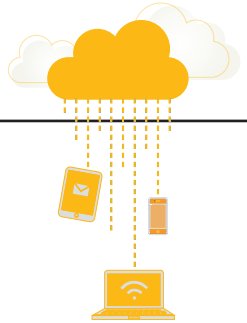
AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

GUÍA

para clientes que contraten servicios de

Cloud Computing



GUÍA

para clientes que contraten servicios de Cloud Computing

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

índice

¿QUÉ ES ‘CLOUD COMPUTING’?

El *cloud computing* o computación en *nube* es una nueva forma de prestación de los servicios de tratamiento de la información, válida tanto para una empresa como para un particular y, también, para la Administración Pública.

Una solución *cloud computing* permite al usuario optimizar la asignación y el coste de los recursos asociados a sus necesidades de tratamiento de información. El usuario no tiene necesidad de realizar inversiones en infraestructura sino que utiliza la que pone a su disposición el prestador del servicio, garantizando que no se generan situaciones de falta o exceso de recursos, así como el sobrecoste asociado a dichas situaciones.

En un entorno de *cloud computing* la gestión de la información está de forma virtual en manos del cliente que contrata los servicios de la *nube*, que la trata a través de Internet accediendo a soluciones de bases de datos, correo electrónico, o cualquier tipo de aplicaciones de acuerdo a sus necesidades. En función del modelo utilizado, los datos pueden no estar realmente en manos del contratista, toda vez que la propiedad, el mantenimiento y gestión del soporte físico de la información, los procesos y las comunicaciones pueden encontrarse en manos de terceros. El proveedor del servicio puede encontrarse en, prácticamente, cualquier lugar del mundo y su objetivo último será proporcionar los servicios citados optimizando sus propios recursos a través de, por ejemplo, prácticas de deslocalización, compartición de recursos y movilidad o realizando subcontrataciones adicionales.

De esta forma, el *cloud computing* representa una nueva forma de utilizar las tecnologías de la información y las comunicaciones, que se basa en emplear técnicas ya existentes de una forma innovadora y, sobre todo, a una nueva escala. Esto último es lo que la hace realmente distinta, ya que permite el uso de recursos de hardware, software, almacenamiento, servicios y comunicaciones que se encuentran distribuidos geográficamente y a los que se accede a través de redes públicas, de forma dinámica, cuando se necesita, mientras se necesita y abonando una tarifa (cuando no es gratuita) sobre lo que se consume; es decir, proporcionando a sus clientes un servicio de tecnologías de información bajo demanda.

Como consecuencia de lo anterior, el mismo contratista puede desconocer la localización precisa de sus datos y no disponer del control directo de acceso a los mismos, de su borrado y de su portabilidad, ya que la información no está físicamente en su poder aunque, si esa información contiene datos de carácter personal, sí está bajo su responsabilidad desde el punto de vista del Reglamento (UE) 2016/679, de 27 de abril de 2016, General de Protección de Datos (RGPD).

ACTORES EN EL MODELO DE 'CLOUD COMPUTING'

Podemos decir que se están utilizando servicios de *cloud computing* cuando encontramos empresas, entidades, departamentos, etc., a los que llamaremos usuarios o clientes, que para implementar sus procesos de tratamiento de información comparten los mismos recursos a través de la red; recursos proporcionados por una entidad distinta, llamada proveedor de servicios de *cloud computing* o proveedor de la *nube*.

Aparte de clientes y proveedores, existen otros actores en el mundo del *cloud computing*. Entre ellos destacan los socios o *partners* de los proveedores de *cloud*. Estos crean, ofrecen y soportan servicios adicionales en la *nube* que venden al usuario final como licencias de uso, por ejemplo, creando una aplicación de marketing que se ejecuta en la *nube* a partir de servicios más básicos de la misma. Los *partners* se sitúan entre el cliente y el proveedor de la *nube*, pudiendo formalizar su relación con este último con distintas figuras contractuales (*reseller*, vendedor independiente, etc).

TIPOS DE 'CLOUD COMPUTING'

No todos los servicios y proveedores de *cloud computing* son iguales, ni lo son las posibles relaciones que se establecen entre clientes y proveedores. Las *nube*s se pueden clasificar de muchas formas atendiendo a varios criterios y lo que más interesa, desde el punto de vista de la normativa

española de protección de datos, es cómo afectan dichas modalidades de implementación al tratamiento de datos de carácter personal.

NUBE PÚBLICA

Hablamos de un servicio de Nube Pública cuando el proveedor de servicios de *cloud* proporciona sus recursos de forma abierta a entidades heterogéneas, sin más relación entre sí que haber cerrado un contrato con el mismo proveedor de servicio. Existen diversas y numerosas soluciones en Nube Pública y prestan sus servicios desde particulares a grandes corporaciones, ya que cualquiera puede contratar con ellos.

NUBE PRIVADA

En el otro extremo podemos hablar de Nube Privada, que la encontramos cuando una entidad realiza la gestión y administración de sus servicios en la *nube* para las partes que la forman, sin que en la misma puedan participar entidades externas y manteniendo el control sobre ella. Una Nube Privada no necesariamente se implementa por la misma entidad que la utiliza, sino que puede contratarse a un tercero que actuará bajo su supervisión y en función de sus necesidades. Las entidades que optan por las Nubes Privadas son aquellas que son complejas y necesitan centralizar los recursos informáticos y, a la vez, ofrecer flexibilidad en la disponibilidad de los mismos, por ejemplo, administraciones públicas y grandes corporaciones, aunque hay ejemplos de Nubes Privadas implementadas en entidades de enseñanza.

OTROS MODELOS

Entre ambos modelos se encuentran soluciones intermedias que tomarán distintos nombres, como pueden ser las Nubes Híbridas, en las que determinados servicios se ofrecen de forma pública y otros de forma privada; las Nubes Comunitarias, cuando dichos servicios son compartidos en una comunidad cerrada; o las Nubes Privadas Virtuales, cuando sobre Nubes Públicas se implementan garantías adicionales de seguridad.

MODALIDADES DE SERVICIO

Los proveedores de la *nube* proporcionan acceso a recursos informáticos a través de la red, y ofrecen una serie de servicios adicionales de valor añadido que acercarán la oferta del proveedor a las necesidades de su cliente. En función de lo completo que sea ese valor añadido podemos decir que tenemos una solución de Infraestructura como Servicio, Plataforma como Servicio o Software

como Servicio. Esta división no puede considerarse rígida, ya que hay proveedores que proporcionan soluciones mixtas en las que se combinan características de todas ellas.

SOFTWARE COMO SERVICIO

Podemos hablar de una Nube de Software (modelo de servicio *Software as a Service* o SaaS), cuando el usuario encuentra en la *nube* las herramientas finales con las que puede implementar directamente los procesos de su empresa: una aplicación de contabilidad, de correo electrónico, un *worlkflow*, un programa para la gestión documental de su empresa, etc.

INFRAESTRUCTURA COMO SERVICIO

Si el valor añadido es nulo, se puede hablar de una Nube de infraestructura (IaaS). En ese caso el proveedor proporciona capacidades de almacenamiento y proceso en bruto, sobre las que el usuario ha de construir las aplicaciones que necesita su empresa prácticamente desde cero. Tal vez se pueda decir que éste es el modelo más primitivo de *nube*, que se inició con los sitios de Internet que proporcionaban capacidad de almacenamiento masivo a través de la red y los servidores de alojamiento web.

PLATAFORMA COMO SERVICIO

Entre estas dos aproximaciones se pueden encontrar otras intermedias llamadas PaaS (Plataforma como Servicio), en las que se proporcionan utilidades para construir aplicaciones, como bases de datos o entornos de programación sobre las que el usuario puede desarrollar sus propias soluciones.

PORTABILIDAD DE LA INFORMACIÓN

Las soluciones que ofrecen los proveedores de *cloud computing* pueden clasificarse como abiertas a la portabilidad o cerradas a la misma. Se podrá considerar una solución abierta a la portabilidad cuanto mayor sea la facilidad de un usuario para transferir todos sus datos y aplicaciones desde un proveedor de *cloud* a otro (o a los sistemas propiedad del cliente), garantizando la disponibilidad de los datos y la continuidad del servicio.

Hay que tener en cuenta que el fin de la relación con el proveedor de *cloud* puede darse no sólo en el caso de rescisión de contrato por parte del cliente sino por otras circunstancias ajenas al mismo, como podría ser el fin de la prestación de algún tipo de servicio por parte del proveedor, el cambio de su política comercial o del marco regulatorio. Es, entonces, un aspecto importante que

debe tenerse en cuenta a la hora de utilizar servicios de *cloud*, sobre todo públicos, pues cuanto más cerrado a la portabilidad sea el proveedor mayor será la dificultad, o incluso imposibilidad, de poder realizar esa transferencia a un coste razonable que haga que, de facto, el cliente esté cautivo del proveedor.

LOCALIZACIÓN DEL PROCESO Y DE LOS DATOS

El proveedor de *cloud computing*, a la hora de implementar los servicios al usuario final, puede ser el prestador único de los mismos cuando todos los recursos para proporcionarlos pertenecen al propio proveedor. Es decir, dispone de toda la infraestructura necesaria, que administra directamente, y no subcontrata a terceros en función de la distinta carga de trabajo que tenga.

SUBCONTRATACIÓN

Por el contrario, puede no tratarse de un prestador final cuando el servicio que ofrece directamente al usuario se construye sobre la subcontratación a terceros de elementos necesarios para implementarlos (hardware, almacenamiento, comunicaciones, etc.), como es el caso de los *partners*. A su vez, los subcontratistas pueden subcontratar de nuevo parte del servicio que proporcionan al prestador final a terceras y sucesivas compañías. Este es un modelo de cadena de subcontrataciones que en teoría podría no tener fin, y cuyo objeto es redimensionar continuamente los recursos de la *nube* de forma dinámica y en función de las condiciones del mercado.

LOCALIZACIÓN

A la hora de decantarse por la utilización de un servicio de *cloud computing*, hay otros condicionantes que hay que tener en cuenta desde el punto de vista de los derechos de los ciudadanos y del ejercicio de las responsabilidades del cliente de dichos servicios.

Es importante identificar qué proveedores de *cloud* están localizados dentro del Espacio Económico Europeo o en países que de una u otra forma garanticen un nivel adecuado de protección de los datos de carácter personal. Esta localización afecta no sólo a la sede del proveedor de *cloud*, sino también a la localización de cada uno de los recursos físicos que emplea para implementar el servicio, de forma directa o subcontratada. Y hay que enfatizar que hay que tener en cuenta la localización de todos los recursos pues, por la misma naturaleza del servicio de *cloud*, los datos pueden estar en cualquier momento en cualquier sitio, pero los derechos y obligaciones relativos a dichos datos han de garantizarse siempre.

TRANSPARENCIA

En relación al control de la localización de los datos de un usuario, un servicio de *cloud* puede ser auditable o transparente (en el sentido de la palabra inglesa *accountable*) cuando el contratista puede reclamar información precisa de dónde, cuándo y quién ha almacenado o procesado sus datos (dentro de los recursos propios del proveedor o de la cadena de subcontrataciones), y en qué condiciones de seguridad se ha producido. En otro caso, nos encontraremos con un servicio opaco al usuario, en el que éste no tiene opción alguna de obtener información precisa de qué ha ocurrido con sus datos ni herramientas para auditar el servicio que se le está proporcionando y en el que su propia información escapa a su control.

LAS GARANTÍAS CONTRACTUALES

La contratación de servicios de *cloud computing* se realizará a través de un contrato de prestación de servicios. Resulta imprescindible que ese contrato incorpore entre sus cláusulas las garantías a las que obliga el RGPD (artículo 28). Para obtener más información sobre estas obligaciones puede acudir a las Directrices para la elaboración de contratos entre responsables y encargados de tratamiento.

A estos efectos hay que destacar, en primer lugar, que el cliente que contrata a un prestador de servicios de Cloud Computing tiene una obligación legal de diligencia para, según el artículo 28.1 del RGPD, elegir "únicamente un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiados, de manera que el tratamiento sea conforme con los requisitos del presente Reglamento y garantice la protección de los derechos del interesado". Este deber de diligencia se traducirá, dadas las características propias de estos servicios, en un abanico de requerimientos de información al proveedor de servicios dirigidos a conocer las garantías que ofrece para la protección de los datos personales de los que sigue siendo responsable. Dicha información le resultará imprescindible para decidir sobre la modalidad de nube y el tipo de servicios que contrata y, específicamente, para discriminar cuál o cuáles le ofrecen garantías adecuadas y elegir entre ellos. El cumplimiento de este deber de diligencia ha de tener como contrapartida por parte del prestador de servicios de Cloud Computing una correlativa diligencia a la hora de facilitar información, en particular sobre los mecanismos que garantizan el cumplimiento de las obligaciones derivadas de la normativa de protección de datos, para poder considerarlo como un provee-

dor transparente, como se establece en el art. 28.3 letra h): "pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el presente artículo, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable", así como en el párrafo final del mismo artículo "el encargado informará inmediatamente al responsable si, en su opinión, una instrucción infringe el presente Reglamento u otras disposiciones en materia de protección de datos de la Unión o de los Estados miembros".

Las opciones sobre la diligencia en la elección del encargado del tratamiento deben documentarse para poder acreditarla.

Atendiendo a la relación contractual establecida entre el cliente y el proveedor de la *nube*, también este contrato se puede clasificar como negociado o de adhesión. Podemos decir que un contrato entre el cliente y el proveedor es negociado si el primero tiene, o se le ofrece, la capacidad para fijar las condiciones de contratación en función del tipo de datos que se van a procesar, las medidas de seguridad exigibles, el esquema de subcontratación, la localización de los datos, la portabilidad de los mismos y cualquier otro aspecto de adecuación a la normativa de protección de datos y a las restricciones que esta regulación implica.

En la mayoría de los casos, sin embargo, lo que se oferta son contratos de adhesión, constituidos por cláusulas contractuales cerradas, en las que el proveedor de *cloud* fija las condiciones con un contrato tipo igual para todos sus clientes, sin que el usuario tenga ninguna opción para negociar sus términos. Este último caso es el más común, sobre todo cuando se encuentra el cliente en una situación de desequilibrio (p.ej.: una pyme frente a un gran proveedor), aunque hay que tener en cuenta que esto no eximirá, a ninguno de los dos, de las responsabilidades que determina la normativa de protección de datos.

RIESGOS DE LA COMPUTACIÓN EN 'NUBE'

El uso de servicios de computación en *nube* ofrece un gran número de ventajas pero presenta también, por sus características, unos riesgos específicos que deben afrontarse con una adecuada elección del prestador. Para ello debe analizarse que las condiciones de prestación tengan en cuenta los elementos que permitan que el tratamiento de datos se realice sin merma de las garantías que le son aplicables.

Podemos agrupar los riesgos en dos grandes categorías: falta de transparencia sobre las condiciones en las que se presta el servicio y falta de control del responsable sobre el uso y gestión de los datos personales por parte de los agentes implicados en el servicio.

FALTA DE TRANSPARENCIA

Es el prestador el que conoce todos los detalles del servicio que ofrece. Por ello, nos enfrentamos a la necesidad de conocer el qué, quién, cómo y dónde se lleva a cabo el tratamiento de los datos que se proporcionan al proveedor para la prestación del servicio. Si este último no da una información clara, precisa y completa sobre todos los elementos inherentes a la prestación, la decisión adoptada por el responsable no podrá tener en consideración de forma adecuada requisitos básicos como la ubicación de los datos, la existencia de subencargados, los controles de acceso a la información o las medidas de seguridad. De esta forma, se dificulta al responsable la posibilidad de evaluar los riesgos y establecer los controles adecuados, de ahí que el cumplimiento de la obligación de diligencia en la elección del prestador del servicio, que antes se señaló, implique, en primer lugar obtener información.

FALTA DE CONTROL

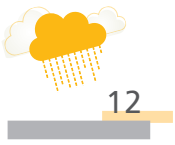
Como consecuencia de las peculiaridades del modelo de tratamiento en la *nube* y en parte también de la ausencia de transparencia en la información, la falta de control del responsable se manifiesta, por ejemplo, ante las dificultades para conocer en todo momento la ubicación de los datos, las dificultades a la hora de disponer de los datos en poder del proveedor o de poder obtenerlos en un formato válido e interoperable, los obstáculos a una gestión efectiva del tratamiento o, en definitiva, la ausencia de control efectivo a la hora de definir los elementos sustantivos del tratamiento en lo tocante a salvaguardas técnicas y organizativas.

UNA ESTRATEGIA PARA EL CLIENTE DE SERVICIOS DE COMPUTACIÓN EN 'NUBE'

Frente a los riesgos descritos, el responsable del tratamiento –p.ej. empresas o administraciones– que pretenda incorporar todo o parte del tratamiento de datos a servicios en la *nube* debería considerar una estrategia de actuación que bien pudiera ser la siguiente:

EVALUAR LOS TRATAMIENTOS Y LOS RIESGOS DE PROTECCIÓN DE DATOS

El cliente ha de estudiar con detalle qué parte o partes de los tratamientos que realiza son susceptibles de ser transferidos a servicios de computación en *nube* considerando no sólo los beneficios, sino igualmente los potenciales riesgos que se van a asumir.



La estrategia de actuación que se sugiere conlleva, de un lado, el estudio sobre los recursos del responsable que son susceptibles de ser o no transferidos a la *nube* en función del nivel de riesgo que presenten, lo que pasa por un conocimiento detallado del responsable sobre los datos personales tratados. Como se ha sugerido, un elemento fundamental será conocer los tratamientos sobre categorías especiales de datos personales (p. ej. los datos de salud). La transferencia de datos a servicios de computación no excluye en principio a ningún tipo de dato, siempre que haya un balance positivo entre los riesgos asumidos y las salvaguardas, en forma de medidas organizativas y técnicas, proporcionadas por el proveedor, a fín de garantizar y poder demostrar que el tratamiento es conforme con el RGPD.

VERIFICAR LAS CONDICIONES EN QUE SE PRESTA EL SERVICIO

Debe verificarse de forma previa a la contratación las condiciones en la que se presta el servicio con el fin de determinar si ofrecen un nivel adecuado de cumplimiento.

Las condiciones ofrecidas por los proveedores se deben contrastar con una lista de control que incluya, entre otros, elementos relativos a la información proporcionada, ubicación del tratamiento, existencia de subencargados, políticas de seguridad, derechos del usuario y obligaciones legales del prestador del servicio.

Es aconsejable comparar las características ofrecidas por varios proveedores, no sólo en términos económicos sino también en relación con los contenidos de la prestación y las garantías de calidad y cumplimiento legal que cada proveedor proporciona en especial, la adhesión del encargado a códigos de conducta o mecanismos de certificación aprobados, podrán utilizarse como elementos para demostrar la existencia de garantías.

En cualquier caso, debe prestarse especial atención a no contratar servicios prestados en *nube* que no reúnan los requisitos legalmente establecidos.

Tener en consideración los procedimientos de salida en caso de cambio de proveedor facilitará que los procesos de retorno de datos se lleven a cabo sin merma de la integridad de los datos y con control pleno del responsable sobre su destino ulterior. En este ámbito son de especial importancia los sistemas que el proveedor proporcione para asegurar, en todo momento, la portabilidad de esos datos.

LO QUE DEBO CONOCER PARA LA CONTRATACIÓN DE SERVICIOS DE 'CLOUD COMPUTING'

La presente guía pretende facilitar el cumplimiento de la normativa de protección de datos en la contratación de servicios de *cloud computing* ofreciendo una información práctica dirigida a pymes, microempresas y profesionales. Asimismo se informa sobre las características específicas de la contratación en las Administraciones Públicas. Para ello, la guía se articula sobre un cuestionario de preguntas y respuestas que trata los aspectos esenciales para la protección de datos personales en estos servicios.

1.- ¿Qué debo analizar y tener en cuenta antes de contratar servicios de '*cloud* computing'?

- Debe evaluar la tipología de datos que trata atendiendo a su mayor o menor sensibilidad (por ejemplo los datos meramente identificativos no son datos sensibles y los relacionados con la salud tienen la máxima sensibilidad).
- Debe informarse sobre los tipos de *nube* (privada, pública, híbrida) y las distintas modalidades de servicios (vea la introducción de esta guía).
- Con esta información debe decidir para qué datos personales contratará servicios de *cloud computing* y cuáles prefiere mantener en sus propios sistemas de información. Esta decisión es importante porque delimitará las finalidades para las que el proveedor de *cloud* puede tratar los datos. En consecuencia, debe garantizarse expresamente que no utilizará los datos para otra finalidad que no tenga relación con los servicios contratados.

2.- Desde la perspectiva de la normativa de protección de datos, ¿cuál es mi papel como cliente de un servicio de '*cloud*'?

- El cliente que contrata servicios de *cloud computing* sigue siendo responsable del tratamiento de los datos personales. Aunque los contrate con una gran compañía multinacional la responsabilidad no se desplaza al prestador del servicio, ni siquiera incorporando una cláusula en el contrato con esta finalidad.
- El que ofrece la contratación de *cloud computing* es un prestador de servicios que en la ley de protección de datos tiene la calificación de 'encargado del tratamiento'.

3.- ¿Cuál es la legislación aplicable?

El modelo de *cloud computing* hace posible que tanto los proveedores de servicios como los datos almacenados en la *nube* se encuentren ubicados en cualquier punto del planeta. Pero, en todo caso:

- El cliente que contrata servicios de *cloud computing* sigue siendo responsable del tratamiento de los datos por lo que la normativa aplicable al cliente y al prestador del servicio es por el RGPD (Reglamento (UE) 2016/679, de 27 de abril de 2016, General de Protección de Datos) y demás normativa de protección de datos que sea aplicable.
- La aplicación de dicha normativa no puede modificarse contractualmente.
- Aunque le informen de que los datos personales están disociados, no cambia la ley aplicable ni la responsabilidad del cliente y del prestador del servicio.

4.- ¿Cuáles son mis obligaciones como cliente?

- Debe ser diligente en la elección del prestador del servicio para que le ofrezca garantías suficientes en el cumplimiento del RGPD y en la protección de los derechos de los interesados.
- Debe formalizar un contrato con las garantías indicadas en el apartado "las garantías contractuales".
- En particular, debe solicitar y obtener información sobre si intervienen o no terceras personas (subcontratistas) en la prestación de servicios de *cloud computing*.

Lo habitual es que intervengan terceras empresas. De ser así:

- Tiene que dar su autorización previa y por escrito, a la participación de terceras empresas, al menos delimitando genéricamente los servicios en los que participarán (p. ej. en el alojamiento de datos). Para ello, el prestador del servicio de *cloud computing* tiene que informarle sobre la tipología de servicios que pueden subcontratarse con terceros.
- Tiene que poder conocer las terceras empresas que intervienen (p. ej. pudiendo acceder a una página web o a través de otras opciones que le facilite el prestador del servicio).
- El proveedor de *cloud* debe asumir en el contrato que los subcontratistas le ofrecen garantías jurídicas para el tratamiento de los datos equivalentes a los que él mismo asume.

– El contrato que firma ha de incorporar cláusulas contractuales para la protección de los datos personales según se detalla en las siguientes preguntas.

5.- ¿Dónde pueden estar ubicados los datos personales? ¿Es relevante su ubicación?

– La localización de los datos tiene importancia porque las garantías exigibles para su protección son distintas según los países en que se encuentren.

– Los países del Espacio Económico Europeo ofrecen garantías suficientes y no se considera legalmente que exista una transferencia internacional de datos. El Espacio Económico Europeo está constituido por los países de la Unión Europea e Islandia, Liechtenstein y Noruega.

– Si los datos están localizados en países que no pertenecen al Espacio Económico Europeo habría una transferencia internacional de datos, en cuyo caso, y dependiendo del país en que se encuentren, deberán proporcionarse garantías jurídicas adecuadas.

6.- ¿Qué garantías se consideran adecuadas para las transferencias internacionales de datos?

– Si se trata de países, territorios, o sectores específicos de actividad que hayan sido declarados de nivel adecuado de protección por la Comisión Europea se podrán llevar a cabo las transferencias internacionales de datos con la única obligación de incluirlas en el registro de actividades de tratamiento (art. 30 RGPD). Se incluyen las empresas establecidas en Estados Unidos que se encuentren certificadas en el esquema del Escudo de Privacidad UE- EE.UU. (para conocer la lista de países con nivel adecuado de protección haga clic aquí).

– En otro caso deberán ofrecerse garantías adecuadas, lo que se podrá hacer mediante diferentes instrumentos (haga clic aquí para conocerlos). Para estas transferencias no se requiere la autorización de la Agencia Española de Protección de Datos, con excepción de aquéllas en las que se utilicen modelos de contratos no aprobados por la Comisión Europea o por la Agencia, que revisten un carácter poco frecuente, o acuerdos administrativos entre autoridades u organismos públicos.

– Pregunte al prestador de servicios de *cloud computing* si hay transferencias internacionales de datos y, en caso afirmativo, con qué garantías.

- Cuando los datos están localizados en terceros países podría suceder que una Autoridad competente pueda solicitar y obtener información sobre los datos personales de los que el cliente es responsable. En este caso el cliente debería ser informado por el proveedor de esta circunstancia (salvo que lo prohíba la ley del país tercero).

7.- ¿Qué medidas de seguridad son exigibles?

- Las medidas de seguridad son indispensables para garantizar la integridad de los datos personales, evitar accesos no autorizados y recuperar la información en caso de que se produzcan incidencias de seguridad.
- Las garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales serán los resultantes de la realización de un Análisis de Riesgos, y en su caso, de la Evaluación de Impacto prevista en el artículo 35 del RGPD.
- Asimismo, el acceso a la información a través de redes de comunicaciones debe contemplar un nivel de medidas de seguridad equivalente al de los accesos en modo local.
- Pregunte al proveedor de *cloud computing* sobre las medidas de seguridad que le ofrece y garantiza.

8.- ¿Cómo puedo garantizar o asegurarme de que se cumplen las medidas de seguridad?

- Como cliente debe tener la opción de comprobar las medidas de seguridad, incluidos los registros que permiten conocer quién ha accedido a los datos de los que es responsable. El proveedor debe poner a su disposición toda la información necesaria para demostrar el cumplimiento de las medidas de seguridad.
- El proveedor de *cloud computing* le acredita que dispone de una certificación de seguridad adecuada.
- Puede acordarse que un tercero independiente audite la seguridad. En este caso, debe conocerse la entidad auditora y los estándares reconocidos que aplicará.
- Solicite información al proveedor de *cloud* sobre cómo se auditarán las medidas de seguridad.

- El cliente debe ser informado sin dilación indebida por el proveedor de *cloud* sobre las incidencias de seguridad que afecten a los datos de los que el propio cliente es responsable, así como de las medidas adoptadas para resolverlas o de las medidas que el cliente ha de tomar para evitar los daños que puedan producirse (p. ej. informar a sus propios clientes sobre cómo proteger su información personal). No olvide que el RGPD obliga al responsable de tratamiento a notificar estas violaciones de seguridad a la autoridad de control, así como a los interesados cuando entrañen un alto riesgo para los derechos y libertades de los mismos.
- El cifrado de los datos personales es una medida que debe valorarse positivamente. Solicite información al proveedor de *cloud* sobre el cifrado de los datos.

9.- ¿Qué compromisos de confidencialidad de los datos personales debo exigir?

- El proveedor del servicio de *cloud* debe comprometerse a garantizar la confidencialidad utilizando los datos sólo para los servicios contratados.
- Asimismo debe garantizar que el personal autorizado a tratar datos personales haya suscrito compromisos de confidencialidad o esté sujeto obligaciones de confidencialidad estatutarias.

10.- ¿Cómo garantizo que puedo recuperar los datos personales de los que soy responsable (portabilidad)?

- La portabilidad significa que el proveedor ha de obligarse, cuando pueda resolverse el contrato o a la terminación del servicio, a entregar toda la información al cliente en el formato que se acuerde, de forma que éste pueda almacenarla en sus propios sistemas o bien optar porque se traslade a los de un nuevo proveedor en un formato que permita su utilización, en el plazo más breve posible, con total garantía de la integridad de la información y sin incurrir en costes adicionales.
- En particular, el cliente debe tener la opción de exigir la portabilidad de la información a sus propios sistemas de información o a un nuevo prestador de *cloud* cuando considere inadecuada la intervención de algún subcontratista o la transferencia de datos a países que estime no aportan garantías adecuadas.
- También es particularmente importante en los casos en que el proveedor de *cloud* modifique unilateralmente las condiciones de prestación del servicio dado su poder de negociación frente al cliente.

– Solicite información y garantías al proveedor sobre la portabilidad de los datos personales.

– Notar que esta portabilidad es independiente del derecho de portabilidad de los datos que asiste al interesado, concretado en el artículo 20 del RGPD.

11.- ¿Cómo puedo asegurarme de que el proveedor de 'cloud' no conserva los datos personales si se extingue el contrato?

– Deben preverse mecanismos que garanticen el borrado seguro de los datos cuando lo solicite el cliente y, en todo caso, al finalizar el contrato. (Un mecanismo apropiado es requerir una certificación de la destrucción emitido por el proveedor de *cloud computing* o por un tercero).

12.- ¿Cómo puedo garantizar el ejercicio de los derechos reconocidos en los artículos 15 a 22 del RGPD (acceso, rectificación, supresión, limitación del tratamiento, portabilidad, oposición y decisiones individuales automatizadas)?

El cliente de *cloud computing*, como responsable del tratamiento de datos, debe permitir el ejercicio de los mencionados derechos a los interesados.

– Para ello, el proveedor de *cloud* debe garantizar su asistencia al responsable y las herramientas adecuadas para facilitar la atención de dichos derechos.

– Infórmese sobre las condiciones que le ofrece el proveedor para cumplir con ese deber de cooperación para garantizar el ejercicio de estos derechos.

EL 'CLOUD COMPUTING' EN LAS ADMINISTRACIONES PÚBLICAS

¿Qué singularidades presenta el 'cloud computing' en las Administraciones Públicas?

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 (puede obtener más información en la pregunta número 6 de esta guía).

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 normativa de protección de datos, las Administraciones Públicas están sujetas a un marco legal específico al cual debe adecuarse la prestación de servicios basados en *cloud computing*:

- Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público (Disposición adicional vigésimo quinta), si bien las referencias a la Ley Orgánica 15/1999 deben entenderse referidas al RGPD.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas que recoge, con las adaptaciones necesarias, las normas antes contenidas en la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos, y algunas de las previstas en el Real Decreto 1671/2009, de 6 de noviembre que desarrollaba 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).

¿Qué aspectos deben tenerse en cuenta al contratar servicios de 'cloud computing'?

- Debe reiterarse especialmente la obligación de diligencia para la elección de un encargado del tratamiento al que se hace referencia en el apartado de "las garantías contractuales", incorporando las correspondientes previsiones en los pliegos de prescripciones.

- La contratación por parte de las Administraciones Públicas de servicios *cloud computing* que impliquen el tratamiento de datos de carácter personal requiere la formalización de un contrato escrito en los términos previstos en el artículo 28 del RGPD.
- Estos requisitos pueden resumirse así:
  - El prestador de servicios de computación en la *nube* tendrá la consideración de encargado de tratamiento, y solo tratará los datos siguiendo las instrucciones documentadas del responsable.
  - El tratamiento se regirá por un contrato que establezca el objeto, la naturaleza y la finalidad del tratamiento, así como el tipo de datos personales, categorías de interesados. y derechos y obligaciones del responsable.
  - Al término de la prestación contractual los datos de carácter personal deberán ser destruidos o devueltos a la entidad contratante responsable, o al encargado del tratamiento que ésta hubiese designado. (Puede obtener más información sobre la devolución y destrucción de los datos en las preguntas número 8 y 9).
- Con respecto a la posible subcontratación de servicios por parte del encargado de tratamiento (el prestador de servicios de *cloud computing*), ésta solo será posible si se reúnen los siguientes requisitos:
  - Que dicho tratamiento se haya especificado en el contrato firmado por la administración contratante y el prestador de servicios de computación en la *nube*. (Sobre cómo cumplir esta obligación infórmese en la pregunta número 4).
  - Que el tratamiento de datos de carácter personal se ajuste a las instrucciones de la administración que actúa como responsable del tratamiento. (Sobre cómo cumplir esta obligación infórmese en las preguntas número 5 y 6).
  - Que el prestador de servicios encargado del tratamiento y el tercero formalicen el contrato en los términos previstos en el artículo artículo 28 del RGPD. En éste contrato se impondrán al tercero las mismas obligaciones de protección de datos que las estipuladas en el contrato entre la administración responsable y el encargado.
- Los contratos de prestación de servicios de *cloud computing* deben especificar las medidas técnicas y organizativas que el prestador de servicios tiene previsto implantar para garantizar un nivel de seguridad de los datos adecuado al riesgo. Asimismo, los especiales requisitos de disponibilidad, confidencialidad e integridad que puedan requerir ciertos

servicios electrónicos prestados por las Administraciones Públicas (por ejemplo en el caso de las sedes electrónicas) deben reflejarse en el contrato mediante un acuerdo de nivel de servicio (SLA) en el que se especifiquen los indicadores de calidad de servicio que van a ser medidos y los valores mínimos aceptables de los mismos. (Sobre cómo cumplir esta obligación, infórmese en las preguntas número 7 y 8).

- De acuerdo con el artículo 62 de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, los órganos de contratación deberán designar un responsable del contrato con el fin de asegurar la correcta realización de la prestación pactada. No obstante, la designación de dicha figura no modifica el régimen de obligaciones y responsabilidades al que está sujeto el responsable del tratamiento en materia de protección de datos de carácter personal.

¿Qué elementos de la seguridad cobran especial relevancia en un entorno 'cloud'?

- Los responsables de tratamiento deberán realizar una Evaluación de Impacto sobre la Protección de Datos (EIPD) con carácter previo a la puesta en marcha de aquellos tratamientos para los que sea probable que conlleven un alto riesgo para los derechos y libertades de los interesados.
- En particular, se requerirá la realización de una EIPD cuando el tratamiento conlleve la elaboración de perfiles sobre los cuales se tomen decisiones con efectos jurídicos, se traten datos sensibles a gran escala o se realice una observación sistemática a gran escala de una zona de acceso público.
- Por su parte, la implantación de servicios de *cloud computing* incide de forma singular en algunos elementos del Esquema Nacional de Seguridad como los siguientes:
  - **Análisis y gestión de riesgos.** La migración de servicios y aplicaciones a entornos de *cloud computing* debe ser objeto de un análisis de riesgos que, en función de la sensibilidad de los datos y el nivel de amenazas, determine, en primer lugar, la conveniencia de esta solución y, en caso afirmativo, los controles y salvaguardas que deben implantarse para mitigar los riesgos hasta un nivel que pueda ser considerado aceptable.
  - **Profesionalidad.** Conlleva la necesidad de que, en cualquier modalidad de prestación de servicios en la *nube*, la seguridad esté atendida, revisada y auditada por personal cualificado.
  - **Protección de la información almacenada y en tránsito.** Debido a la especial sensibilidad de los datos tratados por las Administraciones Públicas, la aplicación de

técnicas robustas de cifrado tanto a los datos en tránsito como a los datos almacenados constituye una medida necesaria para garantizar su confidencialidad. Asimismo, el contrato de prestación de servicios en la *nube* debe contemplar la realización de copias de respaldo de la información de forma que se garantice la plena disponibilidad e integridad de los datos almacenados.

- **Incidentes de seguridad y continuidad de la actividad.** La adopción de modelos de servicio basados en *cloud computing* debe contemplar una adecuada gestión de las incidencias de seguridad y mecanismos que garanticen la continuidad de las operaciones en caso de catástrofes o incidentes severos.
- **Auditoría de la seguridad.** La contratación de servicios de *cloud computing* exige garantizar la realización de las auditorías de seguridad ordinarias y extraordinarias previstas en el artículo 34 del ENS.

Este artículo exige requisitos específicos sobre los criterios, métodos de trabajo y de conducta utilizados; los aspectos respecto de los que debe determinar la auditoría y los criterios metodológicos utilizados.

Asimismo contempla los destinatarios de la auditoría y las conclusiones que deben realizarse sobre ella.

Por tanto, la Administración que contrate servicios de *cloud computing* debe obtener información sobre cómo cumplir estas obligaciones. (Puede obtener información básica sobre esta obligación en la pregunta número 7).

¿Qué requisitos son exigibles en materia de portabilidad e interoperabilidad?

– La contratación de servicios de *cloud computing* por parte de las Administraciones Públicas debe garantizar la portabilidad de los datos entre prestadores de servicios y el ejercicio de los derechos de acceso por parte de los ciudadanos, mediante el uso de formatos estandarizados de datos que cumplan los requisitos establecidos en el Esquema Nacional de Interoperabilidad:

  - Los documentos y servicios de administración electrónica que se pongan a disposición de los ciudadanos o de otras Administraciones Públicas deben encontrarse disponibles, como mínimo, mediante estándares abiertos. Asimismo, deben ser visualizables, accesibles y funcionalmente operables en condiciones que permitan satisfacer el principio de neutralidad tecnológica y eviten la discriminación a los ciudadanos por razón de su elección tecnológica.

- Deben adoptarse medidas organizativas y técnicas necesarias con el fin de garantizar la interoperabilidad en relación con la recuperación y conservación de los documentos electrónicos a lo largo de su ciclo de vida.
- Conservación de los documentos electrónicos en el formato en el que hayan sido elaborados, enviados o recibidos, y preferentemente en un formato correspondiente a un estándar abierto que preserve a lo largo del tiempo la integridad del contenido de los documentos, de la firma electrónica y de los metadatos que lo acompañan. (Puede obtener más información sobre la portabilidad de los datos en la pregunta número 8).

GLOSARIO

IaaS: Infraestructura como servicio. Cuando el proveedor de *cloud* proporciona a sus clientes recursos de procesamiento y almacenamiento a través de la red, sin ningún otro valor añadido.

SaaS: Software como servicio. Cuando el proveedor de *cloud* proporciona al cliente aplicaciones que implementan los procesos de su empresa.

PaaS: Plataforma como servicio. Cuando el proveedor de *cloud* proporciona al cliente las herramientas necesarias para desarrollar sus aplicaciones sobre la *nube*.

Portabilidad: que los datos de un contratista que están en los servidores del proveedor de *cloud* puedan trasladarse a otro proveedor (o a sistemas locales) a elección del contratista y sin pérdida de datos ni de servicio. No se debe confundir con el derecho a la portabilidad de los datos que pueden ejercer los interesados con arreglo al art. 20 del RGPD.Localización: el punto geográfico concreto en el que se encuentran los datos o se realiza el proceso en un servicio de *cloud computing*.

www.aepd.es