FAQ. V.7.3.22

PREGUNTAS FRECUENTES SOBRE LA APLICACIÓN DE LOPDyENS

I.USO DE LA APLICACIÓN. -

I.1.-PARA DARME DE ALTA EN LA APLICACIÓN ¿TIENE QUE SER SIEMPRE CON MI UVUS Y CLAVE PERSONAL O PUEDE SER CON UN UVUS INSTITUCIONAL?

Puede darse de alta con cualquiera de los dos, siempre que utilice para entrar el mismo con el que se haya dado de alta en la aplicación la primera vez.

II.-RESPONSABLES; ENCARGADOS; CORRESPONSABLES.

II.1.- ¿POR QUÉ EXISTEN DOS TIPOS DE RESPONSABLE TECNOLÓGICO? ¿QUÉ PAPEL JUEGA CADA UNO?

El/los Responsable/s Tecnológico/s es/:

El/los Máximo/s Responsable/s de la/s Unidad/es (o persona en quien delegue) donde se ubican los servidores que contienen las aplicaciones y ficheros relativos a los tratamientos. Se encargará/n del establecimiento desde el punto de vista tecnológico y mantenimiento de las medidas técnicas y organizativas que garanticen el cumplimiento de la normativa, en el tratamiento correspondiente.

Pueden existir dos tipos de RT en función de cómo hayan de incluirse las medidas de seguridad técnicas:

Responsable Tecnológico del Aplicativo: es la persona que gestión la aplicación en la que se tratan los datos. En algunas ocasiones las aplicaciones se gestionan en el SIC, siendo éste el responsable tecnológico de los aplicativos.

Responsable Tecnológico de la Infraestructura: es la persona responsable de los servidores que albergan las aplicaciones, y de las infraestructuras en la que se alojan dichos servidores. Si estos están en el CPD principal de la Universidad, las medidas (o una parte de ellas cuando los servidores se alojen en la modalidad de Infraestructura como Servicio) serán responsabilidad del SIC.

II.2.- EL SIGNIFICADO DE CORRESPONSABLE EN UN TRATAMIENTO.

Según el art. 26 del RGPD hay corresponsabilidad cuando:

Delegada de Protección de Datos Universidad de Sevilla, Pabellón de Uruguay, Avda.de Chile s/n, 41013 Sevilla.
dpd@us.es

1. Cuando dos o más responsables determinen conjuntamente los objetivos y los medios del tratamiento serán considerados corresponsables del tratamiento. Los corresponsables determinarán de modo transparente y de mutuo acuerdo sus responsabilidades respectivas en el cumplimiento de las obligaciones impuestas por el presente Reglamento, en particular en cuanto al ejercicio de los derechos del interesado y a sus respectivas obligaciones de suministro de información a que se refieren los artículos 13 y 14, salvo, y en la medida en que, sus responsabilidades respectivas se rijan por el Derecho de la Unión o de los Estados miembros que se les aplique a ellos. Dicho acuerdo podrá designar un punto de contacto para los interesados.

III. MEDIDAS DE SEGURIDAD. -

III.1- LAS PETICIONES RELACIONADAS CON MEDIDAS DE SEGURIDAD EN LA APLICACIÓN ¿DE QUIÉN ES LA RESPONSABILIDAD DE CUMPLIMENTARLAS?

Del Responsable Tecnológico, siguiendo las indicaciones de las medidas organizativas que le indique el RD. También puede desempeñarlas por delegación del RD, si así lo cree conveniente y la persona que se encarga de ello tiene los suficientes conocimientos informáticos, el Gestor o cualquier persona en quien delegue el primero.
El contenido de este apartado debe ser realizado por el RT en coordinación con el RD en función del tipo de tratamiento y de las aplicaciones que se utilicen. Otra cosa es quien debe rellenarlo, puede ser tanto el RT como el gestor, pero la responsabilidad del contenido es del RT.

III.2.- ¿CÓMO SE ESTABLECEN LAS MEDIDAS DE SEGURIDAD PARA GARANTIZAR LA INTEGRIDAD Y CONFIDENCIALIDAD DE LOS DATOS?

La **confidencialidad** se consigue mediante privilegios de acceso a la información. Solo las personas autorizadas podrán acceder a los datos. Cuando la información está en tránsito las conexiones deben ser seguras, utilizando canales de comunicación cifrados que impidan que un tercero pueda acceder a ella (por ejemplo, mediante el uso de https en la navegación cuando hay datos confidenciales.)
La **integridad** es la propiedad de la información que garantiza que esta no ha sido modificada desde el origen al destino.
La integridad debe preservarse no solamente en la transmisión (de origen al destino) sino en el almacenamiento.

Para prevenir ataques activos que produzcan alteración de la información en tránsito, inyección de información espuria o secuestro de la sesión por una tercera parte hay que aplicar distintas medidas de seguridad: proteger accesos, actualizar software, eliminar vulnerabilidades, instalar sistemas de protección específicos.

Delegada de Protección de Datos Universidad de Sevilla, Pabellón de Uruguay, Avda.de Chile s/n, 41013 Sevilla.
dpd@us.es

Para el tema de la integridad de la información en el almacenamiento se recomiendan medidas como los verificadores de integridad y los File Integrity Monitoring (FIM) y en la transmisión la integridad se conserva mediante el uso de protocolos seguros que la tengan en cuenta.

III.3.- ¿A QUIÉN CORRESPONDE ESTABLECER LAS MEDIDAS DE SEGURIDAD DENTRO DEL SERVICIO DÓNDE SE DESARROLLE EL TRATAMIENTO Y HACERLAS CUMPLIR?

Corresponde al Responsable Delegado y al Responsable Tecnológico, coordinadamente.

III.4.- ¿CUÁLES DEBEN SER LAS MEDIDAS DE SEGURIDAD A APLICAR?

Las establecidas en el art.28.5 del RGPD, y las establecidas en la D.A. 1ª de la LOPDyGDD[1] que han de ajustarse a los dispuesto en el R.D. 3/2010, de 8 de Enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración Electrónica. Las medidas aplicadas deben ser proporcionales al tipo de datos y tratamiento que se les dé a estos.

IV. TRANSPARENCIA/EJERCICIO DE DERECHOS. -

IV.1.- CUANDO ENTRO EN LA APLICACIÓN, ¿QUE DIFERENCIA HAY ENTRE "TRANSPARENCIA" Y "EJERCICIO DE DERECHOS DE LOS INTERESADOS? ¿NO ES LO MISMO?

La Transparencia es uno de los principios básicos y directamente aplicables que es necesario cumplir en todo tratamiento de datos personales. Se trata de la información relativa al tratamiento de los datos personales y a los derechos que asisten al interesado, que toda Unidad/Centro o Servicio debe comunicar a los usuarios/interesados, cuyos datos van a ser objeto de tratamiento.
Ejercicio de derechos de los interesados es el procedimiento establecido por la Unidad/Centro/Servicio de la Universidad, para que aquellos puedan ejercitar los derechos reconocidos en la normativa.

IV.2.- ¿CÓMO SE ESTABLECE UN PROCEDIMIENTO PARA QUE EL INTERESADO PUEDA ACCEDER, RECTIFICAR, SUPRIMIR SUS DATOS, ¿E INCLUSO SU BORRADO TOTAL O DERECHO AL OLVIDO?

Existe un procedimiento general que puede consultarse en:
https://sic.us.es/derechos
La Unidad/Servicio/Centro deberá establecer un procedimiento propio y visible a los interesados para que puedan ejercitar este derecho. P.E. puede incluir el enlace al procedimiento general.

[1] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

Delegada de Protección de Datos Universidad de Sevilla, Pabellón de Uruguay, Avda.de Chile s/n, 41013 Sevilla.
dpd@us.es

V.LEGITIMACION DEL TRATAMIENTO. -

V.1.- ¿EN QUÉ CASOS DE LOS ART. 6 AL 9 DEL RGPD[2], HAY QUE PEDIR EL CONSENTIMIENTO Y/O CONSENTIMIENTO INFORMADO?

Se debe pedir el consentimiento informado exclusivamente para aquellas actividades de tratamiento que de acuerdo con los artículos citados se legitimen en esta condición. Cada RD ha definido en el tratamiento qué bases de legitimación son las aplicables en cada caso.
Será necesario solicitar el consentimiento en aquellas actividades de tratamiento de datos personales que esta condición sea base legitimadora. En la aplicación hay que demostrar que se ha solicitado y cómo el responsable del tratamiento lo guarda.

V.2.- ¿QUÉ CONSIDERA EL RGPD COMO TRATAMIENTO LÍCITO?

La licitud o legitimidad del tratamiento es uno de los principios básicos y directamente aplicable del sistema jurídico de protección de datos europeo. Se encuentra regulado en los artículos 6 y 9 del RGPD donde se señalan una serie de condiciones en que se habrán de basar los tratamientos de datos personales para considerarse legítimos/lícitos.

VI. PLAZO DE CONSERVACION. -

VI.1.- ¿CUÁL ES EL PLAZO LEGAL ESTABLECIDO PARA CONSERVAR Y BORRAR LOS DATOS EN EL CASO DE LA US? ¿Y CUÁNDO SE TRATA DE UN ENCARGADO DE TRATAMIENTO EXTERNO?

Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados. Esta valoración la debe de realizar el RD de conformidad con la legislación aplicable al tratamiento y a los datos personales.

VI.2.- ¿CÓMO SE EVIDENCIA QUE LOS DATOS HAN SIDO BORRADOS?

Mediante certificaciones, procesos de borrado… es competencia del RT/RD

VI.3.- ¿QUIÉN Y CUÁNDO SE DEBE REVISAR LA PERTINENCIA PARA CONSERVAR LOS DATOS, CUANDO YA NO SON NECESARIOS?

El RD debe analizar el tratamiento y decidir este aspecto, de conformidad con la legislación aplicable.

Para la eliminación de documentos se deben seguir las siguientes pautas:

[2] 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 y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)

Delegada de Protección de Datos Universidad de Sevilla, Pabellón de Uruguay, Avda.de Chile s/n, 41013 Sevilla.
dpd@us.es

Delegada de Protección de Datos Universidad de Sevilla, Pabellón de Uruguay, Avda.de Chile s/n, 41013 Sevilla.
dpd@us.es