TAREA 1

- **TÍTULO**

LA NUBE Y LA PRIVACIDAD

- **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?

- **RESUELVE:**

1. ¿Cuál es la ley que protege la privacidad de los datos de carácter personal en 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 en la nube que menciona el artículo, menciona cuáles son y si alguno(s) ya se ha(n) adaptado a la normativa europea, destácalo(s).
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 Unión Europea, con lo cual cumpliría con la normativa; 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 o e) todas las recomendaciones a) b) y c) deben cumplirse simultáneamente.

- **RECURSOS**

Se deberá consultar el contenido de la unidad 7, internet, libros, revistas y utilizar medios informáticos para la presentación del caso práctico (Word, Power-Point…), y especialmente el siguiente artículo de El Español hace un buen análisis legal: https://www.elespanol.com/invertia/observatorios/digital/20210207/google-drive-dropbox-mailchimp-riesgos-personales-clientes/556694800_0.html (se adjunta en PDF)

- **CRITERIOS DE CALIFICACIÓN**

A partir de ahora, se dará más peso a la solución técnica que a la presentación.

Solución correcta de la instrucción 1: 1 puntos
Solución correcta de la instrucción 2: 1 puntos
Solución correcta de la instrucción 3: 2 puntos
Solución correcta de la instrucción 4: 2 puntos
El trabajo se entrega en el formato de fichero indicado: 1 punto
Indica tu nombre e identifica la asignatura, unidad y tarea en el documento que entregas: 1 punto
Aportas conclusiones y/o reflexiones: 1 punto
Aporte de información adicional relevante: 1 punto

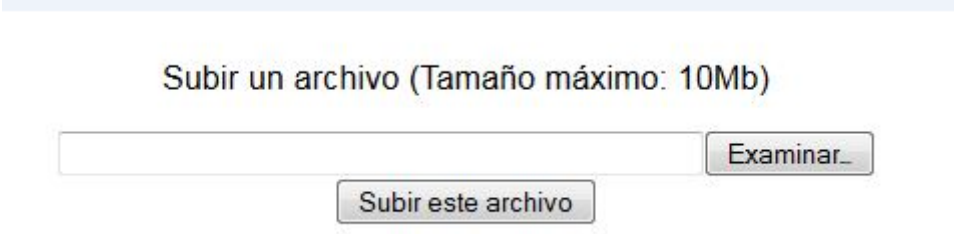
(La calificación final de esta actividad se pondera en base a un máximo de 10 puntos)

- **CÓMO PROCEDER PARA SU EVALUACIÓN**

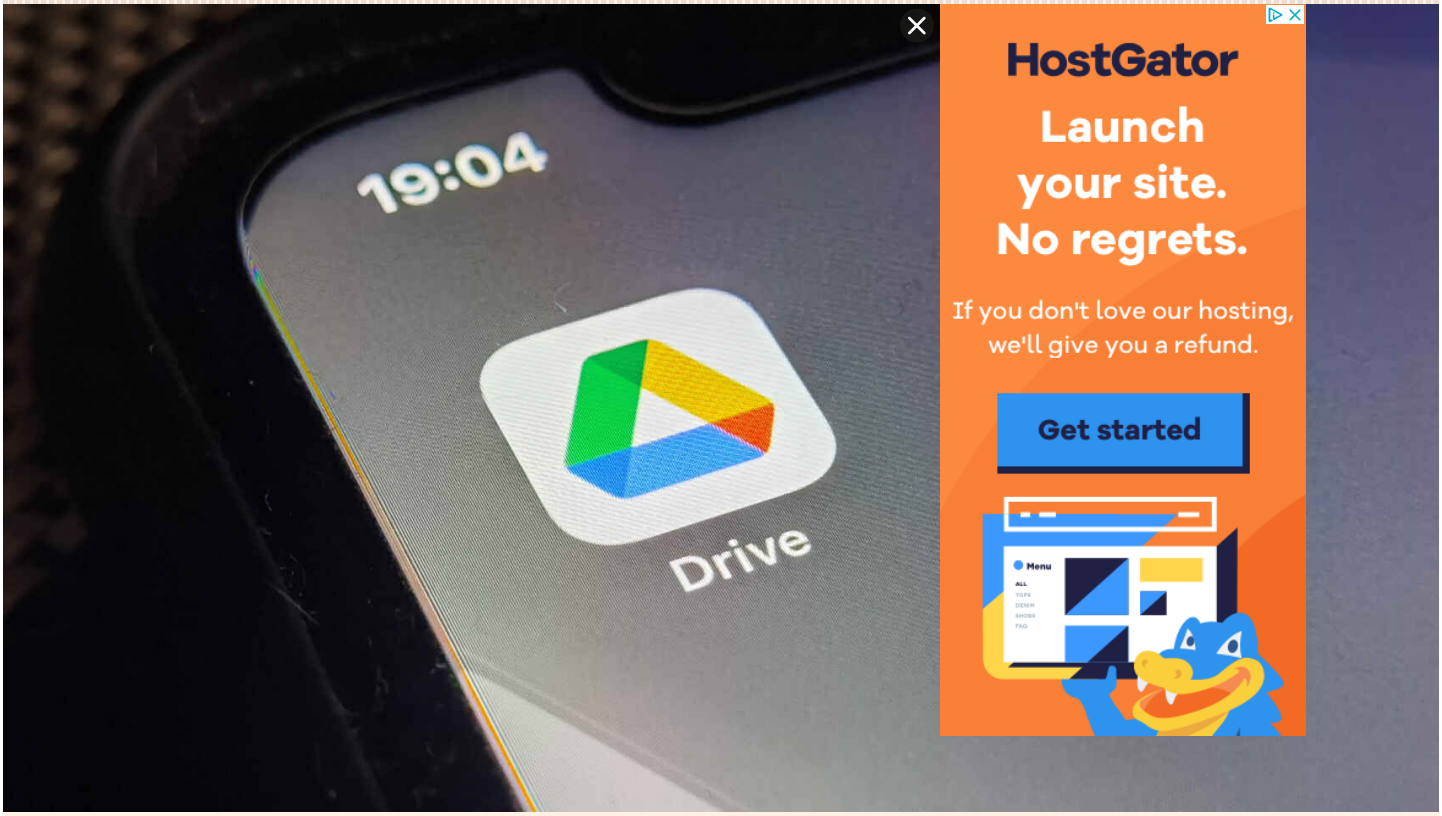
Una vez realizado el caso práctico se deberá generar un documento en **PDF.** El envío se realizará a través de la plataforma de la forma establecida para ello el archivo se nombrará siguiendo las siguientes pautas:

Apellido1_apellido2_nombre_NombredelMódulonºUDnº_Casonº**.pdf**

1. Pulsar en el apartado "Caso práctico" de la unidad correspondiente para obtener el contenido a realizar de la tarea.
2. Realizar la tarea y exportarla en .PDF
3. Para enviar la prueba, pulsar en el apartado "Subir un archivo" tal y como se muestra en la siguiente imagen:



4. Pulsar en "Examinar" y elegir el archivo correspondiente.
5. Pulsar en "Subir este archivo".



Google Drive, en una imagen de archivo. Adrián Raya • Omicrono

Google Drive, Dropbox, Mailchimp… ojo con los riesgos legales de subir datos personales de clientes

El fin del Escudo de Privacidad abre la puerta a nuevas responsabilidades legales en la transferencia internacional de datos personales.

7 febrero, 2021 - 02:11

EN: DROPBOX GOOGLE

Alejandro Álvarez Serrano

Noticias relacionadas

- Los impuestos que llegan en 2021: abróchense el cinturón, las curvas continúan
- Del ERTE al ERE: ¿por qué las empresas se dan cuenta ahora de que no pueden despedir?
- Desmontando la ley del teletrabajo: estos son los puntos que más afectan a los

Son **muchas las entidades -empresas,** pymes y autónomos, fundaciones, ONG- **que utilizan estos medios de almacenamiento digital** y de **difusión masiva de correos electrónicos** en su día a día. Lo que muchas no saben es que están radicados en Estados Unidos y que esto tiene implicaciones y riesgos legales en materia de protección de datos.

Para aclarar un poco el panorama y los roles, es necesario señalar que la pyme, organización o autónomo que utiliza estos medios tiene el rol de "responsable de tratamiento" de los datos personales.

Y cada vez que "sube" información de terceros a estas plataformas estaría realizando una **transferencia internacional de datos, tal como lo define el Reglamento General de Protección de Datos (RGPD).** Y, para cerrar el círculo, **las empresas** como Google Drive, Microsoft One Drive o Dropbox, serán

trabajo digital colaborativo.

El fin del Escudo de Privacidad

Pero sí aclara que el responsable de tratamiento sólo elegirá un encargado del tratamiento de datos personales que ofrezca garantías suficientes en materia de protección de datos; es decir, el responsable debe confirmar que el encargado es originario de un país donde se garanticen niveles de protección de datos similares o superiores a los de la **Unión Europea (UE).** Y de su falta de diligencia -se sobreentiende- se derivarán responsabilidades.

Todo esto estaba solucionado hasta hace pocos meses, cuando en las relaciones entre la Unión Europea y los Estados Unidos regía un marco normativo conocido como Escudo de Privacidad. Pero **desde que se publicó la Sentencia del Tribunal de Justicia de la Unión Europea de 16 de julio de 2020**, también denominada *Scheme II*, este "Escudo" ha quedado invalidado.

Como solución, el RGPD prevé que para una transferencia internacional de datos entre distintas entidades, se puedan pactar CCT o Cláusulas Contractuales Tipo -*SCC*, las siglas en inglés de *Standard Contractual Clauses*-. Pero la citada sentencia también alude a las CCT.

Por una parte, dice que aunque estas cláusulas sean aplicables al exportador y al importador de los datos, no son vinculantes para un tercer país (en este caso, para Estados Unidos).

Por otra, que no hay garantías ni protección equivalentes al art. 52 de la Carta de los Derechos Fundamentales de la Unión Europea en caso de cualquier injerencia de programas de vigilancia, como las que puede realizar el **Gobierno estadounidense** en virtud de la **USA Patriot Act de 2001.**

¿Consentimiento del usuario?

En tercer lugar, el **Tribunal de Justicia de la Unión Europea** considera que la

existentes en la UE que permita a las personas recurrir y contar con garantías sobre sus datos personales transferidos a ese país.

Por otra parte, y reforzando esta idea, el **EDPB (Comité Europeo de Protección de Datos o, en inglés, European Data Protection Board)** también se ha pronunciado sobre la situación legal de **Estados Unidos** en materia de privacidad: "el Derecho estadounidense (...) no garantiza un nivel de protección sustancialmente equivalente" de la normativa europea de protección de datos".

En definitiva, que un proveedor estadounidense de este tipo de servicios cuente con unas **Cláusulas Contractuales Tipo** no da seguridad de estar contratando a un encargado de tratamiento que cumpla con todas las garantías que exige el **Reglamento General de Protección de Datos.**

Pongámonos en el caso de que el usuario nos lo permite: ¿qué ocurriría si el titular de los derechos consiente en que se produzca una transferencia internacional? El RGPD considera que el consentimiento de los titulares de los derechos solo sería suficiente si lo ha hecho de forma explícita y tras haber sido informado de los posibles riesgos que entraña la inexistencia de garantías adecuadas.

Además, la transferencia debe cumplir una serie de requisitos y solo se podrá llevar a cabo si no es repetitiva; si afecta a un número limitado de interesados; si es **necesaria a los fines de intereses legítimos imperiosos** del responsable del tratamiento, pero solo si no prevalecen los intereses o derechos y libertades del interesado; si el responsable del tratamiento evaluó correctamente todas las circunstancias relacionadas con la transferencia y ofreció garantías apropiadas para la protección de datos.

Las alternativas

Por otra parte, el responsable del tratamiento está obligado a informar tanto a la

se convirtió en el primer proveedor *cloud* en trabajar con las autoridades europeas de protección de datos para la aprobación de las cláusulas modelo europeas, fue pionera también en adoptar nuevos estándares técnicos para la privacidad en la nube, y firmes defensores del **GDPR** desde su primera propuesta en el año 2012.

Otras soluciones nube aún no se han adecuado a la **Normativa Europea**, a pesar de que en sus páginas web traten sobre dicha adecuación. Por ejemplo, **Google y Dropbox** -entre otras- no hacen referencia a la realidad vigente tras la STJUE 16/7/2020 en sus términos y condiciones sobre transferencia internacional, y la impresión que ofrecen es que siguen sin adecuarse.

Ante este panorama, una alternativa real es la de que el prestador de servicios, aunque sea de origen estadounidense, tenga ubicados los servidores, la sede, etc. en territorio de la **Unión Europea,** por lo que tendría que cumplir la legislación europea.

Otra solución es la de la anonimización de los datos, de tal modo que no se aporten datos personales –y ya no se esté sujeto a las normas del RGPD- y solo se aporten números que no tengan referencia con personas identificables (puede consultarse en este sentido la Guía publicada por la Agencia Española de Protección de Datos (AEPD) en 2016, y revisada en 2019, sobre la anonimización de datos personales).

Si la pyme, el autónomo, la asociación u ONG quiere seguir utilizando este tipo de servicios de prestadores de **Estados Unidos,** será imprescindible contar con el consentimiento informado y expreso de los interesados. También estar al corriente de las comunicaciones que haga sobre esta materia la UE y también de las medidas que vaya adoptando el proveedor, estudiando pormenorizadamente su política.

En estos casos concretos, será imprescindible que el **Delegado de Protección de Datos** o el bufete que asesore a la entidad en materia de privacidad lleve a cabo auditorías periódicas para detectar posibles cambios y analizar el impacto legal de los mismos.