemplo, en Derecho Laboral se posibilita a la empresa a establecer mecanismos de control del trabajador en el artículo 20.3 del Estatuto de los Trabajadores, como anteriormente se ha mencionado en el presente informe.

En atención a lo anterior, será defendible la utilización de mecanismos de control por parte de la Universidad para evitar que los estudiantes puedan aprovecharse del uso de dispositivos tecnológicos, como ordenadores, *smartphones* y tablets, objeto de análisis del presente informe, para realizar acciones fraudulentas con la finalidad de obtener un beneficio en el momento de elaborar las calificaciones universitarias. Este control estaría fundado en el interés legítimo de la Universidad en preservar su imagen como entidad educativa de calidad, en proteger los intereses de los demás alumnos, que ven afectadas sus valoraciones por el uso fraudulento de unos “tramposos” y en hacer cumplir las normas en materia educativa –régimen disciplinario–.

En este sentido, el Dictamen del Grupo de Trabajo del Artículo 29 sobre tratamiento de datos basados en el interés legítimo¹⁵ se basa en lo establecido en el artículo 7.f) de la Directiva¹⁶, que dice lo siguiente

¹⁴ Informe jurídico nº 0112/2012 de la Agencia Española de Protección de Datos, pág. 2 en relación con el interés legítimo. Disponible en http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/interes_legitimo/commo/pdfs/2012-0112_Inter-ee-s-leg-ii-timo.-Empresas-de-recobro..pdf a 26 de junio de 2015.

¹⁵ SEMPERE, Francisco Javier. “*Dictamen del Grupo del Artículo 29 sobre tratamiento de datos basados en el interés legítimo*”, 2014. Disponible en <http://www.privacidadlogica.es/2014/07/08/dictamen-del-grupo-del-articulo-29-sobre-tratamiento-de-datos-basados-en-el-interes-legitimo/> a fecha de 26 de junio.

¹⁶ Artículo 7.f) de la Directiva 95/46/CE del parlamento europeo y del consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.



“Los Estados miembros dispondrán que el tratamiento de datos personales sólo pueda efectuarse si: [...]

f) es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del artículo 1 de la presente Directiva”.

Es decir, se debe realizar un “balance de intereses” entre el interés legítimo del responsable del tratamiento de datos personales y los derechos y libertades fundamentales de los afectados¹⁷. En casos similares de control empresarial, el Grupo de Trabajo del Artículo 29¹⁸ establece que se entenderá adecuado el tratamiento de datos personales “si se informa a los trabajadores y a sus representantes”.

Además, existe jurisprudencia¹⁹ en relación al tratamiento de datos personales en el ámbito de la educación y, en especial, el control de dispositivos propiedad de los alumnos por personal docente de un centro educativo.

La Sala de lo Contencioso-Administrativo de la Audiencia Nacional resolvió un recurso en relación al acceso a un teléfono móvil, por parte del director de un centro educativo, porque el alumno titular del dispositivo –un menor de 12 años– había efectuado conductas inapropiadas, enseñando determinado material a menores de edad. Para proceder según el régimen disciplinario y, en caso conveniente, sancionar la conducta del menor, el director accedió a los datos de navegación del dispositivo. Asimismo, obligó al menor a dar el número PIN del teléfono y accedió a los contenidos que éste tenía registrados, todo ello sin el consentimiento del menor, el cual al ser menor de 14 años requiere que el consentimiento hubiera sido otorgado por los padres o tutores del alumno. Este recurso contencioso-administrativo fue interpuesto por el padre del menor, ante la negativa de la AEPD a pronunciarse al respeto sobre este asunto.

¹⁷ Informe jurídico nº 0247/2008 de la Agencia Española de Protección de Datos, págs. 8-9 en relación con el interés legítimo. Disponible en <http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/cesion_datos/common/pdfs/2008-0247_Acceso-por-el-empresario-al-correo-electr-oo-nico-de-los-trabajadores.pdf> a fecha 26 de junio de 2015.

¹⁸ Article 29 Data Protection Working Party, “Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC”, WP 217/2014, adoptada el 9 de abril.

¹⁹ Sentencia de la Audiencia Nacional, Sala de lo Contencioso-Administrativo, recurso nº 481/2012, Madrid a 26 de septiembre de 2013. Disponible en <<http://imagenes.publico.es/resources/archivos/2013/10/4/1380890238622sentmovil.pdf>> a 26 de junio de 2015.



En esta sentencia se analiza el interés legítimo del director del centro educativo y se analizan los diferentes articulados en materia de protección de datos que hablan del interés legítimo del responsable del tratamiento.

De esta forma, según establece dicha Sentencia, en virtud de lo dispuesto en las siguientes normas

- el artículo 7.f) de la Directiva, antes mencionado,
- el artículo 6.2 de la LOPD, que establece:
“2. No será preciso el consentimiento cuando los datos de carácter personal se recojan [...] su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado”,
- y el artículo 10.2.a) del Real Decreto 1720/2007, que establece:
*“2. No obstante, será posible el tratamiento o la cesión de los datos de carácter personal sin necesidad del consentimiento del interesado cuando:
a) Lo autorice una norma con rango de ley [...]. El tratamiento o la cesión tengan por objeto la satisfacción de un interés legítimo del responsable del tratamiento o del cesionario amparado por dichas normas, siempre que no prevalezca el interés o los derechos y libertades fundamentales de los interesados [...]. El tratamiento o la cesión de los datos sean necesarios para que el responsable del tratamiento cumpla un deber que le imponga una de dichas normas”,*

el director habría actuado en base a un interés legítimo, protegiendo unos bienes jurídicos que, en el juicio de ponderación realizado, les otorgaba una protección superior respecto del derecho a la intimidad y al secreto de las comunicaciones del afectado, por lo que no primaba el interés del afectado si no del centro educativo y del resto de los alumnos.

En consecuencia, es defendible en virtud de la jurisprudencia en materia laboral y la jurisprudencia en el ámbito educativo, mencionada en el presente apartado, la existencia de una base legal y jurisprudencial que habilitaría a la Universidad a adoptar medidas de control del uso de los dispositivos por parte de los estudiantes durante la realización de las pruebas académicas.



3.3- Seguridad informática:

La seguridad informática tiene como finalidad asegurar que los recursos de un sistema de información de una entidad se usen de forma correcta y sólo puedan acceder a la información aquellas personas que estén autorizadas para ello, con los límites que la propia organización establezca.

Para que se puedan utilizar este tipo de dispositivos tecnológicos durante la realización de las pruebas académicas, de manera que se efectúe el examen electrónicamente, será necesario que el método o herramienta utilizada preste especial atención a la seguridad informática, debiendo garantizarse²⁰:

- a. La integridad, garantizando que los datos no sean alterados una vez el alumno finalice la prueba académica, registrándose todos los accesos que se produzcan a la prueba de cada alumno y qué ha sido modificado o añadido por la persona que accedió.
- b. La confidencialidad, de forma que la información que se posea de cada alumno sea ininteligible para personas no autorizadas en virtud de sus funciones.
- c. La disponibilidad, garantizando que el profesor podrá acceder cuando sea necesario al examen de cada alumno, bien durante el proceso de corrección o en caso de reclamación.
- d. La interoperabilidad, de forma que con independencia del dispositivo que se utilice por el alumno, propio o de la Universidad, el archivo resultante de la prueba académica sea compatible con las aplicaciones utilizadas por la Universidad.
- e. La autenticación, confirmando que las partes intervinientes son quienes dicen ser, en especial garantizándose la identidad del alumno a efectos de certificar que no se ha producido una suplantación de identidad.

3.4- Uso de inhibidores de frecuencia en las aulas:

Una opción para la vigilancia y control de la adecuada utilización de ordenadores, *smartphones* y *tablets*, permitidos a los alumnos durante la realización

²⁰ Artículo publicado en Kioskea, “Introducción a la seguridad informática”, en junio de 2014. Disponible en <<http://es.ccm.net/contents/622-introduccion-a-la-seguridad-informatica>> a 26 de junio de 2015.



de pruebas académicas, podría ser la instalación de inhibidores de frecuencia. Esta no es una alternativa novedosa en España, pues ya ha sido implantada por otras Universidades españolas²¹, aunque existen serias dudas al respecto sobre su conveniencia y legalidad²².

En primer lugar, la Directiva 1999/05/CE del Parlamento Europeo y del Consejo, de 9 de marzo de 1999, sobre equipos radioeléctricos y equipos terminales de telecomunicación y reconocimiento mutuo de su conformidad no respalda el uso de inhibidores al establecer que

“Los Estados miembros sólo podrán restringir la puesta en servicio de equipos radioeléctricos por motivos relacionados con el uso efectivo y apropiado del espectro de radiofrecuencias, la prevención de interferencias que resulten perjudiciales o por motivos relacionados con la salud pública”.

En segundo lugar, el Ministerio del Interior ha cuestionado su utilización para proteger este tipo de intereses público al publicar un Informe de las Fuerzas y Cuerpos de Seguridad del Estado²³ al respecto, de forma que se plantea como una infracción el uso de inhibidores de frecuencia para otras funciones que no sean las propias de los cuerpos de seguridad, salvo la excepción prevista de que se cuente con la correspondiente autorización del órgano competente –la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información (SETSI)–.

Por último, el artículo 33.2 de la Ley General de Telecomunicaciones contempla la opción de que puedan utilizarse los inhibidores de frecuencia para proteger otros intereses públicos, como sería el caso en cuestión, cuando así lo contemple un Real Decreto –actualmente aún no se ha adoptado ningún reglamento al respecto–.

En consecuencia, en la actualidad sólo estaría permitido el uso de inhibidores cuando la Universidad hubiera obtenido la correspondiente autorización de la Secretaría de Estado de Telecomunicaciones pues, de lo contrario, estaría incumpliendo la legislación vigente y, en caso de previa denuncia, le sería de aplicación el régimen sancionador. Esta autorización sólo se concederá cuando, en virtud del

²¹ Zaragoza, I.M. “La Universidad instala inhibidores de frecuencia para evitar que los alumnos copien”. Noticia publicada en el Heraldo de Aragón, disponible en <http://www.heraldo.es/noticias/aragon/la-universidad-instala-inhibidores-para-evitar-trampas-los-examenes.html> a 26 de junio de 2015.

²² CHAVES GARCÍA, José Ramón. “Fraude en la Universidad: copiar impunemente con los smartphone”, diciembre de 2014. Disponible en <<http://contencioso.es/2014/12/26/fraude-en-la-universidad-copiar-impunemente-con-los-smartphone/>> a 26 de junio de 2015.

²³ Informe nº 2010/009 de la Unidad Central de Seguridad Privada, perteneciente al Cuerpo de Policía Nacional, de febrero de 2010, en relación a la utilización de inhibidores de frecuencia. Disponible en <http://www.policia.es/org_central/seguridad_ciudadana/unidad_central_segur_pri/i_reservada/2010/2010_009.pdf> a 26 de junio de 2015.



principio de proporcionalidad –análisis entre bienes jurídicos protegidos e intereses públicos–, el organismo considere que la finalidad de los inhibidores justifique su utilización. Asimismo, tampoco se podrán interceptar en ningún caso las comunicaciones de los estudiantes.

3.5- Uso de otras aplicaciones tecnológicas:

Además de los inhibidores de frecuencia, de los que hemos hablado en el apartado anterior, existirían otras soluciones²⁴ para que la Universidad pudiera controlar las conductas que llevan a cabo los alumnos con los dispositivos que utilizan durante las pruebas académicas.

En el caso de que se utilicen ordenadores para la realización de las pruebas académicas, algunos programas como “Impero” y “Aruba Networks” permiten monitorizar el comportamiento online del usuario del dispositivo, como por ejemplo aquello que sucede en la pantalla del ordenador.

Si se permite el uso de *smartphones* en las pruebas, el programa “Pocket Hound” es un detector de señales de radiofrecuencia que permite conocer si los *smartphones* han recibido algún mensaje.

Otra posibilidad sería instalar la aplicación “ZENworks Mobile Management” en los *smartphones* y que permite controlar el dispositivo (bloquear aplicaciones concretas, geolocalizar al alumno, acceder a los mensajes, etc.).

En cuanto a las *tablets*, la aplicación “Tab Alive” permite que los profesores gestionen el dispositivo, instalando o borrando apps y controlando qué hace el alumno con la *tablet* durante la realización de la prueba.

La cuestión es que muchas de estas aplicaciones han sido desarrolladas por compañías estadounidenses, que salvo excepciones no cumplen con la normativa de protección de datos europea y no están incluidas en “Safe Harbour”. Por ejemplo, sí están en “Safe Harbour” Aruba Network y Tab Alive (están dentro del grupo Hewlett-Packard), así como ZENworks Mobile Management. Impero, por su parte, tiene sede en Europa pero la compañía no se encuadra dentro de “Safe Harbour”.

²⁴ FONT, Susana. “¿Copias en los exámenes? Así te pueden pillar los profes”, noticia publicada en. Disponible en <<http://mobileworldcapital.com/es/459/>> a 26 de junio de 2015.



3.6- Medios de generación de prueba electrónica:

La Universidad, como garantía del correcto desarrollo de las pruebas académicas, debe siempre conservar los exámenes realizados por los alumnos durante un período adecuado, siendo como mínimo la conservación hasta el momento en que finaliza el período de revisión abierto tras la publicación de las calificaciones correspondientes.

La finalidad de esta conservación es, por un lado, la garantía del derecho de defensa del alumno y, por otro, el derecho a recurrir el examen objeto de cuestión.

Como contempla el artículo 299.2 de la Ley de Enjuiciamiento Civil, serán válidos los medios de prueba

“2. También se admitirán, conforme a lo dispuesto en esta Ley, los medios de reproducción de la palabra, el sonido y la imagen, así como los instrumentos que permiten archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase, relevantes para el proceso”.

Por tanto, la realización electrónica de las pruebas académicas y los documentos que se generen estarían amparados por esta disposición. No obstante, para que se consideren como una prueba válida en caso de impugnación de la prueba, se debe garantizar la identidad del autor y la integridad del documento (que no haya sido alterado) y actualmente contamos con algunos métodos para ello.

Entre los medios de prueba válidos, uno de los más habituales es la aportación de un acta notarial, en el que un Notario redactaría un acta de protocolización en que constaría la descripción por el Notario de lo que percibiera por sus propios sentidos en caso de encontrarse en formato electrónico la prueba académica, o si estuviera en formato físico (impreso el examen) daría fe de la identidad, del documento entregado y de la fecha en que lo recibió.

Otro medio de prueba posible sería la utilización de peritos, que mediante un dictamen pericial informático de las características de la prueba electrónica permitirían conocer el contenido o valoración de la prueba académica, pudiendo garantizarse o impugnarse la autenticidad o integridad del documento.

Nuestro ordenamiento jurídico también prevé para ello la posibilidad de realizar firmas de forma electrónica, según recoge la Ley 59/2003, de 19 de diciembre, de Firma Electrónica. De esta manera se podrá identificar al firmante y garantizar la



integridad del contenido del documento firmado de manera electrónica utilizando una firma electrónica.

Sin embargo, dentro de la firma electrónica hay varias modalidades que ofrecen diferentes grados de garantía:

- Firma electrónica. No garantiza que el documento haya sido realmente firmado por la persona que se declara firmante del mismo.
- Firma electrónica avanzada. Permite identificar al firmante, verificar la integridad del documento firmado, garantiza el no repudio del firmante e interviene una autoridad de certificación.
- Firma electrónica reconocida²⁵. Toda aquella que cumpla las siguientes características:
 - Permite identificar al firmante.
 - Permite verificar la integridad del documento firmado, garantizándose que no ha sido alterado el documento por un tercero.
 - Garantiza el no repudio del autor del documento.
 - Cuenta con un tercero de confianza (autoridad de certificación).
 - Está basada en un certificado electrónico reconocido, como el expedido por la Fábrica Nacional de Moneda y Timbre (CERES).
 - Es generada con un dispositivo seguro de creación de firma, como el DNI electrónico del que gran parte de la población dispone.

En conclusión, para la realización de las pruebas académicas mediante dispositivos tecnológicos, efectuándose los exámenes de forma electrónica, lo más conveniente será adoptar un medio de prueba que garantice la autenticación del alumno que lo ha realizado y la integridad del contenido y que tenga una fiabilidad tal que permita probar, sin ningún género de duda, que ha sido un determinado alumno quien realizó dicho examen. En base a esto, el presente informe valorará posteriormente cuáles son los métodos de prueba convenientes.

3.7- Requisitos y opciones de la herramienta a utilizar:

Una vez analizados los aspectos jurídicos y otros elementos técnicos que deben atenderse con el objeto de permitir, de forma segura, la realización de pruebas

²⁵ Portal de la Administración Electrónica, “Base legal de la firma electrónica”, disponible en <<http://firmaelectronica.gob.es/Home/Ciudadanos/Base-Legal.html>> a 26 de junio de 2015.



académicas mediante el uso de dispositivos electrónicos, a lo anterior será necesario añadir una herramienta informática que haga factible la realización, por medios electrónicos, de los exámenes universitarios.

Esta herramienta deberá garantizar al menos la autenticación del alumno que realiza la prueba académica; la integridad del contenido de la prueba; y la disponibilidad de que el profesor pueda acceder al examen para su corrección y, en caso de reclamación, que el alumno pueda acceder al mismo.

En relación con la autenticación, la herramienta deberá exigir que el usuario acceda con un nombre de usuario y contraseña, que será una clave única, los cuales serán comunicados al alumno por la Universidad, quien será el creador de los mismos. La contraseña será privada y será responsabilidad del alumno su guarda de terceros. Además, la herramienta contará con un protocolo mediante el cual se autenticuen las contraseñas contra un servidor de la Universidad, como podría ser el uso del protocolo LDAP (*Lightweight Directory Access Protocol*).

También será necesario que la herramienta permita que, mientras se encuentra el alumno en activo en la misma, habiendo accedido con su usuario y contraseña, éste pueda ser grabado en audio y vídeo para que el profesor pueda corroborar su identidad previamente a comenzar el examen y controlar la conducta del estudiante durante la realización de la prueba académica, guardándose dicha grabación durante el mismo período en que deba conservarse el propio examen. Dentro de esta funcionalidad, existen sistemas de reconocimiento de voz a texto (transcripción), en los que la captura de vídeo del contenido oral podría pasarse a texto como se puede comprobar en el citado Proyecto²⁶, de manera que se podría transcribir un examen realizado a distancia y de forma oral por el alumno, sirviendo la grabación como prueba y utilizándose este programa de transcripción de la voz para tener una copia escrita del mismo.

Otro de los aspectos que deberá incluir la herramienta es contar con un control de los accesos, de manera que únicamente estén autorizados a acceder a las pruebas de los alumnos los respectivos profesores de dicho examen –se fijarán autorizaciones de acceso exclusivas para el personal docente correspondiente y, previa autorización, al personal informático cuando se hubiera registrado algún incidente–, los cuales únicamente podrán proceder a la corrección de la prueba, quedando constancia de todos los comentarios y calificaciones que fijen en cada uno de los ejercicios que forman parte del examen. Toda esa información se recogería en ficheros de log o “log files” para poder consultarla cuando fuera necesario. En consecuencia, deberá quedar

²⁶ PERERO CODOSERO, Juan Manuel. “Desarrollo de un sistema de reconocimiento de habla natural para transcribir contenidos de audio en Internet”. Proyecto fin de carrera, marzo de 2015. Disponible en <<http://arantxa.ii.uam.es/~jms/pfcsteleco/lecturas/20150420JuanManuelPereroCodoserero.pdf>> a fecha 26 de junio de 2015.



constancia del usuario que accedió a la prueba, en qué fecha y hora accedió, a qué exámenes, qué comentarios incluyó, etc.

Toda la información relativa al acceso al archivo de cada prueba académica deberá conservarse, como mínimo, mientras esté abierto el período de revisión de la prueba por si el alumno solicitase una revisión de su calificación.

Asimismo, esta herramienta deberá ser compatible con los sistemas operativos más extendidos, de manera que no se discrimine a la mayoría de los estudiantes.

Respecto a la privacidad y el derecho a la protección de datos de carácter personal, la herramienta que se utilice debería cumplir con el principio de “*privacy by design*”²⁷ o privacidad desde el diseño²⁸. Este principio es una obligación legal que prevé en el futuro Reglamento Europeo de Protección de Datos, que se encuentra actualmente en proceso de tramitación. Este concepto debe entenderse como una estructura de cumplimiento normativo cuyo objetivo es que las organizaciones implementen medidas preventivas desde el diseño de la herramienta de gestión con el fin de aportar las garantías necesarias para proteger la privacidad y el derecho a la protección de datos de carácter personal de los ciudadanos.

Para ello, esta herramienta debe permitir la realización de las pruebas académicas utilizando dispositivos electrónicos, con independencia de su titularidad, sin intervenir en las comunicaciones del propio dispositivo, de manera que se pueda entender como una interceptación ilegítima de las mismas, ni acceder a datos personales que no sean los propios de los que requiera y que se soliciten al alumno para el propio desarrollo de la prueba. Asimismo, esta herramienta no debería exigir ningún tipo de instalación, siendo accesible a través de Internet. De esta forma, se garantizará todo respeto a los derechos fundamentales del alumno al aplicarse medidas técnicas proporcionales y no excesivas con el objetivo de permitir la realización de la prueba y el control, por parte del profesor, de que el alumno no lleva a cabo ninguna conducta fraudulenta con ánimo de copiar o ayudarse de fuentes no autorizadas.

Entre las posibilidades que este despacho ha analizado para el presente informe, sin entrar a valorar las mismas, destacan:

²⁷ VEGA SUÁREZ, Ana M. “*Análisis del Privacy by Design y su mención en el Reglamento General de Protección de Datos de la UE*”, 2013. Disponible en <<http://www.aspectosprofesionales.info/2013/06/analisis-del-privacy-by-design-y-su.html>> a 26 de junio de 2015.

²⁸ ComputerWorld, 2014. “*El Principio de Privacy by Design, en el Reglamento Europeo de Protección de Datos*”. Disponible en <<http://www.computerworld.es/sociedad-de-la-informacion/el-principio-de-privacy-by-design-en-el-reglamento-europeo-de-proteccion-de-datos>> a 26 de junio de 2015.



- VPN:

Una VPN²⁹ (*Virtual Private Network*) es una tecnología que permite conectar uno o varios ordenadores a una red privada usando internet. Esto permite que los usuarios de dicha VPN puedan acceder a los recursos de una organización, permitiendo asegurar la integridad de la información y la confidencialidad al cifrar las comunicaciones.

Otra de las características de una VPN es que permite limitar el acceso mediante privilegios a los usuarios en función del rango, de manera que se podría establecer que los alumnos al utilizar la VPN sólo puedan acceder a la plataforma donde se desarrolla el examen, sin poder tener abiertas otras aplicaciones o páginas de internet.

Además, para garantizar la autenticación de los usuarios a través de una VPN, es posible la utilización de contraseñas de uso único, de manera que sólo el alumno y el profesor autorizado pueda acceder a la prueba académica para su realización y su posterior corrección.

- Intranet:

Una Intranet es una red de uso exclusivo de una organización, de forma que los ordenadores de dicha organización son los únicos que pueden acceder a ese sitio web. Esto permite compartir documentos electrónicamente y que únicamente puedan acceder a la misma los usuarios de la Universidad, estableciendo mecanismos de autenticación.

- Moodle:

Moodle, plataforma utilizada en la actualidad por el cliente, ofrece seguridad en diferentes materias como sería en el servidor, en la autenticación de los usuarios y en las contraseñas. Además, asigna rangos a los diferentes usuarios, permitiendo diferentes formas y grados de interacción con la plataforma, para garantizar una mayor seguridad.

Con respecto a la realización de copias de respaldo, Moodle permite su creación programada, por lo que podría fijarse su realización tras la realización de cada prueba académica, de forma que quedaría asegurada la integridad y disponibilidad de

²⁹ GOUJON, André. “¿Qué es y cómo funciona una VPN para la privacidad de la información?”. Disponible en <<http://www.welivesecurity.com/la-es/2012/09/10/vpn-funcionamiento-privacidad-informacion/>> a 26 de junio de 2015.



los exámenes en caso de que fuese requerida una posterior revisión o como elemento probatorio cuando fuese necesario.

Otra de las ventajas que ofrece el uso de Moodle es que permite conocer al profesor cuando se producen novedades en la plataforma, de forma que por ejemplo cuando cada alumno finaliza la prueba académica, el profesor lo conoce al instante.

Por último, la plataforma Moodle está adaptada a la normativa española de protección de datos de carácter personal, marco que han establecido el Instituto Nacional de Ciberseguridad (INCIBE) y la Agencia Española de Protección de Datos (AEPD).

- Otras plataformas de e-learning:

Existen también otras plataformas que permiten realizar ejercicios utilizando medios electrónicos como podría ser Duolingo. Esta plataforma permite aprender diferentes idiomas mediante pruebas y retos, estableciendo diferentes funcionalidades. Por ejemplo, permite realizar ejercicios de pronunciación basados en el reconocimiento de voz.

Asimismo, para evitar conductas fraudulentas de los usuarios, con la finalidad de ofrecer un servicio certificado de idiomas, utilizan el audio y la imagen que ofrece la cámara frontal del dispositivo del usuario para captar su imagen y comprobar que, durante la realización de las pruebas de certificación, el usuario no utiliza intenta engañar a la aplicación.



4- Universidades que permiten el uso de dispositivos electrónicos para la realización de pruebas académicas:

4.1- Universidades españolas:

- La *Universidad Camilo José Cela* prevé, en su «Normativa para la realización de exámenes por medios electrónicos³⁰», la posibilidad de que sus estudiantes puedan realizar pruebas académicas utilizando dispositivos electrónicos. Se deben cumplir una serie de requisitos por parte del alumno y seguir unas exigencias para que se permita esta modalidad de evaluación.
 - El alumno debe estar cursando estudios fuera del territorio de la Universidad o acreditar que cuenta con una causa justificada, solicitando previamente la realización de la prueba por estos medios.
 - El alumno debe acceder a la plataforma de la Universidad utilizando su nombre de usuario y contraseña, que será comprobada a través de un sistema de autenticación.
 - El profesor podrá comprobar la identidad del alumno, debiendo éste mostrar su DNI mediante una videoconferencia. Asimismo, se podrá vigilar que el alumno no actúa fraudulentamente mediante un control usando una webcam.
 - El examen deberá grabarse por medios electrónicos para dejar prueba de su realización.
 - Será responsabilidad del alumno comprobar que la configuración de su dispositivo es correcta, pudiendo realizar una comprobación de su compatibilidad a través de una plataforma habilitada para ello por la Universidad.
 - Para todo lo anterior, se exigirá que el alumno disponga de conexión a Internet y herramientas de transmisión simultánea de audio (micrófono) y vídeo (webcam).

³⁰ Universidad Camilo José Cela, “Normativa para la realización de exámenes por medios electrónicos”, 2014. Documento disponible en <https://ucjc.blackboard.com/bbcswebdav/institution/UCJC/Oficializaci%C3%B3n%20Ense%C3%B1anza/NORMATIVAS/NORMATIVA%20PARA%20LA%20REALIZACI%C3%93N%20DE%20EX%20C3%81MENES%20POR%20MEDIOS%20ELECTR%C3%93NICOS.pdf> a 26 de junio de 2015.



4.2- Universidades europeas:

- *University of Bristol / Universidad de Bristol (Reino Unido)*³¹. Se permite realizar la prueba académica utilizando un ordenador, estableciéndose en una guía de pruebas prácticas las siguientes reglas:
 - El alumno debe certificar que padece una discapacidad.
 - El alumno no puede acceder a los archivos guardados en el dispositivo.
 - No se permite que los ordenadores utilizados para la realización del examen puedan conectarse a internet.
 - El examen debe imprimirse una vez finalizada la prueba y entregarse al profesor que vigile su realización.

- *University of Southern Denmark / Universidad del Sur de Dinamarca (Dinamarca)*³². Han desarrollado un código de buenas prácticas, que establece:
 - Se permite su utilización para todos los alumnos.
 - Se utiliza la plataforma virtual de la Universidad.
 - Los alumnos pueden utilizar los ordenadores propios o de la Universidad.
 - La inscripción del alumno para realizar una prueba académica utilizando un ordenador implica la aceptación de las condiciones del código de buenas prácticas.
 - El alumno es responsable del funcionamiento de su propio ordenador, debiendo comprobar que su configuración es compatible con la plataforma de la Universidad.
 - El examen se entrega en formato digital pero se le dará al alumno un recibo que prueba la presentación y realización de la prueba.
 - El alumno es responsable de guardar de forma regular el examen.
 - La Universidad podrá comprobar que el alumno no ha utilizado ayudas no permitidas.
 - Se aplicará la normativa disciplinaria si el alumno no respeta este código de buenas prácticas.

Otras Universidades que también prevén la posibilidad de que sus alumnos puedan realizar las pruebas académicas mediante el uso de ordenadores son:

³¹ University of Bristol, “*Use of computers in examinations - a guide to good practice*”. Disponible en <<http://www.bristol.ac.uk/exams/alternative/>> a 26 de junio de 2015.

³² University of Southern Denmark, “*The University of Southern Denmark’s code of practice for using computers at written campus-based examination*”, 2012. Disponible en <http://www.sdu.dk/en/information_til/studerende_ved_sdu/eksamen/generelt_om_eksamen/under_eksamen/skriftlig_proeve_digital> a 26 de junio de 2015.



- La *University of Birmingham / Universidad de Birmingham*³³ (Reino Unido) también prevé la posibilidad de que aquellos alumnos que tengan algún tipo de discapacidad puedan realizar las pruebas académicas utilizando un ordenador si así lo solicitan.
- La *University of Copenhagen / Universidad de Copenhague*³⁴ también prevé la posibilidad de que los alumnos puedan realizar pruebas académicas utilizando ordenadores.

4.3- Universidades no europeas:

- *Swinburne University of Technology / Universidad Tecnológica de Swinburne (Australia)*³⁵. Se permite realizar el examen utilizando un ordenador a los alumnos con el siguiente procedimiento:
 - El alumno asume el riesgo de usar el ordenador durante el examen por la posibilidad de caída del suministro eléctrico, mal funcionamiento del dispositivo o un incorrecto guardado del examen.
 - El alumno debe certificar que padece una discapacidad.
 - El ordenador es titularidad de la Universidad.
 - El alumno utiliza un disco duro donde guarda el examen. Este disco duro es puesto a disposición del alumno por la Universidad.
 - No se permite que los ordenadores utilizados para la realización del examen puedan conectarse a internet.
 - Los alumnos guardaran periódicamente su examen en el disco duro y en la carpeta C del ordenador para no perder el archivo.
 - Una vez finalizado, se permitirá al alumno imprimir el examen.
 - En casos excepcionales se permitirá que el alumno realice la prueba académica con su propio dispositivo, sin que éste tenga acceso a Internet.
- *University of Washington / Universidad de Washington (Estados Unidos)*³⁶. Permiten el uso de ordenadores en pruebas académicas en las siguientes condiciones:

³³ University of Birmingham, "Computer use in an exam". Disponible en <<https://intranet.birmingham.ac.uk/as/cladls/exams/alternative/computer.aspx>> a 26 de junio de 2015.

³⁴ University of Copenhagen, "PC examen". Disponible en <<http://pc-exam.ku.dk/>> a 26 de junio de 2015.

³⁵ Swinburne University of Technology "Use of Computers in Examination", disponible en <<http://www.swinburne.edu.au/stuserv/disability/computers.html>> a 26 de junio de 2015.

³⁶ University of Washington. "Use of Computers on Exams", 2003. Disponible en <<https://www.law.washington.edu/Students/Academics/Exams.aspx>> a 26 de junio de 2015.



- Se debe respetar la política de uso establecida por cada profesor
 - Los alumnos pueden utilizar los ordenadores propios o de la Universidad.
 - Para realizar la prueba se puede utilizar la plataforma de la Universidad, un CD o un USB, que serán propiedad del alumno. Una vez finalizado, se guardará el examen y se enviará en la forma establecida o se entregará el CD o USB utilizado al profesor.
 - La falta de entrega del examen implicará que la calificación del alumno será un suspenso.
 - El alumno asume el riesgo de usar el ordenador durante el examen por la posibilidad de caída del suministro eléctrico, mal funcionamiento del dispositivo o un incorrecto guardado del examen.
 - Los alumnos pueden utilizar la opción “copiar” o “cortar” aquello que hubieran escrito, no estando permitido usar esas opciones cuando se trate de materiales ajenos a la prueba.
 - No se permite que los alumnos puedan acceder a internet durante la prueba.
- *University of Louisville / Universidad de Louisville (Estados Unidos)*³⁷. Fija una política para el uso de ordenadores en exámenes, estableciendo:
- El uso de ordenadores para la realización de pruebas académicas no es un derecho del alumno, si no un privilegio que le concede la Universidad a aquellos estudiantes que cumplan la política establecida.
 - Los exámenes se realizarán a través de la plataforma de la Universidad y se enviarán electrónicamente, aunque el alumno deberá asistir con una unidad USB como herramienta secundaria en caso de fallo en el envío electrónico, pudiendo guardar así su examen. La Universidad no facilitará al alumno un medio externo de guardado de la prueba.
 - El alumno es responsable de que, si utiliza un ordenador propio, este se encuentre actualizado y sea compatible con la plataforma utilizada para la realización de la prueba.

³⁷ University of Louisville. “*Policy and Procedures: Examinations on Computer*”, 2012-2013. Disponible en <<https://www.law.louisville.edu/it/computer-exam-policy>> a 26 de junio de 2015.



5- **Conclusión:**

El cliente, en la reunión mantenida con nuestro despacho, nos solicitó que en el presente informe se incorporase una valoración de la recomendación más adecuada para la puesta en funcionamiento de un sistema que garantice la correcta y segura realización de las pruebas universitarias mediante la utilización de dispositivos electrónicos.

Esta conclusión, en ningún caso, implica la obligación de que el cliente la adopte en su organigrama y sea desarrollada. La recomendación está fundada en los criterios de conveniencia que este despacho, una vez analizados todos los aspectos anteriores en el apartado tercero del presente informe, cree más adecuados en función de la actividad que desarrolla la Universidad Carlos III de Madrid, las decisiones que adoptaron otras organizaciones universitarias observadas así como diferentes aplicaciones cuyas características y funcionamientos beneficiarían al cliente.

A continuación, procederemos a desglosar la solución planteada en el presente informe, motivando el por qué de dicha recomendación.

En base a los anteriores aspectos que se deben tener en cuenta, consideramos que la mejor solución para permitir la realización de las pruebas académicas utilizando dispositivos electrónicos es el desarrollo por parte del cliente de una plataforma de *e-learning*.

Como se mencionó, actualmente la Universidad Carlos III de Madrid utiliza la plataforma Moodle, que licencia a sus usuarios mediante una Licencia Pública General GNU (GNU General Public License o GPL³⁸). La licencia GPL permite la modificación de esta plataforma, pues su código fuente es público, pero implica que toda transformación del mismo deberá ser puesta a disposición de otros usuarios en las mismas condiciones, salvo que se vaya a hacer un uso privado de la plataforma³⁹.

Por tanto, no recomendamos que el cliente modifique la plataforma Moodle que utiliza en la actualidad, pues si desea rentabilizar dicha modificación y diferenciarse de otras Universidades de su entorno, debería desarrollar su propia plataforma, basándose en el principio "*privacy by design*" para garantizar un marco jurídico adecuado a la normativa española y comunitaria.

³⁸ Licencia de Moodle, disponible en <<https://docs.moodle.org/all/es/Licencia>> a 27 de junio de 2015.

³⁹ Organización GNU, "*Preguntas frecuentes acerca de las licencias de GNU*", 2015. Disponible en <<http://www.gnu.org/licenses/gpl-faq.html#WhyDoesTheGPLPermitUsersToPublishTheirModifiedVersions>> a 27 de junio de 2015.



Tampoco creemos que se deba utilizar una VPN, pues en ocasiones requiere la instalación en los diferentes dispositivos, lo que limitaría su uso pues se requeriría que todos los alumnos lo instalaran en sus dispositivos, y sus requerimientos de espacio limitarían a algunos alumnos con dispositivos más anticuados o, por ejemplo, que pueda soportarlo un *smartphone*. Asimismo, otros tipos de VPN no requieren de dicha instalación pero son menos seguras, y tratando datos personales mediante la herramienta de gestión no creemos recomendable dicha opción.

Respecto de la utilización de una intranet de la Universidad, este despacho considera que esta herramienta tiene más utilidad como base de datos que permita buscar información que para la función que se pretende conseguir en este informe.

5.1- Plataforma de *e-learning*:

La alternativa por la que se opta en el presente informe, el desarrollo de una plataforma de *e-learning* propia de la Universidad, basándose en el principio de “*privacy by design*” para cumplir las exigencias legales y garantizar el respeto de la privacidad y del derecho a la protección de datos de carácter personal de los estudiantes. Para ello, esta plataforma debería cumplir los siguientes requisitos:

- Respetar los derechos fundamentales de los alumnos, de manera que en ningún caso se pueda vulnerar el derecho a la intimidad y al secreto de las comunicaciones de los estudiantes, no interceptándose las comunicaciones de los alumnos en ningún caso, siendo una intervención mínima en los dispositivos con el único fin de controlar la realización de la prueba. Para ello la plataforma únicamente captará los datos que sean estrictamente necesarios para la realización de la prueba académica e impedirá el acceso de los usuarios a otras aplicaciones o sitios web distintos de la propia plataforma.

Para bloquear el acceso de los alumnos durante la prueba académica a otras aplicaciones diferentes de la plataforma donde se va a efectuar el examen, se podría desarrollar una “*cookie propia*” de la Universidad, que sería una *cookie* de sesión que analizaría el uso que realiza el usuario del dispositivo e impediría que se pueda hacer un uso distinto del propio de la plataforma, de manera que no sería posible acceder a otra aplicación o a un sitio web durante la prueba o que, en caso de hacerlo, esta actividad quedará registrada y podrá dar lugar a las sanciones disciplinarias correspondientes.

Para ello, se informaría al alumno con carácter previo al comienzo de la realización del examen, cuando fuese a acceder a la plataforma, de que es



condición necesaria para la realización de la prueba utilizando dispositivos electrónicos la aceptación de dicha cookie de forma expresa (clicando en aceptar), informándole de las finalidades de la misma y del control que permitirá de la actividad del estudiante. Hemos redactado en el [Anexo nº 1](#) un ejemplo de cómo sería este aviso de cookies, que no necesitaría de una segunda capa informativa pues, como hemos dicho anteriormente, sería una cookie propia y de sesión, únicamente para el correcto funcionamiento de la plataforma y del desarrollo de la prueba.

- La plataforma en ningún caso permitirá que terceros no autorizados puedan acceder a los datos de carácter personal de los usuarios, estableciéndose las medidas de seguridad informática necesarias para ello. Esta plataforma respetará todo lo estipulado por la LOPD y su normativa de desarrollo, de forma que se garantice el adecuado tratamiento y que únicamente pueda acceder a los datos personales los usuarios que, en el ejercicio de sus funciones, estén autorizados para ello.

Respecto a la captación de datos personales durante la realización de las pruebas académicas mediante el uso de dispositivos, se informará al usuario de que es condición necesaria la captación de su imagen y voz durante la prueba para verificar su identidad. Hemos elaborado en el [Anexo nº 2](#) una cláusula de información, de manera que el usuario deberá consentir dicho tratamiento para poder efectuar el examen, informándose y obteniéndose el consentimiento con una previsión suficiente.

En cualquier caso, se trata de datos de carácter personal de nivel bajo, de manera que no se exigen unas medidas de seguridad excesivas y, como se ha comprobado, la Universidad ya cuenta con ficheros de titularidad pública registrados ante la AEPD.

Además, será posible que estas grabaciones de los alumnos, en el caso de que se trate de exámenes de tipo oral, se puedan transcribir mediante el uso de algún programa⁴⁰ que genere un texto de dicho examen oral, de manera que se genere otra prueba adicional de la realización del examen y del contenido de la prueba realizada por el alumno.

- Establecer mecanismos de seguridad informática que permitan garantizar la integridad del documento generado por el alumno durante la prueba académica, la confidencialidad y disponibilidad de la información, la interoperabilidad de la plataforma y la autenticación de los usuarios que accedan a la plataforma.

⁴⁰ PERERO C., Juan M. *“Desarrollo de un sistema de reconocimiento de habla natural para transcribir contenidos de audio en Internet”*, 2015.



Será especialmente importante que todos los archivos que se generen del examen, no sólo el contenido del propio examen, sino también las grabaciones de los datos personales del alumno y toda actividad que se hubiera desarrollado durante la prueba académica, quede registrada en la plataforma, generándose evidencias de que el alumno realizó la prueba y garantizando que se conserva durante el tiempo necesario el examen y las grabaciones y registros de actividad.

Para garantizar la integridad del documento electrónico generado, una vez el usuario finalice la prueba o hubiera concluido el tiempo establecido para la misma, se guardará un archivo del examen en el servidor de la Universidad. Además, se dará la posibilidad al alumno y al profesor que así lo considere de imprimir una copia del examen tras su finalización.

Para asegurar la disponibilidad del archivo correspondiente al examen, la plataforma realizará nada más finalizar la prueba una copia de respaldo que se almacenará en un lugar distinto de donde estuviera ubicado el servidor de la Universidad.

Para proteger la confidencialidad de los usuarios, la Universidad otorgará a cada uno de ellos un número de identificación del alumno (NIU), de manera que el profesor desconocerá el nombre de los alumnos. La conexión entre el nombre y apellidos del alumno y su correspondiente NIU se realizará a través de la plataforma y sólo será accesible por el estudiante, salvo en caso de que se produzca alguna reclamación en que deberán conocerse estos datos para su correcta investigación.

Respecto de la interoperabilidad de la plataforma, se debe garantizar que la misma funciona con los diferentes sistemas operativos existentes que tengan una mayor implantación en España, siendo el Consejo de Gobierno de la Universidad quien debería establecer cuales se consideran de mayoritarios. En todo caso, se intentará que la plataforma se encuentre comprimida para optimizar el uso de los dispositivos, en especial aquellos de menor capacidad como serían los *smartphones* y las *tablets*, garantizándose que los alumnos puedan realizar las pruebas sin contratiempos. Sin embargo, será responsabilidad de los estudiantes escoger el dispositivo que desean utilizar para efectuar la prueba.

Por último, la plataforma deberá garantizar una correcta autenticación del alumno. Entre los diferentes medios de prueba analizados anteriormente, aconsejamos al cliente descartar que sea un Notario quien de fe de la realización de las pruebas académicas y del contenido de las mismas, pues



conlleva un elevado coste a largo plazo. Respecto a la intervención de los peritos, esto será necesario en todo caso cuando se produzcan conflictos en relación con la prueba, no siendo requerido pues el presente informe plantea una solución eficaz que genere seguridad jurídica al cliente, generándose prueba suficientemente válida para garantizar la realización del examen, la integridad de su contenido y la identidad del autor.

Por ello, creemos que el mejor medio de prueba es exigir que el alumno introduzca su DNI electrónico en un lector externo puesto a su disposición o, en caso de disponer de DNI 3.0⁴¹, identificarse sin necesidad de lector externo. No se permitirá realizar la prueba por estas modalidades si el alumno no dispone de un DNI electrónico (firma electrónica reconocida). Mediante la firma de la prueba utilizando el DNI electrónico del alumno, no quedará ninguna duda, gracias al certificado de la Fábrica Española de Moneda y Timbre, de que el documento ha sido realizado por el alumno en cuestión.

Asimismo, para el aseguramiento de la identidad del usuario, se realizará una comprobación por parte del profesor a través del uso de una videocámara (webcam) o cámara interna que incorpore el dispositivo y se procederá a la grabación de la prueba (audio e imagen) para asegurar que es en todo momento el alumno correspondiente quien desarrolla la prueba y no un tercero que suplanta su identidad. Para dicha captación de la imagen y la voz, que están considerados datos de carácter personal, se informará previamente al estudiante de que es una condición necesaria y que está en su derecho de no prestar su consentimiento, no pudiendo realizar la prueba académica mediante el uso de dispositivos electrónicos.

También se establecerá un registro de acceso al documento, de manera que cualquier modificación del mismo, comentario introducido por el profesor, calificaciones de las diferentes preguntas o ejercicios, etc. queden reflejados en el archivo electrónico. Asimismo, se impedirá que personal no autorizado acceda al documento del examen y quedará constancia de todo acceso una vez finalizado el examen, como se comentó anteriormente respecto al registro de acceso de la plataforma. Para ello sería posible la configuración de un control de accesos mediante ficheros log.

- Que la plataforma permita la elaboración por parte de los docentes de diferentes tipos de exámenes (escrito, tipo test, oral...) y de su desarrollo bien de forma presencial (en aulas de la propia Universidad) o a distancia

⁴¹ TEKNAUTAS, 2015. *“La segunda resurrección del DNI electrónico: para qué podrás usarlo”*. Disponible en http://www.elconfidencial.com/tecnologia/2015-01-12/la-segunda-resurreccion-del-dni-electronico-para-que-podras-usarlo_620665/ a 27 de junio de 2015.



“en línea” (desde cualquier lugar, siempre que se tenga conexión a Internet para acceder a la plataforma). Asimismo, se permitirá que el examen que la prueba sea realizada utilizando dispositivos titularidad de la Universidad o del propio alumno, siendo la plataforma compatible con los sistemas operativos de uso mayoritario en España.

5.2- Desarrollo de las pruebas académicas:

▪ Evaluación presencial:

Si los profesores optasen porque las pruebas académicas se realizasen dentro del recinto de la Universidad mediante una modalidad presencial, efectuándose en un aula habilitada para dicha convocatoria, el procedimiento que le recomendamos al cliente sería el siguiente:

- i. Los alumnos accederían a través de su dispositivo, con independencia de quien fuese el propietario del mismo, a la plataforma que utilizase la Universidad, en dónde deberían autenticarse con el nombre de usuario y la contraseña que les correspondiera.
- ii. El profesor comprobaría los datos de cada alumno, utilizando para ello la webcam o cámara interna del dispositivo. De esta manera, se evitaría que un tercero se registrase con los datos de un alumno, suplantando su identidad. En caso de abandono de la sesión por parte de un alumno, por cualquier hecho como podría ser permitir que un tercero acceda con los datos del alumno para realizar la prueba, el sistema de la plataforma avisaría al profesor, quedando registrado como prueba posterior. Asimismo, se establecerá un aviso previo al abandono de la sesión que garantice que el alumno no finaliza su acceso por error.
- iii. El profesor habilitaría la prueba académica en la plataforma, al contar con el rango de “docente”, para que los alumnos puedan comenzar la prueba.
- iv. Los alumnos deberán introducir su DNI electrónico en el lector externo puesto a su disposición por la Universidad, que será el instrumento utilizado para la firma de la prueba de manera electrónica.
- v. Durante la realización del examen, se permitirá que el alumno pueda guardar de forma periódica su examen para, en caso de que se perdiera la sesión o se produjera algún problema técnico, fuese posible recuperar el contenido de la prueba para su continuación.



- vi. Una vez finalizado el período de tiempo establecido por el profesor para la realización del correspondiente examen, el espacio habilitado para la prueba se cerrará y se guardarán los exámenes en el servidor de la Universidad tal y como se encontraran en ese momento. El envío de la prueba por cada estudiante quedará anotado en el registro de actividad, teniendo constancia del momento de envío de cada uno de los exámenes y el número identificador de cada uno de los alumnos.
- vii. Los alumnos y el profesor podrán proceder a la impresión de una copia de la prueba académica con el fin de proporcionar seguridad adicional y que el alumno tenga la oportunidad de conocer, finalizada la prueba, una calificación aproximada de su rendimiento.
- viii. La cookie de sesión que utilizaría la plataforma durante el desarrollo de la prueba académica permitirá registrar la conducta de los usuarios, de manera que en caso de necesidad podrá ser revisada para verificar que no se ha producido un uso fraudulento del dispositivo. Esta información será almacenada junto a la grabación de la imagen y voz del usuario.

En el caso de que la prueba se desarrollase en formato oral, siendo grabada por medios electrónicos, se informará al alumno de que se va a proceder a grabar su imagen y su voz y que dicho examen será posteriormente transcrito (a través de programas como los antes mencionados) con el fin de que el profesor pueda realizar una calificación más adecuada de la prueba, pudiendo el alumno solicitar una copia de dicha transcripción cuando fuera posible. Esta grabación, como se mencionó anteriormente, será almacenada en el servidor de la Universidad.

Asimismo, como mencionamos con anterioridad, la Universidad podrá garantizar que únicamente se pueden utilizar los dispositivos habilitados para la realización de la prueba académica, mediante el empleo de dispositivos como los inhibidores de frecuencia, siempre que cuenten con la respectiva autorización del organismo competente –la SETSI–, con el fin de evitar un uso indebido de dispositivos como los *smartphones* en aquellas pruebas en que no se haya prevista dicha utilización. También podrá instalar las diferentes aplicaciones que mencionados para controlar los dispositivos, pero consideramos que tanto el uso de inhibidores de frecuencia como de estas aplicaciones es innecesario si se desarrolla, siguiendo el principio “*privacy by design*”, una plataforma acorde a las características que hemos mencionado en el apartado 5.1 del presente informe.



- Evaluación a distancia “en línea”:

A través de la plataforma de *e-learning* se plantearían dos metodologías de examen a distancia “en línea” que serían acordes a la normativa española analizada, que serían bien la realización de la prueba de forma escrita o bien consistente en una prueba oral en la que el alumno debería contestar a las preguntas planteadas sin necesidad de transcribir las respuestas.

Al igual que en la realización de la prueba académica de forma presencial, en el formato a distancia se utilizaría esta plataforma y el usuario deberá autenticarse y utilizar un dispositivo, sea propio o de la Universidad, que permita la grabación de su imagen y de su voz, que serán tratados en los mismos términos que el caso anterior. Asimismo, los usuarios deberán contar con un lector externo que permita introducir el DNI electrónico para identificarse o, en caso de que utilicen un *smartphone* o una *tablet*, como se mencionó, la tecnología NFC permite que con el simple acercamiento del DNI electrónico 3.0 se pueda identificar al usuario.

Además, si la Universidad considera adecuado, y para garantizar el mismo trato que se le otorga a los alumnos que realizan el examen de forma presencial, será posible el envío de la prueba al correo electrónico del alumno en formato PDF, de forma que pueda realizar una copia del mismo. En el caso de que el examen fuera oral, se podrá enviar al alumno una copia de la transcripción del mismo.

5.3- Dispositivos a utilizar y su titularidad:

Como ya se mencionó a lo largo del presente informe, la plataforma de *e-learning* estará adaptada no sólo a ordenadores, si no que será posible, dentro de las limitaciones tecnológicas actuales, su uso mediante *smartphones* y *tablets*, aunque se recomendará a los estudiantes que antes de la realización de una prueba mediante estos dispositivos electrónicos, el alumno proceda a realizar una prueba de su correcto funcionamiento, no siendo responsabilidad de la Universidad que el alumno utilizase un dispositivo inadecuado o desactualizado.

En cualquier caso, la Universidad pondrá a disposición de los estudiantes, dentro de sus limitaciones, dispositivos adecuados para la realización de las pruebas académicas, reservándose el derecho a impedir que dichos dispositivos puedan ser trasladados fuera de sus instalaciones.

Asimismo, el alumno que utilice dispositivos titularidad de la Universidad debe ser consciente de este hecho, siendo informado a través de las Políticas de Uso que



incluimos en el Anexo nº 3 del presente informe, reglas que deberá respetar en todo momento mientras esté en posesión del dispositivo electrónico. En estas Política de Uso también se contemplará la utilización de dispositivos de titularidad del propio alumno.

Las Políticas de Uso de los dispositivos serán de aplicación a todos los estudiantes y en ella se recogerán todas las conductas que no están permitidas, siendo sancionables en virtud de lo dispuesto en la normativa disciplinaria de la Universidad.

Respecto a estos dispositivos, recomendamos que la Universidad exclusivamente permita la utilización de dispositivos que sean de su titularidad, pues se garantiza una mayor seguridad jurídica, de manera que en aplicación por analogía del artículo 20.3 del Estatuto del Trabajador existirá una base jurisprudencial que otorgue garantías de que informando a los alumnos de las reglas de utilización de estos dispositivos y que deben ser respetadas en todo momento, siendo de aplicación en caso contrario la normativa disciplinaria de la Universidad.

Sin embargo, en el caso de que el cliente también desee que los alumnos utilicen sus propios dispositivos, la referida sentencia de la Audiencia Nacional⁴² sería una base jurisprudencial en la que fundar dicho control, aunque ha suscitado cierta polémica y por ello entendemos que no debería ser la opción más recomendable. Pese a ello, permitiría defender un control de los dispositivos que sean titularidad de los estudiantes y que se utilicen para realizar las pruebas académicas, además que la plataforma de *e-learning* que se plantea en el presente informe tiene una mínima intromisión sobre los derechos de los alumnos, pues únicamente registra la actividad de los mismos durante la prueba académica, debiendo los alumnos consentir dicho control, pues sería condición necesaria para poder realizar el examen. Creemos que sería factible y que, informándose adecuadamente a los estudiantes de las Políticas de Uso, de la cookie que utiliza la plataforma durante el desarrollo del examen y de la captación de los datos personales, estaría amparada dicha actuación, pero no se puede controlar totalmente la situación en este caso. Por ejemplo, que un alumno realice la prueba en su ámbito familiar –su vivienda–, podría implicar que se afecte a derechos de terceras personas ya que, como hemos comentado, para garantizar la identificación del alumno y evitar posibles fraudes durante la prueba académica, sería conveniente que durante la duración del examen se grabe la imagen y la voz del estudiante.

En definitiva, en el presente informe hemos abordado las diferentes posibilidades que dispone la Universidad en su deseo de permitir que los estudiantes puedan utilizar dispositivos electrónicos durante las pruebas académicas, considerando el desarrollo de una plataforma propia y la utilización de dispositivos titularidad de la Universidad como la alternativa más factible y que ofrece mayores garantías jurídicas.

⁴² Sentencia de la Audiencia Nacional, Sala de lo Contencioso-Administrativo, recurso nº 481/2012.



5.4- Políticas de Uso de los dispositivos:

En el presente informe, en base a la aplicación analógica del control del uso de los dispositivos en el Derecho Laboral, es defendible y conveniente la elaboración de una Política de Uso de los dispositivos que la Universidad permite utilizar durante la realización de las pruebas académicas.

En estas Políticas de Uso se informará a los alumnos (usuarios del dispositivo) de cuáles son las reglas que deben respetar en todo momento, qué conductas están prohibidas y cómo deben utilizar la plataforma de *e-learning* que la Universidad ha diseñado para el correcto desarrollo de los exámenes por medios electrónicos.

De esta forma, se deberá respetar todo lo establecido en las Políticas de Uso de la Universidad, y en especial los usuarios:

- No podrán utilizar los dispositivos para fines privados o ajenos a los propios de las finalidades previstas, utilizándose de buena fe y para los fines concretos.
- No facilitarán su contraseña de usuario para el acceso a la plataforma a terceros, así como no incumplir las Políticas de Uso y el reglamento disciplinario de la Universidad al realizar conductas fraudulentas para copiar durante la prueba.

Asimismo, en caso de que el usuario se valga de un tercero para llevar a cabo una suplantación de identidad durante la realización de la prueba, el usuario y el tercero colaborador serán objeto de las acciones penales que correspondan, pudiendo serles imputados diversos delitos como la suplantación de identidad (usurpación del estado civil)⁴³.

- Los dispositivos titularidad de la Universidad no son propiedad de los alumnos, que deberán devolverlo cuando así se les comunique.
- Permitir la captación de sus datos de carácter personal (imagen y voz) durante la realización de la prueba, siendo motivo de aplicación de la normativa disciplinaria llevar a cabo comportamientos que dificulten o impidan dicha captación.

⁴³ ABC, 2013. “Detenida por suplantar a una compañera en cinco exámenes universitarios”. Disponible en <http://www.abc.es/sociedad/20131031/rc-detenido-suplantar-companera-cinco-201310311416.html> a 27 de junio de 2015.



- No descargar e instalar en el dispositivo programas adicionales a los autorizados por el profesor correspondiente. El uso de aplicaciones diferentes de las autorizadas durante la realización de la prueba académica derivará en la aplicación de la normativa disciplinaria de la Universidad.
- Estar en posesión de un DNI electrónico que permita la firma electrónica reconocida de los documentos, siendo condición necesaria, al igual que la aceptación del tratamiento de datos personales, para la realización de la prueba académica por medios electrónicos.
- Mantener abierta la sesión de la plataforma durante la realización de la prueba, únicamente finalizando dicha sesión cuando hubiera completado el examen o se hubiera terminado el período de tiempo establecido.
- Tener su dispositivo actualizado y comprobar, previa a la realización de la prueba, su correcto funcionamiento y compatibilidad con la plataforma.
- Los usuarios responderán de los daños que generen, bien sea a la Universidad como a terceros, así como del deterioro, pérdida o sustracción del dispositivo titularidad de la Universidad cuando no cumplan dichas Políticas de Uso.

Hemos redactado, en base al presente informe jurídico, una Política de Uso de los dispositivos, que está adjunta en el [Anexo nº 3](#) del presente informe y que permitirá, de una forma segura tanto para la Universidad como para los alumnos, la utilización de los dispositivos durante la realización de las pruebas académicas.



6- Trabajo futuro:

Al concluir este trabajo, habida cuenta del potencial que puede tener el uso de nuevos dispositivos tecnológicos en la educación, y especialmente en el entorno universitario, cada vez más estrechamente ligado con el ámbito empresarial, es muy posible que dispositivos que están siendo lanzados al mercado actualmente o que lo serán en un futuro cercano, se contemple su utilización con fines educativos y, en concreto, su uso en pruebas académicas.

Algunos dispositivos tecnológicos más “actuales” que están ya en el mercado, como los *smartwatches* y las *smartglasses*, tienen un gran potencial en cuanto al posible impacto que puedan tener en la realización de pruebas académicas por medios electrónicos, pues permiten conectarse con otros dispositivos que posea la persona como su *smartphone*.

Mucho se está hablando de ellos y de su futura introducción en el mercado, pues los *smartcars* pueden suponer otra revolución tecnológica. Aunque parezca una locura, la automatización de la conducción podría permitir que un alumno realice una prueba académica desde su *smartcar* sin necesidad de atender a la carretera y realizar el examen conectando su automóvil con otros aparatos que tengan funcionalidades para ello.

También es probable la comercialización masiva de aparatos de realidad aumentada y realidad virtual, que ya están empezando a comercializarse, aunque están en una etapa embrionaria, y pueden ser otro elemento a tener en cuenta, especialmente para aquellos estudios –ingenierías, por ejemplo– que pueda generar un gran impacto por su utilidad formativa y profesional.

El más que probable impacto que estos novedosos dispositivos podrían tener en la sociedad nos exige plantear un escenario cambiante en los próximos años, introduciéndose en el ámbito cotidiano y, posteriormente, en el contexto educativo, la utilización de estos dispositivos en la formación y evaluación de los estudiantes.

En conclusión, estos nuevos dispositivos y los que están próximamente por llegar hacen impredecible el escenario, a corto y medio plazo, del ámbito educativo, pues aún se desconoce el impacto y las funcionalidades que pueden llegar a alcanzarse con estos aparatos.



7- Bibliografía:

- NARANJO DE LA CRUZ, Rafael. *“Manual de Derecho Constitucional”*, capítulo XVIII, “Derechos fundamentales”, 2012, págs. 489-491.
- AGUADO I CUDOLÀ, Vicenç. *“La presunción de certeza: en el derecho administrativo sancionador”*. Ed. Civitas, 1994.
- RODRÍGUEZ LAINZ, José Luis. *“Estudios sobre el secreto de las comunicaciones: perspectiva doctrinal y jurisprudencial”*. Ed. La Ley, 2011.
- PASCUAL MEDRANO, Amelia. *“El derecho fundamental a la propia imagen: fundamento, contenido, titularidad y límites”*. Ed. Aranzadi, 2003.
- CASTILLA BAREA, Margarita. *“Las intromisiones legítimas en el derecho a la propia imagen: estudio de las circunstancias que legitiman la intromisión en la LO 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen”*. Ed. Thomson Reuters, 2011.
- ABEL LLUCH, Xavier. *“La prueba electrónica”*. Ed. Bosch, 2011.
- GONZÁLEZ-MENESES, Manuel. *“La firma electrónica como instrumento de imputación jurídica : una reflexión de derecho civil sobre la contratación electrónica”*. Ed. Colegio Notarial de Madrid, 2010.
- PERERO CODOSERO, Juan Manuel. *“Desarrollo de un sistema de reconocimiento de habla natural para transcribir contenidos de audio en Internet”*. Proyecto fin de carrera, marzo de 2015.



8- Anexo documental:

▪ Revistas:

- BILLÓN CURRÁS, Margarita; LERA LÓPEZ, Fernando; y ORTIZ SERRANO, Salvador. *“Evidencias del impacto de las TIC en la productividad de la empresa. ¿Fin de la «paradoja de la productividad»?”*. Cuadernos de Economía. Vol. 30, Núm. 82, enero-abril, 2007, págs. 005-036.
- GONZÁLEZ PENDÁS, Paloma. *“Influencia de las TIC en el crecimiento de las TIC en el crecimiento de la productividad. Un análisis descriptivo”*, Revista Economía Industrial (Ministerio de Industria, Energía y Turismo, año 2013, pág. 78.
- ITURRALDE SESMA, Victoria. *“Consideración crítica del principio de permisión según el cual «lo no prohibido está permitido»”*. Anuario de Filosofía del Derecho, Madrid, núm. 15, 1998, págs. 187-218.
- PLANA ARNALDOS, María Carmen. *“El derecho fundamental a la protección de datos fundamentales: el interés legítimo en el tratamiento de los datos”*. Revista Internacional de Trabajo Social y Ciencias Sociales. Ed. Universitas Editorial. ISSN 2173-0512, Nº. 7, 2014, págs. 69-89.
- ROMERO MORENO, Luisa María. *“La seguridad informática en el trabajo con la plataforma ‘Moodle’”*. Revista de Humanidades. ISSN 1130-5029, ISSN-e 2340-8995, Nº. 17, 2010, págs. 169-190.

▪ Artículos, blogs y noticias digitales:

- RODRÍGUEZ CONDE, M^a José. *“Aplicación de las TIC a la evaluación de alumnos universitarios”*. Disponible en http://campus.usal.es/~teoriaeducacion/rev_numero_06_2/n6_02_art_rodriguez_conde.htm a 29 de junio de 2015.
- CARNOY, Martin. *“ICT in Education: Possibilities and Challenges”*. Lección inaugural del curso académico 2004-2005. Disponible en <http://www.uoc.edu/inaugural04/eng/carnoy1004.pdf> a 29/06/2015.
- MARQUÈS GRAELLS, Pere. *“Impacto de las TIC en la enseñanza universitaria”*, 2000 (revisado en 2007). Disponible en <http://ddd.uab.cat/pub/dim/16993748n11/16993748n11a5.pdf> a 29 de junio de 2015.



- FERNÁNDEZ DÍEZ, Antonio. *“Límites y garantías del trabajador en el uso del ordenador de la empresa”*. Disponible en <http://portaljuridico.lexnova.es/articulo/JURIDICO/112513/limites-y-garantias-del-trabajador-en-el-uso-del-ordenador-de-la-empresa> a 29 de junio de 2015.
- Estudios de Grado semipresencial en Biblioteconomía y Documentación en la UC3M. Disponible en http://portal.uc3m.es/portal/page/portal/biblioteconomia_documentacion/estudios/semipresencialidad/FAQs a 29 de junio de 2015.
- Estudios de Grado semipresencial en Humanidades en la UC3M. Disponible en https://portal.uc3m.es/portal/page/portal/titulaciones_grado/hum/plam_semi-presencial/semipresencial_humanidades a 29 de junio de 2015.
- BLASCO GASCÓ, Francisco de Paula. *“Algunas cuestiones del derecho a la propia imagen”*, pág. 38. Disponible en <http://www.derechocivil.net/esp/ALGUNAS%20CUESTIONES%20DEL%20DERECHO%20A%20LA%20PROPIA%20IMAGEN.pdf> a fecha 29 de junio de 2015.
- SEMPERE, Francisco Javier. *“Dictamen del Grupo del Artículo 29 sobre tratamiento de datos basados en el interés legítimo”*, 2014. Disponible en <http://www.privacidadlogica.es/2014/07/08/dictamen-del-grupo-del-articulo-29-sobre-tratamiento-de-datos-basados-en-el-interes-legitimo/> a 29 de junio de 2015.
- Artículo publicado en Kioskea, *“Introducción a la seguridad informática”*, en junio de 2014. Disponible en <http://es.ccm.net/contents/622-introduccion-a-la-seguridad-informatica> a 29 de junio de 2015.
- Zaragoza, I.M. *“La Universidad instala inhibidores de frecuencia para evitar que los alumnos copien”*. Noticia publicada en el Heraldo de Aragón, disponible en <http://www.heraldo.es/noticias/aragon/la-universidad-instala-inhibidores-para-evitar-trampas-los-examenes.html> a 29 de junio de 2015.
- CHAVES GARCÍA, José Ramón. *“Fraude en la Universidad: copiar impunemente con los smartphone”*, diciembre de 2014. Disponible en <http://contencioso.es/2014/12/26/fraude-en-la-universidad-copiar-impunemente-con-los-smartphone/> a 29 de junio de 2015.
- FONT, Susana. *“¿Copias en los exámenes? Así te pueden pillar los profes”*, noticia publicada en. Disponible en <http://mobileworldcapital.com/es/459/> a 29 de junio de 2015.



- Portal de la Administración Electrónica, “*Base legal de la firma electrónica*”, disponible en <http://firmaelectronica.gob.es/Home/Ciudadanos/Base-Legal.html> a 29 de junio de 2015.
- VEGA SUÁREZ, Ana M. “*Análisis del Privacy by Design y su mención en el Reglamento General de Protección de Datos de la UE*”, 2013. Disponible en <http://www.aspectosprofesionales.info/2013/06/analisis-del-privacy-by-design-y-su.html> a 29 de junio de 2015.
- ComputerWorld, 2014. “*El Principio de Privacy by Design, en el Reglamento Europeo de Protección de Datos*”. Disponible en <http://www.computerworld.es/sociedad-de-la-informacion/el-principio-de-privacy-by-design-en-el-reglamento-europeo-de-proteccion-de-datos> a 29 de junio de 2015.
- GOUJON, André. “¿Qué es y cómo funciona una VPN para la privacidad de la información?”. Disponible en <http://www.welivesecurity.com/la-es/2012/09/10/vpn-funcionamiento-privacidad-informacion/> a 29 de junio de 2015.
- Universidad Camilo José Cela, “*Normativa para la realización de exámenes por medios electrónicos*”, 2014. Documento disponible en <https://ucjc.blackboard.com/bbcswebdav/institution/UCJC/Oficializaci%C3%B3n%20Ense%C3%B1anza/NORMATIVAS/NORMATIVA%20PARA%20LA%20REALIZACI%C3%93N%20DE%20EX%C3%81MENES%20POR%20MEDIOS%20ELECTR%C3%93NICOS.pdf> a 29 de junio de 2015.
- University of Bristol, “*Use of computers in examinations - a guide to good practice*”. Disponible en <http://www.bristol.ac.uk/exams/alternative/> a 29 de junio de 2015.
- University of Southern Denmark, “*The University of Southern Denmark’s code of practice for using computers at written campus-based examination*”, 2012. Disponible en [http://www.sdu.dk/en/information til/studerende ved sdu/eksamen/generelt om eksamen/under eksamen/skriftlig proeve digital](http://www.sdu.dk/en/information%20til%20studerende%20ved%20sdu/eksamen/generelt%20om%20eksamen/under%20eksamen/skriftlig%20proeve%20digital) a 29 de junio de 2015.
- University of Birmingham, “*Computer use in an exam*”. Disponible en <https://intranet.birmingham.ac.uk/as/cladls/exams/alternative/computer.aspx> a 29 de junio de 2015.
- University of Copenhagen, “*PC examen*”. Disponible en <http://pc-exam.ku.dk/> a 29 de junio de 2015.



- Swinburne University of Technology *“Use of Computers in Examination”*, disponible en <http://www.swinburne.edu.au/stuserv/disability/computers.html> a 29 de junio de 2015.
- University of Washington. *“Use of Computers on Exams”*, 2003. Disponible en <https://www.law.washington.edu/Students/Academics/Exams.aspx> a 29 de junio de 2015.
- University of Louisville. *“Policy and Procedures: Examinations on Computer”*, 2012-2013. Disponible en <https://www.law.louisville.edu/it/computer-exam-policy> a 29 de junio de 2015.
- Licencia de Moodle, disponible en <https://docs.moodle.org/all/es/Licencia> a 29 de junio de 2015.
- Organización GNU, *“Preguntas frecuentes acerca de las licencias de GNU”*, 2015. Disponible en <http://www.gnu.org/licenses/gpl-faq.html#WhyDoesTheGPLPermitUsersToPublishTheirModifiedVersions> a 29 de junio de 2015.
- TEKNAUTAS, 2015. *“La segunda resurrección del DNI electrónico: para qué podrás usarlo”*. Disponible en <http://www.elconfidencial.com/tecnologia/2015-01-12/la-segunda-resurreccion-del-dni-electronico-para-que-podras-usarlo> 620665/> a 29 de junio de 2015
- ABC, 2013. *“Detenida por suplantar a una compañera en cinco exámenes universitarios”*. Disponible en <http://www.abc.es/sociedad/20131031/rc-detenido-suplantar-companera-cinco-201310311416.html> a 29 de junio de 2015.
- PARRA, Samuel. *“La voz es un dato personal”*. Disponible en <https://www.samuelparra.com/2010/10/20/la-voz-es-un-dato-personal/> a fecha de 29 de junio de 2015.
- CUBILLO, Mercedes. *“Creación de exámenes con Moodle”*. <http://recursostic.educacion.es/observatorio/web/en/software/software-educativo/1081-creacion-de-examenes-con-moodle> a fecha 29 de junio.
- FERNÁNDEZ BURGUEÑO, Pablo. *“¿Es delito suplantar la identidad de otro?”*. Disponible en <http://www.pabloburgueno.com/2010/03/%C2%BFes-delito-suplantar-la-identidad-de-otro/> a 29 de junio de 2015.



- MOGUER, M. *“La universidad Pablo de Olavide investiga una supuesta red de tráfico de exámenes”*. Disponible en <http://sevilla.abc.es/sevilla/20150225/sevi-olavide-investigacion-201502241041.html> a 29 de junio de 2015.
 - MARÍN, Mihaela. *“El mundo en 2030 según las predicciones de Bill Gates”*. Disponible en <http://www.ticbeat.com/innovacion/el-mundo-en-2030-segun-las-predicciones-de-bill-gates/> a 29 de junio de 2015.
 - Xataka. *“Las universidades británicas prohíben los smartwatches en los exámenes”*. Disponible en <http://www.xatakandroid.com/gadgets-android/las-universidades-britanicas-prohiben-los-smartwatches-en-los-examenes> a 29 de junio de 2015.
 - D. MACHARGO, Susana. *“La Universidad se blindo frente al fraude en los exámenes”*. Disponible en <http://www.asturias24.es/secciones/vivir/noticias/la-universidad-se-blinda-frente-al-fraude-en-los-examenes/1400432128> a 29 de junio de 2015.
 - MARTÍNEZ, R. *“Interés legítimo y protección de datos personales en la sentencia de 8 de febrero de 2012 del TS”*. Disponible en <http://lopyseguridad.es/interes-legitimo-y-proteccion-de-datos-personales-en-la-sentencia-de-8-de-febrero-de-2012-del-ts/> a 29 de junio de 2015.
 - Amedeo Maturó. *“El Director de Instituto: el Omnipotente”*. Disponible en <http://www.amedeomaturó.com/2013/10/07/el-director-de-instituto-el-omnipotente/> a 29 de junio de 2015.
- Legislación y normas:
- Constitución española, «BOE» núm. 311, de 29 de diciembre de 1978.
 - Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, «BOE» núm. 115, de 14 de mayo de 1982.
 - Directiva 95/46/CE del parlamento europeo y del consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, «DOUE» núm. 281, de 23 de noviembre de 1995.
 - Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, «BOE» núm. 298, de 14 de diciembre de 1999.



- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, «BOE» núm. 17, de 19 de enero de 2008.
- Article 29 Data Protection Working Party, *“Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC”* (Dictamen del Grupo del Artículo 29 sobre tratamiento de datos basados en el interés legítimo), WP 217/2014, adoptada el 9 de abril.
- Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico, «BOE» núm. 166, de 12 de julio de 2002.
- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, «BOE» núm. 114, de 10 de mayo de 2014.
- Directiva 1999/05/CE del Parlamento Europeo y del Consejo, de 9 de marzo de 1999, sobre equipos radioeléctricos y equipos terminales de telecomunicación y reconocimiento mutuo de su conformidad.
- Ley 59/2003, de 19 de diciembre, de Firma Electrónica, «BOE» núm. 304, de 20 de diciembre de 2003.
- Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil, «BOE» núm. 7, de 8 de enero de 2000.
- Ley 2/2010, de 15 de junio, de Autoridad del Profesor, «BOE» núm. 238, de 1 de octubre de 2010.
- Real Decreto 1791/2010, de 30 de diciembre, por el que se aprueba el Estatuto del Estudiante Universitario, «BOE» núm. 318, de 31 de diciembre de 2010.
- «Guía de buenas prácticas de los estudiantes de la Universidad Carlos III de Madrid», aprobada por el Consejo de Gobierno en su sesión de 29 de noviembre de 2012.
- Adaptación de la normativa reguladora de la realización de exámenes por medios electrónicos a los estudiantes de la Universidad Carlos III de Madrid que se encuentren realizando programas oficiales de intercambio, aprobada por el Consejo de Gobierno en sesión de 20 de octubre de 2006, modificada en sesión de 7 de febrero de 2013.



▪ Jurisprudencia:

- Tribunal Supremo, Sala Segunda, de lo Penal, Sentencia 311/2015, de 27 mayo. JUR 2015\154238, que hace referencia a lo dispuesto en la STC 207/1996.
- Tribunal Constitucional, Sala Primera, de lo Civil, Sentencia 207/1996, de 16 de diciembre, Fundamento Jurídico Tercero (apartado B).
- Tribunal Supremo, Sala Cuarta, de lo Social, Sentencia 6128/2007, de 26 de septiembre, Fundamento Jurídico Cuarto.
- Constitucional, Sala Primera, de lo Civil, Sentencia 18/1981 de 8 de junio, Fundamento Jurídico Segundo.
- Audiencia Nacional, Sala de lo Contencioso-Administrativo, Sentencia 3877/2013 ante el recurso nº 481/2012, 26 de septiembre de 2013.

▪ Informes jurídicos:

- Informe jurídico nº 0112/2012 de la Agencia Española de Protección de Datos, pág. 2 en relación con el interés legítimo.
- Informe jurídico nº 0247/2008 de la Agencia Española de Protección de Datos, págs. 8-9 en relación con el interés legítimo.
- Informe nº 2010/009 de la Unidad Central de Seguridad Privada, perteneciente al Cuerpo de Policía Nacional, de febrero de 2010, en relación a la utilización de inhibidores de frecuencia.
- Informe nº 0392/2011 de la Agencia Española de Protección de Datos, págs. 8-9 en relación con el reconocimiento facial en los accesos a clases.



ANEXOS



ANEXO I: Aviso de Cookies

Previo al acceso a la prueba académica por el usuario (estudiante), se mostrará el siguiente aviso de la utilización de una cookie de sesión por parte de la Universidad con la finalidad de permitir el correcto funcionamiento de la plataforma durante el examen y el control de la conducta del alumno, mediante el registro de su actividad y la captación de su imagen y voz (audio), con la finalidad de garantizar que no se utilizan medios fraudulentos o ayudas externas durante la prueba.

Este aviso actuará como primera y única capa de información, pues según las disposiciones de la Agencia Española de Protección de Datos no será necesario el aviso de la instalación de cookies cuando tengan fines de permitir la prestación del servicio solicitado por el usuario (cookies exentas de informar). Pese a ello, la Universidad dará mediante este aviso la información esencial sobre la cookie utilizada de una forma visible, no pudiendo avanzarse en la plataforma para comenzar el examen sin el consentimiento expreso del usuario aceptando la cookie.

En dicho aviso se establecerá lo siguiente:

“La Universidad Carlos III de Madrid utiliza una cookie de sesión que garantiza el correcto desarrollo de la prueba académica que usted va a realizar a continuación. Esta cookie asegura que no se produzcan, por el usuario, acciones cuya finalidad contravienen la Política de Uso de la presente plataforma y que usted ha aceptado previamente.

Para proceder a la realización del examen por los medios solicitados, usted deberá aceptar expresamente la instalación de dicha cookie realizando ‘clic’ sobre la opción ‘aceptar’ que está situada en la parte inferior del presente aviso. Le informamos que dicha aceptación supone la expresión de su consentimiento para la recogida y tratamiento de sus datos personales”.



ANEXO II: Cláusula informativa

Conforme a lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal, se le informa:

1. Que sus datos personales relativos a su imagen y su voz serán incorporados al fichero automatizado denominado “**ALUMNOS**”, que está debidamente inscrito en la Agencia Española de Protección de Datos, del que es titular la **Universidad Carlos III de Madrid** con el fin de que sus datos sea recogidos y tratados para que la prueba académica se desarrolle respetando la normativa disciplinaria de la Universidad en todo momento.
2. Que usted no está obligado a prestar su consentimiento para la recogida y tratamiento de sus datos personales, pero que de no ser realizado no será posible cumplir su solicitud de realización de las pruebas académicas correspondientes mediante la realización de las mismas por medios electrónicos.
3. Que sus datos no van a ser cedidos a terceros, salvo cuando sea necesario para el correcto desenvolvimiento de los fines para los que se recogen y tratan los datos. Esta cesión se realizará únicamente para que la prueba académica se desarrolle respetando la normativa disciplinaria de la Universidad.
4. Que sus datos personales serán tratados con la confidencialidad exigida por la normativa en materia de protección de datos y se adoptarán las medidas de seguridad que fueran pertinentes.
5. Que, previo al inicio de la prueba académica, se informará al alumno de que será necesaria la instalación de una “cookie de sesión” que permita el desarrollo del examen y, para el control de las conductas del alumno, la captación de la imagen (vídeo) y voz (audio) del estudiante.
6. Que la firma de la presente cláusula informativa se realizará con carácter previo a la realización de la prueba académica, siendo condición necesaria para poder efectuar el examen por medios electrónicos.
7. Que usted podrá ejercer los derechos de acceso, rectificación, cancelación y oposición remitiendo un escrito a la dirección del responsable del fichero, la Universidad Carlos III de Madrid, en el que conste la petición que concreta la solicitud, la dirección a efectos de notificaciones y comunicaciones, copia del



DNI, la firma y fecha. Para ello puede utilizar los modelos publicidad por la Agencia Española de Protección de Datos.

El firmante se hace responsable de la veracidad de los datos aportados y se le ruega que, en el supuesto de producirse alguna modificación en sus datos de carácter personal, nos lo comunique con el fin de mantenerlos actualizados.

Mediante la presente leyenda se cumple con el **deber de información** legal exigido por la normativa de protección de datos y con su firma **otorga su consentimiento** para el tratamiento de sus datos con los fines previstos. Además se le informa que la presente leyenda quedará en poder de la Universidad Carlos III de Madrid con los fines de prueba dispuestos en la legislación aplicable.

En....., a de..... de 20.....

Fdo: _____



ANEXO III: Normas para el uso de los dispositivos

El presente documento tiene la finalidad de dar a conocer a los estudiantes y al personal docente de la Universidad Carlos III de Madrid (en adelante, la “Universidad”) la política de utilización de dispositivos durante la realización de pruebas académicas, informándoles sobre los procedimientos existentes en éste documento respecto al control del uso de los dispositivos y sobre el tratamiento de datos personales durante la utilización de los mismos durante dichos exámenes universitarios.

1- Utilización de dispositivos:

El fundamento de las normas que a continuación se fijan es proteger a la Universidad y a sus estudiantes y personal (en adelante, los “usuarios”) de los riesgos derivados de un uso inadecuado de los sistemas de información –dispositivos como ordenadores, *smartphones* y *tablets*– puestos a su disposición por parte de la Universidad.

Las presentes normas son de aplicación a la totalidad de los usuarios de la Universidad y el presente documento será público y se mantendrá disponible para su consulta, en cualquier momento, a través del sitio web de la Universidad.

En el supuesto de que estas normas fueran objeto de modificación y/o adaptación a nuevas circunstancias o modificaciones legales, se tomarán por parte de la Universidad las medidas precisas al objeto de mantener a los usuarios en conocimiento de las citadas actualizaciones.

1.1- Disposiciones generales:

Los usuarios de la Universidad, durante el período en que utilicen dispositivos para la realización de las pruebas académicas, cuando así esté previsto por la Universidad, deberán en todo momento cumplir las siguientes disposiciones:

- Los dispositivos y los datos e información a los que se acceda, por ejemplo el profesor que acceda a la prueba académica de un alumno para su corrección, no podrán ser utilizados para fines privados o para cualesquiera otros fines ajenos a los propios de las finalidades y obligaciones que tuvieran los usuarios con respecto a la Universidad.
- Los dispositivos facilitados a los usuarios por la Universidad son propiedad de ésta, debiendo ser devueltos cuando así se requiera. Estos dispositivos



se proporcionan exclusivamente para la realización de las pruebas académicas o de las finalidades propias autorizadas por la Universidad, reduciéndose su uso a estos fines.

- Los dispositivos puestos a disposición de los usuarios deben ser utilizados conforme a los principios de buena fe y en todo caso con la finalidad asignada. No estará permitido el uso con fines privados de los dispositivos.
- Los usuarios se comprometen a cumplir las presentes Políticas de Uso, siendo responsables frente a la Universidad y frente a terceros de cualquier daño que pudiera derivarse de dicho incumplimiento, y resarcirá a la Universidad por las indemnizaciones, sanciones o reclamaciones que está se viera obligada a satisfacer como consecuencia de dicho incumplimiento.
- Las anteriores normas permanecerán vigentes con carácter indefinido hasta su modificación o derogación.

1.2- Normas para el uso de la plataforma de la Universidad:

La Universidad, en un esfuerzo por desarrollar una plataforma de *e-learning* que interfiera mínimamente en la privacidad y el derecho a la protección de datos de los usuarios, con el único fin de permitir el correcto desarrollo del examen y del control de la conducta del alumno durante el mismo, requiere que los estudiantes que deseen realizar la prueba académica correspondiente utilizando dispositivos electrónicos para ello, deban aceptar como condición necesaria para poder proceder a dicha ejecución las presentes normas de uso de la plataforma.

Con la finalidad de garantizar el correcto uso de la plataforma, se han adoptado las siguientes normas:

- La plataforma y los datos e información contenidos en la misma no podrán ser en ningún caso objeto de uso para fines privados o para cualesquiera otros fines ajenos a las finalidades previstas.
- Instalación de programas y aplicaciones. La utilización de la plataforma para los fines previstos no requiere de la instalación de ningún programa o aplicación adicional. En caso de que, para la realización de la prueba académica, el profesor autorizase el uso de aplicaciones adicionales, las mismas deberán ser instaladas en los dispositivos por el Servicio de Informática y Comunicaciones de la Universidad, recordando que la plataforma, mediante la herramienta (cookie de sesión) que utiliza, controlará que el alumno no utilice fuentes no autorizadas.



- Autenticación. El usuario accederá a la plataforma con su nombre de usuario y contraseña, y deberá introducir en el lector externo habilitado su DNI electrónico durante todo el período que dure el examen, de forma que se garantice la autoría del mismo por medio de la firma electrónica reconocida que ostenta nuestro Documento de Identidad.
- Confidencialidad. El usuario no revelará su contraseña de la plataforma a un tercero. Asimismo, el usuario no facilitará a terceros ningún dispositivo que le fuera facilitado por la Universidad para la realización de la prueba académica.
- El usuario se compromete a garantizar que en todo momento, durante la realización de la prueba académica, la cámara del dispositivo o webcam se encuentra en funcionamiento y que, además, es posible grabación de audio. La realización de conductas tendentes a impedir la grabación de la imagen y el audio durante la prueba estará tipificada como infracción según la normativa disciplinaria de la Universidad.
- El acceso de los usuarios a la plataforma quedará registrado, así como cualquier actividad que desarrollan en la misma, de forma que se generará prueba no sólo de la realización del examen, si no de cuantas conductas inadecuadas lleve a cabo el alumno así como de los accesos del profesor a la prueba académica de cada alumno.

En todo caso, el acceso del profesor a la prueba deberá producirse durante la fase de corrección y calificación de los exámenes, y únicamente estará permitida la incorporación de comentarios y de notas de valoración del examen. El profesor no estará autorizado, en ningún caso, a modificar la prueba académica, de forma que cualquier incumplimiento del presente documento implicará la adopción de las medidas disciplinarias oportunas.

- Los usuarios que, con intención de utilizar métodos fraudulentos durante la realización de la prueba académica, se ayuden de un tercero que actúe por su cuenta y nombre, utilizando medios físicos o técnicos para suplantar la identidad del usuario que está efectuando el examen, estarán cometiendo posibles conductas delictivas. Asimismo, el tercero que colabore con el usuario en la conducta delictiva, responderá penalmente de sus actos.
- El usuario será responsable frente a la Universidad y frente a terceros de cualquier daño que pudiera derivarse del incumplimiento de las anteriores normas, y resarcirá a la Universidad por las indemnizaciones, sanciones o



reclamaciones que está se viera obligada a satisfacer como consecuencia de dicho incumplimiento.

1.3- Normas a cumplir durante la realización de la prueba académica:

En el período en que se encuentre activo en la plataforma el desarrollo de la prueba académica habilitada, los usuarios deberán respetar las siguientes normas:

- El usuario, previo al comienzo de la prueba, deberá aceptar de forma expresa la cookie de sesión que incorpora la plataforma y que permite la realización de la prueba y el control de la actividad del usuario. Asimismo, el usuario deberá introducir en el lector externo su DNI electrónico, que deberá mantener durante la realización de todo el examen.
- El usuario, también con carácter previo al inicio del examen, debe aceptar que se proceda a la grabación de su imagen y de su voz (audio) a lo largo de la prueba, con la finalidad de garantizar la identidad del autor y de que no se ha infringido la normativa disciplinaria. La realización de conductas tendentes a impedir la grabación de la imagen y el audio durante la prueba estará tipificada como infracción según la normativa disciplinaria de la Universidad.
- Una vez iniciado el examen, el usuario no podrá abandonar la sesión en la plataforma mientras no hubiera finalizado su prueba o se hubiera agotado el período de tiempo establecido para su realización. La cookie que incorpora la plataforma registrará este abandono, lo que supondrá la efectiva entrega del examen en las condiciones en que se encontrara la prueba en el momento inmediatamente anterior al fin de la sesión en la plataforma.
- La prueba finalizará con la entrega del examen por el usuario o cuando se hubiera agotado el período de tiempo establecido. La prueba será guardada en los servidores y la Universidad y únicamente será accesible por el profesor en los términos anteriormente establecidos. Sin embargo, será posible que el alumno pueda solicitar al profesor la impresión de una copia de su prueba.
- Los usuarios que, por medio de un tercero que accede con sus datos a la plataforma, realicen la prueba académica por medios fraudulentos, les será de aplicación la normativa disciplinaria en los términos anteriores.



1.4- Normas de uso de los dispositivos de la Universidad:

Para la realización de las pruebas académicas correspondientes, la Universidad podrá poner a disposición de los alumnos ciertos dispositivos. Estos dispositivos consistirán en ordenadores –de sobremesa o portátiles–, *smartphones* y *tablets*. Asimismo, si fuesen necesarios, se pondrá a disposición de los alumnos dispositivos adicionales como micrófonos y webcams, con la finalidad de que se cumplan los requisitos exigidos en la presente normativa para la realización de los exámenes permitiendo el control de la conducta de los usuarios.

Los dispositivos que la Universidad pone a disposición de los usuarios son, en todo caso, propiedad de ésta. La Universidad podrá solicitar la devolución de cualquier dispositivo puesto a disposición de los usuarios en cualquier momento.

Los usuarios no están habilitados a adquirir o descargar en el dispositivo de la Universidad ninguna aplicación adicional a las que éste tuviera incorporadas. En caso de ser autorizado por el profesor el uso de aplicaciones adicionales, será el Servicio de Informática y Comunicaciones de la Universidad quien proceda a dicha descarga o instalación.

El usuario será responsable de la custodia e integridad de los dispositivos puestos a su disposición. Al objeto de evitar en la medida de la posible pérdida o sustracción de los dispositivos, en especial si se trasladasen fuera de las dependencias de la Universidad, habrán de seguirse las siguientes recomendaciones mínimas de seguridad:

- Se evitará dejar el dispositivo sin vigilancia en lugares públicos y/o fácilmente accesibles por terceros no autorizados.
- Se evitará su depósito en habitáculos sin protección de cerradura o mecanismo de seguridad equivalente.
- Cuando se realice la prueba en lugares públicos, se evitará que la cámara o webcam del dispositivo capte la imagen de terceros, con la finalidad de impedir la vulneración de posibles derechos fundamentales.
- Se impedirá la manipulación del dispositivo por terceros no autorizados.
- Se adoptarán medidas adecuadas para la conservación y buen funcionamiento de los dispositivos, en particular, y sin carácter limitativo, se intentarán evitar caídas, humedades o exposición prolongada a fuentes



de calor. Igualmente, se deberán adoptar medidas adecuadas para evitar la sustracción de dichos dispositivos.

1.5- Normas de uso de los dispositivos de los estudiantes:

Los usuarios de la plataforma que, para el desarrollo de las pruebas académicas utilicen sus propios dispositivos electrónicos, deberán en todo caso conocer que deben respetar las presentes disposiciones generales, las normas para la utilización de la plataforma y reglas a cumplir durante la realización de la prueba.

Especialmente, el usuario que solicite la realización de una prueba académica utilizando sus propios dispositivos, será conocedor de que la plataforma de *e-learning* que utiliza la Universidad exige, como condición necesaria para realizar el examen, la aceptación de una cookie de sesión que garantiza el correcto desarrollo del examen y el control de la actividad realizada por el alumno durante el mismo.

Asimismo, se establece como segunda condición necesaria que el dispositivo utilizado por el estudiante incorpore una herramienta de captación de su imagen y voz (audio) con el fin de que se pueda garantizar que el alumno no realiza un uso fraudulento o se ayuda de fuentes o personas no autorizadas durante la prueba.

El estudiante será responsable de que su dispositivo sea compatible con la plataforma de la Universidad, se encuentre actualizado y que hubiera comprobado su correcto funcionamiento con carácter previo al examen.

Por último, se informará al estudiante que utilice sus propios dispositivos que deberá contar con un mecanismo, como un lector externo de su DNI electrónico, que garantice la autenticación del usuario durante la realización de la prueba, o bien que esté en disposición de un DNI electrónico 3.0 que permite, mediante la aprobación del Documento de Identidad al dispositivo mediante el uso de tecnología NFC, la autenticación del usuario.

2- Medidas de control:

La Universidad se reserva el derecho y la posibilidad de comprobar el correcto cumplimiento de estas normas mediante los procedimientos que estime oportunos a tales efectos. El usuario deberá evitar contar con datos personales en los dispositivos puestos a su disposición con la finalidad de que tales procedimientos de control no puedan vulnerar su intimidad personal.



En todo caso, el control de la actividad del dispositivo se realizará en especial en relación con su utilización durante la prueba académica desarrollada, con el fin de garantizar el adecuado uso del dispositivo para evitar que el alumno utilice fuentes no autorizadas durante el ejercicio.

3- Responsabilidad:

La inobservancia por parte de los usuarios de las normas establecidas en el presente documento podrá dar lugar a responsabilidades personales, civiles o penales, frente a la Universidad, frente a la Administración Pública o frente a cualquier tercero.

4- Tratamiento de datos personales:

La plataforma de *e-learning* desarrollada por la Universidad sólo tratará y utilizará aquellos datos personales que sean necesarios para el desarrollo de las pruebas académicas y la comprobación de la adecuada conducta de los usuarios.

El personal de la Universidad queda obligado a seguir las instrucciones que fije ésta en todo lo que respecta al tratamiento de los datos personales, no pudiendo utilizar y/o tratar los datos para fines distintos de los expresamente indicados – tratamiento confidencial de los datos personales–, debiendo cumplir el deber de secreto respecto de los datos de carácter personal a los que tenga acceso.

Asimismo, la prueba académica y los datos personales asociados a ésta, como la captación de la imagen y la voz del alumno, serán conservados únicamente el tiempo que sea necesario para la garantía del respeto de los derechos del alumno y del control del correcto desarrollo del examen, siendo eliminados los datos de carácter personal una vez se extinga esta necesidad de conservación.

En cualquier caso, se informará al usuario de la plataforma sobre el tratamiento de los datos de carácter personal, siendo la exclusiva finalidad del tratamiento de los mismos la gestión de las pruebas académicas y la vigilancia de la correcta conducta de los estudiantes.

Asimismo, se informará a los estudiantes que sus datos podrán ser cedidos a diversos órganos de la Administración Pública con la finalidad de cumplir con las obligaciones legales que se deriven.



La Universidad, como responsable de un fichero que contiene datos de carácter personal, garantiza y reconoce el ejercicio de los derechos de acceso, rectificación, cancelación y oposición de los datos facilitados que podrá ejercitar en los términos establecidos en la Legislación vigente dirigiéndose, indicando el responsable del fichero, a la dirección que así establezca.

Cualquier modificación que en su caso pueda producirse en los datos de carácter personal suministrados, deberá ser puesta en conocimiento por parte del titular de los mismos a la Universidad, respondiendo el usuario en cualquier caso de la veracidad y exactitud de los datos facilitados en cada momento.

El usuario declara haber leído las correspondientes Políticas de Uso de los dispositivos, comprendiéndola y aceptándola mediante su firma.

Fdo: _____

Fecha: _____