



## **Criterios de seguridad TIC y protección de datos personales en clase y/o evaluación en remoto**

**Versión 14/04/2020**

### **1. Objeto**

Este documento establece los criterios de seguridad TIC y protección de datos personales en la realización de clases y/o evaluaciones mediante herramientas de trabajo en remoto, para garantizar el derecho a la protección a los datos personales en estas actuaciones y circunstancias excepcionales, como consecuencia del estado de alarma.

### **2. Ámbito y marco legal**

El ámbito de estos criterios es el de la realización, mediante herramientas informáticas y de telecomunicaciones, de sesiones virtuales de clases docentes y/o de sesiones virtuales de evaluación del estudiantado de la UPC en el marco único del estado de alarma decretado el 14 de marzo de 2020.

Estos criterios son un acompañamiento al acuerdo de “Medidas urgentes y extraordinarias para garantizar la impartición de docencia a los estudios de la UPC durante la emergencia sanitaria” de la UPC aprobado por el Consejo de Gobierno en fecha 1 de abril de 2020 (Acuerdo CG/2020/02/05).

La Ley Orgánica 4/1981, del 1 de junio, de los estados de alarma, excepción y asedio, permite adoptar medidas con las limitaciones señaladas en su artículo 11, sin que, en ningún caso, se permita la suspensión de derechos y libertades.

La protección de datos es un derecho fundamental, catalogado por el Tribunal Constitucional, como un derecho esencial autónomo, y a la vez independiente del derecho a la intimidad personal y familiar (STC 292/2000, de 30 de noviembre). Este derecho se ha de garantizar incluso en el actual estado de alarma ocasionado por el Covid-19. En esta línea, el Real Decreto 463/2020, de 14 de marzo, de declaración del estado de alarma, no suspende el derecho a la protección de datos, como tampoco lo hace ninguna norma dictada con posterioridad. Con la finalidad de salvaguardar este derecho fundamental, durante el estado de alarma y sus respectivas prórrogas, será de aplicación íntegra la Ley Orgánica 3/2018, de 5 de diciembre, y el Reglamento General de Protección de Datos, al igual que la Ley Orgánica 1/1982, de Protección Civil del Derecho al Honor, a la intimidad personal y familiar y a la propia imagen.

Así lo ha advertido el gabinete jurídico de la Agencia Española de Protección de Datos en el informe 0017/2020 : “*Los tratamientos de datos personales en estas situaciones de emergencia sanitaria, siguen siendo tratadas de conformidad con la normativa de*



*protección de datos personales (RGPD i Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, LOPDGDD), de manera que se aplican todos sus principios, contenidos en el artículo 5 RGPD, y entre ellos el de tratamiento de los datos personales con licitud, lealtad i transparencia, de limitación de la finalidad (en este caso, salvaguardar los intereses vitales / esenciales de las personas físicas), principio de exactitud, y por descontado, y hay que hacer especial hincapié en esto, el principio de minimización de datos. Sobre este último aspecto hay que hacer referencia expresa al hecho de que los datos tratados deberán de ser exclusivamente limitados a las necesarias para la finalidad pretendida, sin que se pueda extender este tratamiento a cualesquiera otros datos personales no estrictamente necesarios para este fin, sin que pueda confundir conveniencia con necesidad, porque el derecho fundamental a la protección de datos se siga aplicando con normalidad".*

En esta coyuntura y, con el objeto de respetar los derechos de todos los miembros de la Comunidad Universitaria, la Universidad, en ejercicio del derecho a su autonomía, se reorganiza y se dota de las herramientas y de los sistemas que tiene al abasto para proseguir con la actividad docente. Para alcanzar este objetivo, todos los miembros de la Comunidad están obligados a colaborar activamente en las acciones que se emprendan. Desde el punto de vista de la realización de clases y pruebas en remoto, la cooperación de los estudiantes se hace indispensable, como también ofrecerles los medios necesarios para poder participar, si no disponen de los elementos técnicos adecuados.

En cuanto a la implicación de los derechos y deberes de los estudiantes universitarios que sean susceptibles de ser trasladados al contexto actual se ha de mencionar el Real Decreto 1791/2010, de 30 de diciembre, por el cual se aprueba el Estatuto del estudiante Universitario. En su artículo 13 se regulan las obligaciones del estudiantado, entre las cuales se encuentra la obligación de cooperación en las actividades propias de la universidad la participación responsable o la contribución a la mejora del funcionamiento de la universidad. Siguiendo esta norma, a través del Acuerdo núm.106/2011 del Consejo de Gobierno se aprobó el Código ético y de buenas prácticas del personal al servicio de la Universitat Politècnica de Catalunya y de su estudiantado, donde se prevé expresamente que los principios que deben regir la actividad universitaria, en cuanto a su personal y al estudiantado, son los de la cooperación, corresponsabilidad, honestidad e integridad, entre mucho otros. El artículo 3.4 de este texto, relativo al estudiantado, establece lo siguiente:

*"El estudiantado mantendrá una actitud participativa en todas las actividades formativas, ha de facilitar la tarea del profesorado y ha de evaluar las actividades de este cuando se le pide. También pondrá en valor su esfuerzo personal en todas las pruebas y actos de evaluación y promoverá esta actitud entre los compañeros de estudio. Por otra parte, procurará participar en los órganos de representación y de gobierno de la Universidad que le corresponda"*

Así, las pautas que se encuentran en el presente documento deberán interpretarse siempre teniendo en cuenta el deber de colaboración de todos los implicados con facilitar la actividad formativa y de evaluación de la Universidad.



### 3. Garantías de seguridad TIC y Protección de Datos Personales

Las medidas que adopten los centros docentes como resultado de la implementación de las indicaciones de la dirección, y bajo el amparo de los criterios generales establecidos por el Vicerrectorado de Política Académica, deben cumplir el máximo posible con las medidas técnicas y organizativas que garanticen la seguridad de la información, la protección de datos personales y su trazabilidad.

Las garantías de seguridad TIC son las indicadas para las administraciones públicas en el Real Decreto 3/2010 y 951/2015 que regula el Esquema Nacional de Seguridad:

**CONFIDENCIALIDAD:** Hay que considerar las consecuencias que tendría su revelación a personas no autorizadas o que no necesitan conocer la información.

**INTEGRIDAD:** Hay que considerar las consecuencias que tendría su modificación por alguien que no está autorizado a modificar la información.

**AUTENTICIDAD:** Hay que considerar las consecuencias que tendría el hecho de que la información no fuera auténtica.

**TRAZABILIDAD:** Hay que considerar las consecuencias que tendría el no poder comprobar a posteriori quien ha accedido a, o modificado, una cierta información.

Las garantías de protección de datos personales son las indicadas por el Reglamento General de Protección de Datos (UE) 2016/679:

Los principios de la protección de datos se aplican a toda la información relativa a una persona física identificada o identificable.

**LICITUD, LEALTAD Y TRANSPARENCIA:** Los datos personales deben ser tratados de manera lícita. Los principios de tratamiento leal y transparente exigen que se informe al interesado que hay la operación de tratamiento y de qué fines tiene. Si los datos personales se obtienen de los interesados, también se les informará de si están obligados a facilitarlos y de las consecuencias de no hacerlo.

**LIMITACIÓN DE LA FINALIDAD:** Los datos personales deben ser recogidos con fines determinados, explícitos y legítimos y posteriormente no se deben tratar de manera incompatible con estos fines.

**MINIMIZACIÓN DE DATOS:** Los datos personales deben ser adecuados, pertinentes y limitados a lo que es necesario en relación con las finalidades para las que se tratan.

**EXACTITUD:** Los datos personales deben ser exactos y, si es necesario, se actualizarán; hay que adoptar las medidas razonables para que se supriman o se rectifiquen sin dilación los datos personales que sean inexactos con las finalidades para las que se tratan.

**LIMITACIÓN DEL PLAZO DE CONSERVACIÓN:** Los datos personales deben ser conservadas de manera que permitan identificar los interesados durante un período no superior al necesario para los fines del tratamiento de datos personales.



**INTEGRIDAD Y CONFIDENCIALIDAD:** Los datos personales deben ser tratadas de forma que se garantice una seguridad adecuada, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de las medidas técnicas u organizativas adecuadas.

#### **4. Información y datos personales en una clase mediante herramientas de trabajo en remoto**

La información mínima que se podría tratar en una clase mediante herramientas de trabajo en remoto, y que es objeto de este informe en cuanto a los criterios de seguridad TIC y protección de datos personales, sería:

- Convocatoria de la sesión docente
- Registro de acceso a la clase de cada estudiante (recomendación)
- Imagen y voz del profesor
- Entorno de trabajo del profesor
- Identificador del profesor a la herramienta informática
- Contenido docente de la materia a explicar
- Imagen y voz de los estudiantes
- Entorno de trabajo de los estudiantes
- Identificador de los estudiantes a la herramienta informática
- Preguntas o comentarios de los estudiantes
- Grabación, en su caso, de la sesión docente (sin la intervención de los estudiantes)
- Grabación, en su caso, de la sesión docente íntegra (con la intervención de los estudiantes)

#### **5. Información y datos personales en una evaluación mediante herramientas de trabajo en remoto**

La información mínima que se podría tratar en una evaluación mediante herramientas de trabajo en remoto, y que es objeto de este informe en cuanto a los criterios de seguridad TIC y protección de datos personales, sería:

- Convocatoria de la sesión de evaluación
- Registro de acceso a la sesión de evaluación de cada estudiante
- Imagen y voz del profesor
- Entorno de trabajo del profesor
- Identificador del profesor en la herramienta informática
- Enunciado del examen de la materia a evaluar
- Imagen y voz de los estudiantes
- Entorno de trabajo de los estudiantes
- Identificador de los estudiantes a la herramienta informática
- Preguntas o comentarios de los estudiantes
- Resoluciones de los exámenes de los estudiantes
- Grabación, en su caso, de la sesión de evaluación (con la intervención de los estudiantes)
- Sistema de envío de la prueba realizada por el estudiante



## 6. Análisis de riesgos

Las herramientas que actualmente ha puesto a disposición de la comunidad la UPC, ya han estado evaluadas desde el punto de vista de riesgos de seguridad TIC y protección de datos.

En el caso de que se utilicen herramientas diferentes de las puestas a disposición por la UPC, haría falta que se hiciera un análisis de riesgos de forma previa a su puesta en funcionamiento, para poder garantizar la seguridad TIC y la protección de datos personales, como se indica a continuación. Esto lo tendrá que hacer quien haya decidido utilizar la herramienta en concreto, a ser posible con la implicación del centro docente.

Este análisis de riesgos nos tiene que permitir evaluar las garantías establecidas en el apartado 3 de este documento, y establecer las medidas técnicas y organizativas necesarias para mitigar los riesgos.

### Riesgos asociados a la **CONFIDENCIALIDAD**:

Es necesario evaluar si la herramienta que se use permite que los datos descritos en los apartados 4 y 5 de este documento no sean revelados a terceras personas no autorizadas o que no necesiten conocer la información.

Del conjunto de información y datos personales, habrá que garantizar que la herramienta que se use, acote al máximo el acceso a la sesión para que solo las personas que tienen que estar presentes puedan acceder.

Además, si la clase es grabada con las intervenciones de los estudiantes, esa grabación solo puede ser accesible para los participantes y utilizar las medidas técnicas que sean necesarias para evitar que el video pueda ser descargado.

En cuanto a las resoluciones del examen de los estudiantes, la herramienta y/o las medidas técnicas y organizativas usadas tienen que garantizar la confidencialidad tal y como se hace con los exámenes presenciales.

### Riesgos asociados a la **INTEGRIDAD**:

De la información y datos personales de las clases y de las evaluaciones, hay que considerar sobretodo la integridad de las convocatorias de las sesiones en remoto, de la grabación de las sesiones, y de las resoluciones de los exámenes de los estudiantes, considerando las consecuencias que tendría su modificación por alguien que no está autorizado a actualizar la información. Se han de evaluar también los riesgos de pérdida, destrucción o daño accidental, mediante la aplicación de las medidas técnicas u organizativas adecuadas.

### Riesgos asociados a la **AUTENTICIDAD**:

En cuanto a la autenticidad, lo que hay que analizar es que la identidad de las personas participantes sea auténtica, y que la resolución de los exámenes de los estudiantes haya sido creada por su autor, y considerar las consecuencias que tendría el hecho de que la información no fuera auténtica.



Para minimizar los riesgos asociados a la autenticidad se tendrán que usar las credenciales de acceso a los sistemas de información de la UPC (nombre de usuario UPC más contraseña, correo electrónico institucional, identificador de G Suite).

#### Riesgos asociados a la **TRAZABILIDAD**:

La herramienta que se use para las clases y/o evaluaciones tiene que permitir guardar un registro de cuando se ha producido, quien ha participado, desde qué equipo se ha puesto a disposición de los participantes, y en el caso de las grabaciones habrá que conocer quien ha accedido y/o la ha modificado, para poder establecer las consecuencias que tendría el no poder rastrear a posteriori el uso que se haya hecho de esa información y datos personales.

#### Riesgos asociados a la **LICITUD, LEALTAD Y TRANSPARENCIA**:

El tratamiento de los datos personales descritos anteriormente para las clases y evaluaciones, es lo que está definiendo al Registro de Actividades de Tratamiento de la UPC como a [F03.21 Gestión y uso del campus virtual](#)

Los datos personales descritos en los apartados 4 y 5 de este documento ya están incluidos en el Registro de Actividades del Tratamiento y, por tanto, los riesgos asociados a la licitud, lealtad y transparencia son que la herramienta que se use para las clases o evaluaciones, así como las medidas técnicas y organizativas que se usen, incluyan otros tipos de datos personales, o que no se informe al interesado que hay la operación de tratamiento y de que finalidades tiene, y también hay el riesgo que no se les informe de si están obligados a facilitarlos y de las consecuencias de no hacerlo.

#### Riesgos asociados a la **LIMITACIÓN DE LA FINALIDAD**:

El principal riesgo asociado a la limitación de la finalidad es que la herramienta que se use para las clases o evaluaciones, así como las medidas técnicas y organizativas que se usen, permitiendo hacer un tratamiento incompatible con la finalidad establecida en el tratamiento de dar soporte a la enseñanza y al aprendizaje de las asignaturas:

- Comunicación entre el estudiantado y el profesorado, y entre el propio estudiantado.
- Realización de actividades y acceso a los recursos propuestos por el profesorado.
- Evaluación por parte del profesorado.

A título de ejemplo, el hecho de que la grabación de la sesión de clase con intervenciones de los estudiantes NO esté restringida a los estudiantes de la asignatura del curso concreto constituiría una vulneración del principio de la limitación de la finalidad.

#### Riesgos asociados a la **MINIMIZACIÓN DE DATOS**:

El principal riesgo asociado a la minimización de datos personales es que la herramienta que se use para las clases o evaluaciones, así como las medidas técnicas y organizativas, traten más datos personales de los que hacen falta.



Hay que determinar si a la sesión de clase han de salir las imágenes y voces de los estudiantes. Hay que preguntarse por la necesidad de que la participación tenga que ser tan visual y sonora. Nos tenemos que preguntar si podemos obtener el mismo resultado docente haciendo la sesión donde solo salga la imagen y voz del profesor, la presentación, y que los estudiantes participen con micrófono y cámara apagados, y que solo participen desde el chat.

Riesgos asociados a la **EXACTITUD**:

El principal riesgo asociado a la exactitud de datos personales es que la herramienta que se use para las clases o evaluaciones, así como las medidas técnicas y organizativas, permita que los datos personales tratados no sean los datos de los estudiantes que están matriculados a una asignatura en concreto.

Riesgos asociados a la **LIMITACIÓN DEL PLAZO DE CONSERVACIÓN**:

El riesgo asociado a la limitación del plazo de conservación es que las grabaciones de las sesiones de clases y/o de las evaluaciones se guarden más allá del tiempo necesario para las finalidades del tratamiento de datos personales.

## 7. Legitimación del tratamiento de datos personales

Si se siguen los criterios establecidos en este documento, la legitimación de este tratamiento de datos personales es el cumplimiento de una misión realizada en interés público (Ley Orgánica 6/2001, de 21 de diciembre, de Universidades), para el tratamiento de sus datos personales, la cual cosa implica que no es necesario el consentimiento del interesado, para las finalidades especificadas:

- Comunicación entre el estudiantado y el profesorado, y entre el propio estudiantado.
- Realización de actividades y acceso a los recursos propuestos por el profesorado.
- Evaluación por parte del profesorado.

Hay que tener presente que si se prevé tratar posteriormente los datos personales para una finalidad diferente de la que motivó la recogida, antes del tratamiento posterior se tiene que proporcionar al interesado información sobre esta otra finalidad y cualquier información adicional pertinente, para que pueda ejercer sus derechos, entre otros si se da el caso, el de no dar el consentimiento para esta nueva finalidad.

## 8. Información que hay que facilitar a los estudiantes

Habrà que informar a los interesados en dos momentos concretos:

- a) En el momento de enviarles un correo electrónico con el enlace de la sesión.
- b) En el momento de iniciar la sesión.

La información básica de protección de datos que se tiene que facilitar es la siguiente:





<b>Responsable del tratamiento</b>	Universitat Politècnica de Catalunya <a href="#">Nombre del centro o unidad con enlace a la página web donde contactar</a> <a href="mailto:dirección_correo_electrónico_de_contacto@upc.edu">dirección correo electrónico de contacto@upc.edu</a>
<b>Datos de contacto del delegado de protección de datos</b>	<a href="#">Universitat Politècnica de Catalunya</a> . ( <a href="https://www.upc.edu/normatives/ca/proteccio-de-dades/normativa-europea-de-proteccio-de-dades/dades-de-contacte-del-delegat-de-proteccio-de-dades">https://www.upc.edu/normatives/ca/proteccio-de-dades/normativa-europea-de-proteccio-de-dades/dades-de-contacte-del-delegat-de-proteccio-de-dades</a> )
<b>Finalidad del tratamiento</b>	<a href="#">F03.21 Gestió i ús del campus virtual</a> . ( <a href="https://rat.upc.edu/ca/registre-de-tractaments-de-dades-personals/F03.21">https://rat.upc.edu/ca/registre-de-tractaments-de-dades-personals/F03.21</a> ) <b>Sesión de clase / de evaluación en remoto del centro XXX año 2020</b>
<b>Legitimación</b>	Basado en el cumplimiento de una misión realizada en interés público (Ley Orgánica 6/2001, de 21 de diciembre, de Universidades)
<b>Destinatarios</b>	Vuestro nombre y apellidos o identificador a la sesión será visible al resto de participantes en el momento de asistir a la sesión. Vuestra imagen y/o voz será accesible al resto de participantes en el caso de que activéis la cámara y/o micrófono en el momento de asistir a la sesión. Vuestros datos no se cederán a terceros, salvo que sea de obligación legal.
<b>Derechos de las personas</b>	<a href="#">Solicitar el acceso, la rectificación o supresión, la limitación del tratamiento. Oponerse al tratamiento. Portabilidad de los datos.</a> ( <a href="https://www.upc.edu/normatives/ca/proteccio-de-dades/normativa-europea-de-proteccio-de-dades/drets">https://www.upc.edu/normatives/ca/proteccio-de-dades/normativa-europea-de-proteccio-de-dades/drets</a> )
<b>Plazo de conservación</b>	<a href="#">Mientras que sea necesario para cualquiera de los propósitos que se describen en nuestra política de conservación.</a> ( <a href="https://www.upc.edu/normatives/ca/proteccio-de-dades/normativa-europea-de-proteccio-de-dades/politica-de-conservacio-de-les-dades-de-caracter-personal">https://www.upc.edu/normatives/ca/proteccio-de-dades/normativa-europea-de-proteccio-de-dades/politica-de-conservacio-de-les-dades-de-caracter-personal</a> )
<b>Reclamación</b>	Si no ha estado satisfecho el ejercicio de vuestros derechos, podéis presentar una reclamación ante la APDCAT: <a href="mailto:apdcatt.gencat.cat">apdcatt.gencat.cat</a>





La información de la tabla anterior, **marcada en color amarillo**, hay que personalizarla según cada centro docente.