

Nombre y apellidos: Christian Castro Navarro

Módulo: Sistemas Informáticos



Título: Explotación de aplicaciones informáticas de propósito general, tarea 1.

Introducción:

La información es el eje de esta materia. Hoy la nube nos envuelve. Ya no podemos escapar de ella. El dilema es la seguridad: ¿está protegida la privacidad de la información en la nube?

Preguntas:

1. ¿Cuál es la ley que protege la privacidad de los datos de carácter personal de la Unión Europea?
2. ¿Cuál es el reglamento en España que adapta esa ley a nuestro país?
3. De los proveedores de servicios de almacenamiento y transferencia de datos en la nube que menciona el artículo, menciona cuales son y si alguno ya se ha adaptado a la normativa europea.
4. Según el artículo, di cuál de las siguientes cosas se recomienda hacer en caso de tener que almacenar información de carácter personal en alguna nube:
 - a) Elegir una que tenga sede en la UE, con lo cual cumplirá con las normativas:
 - b) Anonimizar los datos antes de enviarlos:
 - c) Informar bien al cliente y conseguir su autorización expresa antes de subir sus datos a la nube:
 - d) Conque solo una de las recomendaciones a, b, c se cumpla, es suficiente:
 - e) Todas las recomendaciones:

Solución:

1º El reglamento general de protección de datos RGPD, es el reglamento europeo relativo a la protección de las personas físicas en la que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos. Entro en vigor el 24 de mayo de 2016 y se aplicó el 25 de mayo de 2018. Durante estos dos años las empresas, las organizaciones y organismos, se fueron adaptando para su cumplimiento. Es una normativa a nivel de la Unión Europea, por lo que cualquier empresa de la unión debe acogerse a ella.

2º En España el RGPD dejó obsoleta la Ley Orgánica de Protección de Datos de Carácter General de 1999, siendo sustituida el 6 de diciembre de 2018 la Ley Orgánica de Protección de Datos Personales y garantías de los derechos digitales, acorde con el RGPD.

3º De los servicios mencionados en el artículo son dos los que hacen mención del GDPR en sus páginas web, Dropbox y Google Drive. Aunque como expresa el artículo, no se han terminado de adaptar a lo expuesto a la STJUE 16/7/2020. Por lo tanto, en términos generales ninguno de estos dos servicios cumpliría expresamente lo que en realidad se viene pidiendo en esta ley.



Por un lado, tenemos Dropbox, una de las herramientas de almacenamiento en la nube y envío de datos más extendido. En su página web nos aclara como Dropbox cumple con la normativa RGPD. Entre otros cambios han nombrado a un delegado de protección de datos, han reformulado su programa de privacidad para garantizar que los usuarios puedan ejercer sus derechos como partes interesadas, así como documentar las actividades de procesamiento de datos y reforzar los procesos internos en caso de que se produzcan problemas de seguridad.



También Google implementa estos cambios y someten sus productos a las verificaciones independientes de los controles de seguridad, privacidad y cumplimiento para recibir certificaciones, atestaciones e informes de auditoría que demuestran su cumplimiento. En su web podemos ver estos recursos de cumplimiento según la región, donde nos encontremos.

Por ejemplo, EMEA es la zona de Europa. Entre otras encontramos la adaptación de las normativas para Google Drive al GDPR en Europa.

Por ejemplo, Google Cloud y el RGPD: “En Google Cloud impulsamos iniciativas que priorizan y mejoran la seguridad como la privacidad de los datos personales de los clientes.”

1. En contrato se comprometen a cumplir los requisitos RGPD en todos sus servicios Google GCP y Google Workspace.
2. Añaden más funciones de seguridad para proteger mejor los datos personales.
3. Facilitan la documentación y los recursos necesarios para que se evalúen la privacidad que ofrecen en los servicios.
4. Siguen desarrollando más prestaciones de seguridad.

4º Para este apartado, es importante aclarar que se hace mención de las tres posibles alternativas, pero no dice en ningún momento que estas deban darse en conjunto para que fueran efectivas. La respuesta correcta sería la e) todas las recomendaciones.

Para terminar, me gustaría añadir el problema que realmente supone este tipo de servicios y la falta de información e incluso la desinformación que los proveedores tienen con el cliente final o consumidor final.

Referente a la actividad 3ª de entre todos estos servicios, considero que Dropbox y Google Drive al menos hacen referencia en sus páginas web a este tipo de información. No obstante, como se ha aclarado en la propia actividad no son ni de lejos una alternativa segura para el consumidor final.

Por otro lado, tenemos proveedores de servicios como WhistleB. Que trabaja con Microsoft Azure. Microsoft Azure permite que todos los clientes de Europa sean almacenados y tratados dentro del territorio de la Unión Europea. WhistleB cifra los datos que tiene almacenados de cada cliente y son solamente ellos quienes tienen la clave de cifrado, de este modo es solo el cliente quien tiene acceso a la información y puede dar acceso a quien desee.

Pero, finalmente ¿Es todo esto real?, o solo un espejismo o una distracción. En mi opinión al cliente final o lo que es lo mismo nosotros, estamos realmente desinformados en cuanto a este tema se refiere. Creo que de momento poco podemos hacer en un mundo donde el análisis de datos ha tomado un papel tan importante y se invierte grandísimas cantidades de dinero para seguir recabando datos. Esto lleva dándose desde hace años y nadie nos ha advertido de nada hasta que hemos tenido algunos casos graves, donde se ha dado una filtración de datos importante o se han usado en beneficios propios.

Poco podemos hacer ya, cuando nos han estado acostumbrando a regalar nuestra información más privada a redes sociales sin tener ni idea de quien controla toda esa información.

