



GOBIERNO DEL  
PRINCIPADO DE ASTURIAS

Nº de verificación: 12431205345660732604



Puede verificar la autenticidad de este doc. en [www.asturias.es](http://www.asturias.es)

Datos del registro

Libro: Libro general salidas

Unidad registral: O.I. EDUCACION

JUSTIFICANTE DE REGISTRO DE SALIDA

Nº de registro: SAL2019226970

Fecha y hora de registro: 11/07/2019 14:16

Destinatario: PABLO BELAY FERNÁNDEZ

DNI/CIF:

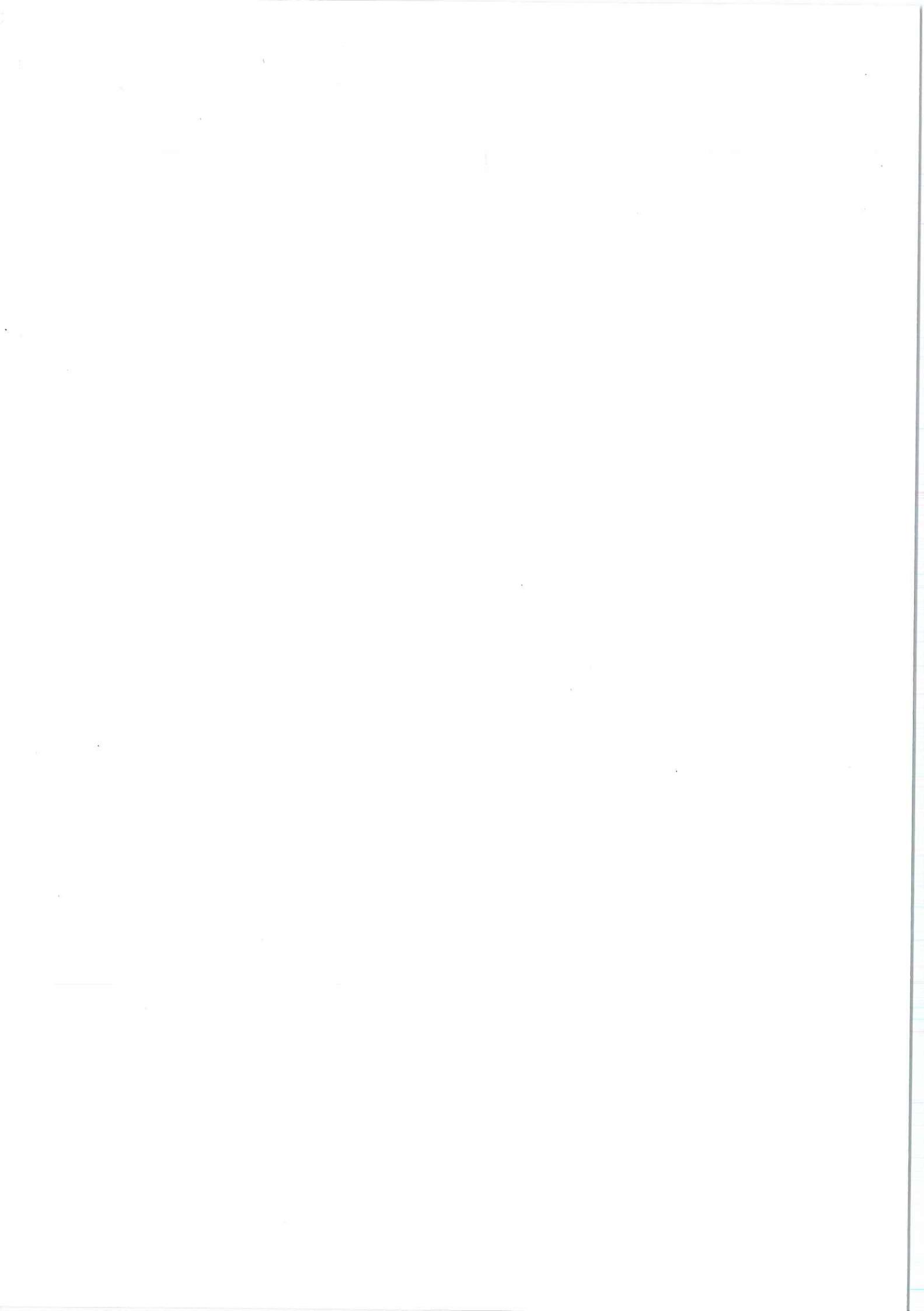
Asunto: NOTIFICACIÓN DE RESOLUCIÓN DE 10 DE JULIO DE 2019 POR LA QUE SE CONCEDE EL ACCESO A LA INFORMACIÓN PÚBLICA SOLICITADA  
EXpte LT 19/2019

Remitente: 925 Servicio de Régimen Jurídico y Normativa

Documentación adjunta:

Puede consultar cada uno de los documentos anexos en [www.asturias.es](http://www.asturias.es)

Nombre	Descripción	CSV
--------	-------------	-----



**SECRETARIA GENERAL TÉCNICA**

**Resolución de 10 de julio de 2019**, por la que se concede el acceso a la información pública solicitada por D. Pablo Belay Fernández.

N/rº. LT 19/2019

**D. Pablo Belay Fernández**  
C/ Campo do Forno, piso 1, puerta 27  
15703 Santiago de Compostela  
LA CORUÑA.

Con fecha 10 de julio de 2019, el Ilm. Sr. Consejero de Educación y Cultura ha dictado la siguiente RESOLUCIÓN:

“En las actuaciones practicadas como consecuencia de la solicitud de acceso a información pública presentada por D. Pablo Belay Fernández ante la Consejería de Educación y Cultura, resultan los siguientes:

**ANTECEDENTES DE HECHO**

**Primero.-** Con fecha de 12 de junio de 2019, D. Pablo Belay Fernández presenta solicitud de acceso a información pública solicitando diversa información en relación con la implantación de la plataforma Office 365 y diferentes tecnologías en la Consejería de Educación y Cultura que se le remita.

El solicitante no alega motivo de su solicitud, a lo que legalmente no está obligado.

**Segundo.-** Con fecha 10 de julio de 2019, el Servicio de Orientación Educativa y Formación del Profesorado remite la información solicitada.

**FUNDAMENTOS DE DERECHO**

**Primero.-** Conforme a los artículos 17 y 20.1 de la LTAIBG en relación con el artículo 21.4 de la Ley del Principado de Asturias 2/1995, de 13 de marzo, de Régimen Jurídico de la Administración y el artículo 14 de la ley del Principado de Asturias 8/2018, de 14 de septiembre, de Transparencia, Buen Gobierno y Grupos de Interés, resulta competente para dictar la presente Resolución el Ilmo. Sr. Consejero de Educación y Cultura.

**Segundo.-** La LTAIBG, en su artículo 12, regula el derecho de todas las personas a acceder a la información pública entendida, según el artículo 13 de la misma norma, como *los contenidos o documentos, cualquiera que sea su formato o soporte, que obren en poder de algunos de los sujetos incluidos en el ámbito de aplicación de este título y que hayan sido elaborados o adquiridos en el ejercicio de sus funciones*. Por lo tanto, la Ley define el objeto de una solicitud de acceso a la información en relación a la que ya existe, por cuanto está en posesión del órgano o unidad que recibe la solicitud, bien porque él mismo la ha elaborado o bien porque la ha obtenido en el ejercicio de las funciones y competencias que tiene encomendadas. Asimismo, el artículo 12 de la mencionada Ley del Principado de Asturias 8/2018 prevé igualmente dicho derecho de acceso a la información pública, determinando que se ejercerá mediante solicitud previa de conformidad con la normativa estatal.

**Cuarto.-** De acuerdo con el informe del Servicio de Orientación Educativa y Formación del Profesorado, la información solicitada tiene el carácter de información administrativa y documentación de expedientes que obran en poder de dicho servicio, en cuanto unidad competente en materia de gestión y mantenimiento del portal Educastur, en la versión pública en modo internet y en la versión corporativa en modo intranet, así como el fomento y apoyo de los correspondientes servicios educativos en línea, según se establece en el Decreto 65/2015, de 13 de agosto, por el que se establece la estructura orgánica básica de la Consejería de educación y Cultura. Además, no se trata de información que suponga perjuicio alguno en relación a los aspectos relacionados en el artículo 14 LTBG.

Por lo tanto, de acuerdo con lo anterior y en lo que respecta a la documentación solicitada, cabe decir lo siguiente:

**I.- Descripción detallada y/o memoria del proyecto de implantación de Office 365 en la Consejería de Educación:** Se facilita memoria del proyecto de implantación de Office 365 (Anexo I).

*2.- Coste anual de mantenimiento de la plataforma Office 365:* En el año 2018 se adjudicó el contrato de mantenimiento de la plataforma, resultando que su coste anual fue por un importe de 3666,30 €. A la vista del escaso número de incidencias atendidas, en el año 2019 se decide no externalizar este servicio, siendo prestado de forma directa por el personal propio de la Administración del Principado de Asturias.

*3.- Copia del pliego de contratación de la plataforma Office 365:* No existe expediente de contratación de la plataforma pues, al ser un servicio gratuito, está excluido de la Ley de Contratos del Sector Público.

*4.- Servicios prestados de la plataforma Office 365:* Los servicios prestados se relacionan en la propia memoria de implantación (ver página 5 del anexo I). También pueden consultarse en la siguiente dirección:

<https://docs.microsoft.com/es-es/office365/servicedescriptions/office-365-platform-service-description/office-365-education#service-availability-for-each-plan>

*5.- Estudio de cumplimiento de los estándares abiertos de la plataforma Office 365:* No se realiza un estudio expreso de los estándares abiertos, ya que, el servicio ofrecido a la comunidad educativa por esta Consejería a través de la plataforma Office 365 cumple con las características señaladas en la definición de la Letra k, del anexo de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos. (Derogada por Ley 39/2015, que no recoge la definición que figuraba en el anexo de la Ley 11/2007), en la que se señala que:

“Un estándar abierto cumple las siguientes condiciones:

- Es público, y su uso está disponible gratuitamente, o a un coste que no implique dificultad para los usuarios.
- Su uso no está sujeto a pagos de ningún tipo de propiedad intelectual o industrial.”

Además, la plataforma cumple con lo establecido en el Esquema Nacional de Seguridad, que se puede consultar en:

[https://www.administracionelectronica.gob.es/pae/Home/pae\\_Estrategias/pae\\_Interoperabilidad\\_Inicio/pae\\_Esquema\\_Nacional\\_de\\_Interoperabilidad.html#.XQHo5W5uLZs](https://www.administracionelectronica.gob.es/pae/Home/pae_Estrategias/pae_Interoperabilidad_Inicio/pae_Esquema_Nacional_de_Interoperabilidad.html#.XQHo5W5uLZs)

*6.- Importe de las facturas emitidas en los últimos 5 años a la compañía Microsoft y descripción del servicio prestado:* No existe ningún contrato y, por consiguiente, ninguna factura emitida por esta compañía relativa a los servicios de Office 365.

*7.- Estudio de interoperabilidad con sistemas libres como puede ser GNU/Linux.* No existe un estudio específico sobre esta materia ya que Office 365 está diseñado para funcionar en cualquier navegador sin importar el sistema operativo, aunque también dispone de aplicaciones para PC, Mac y dispositivos móviles:

<https://products.office.com/es-es/office-system-requirements#coreui-contentrichblock-cs9mei4>

Asimismo, como ya se ha dicho en el punto 5, el servicio cumple con lo establecido en el esquema nacional de interoperabilidad para las Administraciones Públicas

*8.- Información de cómo proteger los datos en la plataforma Office 365.* Se facilitan, como anexo, varios informes de la Agencia Española de Protección de Datos (en adelante, AEPD) sobre consultas planteadas a lo largo del proceso de implantación de la plataforma, que se relacionan a continuación:

- Anexo II: *Informe del Gabinete Jurídico AEPD 0179/2010.*
- Anexo III: *Resolución AEPD de 9 de mayo de 2014, de declaración de adecuación de garantías para las transferencias internacionales de datos a los estados unidos con motivo de la prestación de servicios de computación en nube (Nº. Expediente: TI/00032/2014).*
- Anexo IV: *Informe de Gabinete Jurídico AEPD 463376/2015, de 17 de diciembre de 2015.*

Asimismo, se adjunta como anexo el *Estudio de impacto sobre la privacidad y seguridad Office 365*, elaborado para la Consejería de Educación, Cultura y Deporte del Principado de Asturias, con fecha 18 de agosto de 2014 (Anexo V).

9.- *Procedimiento para autorizar el uso de menores.* Este procedimiento se explica detalladamente en la Memoria de implantación (Ver Anexo I).

10.- *Información si el servicio se encuentra alojado en servidores propios de la Consejería o ha sido externalizado.* Los servicios de Office 365 se ofrecen desde los datacenters de Microsoft. Para más información, consultar el siguiente enlace:

<https://products.office.com/en-us/where-is-your-data-located?geo=Europe#Europe>.

11.- *Estudio de alternativas a la implantación de Office 365.* Se facilitan los estudios previos realizados que fundamentan la decisión de implantación de Office 365 y que se relacionan a continuación:

- Anexo VI: *Estudio sobre Definición del modelo de arquitectura tecnológica.*
- Anexos VII y VIII: Actas de reuniones en las que se decide optar por un modelo en la nube en vez de por la alternativa propuesta por el estudio de Indra.

Asimismo, también ha de tenerse en cuenta el documento que figura en el anexo V, ya mencionado.

Finalmente, ha de advertirse que, para la protección de datos personales el acceso se concede previa disociación de datos de carácter personal y de las rúbricas personales que figuran en la documentación a que se concede acceso.

**Quinto.-** De conformidad con el artículo 17.2 d) LTAIBG, en la solicitud de acceso a la información la persona solicitante debe indicar la modalidad que se prefiera para la información solicitada. En este caso, el dicente solicita que la copia de la información se le remita en formato digital o en papel; como quiera que el artículo 22, 1 LTAIBG establece que el acceso a la información se hará preferentemente por vía electrónica, será el formato digital, a través del correo electrónico, la modalidad que se empleará para la comunicación.

En base a lo expuesto, y de acuerdo con las competencias reguladas en el artículo 14 de la Ley del Principado de Asturias 2/1995, de 13 de marzo, de Régimen Jurídico de la Administración y el artículo 38 de la ley del Principado de Asturias 6/1984, de 5 de julio, del Presidente y del Consejo de Gobierno, a propuesta del Servicio de Régimen Jurídico y Normativa,

#### RESUELVO

**Primero.-** Conceder el acceso a la información pública solicitada por D. Pablo Bely Fernández en los términos expuestos en el fundamento de derecho cuarto, habiendo de facilitársele el acceso a la misma mediante correo electrónico remitido a su dirección de correo electrónico.

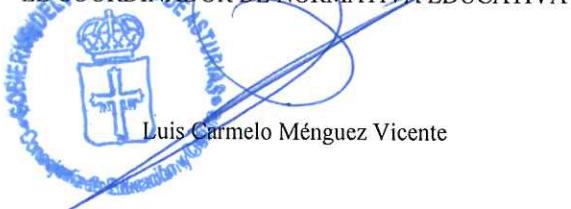
**Segundo.-** Notificar la presente Resolución al solicitante.

Frente a esta Resolución, que pone fin a la vía administrativa, podrá interponerse recurso contencioso-administrativo ante la Sala de lo Contencioso-Administrativo del Tribunal Superior de Justicia de Asturias, en el plazo de dos meses o, previa y potestativamente, reclamación ante el Consejo de Transparencia y Buen Gobierno en el plazo de un mes; en ambos casos, el plazo se contará desde el día siguiente al de la notificación de la presente resolución. Todo ello, sin perjuicio de la posibilidad de interponer cualquier otro recurso que se estime procedente.”

**La que traslado para su conocimiento y efectos, significando que contra la misma cabe interponer los recursos que en su pie se señalan.**

Oviedo, a 11 de julio de 2019

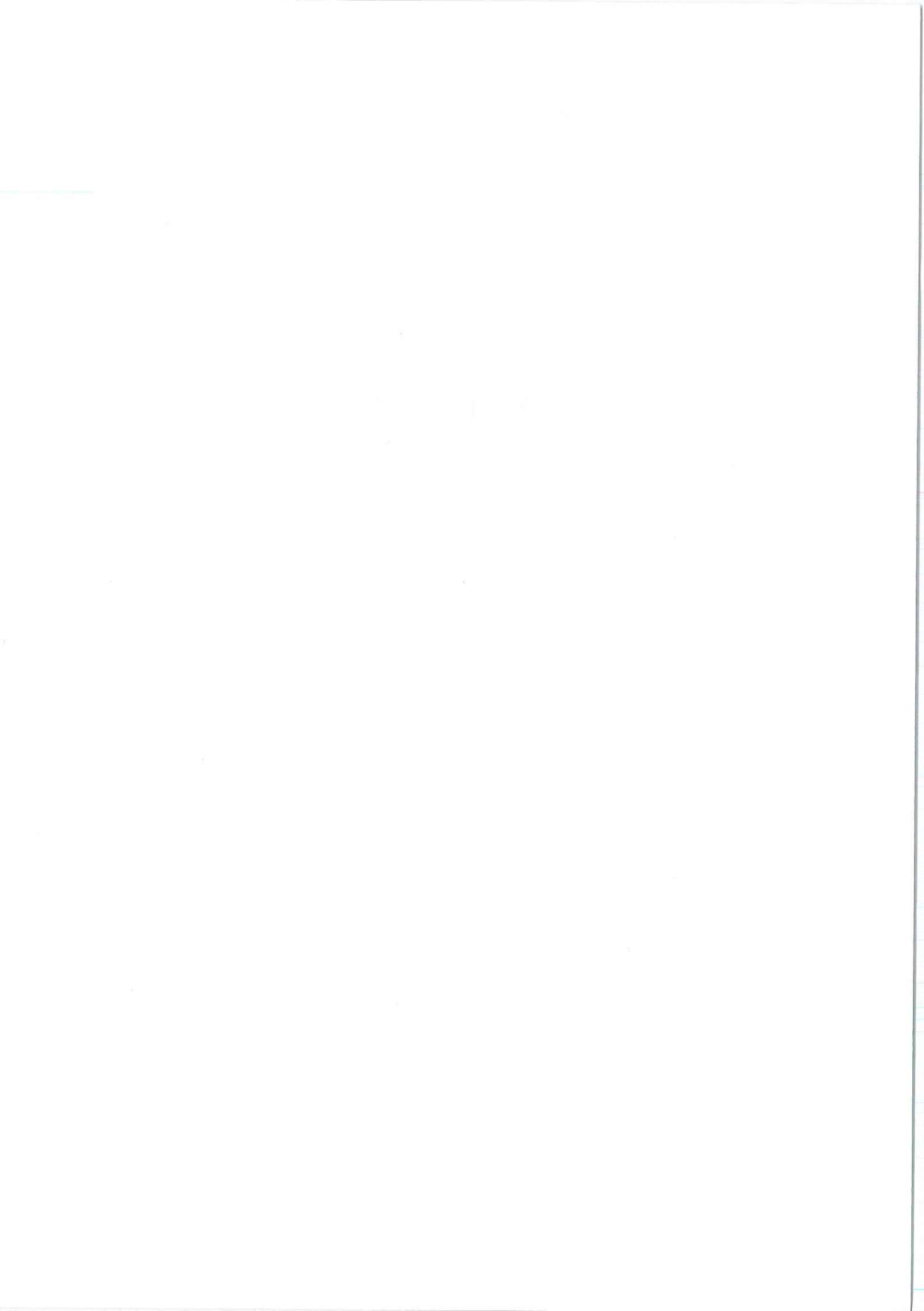
EL COORDINADOR DE NORMATIVA EDUCATIVA



Luis Carmelo Ménguez Vicente



## ANEXO I



# **IMPLANTACIÓN DE EDUCASTUR 365**



**2016-2017**

educastur )))

## IMPLANTACIÓN DE OFFICE 365 DE EDUCASTUR

En 2015 la Consejería de Educación y Cultura inició un proceso de actualización de sus servicios educativos en línea: portal público Educastur, Intranet Educastur, Campus... En 2016 se procedió a la sustitución del antiguo correo electrónico corporativo por el correo del entorno Office 365 (Microsoft) y sus aplicaciones asociadas, de gran interés educativo.

El procedimiento de entrega de credenciales 365 se desarrolló en dos fases: en el tercer trimestre del curso 2015-2016 se procedió a la entrega de las nuevas credenciales para centros educativos y profesorado; en el primer trimestre del curso 2017-2018 se entregaron las credenciales de las cuentas del alumnado.

### Identidad digital Educastur

Centros, profesorado y alumnado poseen una identidad digital institucional, implantada a partir del año 2000 que, antes de la disponibilidad del entorno 365 (1 de julio de 2016), incluía también el acceso al antiguo correo corporativo. Con la adopción del sistema 365 la identidad digital general sigue existiendo para dar acceso a todos los servicios educativos (intranet, SAUCE, campus, blog...), excepto al 365.

Los usuarios Educastur y 365 están sincronizados a través del LDAP (sistema de mantenimiento de usuarios) de Educastur de forma que el mismo usuario de la cuenta general de Educastur es el nombre de usuario que precede a la @ en el usuario 365. La contraseña no está sincronizada.

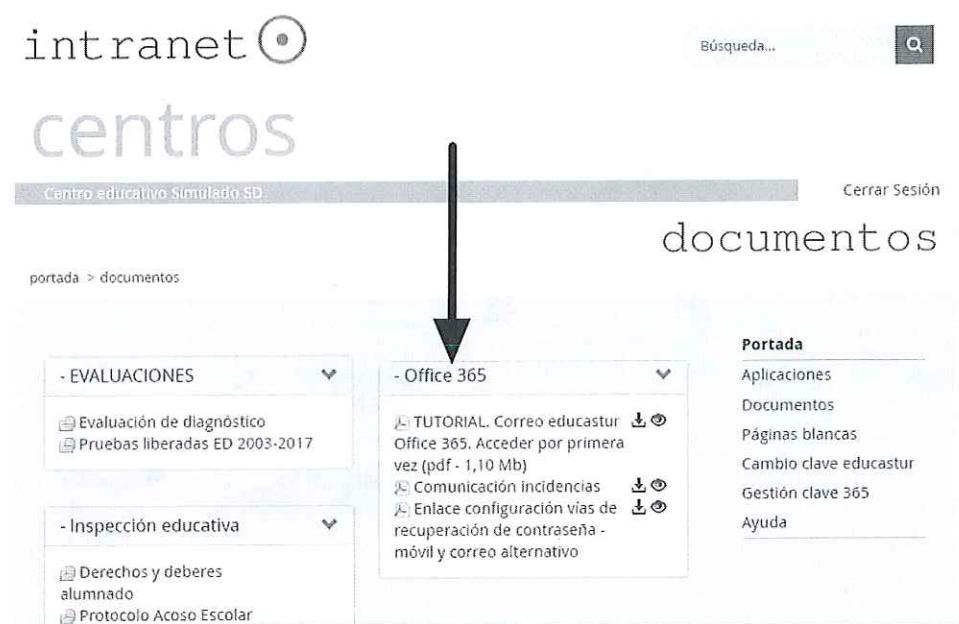


Cuenta institucional general Educastur y cuenta institucional 365  
<https://www.educastur.es/identidad-digital/mapa-id>

## ENTREGA DE CREDENCIALES 365: CENTROS Y PROFESORADO

En junio de 2016 se procedió a la entrega a centros, AMPA y profesorado de una contraseña inicial para el primer acceso al entorno 365; esta contraseña temporal debía ser cambiada por una clave personal en el primer acceso.

Toda la información se trasmitió a los centros mediante el servicio de boletines institucionales de la Consejería y, durante todo el proceso, se facilitó información detallada y actualizada a través del portal público Educastur y de la Intranet Educastur (acceso con cuenta general de Educastur) en la sección *Documentos /Office 365*.



### Distribución a centros educativos públicos

La distribución de credenciales se realizó a través del programa GECE 2000, un repositorio institucional al que todos los centros públicos tienen acceso (cuenta institucional general de Educastur). Para agilizar la entrega de credenciales al profesorado (más de 12.000 cuentas) el propio centro educativo se encargó de la descarga de credenciales y la entrega personal a cada docente del centro; también el centro entregó las credenciales de la AMPA.

Se enviaron sendos boletines oficiales informando del procedimiento:

[2016-05\\_CEN-PRO\\_boletin-centros-publicos-1.pdf](#) (enviado el 18-05-2016)

[2016-05\\_CEN-PRO\\_boletin-centros-publicos-2.pdf](#) (enviado el 02-06-2016)

Modelo de documento de entrega de credenciales para centros públicos:

[2016-05\\_CEN-PRO\\_credenciales\\_centros-publicos.pdf](#)

### Distribución a centros concertados y privados

Los centros concertados y privados no disponían de acceso al repositorio GECE 2000; se enviaron por correo ordinario las credenciales iniciales del centro, del profesorado y de la AMPA y un boletín oficial informando del procedimiento:

[2016-05\\_CEN-PRO\\_boletin-centros-concertados.pdf](#) (enviado el 18-05-2016)

Modelos de documentos de entrega de credenciales para centros concertados y privados:

[2016-05\\_CEN-PRO\\_credenciales\\_centros-publicos.pdf](#) (igual en públicos y concertados)

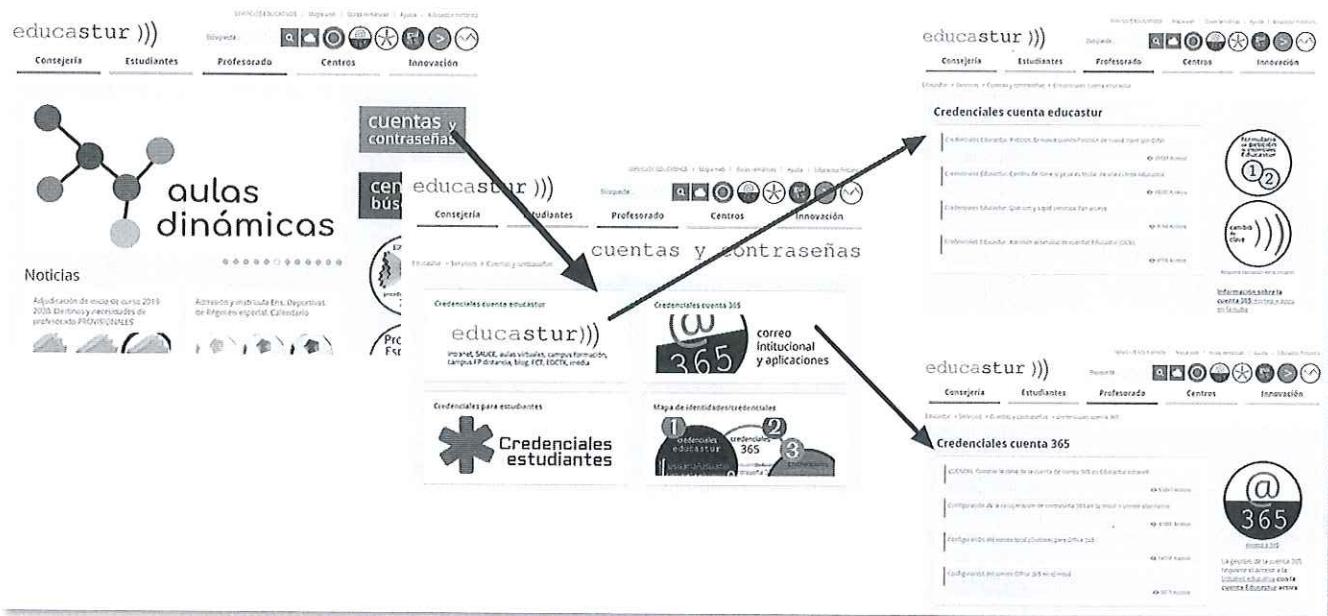
[2016-05\\_CEN-PRO\\_credenciales\\_centros\\_privados.pdf](#)

### Entrega de credenciales 365 al profesorado

Modelo de documento de entrega de credenciales al profesorado:

[2016-05\\_CEN-PRO\\_credenciales\\_profesores.pdf](#)

## Más información sobre cuentas Educastur y 365:



<https://www.educastur.es/identidad-digital>

## ENTREGA DE CREDENCIALES 365: CUENTAS INSTITUCIONALES

En mayo de 2016 se procedió a generar y distribuir las credenciales de las nuevas cuentas 365 que sustituían a las cuentas institucionales utilizadas habitualmente por los diferentes servicios de la Consejería de Educación: Centros, Personal docente, Formación del profesorado, Educastur, Evaluación educativa, etc. Las credenciales se entregaron directamente a las personas responsables de cada servicio de la Consejería, junto con la información y tutoriales necesarios para su activación y uso.

## ENTREGA DE CREDENCIALES 365: ALUMNADO

Al igual que los centros y el profesorado el alumnado asturiano tiene identidad digital de Educastur, la cuenta general de acceso a los servicios educativos. El usuario de esta cuenta está sincronizado con el sistema general de gestión de centros (SAUCE) y con el árbol de usuarios de Educastur (LDAP) de forma que cuando se formaliza una matrícula en el sistema educativo se genera una cuenta de Educastur (general) y una cuenta de 365 (correo y apps de Microsoft). El usuario de la cuenta general es el mismo que precede a la @ en el usuario 365. Estas cuentas son permanentes a lo largo de toda la vida académica.

En el caso del alumnado, la gestión de contraseñas de la cuenta general de Educastur está delegada a los centros educativos que tienen acceso a un servicio específico de recuperación de las contraseñas del alumnado de su centro.

En el momento de la implantación de las cuentas 365 para el alumnado ya se disponía de un servicio en línea de generación y cambio de contraseñas, accesible desde la Intranet Educastur (acceso con cuenta general de Educastur), por lo que el despliegue de las contraseñas iniciales de acceso a 365 fue mucho más sencillo.

Se informó a todos los centros del procedimiento mediante boletines oficiales:

2017-11\_EST\_boletin-credenciales-estudiantes.pdf (enviado el 14-11-2017)

Documento adjunto: 2017-11\_EST\_credenciales-estudiantes-info-centros.pdf

**Credenciales para estudiantes**

**Credenciales de acceso a servicios en línea para estudiantes**

15/11/2017

**Guía de credenciales**

Guía de credenciales (pdf, 1,9 MB)

<https://www.educastur.es/identidad-digital/credenciales-estudiantes>

La Guía se ofrece en formato de presentación (Genial.ly), para que los centros puedan utilizarla en sesiones informativas con las familias, y con código de inserción para publicarla en sus webs o blogs; también se publicó un documento textual a modo de información general o como carta informativa para que los centros enviaran a las familias.

2017-11\_EST\_credenciales-estudiantes-info-general.pdf (información general)  
2017-11\_EST\_credenciales-estudiantes\_guia.pdf (guía credenciales)

### Procedimiento de entrega de credenciales

Cada centro accedía a la aplicación *Cuentas de alumnado* (Intranet Educastur) y entregaba las credenciales Educastur (cuenta general) a cada alumna y alumno o a sus familias. Con la cuenta Educastur se accede a la aplicación de gestión de cuentas 365 en la Intranet Educastur y se genera automáticamente una contraseña inicial para acceder a 365. Al entrar por primera vez el sistema solicita una contraseña personal nueva.

intranet

profesorado

BEATRIZ FERZ GARCIA

portada

clave 365

páginas blancas

cambio clave 365

Este servicio permite a personal docente, centros educativos y estudiantes generar la primera clave de acceso al correo 365 u obtener una nueva clave siempre que sea necesario.

Si quiere cambiar su contraseña del correo, pulse el botón "Cambiar contraseña".

correo@educastur.org

Cambiar contraseña

AVISO Documentos/Escuelas concertadas Dispositivo Proyecto Configurador web y

Portada Aplicaciones Documentos Páginas blancas Cambio clave educastur Gestión clave 365 Ayuda

@ 365

Acceso a 365

<https://intranet.educastur.es> (acceso con cuenta general Educastur)

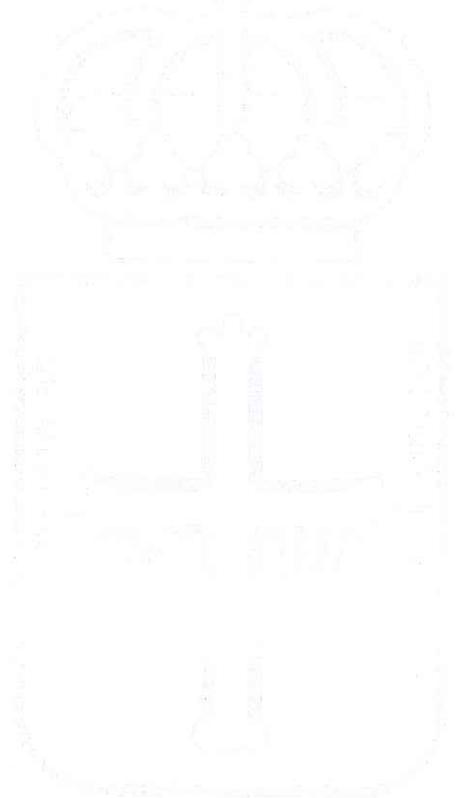
## APLICACIONES DISPONIBLES EN EDUCASTUR 365 (JULIO 2019)

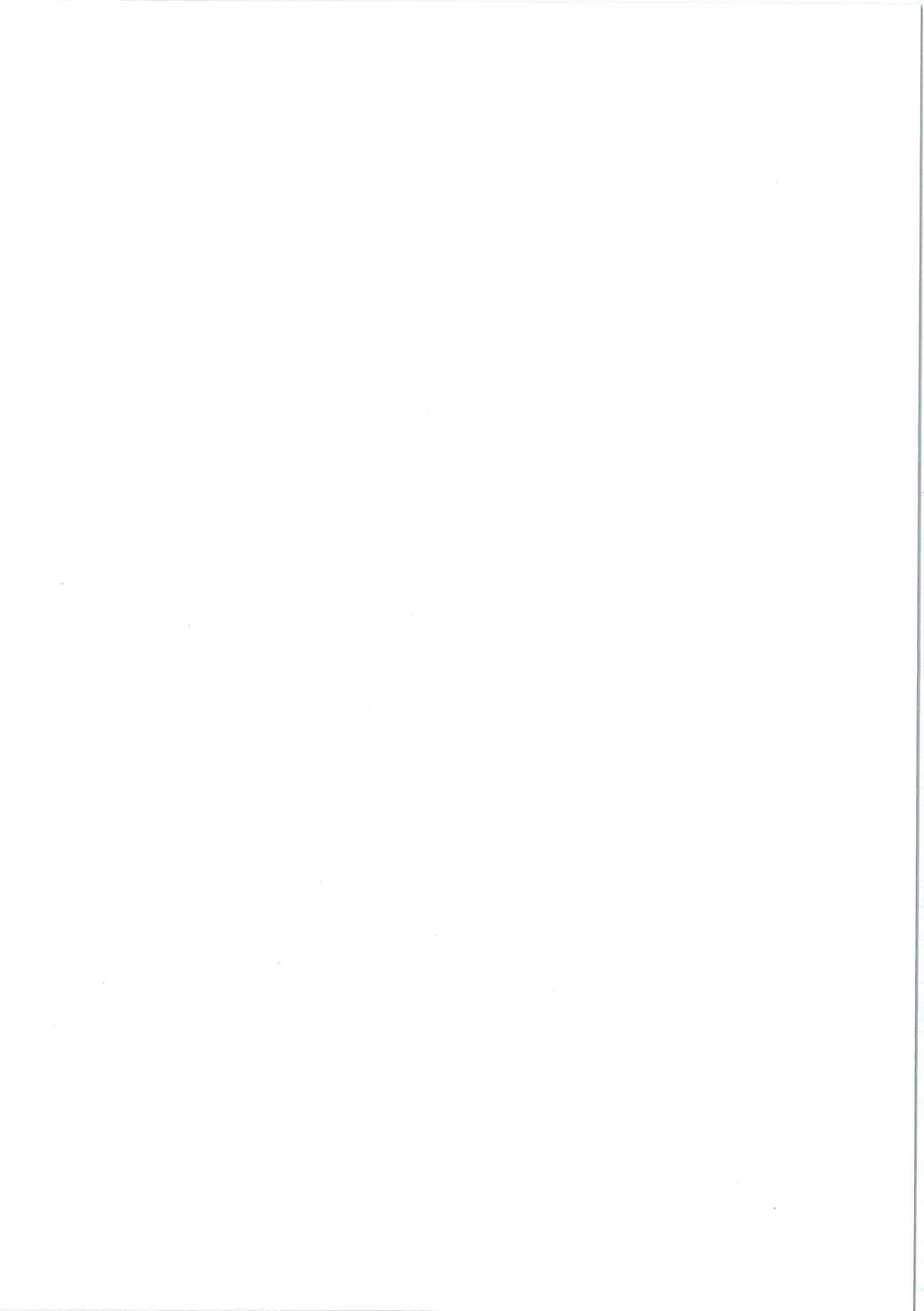
The screenshot shows the 'Sus aplicaciones' (Your apps) section of the Microsoft Office 365 portal. At the top, there's a search bar and a 'Instalar Office' (Install Office) button. Below the header, there are two main sections: 'Todas sus aplicaciones' (All your apps) and 'Office 365'. The 'Office 365' section lists various applications with their descriptions and 'Obtener más información' (Get more information) links:

- Admin.** Su portal web de administración (para administrar las cuentas de usuario y la configuración de cada suscripción). [Obtener más información →](#)
- Calendario.** Planea y comparte horas de reuniones y eventos, y obtenga avisos automáticos. [Obtener más información →](#)
- Class Notebook.** Organice su programa de lecciones y el contenido del curso en un bloc de notas digital propio. Cree un área de trabajo donde pueda proporcionar información personalizada a cada alumno. [Obtener más información →](#)
- Contactos.** Organice la información de contacto de todos sus amigos, familia, compañeros de trabajo y conocidos en un solo lugar. Mantenerse en contacto es más rápido que nunca. [Obtener más información →](#)
- Cumplimiento.** Cumple las normas legales, reguladoras y técnicas de tu organización relativas al uso de los datos y la seguridad de los contenidos. [Obtener más información →](#)
- Dynamics 365.** Rompa las barreras entre las aplicaciones y los procesos empresariales con Microsoft Dynamics 365. [Obtener más información →](#)
- Excel.** Consiga mejores resultados con la herramienta que ya conoce. Descubra datos, córtese a ellos, modélelos, analícelos y visualice las conclusiones. [Obtener más información →](#)
- Flow.** Crea flujos de trabajo entre aplicaciones, archivos y datos para automatizar las tareas largas y centrarse en las siguientes. [Obtener más información →](#)
- Forms.** Cree encuestas, cuestionarios y sondeos en cuestión de minutos. Envíelos a todos los usuarios y vea los resultados en tiempo real. [Obtener más información →](#)
- Kaiwala.**
- OneDrive.** Almacene los archivos en un solo lugar, compártalos con otros usuarios y obtenga acceso a ellos desde cualquier dispositivo conectado a Internet. [Obtener más información →](#)
- OneNote.** Capture notas tecleando, dibujando o escribiendo. OneNote le permite organizar y reutilizar las notas en todos los dispositivos. [Obtener más información →](#)
- Outlook.** Use un correo electrónico de categoría empresarial con la experiencia satisfactoria y conocida de Outlook; a la que puede obtener acceso desde un equipo de escritorio o un explorador web. [Obtener más información →](#)
- Planner.** Crea planes, organiza y asigna tareas, comparte archivos, chatea sobre aquello en lo que esté trabajando y obtenga actualizaciones del progreso con Planner. [Obtener más información →](#)
- PowerApps.** Crea aplicaciones móviles y web con los datos que tu organización ya usa. [Obtener más información →](#)
- PowerPoint.** Aumenta la calidad de sus presentaciones. Diseña de forma profesional. [Obtener más información →](#)
- Seguridad.**
- Staff Notebook.** Colabore con los profesores y con el personal para compartir notas, directivas, procedimientos, fechas límite y calendarios. [Obtener más información →](#)
- Stream.** Comparte videos de clases, reuniones, presentaciones, sesiones de aprendizaje u otros videos con los miembros de su empresa o centro académico. [Obtener más información →](#)
- Sway.** Cree y comparta informes, presentaciones, historias personales y otros documentos que sean atractivos e interactivos. Sway se encargará del diseño. [Obtener más información →](#)
- Tareas.** Crea y administra las tareas en Outlook. [Obtener más información →](#)
- Teams.** El espacio de trabajo para equipos personalizable y basado en chat de Office 365. [Obtener más información →](#)
- To-Do.** Administre, priorice y complete las tareas más importantes que necesita realizar cada día. [Obtener más información →](#)
- Word.** Escriba mejor que nunca. Pase de una página en blanco a un documento perfecto sin apenas esfuerzo. [Obtener más información →](#)
- Yammer.** Póngase en contacto con las personas adecuadas, comparta información con los equipos y organícelos los proyectos con los compañeros. [Obtener más información →](#)

At the bottom, there are sections for 'Otras' (Other) and 'Microsoft Educator Community'.

## ANEXO II







I

La consulta plantea, en primer lugar, si resulta necesario el consentimiento de los padres de alumnos de edades que podrían llegar a un mínimo de diez años de edad para la creación a los mismos de una cuenta de correo electrónico en el marco de la implantación e un programa “que impulsa el empleo de las nuevas tecnologías en las aulas”.

Como punto de partida, debe indicarse que la legislación de protección de datos no resulta en sí misma aplicable de modo directo a la creación de una cuenta de correo electrónico. No obstante, dicha creación y el uso de dicha cuenta implicará el tratamiento por parte del prestador de ese servicio de los datos de carácter personal del usuario, lo que hace que sí hayan de ser tenidas en cuenta las mencionadas normas.

Dicho esto, si se parte del hecho de que el Programa es de implantación necesaria en el ámbito de la administración educativa de la Comunidad Autónoma, sería preciso tener en cuenta que el artículo 6.1 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal, dispone que “El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa”, añadiendo el artículo 6.2 que dicho consentimiento no será preciso cuando los datos “se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento”.

Teniendo esto en cuenta, de los escuetos términos de la consulta parece desprenderse que es uno de los objetivos del programa la implantación del uso de las nuevas tecnologías en el ámbito escolar, siendo así necesario para un verdadero cumplimiento de dicho objetivo la creación de las mencionadas cuentas, por lo que podría entenderse que el tratamiento resulta necesario para el adecuado desarrollo de la relación jurídica que vincula al alumno con el centro escolar, no siendo así necesario su consentimiento para el tratamiento de tales datos.

Ahora bien, la conclusión que acaba de alcanzarse legitimaría el tratamiento en el supuesto en que los datos referidos a la atribución y el empleo de la relación de correo electrónico se lleven exclusivamente a cabo para el adecuado mantenimiento o cumplimiento de la relación que vincula al alumno con el centro. De este modo, debería recaer sobre el propio centro o sobre la administración educativa de la Comunidad Autónoma la responsabilidad por el mencionado tratamiento, que sólo podría llevarse a cabo para el cumplimiento de los fines que se han venido describiendo y que se



encuentran directamente vinculados a las competencias de la Administración educativa y del centro al que asista el menor.

Lo que acaba de indicarse resulta especialmente relevante si se tiene en cuenta el hecho de que la consulta plantea la posible apertura de cuentas de correo electrónico referidas a determinados “proveedores de este tipo de servicios”.

Atendiendo a lo que acaba de indicarse, para que ello sea posible, los mencionados proveedores deberían mantener en relación con el tratamiento de datos derivados de la apertura de cuentas de correo la condición de encargado del tratamiento, siendo de aplicación a los mismos el régimen establecido en el artículo 12 de la Ley Orgánica 15/1999 y en la Sección Tercera del Capítulo II de su Reglamento de desarrollo, aprobado por Real decreto 1720/2007, de 21 de diciembre.

En particular, debe recordarse que, conforme dispone el artículo 12.2 de la Ley Orgánica “La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas”, añadiendo el precepto que “En el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 de esta Ley que el encargado del tratamiento está obligado a implementar”.

Asimismo, el artículo 12.4 dispone que “En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado, también, responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personal”.

La cuestión se plantea por el hecho de que las condiciones generales de privacidad de los proveedores de estos servicios, y en particular de los que se citan en la consulta, suelen implicar el tratamiento de datos de los titulares de las cuentas para determinadas finalidades que en ningún caso podrían encajar entre las que justificarían el tratamiento de los datos sin consentimiento de los mencionados titulares, pudiendo en particular hacerse referencia al posible uso de los datos para finalidades relacionadas con la remisión publicitaria asociada al correo recibido o enviado.

De este modo, en tanto los proveedores del servicio empleasen los datos para estas finalidades, su posición jurídica no podría ser la de encargado del tratamiento, generándose una relación directa entre aquéllos y el interesado que otorgaría a los mismos la condición de responsable, tal y como determina



el artículo 20.1, párrafo último, del Reglamento de desarrollo de la Ley Orgánica 15/1999, así como el ya citado artículo 12.4 de la Ley Orgánica 15/1999.

Ello sí exigiría que los interesados debieran prestar su consentimiento para el tratamiento de sus datos asociados a la creación de la cuenta de correo electrónico, en lo que se refiere a cualquier uso de los datos que excediera de la relación entre el alumno y el Centro o la Administración Educativa, procediendo la aplicación de las normas legales y reglamentarias relativas a la prestación del mencionado consentimiento.

En particular, dado que la consulta se refiere a alumnos que podrían tener la edad de diez años, debería tenerse en cuenta que conforme al artículo 13.1 del Reglamento "Podrá procederse al tratamiento de los datos de los mayores de catorce años con su consentimiento, salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela. En el caso de los menores de catorce años se requerirá el consentimiento de los padres o tutores".

De este modo, sí podría resultar necesario el mencionado consentimiento de los padres o tutores del menor en caso de que el servicio sea prestado por un proveedor de servicios de Internet que no fuera a limitar su actuación a la mera prestación del servicio a la Administración autonómica.

Por todo ello, y en relación con esta primera cuestión, sería conveniente que las direcciones fueran otorgadas por la propia Administración autonómica y no atribuidas en relación con un prestador de servicios de la sociedad de la información cuya política de privacidad implique el tratamiento de datos que excede de la finalidad pretendida, no resultando necesario, en caso de atribuirse las cuentas directamente por la Administración, el consentimiento del interesado ni de sus representantes legales.

## II

En segundo lugar, la consulta plantea quién será responsable del tratamiento en relación con el uso por los centros privados y concertados de una aplicación informática, alojada en los servidores de la Administración autonómica, con distintos grados de acceso en virtud del colectivo afectado y en que se incluyen datos relacionados con distintas cuestiones.

Ante todo, es preciso indicar que los términos de la consulta no permiten analizar detenidamente el funcionamiento o las funcionalidades de la aplicación, ni los grados o rangos de acceso a la misma. Asimismo, se desconoce si la aplicación implica el acceso y uso de los datos por parte de la propia administración educativa autonómica o si en la práctica se está únicamente haciendo referencia a la creación por dicha administración de una



aplicación que podrá ser empleada por los centros, incluso con carácter preceptivo en relación con los de titularidad pública y los concertados.

No obstante, de los términos de la consulta parece, efectivamente, desprenderse que nos encontramos simplemente ante la creación y alojamiento de la mencionada aplicación, que será directamente empleada en el ámbito de cada uno de los centros.

En ese caso, sería aplicable la doctrina ya sostenida por la Agencia en relación con casos similares, pudiendo hacerse referencia al informe de 16 de junio de 2008, en que se señalaba, con expresa referencia a la normativa aplicable a dicha Comunidad, que debería analizarse para el caso de la ahora consultante, lo siguiente:

*"La Orden de 20 de julio de 2006, de la Consejería de Educación de Andalucía, por la que se regulan los ficheros automatizados con datos de carácter personal gestionados por la Consejería de Educación en el ámbito de los sistemas SÉNECA y PASEN, señala en su Anexo I que dichos sistemas "proporcionan la infraestructura técnica para el manejo de la información académica y de gestión de los centros educativos dependientes de la Consejería de Educación de la Junta de Andalucía", añadiendo que "esto incluye a los centros educativos de carácter público de la Comunidad y a los centros educativos concertados que utilizan estos sistemas para el soporte de determinados procesos de gestión".*

*En consecuencia, debe diferenciarse entre los ficheros de datos regulados por la citada Orden y los propios sistemas SÉNECA y PASEN, definidos por el propio texto como herramientas de manejo de la información y gestión académica de los centros integrados en el sistema educativo público de la Comunidad Autónoma.*

*En este sentido, el artículo 3.1 de la Ley 17/2007, de 10 de diciembre, de Educación de Andalucía establece que "el Sistema Educativo Público de Andalucía es el conjunto de centros, servicios, programas y actividades de las administraciones públicas de la Comunidad Autónoma o vinculados a las mismas, orientados a garantizar el derecho de la ciudadanía a una educación permanente y de carácter compensatorio, reconocido en el artículo 21.1 del Estatuto de Autonomía para Andalucía", añadiendo el apartado 3 que el Sistema está compuesto por los centros docentes públicos de titularidad de la Junta de Andalucía o de las Corporaciones Locales u otras Administraciones Públicas, así como por los centros docentes privados concertados, sin perjuicio de la legislación específica que pudiera resultar de aplicación a los mismos.*

*Dentro del ámbito competencial de la mencionada Comunidad Autónoma, la Ley 17/2007 contiene en su Título V determinadas previsiones tendentes a uniformar la gestión de los procesos*



*automatizados de datos por parte de los centros integrados en el Sistema Público.*

Así, el artículo 142.1 dispone que “la Administración educativa favorecerá el funcionamiento en red de los centros educativos, con objeto de compartir recursos, experiencias e iniciativas y desarrollar programas de intercambio de alumnado y profesorado”.

Por su parte, conforme al artículo 151 “La Administración educativa facilitará e impulsará la realización de trámites administrativos a través de Internet, así como la relación electrónica de la ciudadanía con los centros docentes. A tales efectos, se prestará especial atención a los procedimientos de escolarización y matriculación del alumnado, así como a los que realizan los miembros de la comunidad educativa, particularmente el profesorado”.

De lo dispuesto en la Orden de creación de ficheros y la Ley 17/2007 se desprende, como se ha venido indicando que los sistemas SÉNECA y PASEN se configuran como herramientas encaminadas a facilitar y agilizar los trámites relacionados con la gestión de los centros integrados en el Sistema Educativo Público de Andalucía, debiendo en consecuencia diferenciarse entre el propio sistema, como aplicación puesta a disposición de los Centros por la Administración Autonómica, en desarrollo de los artículos 142.1 y 151 de la Ley, de los propios ficheros previstos en la Orden o aquellos de los que en uso de la aplicación sean creados y gestionados por los centros integrados en el sistema.

De este modo, la situación es en principio similar a la de los sistemas de información existentes en otras áreas de actividad cuya competencia corresponda al sector público. Así, en principio, no cabría apreciar diferencia entre los sistemas analizados y otros que fueran desarrollados, por ejemplo, para la gestión de las historias clínicas en el ámbito del Sistema sanitario de una determinada Comunidad Autónoma o los que fueran desarrollados por un determinado departamento para la gestión de recursos humanos o la gestión presupuestaria de los restantes Departamentos integrantes de dicha Administración.

Consecuencia de lo que acaba de indicarse es que los Centros concertados, dotados de personalidad enteramente independiente de la Administración educativa autonómica serán responsables de los ficheros relacionados con la utilización de la herramienta o sistema informático puesto a su disposición, siendo tales ficheros diferentes de los creados expresamente para el ámbito de la Administración Pública por su propia Orden de creación.”



La conclusión mantenida en el citado informe sería igualmente extrapolable a los centros privados, que ostentarían igualmente la condición de responsable del tratamiento.

Asimismo, y teniendo en cuenta que la consulta indica que la aplicación se alojaría en los propios servidores de la Comunidad Autónoma, la misma actuaría en relación con el uso de la aplicación por los centros privados y concertados como encargada del tratamiento, debiendo dar cumplimiento a lo dispuesto en el artículo 12 de la Ley Orgánica y en los artículos 20 a 22 de su Reglamento de desarrollo.

## ANEXO III







**RESOLUCIÓN DE DECLARACIÓN DE ADECUACIÓN DE GARANTÍAS PARA LAS TRANSFERENCIAS INTERNACIONALES DE DATOS A LOS ESTADOS UNIDOS CON MOTIVO DE LA PRESTACIÓN DE SERVICIOS DE COMPUTACIÓN EN NUBE**

Nº Expediente: TI/00032/2014

Vista la solicitud formulada por D. A.A.A., en nombre y representación de la compañía MICROSOFT CORPORATION, y presentada ante esta Agencia Española de Protección de Datos (AEPD), y teniendo en cuenta los siguientes

**ANTECEDENTES DE HECHO**

**Primero.-** Con fecha 12 de febrero de 2014, la entidad MICROSOFT CORPORATION presentó un escrito en el que expone que presta los servicios de computación en nube (cloud computing) denominados: OFFICE 365, MICROSOFT DYNAMICS CRM ONLINE y WINDOWS AZURE (en adelante MOS: MICROSOFT ONLINE SERVICES) a través de MICROSOFT IRELAND OPERATIONS LIMITED (MIOL), establecida en Irlanda, que ofrece a los clientes la firma, junto con el correspondiente contrato comercial, de un acuerdo de tratamiento de datos.

Que los servicios MOS son prestados por MIOL por sí mismo o a través de subcontratistas, siendo Microsoft Corporation, sociedad matriz del Grupo Microsoft establecida en los Estados Unidos, el subcontratista principal que, a su vez, presta los servicios por sí misma o a través de subcontratistas que pueden estar situados fuera del Espacio Económico Europeo (EEE).

Que, con la finalidad de aportar las garantías suficientes para las transferencias de datos a MICROSOFT CORPORATION y a sus subcontratistas, ofrece a sus clientes la posibilidad de firmar las cláusulas contractuales tipo, adoptadas por la Comisión Europea en su Decisión 2010/87/UE, y un acuerdo suplementario a dichas cláusulas para adecuar a las características de los servicios de computación en nube la realización de las auditorías de las actividades de tratamiento y la subcontratación de operaciones de tratamiento con subencargados ulteriores del tratamiento.

Aporta un ejemplar de cada uno de los documentos que conforman el esquema de garantías contractuales y solicita que, al amparo de lo dispuesto en los artículos 33 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) y 70.2 de su Reglamento de desarrollo, aprobado por el Real Decreto 1720/2007, de 21 de diciembre (RLOPD), por el Director de la AEPD se declare que las garantías establecidas en la documentación que presenta son adecuadas para realizar



transferencias de datos personales a los Estados Unidos y que los clientes que contraten los servicios MOS y suscriban los contratos aportados queden autorizados a realizarlas siempre y cuando las notifiquen previamente al Registro General de Protección de datos (RGPD).

**Segundo.-** La solicitud formulada por Microsoft Corporation incluye la siguiente documentación:

- Acreditación de la representación que ostenta la persona que actúa en nombre de Microsoft Corporation
- Acuerdo de tratamiento de datos para la contratación de los servicios Office 365 y Microsoft Dynamics CRM Online, a suscribir entre el cliente, responsable del tratamiento, y MIOL
- Acuerdo de tratamiento de datos para la contratación de los servicios Windows Azure, a suscribir entre el cliente, responsable del tratamiento, y MIOL
- Modelo de contrato que incluye las cláusulas contractuales tipo adoptadas por la Decisión de la Comisión Europea 2010/87/UE para la contratación de los servicios Office 365 y Microsoft Dynamics CRM Online, a suscribir entre el cliente, responsable del tratamiento exportador de datos, y Microsoft Corporation
- Modelo de contrato que incluye las cláusulas contractuales tipo adoptadas por la Decisión de la Comisión Europea 2010/87/UE para la contratación de los servicios Windows Azure, a suscribir entre el cliente, responsable del tratamiento exportador de datos, y Microsoft Corporation
- Acuerdo suplementario a las cláusulas contractuales tipo para la contratación de todos los servicios MOS, a suscribir entre el cliente, responsable del tratamiento exportador de datos, y Microsoft Corporation

**Tercero.-** Los detalles de las transferencias a las que se refiere la solicitud se especifican en el apéndice 1 de las cláusulas contractuales tipo y en el acuerdo suplementario, y se exponen a continuación:

- a) Cláusulas contractuales tipo adoptadas por la Decisión de la Comisión Europea 2010/87/UE para la contratación de los servicios Office 365 y Microsoft Dynamics CRM Online y acuerdo suplementario:
  - El exportador será un cliente de los servicios online
  - El importador es Microsoft Corporation, compañía establecida en EEUU
  - Las categorías de interesados y de datos personales se entienden comprensivas de toda persona física identificada o identificable cuyos datos personales sean tratados por el cliente en los servicios online
  - Los datos personales a transferir incluyen datos especialmente protegidos, de cualquier sensibilidad
  - Los datos personales transferidos serán sometidos a las siguientes operaciones básicas de tratamiento: los datos del cliente serán objeto de las operaciones de tratamiento asociadas a los servicios online contratados, incluyendo, entre otras, el almacenamiento, acceso y su transmisión.



b) Cláusulas contractuales tipo adoptadas por la Decisión de la Comisión Europea 2010/87/UE para la contratación de los servicios Windows Azure y acuerdo suplementario:

- El exportador será un cliente usuario de los servicios Core Platform
- El importador es Microsoft Corporation, compañía establecida en EEUU
- Las categorías de interesados y de datos personales se entienden comprensivas de toda persona física identificada o identifiable cuyos datos personales sean tratados por el cliente en los servicios online
- Los datos personales a transferir incluyen datos especialmente protegidos, de cualquier sensibilidad
- Los datos personales transferidos serán sometidos a las siguientes operaciones básicas de tratamiento: los datos del cliente serán objeto de las operaciones de tratamiento asociadas a los servicios Core Platform contratados, incluyendo, entre otras, el almacenamiento, acceso y su transmisión.

## FUNDAMENTOS DE DERECHO

### I

Es competente para dictar la presente resolución el Director de la Agencia Española de Protección de Datos conforme a lo dispuesto en el artículo 33 y 37.1.l) de la LOPD.

### II

En la tramitación del presente procedimiento se han observado las normas previstas en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común y en los artículos 137 y siguientes del RLOPD.

### III

El supuesto objeto de análisis en la presente resolución reviste ciertas especialidades respecto de los que han venido tradicionalmente siendo objeto de resoluciones de autorización de transferencias internacionales de datos. Ello se debe, en primer lugar, al hecho de que la documentación que ha de ser analizada ha sido presentada no por el exportador, sino por el importador de datos personales. Además, dicha documentación, formada por los correspondientes contratos relacionados con los servicios mencionados al comienzo de esta resolución, sus respectivos acuerdos suplementarios y adendas sobre el tratamiento de datos de carácter personal, se refiere a las garantías establecidas con carácter general en los supuestos de contratación de los servicios de computación en nube prestados por MIOL, sin hacer mención de un supuesto concreto de transferencia internacional de datos.

De este modo, el objeto de la presente resolución no puede ser la autorización de una concreta transferencia internacional, sino la determinación de si las garantías contenidas en la documentación aportada por Microsoft Corporation pueden considerarse adecuadas para permitir la realización de una transferencia internacional de datos en caso de que las mismas sean efectivamente cumplimentadas por los exportadores de datos que



pretendan la contratación con MIOL de los servicios de computación en nube a los que los contratos, siempre completados con su respectivos acuerdos suplementarios, se refieren.

A este respecto cabe señalar que el artículo 33.1 de la LOPD establece como norma general que *"No podrán realizarse transferencias temporales ni definitivas de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento con destino a países que no proporcionen un nivel de protección equiparable al que presta la presente Ley, salvo que, además de haberse observado lo dispuesto en ésta, se obtenga autorización previa del Director de la Agencia Española de Protección de Datos, que sólo podrá otorgarla si se obtienen garantías adecuadas"* y el artículo 37.1.l) LOPD atribuye a la AEPD la función de *"ejercer el control y adoptar las autorizaciones que procedan en relación con los movimientos internacionales de datos,..."*.

De este modo, nada obsta a que por parte de esta Agencia pueda valorarse y resolverse si un determinado marco contractual, en el que se establezcan las distintas salvaguardas para que un cierto importador de datos de carácter personal proceda al tratamiento de aquéllos a los que el contrato se refiera, pueda incorporar garantías adecuadas a los efectos de permitir las futuras transferencias de datos que se lleven a cabo en el ámbito estricto de ese marco contractual.

Por este motivo, la presente resolución no podrá proceder automáticamente a la autorización de las transferencias internacionales de datos que fueran a llevarse a cabo, al no aparecer individualizada la entidad responsable que actuará en la transferencia como exportadora de los datos de carácter personal, pero sí podrá determinar si las transferencias que pudieran tener lugar conforme a las cláusulas sometidas al parecer de esta Agencia proporcionan las garantías suficientes para que una determinada transferencia internacional, realizada cumpliendo aquéllas, pueda considerarse merecedora de la correspondiente autorización, sin que para ello sea necesario recabar nuevamente el parecer de esta Agencia sino simplemente proceder a su notificación a la misma

#### IV

La entidad interesada manifiesta que es un prestador de servicios de computación en nube que ofrece a sus clientes la posibilidad de suscribir un conjunto de contratos para que, en los supuestos en los que se vayan a tratar datos de carácter personal, se aporten las garantías suficientes que permitan el flujo de datos a los Estados Unidos, país que no está declarado con un nivel de protección adecuado, y solicita que la Agencia Española de Protección de Datos considere que las transferencias internacionales de datos que como consecuencia de la contratación de los servicios MOS se realicen con destino a los Estados Unidos, utilizando el esquema de garantías que presenta, queden autorizados por proporcionar un nivel de protección suficiente.

La contratación de cualquier servicio MOS se realiza por el cliente, responsable del tratamiento, con Microsoft Ireland Operations Limited (MIOL), establecida en Irlanda, que actúa como encargado del tratamiento por lo que, junto al contrato comercial, ambas partes suscriben un acuerdo de tratamiento de datos. Aportan dos modelos de acuerdo, uno para los servicios Office 365 y Microsoft Dynamics CRM Online y otro para los



servicios de Windows Azure, en los que se contienen los extremos establecidos en el artículo 17 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos y en el 12 de la LOPD, así como la autorización del cliente para la subcontratación de los servicios prestados por MIOL y la posibilidad de que sean transferidos, así como conservados y tratados, a los Estados Unidos.

Así mismo, ofrecen al cliente la posibilidad de firmar con Microsoft Corporation, como importador de datos, las cláusulas contractuales tipo adoptadas por la Comisión Europea en su Decisión 2010/87/UE, que en su apéndice 1 establece los detalles de la transferencia de manera específica, por una parte, para los servicios Office 365 y Microsoft Dynamics CRM Online y, por otra, para los servicios de Windows Azure, y un acuerdo suplementario con la finalidad de adecuar a las características de los servicios de computación en nube la realización de las auditorías de las actividades de tratamiento cubiertas por las cláusulas y la subcontratación con subencargados ulteriores del tratamiento.

En este punto, debe tenerse en cuenta lo señalado por el Grupo de Trabajo creado por el artículo 29 de la Directiva 95/46/CE en su Dictamen 05/2012 sobre la computación en nube, adoptado el 1 de julio de 2012 (WP 196), en cuyo apartado 3.3.1 se señala lo siguiente:

*"El cliente determina el objetivo último del tratamiento y decide sobre la externalización de este tratamiento y la delegación de la totalidad o de parte de las actividades de tratamiento a una organización externa. El cliente actúa por tanto como responsable del tratamiento. La Directiva define al responsable del tratamiento como «la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que sólo o conjuntamente con otros determine los fines y los medios del tratamiento de datos personales». El cliente, como responsable del tratamiento, debe aceptar la responsabilidad de respetar la legislación sobre protección de datos, y es responsable y está sujeto a todas las obligaciones legales que figuran en la Directiva 95/46/CE. El cliente podrá encargar al proveedor que elija los métodos y medidas técnicas y de organización adecuados para alcanzar los fines del responsable del tratamiento."*

*"El proveedor es la entidad que presta los servicios de computación en nube de las distintas formas que se han mencionado. Cuando el proveedor suministra los medios y la plataforma, actuando en nombre del cliente, se considera que es el encargado del tratamiento es decir, con arreglo a la Directiva 95/46/CE, «la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento»."*

Añade específicamente el Dictamen que *"el responsable del tratamiento debe elegir un proveedor que garantice el cumplimiento de la legislación sobre protección de datos. Debe prestarse una atención especial a las características de los contratos, que deberán incluir una serie de garantías de protección de datos normalizadas, incluidas las señaladas por el Grupo de Trabajo en el punto 3.4.3 (Medidas técnicas y de organización) y en el punto 3.5 (Flujos de datos transfronterizos), así como cualesquiera mecanismos adicionales que puedan resultar adecuados para facilitar la diligencia debida"*



y la responsabilidad (como auditorías de terceros independientes y certificaciones de los servicios de un proveedor – véase el apartado 4.2)”. Y concluye lo siguiente:

*“Los proveedores (como encargados del tratamiento) tienen la obligación de garantizar la confidencialidad. La Directiva 95/46/CE establece que: «Las personas que actúen bajo la autoridad del responsable o del encargado del tratamiento, incluido este último, solo podrán tratar datos personales a los que tengan acceso, cuando se lo encargue el responsable del tratamiento o salvo en virtud de un imperativo legal». El acceso a los datos por parte del proveedor durante la prestación de servicios también se rige fundamentalmente por el requisito de cumplir las disposiciones del artículo 17 de la Directiva – véase el apartado 3.4.2.*

*Los encargados del tratamiento deben tener en cuenta el tipo de nube en cuestión (pública, privada, comunitaria o híbrida / IaaS, SaaS o PaaS [véase el anexo A) Modelos de implantación - b) Modelos de prestación de servicios]) y el tipo de servicio contratado por el cliente. Los encargados del tratamiento son responsables de la adopción de las normas de seguridad, de conformidad con las disposiciones de la legislación de la UE aplicadas en las jurisdicciones del responsable y del encargado del tratamiento. Los encargados del tratamiento deben también apoyar y asistir al responsable del tratamiento a respetar los derechos (ejercidos) de los interesados”*

De este modo, la transferencia internacional que se plantea a partir de la documentación presentada debe reunir los requisitos necesarios para la transmisión transfronteriza de datos de un responsable del tratamiento (el exportador, cliente de los servicios) a un encargado del tratamiento (la entidad prestadora de los servicios de computación en nube). Por este motivo, se considera que la adopción, como base esencial de la transferencia, de las cláusulas contractuales contenidas en el Anexo de la Decisión 2010/87/UE puede considerarse adecuada.

## V

El artículo 1 de la citada Decisión dispone que “se considerará que las cláusulas contractuales tipo incluidas en el anexo ofrecen las garantías adecuadas con respecto a la protección de la vida privada y de los derechos y libertades fundamentales de las personas, así como respecto al ejercicio de los correspondientes derechos, según exige el artículo 26, apartado 2 de la Directiva 95/46/CE”. Y el primer inciso del primer párrafo del artículo 2 añade que “La presente Decisión aborda únicamente la adecuación de la protección otorgada por las cláusulas contractuales tipo establecidas en el anexo para la transferencia de datos personales a los encargados del tratamiento”.

La documentación aportada introduce, no obstante determinadas especialidades en el contenido de la relación contractual entre el cliente de los servicios y el importador de datos, referidas esencialmente a la realización de auditorías y a la posible subcontratación de servicios de computación en nube. Ello impide valorar de una forma directa si el conjunto del clausulado cumple efectivamente con las garantías exigidas por la citada Decisión, dado que una modificación en las cláusulas tipo no permite entender de una forma directa que las mismas se siguen ajustando a los estándares adoptados por la Comisión.



Así, por lo que respecta a las auditorías, la cláusula 5.f) de la Decisión 2010/87/UE estipula que el importador “*ofrecerá a petición del exportador de datos sus instalaciones de tratamiento de datos para que se lleve a cabo la auditoría de las actividades de tratamiento cubiertas por las cláusulas*” y que “*será realizada por el exportador de datos o por un organismo de inspección compuesto por miembros independientes con las cualificaciones profesionales necesarias y sujetos a la confidencialidad, seleccionado por el exportador de datos...*”. A su vez, la cláusula 12.2 determina que “*El importador de datos y el subencargado garantizan que, a petición del exportador o de la autoridad de control, pondrá a disposición sus instalaciones de tratamiento de datos para que se lleve a cabo la auditoría de las medidas mencionadas en el apartado 1 (relativas a las obligaciones una vez finalizada la prestación de los servicios de tratamiento de datos personales).*

La segunda de las modificaciones de las cláusulas tipo de la Decisión 2010/87/UE afecta a lo estipulado en la cláusula 11, que dispone en su apartado 1 que “*El importador de datos no subcontratará ninguna de sus operaciones de procesamiento llevadas a cabo en nombre del exportador de datos con arreglo a las cláusulas sin previo consentimiento por escrito del exportador de datos. Si el importador de datos subcontrata sus obligaciones con arreglo a las cláusulas, con el consentimiento del exportador de datos, lo hará exclusivamente mediante un acuerdo escrito con el subencargado del tratamiento de datos, en el que se le impongan a este las mismas obligaciones impuestas al importador de datos con arreglo a las cláusulas. En los casos en que el subencargado del tratamiento de datos no pueda cumplir sus obligaciones de protección de los datos con arreglo a dicho acuerdo escrito, el importador de datos seguirá siendo plenamente responsable frente al exportador de datos del cumplimiento de las obligaciones del subencargado del tratamiento de datos con arreglo a dicho acuerdo*”. Por otra parte, en el documento de preguntas más frecuentes relacionadas con las cláusulas 2010/87/UE, adoptado el 12 de julio de 2010 por el Grupo de Trabajo del artículo 29, se analiza el modo en que debe ser interpretada dicha previsión señalando que la firma de un único contrato para los supuestos de contratación no sería posible en el contexto de las cláusulas.

El acuerdo suplementario a las cláusulas contractuales tipo introduce determinadas estipulaciones que, como más adelante se expone, modifican sustancialmente el contenido de las cláusulas establecidas en el citado Anexo, lo que impide que se produzca de modo automático el efecto previsto en el artículo 1 de la citada Decisión, lo que exigirá proceder a su valoración, a fin de determinar si pueden ser consideradas como garantías suficientes a los efectos establecidos en el artículo 33.1 de la LOPD.

No obstante, es preciso tener en cuenta que las cláusulas referidas a “Definiciones”, “Detalles de la transferencia”, “Cláusula de tercero beneficiario”, “Obligaciones del exportador de datos”, “Obligaciones del importador de datos”, salvo el apartado f) sobre la realización de auditorías que ha quedado modificado por el acuerdo suplementario, “Responsabilidad”, “Mediación y Jurisdicción”, “Cooperación con las autoridades de control”, “Legislación aplicable”, “Subtratamiento de datos”, con la interpretación que se le da en el acuerdo suplementario, y la relativa a las “Obligaciones una vez finalizada la prestación de servicios de tratamiento de los datos personales”, con la excepción de lo dispuesto en esta última cláusula sobre la realización de la auditoría, que igualmente se ha adecuado a las características de los servicios de computación en nube en el acuerdo suplementario a dichas cláusulas, son las mismas que las de la Decisión 2010/87/UE.



De este modo, y con las salvedades indicadas, que posteriormente se analizarán, los contratos vienen a incorporar en su mayor parte el clausulado de la citada Decisión, por lo que ha de considerarse que proporcionan las garantías que han sido consideradas adecuadas por dicha Decisión.

## VI

Como ya se ha indicado, y una vez se ha puesto de manifiesto que la mayor parte del clausulado aportado reproduce lo establecido en la Decisión 2010/87/UE, es preciso valorar a continuación si aquellos aspectos en los que las cláusulas se apartan de la literalidad del Anexo de dicha Decisión las garantías aportadas permiten que puedan seguir siendo adecuadas para que proceda autorizar las transferencias internacionales de datos basadas en las cláusulas que se están analizando.

El artículo 33.1 de la LOPD dispone que “*No podrán realizarse transferencias temporales ni definitivas de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento con destino a países que no proporcionen un nivel de protección equiparable al que presta la presente Ley, salvo que, además de haberse observado lo dispuesto en ésta, se obtenga autorización previa del Director de la Agencia de Protección de Datos, que sólo podrá otorgarla si se obtienen garantías adecuadas*”.

Por su parte, el artículo 70.1 del RLOPD dispone que “*Cuando la transferencia tenga por destino un Estado respecto del que no se haya declarado por la Comisión Europea o no se haya considerado por el Director de la Agencia Española de Protección de Datos que existe un nivel adecuado de protección, será necesario recabar la autorización del Director de la Agencia Española de Protección de Datos*”.

En atención a lo anterior, el artículo 70.2 del RLOPD estipula que: “*La autorización podrá ser otorgada en caso de que el responsable del fichero o tratamiento aporte un contrato escrito celebrado entre el exportador y el importador, en el que consten las necesarias garantías de respeto a la protección de la vida privada de los afectados y a sus derechos y libertades fundamentales y se garantice el ejercicio de sus respectivos derechos*”.

Exigencia de garantías suficientes cuyo origen se encuentra en el artículo 26.2 de la Directiva 95/46/CE, que dispone: “*...los Estados miembros podrán autorizar una transferencia o una serie de transferencias de datos personales a un tercer país que no garantice un nivel de protección adecuado con arreglo al apartado 2 del artículo 25, cuando el responsable del tratamiento ofrezca garantías suficientes respecto de la protección de la vida privada, de los derechos y libertades fundamentales de las personas, así como respecto al ejercicio de los respectivos derechos; dichas garantías podrán derivarse, en particular, de cláusulas contractuales apropiadas.*”

Se hace, por tanto, necesario valorar si las condiciones establecidas en los contratos presentados ofrecen esas garantías suficientes. Para ello hay que examinar si las estipulaciones del acuerdo suplementario a las cláusulas contractuales tipo de la Decisión 2010/87/UE, que las modifican en los dos aspectos señalados en el Fundamento de Derecho anterior, así como las incluidas en los acuerdos sobre el tratamiento de datos de



servicios MOS, que forman parte integrante del contrato, constituyen garantías suficientes.

## VII

En lo que respecta a la potestad del cliente, exportador de datos, de realizar la auditoría de las actividades de tratamiento que implica la transferencia internacional de datos o de seleccionar el auditor, el punto 2 del acuerdo suplementario a las cláusulas contractuales tipo indica que “*el cliente acepta ejercitar su facultad de auditoría prevista en las cláusulas 5 (f) y 12 (2) de las Cláusulas Contractuales Tipo instruyendo a Microsoft Corporation a llevar a cabo la auditoría según lo descrito en el Acuerdo de Tratamiento de Datos y sin perjuicio del derecho a cambiar esta instrucción, según se reconoce en el mismo, cuyas disposiciones se entienden incorporadas al presente Acuerdo Suplementario mediante esta referencia*”.

En el punto 4 b (ii) y 4 c (ii) de los acuerdos de tratamiento de datos para la contratación de los servicios Office 365 y Microsoft Dynamics CRM Online y Windows Azure, respectivamente (MOS) se indica que “*Microsoft auditará la seguridad de los ordenadores y el entorno de computación que utilice en el tratamiento de los Datos del Cliente (incluidos los datos personales) en los Servicios Online (Servicios Core Platform), así como los centros de datos físicos desde los que Microsoft presta los Servicios Online (todos los Servicios Windows Azure exceptuando Content Delivery Network). Esta auditoría: (a) se realizará al menos anualmente; (b) se ejecutará de acuerdo con los estándares ISO 27001; (c) será realizada por terceros profesionales en materia de seguridad, a elección y coste de Microsoft; (d) dará como resultado un informe de auditoría (“Informe de Auditoría Microsoft”), que constituirá información confidencial de Microsoft; y (e) podrá realizarse para otros fines adicionales al cumplimiento de esta cláusula (por ejemplo, como parte de los procedimientos habituales de Microsoft en materia de seguridad interna o para satisfacer otras obligaciones contractuales)*”.

A la vista de esta información, debe valorarse si resulta posible interpretar que la facultad de los clientes de MOS de auditar las actividades de tratamiento se entendería colmada satisfactoriamente, si las partes acuerdan en las cláusulas, la posibilidad de que la auditoría se lleve a cabo mediante la contratación por la consultante de un tercero independiente, que goce de las adecuadas garantías de independencia de la importadora y acreditación de las labores de control llevadas a cabo por la misma.

Esta cuestión ha sido analizada por el Grupo de Trabajo del artículo 29 en el apartado 4.2 de su documento WP196 al indicar: “la realización de auditorías individuales de datos alojados en un medio de servidores virtualizados con múltiples operadores puede ser poco práctica desde el punto de vista técnico y puede en algunos casos aumentar los riesgos para los controles físicos y lógicos de seguridad de las redes. En tales casos, podrá considerarse que la auditoría por un tercero de reconocido prestigio elegido por el responsable del tratamiento puede sustituir el derecho de un responsable del tratamiento de realizar una auditoría.

De este modo, tomando en cuenta los criterios sustentados por el Grupo de Trabajo del artículo 29 en el citado Dictamen (WP196) sería posible considerar que la auditoría a la que se refieren los documentos contractuales aportados por Microsoft Corporation podría



ser considerada una garantía adecuada para la transferencia de datos derivada de la contratación de un servicio de computación en nube prestada por la misma (MOS).

Como se ha reproducido, el acuerdo suplementario a la cláusulas contractuales tipo y los dos acuerdos sobre tratamiento de datos en los servicios online (MOS) incorporan la posibilidad de que el cliente acepte que sea el importador quien audite, al menos anualmente, la seguridad de los ordenadores y el entorno de computación que utilice el tratamiento de los datos del cliente, llevándose a cabo la auditoría por terceros profesionales en materia de seguridad y concediéndose al cliente, si así lo solicita, el acceso a la información mediante un resumen confidencial del informe de auditoría llevada a cabo. Asimismo, se indica que si el cliente desea cambiar esta instrucción acerca del ejercicio de su facultad de auditoría tiene derecho a hacerlo según lo mencionado en las cláusulas contractuales tipo, solicitándolo por escrito.

Por ello, cabe considerar que estas condiciones proporcionan garantías suficientes para la transmisión de datos a los Estados Unidos en el marco de la prestación de servicios de computación en nube a los que se refiere el presente expediente.

### VIII

La segunda de las modificaciones respecto a las cláusulas tipo contenidas en la Decisión 2010/87/UE se refiere a la subcontratación de la prestación de los servicios de tratamiento de datos, y se concreta en la posibilidad de llevar a cabo la firma de un único contrato con cada uno de los posibles subencargados del tratamiento, de modo que ese contrato cubra todos los tratamientos que éstos lleven a cabo respecto de los datos de los clientes del importador.

El apartado 3 del acuerdo suplementario a las cláusulas contractuales tipo señala a este respecto que "Microsoft Corporation podrá contratar a otras empresas para que presten servicios ilimitados en su nombre, tales como prestar servicios de soporte al Cliente. A cualquiera de estos subencargados únicamente se le permitirá obtener los Datos del Cliente para prestar los servicios que Microsoft Corporation le ha contratado que preste, y tendrá prohibido utilizar los Datos del Cliente con cualquier otra finalidad. Microsoft Corporation seguirá siendo responsable del cumplimiento de las obligaciones derivadas de las Cláusulas contractuales Tipo y del presente Acuerdo Suplementario por parte de sus subencargados. Todo subencargado al que Microsoft Corporation transfiera Datos del Cliente, incluso si es empleado con fines de conservación, habrá celebrado contratos por escrito con Microsoft Corporation que exijan que el subencargado cumpla unas condiciones no menos protectoras que las establecidas en las Cláusulas Contractuales Tipo y en el presente Acuerdo Suplementario; dichos contratos escritos también podrán ser de aplicación al tratamiento de datos de otros clientes. El Cliente ha consentido previamente que Microsoft Corporation transfiera los Datos del Cliente a los subencargados según lo descrito en las Cláusulas Contractuales Tipo y el presente Acuerdo Suplementario. Salvo por lo indicado más arriba o lo que el Cliente pueda autorizar de otro modo, Microsoft Corporation no transferirá a ningún tercero (ni siquiera con fines de conservación) datos personales que el Cliente proporcione a Microsoft Corporation a través del uso de los Servicios Online".

A su vez, en el apartado 3 e) de los acuerdos sobre tratamiento de datos en servicios MOS se estipula que cada servicio MOS dispone de un sitio web que enumera los



subcontratistas que están autorizados a acceder a los datos del cliente y que, al menos 14 días antes de autorizar que un nuevo subcontratista acceda a los datos del cliente, Microsoft actualizará el correspondiente sitio web y proporcionará al cliente un mecanismo para obtener la notificación de dichas actualizaciones. Añade dicho apartado que si el cliente no aprueba a un nuevo subcontratista aquél podrá dar por terminado el servicio MOS afectado sin penalización alguna, remitiendo por escrito, antes de que finalice el periodo de notificación, una notificación de terminación que incluya una explicación de los motivos de la aprobación, y si el servicio online forma parte de una suite, o similar fórmula de contratación conjunta de varios servicios, la terminación se aplicará a la suite completa.

Como cuestión previa, el artículo 21 del RLOPD regula la subcontratación de servicios por un encargado del tratamiento, señalando lo siguiente:

*"1. El encargado del tratamiento no podrá subcontratar con un tercero la realización de ningún tratamiento que le hubiera encomendado el responsable del tratamiento, salvo que hubiera obtenido de éste autorización para ello. En este caso, la contratación se efectuará siempre en nombre y por cuenta del responsable del tratamiento.*

*2. No obstante lo dispuesto en el apartado anterior, será posible la subcontratación sin necesidad de autorización siempre y cuando se cumplan los siguientes requisitos:*

*a) Que se especifiquen en el contrato los servicios que puedan ser objeto de subcontratación y, si ello fuera posible, la empresa con la que se vaya a subcontratar.*

*Cuando no se identificase en el contrato la empresa con la que se vaya a subcontratar, será preciso que el encargado del tratamiento comunique al responsable los datos que la identifiquen antes de proceder a la subcontratación.*

*b) Que el tratamiento de datos de carácter personal por parte del subcontratista se ajuste a las instrucciones del responsable del fichero.*

*c) Que el encargado del tratamiento y la empresa subcontratista formalicen el contrato, en los términos previstos en el artículo anterior.*

*En este caso, el subcontratista será considerado encargado del tratamiento, siéndole de aplicación lo previsto en el artículo 20.3 de este Reglamento".*

Una previsión similar se contiene en el apartado 1 de la cláusula 11 del Anexo de la Decisión 2010/87/UE, que impone al importador la necesidad de haber obtenido la autorización por escrito del exportador para que la subcontratación ulterior pueda tener lugar.

Por otra parte, el Dictamen del Grupo de Trabajo del artículo 29 (WP196), al que ya se ha hecho referencia, señala, dentro de las directrices para los clientes y proveedores de servicios de computación en nube, lo siguiente:

*"En los contratos entre proveedores y clientes deberán preverse disposiciones relativas a los subcontratistas. Los contratos deberán especificar que sólo podrá contratarse a subencargados del tratamiento previa autorización general del responsable del*



*tratamiento, en consonancia con la inequívoca obligación del encargado del tratamiento de informar al responsable de cualquier cambio previsto a este respecto, conservando el responsable del tratamiento en todo momento la posibilidad de oponerse a tales cambios o de rescindir el contrato. Debe existir una clara obligación para el proveedor de nombrar a todos los subcontratistas contratados. El proveedor deberá firmar un contrato con cada subcontratista que refleje las cláusulas de su contrato con el cliente; el cliente deberá asegurarse de que cuenta con posibilidades contractuales de recurso en caso de infracción del contrato por parte de los subcontratistas del proveedor (véase el punto 3.3.2)."*

Es decir, que si el cliente de los servicios MOS puede conocer la identidad de los subencargados y de las actividades que desplieguen no resultará un obstáculo el que la subcontratación se pueda acordar en un solo contrato con cada uno de los subcontratistas, siempre que el mismo especifique los servicios a prestar, y siempre que además se establezca un sistema que permita a los clientes conocer la identidad de los subencargados y su ubicación para el caso de transferencias ulteriores.

El acuerdo suplementario a las cláusulas contractuales incorpora la autorización del cliente para el uso de subencargados y, al propio tiempo, garantiza que los datos sólo se utilizarán para la prestación de los servicios subcontratados, con la prohibición de su utilización para cualquier otra finalidad, indicando expresamente que Microsoft Corporation es el responsable del cumplimiento de las cláusulas contractuales tipo y del acuerdo suplementario. Además, se añade expresamente que el subencargado habrá de firmar un contrato por escrito, que incluirá garantías no menos protectoras que las de las cláusulas tipo y el acuerdo suplementario.

Por otra parte, en los acuerdos sobre el tratamiento de datos, que forman parte de los contratos se estipula que cada servicio online dispone de un sitio web que enumera los subcontratistas que están autorizados a acceder a los datos del cliente. Al menos 14 días antes de autorizar que un nuevo subencargado acceda a los datos del cliente Microsoft actualizará el sitio web, y proporcionará una notificación a todos los clientes que se hayan suscrito a su recepción, y si el cliente no aprueba a un nuevo subcontratista podrá terminar el servicio online afectado sin penalización alguna remitiendo un escrito, antes de que finalice el periodo de notificación, explicando los motivos de la no aprobación.

Por todo ello, cabe considerar que las estipulaciones relativas a la subcontratación de los servicios de computación en nube que impliquen tratamiento de datos personales aportan garantías adecuadas para que el flujo de datos a los Estados Unidos pueda llevarse a cabo, conforme a lo establecido en el artículo 33.1 de la LOPD.

## IX

Al propio tiempo, no puede ignorarse que tanto el acuerdo suplementario a las cláusulas contractuales tipo como los acuerdos sobre tratamiento de datos de los servicios MOS vienen a especificar con mayor precisión una serie de extremos que constituyen las garantías contenidas en la Decisión 2010/87/UE, especificando aún más las obligaciones del prestador de servicios. En particular, y además de las garantías establecidas en materia de auditoría de seguridad y subcontratación de los servicios, que al apartarse de la literalidad de la citada Decisión han exigido un estudio detallado en la presente resolución, deben tenerse particularmente en cuenta las condiciones estipuladas en los



acuerdos sobre el tratamiento de datos en los servicios online (MOS) en lo que respecta a la seguridad de los datos, incluidos en su apartado 4, así como la referencia a la notificación de incidentes de seguridad a la que se refiere el apartado 5 de dicho documento.

Además, el punto 6 del acuerdo suplementario añade que "El Cliente reconoce y acepta que, con independencia de que la exportación de datos personales aquí contemplada esté amparada por la Autorización AEPD, el Cliente tiene imperativamente, según la normativa española sobre protección de datos, la obligación propia de notificar a la AEPD la modificación de su inscripción del fichero o ficheros, mediante notificación en la que indique que procede a la exportación de datos personales a Microsoft Corporation al amparo de la Autorización AEPD. Esta notificación deberá especificar necesariamente, según la mencionada normativa, el fichero o ficheros del Cliente respecto de los que utilizará los Servicios Online".

Todo ello conduce a la conclusión de que las garantías aportadas en los contratos remitidos, siempre que los mismos incorporen tanto el acuerdo suplementario como las correspondientes adendas que han sido objeto de presentación ante esta Agencia Española de Protección de Datos, reúnen las garantías adecuadas exigidas por el artículo 33.1 de la LOPD para que quepa considerar susceptibles de autorización las transferencias internacionales de datos que pudieran llevarse a cabo como consecuencia de esos documentos.

## X

La conclusión que acaba de alcanzarse conduce al necesario análisis de las consecuencias que pueden considerarse derivadas de esa declaración, toda vez que en el presente supuesto la valoración efectuada se lleva a cabo respecto del modelo contractual aportado y no en referencia a un supuesto concreto de transferencia internacional de datos de carácter personal.

Así, una vez consideradas adecuadas las garantías establecidas en el modelo contractual objeto de análisis en la presente resolución, la firma concreta del contrato por parte de un determinado cliente que pretenda la prestación de los servicios MOS a los que el modelo se refiere reuniría necesariamente las mismas garantías que se han valorado en la presente resolución.

De este modo, toda vez que el nivel adecuado de garantías ha sido suficientemente acreditado, la exigencia específica de una autorización individualizada de transferencia internacional de datos por cada uno de los clientes del servicio, siempre ajustada al artículo 33.1 de la LOPD en caso de reproducir ese marco contractual, ocasionaría una carga innecesaria al exportador solicitante, toda vez que la conclusión material del expediente resultaría prejuzgada por el contenido de esta resolución.

Por ello, establecido que las garantías aportadas son suficientes para llevar a cabo las transferencias internacionales de datos, parece razonable considerar que la declaración contenida en esta Resolución supone igualmente la autorización de las transferencias internacionales de datos que se lleven a cabo mediante la firma de las cláusulas contractuales analizadas, siempre que se observen una serie de requisitos:



- Las transferencias internacionales de datos deberán ajustarse a lo establecido en la presente resolución y en las cláusulas de los contratos presentados. Dichos contratos deberán incorporar el clausulado y la totalidad de los acuerdos suplementarios, anexos y adendas que han sido objeto de la presente resolución, dado que solamente en ese caso las garantías aportadas podrán considerarse suficientes con arreglo a la misma.
- El cliente, exportador de datos, deberá encontrarse en la situación de poder acreditar en todo momento ante esta Agencia que la transferencia se ha realizado con las garantías que aquí se han valorado, lo que exigirá la constancia documental de los contratos firmados con el prestador de servicio y con el importador de los datos.
- Con anterioridad a la realización de cualquier transferencia internacional de datos que pretenda ampararse en la presente resolución, el responsable del fichero deberá notificarla a la Agencia Española de Protección de Datos a fin de que se proceda a su inscripción en el Registro General de Protección de Datos, quedando identificados el fichero o ficheros a cuyos datos se refiera la transferencia internacional, con referencia a esta resolución.
- En todo caso, el alcance de la transferencia internacional de datos que se lleve a cabo deberá resultar ajustado a la estructura del fichero, categorías de datos y finalidades del tratamiento establecidas en la inscripción del correspondiente fichero, cuyos datos vayan a ser objeto de transferencia para la prestación del servicio.

## XI

Por último, debe recordarse que en todo caso, de conformidad con lo establecido en el artículo 70.3 del RLOPD, la transferencia o transferencias podrán denegarse o suspenderse temporalmente, con arreglo al procedimiento previsto en la sección segunda del capítulo V del Título IX del RLOPD, cuando concurra alguna de las circunstancias establecidas en el artículo 70.3 del citado Reglamento; es decir:

- a) Que la situación de protección de los derechos fundamentales y libertades públicas en el país de destino o su legislación impidan garantizar el íntegro cumplimiento del contrato y el ejercicio por los afectados de los derechos que el contrato garantiza.
- b) Que la entidad destinataria haya incumplido previamente las garantías establecidas en las cláusulas contractuales aportadas.
- c) Que existan indicios racionales de que las garantías ofrecidas por el contrato no están siendo o no serán respetadas por el importador.
- d) Que existan indicios racionales de que los mecanismos de aplicación del contrato no son o no serán efectivos.
- e) Que la transferencia, o su continuación, en caso de haberse iniciado, pudiera crear una situación de riesgo de daño efectivo a los afectados.

De manera que, no obstante la autorización concedida, la transferencia puede denegarse o suspenderse temporalmente si se diera alguna de estas circunstancias y sin perjuicio de las suspensiones que puedan acordarse de conformidad con lo estipulado en el contrato presentado.

En consecuencia, vistos los preceptos citados y demás de general aplicación, el Director



de la Agencia Española de Protección de Datos

## RESUELVE

**Primero.-** Considerar adecuadas las garantías establecidas en los modelos de contratos aportados por MICROSOFT CORPORATION para la transferencia internacional de datos con destino a dicha entidad, establecida en los Estados Unidos, con motivo de la prestación de los servicios OFFICE 365, MICROSOFT DYNAMICS CRM ONLINE y WINDOWS AZURE (MOS) y actuando como encargado del tratamiento.

**Segundo.-** Considerar autorizadas las transferencias internacionales de datos con destino a los Estados Unidos que se realicen al amparo de las cláusulas contractuales mencionadas, siempre que se cumplan las siguientes condiciones:

1. La finalidad de la transferencia será la prestación de los servicios OFFICE 365, MICROSOFT DYNAMICS CRM ONLINE y WINDOWS AZURE (MOS) por parte de MICROSOFT CORPORATION, actuando como encargado del tratamiento. Los datos se transfieren en las condiciones y con todas las garantías reseñadas en los Fundamentos de Derecho anteriores.
2. La autorización sólo podrá entenderse concedida en caso de que el contrato firmado entre los responsables exportadores de los datos y MICROSOFT CORPORATION incorpore la totalidad de los documentos que se han aportado para la adopción de la presente resolución para cada uno de los servicios a los que la misma se refiere.
3. El exportador de datos deberá notificar al RGPD los ficheros cuyos datos vayan a ser objeto de transferencia internacional con carácter previo, con indicación de su denominación y código de inscripción en el RGPD, indicando que se producirá la transferencia internacional de los datos al amparo de la presente resolución.
4. El alcance de la transferencia internacional de datos que se lleve a cabo deberá resultar ajustado a la estructura del fichero, categorías de datos y finalidades del tratamiento establecidas en la inscripción del correspondiente fichero.
5. El exportador de datos deberá poner a disposición de la AEPD, cuando le fueran requeridos, los contratos de prestación de servicios que haya suscrito con MICROSOFT IRELAND OPERATIONS LIMITED (MIOL) y MICROSOFT CORPORATION.
6. La autorización de transferencia internacional podrá denegarse o suspenderse cuando concurre alguna de las circunstancias recogidas en el artículo 70.3 del RLOPD; es decir:
  - a) Que la situación de protección de los derechos fundamentales y libertades públicas en el país de destino o su legislación impidan garantizar el íntegro cumplimiento del contrato y el ejercicio por los afectados de los derechos que el contrato garantiza.
  - b) Que la entidad destinataria haya incumplido previamente las garantías establecidas en las cláusulas contractuales aportadas.
  - c) Que existan indicios racionales de que las garantías ofrecidas por el contrato no están siendo o no serán respetadas por el importador.



- d) Que existan indicios racionales de que los mecanismos de aplicación del contrato no son o no serán efectivos.
- e) Que la transferencia, o su continuación, en caso de haberse iniciado, pudiera crear una situación de riesgo de daño efectivo a los afectados.

**Tercero.-** Ordenar que se dé traslado de la presente resolución al Registro General de Protección de Datos.

**Cuarto.-** Ordenar que se dé traslado de la presente resolución al Ministerio de Justicia, de conformidad con el artículo 139 del RLOPD, al efecto de que se proceda a su notificación a la Comisión Europea y a los demás Estados miembros de la Unión Europea de acuerdo a lo previsto en el artículo 26.3 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995.

**Quinto.-** Ordenar que, de conformidad con lo establecido en el apartado 2 del artículo 37 de la LOPD, la presente resolución se haga pública, una vez haya sido notificada a los interesados, en los términos previstos en artículo 116 del RLOPD.

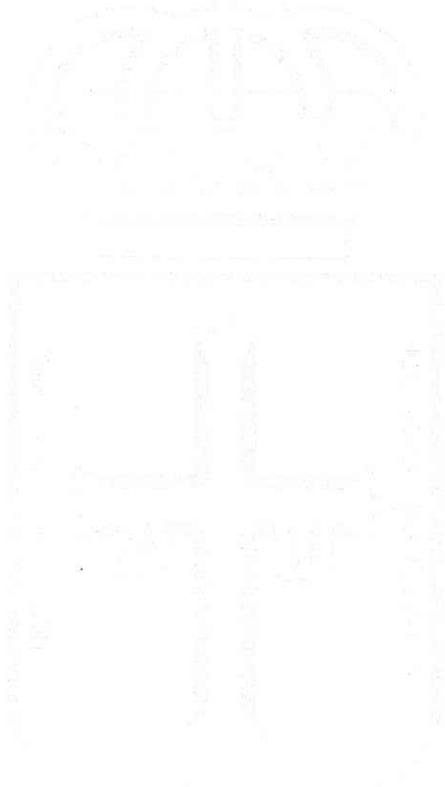
**Sexto.-** Notificar la presente resolución al solicitante.

Contra esta Resolución, que pone fin a la vía administrativa, se podrá interponer, potestativamente, recurso de reposición ante el Director de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución o directamente recurso contencioso-administrativo ante la Sala de lo Contencioso Administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso Administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, de conformidad con lo previsto en el artículo 46.1 del referido texto legal.

Madrid, 9 de mayo de 2014  
EL DIRECTOR DE LA AGENCIA ESPAÑOLA  
DE PROTECCIÓN DE DATOS

José Luis Rodríguez Álvarez

## ANEXO IV







AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS
SALIDA
Nº 348738/2015
Fecha: 21 Dic 2015

N/REF: 463376/2015

Sra; Dña María Vallina Paco.  
D. G. Ordenación Académica e Innovación Educativa  
GOBIERNO DEL PRINCIPADO DE ASTURIAS  
Plaza de España 5, 4<sup>a</sup> Planta  
33007, Oviedo, Asturias

S/REF.: 2015020704021381

En contestación a su escrito con entrada en esta Agencia el día 25 de noviembre de 2015, adjunto informe elaborado al efecto por nuestro Gabinete Jurídico.

Mar España Martí  
Directora de la Agencia Española de Protección de Datos

De conformidad con lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, se informa qué los datos personales necesarios para dar respuesta a la consulta planteada han sido incorporados al fichero "Gestión de Informes Jurídicos" del que es responsable la Agencia Española de Protección de Datos, creado por la Resolución del Director de la Agencia de fecha 24 de marzo de 2009 (B.O.E. de 7 de abril de 2009), con la finalidad de poder tramitar su solicitud y remitirle el correspondiente informe. Ud. podrá ejercitar sus derechos de acceso, rectificación, cancelación y oposición ante la Agencia Española de Protección de Datos, calle Jorge Juan 6, 28001 Madrid.

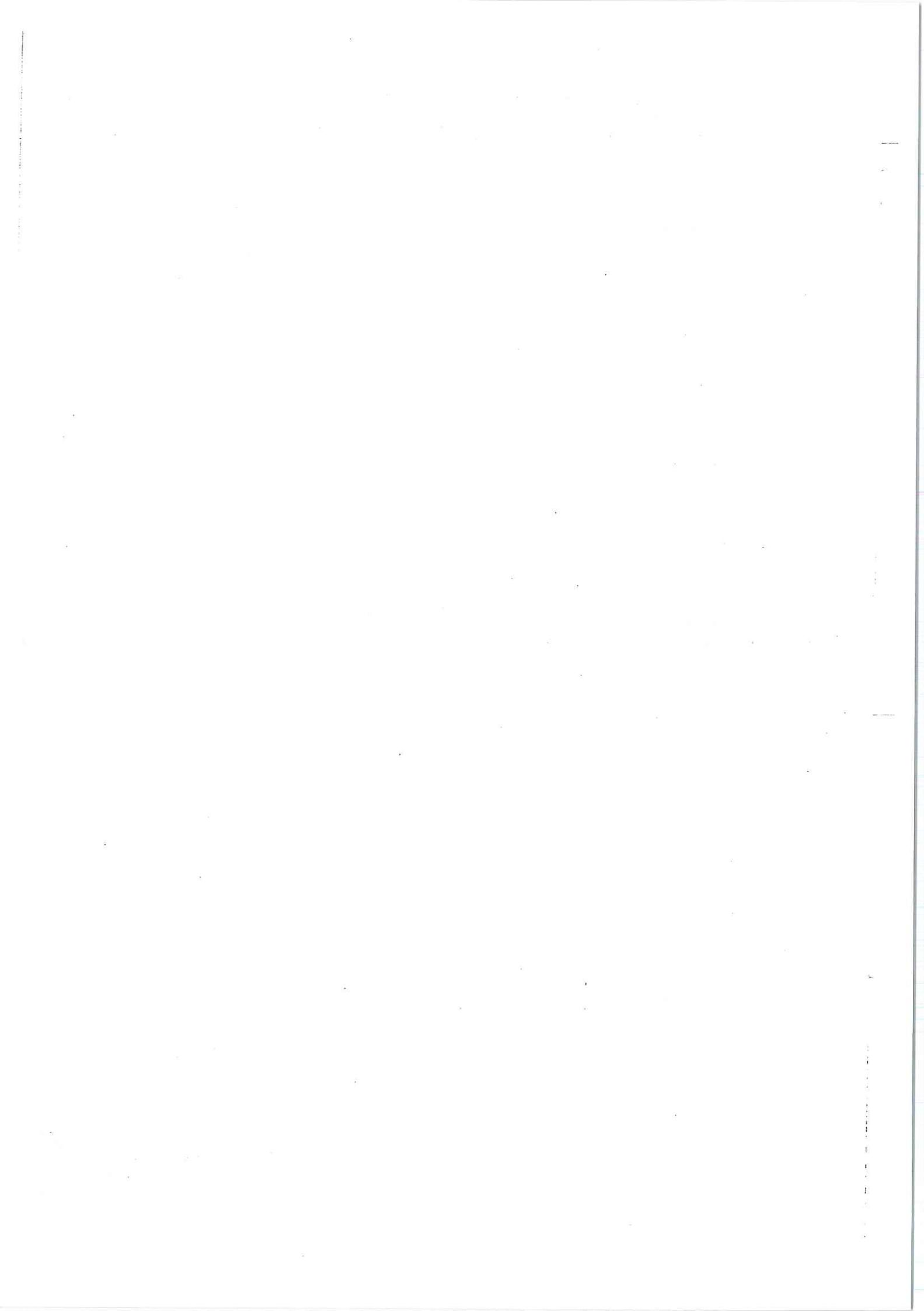
c. Jorge Juan 6

28001 Madrid

[www.agpd.es](http://www.agpd.es)

Código Seguro De Verificación:	APDPF57B4EEDCF2EDE870350-77014	Fecha:	18/12/2015
Nombre:	Este documento incorpora firma electrónica reconocida de acuerdo a la Ley 59/2003, de 19 de diciembre, de firma electrónica.		
Firmado Por:	La Directora - Mar España Martí		
Url De Verificación:	<a href="http://sedeagpd.gob.es">http://sedeagpd.gob.es</a> CVS=/code/APDPF57B4EEDCF2EDE870350-77014	Página:	1/1







N/REF: 463376/2015

Examinada su solicitud de informe, remitida a este Gabinete Jurídico, referente a la consulta planteada por la Dirección General de Ordenación Económica e Innovación Educativa del Principado de Asturias, cúmpleme informarle lo siguiente:

La consulta plantea si resulta conforme a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su Reglamento de desarrollo aprobado por el Real Decreto 1726/2007, de 21 de diciembre, la transferencia internacional de datos derivada de la contratación del paquete "Office 365" de Microsoft, teniendo en cuenta la doctrina derivada de la sentencia del Tribunal de Justicia de la Unión Europea de 6 de octubre de 2015, recaída en el asunto C-362/14, en que se declara inválida la Decisión de la Comisión 2000/520/CE de 26 de julio de 2000, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América.

La consecuencia de la sentencia mencionada es que como consecuencia de la anulación que la misma lleva a cabo, no cabrá considerar que los Estados Unidos de América ofrecen un nivel adecuado de protección a los efectos previstos en la normativa de protección de datos, nivel que sí se apreciaba, hasta ese momento, respecto de las empresas adheridas a los mencionados principios de puerto seguro.

Sin embargo, ello no supone que necesariamente queden vedadas las transferencias internacionales de datos a los Estados Unidos. A tal efecto, cabe recordar que el artículo 70.1 del Reglamento de desarrollo de la Ley Orgánica 15/1999 dispone que "cuando la transferencia tenga por destino un Estado respecto del que no se haya declarado por la Comisión Europea o no se haya considerado por el Director de la Agencia Española de Protección de Datos que existe un nivel adecuado de protección, será necesario recabar la autorización del Director de la Agencia Española de Protección de Datos". El artículo 70.2 del citado Reglamento añade que "la autorización podrá ser otorgada en caso de que el responsable del fichero o tratamiento aporte un contrato escrito, celebrado entre el exportador y el importador, en el que consten las necesarias garantías de respeto a la protección de la vida privada de los afectados y a sus derechos y libertades fundamentales y se garantice el ejercicio de sus respectivos derechos".

Pues bien, teniendo en cuenta estas previsiones y los servicios en nube

c. Jorge Juan 6  
28001 Madrid.

[www.agpd.es](http://www.agpd.es)

Código Seguro De Verificación	APDPFA82C74C0F4E8F2D19B80-13884	Fecha	17/12/2015
Normativa	Este documento incorpora firma electrónica reconocida de acuerdo a la Ley 59/2003, de 19 de diciembre, de firma electrónica.		
Firmado Por	Abogado Del Estado Jefe - Agustín Puente Escobár		
Url De Verificación	<a href="http://sedeagpd.gob.es">http://sedeagpd.gob.es</a> CVS=/code/APDPFA82C74C0F4E8F2D19B80-13884	Página	1/3





a los que concretamente se refiere la consulta, por medio de resolución de esta Agencia de 9 de mayo de 2014, recaída en el expediente de autorización de transferencias internacionales de datos con referencia TI/32/2014 se acordaba expresamente lo siguiente:

*"Primero.- Considerar adecuadas las garantías establecidas en los modelos de contratos aportados por MICROSOFT CORPORATION para la transferencia internacional de datos con destino a dicha entidad, establecida en los Estados Unidos, con motivo de la prestación de los servicios OFFICE 365, MICROSOFT DYNAMICS CRM ONLINE y WINDOWS AZURE (MOS) y actuando como encargado del tratamiento.*

*Segundo.- Considerar autorizadas las transferencias internacionales de datos con destino a los Estados Unidos que se realicen al amparo de las cláusulas contractuales mencionadas, siempre que se cumplan las siguientes condiciones:*

1. *La finalidad de la transferencia será la prestación de los servicios OFFICE 365, MICROSOFT DYNAMICS CRM ONLINE y WINDOWS AZURE (MOS) por parte de MICROSOFT CORPORATION, actuando como encargado del tratamiento. Los datos se transfieren en las condiciones y con todas las garantías reseñadas en los Fundamentos de Derecho anteriores.*
2. *La autorización sólo podrá entenderse concedida en caso de que el contrato firmado entre los responsables exportadores de los datos y MICROSOFT CORPORATION incorpore la totalidad de los documentos que se han aportado para la adopción de la presente resolución para cada uno de los servicios a los que la misma se refiere.*
3. *El exportador de datos deberá notificar al RGPD los ficheros cuyos datos vayan a ser objeto de transferencia internacional con carácter previo, con indicación de su denominación y código de inscripción en el RGPD, indicando qué se producirá la transferencia internacional de los datos al amparo de la presente resolución.*
4. *El alcance de la transferencia internacional de datos que se lleve a cabo deberá resultar ajustado a la estructura del fichero, categorías de datos y finalidades del tratamiento establecidas en la inscripción del correspondiente fichero.*
5. *El exportador de datos deberá poner a disposición de la AEPD, cuando le fueran requeridos, los contratos de prestación de servicios que haya suscrito con MICROSOFT IRELAND OPERATIONS LIMITED (MIOL) y MICROSOFT CORPORATION (...).*

Código Seguro De Verificación	APDPFA82C74C0F4E8F2D19B80-13884	Fecha	17/12/2015
Normativa	Este documento incorpora firma electrónica reconocida de acuerdo a la Ley 59/2003, de 19 de diciembre, de firma electrónica.		
Firmado Por	Abogado Del Estado Jefe - Agustín Puente Escobar		
Url De Verificación	<a href="http://sedeagpd.gob.es">http://sedeagpd.gob.es</a> ----- CVS=/code/APDPFA82C74C0F4E8F2D19B80-13884	Página	2/3





Quiere ello decir que, con independencia de la doctrina sentada en la sentencia de 6 de octubre de 2015, esta Agencia ya ha considerado que las transferencias internacionales de datos que pudieran llevarse a cabo mediante la contratación de los servicios mencionados en la resolución reúnen garantías suficientes que permiten su autorización, sin que sea preciso para el responsable, en este caso la consultante, obtener una autorización específica para llevar a cabo dichas transferencias, siempre y cuando se notifiquen al registro las transferencias realizadas en el apartado correspondiente del formulario de notificación del fichero para su inscripción. En consecuencia, la transferencia, siempre que se cumplan los requisitos señalados en el apartado segundo de la resolución que acaba de reproducirse serán conformes a la Ley Orgánica, no viéndose afectadas por la sentencia.

Es cuanto tiene el honor de informar.

Agustín Puente Escobar  
Abogado del Estado Jefe del Gabinete Jurídico

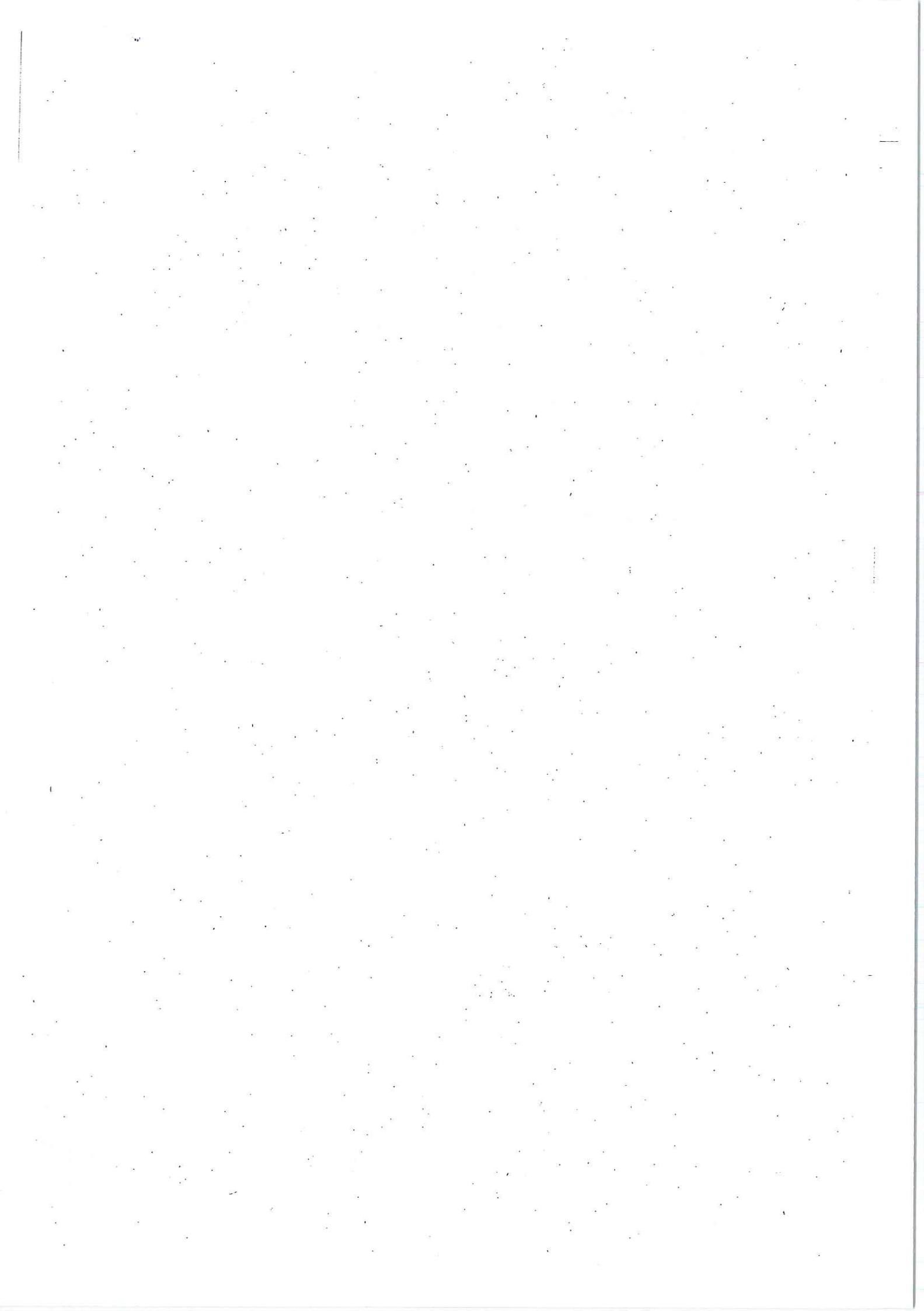
SRA. DIRECTORA DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE  
DATOS

c. Jorge Juan 6  
28001 Madrid

[www.agpd.es](http://www.agpd.es)

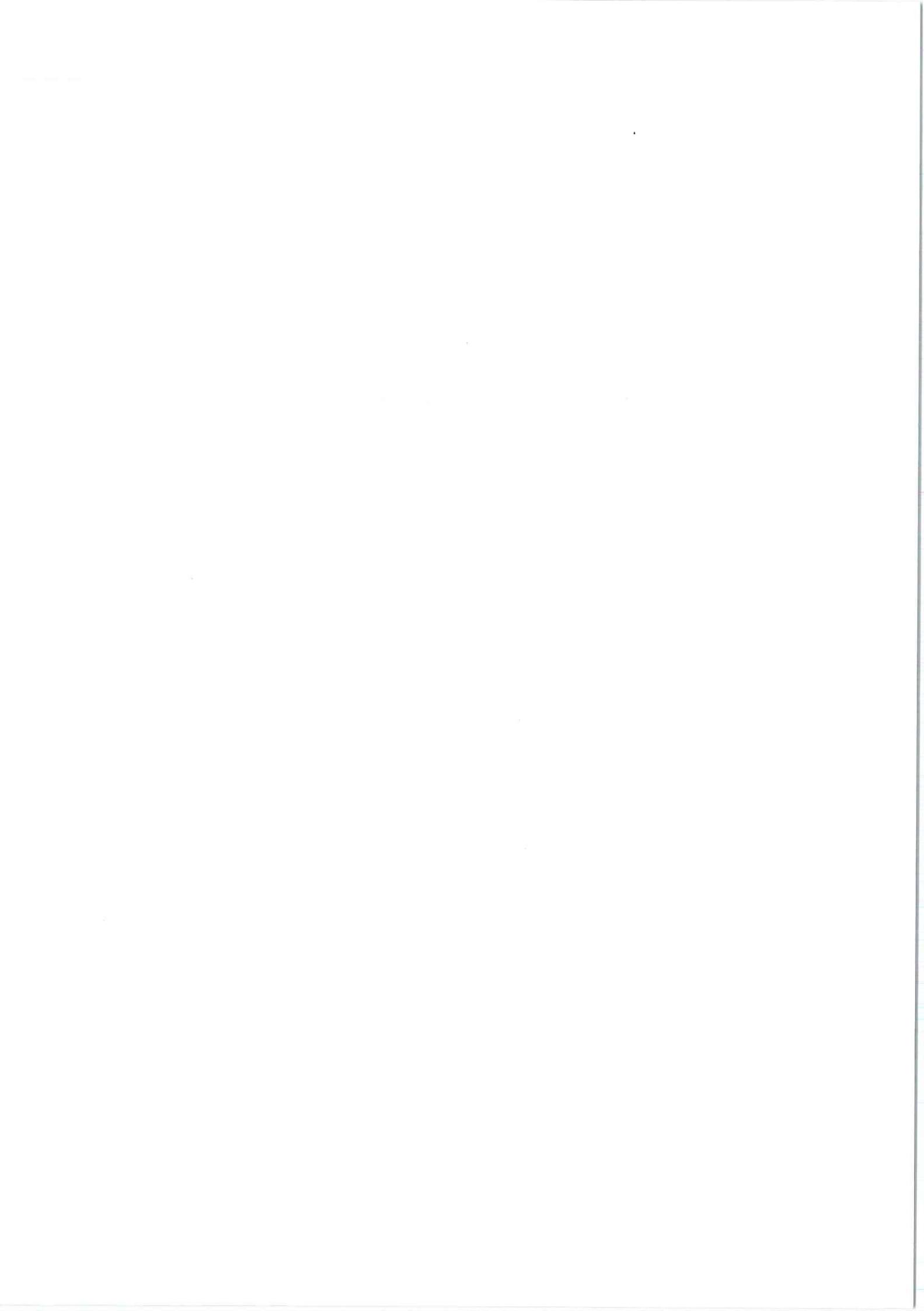
Código Seguro De Verificación:	APDPFA82C74C0F4E8F2D19B80-13884	Fecha:	17/12/2015
Normativa:	Este documento incorpora firma electrónica reconocida de acuerdo a la Ley 59/2003, de 19 de diciembre, de firma electrónica.		
Firmado Por:	Abogado Del Estado Jefe - Agustín Puente Escobar		
Url De Verificación:	<a href="http://sedeagpd.gob.es">http://sedeagpd.gob.es</a> CVS=/code/APDPFA82C74C0F4E8F2D19B80-13884		
	Página:	3/3	

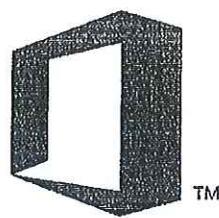




## ANEXO V







# Office 365

## Estudio e Impacto sobre la Privacidad y Seguridad

Oviedo, 18 de agosto de 2014

Elaborado por:

LOPD (Consultor de Seguridad).  
LOPD

Realizado para:

Consejería de Educación Cultura y Deporte del Principado de Asturias.

(Servicio de Formación del Profesorado y Apoyo a la Innovación Educativa).

## **Objetivo del informe, cuestiones a auditar y resumen de conclusiones.**

El objetivo del presente informe, es dar respuesta a las dudas planteadas por la Consejería de Educación del Principado de Asturias en cuanto al uso y migración de las cuentas de correo existentes (principalmente de Educastur) a los servicios de la “nube” de Microsoft bajo la denominación de “*Office 365 For Education*” (en su modalidad gratuita A2).

A lo largo de una serie de reuniones previas celebradas por parte de este consultor con todos los departamentos implicados en la gestión, migración y creación de nuevas cuentas de correo, se mostró una gran preocupación en cuanto al cumplimiento tanto de normativas relativas a la privacidad de los usuarios, así como a la integridad, ubicación y seguridad de sus datos.

En concreto, las cuestiones y apartados a auditar son los siguientes:

- Verificar el cumplimiento de la Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal, (en adelante LOPD) en la adopción de Office 365. Especialmente, en cuanto a las transferencias Internacionales de datos.
- Conocer el funcionamiento de Microsoft respecto a la privacidad de los usuarios (publicidad, cesión de datos a terceros o anunciantes, borrado, ubicación, etc).
- Evaluar las medidas de seguridad implementadas por Microsoft para garantizar en la medida de lo posible, unos adecuados y necesarios niveles de privacidad e integridad de los datos y cuentas de usuario.

## **Conclusiones (resumen).**

En cuanto al cumplimiento de la LOPD, se ha podido comprobar que en la actualidad, Microsoft es el único proveedor de “Cloud” o computación en la nube que cumple con los requerimientos de la Agencia Española de Protección de Datos (en adelante AEPD). Hecho que ha sido avalado por una Resolución de mayo de 2014.

Sobre cómo gestiona Microsoft las cuestiones de privacidad, se ha verificado que salvo en situaciones concretas que se amplían a lo largo del presente informe, los datos del usuario sólo se usan para la prestación y mantenimiento de los diferentes servicios de “Office 365”.

En lo relativo a la seguridad y protección frente a ataques telemáticos, posibles fugas de información o pérdida de datos, se ha comprobado que Microsoft cuenta con certificaciones solventes como ISO 27001, junto adecuadas medidas de seguridad y gestión de incidentes.

\* **Nota:** se incluyen entre los textos del presente informe, enlaces o hipervínculos externos a documentación relacionada para una mejor comprensión del mismo (en color azul).

## Cumplimiento LOPD y transferencias internacionales de datos.

Para comprender la problemática asociada a este punto, hay que remontarse al año 2010, momento en el que Microsoft comenzó a firmar acuerdos con la UE respectivas a las denominadas *Cláusulas Contractuales Tipo* ([Decisión 2010/87/UE](#), acceso al PDF).

Unas cláusulas, en las que se regula el hecho de exportar datos fuera de la Unión Europea para países miembros de la UE. En el caso que nos ocupa, a Estados Unidos.

Estas Cláusulas Tipo, no eran aplicables en España como sucede en otros países de la UE a efectos de LOPD, ya que estaban consideradas como insuficientes en cuanto a garantías y cumplimiento normativo, según el criterio de la AEPD para realizar transferencias de datos internacionales de forma automatizada.

Cabe destacar sobre estas transferencias lo que se establece en el artículo 33.1 de la LOPD como norma general:

*“No podrán realizarse transferencias temporales ni definitivas de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento con destino a países que no proporcionen un nivel de protección equiparable al que presta la presente Ley.”*

*“Salvo que, además de haberse observado lo dispuesto en ésta, se obtenga autorización previa del Director de la Agencia Española de Protección de Datos.”*

*“Que sólo podrá otorgarla si se obtienen garantías adecuadas” y el artículo 37.1.l) LOPD atribuye a la AEPD la función de “ejercer el control y adoptar las autorizaciones que procedan en relación con los movimientos internacionales de datos,...”.*

Debido a la naturaleza y complejidad del “Cloud Computing” (o “computación en la nube”), donde un dato o fichero puede estar en diferentes localizaciones geográficas al mismo tiempo, además de necesitar un soporte técnico ”24 x 7”, el mencionado hecho de no poder aplicar esas cláusulas en España con compañías que almacenan datos fuera de la UE, como es el caso de Microsoft con “Office 365”, bloqueaba la contratación y el cumplimiento normativo en cuanto a la LOPD.

Para solventar esta situación, tal y como podemos leer en la [Resolución de la AEPD con N° Expediente: TI/00032/2014](#) con fecha 9 de mayo de 2014 (se adjunta al presente estudio dicha resolución en formato PDF), el pasado 12 de febrero de 2014, Microsoft Corporation presentó un documento para su revisión ante la AEPD exponiendo lo siguiente:

*Que presta los servicios de computación en nube denominados:*

*OFFICE 365, MICROSOFT DYNAMICS CRM ONLINE y WINDOWS AZURE (en adelante MOS: MICROSOFT ONLINE SERVICES) a través de su subsidiaria MICROSOFT IRELAND OPERATIONS LIMITED (MIOL), con sede en Irlanda, ofreciendo a sus clientes la firma, junto con el correspondiente contrato comercial, de un acuerdo relativo al tratamiento de datos.*

*Que los servicios MOS son prestados por MIOL por sí mismo o a través de subcontratistas, siendo Microsoft Corporation, sociedad matriz del Grupo Microsoft establecida en los Estados Unidos, el subcontratista principal que, a su vez, presta los servicios por sí misma o a través de subcontratistas que pueden estar situados fuera del Espacio Económico Europeo (EEE).*

*Que, con la finalidad de aportar las garantías suficientes para las transferencias de datos a MICROSOFT CORPORATION y a sus subcontratistas, ofrece a sus clientes la posibilidad de firmar las cláusulas contractuales tipo, adoptadas por la Comisión Europea en su Decisión 2010/87/UE, y un acuerdo suplementario a dichas cláusulas para adecuar a las características de los servicios de computación en nube la realización de las auditorías de las actividades de tratamiento y la subcontratación de operaciones de tratamiento con subencargados ulteriores del tratamiento.*

*Aportando para proceder a su revisión un ejemplar de cada uno de los documentos que conforman el esquema de garantías contractuales y solicita que, al amparo de lo dispuesto en los artículos 33 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) y 70.2 de su Reglamento de desarrollo, aprobado por el Real Decreto 1720/2007, de 21 de diciembre (RLOPD), por el Director de la AEPD se declare que las garantías establecidas en la documentación que presenta son adecuadas para realizar transferencias de datos personales a los Estados Unidos y que los clientes que contraten los servicios MOS y suscriban los contratos aportados queden autorizados a realizarlas siempre y cuando las notifiquen previamente al Registro General de Protección de datos (RGPD).*

Tras el pertinente estudio por parte de la AEPD de la documentación aportada por Microsoft Corporation, las nuevas cláusulas o acuerdos suplementarios aplicables al reglamento Español en protección de datos, han sido fundamentales para que la AEPD haya considerado favorable el cambio a tenor de lo que podemos leer en la Resolución:

*Al propio tiempo, no puede ignorarse que tanto el acuerdo suplementario a las cláusulas contractuales tipo como los acuerdos sobre tratamiento de datos de los servicios MOS vienen a especificar con mayor precisión una serie de extremos que constituyen las garantías contenidas en la Decisión 2010/87/UE, especificando aún*

*más las obligaciones del prestador de servicios.*

*En particular, y además de las garantías establecidas en materia de auditoría de seguridad y subcontratación de los servicios, que al apartarse de la literalidad de la citada Decisión han exigido un estudio detallado en la presente esolución, deben tenerse particularmente en cuenta las condiciones estipuladas en los acuerdos sobre el tratamiento de datos en los servicios online (MOS) en lo que respecta a la seguridad de los datos, incluidos en su apartado 4, así como la referencia a la notificación de incidentes de seguridad a la que se refiere el apartado 5 de dicho documento.*

*Además, el punto 6 del acuerdo suplementario añade que "El Cliente reconoce y acepta que, con independencia de que la exportación de datos personales aquí contemplada esté amparada por la Autorización AEPD, el Cliente tiene imperativamente, según la normativa española sobre protección de datos, la obligación propia de notificar a la AEPD la modificación de su inscripción del fichero o ficheros, mediante notificación en la que indique que procede a la exportación de datos personales a Microsoft Corporation al amparo de la Autorización AEPD.*

*Esta notificación deberá especificar necesariamente, según la mencionada normativa, el fichero o ficheros del Cliente respecto de los que utilizará los Servicios Online*

Este y otros hechos recogidos en la resolución TI/00032/2014 con fecha 9 de mayo de 2014, han hecho posible han que **la AEPD haya dictaminado a favor de Microsoft** (siempre bajo determinadas circunstancias y garantías expuestas en la Resolución) lo siguiente:

*La conclusión que acaba de alcanzarse conduce al necesario análisis de las consecuencias que pueden considerarse derivadas de esa declaración, toda vez que en el presente supuesto la valoración efectuada se lleva a cabo respecto del modelo contractual aportado y no en referencia a un supuesto concreto de transferencia internacional de datos de carácter personal.*

*Así, una vez consideradas adecuadas las garantías establecidas en el modelo contractual objeto de análisis en la presente resolución, la firma concreta del contrato por parte de un determinado cliente que pretenda la prestación de los servicios MOS a los que el modelo se refiere reuniría necesariamente las mismas garantías que se han valorado en la presente resolución.*

*De este modo, toda vez que el nivel adecuado de garantías ha sido suficientemente acreditado, la exigencia específica de una autorización individualizada de transferencia internacional de datos por cada uno de los clientes del servicio,*

*siempre ajustada al artículo 33.1 de la LOPD en caso de reproducir ese marco contractual, ocasionaría una carga innecesaria al exportador solicitante, toda vez que la conclusión material del expediente resultaría prejuzgada por el contenido de esta resolución.*

*Por ello, establecido que las garantías aportadas son suficientes para llevar a cabo las transferencias internacionales de datos, parece razonable considerar que la declaración contenida en esta Resolución supone igualmente la autorización de las transferencias internacionales de datos que se lleven a cabo mediante la firma de las cláusulas contractuales analizadas, siempre que se observen una serie de requisitos.*

El párrafo anterior es un extracto del dictamen recogido en la Resolución y cabe destacar que la autorización de la AEPD, se aplica tanto a clientes corporativos de un ámbito empresarial, como a las Administraciones Públicas.

Así, la citada Resolución ampara la exportación de datos a Microsoft Corporation en Estados Unidos y, a través de las fórmulas establecidas en las *Cláusulas Contractuales Tipo*, establece la posibilidad de efectuar la transferencia de datos a subcontratistas con sede en países terceros siempre que se cumplan los requisitos exigidos para ello por la AEPD.

De este modo, los clientes o usuarios de este tipo de servicios que firmen contratos con Microsoft Corporation, cuentan con la autorización de la AEPD para proceder a la citada exportación de datos, inherente al uso de los servicios “Cloud” o de computación en la nube de Microsoft y en el caso que nos ocupa, aplicable también a “Office 365 for Education”.

Tal y como recoge la Resolución, sin necesidad de solicitar una autorización previa para ello, sino sólo bajo la obligación de notificarlo previamente a la AEPD utilizando el código otorgado a Microsoft para dicha finalidad.

Para finalizar con este punto, se recomienda ampliar información sobre las Cláusulas Modelo en el sitio web que Microsoft ha puesto a disposición de los usuarios.

## **Microsoft Office 365 y la privacidad de los usuarios.**

Este era otro de los puntos críticos en la adopción de los servicios de la nube de Microsoft que más preocupación provocó en las reuniones previas a este informe.

El motivo no es otro que la naturaleza y tipo de usuarios que formarán una gran parte de las futuras cuentas que serán gestionadas con Office 365 (estudiantes y menores de edad).

Hasta la fecha, estas cuentas de correo eran gestionadas y almacenadas en centros de datos propios, con un control total sobre los mismos.

Al externalizar y proporcionar vía web el servicio de correo corporativo, junto a otras funcionalidades de Office 365, se generaron dudas razonables en cuanto a la visualización de publicidad contextual dependiendo de los hábitos y preferencias de navegación del usuario.

Publicidad también según el contenido de los ficheros almacenados tanto en “OneDrive” (se contará con 7 gb de espacio para el almacenamiento de datos), así como ficheros adjuntos en el correo electrónico (estarán disponibles 25 gb para cada una de las cuentas) o páginas web visitadas, además de otros parámetros usados para estos fines publicitarios.

Por parte de los representantes de Microsoft Ibérica con los que se trataron estas dudas, (como este consultor pudo comprobar en alguna de las reuniones), se aseguró de forma tajante que **en ningún caso, se mostraría este tipo de publicidad directa en el navegador del usuario, y tampoco de forma indirecta** (por ejemplo, en el correo electrónico).

Con el fin dar respuesta a cuestiones de privacidad y seguridad, Microsoft Corporation ha puesto a disposición del público a través de su “Centro de Confianza Office 365”, múltiple información sobre cómo gestionan estos temas y qué uso hacen de los datos del usuario.

De entre todas las preguntas y respuestas, recopilamos y analizamos las más relevantes:

**Pregunta: ¿Quién es el propietario de los datos que almacenamos en su servicio? ¿Usarán nuestros datos para generar productos publicitarios?**

**Respuesta:** Como cliente de Office 365, es propietario y tiene el control de sus datos. Solo usamos sus datos para brindarle el servicio al que se ha suscrito. Como proveedor del servicio, no examinamos sus correos electrónicos o documentos con fines publicitarios

En el apartado destinado a informar sobre el uso que se hace de los datos, podemos leer:

*¿Cómo usa mis datos Office 365 o Dynamics CRM Online?*

En la siguiente tabla se explica cómo utiliza Microsoft sus datos de cliente de Office 365

Uso de datos de cliente de Office 365 y Dynamics CRM Online	Datos de cliente (a excepción del contenido)	Contenido
Funcionamiento y resolución de problemas de los servicios	Sí	Sí
Seguridad, prevención de correo no deseado y malware	Sí	Sí
Comunicaciones de servicios	Sí	No
Mejora de los servicios adquiridos	No	No
Publicidad	No	No
Revelación voluntaria a una autoridad legal	No	No
Marketing directo	No	No

Como se puede ver, Microsoft afirma que no usa ningún dato del usuario destinado a fines publicitarios, pero es conveniente destacar todas las preguntas y respuestas ampliadas.

A continuación, procedemos a reseñar las más comunes e importantes (incluyendo las relativas a petición de información por las autoridades o requerimientos judiciales).

**Pregunta: ¿Cómo usa mis datos Office 365 para mantener el servicio?**

Respuesta: Los datos de cliente solo se utilizarán para prestar el servicio, excepto que el usuario indique otro uso.

Además de las transacciones diarias, el funcionamiento del servicio puede incluir el uso de los datos de cliente en las siguientes circunstancias:

Resolución de problemas con el objeto de prevenir, detectar y solucionar problemas que repercutan en el funcionamiento de los servicios.

Mejora constante de características o requisitos de mantenimiento continuado de la seguridad que conllevan la detección de amenazas nuevas y en evolución, o la protección frente a estas, que pongan en peligro los servicios o datos de cliente

(como malware o correo electrónico no deseado).

Disponibilidad de características de servicio personalizadas o basadas en deducciones.

**Pregunta:** *¿Office 365 o Dynamics CRM Online comparten datos o sistemas con algún servicio admitido por el anunciante? ¿Office 365 o Dynamics CRM Online utilizan técnicas de minería de datos con los datos de cliente para sus anunciantes?*

Respuesta: No. Office 365 y Dynamics CRM Online utilizan sistemas independientes que se conservan en distintas ubicaciones físicas y lógicas respecto de los servicios admitidos por el anunciante y los sistemas que ejecuta Microsoft, y no existe un flujo de datos entre ambos sistemas ni su uso para crear perfiles destinados a publicidad o para generar publicidad para los usuarios finales.

**Pregunta:** *¿Office 365 o Dynamics CRM Online pueden utilizar o revelar los datos sin mi permiso?*

Respuesta: En cierto número limitado de circunstancias, es posible que Microsoft deba revelar datos de cliente sin su consentimiento previo, lo cual incluye situaciones en las que esto es necesario para satisfacer requisitos legales.

**Pregunta:** *¿Cuál es el proceso que siguen Office 365 y Dynamics CRM Online si una autoridad legal solicita mis datos? ¿Cómo actúa Microsoft cuando recibe una citación o un mandato legal para presentar la información de los clientes?*

Respuesta: Office 365 y Dynamics CRM Online creen que sus clientes deben controlar su propia información en la medida de lo posible.

Consecuentemente, si una entidad gubernamental se dirige a Microsoft directamente para solicitar información que hospedamos en nombre de nuestros clientes de Office 365 o Dynamics CRM Online, en primer lugar, Microsoft intentará remitir la entidad al cliente para ofrecerle la oportunidad de determinar cómo responder. Si, aun así, debe responder a la solicitud, Microsoft proporcionará únicamente la información perteneciente a sus clientes de Office 365 o Dynamics CRM Online cuando se le solicite legalmente, restringirá la presentación de información a aquella cuya revelación se requiera y hará todo lo posible para notificar al cliente empresarial con antelación a cualquier presentación, a no ser que esto se haya prohibido por vía legal.

Por lo general, esta notificación se efectuará por correo electrónico a uno o más de

los administradores que el cliente haya indicado en el portal de Microsoft Online Services. Es responsabilidad del cliente mantener actualizada la información de contacto.

**Pregunta: ¿Qué son los datos de uso y cómo los utiliza Microsoft?**

Respuesta: Los datos de uso se utilizan para prestar el servicio.

El término "datos de uso" puede hacer referencia a cualquier cantidad de puntos de datos relacionados con Office 365 y Dynamics CRM Online. "Datos de uso" puede hacer referencia al número promedio de mensajes de correo electrónico que recibe diariamente un usuario final, el número de licencias en la suscripción de un cliente o la cantidad de electricidad que requiere Microsoft para prestar servicios Office 365.

Somos conscientes de que la mayor preocupación de nuestros clientes está asociada al modo en que tratamos la información de identificación personal sobre las interacciones de los usuarios finales con los servicios. Es posible que este tipo de datos se utilice para las operaciones cotidianas y para el mantenimiento de los servicios (como se describió anteriormente), así como para las comunicaciones de servicios a los administradores, incluidos mensajes de correo electrónico sobre el acceso o uso de los servicios por parte de los usuarios finales.

Por ejemplo, un administrador podría recibir una notificación de Microsoft cuando un usuario final está próximo a alcanzar los límites de uso o de almacenamiento.

**Pregunta: ¿Cuáles son las comunicaciones de servicios que recibirán los administradores?**

Respuesta: Los administradores pueden recibir diversos tipos de comunicaciones de Microsoft relacionadas con el uso de los servicios.

Asimismo, pueden recibir comunicaciones sobre el funcionamiento de los servicios, incluidos el mantenimiento programado y nuevas características o funcionalidades.

De toda esta información, es conveniente reseñar que **los administradores de la plataforma deberán prestar una especial atención** a las comunicaciones por parte de Microsoft sobre cualquier tipo de requerimiento, límites de uso, cambio en las condiciones de servicio o cualquier tema relativo a la privacidad del usuario.

Tal y como hemos visto en una de las preguntas respondidas:

*Microsoft proporcionará únicamente la información perteneciente a sus clientes de Office 365 o Dynamics CRM Online cuando se le solicite legalmente, restringirá la*

*presentación de información a aquella cuya revelación se requiera y hará todo lo posible para notificar al cliente empresarial con antelación a cualquier presentación, a no ser que esto se haya prohibido por vía legal.*

Cabe la posibilidad y así se afirma de que se impida la notificación a las partes interesadas respecto a un requerimiento judicial o petición de información por los Cuerpos y Fuerzas de Seguridad del Estado (como volveremos a leer más adelante: “petición legal o del cliente”).

En ese punto, no se aclara si los requerimientos o peticiones de información prohibidos por vía legal, pueden venir también de un miembro fuera de la U.E, como por ejemplo Estados Unidos, aunque se entiende que sí al ser el País donde está la sede de Microsoft Corporation.

Deben tenerse también en cuenta las revelaciones del ex Analista de la C.I.A y antiguo empleado de la NSA Eduard Snowden, respecto a programas de espionaje masivo como PRISM por parte del gobierno E.E.U.U, en las que se afirmaba que junto a otros, Microsoft había participado en la cesión de datos de ciudadanos residentes fuera de Estados Unidos.

Los datos que supuestamente la NSA es capaz de obtener con PRISM, incluyen correos electrónicos, vídeos, chat de voz, fotos, direcciones IP, notificaciones de inicio de sesión, transferencia de archivos y detalles sobre perfiles en redes sociales.

Microsoft ha negado su participación en el programa PRISM a pesar de las filtraciones respondiendo lo siguiente:

*Nosotros proveemos datos de los clientes cuando recibimos una orden judicial o una citación para hacerlo y nunca de forma voluntaria.*

*Adicionalmente, solo cumplimos con peticiones acerca de cuentas o identificadores específicos. Si el Gobierno tiene un programa nacional de seguridad para recopilar datos de clientes voluntariamente, nosotros no participamos en él.*

**Nota del consultor**, esta respuesta que se extrae de Wikipedia, proviene de una reputada fuente online como TechCrunch, donde fue publicada el 6 de junio de 2013 originalmente.

Obviamente, el hecho de que Microsoft niegue su participación en programas como PRISM, no es suficiente garantía como para creer que así sea, por lo que la recomendación es que habrá que prestar en todo momento una atención especial y continuada sobre cuestiones de privacidad y cesión de datos bien de forma indiscriminada o no justificada.

Otras preguntas y respuestas de Microsoft: Legalidad, Privacidad y Publicidad en la nube.

**Pregunta:** *¿El proveedor de servicios en la nube usa los datos de los clientes con otros*

*fines o en modos ajenos a la prestación del servicio? En caso afirmativo, ¿cuáles son estos fines? Por ejemplo, ¿se procesarán los datos de los clientes para crear perfiles que se usarán en publicidad o con otros fines comerciales? ¿O se divulgarán a terceros (que no sean subcontratistas o cuando no exista una obligación legal)?*

Respuesta: Referencia del dictamen del GT29: sección 3.4.1.2 (Especificación y limitación de la finalidad). El GT29 exige que "los datos personales sean recogidos con fines determinados, explícitos y legítimos, y no sean tratados posteriormente de manera incompatible con dichos fines" y señala que los clientes de servicios en la nube son los responsables de "garantizar que el proveedor [...] no trate [...] (ilegalmente) los datos personales para otros fines".

Office 365: los servicios en la nube empresariales de Microsoft solo usan los datos de los clientes para prestar los servicios. Esto puede incluir la solución de problemas destinada a prevenir, detectar y reparar fallos que repercutan en el funcionamiento de los servicios y la mejora de las características que permiten detectar y proteger frente a amenazas al usuario emergentes o en evolución (como el malware o el correo no deseado). Office 365 no crea productos publicitarios con los datos de los clientes. No examinamos los correos ni los documentos para elaborar análisis, extraer datos, hacer publicidad ni mejorar el servicio.

Microsoft no difundirá datos de clientes a terceros (incluidos los organismos encargados de la aplicación de la ley, otras entidades gubernamentales o demandantes civiles y excluyendo a nuestros subcontratistas) salvo por petición del cliente u obligación legal.

*Pregunta: Si el proveedor de servicios en la nube ofrece servicios empresariales y de consumidor, ¿significa que combina los datos empresariales del consumidor con los datos que recoge de los servicios del consumidor? En caso afirmativo, ¿de qué forma y con qué finalidad?*

Respuesta: Referencia del dictamen del GT 29: sección 3.4.1.2 (Especificación y limitación de la finalidad) y sección 3.3.1 (Clientes y proveedores de servicios de computación en la nube).

Office 365: los servidores empresariales en la nube de Microsoft están física y/o lógicamente separados de los servidores destinados a los servicios al consumidor en línea. Los datos empresariales de los clientes, los datos existentes en los servicios al consumidor en línea de Microsoft y los datos creados en, o resultantes de, las actividades de exploración, indización o extracción de datos llevadas a cabo por Microsoft no se mezclan a menos que el cliente lo haya autorizado previamente.

*Pregunta: ¿El proveedor de servicios en la nube examina o extrae contenido de los*

*clientes, como mensajes de correo o documentos? En caso afirmativo, ¿con qué fines?*

Respuesta: Referencia del dictamen del GT 29: sección 3.4.1.2 (Especificación y limitación de la finalidad) y sección 3.3.1 (Clientes y proveedores de servicios de computación en la nube).

Office 365: Microsoft no examina correos ni documentos con fines publicitarios. Los servicios empresariales de Microsoft mantienen, examinan e indizan los datos de los clientes para ofrecer características útiles que permiten a los clientes acceder y organizar los datos de cliente. Por ejemplo, los usuarios finales pueden buscar fácilmente sus documentos y otro contenido en Office 365.

Como se puede leer, en todos los bloques anteriores de preguntas y respuestas, Microsoft insiste en que no accede al contenido de los correos, no usa datos con fines publicitarios, ni cede dichos datos, (salvo “*por petición del cliente u obligación legal*” ) o sólo para dar el servicio o nivel de soporte técnico requerido.

*Pregunta: Si el proveedor de servicios en la nube también ofrece servicios al consumidor, ¿aquel mezcla los datos empresariales y los datos recopilados de estos servicios al consumidor?*

Respuesta: Referencia del dictamen del GT 29: sección 3.4.3 (Medidas técnicas y de organización para garantizar la protección de los datos y su seguridad).

Office 365: el servicio comercial de Office 365 está separado lógicamente de los servicios al consumidor en línea. Los datos empresariales de los clientes y los datos existentes en los servicios al consumidor en línea de Microsoft no se mezclan a menos que el cliente lo haya autorizado previamente.

*Pregunta: ¿El proveedor de servicios en la nube aplica protecciones seguras a las transferencias de datos en la nube?*

Respuesta: El GT 29 concluye señalando que los mecanismos tradicionales para transferir datos fuera del Espacio Económico Europeo tienen "limitaciones" cuando se aplican a la nube. El Grupo apunta a las directrices de puerto seguro (Safe Harbor) y avisa a los clientes de que "el único compromiso del importador de datos con las directrices de puerto seguro puede no ser suficiente" para las transferencias de datos a proveedores con sede en EE. UU. También recuerda a los clientes en la nube la necesidad de garantizar el cumplimiento con las obligaciones legales nacionales que resulten de aplicación.

**Nota del Consultor:** El “GT 29”, se refiere a un Grupo de Trabajo del Artículo 29 de la UE (GT 29), un grupo relacionado con el “Cloud”, constituido por las autoridades de protección de datos nacionales de la Unión Europea para velar por su cumplimiento.

Sobre los controles de privacidad y si se ofrecen al usuario, Microsoft responde:

*Los controles de privacidad se habilitan de forma predeterminada para todos los clientes del servicio y le permitimos activar y desactivar las características que afectan a la privacidad para satisfacer las necesidades de su organización. Nos comprometemos contractualmente con las promesas que hacemos en cuanto a la privacidad y seguridad mediante el acuerdo de procesamiento de datos (DPA).*

Sobre la visibilidad y dónde se almacenan los datos en el servicio Microsoft responde:

*Somos transparentes sobre donde se encuentran los datos. Para más información, vaya a la sección Dónde están mis datos en el Centro de confianza de Office 365.*

Esta afirmación debe ser necesariamente cuestionada ya que ellos mismos argumentan que:

*Es política general de Microsoft no revelar la ubicación de los centros de datos. Microsoft dispone de entre 10 y 100 centros de datos ubicados en todo el mundo.*

No obstante, Microsoft ofrece información al respecto en forma de “mapas de datos”:

País, región o plan	Mapa de datos
América del Norte	<a href="#">Ver [en inglés]</a>
América del Sur	<a href="#">Ver [en inglés]</a>
Europa, Oriente Medio, África	<a href="#">Ver [en inglés]</a>
Asia, Australia	<a href="#">Ver [en inglés]</a>
Planes de Office 365	
Administración Pública	<a href="#">Ver [en inglés]</a>

Y sobre el caso que nos ocupa, en relación a la Unión Europea, podemos leer en relación a la ubicación final de los datos:

*Para los clientes que especifican una ubicación en la Unión Europea en el cuadro desplegable de país o región: Dublín, Irlanda, Amsterdam, Países Bajos, Estados Unidos.*

Es de interés también conocer los motivos por los que Microsoft realizaría un **movimiento de datos** entre regiones diferentes a la originaria:

*Los requisitos para proporcionar los servicios pueden implicar la transferencia de algunos datos al personal o los subcontratistas de Microsoft fuera de la región de almacenamiento principal o que estos accedan a tales datos.*

*Por ejemplo, para dirigir la latencia, puede que los datos de enrutamiento deban copiarse a centros de datos distintos de diferentes regiones.*

*Además, el personal que posee los conocimientos más técnicos para solucionar problemas de servicio específicos puede localizarse en ubicaciones distintas de la ubicación principal y puede necesitar acceso a sistemas o datos para resolver un problema.*

Sobre si avisará Microsoft cuando los datos de cliente se transfieran a otro País, responden;

*No. Pero Microsoft enviará un aviso en el caso de que cambie la información sobre mapas de datos de Office 365 y Microsoft Dynamics CRM Online a la que se hace referencia en la tabla anterior.*

*Este aviso se enviará a los administradores que hayan seleccionado la opción sobre "notificaciones de cumplimiento" en la parte "perfil" de Microsoft Online Services.*

En base a esta respuesta, se recomienda encarecidamente revisar y activar esa opción en el perfil del administrador (notificaciones de cumplimiento), caso de que no esté activadas por defecto.

## **Office 365. Seguridad, copias de respaldo e integridad de los datos.**

Llegados al último punto a revisar en base a las dudas sobre la seguridad de Office 365 planteadas por la Consejería de Educación al consultor, es importante mencionar que los dos puntos anteriores, (cumplimiento LOPD y Privacidad) están estrechamente relacionados con la seguridad e integridad tanto de las cuentas de usuario, como de los datos de las mismas.

Una gran parte de lo anteriormente expuesto es válido para este punto, aunque hay algunos aspectos relativos a la seguridad de importancia y que se destacan a continuación.

Microsoft tiene dos documentos publicados sobre cuestiones de Seguridad Informática de interés para este estudio. Los dos están relacionados con la gestión e implementación de la seguridad en la “nube” de Microsoft y Office 365.

“Security in Office 365 Whitepaper”. (Publicado en mayo de 2014)

“Securing Microsoft’s Cloud Infrastructure”. (Publicado en mayo de 2009).

En ellos se mencionan aspectos de vital importancia sobre cómo implementan y despliegan sus productos en la nube, y también sobre las medidas de seguridad que ponen en marcha entre las que se incluyen: Controles de acceso físicos a los datos, medidas proactivas contra ataques de Denegación de Servicio (DoS), escaneos de puertos, infecciones por malware, cifrado de datos y comunicaciones, fortaleza y tipos de contraseñas, seguridad en sus aplicaciones web, auditorias y cumplimiento normativo, seguridad de los datos, etc.

Se puede leer un resumen de estas medidas de seguridad en:

*Las 10 principales características de seguridad y privacidad de Office 365.*

*Restringimos el acceso a los centros de datos físicos al personal autorizado y hemos implementado varias capas de seguridad física, como lectores biométricos, sensores de movimiento, acceso seguro las 24 horas del día, vigilancia con cámaras de vídeo y alarmas de infracciones contra la seguridad.*

*Habilitamos el cifrado de datos tanto de manera estática como a través de la red, ya que los datos se transmiten entre un centro de datos y el usuario.*

*No extraemos sus datos ni accedemos a ellos con fines publicitarios.*

*Solo usamos los datos del cliente para brindar el servicio; no examinamos su buzón de ninguna otra forma sin su permiso.*

*Periódicamente, hacemos copia de seguridad de sus datos.*

*No eliminaremos todos los datos de su cuenta al finalizar el plazo de servicio hasta que haya tenido tiempo de aprovechar la portabilidad de datos que ofrecemos.*

*Hospedamos los datos de los clientes en la región.*

*Aplicamos contraseñas "seguras" para aumentar la seguridad de sus datos.*

*Permitimos que active y desactive características relacionadas con la privacidad para ajustarlas a sus necesidades.*

*Nos comprometemos por contrato a cumplir las promesas formuladas aquí con el acuerdo de procesamiento de datos (DPA). Para más información sobre el DPA, visite la sección Acuerdo de procesamiento de datos de la página Control de calidad externo.*

Varias de las afirmaciones que hace Microsoft aquí, han sido analizados en la anterior sección del informe dedicada a la Privacidad. En base a esa información, uno de los puntos a aclarar sería el relativo a la **eliminación de los datos y cuenta del usuario** en base a esta información: "*hasta que haya tenido tiempo de aprovechar la portabilidad de datos que ofrecemos*".

Se debería especificar el tiempo exacto y si existe una forma de proceder a un borrado de datos y cuenta asociada al perfil de forma permanente e inmediata. No obstante, tal y como este Consultor ha podido leer en el apartado sobre el acceso a los datos, se entiende que es por un tiempo máximo de 90 días (extracto):

*Vencimiento o rescisión del servicio en línea. Tras el vencimiento o la rescisión de la suscripción del servicio en línea, debe ponerse en contacto con Microsoft e informarnos de si:*

- (1) se ha de deshabilitar su cuenta y, a continuación, eliminar los datos de cliente; o*
- (2) se han de conservar los datos de cliente en una cuenta con funciones limitadas durante al menos 90 días tras el vencimiento o la rescisión de la suscripción (el "periodo de retención") de forma que pueda extraer los datos.*

*Si señala (1), no podrá extraer los datos de cliente desde su cuenta. Si no señala ninguna de las opciones, conservaremos los datos de cliente según (2).*

*Tras el vencimiento del periodo de retención, deshabilitaremos la cuenta y, a continuación, eliminaremos los datos de cliente. Las copias de seguridad o almacenadas en la memoria caché se purgarán en un plazo de 30 días a partir de la finalización del periodo de retención.*

Todo ello dependiendo de la opción que decida el usuario, aunque es de esperar (no estaría

de más aclararlo) que si el borrado lo realiza un administrador, esa eliminación sea efectiva de inmediato salvo por causas debidamente justificadas o requerimientos legales.

Información relacionada sobre cumplimiento legal, Privacidad y normas de calidad:

### *Las 10 principales normas de cumplimiento de Office 365*

*Ley de transferencia y responsabilidad de seguros de salud (HIPAA): la HIPAA se exige a los clientes que puedan ser "entidades afectadas" [...].*

*Acuerdos de procesamiento de datos (DPA): damos a los clientes garantías contractuales adicionales mediante los DPA con respecto al control y protección de datos del cliente que ejerce Microsoft. Al firmar los DPA adoptamos más de 40 compromisos específicos de seguridad recopilados a partir de normativas internacionales. (Los clientes con acuerdos empresariales deben ponerse en contacto con el representante de su cuenta para obtener el DPA).*

*Ley federal estadounidense de protección de la información (FISMA): FISMA exige a los organismos federales estadounidenses que desarrollen, documenten e implementen controles que aseguren la información y los sistemas de información. En la sección Preguntas más frecuentes sobre la ley FISMA se describe la forma en que el servicio Office 365 cumple los procesos de seguridad y privacidad relacionados con esta ley.*

*ISO 27001: ISO 27001 es una de las mejores referencias sobre seguridad disponibles en el mundo. Office 365 es el principal servicio público en la nube de productividad empresarial que ha implementado el estricto conjunto de controles físicos, lógicos, procedimentales y administrativos definidos por ISO 27001.*

*Cláusulas modelo de la Unión Europea (UE): la directiva sobre protección de datos de la UE, instrumento fundamental de la legislación sobre derechos humanos y la privacidad de la UE, exige a nuestros clientes en la Unión Europea que legitimen la transferencia de datos personales fuera de la UE. Se reconocen las cláusulas modelo de la UE como método preferido para legitimar la transferencia de datos personales fuera de la UE en entornos de informática en nube. El ofrecimiento de las cláusulas modelo de la UE implica invertir y crear los controles y procesos operativos necesarios para satisfacer los requisitos exactos de estas cláusulas. Si un proveedor del servicio de nube no está dispuesto a acceder a las cláusulas modelo de la UE, un cliente no tendría la seguridad de que pueda cumplir con los requisitos de la directiva sobre protección de datos de la UE para la transferencia de datos personales desde la Unión Europea a jurisdicciones que no ofrezcan una "protección adecuada" de los datos personales. En la sección Preguntas más frecuentes sobre las cláusulas modelo de la UE se describe el enfoque refrendado*

*por un organismo regulador de Microsoft con respecto a estas cláusulas.*

*Principios de Puerto Seguro de la UE y EE. UU. estos principios también permiten a los usuarios transferir legalmente datos personales fuera de la Unión Europea en virtud de la directiva sobre protección de datos de la UE. Office 365 sigue los principios y procesos estipulados en los Principios de Puerto Seguro de la UE y EE. UU.*

*Ley de derechos educacionales y privacidad de la familia (FERPA): FERPA exige requisitos a las organizaciones educativas de Estados Unidos con respecto al uso o la confidencialidad de los registros de educación de los alumnos, incluido el correo electrónico y los datos adjuntos. Microsoft acepta las restricciones de uso y confidencialidad exigidas por FERPA que limitan el uso que hacemos de los registros de educación de los alumnos, lo que incluye no examinar correos electrónicos ni documentos con fines publicitarios.*

*Certificación SSAE 16 (Statement on Standards for Attestation Engagements No. 16): Office 365 se ha sometido a auditorías realizadas por terceros independientes y puede proporcionar informes de tipo I y tipo II de SOC 1 de SSAE16 sobre la forma en que el servicio implementa controles.*

*Ley PIPEDA (Personal Information Protection and Electronic Documents Act) canadiense: esta ley está relacionada con la manera en que organizaciones del sector privado recopilan, usan y revelan información personal en el curso de actividades comerciales. Microsoft admite el cumplimiento con PIPEDA a través de nuestra administración de Office 365.*

*Ley GLBA (Gramm-Leach-Bliley Act): esta ley exige que las entidades financieras implementen procesos para proteger la información personal no pública de sus clientes [...]*

En base a esta información, se recomienda encarecidamente a la hora de firmar el contrato de prestación de servicios con Microsoft, **aclarar el contenido y alcance de los “DPA”** (Acuerdos de Procesamiento de Datos) y los compromisos específicos de seguridad:

*Acuerdos de procesamiento de datos (DPA): damos a los clientes garantías contractuales adicionales mediante los DPA con respecto al control y protección de datos del cliente que ejerce Microsoft.*

También verificar que se cumple con lo exigido por la AEPD en lo relativo a las **Cláusulas modelo de la UE** en cuestión de Protección de Datos Personales y en concreto, las adicionales que afectan a la Legislación Española, analizada en el primer punto (LOPD).

## **Office 365. Conclusiones finales y recomendaciones.**

Habiendo auditado y contrastado la información que proporciona Microsoft sobre “Office 365 para la Educación”, así como otras fuentes y recursos externos, se puede afirmar que el producto consta de los controles y medidas necesarias para proporcionar unos niveles adecuados de Seguridad y Privacidad para unos recursos externalizados y en la “nube”.

Junto a las anteriores expuestas en puntos anteriores y más concretas, la recomendación general para la Consejería de Educación habiendo analizado estas cuestiones de privacidad, seguridad, ubicación y uso de los datos, es informar de forma clara y concisa en las condiciones legales y de uso a los usuarios sobre quién almacena la información, la utilización que debe hacerse de ella, aclarando el papel de Microsoft como proveedor de servicios, y de la Consejería de Educación como administradores de las cuentas de usuario.

De igual forma, informar en las condiciones legales y de uso sobre cuáles son las responsabilidades de la Consejería de Educación, las de Microsoft y las del usuario en la gestión y uso de los recursos y herramientas englobadas en “Office 365 para la Educación”.

También vigilar posibles cambios en las condiciones de uso del servicio que afecten al usuario final dado el marco normativo tan cambiante en lo relativo al “*Cloud Computing*”.

Sería recomendable dotar de una necesaria y adecuada formación en Privacidad y Seguridad tanto al personal docente, como al administrativo y técnico que gestione las cuentas.

Dado que el uso mayoritario de “Office 365” está basado en el navegador del usuario, se recomienda reforzar los niveles de Privacidad y Seguridad modificando la configuración por defecto, además de instalando plugins para impedir el rastreo y recopilación de datos de navegación, o la visualización de publicidad en línea.

En concreto, la recomendación sería el uso de DoNotTrack Plus, junto a AdBlock +. Ambos plugins están disponibles para los navegadores Mozilla Firefox y Google Chrome. Sobre la modificación en la configuración por defecto del navegador, se proporcionaría por parte del Consultor, la información técnica necesaria y una “configuración tipo” al personal técnico.

Y para que así conste, se firma en Oviedo a 18 de agosto de 2014.

LOPD  
Fdo

