INFORME DE SEGURIDAD
LEY DE PROTECCIÓN DE DATOS
LOPD 15/1999 - RD 1720/2007

Google Apps For Education
Microsoft Office 365

UNIVERSIDAD DE VIGO

Área TIC

EL ‘CLOUD COMPUTING’ EN LAS ADMINISTRACIONES PÚBLICAS

CONSIDERACIONES GENERALES

GOOGLE APPS FOR EDUCATION

1. Cumplimiento de “Google Apps For Education” respecto al Esquema Nacional de Seguridad
2. Cumplimiento de “Google Apps For Education” respecto a la Ley Orgánica de Protección de Datos y su Reglamento de Desarrollo
3. Foro de Universidades en la Nube (FUN)

Conclusiones

Referencias

MICROSOFT OFFICE 365

1. Cumplimiento de “Google Apps For Education” respecto al Esquema Nacional de Seguridad
2. Cumplimiento de “Google Apps For Education” respecto a la Ley Orgánica de Protección de Datos y su Reglamento de Desarrollo
3. Código de conducta para proteger los datos personales en la nube: ISO/IEC 27018

Conclusiones

Referencias

EL 'CLOUD COMPUTING' EN LAS ADMINISTRACIONES PÚBLICAS

CONSIDERACIONES GENERALES

El volumen y la sensibilidad de los datos que gestionan las Administraciones Públicas conllevan unos riesgos específicos que deben ser objeto de un análisis riguroso en cada escenario en el que se plantee su utilización. Estos riesgos específicos aconsejan la adopción de cautelas adicionales en su implantación, de forma que no se vean comprometidos los derechos y la seguridad de los ciudadanos.
La posibilidad de tratamiento de los datos fuera del territorio nacional, característica del *cloud computing*, constituye un elemento de especial relevancia en el caso de las Administraciones Públicas. En este sentido, debe tenerse en cuenta que la normativa que regula los movimientos internacionales de datos es aplicable tanto a entidades públicas como privadas.

En particular, debe tenerse muy presente que Autoridades competentes de terceros países en los que se traten datos personales en el marco de los servicios de *cloud computing* podrían solicitar y acceder a la información de la que las Administraciones públicas son responsables, en algunos casos, sin que se le informe de esta circunstancia. Por ello es fundamental obtener información del prestador de servicios de *cloud computing* sobre si existe esta posibilidad en alguno de los países donde se vayan a tratar los datos, si la Administración contratante puede conocer o no tales requerimientos, así como las decisiones que puede tomar al respecto. La trascendencia de estos posibles accesos es un factor muy relevante para decidir sobre la contratación de estos servicios y el proveedor que los vaya a prestar.

Además de la **LOPD** y de su **Reglamento de Desarrollo**, las Administraciones Públicas están sujetas a un marco legal específico al cual debe adecuarse la prestación de servicios basados en *cloud computing*:

- Ley de Contratos del Sector Público. (RD Legislativo 3/2011, de 14 de noviembre).
- Ley 11/2007 de Acceso Electrónicos de los Ciudadanos a los Servicios Públicos, y RD 1671/2009 que desarrolla parcialmente esta ley.
- El Esquema Nacional de Seguridad (ENS) y el Esquema Nacional de Interoperabilidad (ENI) (Reales Decretos 3/2010 y 4/2010, de 8 de enero), previstos en el artículo 42 de la Ley 11/2007, de acceso electrónico de los ciudadanos a los Servicios Públicos.

GOOGLE APPS FOR EDUCATION

Google Apps for Education es un paquete de aplicaciones Web personalizables y escalables.

La licencia es totalmente gratuita, y sin publicidad, para alumnos, docentes y personal administrativo del establecimiento. Permite al centro otorgar diferentes servicios a los docentes/ alumnos, por ejemplo, haciendo que los alumnos solo puedan comunicarse dentro del dominio de la universidad, si esa es la política del mismo, mientras que los docentes pueden hacerlo hacia el exterior también. Incrementa la implicación y comunicación en tiempo real a través del calendario, documentos compartidos, como planilla de cálculo, procesador de texto, formularios, presentaciones, dibujos, sitios públicos o privados, grupos o foros de discusión, entre otras.

Las aplicaciones que incluye son:

- Gmail: La protección contra spam, la potente búsqueda y los calendarios integrados de Gmail ayudan a aumentar la productividad.
- Classroom te ayuda a mantener las clases organizadas y a mejorar la comunicación con los alumnos.
- Documentos: Crea y edita documentos, hojas de cálculo y presentaciones directamente desde el navegador.
  Varias personas pueden trabajar en simultáneo y cada cambio que hagan se guardará automáticamente.
- Drive: Guarda archivos de trabajos en Drive, con acceso a ellos desde cualquier dispositivo, compartiéndolos instantáneamente.
- Calendarios: calendarios que se pueden compartir y que integran a la perfección Gmail, Drive, Contactos, Sites y Hangouts.
- Sitios: Creación de un sitio Web para tu clase, tu equipo o un proyecto, todo sin escribir una sola línea de código.
- Hangouts: Contacto, en cualquier momento mediante video, voz o texto. Usa chat de texto para preguntas rápidas y Hangouts para videollamadas grupales, horas de consulta virtual y excursiones.

Al contratar dicho servicio, el usuario concede a Google el tratamiento de determinados datos personales y por tanto la relación entre ambas partes se encuentra sujeta a la normativa de protección de datos. De hecho, tal como se describe en los propios términos y condiciones, Google reconoce ser el **Encargado del Tratamiento** durante la prestación del servicio "Google Apps for Education":

"(…) For the purposes of this Agreement and in respect of Customer Personal Data, the parties agree that Customer shall be the controller and Google shall be a processor. Within the scope of this Agreement, Customer shall comply with its obligations as a controller and Google shall comply with its obligations as a processor under the Data Protection Legislation".

Lamentablemente, en dichos términos y condiciones, a los que se adhiere el usuario *de facto* al contratar el servicio "Google Apps for Education", no se contemplan las obligaciones exigidas por la normativa de protección de datos del *"art. 12 LOPD.- Acceso a los datos por cuenta de terceros"*. En este caso pues, de acuerdo con la normativa, si el usuario contrata este servicio sin haber firmado un **contrato de encargado del tratamiento** puede incurrir en una infracción leve (art. 44.2.d) LOPD) y ser sancionado con una **multa de hasta 40.000 euros**. Por otro lado, considerando que este servicio realiza además **transferencias internacionales** a empresas ubicadas a países con un nivel no adecuado de protección, el usuario puede incurrir también en otra infracción tipificada como muy grave (art.44.4.d) LOPD) y la sanción podría llegar a ascender hasta **600.000 euros**.

En este sentido, tal como han alertado algunas Autoridades de Protección de Datos, el usuario que contrata el servicio "Google Apps for Education" asume algunos **riesgos** y por tanto es necesario realizar los trámites oportunos para cumplir con la normativa.

A raíz de ello, con el fin de que usuarios de "Google Apps for Education" pudieran cumplir con la normativa de protección de datos, Google ha establecido **un mecanismo (opt-in)** mediante el cual éstos pueden adherirse voluntariamente a la Adenda de Tratamiento de Datos.

La Adenda de Tratamiento de Datos se trata de un documento que cumple con los requisitos esenciales de la normativa de protección de datos en lo que respecta al contrato de encargado del tratamiento. Asimismo, ofrece unas Cláusulas Contractuales Tipo, a los efectos de regular las transferencias internacionales de datos efectuadas a países con un nivel no adecuado de protección en cumplimiento de lo establecido por la Comisión Europea (Decisión 2001/497/CE).

En esta Adenda de Tratamiento de Datos se tiene ya en cuenta la entrada en vigor del Reglamento Europeo:

"version 1.6 of the Data Processing Amendment will apply (in relation to G Suite Agreements) until 24 May 2018 inclusive and, as from 25 May 2018 (when the EU's General Data Protection Regulation comes into force), will be replaced by Version 2.0 of the Data Processing Amendment (below)"

Así pues, atendido el marco legal al que se encuentra sujeto el servicio "Google Apps for Education", **es importante que sus usuarios se adhieran** a los citados documentos para **cumplir con la normativa de protección de datos** y de esa forma evitar cualquier irregularidad en materia de protección de datos. Los citados acuerdos pueden aceptarse a través de un proceso de línea que se describe **aquí**.

1. Cumplimiento de"Google Apps For Education" respecto al Esquema Nacional de Seguridad

Se adjunta certificado emitido de cumplimiento a 16 de octubre del 2017, y renovable el 16 de octubre del 2019.

https://cloud.google.com/files/GoogleCloud-CertificadoENS2017.pdf

Este certificado ha sido emitido por la prestigiosa empresa BDO AUDITORES, S.L.P.

2. Cumplimiento de "Google Apps For Education" respecto a la Ley Orgánica de Protección de Datos y su Reglamento de Desarrollo.

Las transferencias internacionales de datos, se regulan en los artículos 33 y 34 de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (LOPD) y en el Título VI del Reglamento de desarrollo de la Ley Orgánica de Protección de Datos de Carácter Personal, aprobado por el Real Decreto 1720/2007, de 21 de diciembre, (RLOPD).

Una transferencia internacional de datos, es un tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo (EEE), bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español (art. 5.1.s) RLOPD).

El exportador de datos es la persona física o jurídica, pública o privada, u órgano administrativo situado en territorio español que realiza una transferencia de datos de carácter personal a un país tercero (art. 5.1.j) RLOPD).

El importador de datos es la persona física o jurídica, pública o privada, u órgano administrativo receptor de los datos, en caso de transferencia internacional de los mismos a un tercer país, ya sea responsable del tratamiento, encargado del tratamiento o tercero. (art. 5.1.ñ) RLOPD).

Para realizar transferencias internacionales de datos, será necesaria la Autorización previa de la Directora de la Agencia Española de Protección de Datos, salvo que se ampare en alguno de los supuestos de excepción previstos en los apartados a) a j) del artículo 34 de la LOPD o cuando el Estado en el que se encuentre el importador ofrezca

un nivel adecuado de protección, supuestos en los que en todo caso se deberán notificar las transferencias internacionales de datos al Registro General de Protección de Datos para su inscripción a través de sistema NOTA de notificación de ficheros.

La Autorización de transferencia internacional de datos no excluye en ningún caso la aplicación de las disposiciones contenidas en la LOPD y en el RLOPD.

Países con un nivel adecuado de protección.

Hasta la fecha han sido declarados como países con nivel adecuado de protección los siguientes:

Suiza. Decisión 2000/518/CE de la Comisión, de 26 de julio de 2000

Canadá. Decisión 2002/2/CE de la Comisión, de 20 de diciembre de 2001, respecto de las entidades sujetas al ámbito de aplicación de la ley canadiense de protección de datos

Argentina. Decisión 2003/490/CE de la Comisión, de 30 de junio de 2003

Guernsey. Decisión 2003/821/CE de la Comisión, de 21 de noviembre de 2003

Isla de Man. Decisión 2004/411/CE de la Comisión, de 28 de abril de 2004

Jersey. Decisión 2008/393/CE de la Comisión, de 8 de mayo 2008

Islas Feroe. Decisión 2010/146/UE de la Comisión, de 5 de marzo de 2010

Andorra. Decisión 2010/625/UE de la Comisión, de 19 de octubre de 2010

Israel. Decisión 2011/61/UE de la Comisión, de 31 de enero de 2011

Uruguay. Decisión 2012/484/UE de la Comisión, de 21 de agosto de 2012

Nueva Zelanda. Decisión 2013/65/UE de la Comisión, de 19 de diciembre de 2012

Estados Unidos. Aplicable a las entidades certificadas en el marco del Escudo de Privacidad UE-EE.UU. Decisión (UE) 2016/1250 de la Comisión, de 12 de julio de 2016. En la página web del Escudo de privacidad se accede a la relación de las entidades certificadas: https://www.privacyshield.gov/list

El **Puerto Seguro**, o Safe Harbour, venía a simplificar las transferencias internacionales de datos realizadas hacia empresas de Estados Unidos. Pero la Sentencia del Tribunal de Justicia de la Unión Europea de 6 de octubre de 2015 ha venido a dar un sonoro portazo a este sistema.

Google Apps For Education estaba adherida al Safe Harbour.

El Safe Harbour ha sido sustituido por el Escudo de Privacidad UE-EE.UU. (que viene a ser prácticamente lo mismo).

El **Escudo de Privacidad** ofrece una serie de derechos y obliga a las empresas a proteger los datos personales de modo acorde con los "Principios de privacidad". Consulte la Guía acerca del Escudo de Privacidad EE.UU.-UE

¿Qué es el Escudo de Privacidad UE - EE. UU. y por qué lo necesitamos?

La Unión Europea (UE) y los Estados Unidos (EE. UU.) mantienen fuertes lazos comerciales. Las transferencias de datos personales constituyen una parte importante y necesaria de la relación transatlántica, en particular, en la economía digital global de hoy en día. Son muchas las operaciones en las que se recaban y usan datos personales, por ejemplo, nombre, número de teléfono, fecha de nacimiento, domicilio y dirección de correo electrónico, número de tarjeta de crédito, número de seguridad social, nombre de usuario, sexo y estado civil o cualquier otro tipo de información que permita identi carnos. Por ejemplo, existe la posibilidad de que recabe nuestros datos en la UE una sucursal, o un socio comercial de una empresa estadounidense que los usará posteriormente en los EE. UU.

Eso es lo que sucede, por ejemplo, cuando compramos bienes o contratamos servicios a través de internet, cuando usamos las redes sociales o servicios de almacenamiento en la nube, o en el caso de los empleados de empresas con sede en la UE pero que utilizan otra empresa en los EE. UU. (p. ej. la sociedad matriz) para tratar los datos personales. La legislación de la UE exige que los datos personales sigan gozando de un alto nivel de protección al ser transferidos a EE. UU.

Y aquí es donde interviene el Escudo de Privacidad entre la UE y los EE. UU. El Escudo de Privacidad permite que los datos personales se trans eran de una empresa de la UE a otra de los Estados Unidos, únicamente si dicha empresa procesa (es decir, usa, almacena y trans ere posteriormente) los datos personales con arreglo a una serie de normas de protección y salvaguardias bien de nidas. La protección conferida a los

datos personales se aplica con independencia de si se es o no ciudadano de la Unión Europea.

¿Cómo funciona el Escudo de Privacidad?

Para transferir datos personales desde la UE a los EE. UU., se dispone de diversas herramientas tales como cláusulas contractuales, normas corporativas vinculantes y el Escudo de Privacidad. Si se utiliza el Escudo de Privacidad, las empresas estadounidenses deben primero adscribirse a este marco en el registro a tal efecto del Departamento de Comercio de los EE. UU. Las obligaciones aplicables a las empresas sujetas al Escudo de Privacidad están descritas en los «Principios de privacidad». Dicho Departamento es responsable de gestionar y administrar el Escudo de Privacidad y de garantizar que las empresas respeten sus compromisos. Para disponer de certi cación, las empresas deben contar con una política de privacidad acorde con los Principios de privacidad, así como renovar anualmente su «a liación» al Escudo de Privacidad. En caso de no hacerlo, ya no podrán recibir y usar datos personales de la UE conforme a este marco.

Si desea saber si una empresa de los EE. UU. forma parte del Escudo de Privacidad, puede consultar la Lista del Escudo de Privacidad en el sitio web de su Departamento de Comercio (https://www.privacyshield.gov/welcome). En esta lista se incluyen los datos de todas las empresas que forman parte del Escudo de Privacidad, del tipo de datos personales que utilizan y del tipo de servicios que ofrecen. Y, además, una lista de las empresas que ya no forman parte del Escudo de Privacidad, lo que signi ca que ya no les está permitido recibir datos personales según lo establecido por el Escudo de Privacidad. Asimismo, estas empresas solo podrán guardar sus datos personales si se comprometen ante el Departamento de Comercio a que seguirán aplicando los Principios de privacidad.

Como podemos observar en este enlace **https://www.privacyshield.gov/participant_search** la compañía Google LLC está adherida al Escudo Seguro.

3. Foro de Universidades en la Nube (FUN)

El 15 de noviembre del 2011, Google anunció la creación del Foro de Universidades en la Nube (FUN) con la incorporación de catorce universidades españolas a su programa de Google Apps for Education. Los 400.000 nuevos usuarios de estas universidades se suman a los más de 15 millones de usuarios que ya utilizan Google Apps for Education a nivel mundial. Las herramientas de Google Apps que se van a implementar permitirán a las universidades trabajar en un entorno 100% web o lo que viene denominándose cloud computing.
Las universidades que inicialmente participaron fueron las siguientes:

> la IE University, Universidad Alfonso X el Sabio, Universidad Católica de Murcia, Universidad Complutense de Madrid, Universidad de Deusto, Universidad de Extremadura, Universidad de la Laguna, Universidad de León, Universidad de Navarra, Universidad Miguel Hernández de Elche, Universidad Pompeu Fabra, Universitat Autonoma de Barcelona, Universitat Jaume I, Universidad de Girona.

Todas ellas forman parte de un nuevo programa que Google ha denominado Foro de Universidades en la Nube (FUN). Esta agrupación desarrollada por Google tiene como objetivo crear un espacio en el que todas las universidades adheridas puedan compartir sus códigos de buenas prácticas e ideas además de ayudarles a mantener el contacto entre ellos. Además, con la creación de este grupo Google podrá establecer un contacto directo y simultáneo con las instituciones educativas para explicarles por ejemplo el funcionamiento de nuevas aplicaciones e informarles de novedades en Google Apps.

El acuerdo alcanzado por FUN con Google ofrecerá a los alumnos, profesores y personal administrativo, una serie de herramientas personalizables para trabajar en conjunto y para que los estudiantes puedan aprender de la manera más efectiva. Este conjunto de herramientas incluye; correo electrónico, procesadores de texto, instrumentos de comunicación y almacenamiento de ficheros privados y compartidos, configurando un 'escritorio virtual' que aumenta en espacio y servicios la actual cuenta de correo electrónico de los alumnos y que será accesible tanto a través de Internet como de dispositivos móviles.

Conclusiones

La utilización de los servicios ofrecidos por Google Apps For Education es favorable siempre y cuando se cumplan los siguientes requisitos:

1. Google Apps For Education cumple con el Esquema Nacional de Seguridad: ***se observa que se le ha concedido el certificado ENS durante el periodo Octubre 2017 – Octubre 2019***

2. Google Apps For Education cumple con los requisitos de la Ley Orgánica de Protección de Datos en cuanto a las transferencias internacionales de datos, ***estando adherida a lo que se conoce como Escudo de Privacidad EU – EE.UU***.
   Google Apps For Education, como proveedor de servicios en la nube, actúa como **Encargado de Tratamiento**, de todos aquellos datos susceptibles de tratamiento desde su plataforma.
   Para dar cumplimiento al artículo 12. Encargado de Tratamiento, la Universidad de Vigo deberá firmar el Contrato de Encargado de Tratamiento con Google.
   Este trámite lo facilita Google, y está explicado en la parte superior de este informe.

3. Como aspecto complementario, se recomienda formar parte del FUN (Foro de Universidades en la Nube).

Referencias

www.agpd.es

https://www.agpd.es/portalwebAGPD/canalresponsable/transferencias_internacionales/index-ides-idphp.php

https://espana.googleblog.com/2011/11/13-universidades-espanolas-se-suben-la.html

https://support.google.com/a/answer/2888485?hl=en

https://administracionelectronica.gob.es/ctt/ens#.Wi5cRLpFxYc

https://www.privacyshield.gov/participant_search#

MICROSOFT OFFICE 365

Incluye las aplicaciones de Office 2016: acceso a archivos desde cualquier lugar, tanto en línea como sin conexión, actualizaciones de seguridad mensuales y nuevas características enriquecidas.

Microsoft Corporation, al igual que Google, actúa como Encargado del tratamiento de todos aquellos datos que se traten desde sus plataformas.

1. Cumplimiento de "Microsoft Office 365" respecto al Esquema Nacional de Seguridad

Microsoft Office 365, ha obtenido la certificación del Esquema Nacional de Seguridad (ENS) de Nivel Alto. El ENS, regulado por el Real Decreto 3/2010, de 8 de enero, se encarga de controlar la política de seguridad que se ha de aplicar en cuanto a la utilización de medios electrónicos, con el fin de ofrecer una protección adecuada a la información de las personas en su relación con la Administración Pública. De esta manera, Microsoft añade una nueva certificación a las previamente conseguidas como la ISO 27001/27018 o la Resolución TI/32/2014 de la AEPD, que confirma las garantías adecuadas de la nube de la compañía, con el objetivo de cumplir con los más altos estándares tanto a nivel español como dentro de Europa.

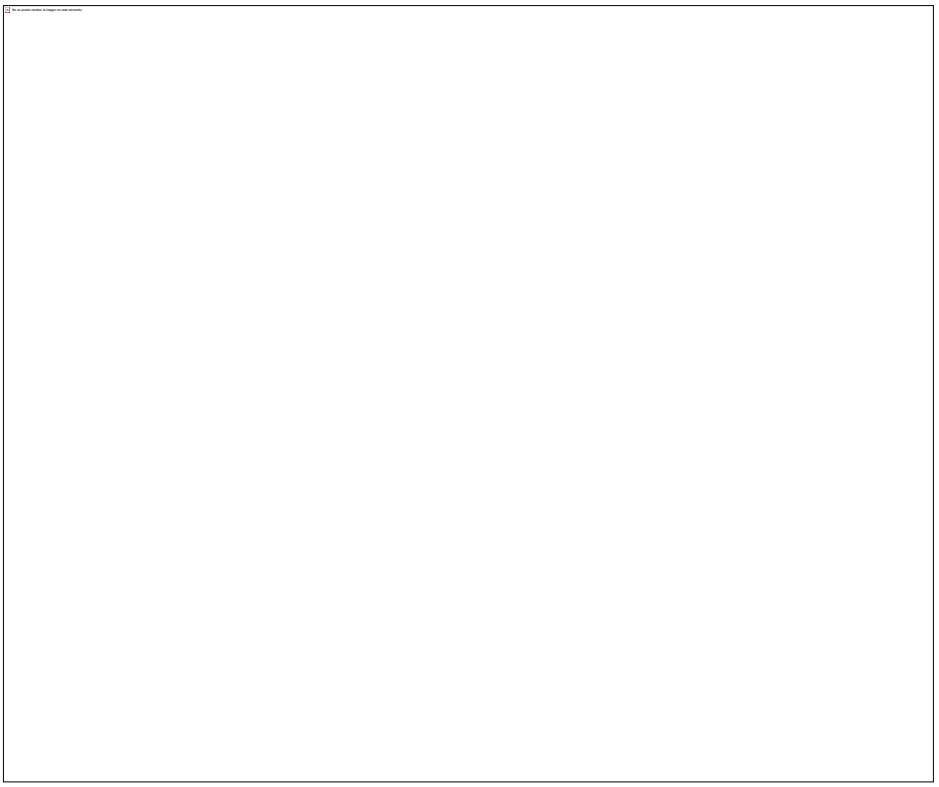
2. Cumplimiento de "Microsoft Office 365" respecto a la Ley Orgánica de Protección de Datos y su Reglamento de Desarrollo.

La certificación anterior se une a la ISO 27001/27018 y a la Resolución TI/32/2014 de la AEPD con las que ya contaba Microsoft, confirmando todas las garantías para sus servicios en la nube. La compañía cumple así con los más altos estándares tanto en España como en Europa.

Se adjunta la Resolución de la Agencia de Protección de Datos, donde en ella, Office 365 y Microsoft Azure certifican cumplir con las exigencias actuales legales en materia de seguridad. Microsoft demuestra una vez la importancia que da al cuidado de la información almacenada por sus clientes en sus servicios en la nube. Las administraciones públicas pueden estar tranquilas, trabajando con Microsoft sus datos están bien protegidos.

Al igual que en el caso de Google, Microsoft también está adherida a lo que llamamos **Escudo de Privacidad UE-EE.UU**:

Como podemos observar en este enlace **https://www.privacyshield.gov/participant_search** la compañía Microsoft está adherida al Escudo Seguro.



3. Código de conducta para proteger los datos personales en la nube: ISO/IEC 27018

La Organización Internacional de Normalización (ISO) es una organización no gubernamental independiente y la mayor entidad de desarrollo de normas internacionales voluntarias del mundo. La familia de normas ISO/IEC 27000 ayuda a que organizaciones de todos los tipos y tamaños mantengan seguros sus activos de información.

En 2014, la ISO adoptó ISO/IEC 27018:2014, un addendum a ISO/IEC 27001, el primer código de conducta internacional para la privacidad de la nube. Basándose en las leyes de protección de datos de la Unión Europea, ofrece instrucciones específicas para que los proveedores de servicios en la nube (CSP) **que actúan como Encargados del tratamiento de datos personales** (PII) evalúen los riesgos e implementen los controles más modernos para proteger dicha información.

Al seguir las normas de ISO/IEC 27001 y el código de conducta integrado en ISO/IEC 27018, Microsoft, el primer proveedor de nube que incorporó este código de práctica, demuestra que sus directivas y procedimientos de privacidad son sólidos y cumplen con sus estrictas normas.

- **Los clientes de los servicios en la nube de Microsoft saben dónde se almacenan sus datos**. Puesto que la norma ISO/IEC 27018 exige que los CSP certificados informen a los clientes de los países en los que pueden estar almacenados sus datos, los clientes de los servicios en la nube de Microsoft tienen la información que necesitan para cumplir cualquier norma de seguridad de la información aplicable.
- **Los datos de los clientes no se usarán con fines de marketing o publicidad sin su consentimiento explícito**. Algunos CSP usan datos de los clientes para sus propios fines comerciales, incluida publicidad personalizada. Puesto que Microsoft ha adoptado la norma ISO/IEC 27018 para sus servicios en la nube empresarial dentro del ámbito aplicable, los clientes pueden estar seguros de que sus datos nunca se usarán para dichos fines sin su consentimiento explícito, y que dicho consentimiento no puede ser una condición para el uso del servicio en la nube.
- **Los clientes de Microsoft saben lo que ocurre con los PII**. La norma ISO/IEC 27018 exige una directiva que permita la devolución, transferencia y eliminación segura de datos personales en un período de tiempo razonable. Si Microsoft trabaja con otras compañías que necesitan acceso a sus datos de cliente, Microsoft revela por adelantado las identidades de esos subencargados del tratamiento de datos.
- **Microsoft solo cumplirá las solicitudes jurídicamente vinculantes de divulgar datos de los clientes**. Si Microsoft tiene que cumplir con dicha solicitud, como ocurre en el caso de una investigación penal, siempre se lo notificará al cliente a menos que la ley lo prohíba.

Conclusiones

La utilización de los servicios ofrecidos por Microsoft Office 365 es favorable siempre y cuando se cumplan los siguientes requisitos:

1. Microsoft Office 365 cumple con el Esquema Nacional de Seguridad: ***se observa que se le ha concedido el certificado ENS.***

2. Microsoft Office 365 cumple con los requisitos de la Ley Orgánica de Protección de Datos en cuanto a las transferencias internacionales de datos, ***estando adherida a lo que se conoce como Escudo de Privacidad EU – EE.UU***.
   Microsoft Office 365, como proveedor de servicios en la nube, actúa como **Encargado de Tratamiento**, de todos aquellos datos susceptibles de tratamiento desde su plataforma.
   Para dar cumplimiento al artículo 12. Encargado de Tratamiento, la Universidad de Vigo deberá firmar el Contrato de Encargado de Tratamiento con Microsoft.
   (Este Acuerdo no está visible, por lo que entendemos que Microsoft lo proporciona al contratar sus servicios).

3. Dos aspectos más a tener en cuenta:

   a. **Resolución** de la Agencia de Protección de Datos favorable a Microsoft, con respecto al cumplimiento de la LOPD y RD (adjunta en la pág. 15 de este informe);

   b. **Cumplimiento** del Código de conducta para proteger los datos personales en la nube: ISO/IEC 27018.

Referencias

www.agpd.es

https://www.agpd.es/portalwebAGPD/canalresponsable/transferencias_internacionales/index-ides-idphp.php

https://espana.googleblog.com/2011/11/13-universidades-espanolas-se-suben-la.html

https://support.google.com/a/answer/2888485?hl=en

https://administracionelectronica.gob.es/ctt/ens#.Wi5cRLpFxYc

https://www.privacyshield.gov/participant_search#

https://www.microsoft.com/es-xl/TrustCenter/Compliance/ISO-IEC-27018

https://products.office.com/es-es/business/office-365-trust-center-eu-model-clauses-faq