

## COMUNICADO ESPECIAL PRIVACIDAD Y COVID-19

Estimado/a alumno/a de la Escuela Universitaria de Osuna,

Como bien sabes, con fecha 1 de abril de 2020, se publicó un [Acuerdo de los Rectores y Rectoras de las Universidades Públicas de Andalucía y del Consejero de Economía, Conocimiento, Empresas y Universidad de la Junta de Andalucía](#); mediante el cual se aprobó mantener toda la docencia en formato online durante lo que resta del curso 2019-2020; así como preparar con la mayor celeridad posible un marco general de contingencia para determinar la forma de proceder en cuanto a prácticas que no puedan desarrollarse en formato online, mecanismos de evaluación, guías docentes, adaptación del calendario académico y desarrollo de TFG y TFM.

Esta situación novedosa, aunque no esperada ni deseada, está empujándonos a formas hasta ahora inexploradas de enseñar y aprender en el ámbito universitario. Todos coincidimos en que es lo mejor para la sociedad. Sin embargo, no podemos perder de vista que estos sistemas *online* entrañan sus propios riesgos y determinan la necesidad de que, como miembros de la comunidad universitaria, debemos adaptar nuestra forma de enseñar, aprender y evaluar; y al mismo tiempo, tener en cuenta ciertas precauciones de privacidad, seguridad y confidencialidad.

A través del presente comunicado, nos gustaría informarte de que esta situación también tiene implicaciones en relación con el tratamiento de tus datos personales, tanto por la Escuela Universitaria de Osuna, como en relación con las distintas herramientas que docentes y alumnos están utilizando para el estudio desde casa.

En primer lugar, deseamos recordarte cómo tratamos los datos personales en la Escuela Universitaria, y para ello puedes echarle un vistazo a nuestra [política de privacidad](#) publicada en la página web. El tratamiento de tus datos personales por parte de nuestra organización puede sufrir alguna modificación, relacionada exclusivamente con la adaptación de la docencia al ámbito virtual. En relación con lo anterior, hemos preparado un documento informativo sobre esta nueva actividad de tratamiento, al que puedes acceder [desde aquí](#).

Es **muy importante**, también, tener en cuenta todas aquellas circunstancias que rodean los **sistemas de evaluación en el nuevo entorno online**. La Escuela Universitaria ha elaborado un comunicado sobre esta materia, y que es de obligada lectura y cumplimiento por parte de todos los miembros de la comunidad universitaria.

En relación con las herramientas para la docencia online, la EUOsuna mantiene la actividad de sus sistemas y aplicativos habituales, como la plataforma virtual Educ@. De forma añadida, los docentes han venido recomendando y utilizando otro tipo de aplicaciones y herramientas para llevar a cabo sus clases o sus enseñanzas a través de Internet, tales como Google Meet, Zoom, Youtube, Blackboard o incluso grupos de Whatsapp. E

En cuanto a las aplicaciones de carácter externo, su uso no está soportado por la Escuela Universitaria, de modo que resulta de exclusiva responsabilidad de alumnos y docentes la decisión sobre su utilización. Sí está soportado el uso de las plataformas Google Meet y Educ@, al ser herramientas de uso corporativo en la Escuela.

Debe tenerse en cuenta que el uso de las distintas herramientas implicará la aceptación de unos términos legales y unas políticas de privacidad que, si bien en la mayoría de los casos cumplirán con los requisitos normativos, deberán ser leídas y aceptadas por todos los usuarios, con carácter previo a su registro y/o uso. Cada aplicación tiene sus propios términos de privacidad y seguridad, como [Google Meet](#), [Zoom](#), [Youtube](#), o [Whatsapp](#).

Por otro lado, en materia de Ciberseguridad, los organismos competentes en nuestro país han emitido diversos documentos con pautas a seguir para los usuarios de servicios en Internet. Así, es obligatorio echar un vistazo a las [recomendaciones del CCN-CERT](#), y también a la [nota técnica](#) emitida por la Agencia Española de Protección de Datos.

Como resumen de las medidas de protección del entorno informático y de protección de la confidencialidad en el ámbito de la educación online proporcionada por la EUOsuna, te recomendamos, de forma no exhaustiva, que observes cuanto menos las siguientes pautas:

### 1) Protege el dispositivo o los dispositivos electrónicos con los que estudias:

- a) Utiliza un antivirus y un cortafuegos (firewall): Existen muchos gratuitos y confiables (Avast, AVG, McAfee, Kaspersky, etc.).
  - Si estudias con ordenadores bajo entorno Windows, probablemente se encuentren protegidos de forma básica con Windows Defender. En ese caso, deberás mantener actualizadas correctamente las definiciones de virus y el propio programa.
  - En el caso de los dispositivos móviles, también existen soluciones gratuitas antivirus y/o antimalware en las tiendas oficiales de aplicaciones.
- b) Mantén actualizado el sistema operativo y los programas que utilices.
- c) No uses cuentas personales para acceder a los servicios de la Universidad o sistemas de correo electrónico de otras organizaciones. Debes usar la cuenta de correo electrónico proporcionada por la Escuela Universitaria.
- d) (Idealmente) conéctate al servidor de la empresa sólo a través de la Red Privada Virtual (VPN) que te han habilitado. (Sistemas gratuitos alternativos al VPN: Cyberghost, Hide.me, Opera VPN).

### 2) Protege la información:

- a) Utiliza y guarda contraseñas seguras (si deseas almacenarlas de modo seguro puedes utilizar la aplicación KeePass, etc).
- b) No debes compartir documentos e información de la Escuela Universitaria en entornos no seguros o con terceras personas fuera de la Escuela.
- c) Si se trata de documentos con un alto nivel de confidencialidad, te recomendamos que se compartan de modo cifrado, y compartiendo la contraseña con el destinatario por otro medio (por teléfono, por ejemplo). También se pueden compartir en mejor compartirlos en entornos propios controlados (Gdrive, Dropbox, Microsoft 365, etc.).
- d) Realiza copias de seguridad periódicas de la información que tratas y generas, independientemente que se refiera a datos de carácter personal o no.
- e) Si tienes que borrar datos o documentos, bórralos de forma segura (aquí podemos utilizar aplicaciones como Eraser o Undelete 360).

- f) Si deseas mayor protección, puedes cifrar el disco duro de tu PC o los pendrive, a través de programas como Bitlocker, Verocrypt, o USB Safeguard.

**3) Protege tu conexión a Internet:**

- a) Te recomendamos revisar el router-wifi con tu operador para que esté actualizado y con las medidas básicas de seguridad activadas (para ello puedes llamar al Servicio de Atención al Cliente de tu proveedor de Internet).
- b) No uses redes wifi abiertas y/o públicas.

**4) Respeta la confidencialidad de los datos y de la documentación:**

- a) Según la normativa de protección de datos, debes guardar secreto sobre cualquier dato de carácter personal que llegue a tu conocimiento, fuera del ámbito estrictamente universitario y de la finalidad para la cual se te ha comunicado.
- b) Toda la información que se te comunica por parte de la Escuela Universitaria tiene por defecto carácter confidencial, por lo que no deberá comunicarse fuera del ámbito para el cual se ha generado (del curso, de la asignatura, etc.). Salvo que se te haya autorizado expresamente para ello.
- c) En el caso de que puedas desarrollar prácticas con centros colaboradores de la Escuela Universitaria, se te recuerda que debes guardar también la más estricta confidencialidad con respecto a aquellos datos o documentos a los que puedas tener acceso (así lo dispone, por ejemplo, el art. 6 de la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente).

Atentamente,

Jefatura de Estudios