REALIZACIÓN DE ACTIVIDADES EDUCATIVAS NO PRESENCIALES EN LOS CENTROS EDUCATIVOS DE LA COMUNIDAD DE MADRID

A partir de la situación excepcional provocada por el confinamiento para evitar el contagio del virus COVID19, se ha extendido entre los centros educativos el uso de medios electrónicos como apoyo en la función de educar y evaluar, de modo que es posible intercambiar contenido audiovisual entre profesores y alumnos, con las precauciones necesarias para hacerlo de manera segura.

El presente documento tiene por finalidad dar respuesta a varias cuestiones frecuentes en el momento presente:

- ¿Tienen los alumnos obligación de conectar su cámara cuando acuden a clase mediante videoconferencia?
- ¿Se puede grabar al alumnado durante la realización de actividades educativas no presenciales, y en especial si éstas van a servir como instrumento de evaluación?
- ¿Se necesita previamente solicitar consentimiento expreso del alumno o de sus tutores legales para conectar la cámara o para grabar la clase o un examen?
- ¿A través de qué plataformas pueden realizarse estas grabaciones?
- Las grabaciones de las pruebas de evaluación, ¿pueden realizarse en el domicilio del alumno?

CONSIDERACIONES GENERALES

La Agencia Española de Protección de Datos (AEPD), en sus "Recomendaciones para proteger los datos personales en situaciones de movilidad y teletrabajo", realiza una serie de recomendaciones dirigidas al personal que participa en las operaciones de tratamiento, y que es aplicable a la actividad docente en los centros educativos:

✓ **Respetar la política de protección de la información en situaciones de movilidad definida por el responsable.**

✓ **Proteger el dispositivo utilizado en movilidad y el acceso al mismo**

- La persona empleada, en nuestro caso el profesional de la enseñanza debe definir y utilizar contraseñas de acceso robustas y diferentes a las utilizadas para acceder a cuentas de correo personales, redes sociales y otro tipo de aplicaciones utilizadas en el ámbito de su vida personal.

- No se debe descargar ni instalar aplicaciones o software que no hayan sido previamente autorizados por la organización.

- Si el equipo utilizado para establecer la conexión remota es personal, debe evitarse simultanear la actividad personal con la profesional y definir perfiles independientes para desarrollar cada tipo de tarea.

- Siempre ha de verificarse la legitimidad de los correos electrónicos recibidos, comprobando que el dominio electrónico del que procede es válido y conocido, y desconfiando de la descarga de ficheros adjuntos con extensiones inusuales o el establecimiento de conexiones a través de enlaces incluidos en el cuerpo del correo que presenten cualquier patrón fuera de lo normal.

✓ **Garantizar la protección de la información que se está manejando**

- Tanto en lugares públicos como en el entorno domésticos es obligado adoptar las precauciones necesarias para garantizar la confidencialidad de la información que se está gestionando.

- Si habitualmente se genera y trabaja con papel, durante situaciones de movilidad es importante minimizar o evitar la entrada y salida de documentación en este soporte y extremar las precauciones para evitar accesos no autorizados por parte de terceros. Es recomendable digitalizar los documentos y guardarlos en la nube corporativa para acceder a ella mediante credenciales. De esta manera, además de proteger la privacidad y confidencialidad, evitamos la diseminación de virus y bacterias.

- La información en soporte papel, incluyendo borradores, no se puede desechar sin garantizar que es adecuadamente destruida. Si es posible, no arrojar papeles enteros o en trozos en papeleras de hoteles, lugares públicos o en la basura doméstica a los que alguien podría acceder y recuperar información de carácter personal.

- Conviene extremar las precauciones para evitar el acceso no autorizado a la información personal, propia y de terceros, manejada, no dejando a la vista ningún soporte de información en el lugar donde se desarrolle el teletrabajo y bloqueando las sesiones de los dispositivos cuando estos estén desatendidos. Es recomendable en el caso de que el dispositivo pueda ser compartido por varias personas que el profesor tenga una clave de acceso a sus carpetas y que cada usuario acceda a las suyas mediante sus credenciales.

- Se debe evitar exponer la pantalla a la mirada de terceros. Si se trabaja habitualmente desde lugares públicos, es recomendable utilizar un filtro de privacidad para la pantalla.

✓ **Guardar la información en los espacios de red habilitados**

- Resulta fundamental para la seguridad de la información en el teletrabajo evitar almacenar la información de forma local en el dispositivo utilizado, siendo necesario para mantener la información de manera estanca en los recursos de almacenamiento compartidos o en la nube proporcionados por la organización.

- Si se permite la utilización de equipos personales, no utilizar bajo ningún concepto aplicaciones no autorizadas en la política de la entidad para compartir información

(servicios en nube de alojamiento de archivos, correos personales, mensajería rápida, etc.)

- ✓ **Si hay sospecha de que la información ha podido verse comprometida comunicar con carácter inmediato la brecha de seguridad**

  - Cualquier anomalía que pueda afectar a la seguridad de la información y a los datos personales tratados debe notificarse al responsable, sin dilación y a la mayor brevedad posible, a través de los canales definidos al efecto.

  - Ante cualquier cuestión que pueda suscitarse en el contexto de las situaciones de movilidad y que puedan representar un riesgo para la protección de la información y el acceso a los recursos corporativos el empleado debe consultar con la Delegación de Protección de Datos y con el responsable de seguridad de la información (en nuestro caso, Madrid Digital o EducaMadrdid), o los perfiles responsables designados al efecto, trasladándoles toda información de interés de la que tenga constancia.

La función educativa, que incluye el uso de toda clase de herramientas, está otorgada por la Ley Orgánica de Educación (LOE), pero como cualquier actividad que implica el tratamiento de información y de datos personales está sometida a la normativa sobre seguridad de la información y sobre protección de datos.

OBLIGACIÓN DE ASISTIR A CLASE, TANTO EN EL AULA FÍSICA COMO EN EL AULA VIRTUAL Y POSIBILIDAD DE GRABAR LA REUNIÓN

- **ASISTENCIA OBLIGATORIA**

Es necesario estar al corriente de que la normativa que se aplica en primer lugar es la sectorial, en nuestro caso la educativa, pero cuando sea necesario el tratamiento de datos personales, se aplicará siguiendo los criterios que establece la legislación sobre protección de datos.

Por ello, es de aplicación la Ley Orgánica 8/1985, de 3 de julio, reguladora del Derecho a la Educación, que establece que las enseñanzas primaria y secundaria son obligatorias. Para las enseñanzas no obligatorias existe la obligación de asistir con regularidad a las clases para no perder el derecho a la evaluación continua. Además, dicha ley señala como deber básico de los alumnos “Asistir a clase con puntualidad”.

El uso de distintas herramientas no cambia la naturaleza de una clase entre profesor y alumnos en la modalidad presencial, donde la asistencia a clase es obligatoria salvo justificación por enfermedad, o el resto de los motivos que están contemplados en el funcionamiento de los centros educativos. Es presencial tanto la asistencia a las aulas físicas como a las aulas virtuales, que además puede ser simultánea.

En las clases presenciales los profesores pasan lista y comprueban quiénes de sus alumnos asisten a ellas. Por lo tanto, al poseer la clase en remoto la misma la naturaleza que la presencial por tener los mismos fines, es obligado que los alumnos asistan en ambos casos y permanezcan conectados durante todo el tiempo que el profesor considere necesario, en

función de criterios educativos, de la madurez del alumno o de la actividad concreta que se esté llevando a cabo ese día en el aula, de modo que el profesor pueda comprobar que se encuentran presentes y que puede interactuar con los alumnos o estos entre sí.

La falta de justificación a una clase en remoto debe tener como resultado las mismas consecuencias, es decir, si un alumno no tiene justificación para faltar a clase, se penaliza anotándolo en el parte de faltas, tanto si la clase es presencial como remota.

DERECHO A LA PRIVACIDAD

Como consecuencia de todo lo expuesto, no se puede invocar el derecho a la privacidad para evitar conectarse a la clase en remoto (la privacidad afecta al grupo formado por el profesor y los alumnos frente a terceros, no entre los alumnos y el profesor entre sí) porque, como hemos señalado, primero se aplican las normas en materia educativa, que obviamente incluye el debido respeto a la normativa sobre protección de datos personales.

En este sentido, para preservar su privacidad cuando los alumnos se conecten, estos deberían utilizar un fondo neutro o situarse de espaldas a una pared de modo que se evite mostrar símbolos o rasgos de su vida personal, íntima o familiar y mostrar, en general, su rostro, pues puede haber asignaturas que requieran mostrar al alumno de cuerpo entero, como en educación física, o de manera que pueda observarse su actividad, como puede ser tocando un instrumento, dibujando, escribiendo o manejando algún objeto.

- **DEBER DE GARANTIZAR LA SEGURIDAD**

Por su parte, el profesor debe asegurarse de que los alumnos se conectan a la sesión mediante una contraseña específica y robusta. De esta forma se puede evitar que puedan acceder intrusos externos y también que puedan conectarse inesperadamente profesores y/o alumnos de otros grupos por error. Igualmente deben nombrarse las sesiones de los grupos de manera inequívoca, utilizando nombres que permitan vincular sin dudas no solo a los alumnos o su grupo, sino también la asignatura, el profesor y el centro. De este modo conseguiremos que puedan conectarse a nuestra sesión extraños con una contraseña y nombre comunes o sencillas.

Es importante también tener en cuenta que cuando se trabaja con usuarios registrados e invitados sin pasar por el aula virtual, debe elegirse la herramienta que permita activar la opción de generación aleatoria de nombres de sesión y proporcionar una contraseña a los destinatarios, por ejemplo, poniéndola en el aula virtual para los alumnos, o en Roble para los padres o, como última opción y de manera excepcional, por el correo electrónico corporativo. Asimismo, para mayor seguridad, debería estar activa la opción que autoriza a entrar en la reunión al invitado que intenta conectarse, para poder comprobar antes su identidad.

- **CONTROL DE LA ACTIVIDAD**

Además, el profesor dirige la sesión en todos los sentidos, silenciará o dará la palabra al alumno que considere, grabará, en su caso, la sesión o las partes que crea necesarias y se asegurará de que la sesión queda cerrada una vez que termine esta, para evitar que algunos alumnos continúen conectados. Debe informarse tanto a los alumnos como sus familias que

no están autorizados para difundir o publicar contenidos de la sesión de clase, porque es un ámbito restringido al profesor y a los alumnos del grupo y que los alumnos mayores de edad o los tutores legales de los alumnos menores serán los únicos responsables del uso inadecuado de las imágenes.

- **GRABACIÓN OPCIONAL DE LAS CLASES**

Ahora bien, las circunstancias son bien distintas cuando ya no hablamos de la asistencia remota sino de la grabación de la clase, ya que esta no conlleva una obligación legal y debemos tener muy presente el principio de proporcionalidad y establecer de antemano los motivos o finalidades que aconsejan grabar una sesión.

Por ejemplo, podríamos grabar una clase para poner exclusivamente los contenidos relevantes a disposición de los alumnos que por algún motivo plenamente justificado no pudieron conectarse en directo o en caso de que la plataforma o los servidores no hayan estado activos durante el tiempo en que habría tenido lugar la sesión o simplemente el profesor los va a incorporar como un material más de trabajo.

Además, el profesor evitará grabar a los alumnos innecesariamente, tanto si hay alumnos en el aula presencial como si asisten en remoto y deben tener conectada su cámara. Los alumnos deben conocer las circunstancias en las que se producirá la grabación y serán informados de ello y de cómo serán tratados sus datos, alojándolos siempre en servidores corporativos y conservándolos durante el tiempo estrictamente necesario.

Para poder demostrar el cumplimiento de los principios sobre protección de datos, si se considera necesario grabar contenidos educativos durante la sesión de clase, se deben determinar por cada departamento las condiciones para ello, además de ser revisadas y aprobadas por el claustro en base a dicho criterio de proporcionalidad cuando se implante esta herramienta de manera general en el centro.

NO SE NECESITA SOLICITAR CONSENTIMIENTO EXPRESO PARA GRABAR LAS CLASES O LAS PRUEBAS DE CONTROL. SÍ SE NECESITA PARA DIFUNDIR O PUBLICAR DICHAS GRABACIONES

Se pueden hacer grabaciones para la actividad educativa y es legal (artículo 6.1.c) y e) del Reglamento General de Protección de Datos) porque es una obligación para la Administración ejercerla, tiene otorgadas todas las competencias necesarias para hacerlo y no precisa para ello el consentimiento. Lo que no se puede hacer sin consentimiento es difundir (aunque sea de manera restringida) o publicar las grabaciones, porque esto constituye otra finalidad no relacionada con la actividad educativa, que podría suponer una infracción de la Ley Orgánica de Protección de Datos e incluso podría llegar a constituir un delito contra la intimidad.

Los centros educativos recibieron a través de las DAT los modelos de consentimiento oficial que están destinados a informar a las familias de las circunstancias en las que se debe o no solicitar el consentimiento y que están disponibles y actualizados en la página web de la Delegación de protección de datos.

Así, en el ejercicio de la actividad educativa no es necesario solicitar el consentimiento. Lo que no podemos dejar de hacer, porque es una obligación impuesta por el Reglamento General de Protección de Datos, es informar a los titulares de los datos personales o a sus representantes legales del uso que se hace de los mismos. Se debe informar antes de poner en marcha el tratamiento, habiendo analizado y mitigado los riesgos para la privacidad y seguridad de los datos.

Si la sesión va a ser grabada por el profesor este debe informar previamente a los alumnos e informarles de que la grabación se guardará de forma segura en el Aula Virtual o en la nube o Cloud del centro educativo, del departamento o del profesor y que será conservada durante el tiempo necesario, como cualquier otro tipo de prueba, pero también aconsejamos que al inicio de las clases en línea o mediante un mensaje personal se dé a conocer a los alumnos y profesores la siguiente información:

> ***Si los alumnos o sus familias desean grabar la sesión docente o de evaluación, deben saber que su destino ha de ser exclusivamente para el uso en el ámbito personal y familiar, siendo los autores y receptores de las grabaciones los únicos responsables de un eventual uso inadecuado de las mismas, como puede ser la publicación de contenido audiovisual sin el consentimiento de personas ajenas que figuren en el mismo. La difusión y publicación de contenido audiovisual sin consentimiento puede ser objeto de una sanción económica por parte de la Agencia Española de Protección de datos, de acuerdo con el Título IX de la LODGDD (artículos 70 a 78).***

PLATAFORMAS AUTORIZADAS PARA REALIZAR ESTAS GRABACIONES

Como todos los centros educativos públicos de la Comunidad de Madrid deberían saber, la Consejería de Educación y Juventud dictó con fecha 11 de marzo unas instrucciones para que los centros pudieran trabajar a distancia y en línea. En el apartado 4 de la Resolución conjunta de las Viceconsejerías de Política Educativa y de Organización Educativa de 10 de marzo, se indica lo siguiente:

> *"Los centros docentes tendrán a su disposición la plataforma EducaMadrid y todas sus herramientas: aulas virtuales, mediateca educativa, comunidades virtuales, EducaMadrid Cloud, así como otras que pueda facilitar la Consejería de Educación y Juventud".*

En el apartado "Recursos" del portal EducaMadrid podemos encontrar las aplicaciones complementarias que la Consejería ha puesto a disposición de los centros para el teletrabajo**, videoconferencias mediante WebEx y Jitsi**, y como complemento **Microsoft Teams** cuyas instrucciones debe seguirse para ponerlas en funcionamiento. En caso de mal funcionamiento o cualquier otra incidencia con EducaMadrid o las demás aplicaciones, los centros deben ponerse en contacto con el Portal CAU de EducaMadrid.

La situación excepcional de salud pública que no permite siempre realizar la prestación educativa con normalidad, aconseja complementar los recursos de la Consejería, responsable de los tratamiento de datos personales, con otros externos, decidiendo sobre la finalidad, los medios y uso de la plataforma y tomando las medidas técnicas y organizativas necesarias para el cumplimiento de la normativa sobre protección de datos.

Elegir otras aplicaciones o plataformas distintas a las establecidas por la Consejería supone que el profesor y el centro educativo asumen responsabilidades que corresponde al responsable del tratamiento de datos personales, concretamente, a la Dirección General de Bilingüismo y Calidad de la Enseñanza, que entre sus competencias ostenta la de elaborar las directrices de uso de las plataformas informáticas de los centros docentes, así como a la Dirección General de Educación Infantil, Primaria y Educación Especial y a la Dirección General de Educación Secundaria, Formación Profesional y Régimen Especial[1], que también son responsables del tratamientos de los datos personales que se tratan en los centros educativos que les atañen y de que estos cumplan con la normativa en materia de protección de datos personales.

La Ley orgánica de protección de datos personales[2] ha modificado la LOE (Disposición adicional vigesimotercera) sobre el tratamiento de los datos que se recogen por los centros educativos, pero no ha modificado las competencias de los centros educativos públicos, que siguen siendo elaborar, aprobar y ejecutar un proyecto educativo y un proyecto de gestión, así como las normas de organización y funcionamiento del centro de acuerdo con los criterios y directrices que establezcan las Administraciones educativas, de modo que entre sus competencias no se encuentra la de establecer finalidades y medios sobre protección de datos, ya que estos forman parte de las políticas educativas, pero no del criterio que cada centro educativo pueda llegar a establecer.

La Disposición Adicional Primera del Decreto de estructura de la Consejería de Educación y Juventud dispone lo siguiente:

> *"Responsables de protección de datos personales.*
>
> ***Los diferentes centros directivos de la consejería son responsables del tratamiento de los datos personales en su respectivo ámbito de actividad y les corresponde la gestión, coordinación y dirección del tratamiento de los datos, así como la determinación de los fines y medios para garantizar el cumplimiento de la normativa en materia de protección de datos.".***

Aunque **el director de un centro educativo** público ejerce sus competencias de acuerdo con la autonomía de gestión que le otorga la Ley Orgánica de Educación, **no es responsable del tratamiento de datos de carácter personal**, dado que el centro público **no es un órgano directivo con capacidad de decisión sobre el tratamiento de datos personales**, sino que forma parte de la estructura orgánica de la Consejería, sigue sus directrices y ejecuta las políticas de seguridad y privacidad que le son encomendadas.

Solo está justificado el uso de plataformas ajenas cuando no se han puesto a disposición de los centros los medios o herramientas adecuados. Si el centro no utiliza las aplicaciones recomendadas, tendrá que contar para el uso de otras externas con la aprobación de la Consejería y la supervisión de la Delegación de protección de datos, que velarán por que los centros no se separen de los criterios sobre privacidad y seguridad de la información.

[1] Decreto 288/2019, de 12 noviembre, del Consejo de Gobierno, por el que se establece la estructura orgánica de la Consejería de Educación y Juventud. Art. 8.1.k), l) y n), Art. 10.1.i), p) y q) y Art. 14.1e) y l)
[2] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

Además, en caso de incidencias de cualquier clase, incluidas brechas de seguridad o vulneración de la política de privacidad, si el centro educativo utilizase herramientas ajenas sin que el responsable tenga conocimiento de ello, **es aquel quien debe responder ante su comunidad educativa y ante el responsable del tratamiento**.

Antes de utilizarlas, se deberá realizar un análisis de riesgos o evaluación de impacto en su caso[3], recabar la validación de su uso por parte de la DG de Bilingüismo y Calidad de la Enseñanza y de la Delegación de Protección de datos, e incluirlas en la PGA después de aprobar su uso, tal como se indica en el modelo de consentimiento oficial que está publicado en la página web de la Delegación de protección de datos.

En este sentido, la AEPD, en sus "Recomendaciones para proteger los datos personales en situaciones de movilidad y teletrabajo", señala la necesidad de realizar un análisis de riesgos en el que **se evalúe la proporcionalidad entre los beneficios a obtener de un acceso a distancia y el impacto potencial de ver comprometido el acceso a la información de carácter personal.**

Por todas estas razones, de la misma manera que no se debe utilizar el correo personal para cuestiones profesionales, tampoco se deben introducir datos de carácter confidencial que pertenecen a nuestra organización en plataformas externas y menos aún sin haber realizado un análisis de riesgos sobre seguridad y privacidad de los datos, aplicando técnicas de anonimización robustas. Esto no significa que no puedan utilizarse otras plataformas, pero utilizar otras nubes implica alojar innecesariamente en servidores ajenos datos de todo tipo, incluidos los de carácter personal o profesional, todos ellos de carácter confidencial, porque pertenecen a la organización para la que trabajamos, es decir, la Comunidad de Madrid y, por ello, es esta quien debe decidir si pueden o no utilizarse ciertas aplicaciones o plataformas, si llega a un acuerdo con el prestador del servicio, así como sobre las categorías y cantidad de datos personales y la forma en que van a ser tratados.

EducaMadrid y otras plataformas o aplicaciones puestas a disposición de los centros educativos ofrecen soporte a los usuarios para cualquier tipo de incidencia, de modo que **solamente en el caso de imposibilidad de utilizar estas herramientas,** podrían optar por otras herramientas, obteniendo previamente, como se ha dicho, el consentimiento **informado** de los profesores, de los alumnos o sus familias.

También se debe evitar introducir en ellas datos de carácter personal, salvo los estrictamente necesarios para el acceso a las mismas**. El centro educativo debe velar por que se utilicen los datos personales objetivos mínimos posibles,** como datos de contacto, profesionales o administrativos, y evitando la incorporación de datos subjetivos, como el razonamiento, las valoraciones o los datos de actuación y conducta. Si se utilizasen formularios deberían poder descargarse en local y una vez resueltos, deberían compartirse a través de las aplicaciones de EducaMadrid. Todo ello, además de para evitar alojar innecesariamente datos personales y confidenciales de los alumnos en plataformas ajenas, para **evitar participar en la formación de la huella digital de los menores, cuyo interés superior debe estar en todo momento por encima de cualquier otro derecho.**

[3] Véase a nueva Guía para gestionar el riesgo de los tratamientos de datos personales y realizar evaluaciones de impacto de la AEPD

Para mayor información sobre el uso de aplicaciones en el teletrabajo esta Delegación tiene publicada en su página web el Informe sobre el uso de plataformas ajenas a las corporativas para el teletrabajo.

Es recomendable asimismo la lectura de los siguientes informes elaborados por el Grupo de Trabajo Intersectorial de CRUE Universidades Españolas[4]:

- "***Informe sobre sobre Procedimientos de Evaluación no Presencial. Estudio del Impacto de su Implantación en las Universidades Españolas y Recomendaciones",***
- ***Informe sobre el impacto normativo de los procedimientos de evaluación online: protección de datos y garantía de los derechos de las y los estudiantes***

De este último informe pueden extraerse las siguientes conclusiones relativas a los **acuerdos o contratos de encargados de tratamiento** realizados por la universidad, que puede entenderse también de aplicación al centro educativo privado o concertado o a la Dirección General competente sobre la elaboración de las directrices de uso de las plataformas informáticas de los centros docentes:

- El proveedor de servicios debe haber sido contratado por la institución. 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

[4] Anteriormente "Conferencia de Rectores de Universidades Españolas", constituida en el año 1994, es una asociación sin ánimo de lucro formada por un total de 76 universidades españolas: 50 públicas y 26 privadas. CRUE Universidades Españolas es el principal interlocutor de las universidades con el gobierno central y desempeña un papel clave en todos los desarrollos normativos que afectan a la educación superior de nuestro país.

los datos incluidos en la plataforma distintos de los proporcionados por la propia universidad.

GRABACIONES AL ALUMNADO EN SU DOMICILIO DURANTE LA REALIZACIÓN DE ACTIVIDADES EDUCATIVAS NO PRESENCIALES QUE VAYAN A SERVIR COMO INSTRUMENTO DE EVALUACIÓN

Para la validez de la prueba de conocimiento, aptitud o examen, debemos tener siempre presente el principio de proporcionalidad. Ello requiere evitar, por ejemplo, establecer la obligación de grabar con el teléfono móvil personal del alumno el entorno doméstico en el que éste se encuentra y comunicar al profesor la grabación, ya que puede resultar una medida desproporcionada para los fines que se pretenden por parte del centro educativo, que deberá diseñar pruebas que permitan valorar los conocimientos del alumno sin invadir o sobreexponer su esfera íntima.

La AEPD se ha pronunciado sobre la legalidad de la grabación de exámenes orales, siempre que las normas internas tengan prevista esta técnica de evaluación, así como sobre la grabación de las sesiones docentes[5].

Pero también ha analizado los aspectos relativos a la privacidad en las pruebas online[6] en un Informe jurídico

> *"… **los centros educativos deberán abstenerse de solicitar al alumno en desarrollo de pruebas de evaluación online o exámenes orales elementos de prueba obtenidos mediante la grabación, en su domicilio, del entorno de su persona, pues ello podría suponer una invasión de su entorno doméstico o de intimidad**.*
>
> *En este sentido, hemos destacado que, para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres siguientes requisitos o condiciones: «si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto).*
>
> *Por consiguiente, cualquier medida de control que se adopte debe superar este juicio de proporcionalidad, determinando si la medida es adecuada, necesaria y equilibrada, ya que en otro caso resulta desproporcionada y por ello contraria a la normativa de protección de datos."*

Sobre el tipo de pruebas o evaluación en línea, las Universidades Públicas de Castilla y León han elaborado una guía de recomendaciones que pueden ser aplicables o adaptadas al

[5] Informe jurídico 2019-0036
[6] Informe jurídico 2020-0036

sistema de evaluación en las enseñanzas no universitarias.[7] En ella se plantea que las herramientas de control biométrico deben ser el último recurso y se apuesta por la aproximación a una evaluación continua que limite el peso de las pruebas finales tradicionales en la docencia presencial.

En este sentido, se plantea el escenario ideal que *"… sería el que sustituye las pruebas finales por un modelo de evaluación continua al 100% en el que se añadirían más actividades de evaluación continua a las que estuviesen previamente definidas, evitando en la medida de lo posible las pruebas finales de evaluación. Si esto no fuera factible, al menos se tendría que minimizar el peso de la prueba final para que esta se considerara como una prueba más de evaluación continua.*

En general cuando se recurra a la realización de exámenes orales o examen de respuesta escrita, ya sean síncronos o asíncronos, se recomienda evitar preguntas que requieran respuestas memorísticas o que se puedan buscar en Internet. Se deberían sustituir por preguntas de reflexión, que evalúen comprensión, discriminación o valoración o que requieran la aplicación de algún tipo de proceso cognitivo, por ejemplo, provocando que deban realizar algún trabajo previo antes de emitir una respuesta".

El RGPD establece en su Artículo 24 la Responsabilidad del responsable del tratamiento: "*1. **Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento**".*

Esto requiere que el centro educativo aplique esas medidas con responsabilidad proactiva, de modo que los datos recogidos sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»[8]) e integrará las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del Reglamento y proteger los derechos de los interesados[9].

Asimismo, tal como señala la AEPD, debe aplicarse el **principio de proporcionalidad**[10], es decir, siempre que resulte posible se deben adoptar otros medios menos intrusivos a la intimidad de las personas con el fin de prevenir interferencias injustificadas en los derechos y libertades fundamentales.

Por otra parte, desde el punto de vista profesional, por cuestiones de seguridad y confidencialidad, además de las de privacidad de los datos, se debe evitar alojar información personal en servidores ajenos a los de la Consejería, pues la información que procede de la actividad educativa pertenece a la Comunidad de Madrid.

Los alumnos también pueden remitir vídeos a los profesores, pero deben evitar, siempre que sea posible, hacerlo a través del correo electrónico. La forma más adecuada es compartirlo en el Aula Virtual o en su nube de EducaMadrid (Cloud) con el profesor o, en el caso excepcional de que no fuese posible, compartir el enlace en su nube privada,

[7] Guía de Recomendaciones para la evaluación online en las Universidades Públicas de Castilla y León
[8] Artículo 5.1.c) del Reglamento General de Protección de Datos (RGPD)
[9] Artículo 25 de RGPD
[10] AEPD Informe jurídico 0186/2017

recomendándoles que los documentos donde aparezcan sus datos personales estén cifrados. Igualmente, el profesor debe compartir la información con ellos por el mismo sistema, nunca en sus dispositivos personales (portátil, ordenador, memoria externa, etc.), porque en caso de pérdida, extravío o acceso no permitido, puede haber una brecha de seguridad que habría que comunicar a la Agencia Española de Protección de datos.

Si el alumno no tuviese otra opción que remitirlo por el correo electrónico, deberá tener asignado un código que irá incluido en el nombre del archivo que remita (por ejemplo, Actividad1_Códigodealumno). Nunca se debe poner el nombre del alumno en el asunto, el cuerpo o el nombre del archivo que se remita y es aconsejable que se utilice el cifrado del documento con una contraseña. En la página web de la Delegación se puede consultar la forma de cifrar documentos.

RECOMENDACIONES GENERALES

La administración educativa debe realizar o actualizar las siguientes tareas:

- Dotar de seguridad jurídica a los tratamientos de datos personales vinculados a las nuevas modalidades para impartir la docencia y para la evaluación mediante las necesarias **reformas normativas en los reglamentos de evaluación y en la programación de las actividades docentes**.
- **Revisar el impacto de los tratamientos** existentes con las nuevas condiciones de trabajo para modificar cuando proceda los tratamientos preexistentes o crear los nuevos que sean necesarios.
- **Incrementar las condiciones de transparencia, incluyendo el deber de informar en todos los soportes que sean necesarios**, como PGA, notificaciones en el Aula virtual o al inicio de las pruebas, envío de circulares a profesores y alumnos, políticas de privacidad en las páginas web de las DAT y de los centros educativos, así como el uso de una imagen gráfica en la primera pantalla de los contenidos audiovisuales o de las pruebas.
- **Suscribir los contratos de encargo del tratamiento de datos personales con nuevos proveedores de servicio y revisar los preexistentes, que deben contener las cláusulas sobre protección de datos**.
- Revisar y actualizar las políticas y normativas de seguridad.
- **Diseñar una formación básica del profesorado** mediante guías informativas, videos explicativos, y/o formación específica **que le permita trabajar con seguridad a lo largo del curso escolar.**
- **Diseñar procesos de formación básica para el alumnado** mediante guías informativas, vídeos explicativos, y/o formación específica que evite conductas inadecuadas que puedan poner en riesgo la privacidad y confidencialidad de los datos.

- Tener en cuenta 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.

- La Delegación de Protección de Datos, 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).

- Especial importancia debe otorgarse a la transparencia y a las medidas de preservación de la vida privada y familiar en relación con la captación de imágenes durante la realización de las vídeo clases o de los exámenes. Por esta razón **se recomienda informar a los alumnos y sus familias**:

    - Sobre la **naturaleza de la grabación de imágenes** definiendo de modo preciso el campo de acción de la webcam. En particular en aquellos casos en los que la orientación de ella implique capturar 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 el respeto por la privacidad del alumno durante la realización de la prueba, evitando interferir en su entorno.

    - 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 finalidad y autorización**.

    - Sobre la **exención de responsabilidad de los centros** educativos**, así como del responsable** del tratamiento en caso de no seguirse las recomendaciones.

    - Sobre las eventuales **consecuencias académicas**, si las hubiera, **de no seguir estas recomendaciones.**

    - Cuando las técnicas de evaluación puedan implicar la captación de datos de otras personas por los alumnos, **los tratamientos serán responsabilidad de la Consejería**. Es la institución la que define la naturaleza de la prueba, y los medios para su realización. La capacidad del estudiante para, por ejemplo, acotar el 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 Consejería o, en su caso, el centro privado o concertado. Por ello, en caso de admitir trabajos de esta clase, deberán establecerse estrategias de anonimización o seudonimización.

DELEGACIÓN DE PROTECCIÓN DE DATOS

2021