



# Informe sobre el impacto normativo de los procedimientos de evaluación online: protección de datos y garantía de los derechos de las y los estudiantes

Ricard Martínez Martínez (Universidad de Valladolid, Universidad de Burgos, Universidad de Salamanca, Universidad de La Laguna, y Universitat Politècnica de València)

Mónica Arenas Ramiro (Universidad de Alcalá)

José Pascual Gumbau Mezquita (Universitat Jaume I)

Condiciones de uso del documento	
	Este documento se crea a disposición de las universidades españolas a las que se otorga permiso para su uso y adaptación.
	Cuando la función de delegado de protección de datos y/o de asesoramiento jurídico se haya externalizado se prohíbe cualquier uso externo, modificación o adaptación para su explotación comercial como servicio en cualquier entorno, y en particular en entornos de formación o educativos ajenos al de la propia universidad integrada en CRUE.

## Índice

<b>01</b>	<b>1. Escenarios de realización de exámenes online</b>
<b>04</b>	<b>2. Protección de datos personales</b>
<b>04</b>	2.1 Legitimación y condiciones de los tratamientos
<b>05</b>	2.2 Legitimación y condiciones de los tratamientos de categorías especiales de datos
<b>07</b>	2.3 Legitimación y condiciones de los tratamientos consistentes en la captación y grabación de imágenes
<b>11</b>	2.4 La captación de datos por las y los estudiantes o de los propios estudiantes
<b>13</b>	2.5 Aplicaciones móviles. Servicios no concertados. Bring Your Own device-BYOD
<b>14</b>	2.6 El tratamiento de la información ante las incidencias en el proceso de evaluación
<b>15</b>	2.7 Publicación de notas y tratamiento de datos en los procesos de revisión de las pruebas de evaluación
<b>18</b>	2.8. Derechos de supresión y oposición al tratamiento.
<b>19</b>	2.9 Servicios externos: el contrato de encargado del tratamiento
<b>20</b>	2.10 Garantía del cumplimiento normativo de la universidad
<b>22</b>	<b>3. Protección, disponibilidad, portabilidad y resiliencia</b>
<b>28</b>	<b>4. Recomendaciones</b>
<b>28</b>	4.1 Recomendaciones generales
<b>29</b>	4.2 Recomendaciones específicas

## ABREVIATURAS

<b>AEPD</b>	<b>Agencia Española de Protección de Datos</b>
<b>ENS</b>	Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica
<b>LOPDGDD</b>	Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales
<b>LOU</b>	Ley Orgánica 6/2001, de 21 de diciembre, de Universidades
<b>RGPD</b>	Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos

## 1. Escenarios de realización de exámenes online

De acuerdo con la información disponible los tipos de evaluación que podrían ser realizados por las Universidades son los que siguen:

1. Examen oral.
2. Prueba escrita abierta.
3. Prueba objetiva.
4. One minute paper.
5. Trabajo académico.
6. Mapas conceptuales.
7. Diario reflexivo.
8. Portafolio.
9. Observación.
10. Proyectos.
11. Problemas/Casos.

Se han identificado al menos tres canales para la realización de estos tipos de evaluación sobre los que se proyectará el análisis relativo al cumplimiento normativo a integrar en los escenarios definidos por el grupo de trabajo:

1. Aula virtual.
2. Canales de videoconferencia.
- 3.-Entornos de trabajo en cloud.

De entre los canales posibles se han excluido:

A. Las técnicas de proctoring en la medida en la que como se señala en la sección 2.3 pueden plantear particulares dificultades o riesgos en materia de:

- Proporcionalidad.
- Predeterminación normativa.
- Necesidad de desarrollar una evaluación de impacto relativa a la protección de datos.

B.-El correo electrónico. El uso de esta herramienta presenta a nuestro juicio los siguientes riesgos:

- En muchas instituciones universitarias no existe una separación neta entre usos profesionales y privados. Ello implica dificultades muy específicas en el acceso al contenido de los mismos. En el contexto actual, los riesgos de afectación a la vida privada y al secreto de las comunicaciones de un profesor que eventualmente se encontrase en una UCI harían muy difícil la recuperación de pruebas de evaluación sin el concurso de un juez. Tamaño esfuerzo desproporcionado no sólo desaconseja su uso sino que incluso aconseja su expresa y estricta prohibición.
  - De la capacidad de almacenamiento de este tipo de sistemas de información y del modelo de gestión individual por cada usuario pueden derivar riesgos:
  - Borrado accidental.
  - Clasificación inadecuada y dificultades de localización y recuperación.
  - Descarga de datos en unidades locales no autorizadas.
  - Ataques informáticos.

- Por último, en una lista que no es exhaustiva, el gestor de correo, especialmente cuando el profesor utiliza descargas en archivos locales (POP3) puede plantear serios problemas de copiado de seguridad, trazabilidad, y disponibilidad de la información.

Sin perjuicio de los tratamientos específicos de datos personales a los que se refieren los epígrafes posteriores cabe identificar los distintos tratamientos que se producen, con carácter general, en todos los escenarios o canales descritos. Todos ellos cumplen con finalidades comunes que por razones de economía de medios y usabilidad no se incluyen en la tabla posterior:

1. Identificación de las personas evaluadas y de los evaluadores.
2. Gestión administrativa y académica de las pruebas.
3. Controles sobre el normal desarrollo de la prueba y garantía de las exigencias de transparencia y seguridad jurídica de los procesos de evaluación.
4. Corrección de las pruebas.
- 5.-Procesos de revisión ordinaria o primera revisión de las pruebas.

Del mismo modo, resulta común a todos los tipos de prueba el empleo de datos de identificación, si bien en algunos casos posee una naturaleza cualificada. En este sentido el uso de datos de identificación al que se refiere este documento integra dos tipos de procedimiento:

1. Uso de claves concertadas en el acceso a los sistemas de información.
2. Verificación visual de la identidad de los estudiantes y de sus acciones durante la prueba.

En principio, y de acuerdo con una clasificación aproximada, se han identificado distintos tipos de canales para el desarrollo de las pruebas e identificado tratamientos específicos que se suman a los usuales:

Canal	Titularidad	Tipo	Tratamiento
			Común: identificación Seguimiento mediante webcam
<b>Aula virtual</b>	Propia (puede existir un proveedor de servicios de alojamiento)  Integra o usa herramientas antiplagio ajenas	2. Prueba escrita abierta.	
		3. Prueba objetiva.	
		4. One minute paper.	
		5. Trabajo académico.	Datos incorporados a las tareas: entrevistas, grabaciones, videos, fotografías.
		6. Mapas conceptuales.	
		7. Diario reflexivo.	Datos subjetivos o de personalidad
		8. Portafolio.	Datos incorporados a las tareas: entrevistas, grabaciones, videos, fotografías
		10. Proyectos.	Datos incorporados a las tareas: entrevistas, grabaciones, videos, fotografías
11. Problemas/Casos.			
			Seguimiento mediante webcam Grabaciones
<b>Videoconferencia</b>	Proveedor de servicios	1. Examen oral.	Seguimiento mediante webcam
		2. Prueba escrita abierta.	

	* Se desconoce si existen herramientas propias o instaladas localmente.	3. Prueba objetiva. 9. Observación.	Grabaciones Seguimiento mediante webcam Grabaciones
<b>Entornos de trabajo en cloud</b>	Proveedor de servicios	4. One minute paper.	
		6. Mapas conceptuales.	Datos incorporados a las tareas: entrevistas, grabaciones, videos, fotografías
		9. Observación.	

En la siguiente tabla se incluyen finalidades y tipos de datos cualificados en el contexto del tipo de pruebas.

Prueba	Finalidad	Datos	Tratamiento
Común	Controlar actuaciones arbitrarias o ilícitas	Con carácter común: profesor responsable, identificación del estudiante que se examina	Depende de cada prueba
1. Examen oral.	Registro de la prueba	Imagen y voz	Grabación
2. Prueba escrita abierta.	Antiplagio	Datos de estudiantes plagiados	Analítica de datos
3. Prueba objetiva.	Antiplagio	Datos de estudiantes plagiados	Analítica de datos
4. One minute paper.	Antiplagio	Datos de estudiantes plagiados	Analítica de datos
5. Trabajo académico.	Antiplagio	Datos de estudiantes plagiados	Analítica de datos
6. Mapas conceptuales.	Antiplagio	Datos de estudiantes plagiados	Analítica de datos
7. Diario reflexivo.	Antiplagio	Datos de estudiantes plagiados	Analítica de datos
8. Portafolio.	Antiplagio	Imagen y voz Datos de personas participantes	Grabación
9. Observación.	Registro de la prueba	Imagen y voz	Grabación
10. Proyectos.	Antiplagio	Imagen y voz Datos de personas participantes	Grabación
11. Problemas/Casos.	Antiplagio	Datos de estudiantes plagiados	Analítica de datos

## 2. Protección de datos personales

### 2.1 Legitimación y condiciones de los tratamientos de datos personales

La Ley Orgánica 6/2001, de 21 de diciembre, de Universidades, en adelante LOU, atribuye en su artículo 1 a las universidades la prestación del servicio público de educación superior. Por otra parte, conforme dispone el artículo 2.2.f de esta Ley orgánica, integra la autonomía universitaria la verificación de conocimientos de los estudiantes. Esta facultad viene completada por el artículo 46 de la LOU que cuyo párrafo primero configura el estudio como un derecho-deber de los estudiantes, ordenando el tercero a las universidades establecer los procedimientos de verificación de los conocimientos de los estudiantes. De la misma forma se establece el derecho de los estudiantes a una evaluación objetiva en el Real Decreto 179/2010, de 30 de diciembre, por el que se aprueba el Estatuto del Estudiante Universitario (en adelante, Estatuto del Estudiante).

El desarrollo de un examen requiere de la identificación de las personas que concurren a la prueba, tal y como dispone el art. 25.7 del citado Estatuto del Estudiante, así como la evaluación de los conocimientos que la misma trata de acreditar. Por otra parte, en el contexto del llamado proceso de Bolonia, la evaluación no se proyecta sobre los conocimientos strictu sensu sino sobre las competencias adquiridas por las y los estudiantes, competencias evaluables que deben constar en las Memorias de los Planes de estudio correspondientes y, por tanto, en las conocidas como Guías o Programas docentes de las asignaturas (como se recoge en el Anexo del Real Decreto 1393/2007, de 29 de octubre, por el que se establece la ordenación de las enseñanzas universitarias oficiales).

Toda esta tarea comporta necesariamente el tratamiento de datos personales en los términos en los que resultan definidos por el artículo 4 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, en adelante RGPD.

1) «datos personales»: toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;

2) «tratamiento»: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción;

Así pues, más allá de las condiciones básicas de todo tratamiento, recogidas en el artículo 5 del RGPD y basadas en los principios de licitud, minimización y finalidad, entre otros, y con independencia de la naturaleza pública o privada de las universidades, desde el punto de vista del juicio de legitimación y legalidad que exige el artículo 6 del RGPD, los tratamientos necesarios para la evaluación universitaria encontrarían acogida, al menos, en alguna de las siguientes condiciones definidas por el precepto:

b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;

c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;

e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;

Con motivo de la realización de un examen se vienen tratando distintos tipos de datos, en el mundo físico:

- Apellidos y nombre de las y los estudiantes.
- La imagen o fotografía de las y los estudiantes en sus carnets de estudiantes o documentos identificativos.
- Datos relacionados con las asignaturas.
- Datos relacionados con el profesorado responsable.
- Datos relacionados con la evaluación y calificación de las pruebas, incluidas las anotaciones subjetivas derivadas de la corrección.

Por otra parte, en el contexto de la evaluación continuada en entornos de aula virtual con carácter adicional se tratan aquellos datos necesarios para el acceso e identificación de las personas. Usualmente:

- Datos disponibles en entornos online de aula (nombre, apellidos, correo electrónico y/o fotografía), mediante la consulta de un repositorio en -orla- o la ficha de estudiante dependiendo de la configuración de los distintos sistemas de información.
- Procedimientos de autenticación que usualmente consisten en sistemas de clave concertada equivalentes al previsto por el artículo 9.2.c) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

Sin perjuicio de las obligaciones específicas que el artículo 9.3 de la Ley 39/2015, así como la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público (modificadas en este extremo por el Real Decreto Ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones), puedan imponer a las universidades públicas cuando externalicen el servicio, se considera que las causas de legitimación señaladas en el epígrafe anterior resultan de plena aplicación a estos tratamientos.

## 2.2 Legitimación y condiciones de los tratamientos de categorías especiales de datos

Por otra parte, la evaluación podría implicar el tratamiento de al menos dos categorías especiales de datos definidas por el artículo 4 del RGPD:

15) «datos relativos a la salud»: datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud;

En primer lugar, en relación con los datos relativos a la salud (también incluidos en la definición de tratamientos de categorías especiales de datos prevista en el art. 9.1 del RGPD), debe señalarse que las universidades deben adoptar políticas de atención a la diversidad en virtud de lo dispuesto por la Disposición adicional vigésimo cuarta de la LOU, así como por el

artículo 26 del Estatuto del Estudiante y, con carácter general, por lo dispuesto por el artículo 20.c) del Real Decreto Legislativo 1/2013, de 29 de noviembre, por el que se aprueba el Texto Refundido de la Ley General de derechos de las personas con discapacidad y de su inclusión social. Estas normas, además de ser muy precisas en la invocación del llamado principio de accesibilidad universal, ordenan a la institución universitaria adoptar las políticas activas necesarias. Así, citando el tercer apartado de la Disposición adicional vigésimo cuarta de la LOU:

3. Las universidades promoverán acciones para favorecer que todos los miembros de la comunidad universitaria que presenten necesidades especiales o particulares asociadas a la discapacidad dispongan de los medios, apoyos y recursos que aseguren la igualdad real y efectiva de oportunidades en relación con los demás componentes de la comunidad universitaria

Debe señalarse no obstante que usualmente tales datos han sido objeto de tratamiento bien durante el proceso de matrícula, bien en relación con la solicitud de soporte a las unidades de gestión.

Por otra parte, en el contexto de un escenario como el que plantea la pandemia de coronavirus existente cabe considerar la posibilidad de que las y los estudiantes puedan solicitar ya sea algún tipo de adaptación, ya sea algún tipo de beneficio o ayuda, en virtud también del tratamiento de sus datos de salud por darse de dos tipos de situación:

- El padecimiento de la enfermedad.
- Cualquier otra situación sobrevenida, tales como, por ejemplo, la situación familiar en aquellos casos en los que no habiendo contraído la enfermedad personalmente sí lo hayan hecho personas o familiares que convivan en el domicilio afectando a las condiciones de estudio y/o al espacio físico de ubicación personal y a los medios materiales correspondiente.

En tales casos, si bien resulta evidente que una interpretación teleológica de las previsiones de la LOU, e incluso de lo que podría definirse como cláusula de estado social, no es menos cierto, que la comunicación de dichos datos de salud se realiza a instancia de las personas interesadas lo que facilitaría la obtención del consentimiento al que se refiere el artículo 9 del RGPD:

#### Artículo 9

##### Tratamiento de categorías especiales de datos personales

1. Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientaciones sexuales de una persona física.
2. El apartado 1 no será de aplicación cuando concurra una de las circunstancias siguientes:
  - a) el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado;

En la medida en la que el artículo 9 de la LOPDGDD no establece el doble requisito de consentimiento y habilitación legal para el tratamiento de datos de salud, y la solicitud de adaptación por causas de salud sobrevenidas se basaría en la libre voluntad de las personas interesadas, el consentimiento podría resultar un expediente eficaz para legitimar el tratamiento.



En el caso de la biometría, vista:

- La posición adoptada por el Working Party, también conocido como GT29 o Grupo de Trabajo del artículo 29, -hoy Comité Europeo de Protección de Datos o EDPB por sus siglas en inglés-, en sus Directrices sobre el consentimiento y el Dictamen 3/2012 del Working Party sobre la evolución de las tecnologías biométricas.
- El Informe de la Agencia Española de Protección de Datos núm. Informe 0392/2011, anterior a la actual regulación, aplicable desde el 2018, el regulador se refería al tratamiento de los datos necesarios para el reconocimiento de los alumnos de un determinado centro universitario a través de programas de reconocimiento facial para la identificación de los mismos en la realización de las correspondientes pruebas.
- El Informe de la AEPD núm. 0186/2017 sobre grabación de las imágenes de los alumnos durante la realización de los exámenes en el entorno de una Universidad.
- El extenso informe de la AEPD en relación con los tratamientos de datos efectuados en el ámbito universitario (Informe jurídico núm. 2019-0036)
- La sentencia del Tribunal Constitucional número STC 76/2019, que declaró inconstitucional el art. 58.bis).1 de la Ley Orgánica 5/1985, del Régimen Electoral General (LOREG).

El subgrupo de trabajo, integrado por delegados y delegadas de protección de datos de las universidades, ha considerado excluir de estas recomendaciones las técnicas de reconocimiento facial. Debido a su complejidad técnica, y al alto grado de exigencia que la legislación plantea al uso de datos biométricos, no es posible abordar esta cuestión sino desde la técnica de una evaluación de impacto relativa a la protección de datos. Por otra parte, la indefinición de las normas obliga a un proceso de interpretación de las habilitaciones para su uso que hace recomendable:

- Obtener un pronunciamiento expreso de las autoridades de protección de datos con competencia en la materia o definir junto con ellas el modelo de cumplimiento.
- Considerar las condiciones de regulación que ofrezcan una adecuada seguridad jurídica.

### 2.3 Legitimación y condiciones de los tratamientos consistentes en la captación y grabación de imágenes

En los exámenes ordinarios en el mundo físico no existen tratamientos de imágenes puesto que es el profesorado el que:

- Requiere de la exhibición de documentos que adveren y confirmen la identidad de la persona examinada.
- En los exámenes orales se produce una interacción directa.

La completa migración de los exámenes a un entorno online puede plantear tratamientos relacionados con la imagen del profesorado, de las personas examinadas y/o de su entorno inmediato. A saber:

- Grabación de los exámenes orales.
- Visionado del estudiante en tiempo real y de su entorno.

En el mundo académico cada vez se comprueba un mayor grado de sofisticación en la copia en los exámenes y cuyos riesgos se agravan en un entorno online. Así, baste citar, por ejemplo, el uso de auriculares *bluetooth* desde los que recibir instrucciones y contenidos. Pues bien, en un examen realizado online nada impide incrementar las posibilidades de actuación ilícita mediante el uso de buscadores, mensajerías privadas, wearables y cualesquiera otros ingenios tecnológicos.

En este sentido, podría afirmarse que se producen las «determinadas circunstancias» a las que alude el Informe de la AEPD núm. 0186/2017 sobre grabación de las imágenes de los alumnos durante la realización de los exámenes, que ahora podrían justificar dicha grabación.

Por otra parte, debe señalarse que, en las circunstancias actuales de confinamiento, el objeto de la captación por una webcam podría alcanzar no sólo al estudiante sino al espacio de vida privada y familiar tutelado por el artículo 18.1 de la Constitución Española y 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.

Desde el punto de vista del juicio de proporcionalidad resulta evidente que la medida consistente en tener una visión del estudiante, sin usar técnicas biométricas de reconocimiento facial:

1. Es una medida susceptible de conseguir el objetivo propuesto.
2. No existe otra medida más moderada para la consecución de tal propósito con igual eficacia.
3. A nuestro juicio resulta ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto.

Por otro lado, sin perjuicio de que en este caso podría invocarse la facultad del artículo 46.3 de la LOU a la competencia de las universidades para establecer los procedimientos de verificación de los conocimientos de los estudiantes, resulta necesario acudir a la regulación a fin de encontrar fundamentos adicionales.

En primer lugar, Ley Orgánica 1/1982 señala en su artículo segundo:

Artículo segundo

Uno. La protección civil del honor, de la intimidad y de la propia imagen quedará delimitada por las leyes y por los usos sociales atendiendo al ámbito que, por sus propios actos, mantenga cada persona reservado para sí misma o su familia.

Dos. No se apreciará la existencia de intromisión ilegítima en el ámbito protegido cuando estuviere expresamente autorizada por Ley o cuando el titular del derecho hubiere otorgado al efecto su consentimiento expreso (...)

Por otra parte, el artículo 46 de la LOU reconoce a los estudiantes el derecho a:

b) La igualdad de oportunidades y no discriminación por razones de sexo, raza, religión o discapacidad o cualquier otra condición o circunstancia personal o social en el acceso a la universidad, ingreso en los centros, permanencia en la universidad y ejercicio de sus derechos académicos.

(...)

l) La formación en el uso y seguridad de los medios digitales y en la garantía de los derechos fundamentales en Internet.

Asimismo, el Estatuto del Estudiante Universitario, dispone:

Artículo 7. Derechos comunes de los estudiantes universitarios.

1. Los estudiantes universitarios tienen los siguientes derechos comunes, individuales o colectivos:

(...)

g) A ser informado de las normas de la universidad sobre la evaluación y el procedimiento de revisión de calificaciones.

h) A una evaluación objetiva y siempre que sea posible continua, basada en una metodología activa de docencia y aprendizaje.

u) A ser informados y a participar de forma corresponsable en el establecimiento y funcionamiento de las normas de permanencia de la universidad aprobadas por el Consejo Social de la misma.

(...)

A todos aquellos derechos reconocidos en la legislación general, en la normativa propia de las Comunidades Autónomas, así como en los Estatutos y normas propias de las universidades.

Artículo 13. Deberes de los estudiantes universitarios.

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:

(...)

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, el artículo 29.3 de este Estatuto, regula la comunicación de las calificaciones y señala que el profesorado debe conservar material escrito, soporte papel o electrónico o documento correspondiente de las pruebas orales. De este marco normativo podría inferirse la existencia de una legitimación para:

- El control de los estudiantes durante sus pruebas de evaluación online mediante la mera visualización de imágenes mediante la activación de su webcam.
- La grabación de los exámenes orales en la medida en la que, además, esta medida opera como salvaguarda del derecho a la revisión de la calificación que suelen conceder los Estatutos y reglamentos correspondientes de distintas universidades.

No obstante, debemos tener en cuenta también las ya mencionadas obligaciones de información que el citado Estatuto del Estudiante Universitario señala en su artículo 12 para la efectividad de los derechos de los estudiantes. No sólo se debe informar a los mismos tanto del procedimiento de evaluación y del de revisión, sino también facilitarles su ejercicio.

Asimismo, el artículo 25.2 del citado Estatuto señala que los procedimientos de evaluación de los aprendizajes deberán establecerse en los correspondientes planes aprobados por los órganos que proceda, y que su alteración, dispone su apartado 4, no podrá producirse salvo que se dé una imposibilidad sobrevenida, lo que nos situaría en el caso actual. No obstante, esa modificación deberá realizarse según los procedimientos establecidos existentes, consultando tanto a profesorado como a estudiantes.

Así pues, y como la Agencia Española de Protección de Datos señala, tanto el visionado de los estudiantes realizando una prueba de evaluación, como la grabación oral de cualquier de sus pruebas, exigiría ciertas salvaguardas o garantías adicionales:

- Predeterminación normativa, al menos en términos procedimentales, mediante la inclusión de previsiones específicas en las normativas de evaluación y/o realización

de exámenes, así como en las correspondientes guías o programas docentes, aprobada por los órganos competentes.

- Una adecuada transparencia que debería desplegarse en hasta tres ámbitos:
  - La inclusión de referencias expresas a esta circunstancia en los programas o guías docentes y aulas virtuales con suficiente antelación.
  - La notificación expresa a las y los estudiantes de las condiciones de uso de sus webcam. En particular con recomendaciones específicas ordenadas a evitar la captación de imágenes relativas a la vida familiar excluyendo la responsabilidad de la universidad respecto de la captación siquiera incidental de tales imágenes.
  - La notificación expresa a las y los estudiantes de aquellos extremos exigidos por la normativa de protección de datos, tales como la base de legitimación, finalidad, periodo de conservación o responsable ante el que ejercer sus correspondientes derechos en la materia, en el caso de que se graben sus imágenes.
  - La notificación expresa a las y los estudiantes de las consecuencias de grabar las imágenes a las que puedan tener acceso en pruebas de evaluación en las que aparezcan varios estudiantes. Se debe informar sobre la no grabación ni utilización por parte de los mismos de las imágenes a las que pudieran tener acceso en su proceso de evaluación.
  - La información debería realizarse al menos en tres capas:
    - Guía docente.
    - Sistemas de notificación en el aula virtual.
    - Al inicio de la prueba.
- La definición de los roles, obligaciones y responsabilidades del profesorado en esta materia.
- La definición del método de grabación de aquellos exámenes orales que impliquen trasladar al mundo virtual el principio de publicidad mediante presencia de otros estudiantes que se aplica por distintas instituciones universitarias.

Por otra parte, cabe referirse a la eventual captación y grabación de imágenes del profesorado. En los supuestos de grabación resulta necesario señalar el impacto que en la esfera de derechos de este posee la relación laboral o funcional que le une a la institución universitaria.

El Tribunal Constitucional viene reconociendo desde antiguo, -véanse las SSTC 170/1984 y 99/1994-, la existencia de una esfera de vida privada del trabajador que alcanza a su propia imagen. Posteriormente en la STC 98/2000, si bien admite la captación de imágenes considera desproporcionada la de sonidos considerando que

(...) el uso de un sistema que permite la audición continuada e indiscriminada de todo tipo de conversaciones, tanto de los propios trabajadores, como de los clientes del casino, constituye una actuación que rebasa ampliamente las facultades que al empresario otorga el art. 20.3 LET y supone, en definitiva, una intromisión ilegítima en el derecho a la intimidad consagrado en el art. 18.1 CE.

En el caso que nos ocupa, la eventual grabación de la realización de un examen oral por parte de un profesor no opera en absoluto como una medida de control empresarial. Su función es en este caso instrumental al derecho a la educación en la medida en el que permite al profesional una revisión y una evaluación de la persona examinada, y ofrece a esta última los elementos de prueba necesarios ante una eventual impugnación del examen. Asimismo, obedece a la obligación establecida de conservación de las evidencias de las pruebas de evaluación que recoge no sólo el Estatuto del Estudiante Universitario (artículo 29.3), sino recogida en la mayoría de normas de evaluación aprobadas por las universidades.

De nuevo aquí deberán adoptarse las debidas salvaguardas:

- Predeterminación normativa, al menos en términos procedimentales, mediante la inclusión de previsiones específicas en las normativas de evaluación y/o realización de exámenes, así como en las guías o programas docentes.
- Una adecuada transparencia mediante notificación directa al profesorado.
- La definición de los roles y responsabilidades del profesorado en esta materia.
- Principio de limitación de finalidad.
  - En esta materia es fundamental adoptar disposiciones específicas ordenadas a la consecución de la garantía del derecho fundamental a la protección de datos de las y los estudiantes, así como de derechos consustanciales a la realización de las pruebas como la salvaguardia de la autoría y la propiedad intelectual, e incluso el derecho a la propia imagen u honor profesional de las personas examinadas. Ello implica necesariamente asegurar garantías adecuadas ordenadas a asegurar:
    - Que el uso de las grabaciones se limitará estrictamente a los fines propios de la evaluación.
    - Que no se utilizarán las mismas para ninguna otra finalidad no admitiendo usos compatibles sin consentimiento de las personas concernidas.
    - Que no se comunicarán a terceros que no estén implicados en el proceso de evaluación y no tengan competencia, sean responsables o estén facultados para evaluar al estudiante o grupo de estudiantes en cuestión.

## 2.4 La captación de datos por las y los estudiantes o de los propios estudiantes

Algunas de las técnicas de evaluación pueden comportar la captación de datos o imágenes por parte de los estudiantes, ya sean propias o ajenas. En concreto tales circunstancias de acuerdo con la descripción técnica facilitada podrían darse en los siguientes casos.

- |                        |                      |
|------------------------|----------------------|
| 6. Mapas conceptuales. | 9. Observación.      |
| 7. Diario reflexivo.   | 10. Proyectos.       |
| 8. Portafolio.         | 11. Problemas/Casos. |

En este sentido cabe distinguir dos supuestos:

### **1. La inclusión de datos del propio estudiante.**

Algunas de estas pruebas, y particularmente el llamado diario reflexivo, el portafolio y la observación, pueden implicar un tratamiento de datos personales del estudiante que trascienda la mera identificación. No es ocioso recordar, que se trata de evaluar las competencias y capacidades adquiridas.

Ello puede implicar el tratamiento de datos relativos a la propia personalidad de la persona examinada como por ejemplo la capacidad de expresarse. Por otra parte, ya sea por la naturaleza de algunas titulaciones, -como por ejemplo las vinculadas a la psicología, el trabajo o la intervención social o equivalentes, la sociología o la ciencia política-, pueden implicar una alta carga de subjetividad y pueden implicar o provocar el tratamiento de categorías especiales de datos personales en tanto que se pueden manifestar opiniones políticas o relacionadas con creencias religiosas.

Por ello, es indispensable reiterar la necesidad de una aplicación estricta del principio de limitación de finalidad a la que se aludía en la sección anterior y que se reconoce de forma expresa en el artículo 5 del RGPD. Asegurando que:

- Que el uso de los datos, de documentos que contengan expresiones subjetivas o las grabaciones se limitará estrictamente a los fines propios de la evaluación.
- Que no se utilizarán los mismos para ninguna otra finalidad, no admitiendo usos compatibles sin consentimiento de las personas concernidas.
- Que no se comunicarán a terceros que no estén implicados en el proceso de evaluación y no tengan competencia, sean responsables o estén facultados para evaluar al estudiante o grupo de estudiantes en cuestión.

### **2. Elaboración de materiales por los estudiantes.**

Por último, en aquellas técnicas de evaluación que puedan implicar la realización de tareas por los estudiantes que supongan el tratamiento de datos personales, imágenes o sonidos de otras personas, será imprescindible que el tutor de la asignatura incluya en su plan formativo el aprendizaje de las competencias que aseguren que el o la estudiante será capaz de:

- Aplicar criterios de anonimización de los datos.
- Entender, conocer y aplicar los principios éticos de la investigación.
- Obtener cuando proceda los debidos consentimientos informados para:
  - La participación de los sujetos en la investigación.
  - El tratamiento de datos personales.
  - El tratamiento de imágenes y sonidos.
- Conocer sus deberes de secreto, seguridad y confidencialidad.
- Salvaguardar y adoptar las debidas cautelas cuando las personas interesadas pudieran ser menores, personas con diversidad funcional, personas vulnerables o en riesgo, y/o personas incapacitadas.

Todo ello, sin perjuicio de seguir los procedimientos que sean preceptivos en los casos en los que deba someterse al correspondiente Comité de Ética y de la normativa específica para los Trabajos Fin de Grado o Fin de Máster, que deberán tener en cuenta estas circunstancias

## 2.5 Aplicaciones móviles. Servicios no concertados. Bring Your Own device-BYOD

No es ajena a la práctica universitaria el uso de herramientas como aplicaciones móviles con fines de innovación docente. El uso de estas aplicaciones o servicios no concertados plantea problemas relevantes en protección de datos cuando responden a una iniciativa individual del profesorado por distintas razones:

- Generalmente el profesor los utiliza mediante una licencia gratuita a disposición de usuarios finales.
  - Por ejemplo, utilizar herramientas de encuesta no licenciadas como las que ofrecen proveedores como SurveyMonkey cuando la institución ha licenciado por ejemplo servicios muy estandarizados como Lime. O a la inversa.
- Los proveedores excluyen en tales casos su condición de encargados del tratamiento.
- Usualmente esto implica vulnerar las políticas y normativas sobre seguridad de la información de la institución universitaria.
- Muchos servicios, y en particular las aplicaciones móviles se orientan a usuario final lo que implica:
  - Obligar materialmente al estudiante a contratar con una entidad privada para poder superar la evaluación.
  - Obligar al estudiante a una invasión en una esfera muy personal, la de su teléfono móvil, concediendo permisos a terceros que en más ocasiones de las deseables comportan permisos de localización, acceso a micrófono, cámara y almacenamiento, o a la lista de contactos.
  - Obligar al estudiante a soportar la comercialización o monetización de su privacidad.

Por ello, se aconseja evitar estas prácticas por cuanto podrían vulnerar el derecho fundamental a la protección de datos de las y los estudiantes, obligar a un consentimiento forzado en la contratación con terceros, y poner en riesgo la seguridad de la organización. Tal y como se fundamentó en anteriores apartados, la prestación del consentimiento del estudiante a instalarse una aplicación para la realización de una prueba de evaluación a la que no puede negarse sin vulnerar sus derechos educativos, no supone un consentimiento libre y por tanto no sería un consentimiento válido.

En segundo lugar, una de las consecuencias de la virtualización de los exámenes puede consistir en el uso de sus propios dispositivos como herramienta complementaria. No nos referimos aquí, al empleo de dispositivos propios como medios necesarios para la realización de la prueba. Es evidente, que el acceso al aula virtual o al entorno se realiza mediante el uso de los terminales de las y los estudiantes.



Nos referimos al uso por ejemplo del terminal móvil para funciones instrumentales complementarias, como por ejemplo para incluir una segunda cámara de modo que la webcam del ordenador se centre en el estudiante y la del terminal complementario registre la habitación. En nuestra opinión, esta podría ser una práctica de riesgo cuando se exija utilizar recursos estrictamente privados del estudiante como canales de WhatsApp. En consecuencia, en caso de ser necesarias tales prácticas:

- Deberá realizarse con carácter previo una evaluación de riesgos y adoptar medidas que garanticen que en ningún caso el acceso al terminal complementario afecte a la esfera de vida privada del estudiante.
- Únicamente se utilizarán aplicaciones corporativas debidamente licenciadas en los términos del párrafo anterior, que sean totalmente transparente e informen tanto de los usos como finalidades y demás términos obligatorios conforme a la normativa de protección de datos.

## 2.6 El tratamiento de la información ante incidencias en el proceso evaluación.

No podemos olvidar, como ha quedado dicho, que los procedimientos deber realizarse con las correspondientes medidas de seguridad, garantizando un proceso objetivo e igualitario y que los estudiantes están obligados a tener una presencia corresponsable en la Universidad, absteniéndose de utilizar o cooperar en procedimientos fraudulentos en las pruebas de evaluación (art. 13.2.d) Estatuto del Estudiante Universitario).

Ante las incidencias que se produzcan durante la realización de las pruebas de evaluación, se derivarán unas consecuencias que no diferirán de si las incidencias se producen en una prueba fuera del mundo on line. Tal y como disponen la LOU y el Estatuto del Estudiante Universitario, entre los deberes del estudiante está el tener un comportamiento responsable en la universidad, lo que muchas universidades recogen en sus estatutos y en su normativa sobre procedimientos de evaluación, llegando algunas a tener normas o códigos sobre un comportamiento ético en la institución. En este sentido, si se detectara una actuación fraudulenta, se aplicaría la normativa universitaria correspondiente, así como el Decreto de 8 de septiembre de 1954, directamente aplicable y se deberán seguir los procedimientos previstos en la normativa universitaria.

No obstante, las incidencias se pueden producir no sólo por un comportamiento ilícito, sino motivadas por cuestiones técnicas o, también, por cuestiones sobrevenidas no imputables a ninguno de los sujetos que intervienen. Son las universidades las que deben diseñar los mecanismos de garantía de los derechos de los estudiantes y de sus procesos de evaluación o verificación de conocimientos (artículo 46.2 y 3 LOU). En estos casos y como también dispone el Estatuto del Estudiante Universitario, la universidad, conforme a su normativa, les tendrá que habilitar un día y horas diferentes para la realización de la prueba que no hayan podido realizar o si no han podido concurrir por “motivos previstos en sus respectivas normativas” (artículo 25.5).

En relación con los tratamientos de datos que puedan producirse en estas situaciones sólo cambia el escenario. Así las cosas, cosas, la comunicación de la información obtenida o grabada durante una prueba de evaluación en la que se haya detectado un comportamiento ilícito deberá seguir los cauces previstos en la normativa universitaria y ser comunicada única



y exclusivamente a los órganos competentes con la citada finalidad, estando cubiertas por la habilitación legal citada. Asimismo, deberán seguirse las medidas de seguridad que eviten la alteración de las evidencias, así como evitar la comunicación de la información a sujetos que no tengan competencia en el procedimiento sancionador. Las consecuencias serán las previstas en la citada normativa académica, así como en el Decreto de Disciplina Académica, y de ello sería conveniente avisar a los estudiantes. Si bien es cierto que el desconocimiento de la norma no exime de su cumplimiento, el citado Decreto de Disciplina Académica, así como las consecuencias de una conducta fraudulenta son desconocidas entre la gran mayoría del estudiantado, que puede entender que la norma no aplica al entorno on line.

En relación con la posibilidad de realizar las pruebas en otro día y hora, deberá seguirse el procedimiento previsto en la normativa académica, teniendo en cuenta las previsiones relacionadas con los plazos de celebración, así como la accesibilidad para los estudiantes con diversidad funcional. Dada la peculiaridad de uso del entorno on line, con el fin de asegurar la conexión y el soporte técnico, se recomienda tener en cuenta los casos y la disponibilidad técnica para la repetición de la prueba.

En todo este procedimiento de evaluación en un entorno on line debemos tener en cuenta especialmente los casos de personas con diversidad funcional. Tal y como disponen la LOU y el Estatuto del Estudiante Universitario, concretamente en su artículo 26, las citadas pruebas deberán adaptarse a las necesidades de dichas personas, y concretamente se indica que deberán realizarse las correspondientes “adaptaciones metodológicas, temporales y espaciales”. No obstante, dichas adaptaciones tendrán que respetar igualmente los principios generales en materia de protección de datos que se recogen en el presente documento.

Finalmente, debemos señalar que la exigencia de igualdad prevista tanto en la LOU como en el Estatuto del Estudiante Universitario como derechos de los estudiantes, como manifestación de nuestro derecho a la igualdad previsto constitucionalmente en el artículo 14 y como mandato a los poderes públicos en el art. 9.2, removiendo los obstáculos a dicha consecución real, se deben unir con la garantía del derecho fundamental a la educación reconocido en el artículo 27 de nuestra Carta Magna. Todo ello nos obliga a tener en cuenta todos aquellos supuestos de casos de estudiantes que, por circunstancias sobrevenidas durante el confinamiento y con motivo del Covid19, ven en peligro el disfrute de su derecho a la educación en las condiciones en las que lo venían disfrutando y su derecho a ser evaluados de forma objetiva, como establecen las normas. En estos casos, dentro de los procedimientos que las universidades estimen pertinentes para dar cobertura a los mismos (becas o facilitación de equipos o material informático, por ejemplo), se deben extremar las medidas de seguridad, así como la transparencia en la información suministrada a los mismos, garantizando en todo caso su privacidad.

## **2.7 Publicación de notas y tratamiento de datos en los procesos de revisión de las pruebas de evaluación.**

Existen dos tramites consustanciales a un proceso de evaluación. El primero de ellos consiste en la publicación de las notas. A tal efecto, debe destacarse que se prevé la publicación de notas en la reforma operada por la Ley Orgánica 4/2007, de reforma de la LOU:

Disposición adicional vigésima primera. Protección de datos de carácter personal.

1. Lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, será de aplicación al tratamiento y cesión de datos derivados de lo dispuesto en esta Ley Orgánica.

Las universidades deberán adoptar las medidas de índole técnica y organizativa necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, tratamiento o acceso no autorizados.

(...)

3. No será preciso el consentimiento de los estudiantes para la publicación de los resultados de las pruebas relacionadas con la evaluación de sus conocimientos y competencias ni de los actos que resulten necesarios para la adecuada realización y seguimiento de dicha evaluación.

En esta materia, en un reciente Informe la Agencia Española de Protección de Datos ha señalado que:

como señalaba el informe 178/2014, el legislador ha reconocido la existencia de un interés público, por lo que la publicación de las calificaciones universitarias encontraría su base jurídica en lo previsto en el artículo 6.1.e) del RGPD (el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento) derivada de una competencia atribuida por una norma con rango de ley conforme al artículo 8.2 de la LOPDGDD.

Por otro lado, aun no tratándose los procedimientos de evaluación de procedimientos de concurrencia competitiva, las calificaciones obtenidas van a tener incidencia, tal y como se plantea en la consulta, en el otorgamiento de las matrículas de honor limitadas a un número de estudiantes, así como también en la concesión de premios extraordinarios, por lo que también podría apreciarse un interés legítimo de los alumnos del grupo en el conocimiento de las calificaciones de sus compañeros, al amparo de lo previsto en la letra f) del artículo 6.1. del RGPD.

## II

Por lo tanto, siendo lícita la publicación de las notas obtenidas conforme a lo indicado en el apartado anterior, deberá respetarse en todo caso los principios recogidos en el artículo 5 del RGPD, especialmente los de limitación de la finalidad, minimización de datos, limitación del plazo de conservación, integridad y confidencialidad, realizando la publicación de modo que suponga la menor injerencia en los derechos y libertades de los interesados, lo que excluye la posibilidad de un conocimiento generalizado de las calificaciones, como podría ocurrir en el caso de que se procediera a su publicación en internet, en el que el riesgo se incrementaría además como consecuencia de la posible indexación por los motores de búsqueda.

Por ello se considera como medio preferente para proceder a dicha publicación, que la misma se realice en una intranet o aula virtual en la que estuviera limitado el acceso a los profesores y compañeros del grupo. En el caso de que no fuera posible, podrá realizarse en los tablones de anuncios del centro, siempre que no se encuentren en las zonas comunes de los centros, se garantice que el acceso a los mismos queda restringido a dichas personas y se adopten las medidas necesarias para evitar su público conocimiento por quienes carecen de interés en el mismo.

En cuanto a los datos a publicar, atendiendo al principio de minimización, deberán limitarse al nombre y apellidos del alumno y la calificación obtenida. Solo en el caso de que hubiera alumnos con los mismos nombres y apellidos, deberá publicarse para ellos el número del DNI, aplicando lo previsto en el apartado 1 párrafo primero de la disposición adicional séptima de la LOPDGDD. Por lo tanto, solo en el caso de coincidencia del nombre y apellidos, se publicarán cuatro cifras aleatorias de su documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente, recomendándose por esta Agencia que se sigan los criterios contenidos en el documento “Orientación para la aplicación provisional de la disposición adicional séptima de la LOPDGDD”, disponible en [www.aepd.es](http://www.aepd.es).

Y en cuanto al tiempo en el que deberá mantenerse dicha publicación, los datos deberán ser “mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales” (artículo 5.1.e). Por tanto, en el caso de las calificaciones provisionales, tal y como se refiere en la consulta, mientras transcurre

el plazo para presentar reclamaciones, y las calificaciones definitivas durante el tiempo imprescindible que garantice su conocimiento por todos los interesados.

En todo caso, en virtud de la autonomía universitaria reconocida en el artículo 27 de la Constitución Española y en la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades, y ostentando la Universidad consultante la condición de responsable del tratamiento conforme al RGPD, a la misma corresponderá apreciar la necesidad de proceder a la publicación de las calificaciones y la forma en la que deberá realizarse la misma, atendiendo a los criterios señalados en el presente informe y al principio de responsabilidad proactiva en el que se fundamenta la vigente normativa en materia de protección de datos personales.

Asimismo, debemos tener en cuenta lo dispuesto en la LOPDGDD en su Disposición Adicional Séptima sobre la “Identificación de los interesados en las notificaciones por medio de anuncios y publicaciones de actos administrativos” y las Orientaciones de la AEPD sobre la aplicación de dicha Disposición en lo relativo, concretamente, a forma en la que proceder ante la publicación del documento nacional de identidad, pasaporte o número equivalente.

De lo anterior se desprende que:

- No deben publicarse notas en espacios abiertos a los buscadores.
- Se utilizarán los procedimientos de publicación y calificación dispuestos en el aula virtual.
- Los sistemas de publicación de notas asegurarán que únicamente se contenga información relativa a:
  - La asignatura.
  - Nombre y apellidos del estudiante.
  - La calificación.
  - Únicamente en caso de una coincidencia exacta en nombres y apellidos se publicarán cuatro cifras aleatorias de su documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente.
  - La publicación únicamente se mantendrá accesible durante el periodo previsto en la normativa para el proceso de revisión mientras transcurre el plazo para presentar reclamaciones, y en las calificaciones definitivas durante el tiempo imprescindible que garantice su conocimiento por todos los interesados.
  - Se desaconseja la publicación mediante el uso de documentos adjuntados a repositorios en el aula como documentos PDF.
  - Resulta conveniente integrar información dirigida a los estudiantes que les indique la finalidad de la publicación y la prohibición expresa de hacer uso para fines diferentes y en particular proceder a la publicación de la información relativa a las calificaciones de otras personas.

Por último, el segundo de los trámites en todo proceso de evaluación no podemos olvidar que es el tema de las necesarias y obligatorias revisiones de las pruebas de evaluación, a la que tanto la LOU como el Estatuto del Estudiante Universitario reconocen como un derecho de los estudiantes.

En este sentido, nos debemos plantear la forma de llevar a cabo la misma en tanto que el Estatuto del Estudiante Universitario (artículo 30) señala expresamente que “en cualquier

caso, la revisión será personal e individualizada” y que los estudiantes tendrán “acceso a sus propios ejercicios”.

La forma en la que se de acceso será, como dice la propia norma, la prevista en las normas autonómicas y de la propia universidad, siendo el Profesorado responsable de la asignatura el responsable de conservar el material en esta ocasión, en los entornos virtuales habilitados por la propia Universidad.

No obstante, en el caso de las revisiones on line se debe recordar que se utilizarán los medios establecidos por la Universidad y, en ningún caso, lo que desaconsejamos, el uso de medios personales como el correo institucional o personal. Se deberá avisar de este extremo a los estudiantes, más acostumbrados al uso del correo personal que al institucional o al propio de las Aulas virtuales. Por otro lado, deberá garantizarse la conservación de la prueba y de los datos personales asociados a la misma al menos durante el periodo previsto en la correspondiente normativa académica.

Asimismo, debemos recordar por último que de la misma manera que los procedimientos de evaluación debían ser adaptados a las necesidades específicas de los estudiantes con diversidad funcional, de la misma forma las revisiones deberán conllevar las adaptaciones metodológicas, temporales y espaciales necesarias, lo que implicará una coordinación a nivel técnico.

## 2.8 Derechos de supresión y oposición al tratamiento

En los tratamientos de datos personales en un proceso de evaluación tanto las y los estudiantes como el profesorado, son titulares de los derechos que el RGPD y la LOPDGDD les atribuyen. Estas facultades, que integran el contenido esencial del derecho fundamental a la protección de datos son los derechos a ser informados, o transparencia, acceso, rectificación, supresión, oposición, portabilidad, limitación del tratamiento (arts. 12 a 23 RGPD y arts. 11 a 18 LOPDGDD).

Con carácter general, la base de legitimación para el tratamiento invocada en el marco de un proceso de evaluación no es el consentimiento. Por ello, sin desconocer que las personas interesadas siempre podrán invocar sus derechos, no es menos cierto que debe tenerse en cuenta que:

- Por su propia naturaleza la conservación de una prueba de evaluación únicamente admitiría la rectificación en caso como los relativos a la identificación de las personas concernidas.
- Asimismo, resulta materialmente imposible rectificar un registro de audio o video.
- La oposición al tratamiento o la supresión de datos personales relacionados con aquellos extremos que configuren la prueba sujeta a evaluación usualmente resultará denegada prevaleciendo el deber de conservación de la misma.
- No obstante, lo anterior, deberían considerarse los supuestos de oposición al tratamiento cuando deriven de circunstancias relacionadas con la diversidad, funcional, o la violencia de género. Se recomienda por ello, que la información previa a la realización del examen disponga de un cauce formal que permita a la institución universitaria conocer tales supuestos con la debida antelación.

## 2.9 Servicios externos: el contrato de encargado del tratamiento

Como se ha señalado algunos de los canales susceptibles de ser utilizados para la evaluación, y en algunos casos, el alojamiento de canales propios, son objeto de contratación a proveedores externos. Por otra parte, las herramientas antiplagio suelen ser provistas por terceros. A tal efecto resultará de aplicación lo dispuesto en el artículo 28 del RGPD y en particular de su párrafo tercero:

3. El tratamiento por el encargado se regirá por un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros, que vincule al encargado respecto del responsable y establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable. Dicho contrato o acto jurídico estipulará, en particular, que el encargado:

a) tratará los datos personales únicamente siguiendo instrucciones documentadas del responsable, inclusive con respecto a las transferencias de datos personales a un tercer país o una organización internacional, salvo que esté obligado a ello en virtud del Derecho de la Unión o de los Estados miembros que se aplique al encargado; en tal caso, el encargado informará al responsable de esa exigencia legal previa al tratamiento, salvo que tal Derecho lo prohíba por razones importantes de interés público;

b) garantizará que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria;

c) tomará todas las medidas necesarias de conformidad con el artículo 32;

d) respetará las condiciones indicadas en los apartados 2 y 4 para recurrir a otro encargado del tratamiento;

e) asistirá al responsable, teniendo cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que este pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados establecidos en el capítulo III;

f) ayudará al responsable a garantizar el cumplimiento de las obligaciones establecidas en los artículos 32 a 36, teniendo en cuenta la naturaleza del tratamiento y la información a disposición del encargado;

g) a elección del responsable, suprimirá o devolverá todos los datos personales una vez finalice la prestación de los servicios de tratamiento, y suprimirá las copias existentes a menos que se requiera la conservación de los datos personales en virtud del Derecho de la Unión o de los Estados miembros;

h) pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el presente artículo, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable.

En relación con lo dispuesto en la letra h) del párrafo primero, el encargado informará inmediatamente al responsable si, en su opinión, una instrucción infringe el presente Reglamento u otras disposiciones en materia de protección de datos de la Unión o de los Estados miembros.

En esta materia y, habida cuenta de la experiencia, deben plantearse algunas recomendaciones específicas:

- El proveedor de servicios debe haber sido contratado por la universidad. Bajo ningún concepto resulta admisible usar medios distintos de los corporativos tales como:
  - El recurso a canales privados, como espacios en redes sociales, o mensajerías creadas desde el teléfono móvil particular.
  - El uso de sistemas de video particulares.

- El uso de repositorios distintos de los habilitados en la universidad.
- La publicación de encuestas o test en medios no dispuestos por la institución universitaria.
- Es necesario la debida diligencia en la elección del proveedor, que deberá garantizar:
  - Unas medidas de seguridad adecuadas.
  - Garantías de resiliencia, y en particular de disponibilidad.
  - Garantías de portabilidad de la información.
  - El tratamiento de datos en territorios con un nivel de protección equivalente (Espacio Económico Europeo o países con nivel de adecuación reconocido por la Comisión Europea).
  - Garantías adicionales en las herramientas antiplagio respecto de la adecuación al RGPD de las técnicas de analítica de datos empleadas y la legitimidad en el origen de los datos incluidos en la plataforma distintos de los proporcionados por la propia universidad.

## 2.10 Garantía del cumplimiento normativo de la universidad

Los epígrafes anteriores subrayan aquellos elementos cuya relevancia merece de una atención específica. Obviamente, las universidades deberán garantizar un cumplimiento integral considerando las previsiones normativas que a continuación se exponen de modo esquemático.

RGPD Obligaciones Generales	
Obligación	Art.
Deber de probar el cumplimiento del RGPD y en particular del consentimiento	5, 7
Responsabilidad proactiva	5,24
Legitimación o base jurídica del tratamiento	6
Obtención del consentimiento de menores	8
Legitimación para el de categorías especiales de datos	9
Transparencia y derechos a la transparencia y los derechos de acceso, rectificación, supresión, limitación del tratamiento, portabilidad y oposición al tratamiento	12 a 23
Definir roles y responsabilidades en caso de corresponsabilidad en el tratamiento	26
Diseñar el sistema de información conforme a las reglas de protección de datos desde el diseño y por defecto	25
Analizar los riesgos asociados al tratamiento, y en su caso, realizar una evaluación de impacto en la protección de datos	24, 35, 36
Analizar riesgos y diseñar e implementar medidas de seguridad	32 a 34
Implicar al delegado de protección de datos	37 a 39

Definir un proceso de autorización e integrar el tratamiento en el registro de actividades de tratamiento	30
Considerar las prestaciones por terceros, o la universidad como sujeto prestador y formalizar un contrato de encargo del tratamiento	28
Considerar posibles flujos internacionales de datos personales	44 a 50

RGPD Previsiones específicas	
Previsión	Art.
Compatibilidad de la finalidad para el uso con fines de investigación y posibilidad de mantenimiento de los datos más allá de su ciclo de vida para estos fines.	5
Investigación epidemiológica (salud pública) sin consentimiento	9.1.i)
Excepciones al derecho de información o transparencia cuando los datos no se obtuvieron directamente del interesado	14.5.b
Excepciones al derecho de supresión	17.3.d
Derecho de oposición al tratamiento y excepciones	21.6
Legitimación del tratamiento adoptando garantías específicas	89

LOPDGDD Obligaciones generales	
Obligación	Art. LOPDGG
Obtención del consentimiento de las personas interesadas sin necesidad de ley específica	6, 9
Consentimiento de los menores	8
Transparencia (información por capas)	11
Derecho de acceso (remoto)	13
Criterios sobre riesgos a considerar en la evaluación de impacto en la protección de datos	28.2.c/d
Supuestos de corresponsabilidad	29
Registro de las actividades de tratamiento público	31.2
Bloqueo de los datos	32
Encargado del tratamiento	33
Delegado de protección de datos	34.1.b, 36, 37
Transferencias internacionales de datos personales con intervención de la Agencia Española de Protección de Datos	41-43
Medidas de seguridad. Esquema Nacional de Seguridad en el Sector Público.	DA-1



### 3. Protección, disponibilidad, portabilidad y resiliencia

Tanto el delegado de protección de datos, el responsable del tratamiento y el responsable de seguridad de la información deben participar desde el inicio en el proceso de diseño institucional del modelo de evaluación en línea, dado que aplica el principio de seguridad proactiva desde el diseño y por defecto (Artículo 25 del RGPD), con el fin de diseñar y aplicar las medidas técnicas u organizativas apropiadas (Artículo 5.2 del RGPD).

La identificación y diseño de dichas medidas se debe realizar, en el escenario de la evaluación online, mediante el análisis conjunto del proceso de evaluación, el entorno que le va a dar soporte, y los riesgos asociados.

El diseño y uso de un entorno digital conlleva la asunción de ciertos riesgos que se deben identificar, prever y mitigar dentro de lo posible. Todo ello con el fin último de proteger y asegurar la disponibilidad, la portabilidad y la resiliencia del servicio online que se usará.

#### **Protección**

Como principio de actuación se debe "evaluar sin discriminar", bien sea por medios presenciales u online, y para ello se debe proteger y asegurar el entorno digital y a los usuarios.

- La universidad debe garantizar el cumplimiento de la legalidad vigente y la no discriminación de las personas en el proceso de evaluación en línea mediante el uso de entornos digitales, protegiendo los derechos y las libertades de las personas.
- Se debe minimizar el impacto de las decisiones que se tomen sobre los usuarios: el entorno digital debería ser lo más parecido al conjunto de las herramientas habituales en el entorno presencial, añadiendo las mínimas imprescindibles para la comunicación síncrona o asíncrona entre la universidad y el estudiante.
- Todos los usuarios tienen derecho a acceder al entorno digital en las mismas condiciones, independientemente de su condición personal, social, económica o geográfica.
- Se debe garantizar un acceso de calidad atendiendo a la posible brecha digital debido a las competencias digitales de los usuarios.
- Se debe garantizar el acceso en condiciones de igualdad para las personas situadas en entornos rurales, mal comunicadas y con necesidades especiales.
- Se deben prever alternativas en caso de problemas durante la realización de las evaluaciones online.
- Se debe prever la publicidad de los procedimientos y cambios normativos (art 46.2.d LOU); la transparencia en el uso de los entornos digitales y la no exclusión por motivo de vulnerabilidad.
- Se debe mantener la legitimidad del tratamiento de datos y el respeto a los derechos digitales de las personas (Título décimo de la LOPDGDD).
- Es obligación del responsable del tratamiento de datos de la Universidad aplicar medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento de datos personales es conforme con el Reglamento (Artículo 24.1 del RGPD). De tal manera, se garantizará una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y



contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas de «integridad y confidencialidad» (Artículo 5.1.f del RGPD).

- Respecto a la seguridad del entorno online, según la Disposición adicional primera de la LOPDGDD se asigna la obligación de las Administraciones Públicas a cumplir con el Esquema Nacional de Seguridad (ENS). Además, se hace extensible la obligación a terceras partes que den servicio a estas Administraciones Públicas.
  - *El Esquema Nacional de Seguridad incluirá las medidas que deban implantarse en caso de tratamiento de datos personales para evitar su pérdida, alteración o acceso no autorizado, adaptando los criterios de determinación del riesgo en el tratamiento de los datos a lo establecido en el artículo 32 del Reglamento (UE) 2016/679.*
  - *En los casos en los que un tercero preste un servicio en régimen de concesión, encomienda de gestión o contrato, las medidas de seguridad se corresponderá con las de la Administración pública de origen y se ajustarán al Esquema Nacional de Seguridad.*
- En el caso de las universidades privadas, a pesar de no tener la obligación legal recogida en la ley 3/2018 para aplicar este conjunto de medidas, es recomendable adaptar un conjunto de controles similar al citado.

### **Disponibilidad**

La disponibilidad es una de las dimensiones del ENS que son clave en los procesos de evaluación y se deberán garantizar desde el punto de vista del estudiantado, del profesorado y de los servicios de información gestionados por el personal TIC de las universidades.

Desde el punto de vista del estudiantado se deberá garantizar que tiene los recursos técnicos suficientes (equipamiento informático, webcams, conexión a Internet, etc.) para poder participar en el proceso de evaluación, que disponen de las competencias digitales adecuadas para poder participar en la evaluación y que se atiende a las posibles diversidades funcionales que puedan presentarse ofreciendo las adaptaciones necesarias.

Por lo que respecta al profesorado, también será necesario garantizar que dispone de los recursos técnicos y competencias requeridas para realizar el proceso de evaluación, que puede confirmar la identidad del estudiantado y la autoría de las tareas realizadas y que puede acceder a las evidencias necesarias para poder realizar la evaluación

El personal TIC que gestiona los sistemas de información deberá trazar, monitorizar y poder garantizar un uso normal y bien dimensionado de las aplicaciones utilizadas en la evaluación, bien en régimen on-premise o a través de terceras partes. También deberán poder dar soporte al almacenamiento y custodia segura de las evidencias de la evaluación por los periodos legales que se requieran.

### **Portabilidad**

Con independencia de las herramientas utilizadas en el proceso de evaluación, se deberá garantizar la portabilidad de las evidencias entre las diferentes plataformas usadas y los sistemas de información de las universidades.

En caso de no resultar posible la portabilidad de la información del proceso de evaluación se deberá disponer de un acuerdo de servicio con el proveedor de la herramienta que garantice

la durabilidad y accesibilidad a las evidencias durante el período de revisión y guarda legal para poder atender a las posibles reclamaciones de los estudiantes, auditorías por parte de agencias de calidad o por cumplimiento normativo.

### Resiliencia

Los entornos digitales que presten servicio a la evaluación se deberán ofrecer con una capacidad de resiliencia suficiente como para no desvirtuar las pruebas y garantizando la equidad en la valoración del aprendizaje. Para conseguirlo se deberá diseñar el entorno con la redundancia y dimensionado suficientes como para soportar la carga prevista o asumir posibles contingencias temporales derivadas de una planificación sobrevenida o posibles ataques de denegación de servicio, así como contemplar recursos alternativos que permitan ofrecer un “plan B” en caso de necesidad.

Se deberán establecer protocolos de trazabilidad y actuación en el caso de interrupciones del proceso de forma que el personal TIC pueda recuperar el servicio y tanto estudiantado como profesorado sepan cómo actuar en dicha situación.

Durante el período de evaluación es muy importante que tanto el estudiantado como el profesorado tengan contacto directo y sencillo con el personal TIC que puedan resolver cualquier incidencia dentro de los posibles problemas derivados de esta nueva metodología y dentro de los protocolos establecidos de contingencia durante el proceso de evaluación.

### Riesgos

Derivados de la protección, disponibilidad, portabilidad y la resiliencia del servicio online se deben identificar y analizar los riesgos asociados con el fin de que cada universidad diseñe y aplique las medidas técnicas u organizativas apropiadas a su entorno digital concreto. En la siguiente tabla sugerimos algunos de los posibles riesgos existentes.

Aplica el principio de responsabilidad proactiva (Artículo 5.2 del RGPD). El responsable del tratamiento de datos personales será responsable del cumplimiento de lo dispuesto en el Artículo 5.1 del RGPD y deberá ser capaz de demostrarlo.

### Riesgos potenciales desde el punto de vista de los diferentes actores y momentos

	Antes de la evaluación	Durante la evaluación	Tras la evaluación
Estudiantado	<ul style="list-style-type: none"> <li>* No disponer de equipamiento y conexión a Internet adecuados</li> <li>* No disponer de suficientes competencias digitales</li> <li>* Falta de formación en las herramientas de evaluación online, incluyendo la notificación de incidencias durante las pruebas</li> <li>* Desconocer solución alternativa en caso de fallo para dar solución en tiempo</li> </ul>	<ul style="list-style-type: none"> <li>* Problemas de acceso a servicio para la evaluación</li> <li>* Problemas con credenciales de acceso</li> <li>* Desconexión temporal en evaluación síncrona</li> <li>* Pérdida de datos de sesión o aplicación por problemas hardware</li> <li>* Dificultad personal para realizar la prueba síncrona</li> </ul>	<ul style="list-style-type: none"> <li>● Dificultad para Ejercer los derechos sobre la evaluación</li> </ul>

	<p>razonable</p> <ul style="list-style-type: none"> <li>* No disponer de lugar adecuado para la realización de la evaluación</li> <li>* Desconocer la normativa de evaluación actualizada</li> <li>* Incorrecta identificación de necesidades especiales en caso de discapacidad</li> <li>* No usar una página oficial para descarga de software, si se requiere</li> </ul>	<ul style="list-style-type: none"> <li>* Fiabilidad de la verificación de identidad</li> <li>* Uso de material no permitido</li> <li>* Plagio de contenidos</li> <li>* No aceptación de grabación (si hace falta) o de uso de herramientas de terceros si envía datos personales</li> <li>* Grabación de sesión de vídeo por alumnado sin legitimación</li> <li>* Problemas con la notificación de incidencias.</li> </ul>	
<p>Profesorado</p>	<ul style="list-style-type: none"> <li>* No disponer de equipamiento y conexión a Internet adecuados</li> <li>* No disponer de suficientes competencias digitales</li> <li>* Desconocer la normativa de evaluación actualizada</li> <li>* Falta de formación en las herramientas de evaluación online, incluyendo la notificación de incidencias durante las pruebas.</li> <li>* No publicar información detallada sobre el procedimiento para la evaluación</li> <li>* No realizar una correcta adaptación de evaluación en casos de necesidades especiales por diversidad funcional o discapacidad</li> <li>* No dar a conocer una alternativa en caso de fallo para dar una solución en tiempo razonable</li> <li>* No disponer de un protocolo de actuación ante posible detección de fraude</li> <li>* No proteger adecuadamente los equipos</li> </ul>	<ul style="list-style-type: none"> <li>* Problemas de acceso a servicio para la evaluación</li> <li>* Problemas con credenciales de acceso</li> <li>* Desconexión temporal en evaluación síncrona</li> <li>* Problemas con la notificación de incidencias.</li> <li>* No disponer de suficiente personal para la realización de la evaluación y posibles contingencias</li> <li>* Dificultades para verificar la identidad del estudiantado</li> <li>* Indisponibilidad o mal funcionamiento del sistema detector de plagios</li> <li>* Uso de herramientas no autorizadas para realizar la evaluación</li> <li>* Configuración errónea del entorno de evaluación</li> <li>* No registrar las evidencias requeridas para la evaluación</li> <li>* Ejecución errónea de protocolo ante detección de</li> </ul>	<ul style="list-style-type: none"> <li>* Almacenamiento de evidencias de evaluación en entornos no seguros (ordenador personal, móvil, USB sin cifrar, etc.)</li> <li>* Utilización de evidencias de evaluación para fines distintos a los previstos</li> <li>* No proteger adecuadamente los equipos personales/ de trabajo</li> </ul>

	<p>personales/ de trabajo</p> <ul style="list-style-type: none"> <li>* No usar una página oficial para descarga de software, si se requiere</li> </ul>	<p>fraude</p> <ul style="list-style-type: none"> <li>* No proteger adecuadamente los equipos personales/ de trabajo</li> </ul>	
Personal TIC	<ul style="list-style-type: none"> <li>* Desconocimiento de nuevas herramientas</li> <li>* Dificultades de integración con servicios existentes</li> <li>* No disponer de DPA Y SLA en servicios de terceros</li> <li>* Falta de métricas para dimensionar los sistemas</li> <li>* Dificultad para ofrecer entorno requerido de examen/prácticas/labs</li> <li>* Diseño poco seguro por la premura o baja seguridad</li> <li>* No usar cifrado en las comunicaciones</li> <li>* Entorno para examen poco accesible para personas con discapacidad</li> <li>* Falta de procedimiento de gestión de incidencias durante las pruebas.</li> <li>* Falta de definición del registro de actividades de los usuarios.</li> <li>* Falta de personal de soporte durante pruebas</li> <li>* Falta de solución alternativa en caso de fallo para dar solución en tiempo razonable</li> <li>* No identificar la página oficial para descarga de software, si se requiere</li> <li>* No comprobar que la solución está dentro de la declaración de aplicabilidad</li> <li>* Ausencia de análisis de riesgos actualizado al nuevo</li> </ul>	<p>fraude</p> <ul style="list-style-type: none"> <li>* Imposibilidad de ofrecer el dimensionamiento requerido (hardware, licencias software, etc.)</li> <li>* Caídas de servicio propio</li> <li>* Caídas de servicio de terceros</li> <li>* Fallos en servicios de identidad</li> <li>* Caídas en comunicaciones para servicios on-premise</li> <li>* Falta de trazabilidad en acciones de usuario ante posibles reclamaciones</li> <li>* No ofrecer atención al usuario en el examen</li> <li>* Falta de personal de soporte durante el examen</li> <li>* Falta de evidencia de aceptación para grabaciones o uso de herramientas de terceros que envíe datos personales</li> <li>* Falta de protección frente a cortes de energía, incendios o inundaciones on-premise</li> <li>* Falta de protección frente a posibles ataques de denegación de servicio</li> </ul>	<ul style="list-style-type: none"> <li>* No disponer de almacenamiento de evidencias de la evaluación durante periodo de corrección y reclamación</li> <li>* No disponer de almacenamiento de evidencias de la evaluación durante periodo de conservación legal</li> <li>* No disponer de almacenamiento con trazabilidad para el acceso</li> <li>* Falta de copias de seguridad del período mínimo para la revisión legal</li> <li>* No disponer de estrategia de almacenamiento seguro de grandes cantidades de información</li> </ul>

	escenario  * Ausencia de evaluación de impacto y plan de continuidad actualizados al nuevo escenario		
--	--	--	--

## 4.Recomendaciones

### 4.1 Recomendaciones generales

Con carácter general resultaría aconsejable para las universidades:

1. Dotar de seguridad jurídica a los tratamientos vinculados a las nuevas modalidades de evaluación mediante las oportunas reformas normativas en sus reglamentos de evaluación y/o revisión de exámenes, así como en las correspondientes guías o programas docentes.
2. Revisar el impacto en los tratamientos preexistentes de las nuevas condiciones de evaluación adoptando las decisiones pertinentes para:
  - Modificar tratamientos preexistentes.
  - Tramitar, autorizar e incorporar nuevos tratamientos al registro de actividades de tratamiento.
3. Incrementar las condiciones de transparencia. La información por capas debe entenderse en el contexto como información integrada en distintos soportes:
  - Guía docente.
  - Sistemas de notificación en el aula virtual.
  - Al inicio de la prueba.
4. Revisar los contratos preexistentes con proveedores de servicios.
5. Revisar y actualizar las políticas y normativas de seguridad.
6. Diseñar procesos de formación básica del profesorado mediante guías informativas, videos explicativos, y/o formación específica.
7. Diseñar procesos de formación básica del estudiantado mediante guías informativas, vídeos explicativos, y/o formación específica.
8. Tener en cuenta, tal y como establece la normativa, la necesidad de adaptaciones curriculares o de adaptar los procedimientos de evaluación con las correspondientes medidas de seguridad y de información adaptada para los casos de personas con diversidad funcional.
9. Considerar los procedimientos de atención de los derechos de acceso, rectificación, supresión, portabilidad, limitación u oposición al tratamiento habida cuenta de la específica naturaleza de los tratamientos asociados a una evaluación.
10. Ofrecer cauces que permitan identificar situaciones de vulnerabilidad, diversidad funcional o violencia de género que exijan adoptar disposiciones específicas o adaptaciones o estimar el ejercicio del derecho de oposición al tratamiento.
11. El DPD, el responsable del tratamiento y el responsable de seguridad deben participar desde el inicio en el diseño institucional del modelo de evaluación en línea, dado que aplica el principio de seguridad proactiva desde el diseño y por defecto (Artículo 25 del RGPD).
12. Cada universidad debe diseñar y aplicar las medidas técnicas u organizativas apropiadas a su entorno digital concreto a partir del análisis de riesgo de los ítems sugeridos en la tabla de la sección 3, adaptando la política de seguridad de la información y la declaración de aplicabilidad si es el caso.

## 4.2 Recomendaciones específicas

Junto al cumplimiento ordinario de la normativa, el análisis de las distintas metodologías de evaluación sitúa la captación y grabación de imágenes como la práctica que requiere de mayor atención. En este sentido, resultaría recomendable:

1. Proceso de decisión respecto del uso de tales medios.

Resulta imprescindible que exista un análisis documentado de los riesgos vinculados al tratamiento de imágenes del que deriven la adopción de garantías específicas.

2. Transparencia sobre los procesos de uso de técnicas vinculadas a la captación de imágenes por webcams.

En este ámbito la transparencia resulta imprescindible. En este sentido se ha señalado ya con anterioridad la necesidad de informar al menos en tres capas:

- Guía docente.
- Sistemas de notificación en el aula virtual.
- Al inicio de la prueba.

Esta estrategia puede completarse mediante el uso de:

- Envíos de circulares al profesorado y a los estudiantes.
- -Políticas de privacidad en el *website* de la Universidad y/o en el aula virtual.
- Uso de una imagen gráfica en la primera pantalla de las transparencias que eventualmente se empleen.

<p>Examen virtual grabado</p> 		
<p><b>Finalidad:</b> prestación del servicio Público de educación superior (art. 1 LOU)  <b>Responsable:</b> Universidad de _____.  Derechos de acceso, rectificación, supresión, portabilidad, limitación u oposición al tratamiento conforme a políticas de privacidad <a href="http://bit.ly/2vHmcEM">http://bit.ly/2vHmcEM</a>  <b>Propiedad intelectual:</b> uso exclusivo en el entorno de aula virtual. Queda prohibida la difusión, distribución o divulgación de la grabación de las clases y particularmente su compartición en redes sociales o servicios dedicados a compartir apuntes. La infracción de esta prohibición puede generar responsabilidad disciplinaria, administrativa o civil  Fuente de las imágenes: <a href="https://pixabay.com/es">https://pixabay.com/es</a></p>		

Información gráfica para grabación

<p>Examen virtual controlado mediante webcam SIN GRABACIÓN</p> 		
<p><b>Finalidad:</b> prestación del servicio Público de educación superior (art. 1 LOU)  <b>Responsable:</b> Universidad de _____.  Derechos de acceso, rectificación, supresión, portabilidad, limitación u oposición al tratamiento conforme a políticas de privacidad <a href="http://bit.ly/2vHmcEM">http://bit.ly/2vHmcEM</a>  <b>Propiedad intelectual:</b> uso exclusivo en el entorno de aula virtual. Queda prohibida la difusión, distribución o divulgación de la grabación de las clases y particularmente su compartición en redes sociales o servicios dedicados a compartir apuntes. La infracción de esta prohibición puede generar responsabilidad disciplinaria, administrativa o civil  Fuente de las imágenes: <a href="https://pixabay.com/es">https://pixabay.com/es</a></p>		

Información gráfica para control remoto

### 3. Transparencia y medidas de preservación de la vida privada y familiar.

La captación de imágenes durante la realización de un examen virtual puede, siquiera incidentalmente, afectar a la vida privada y familiar. Por ello se recomienda informar a los estudiantes:

- Sobre la naturaleza de la captación de imágenes definiendo de modo preciso el campo de acción de la webcam. En particular en aquellos casos en los que la orientación de la misma implique la obtención de imágenes que abarquen parte de la estancia en la que el estudiante desarrolla la actividad.
- Sobre la necesidad de informar a la familia de tales circunstancias y recomendar su no acceso al entorno durante la realización de la prueba.
- Sobre la prohibición de captar imágenes de terceros, ya sea del profesorado, ya sea de otros compañeros o compañeras durante el proceso de evaluación sin la correspondiente autorización.
- Sobre la exención de responsabilidad de la universidad en caso de no seguirse las recomendaciones.
- Sobre las eventuales consecuencias académicas, si las hubiera de no seguir estas recomendaciones.

### 4. Técnicas de evaluación que implican la captación de datos de otras personas por los estudiantes.

En nuestra opinión, cuando la naturaleza de la prueba implica el uso de metodologías de trabajo que pueden comportar una actividad materialmente investigadora, o que requiera de la interacción y el tratamiento y/o análisis de datos personales de otras personas, los tratamientos serán responsabilidad de la universidad. Es la institución la que define la naturaleza de la prueba, y los medios para su realización. En nuestra opinión, la capacidad del estudiante para, por ejemplo, acotar la temática objeto de un trabajo académico, no le convierte en absoluto en responsable de un tratamiento. A nuestro juicio, en el contexto de un trabajo evaluable el responsable del tratamiento será sin duda la universidad.

En virtud de ello se recomienda al menos, y al margen de las obligaciones relacionadas con las evaluaciones por los Comités de ética de las Universidades:

- Excluir expresamente tareas que impliquen un tratamiento de datos personales.
- En caso de admitir trabajos que impliquen el tratamiento de datos personales, se recomienda:
  - Recomendar el uso de estrategias de anonimización o de seudonimización.
  - Proporcionar a las y los estudiantes y profesores:
    - Formación previa básica en materia de ética y protección de datos.
    - Un procedimiento de declaración de los tratamientos y asistencia en el cumplimiento normativo.
    - Documentos tipo para la obtención de consentimientos informados.
    - Indicaciones específicas en materia de seguridad y secreto.



- Recomendaciones para aquellos tratamientos que impliquen el uso de categorías especiales de datos, datos de menores, personas incapacitadas o vulnerables.
- Espacios de trabajo y repositorios seguros para el almacenamiento de la información objeto de tratamiento.

5.-En relación con la publicación de las notas y los procesos de revisión de examen se recomienda:

- Evitar la publicación de calificaciones provisionales a través de canales no oficiales de comunicación con el estudiantado de la institución para cumplir con las normativas de protección de datos y de reclamaciones. En ese sentido, lo más recomendable sería usar los módulos de gestión de calificaciones de la propia plataforma institucional.
- Definir claramente las condiciones de publicación de las notas en el aula virtual:
  - No deben publicarse notas en espacios abiertos a los buscadores.
  - Se utilizarán los procedimientos de publicación y calificación dispuestos en el aula virtual.
  - Los sistemas de publicación de notas asegurarán que únicamente se contenga información relativa a la asignatura, nombre y apellidos del estudiante y la calificación.
  - Únicamente en caso de una coincidencia exacta en nombres y apellidos se publicarán cuatro cifras aleatorias de su documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente.
  - La publicación únicamente se mantendrá accesible durante el periodo previsto en la normativa para el proceso de revisión mientras transcurre el plazo para presentar reclamaciones, y en las calificaciones definitivas durante el tiempo imprescindible que garantice su conocimiento por todos los interesados.
  - Se desaconseja la publicación mediante el uso de documentos adjuntados a repositorios en el aula como documentos PDF.
  - Resulta conveniente integrar información dirigida a los estudiantes que les indique la finalidad de la publicación y la prohibición expresa de hacer uso para fines diferentes y en particular proceder a la publicación de la información relativa a las calificaciones de otras personas.
- En el caso de las revisiones on line se debe recordar que se utilizarán los medios establecidos por la Universidad. Se desaconseja el uso de medios personales, así como el correo institucional o personal.
- Deberá garantizarse la conservación de la prueba y de los datos personales asociados a la misma, al menos, durante el periodo previsto en la correspondiente normativa académica. Se recomienda la conservación en los espacios virtuales habilitados por las universidades.