

RECOMENDACIONES SOBRE PROTECCIÓN DE DATOS EN LA GRABACIÓN DE CLASES VIRTUALES POR VIDEOCONFERENCIA

La actual situación, derivada de la pandemia por COVID-19 y la prórroga del estado de alarma hasta el 9 de mayo de 2021, ha generalizado nuevos sistemas de docencia no presencial y a distancia así como el uso de herramientas digitales que implican nuevos retos para garantizar la seguridad del tratamiento de la información y dar cumplimiento a la legislación de protección de datos personales.

La grabación de una clase por videoconferencia puede cumplir, entre otras, con las siguientes funciones legítimas:

- Garantizar la accesibilidad a los contenidos por parte de estudiantes que no se hayan podido conectar para que la tengan disponible.
- Ofrecer la posibilidad de su visionado posterior en modelos de formación asíncrona.
- Constituir un material de estudio para la preparación de la evaluación.

1. ¿Qué herramienta o plataforma de docencia virtual debo utilizar para grabar las clases?

Las herramientas y plataformas de docencia virtual realizan un tratamiento de datos personales y, por tanto, deben cumplir con todos los requisitos y garantías legales previstas en la normativa sobre protección de datos de carácter personal.

Deben utilizarse las aplicaciones oficiales con licencia institucional aprobados por la UAM y puestas a disposición de la comunidad universitaria para el desarrollo de las sesiones docentes por cumplir las garantías legales y de seguridad adecuadas. El uso de otras herramientas puede conllevar riesgos de seguridad.

Puedes consultar los recursos disponibles en [Cómo impartir docencia a distancia](#).

El almacenamiento de la grabación se hará preferentemente en la plataforma Moodle con acceso restringido y, en ningún caso, se realizará fuera de los entornos oficiales por los riesgos que conllevan.

Solo se permitirá la reproducción del material grabado, no permitiéndose ni la descarga ni la distribución a terceros de los enlaces.

2. ¿Se pueden grabar las clases virtuales por videoconferencia?

Las grabaciones de imagen, sonido y texto en el entorno de las plataformas de docencia virtual o por videoconferencia constituyen un tratamiento de datos personales, además que

se ven involucrados otros derechos como son el derecho a la propia imagen u honor de las personas participantes además de la salvaguardia de la autoría y propiedad intelectual de los contenidos expuestos.

En lo que afecta a la protección de datos, hay que diferenciar entre:

- ❑ Si la grabación la realiza el profesor en el ejercicio de su función docente y siempre que su acceso se limite a la comunidad universitaria (profesores y alumnos) a los que vaya dirigida, sin que pueda ser utilizada posteriormente para otros fines, estará amparada en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento (art 6.1.e) del RGPD).

Con carácter general, se recomienda emplear la grabación del sistema de la plataforma o aula virtual por defecto y, en la medida de lo posible, la grabación se refiera exclusivamente a la exposición del docente. A fin de respetar al máximo los derechos del alumnado, se deberá:

- Informar previamente que la sesión va a ser grabada y de la finalidad del tratamiento.
 - Se debe advertir que desactiven e inhabiliten la cámara y micrófono de su dispositivo si no desean ser visualizados o grabados.
 - Favorecer las preguntas e interacciones sin activar la cámara preferiblemente a través del chat.
 - Solo se permite la reproducción del material grabado; no permitiéndose ni la descarga ni la distribución a terceros de los enlaces.
-
- ❑ Si un alumno o alumna quisiera grabar la clase por sus propios medios deberá contar con el consentimiento expreso de todos los asistentes, tanto del docente como del resto de los alumnos, si su imagen o su voz pudieran ser objeto de grabación y ser identificadas (art 6.1.a) del RGPD).

3. ¿De qué hay que informar cuando se graben las clases por videoconferencia?

Cuando se vaya a llevar a cabo la grabación de la sesión docente, con carácter previo al inicio de la clase y siempre antes de grabar, se deberá informar de la finalidad concreta de dicha grabación y del uso que se le va a dar de manera que el alumnado que no quiera ser grabado pueda desactivar o inhabilitar su cámara/micrófono.

También debe advertirse al alumnado que debe preparar o acondicionar adecuadamente su espacio de interacción, de manera que se proteja la intimidad familiar y la de terceros, evitando la captación incidental de imágenes no deseadas por la Universidad o posibles interrupciones molestas.

En su caso, se debe avisar al alumnado que queda terminantemente prohibido la captación y/o grabación de la sesión, así como su reproducción o difusión, en todo o en parte, sea cual sea el medio o dispositivo utilizado.

De acuerdo con los principios de transparencia e información, se recomienda al inicio de la sesión leer la siguiente cláusula informativa para que aquellas personas que no quieran ser grabadas puedan apagar su webcam:

Cláusula informativa

«Esta sesión será objeto de grabación con la finalidad de garantizar la accesibilidad de sus contenidos a todos los estudiantes de acuerdo con la prestación del servicio de educación superior (art. 1 LOU).

Los alumnos deben adoptar las medidas adecuadas para garantizar las condiciones de privacidad en las que se ha de desarrollar la videoconferencia para proteger su privacidad e intimidad familiar, advirtiéndose que la UAM no es responsable por la captación o grabación de imágenes que afecten a la esfera de vida privada y familiar.

Se recomienda a los asistentes que desactiven e inhabiliten la cámara y micrófono de su dispositivo si no desean ser grabados o visualizados por el resto de los participantes.

Queda prohibida la captación y/o grabación de la sesión, así como su reproducción o difusión, en todo o en parte, sea cual sea el medio o dispositivo utilizado. Cualquier actuación indebida comportará una vulneración de la normativa vigente, pudiendo derivarse las pertinentes responsabilidades legales.

Recordamos que en la Web de la Universidad Autónoma de Madrid puede encontrar las [políticas de privacidad](#), pudiendo ejercer los derechos de acceso, rectificación, supresión, portabilidad, limitación u oposición al tratamiento ante nuestra delegada de protección de datos delegada.protecciondedatos@uam.es”

4. ¿Se puede ejercer el derecho de limitación u oposición a ser grabado en el desarrollo de una clase virtual?

Aunque la grabación de la clase por videoconferencia está amparada en la función educativa de la Universidad y tiene como finalidad garantizar la accesibilidad a los contenidos docentes por parte de estudiantes que no se hayan podido conectar para que la tengan disponible, la participación e intervención tanto del profesorado como del alumnado debe basarse en el consentimiento libre y voluntario tanto por razones de propiedad intelectual como por derechos de imagen de modo que quien no quiera ser grabado debe poder desactivar o inhabilitar su cámara/micrófono.

No obstante, se podrá ejercer el derecho de acceso, rectificación, limitación u oposición al tratamiento cuando exista una justificación adecuada por parte del interesado que deba prevalecer sobre los intereses de la institución a tratar sus datos personales.

La solicitud se resolverá por la [Delegada de Protección de Datos](#) de la Universidad según el procedimiento establecido al efecto.

5. ¿Se pueden difundir/publicar las clases grabadas?

La difusión, distribución o divulgación de la grabación de las clases por parte del estudiantado y, particularmente, su compartición en redes sociales atenta contra el derecho fundamental a la protección de datos, el derecho a la propia imagen y los derechos de propiedad intelectual.

Tales usos se consideran prohibidos y podrían generar responsabilidad disciplinaria, administrativa, civil o penal a la persona infractora si se realiza sin la autorización por parte del profesor y el consentimiento expreso de las personas afectadas.

El profesorado puede reutilizar el material generado para otros fines académicos, como puede ser su publicación en un blog, webinar o MOOC, únicamente cuando se grabe su intervención o presentación, no la de estudiantes o terceras personas. En el supuesto de que el alumnado pudiera ser objeto de grabación y su imagen o voz ser identificadas, se requerirá el consentimiento previo y expreso de todos los intervinientes afectados para su publicación o divulgación,

6. ¿Qué se considera por difusión ilegítima de imágenes o videos y qué se puede hacer?

La imagen es un dato personal y, por tanto, la captación, reproducción y difusión de fotografías y vídeos en los que aparecen terceros a través de dispositivos móviles en redes sociales (por ejemplo, Facebook, Youtube, Instagram o Twitter), mediante servicios de mensajería instantánea (por ejemplo, Whatsapp o Telegram) o por correo electrónico debe hacerse de manera lícita y con el previo consentimiento o autorización de las personas afectadas en aras de proteger los datos personales y el derecho al honor, a la intimidad personal y a la propia imagen.

El primer paso para eliminar los videos o imágenes es hacer uso de los mecanismos y formularios que los buscadores, foros, blogs y redes sociales ofrecen para comunicarles la vulneración de la privacidad o la publicación de contenidos inapropiados. Será necesario que se identifique el perfil social a través del que se están difundiendo las imágenes o videos no consentidos así como el enlace o dirección web.

Asimismo, también puedes dirigirte a la [Delegada de Protección de Datos](#) de la UAM o a la [Agencia Española de Protección de Datos](#) poniendo en su conocimiento esta situación.

7. ¿En qué responsabilidades puede incurrir quien difunda ilegítimamente imágenes o vídeos de terceras personas sin consentimiento?

Quien difunda ilegítimamente imágenes o vídeos de terceros puede incurrir en distintos tipos de responsabilidades:

- **Responsabilidad en materia de protección de datos:** la difusión de datos de una persona física (en contenidos tales como imágenes, audios o vídeos que permitan identificarla), publicados en diferentes servicios de internet sin consentimiento se considera una infracción de la normativa de protección de datos personales. La Agencia Española de Protección de Datos (AEPD) es competente para sancionar estas conductas con multas.

- **Responsabilidad disciplinaria:** Si la difusión de las imágenes o vídeos la lleva a cabo el alumnado se le aplicará el Reglamento de disciplina académica pudiéndose aplicar, en los

casos más graves, la sanción de expulsión temporal o permanente del Centro. Si la realiza un funcionario público o personal laboral se le aplicará el régimen disciplinario previsto en el Estatuto Básico del Empleado Público.

- **Responsabilidad penal:** la difusión y la cesión a terceros de imágenes o vídeos sin consentimiento, que menoscaben la intimidad de una persona física, son constitutivas de un delito contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio en los términos establecidos en el art 197 y siguientes del Código Penal.

- **Responsabilidad civil o patrimonial:** se deberá responder por los daños y perjuicios causados a la persona afectada, tanto los de carácter patrimonial como los de carácter moral.

Más información: Documentos de la CRUE

- [Guía sobre la protección de datos personales en el ámbito universitario en tiempos del COVID-19](#)