DIPUTACIÓ DE VALÈNCIA

Protecció de Dades i Seguretat de la Informació

Cuadernos DivalData

Cuadernos dirigidos a delegados,
responsables y especialistas en protección
de datos personales

Cuaderno nº 31 | Enero 2023

Privacidad y servicios cloud en el sector público

Í N D I C E

Privacidad y servicios cloud en el sector público

	Página
Introducción	**2**
Cloud Computing	**3**
Tipos de Cloud Computing	**4**
Modalidades del Servicio	**5**
Cumplimiento basado en el Riesgo	**6**
Esquema Nacional de Seguridad	**8**
Medida de Seguridad	**9**
Noticias y material complementario	**10**

Os invitamos a trasladarnos aquellas temáticas que resulten de vuestro interés para los próximos boletines informativos. Estas peticiones deberán dirigirse a:

Diputación de Valencia

Dpto. de Protección de Datos y Seguridad de la Información

Pl. de Manises, 4 46003 Valencia

email: dpdsi@dival.es

SUSCRIPCIONES

Si deseas suscribirte a nuestra publicación accede al siguiente

enlace

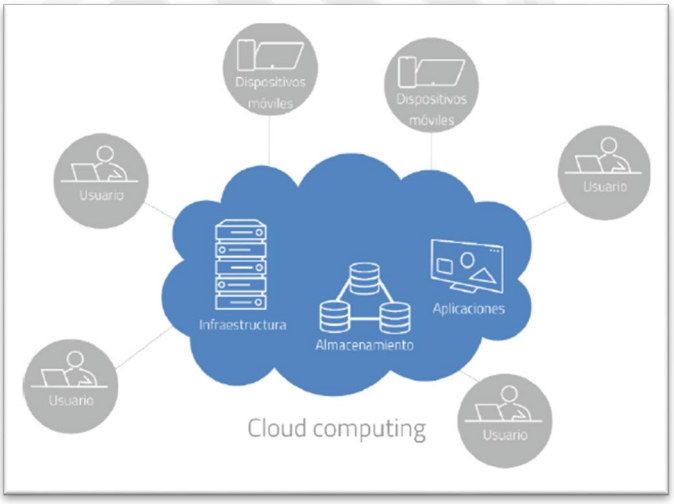
"La principal novedad que introdujeron estas normas fue la de apostar por una Administración Pública, íntegramente electrónica, con "papel cero" e interconectada".

INTRODUCCIÓN

Desde hace algunos años las organizaciones han venido adaptándose a los continuos cambios que se han producido en la sociedad, así como a los grandes avances tecnológicos que hoy en día nos permiten acceder a cualquier tipo de servicio, de forma rápida y sencilla a través de Internet.

En concreto, las administraciones públicas han sufrido una auténtica revolución desde la entrada en vigor de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público. La principal novedad que introdujeron estas normas fue la de apostar por una Administración Pública, íntegramente electrónica, con "papel cero" e interconectada, para así facilitar las relaciones electrónicas de los ciudadanos y las empresas con la Administración.

A raíz de la entrada en vigor de estas normas, toda la documentación, contenga o no datos personales, pasó a digitalizarse de forma masiva, lo que provocó que los expedientes ya no se conservasen únicamente en los espacios de trabajo, como escritorios o estanterías, sino que pasaron a entornos web mediante la computación en nube o *cloud computing* con todas las ventajas e inconvenientes que este servicio pueda conllevar.



CLOUD COMPUTING

El *cloud computing* o computación en nube es una nueva forma de prestación de los servicios de tratamiento de la información.

Esta solución permite a la organización optimizar la asignación y el coste de los recursos asociados a sus necesidades de tratamiento de información.

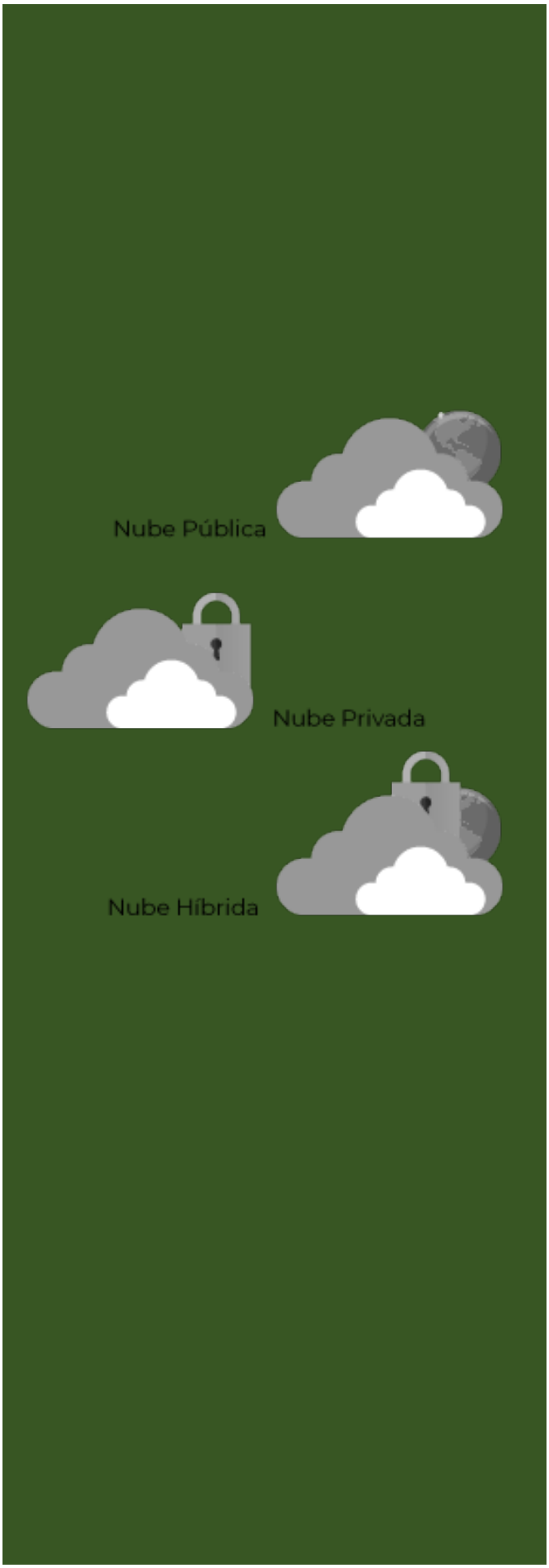
La organización no tiene necesidad de realizar inversiones en infraestructura sino que utiliza la que pone a su disposición el prestador del servicio, garantizando que no se generan situaciones de falta o exceso de recursos, así como el sobrecoste asociado a dichas situaciones.

En un entorno de *cloud computing* la gestión de la información está de forma virtual en manos de la organización 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 con sus necesidades.

El proveedor del servicio puede encontrarse en, prácticamente, cualquier lugar del mundo y su objetivo último será proporcionar los servicios optimizando sus propios recursos a través de, por ejemplo, prácticas de deslocalización, compartición de recursos y movilidad o realizando subcontrataciones adicionales.

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 las organizaciones un servicio de tecnologías de información bajo demanda.

"El proveedor del servicio puede encontrarse en, prácticamente, cualquier lugar del mundo y su objetivo último será proporcionar los servicios optimizando sus propios recursos."



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 nubes se pueden clasificar de muchas formas atendiendo a varios criterios:

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 organizaciones, 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 organizaciones.

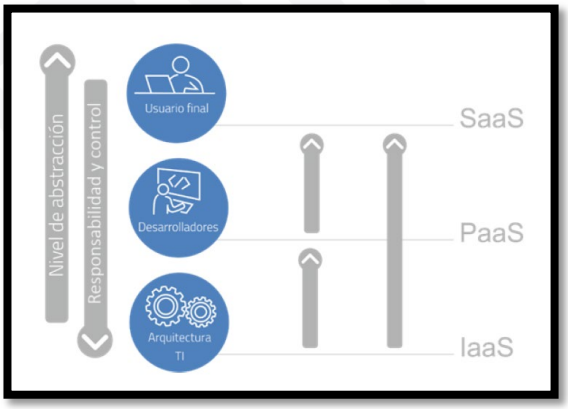
OTROS MODELOS: entre ambos modelos se encuentran soluciones intermedias que tomarán distintos nombres, como pueden ser las Nubes Híbridas, en las que determinados servicios se ofrecen de forma pública y otros de forma privada; las Nubes Comunitarias, cuando dichos servicios son compartidos en una comunidad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

"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."

MODALIDADES DEL SERVICIO

Ahora bien, se ofrecen una serie de categorías de servicio que se detallan a continuación:

- **IAAS (Infrastructure as a Service):** se encarga de entregar una infraestructura al usuario, proporcionando recursos de procesamiento y almacenamiento a través de la red, sin ningún otro valor añadido. El proveedor se encarga de la administración de la infraestructura y el cliente tiene el control sobre los sistemas operativos, almacenamiento y aplicaciones desplegadas, así como el control de los componentes de red.
- **PAAS (Platform as a Service):** se encarga de entregar una plataforma a la organización cliente. El cliente no administra ni controla la infraestructura, pero tiene el control sobre las aplicaciones instaladas y su configuración, y puede incluso instalar nuevas aplicaciones.
  Se proporcionan herramientas y utilidades para desarrollar aplicaciones sobre la nube como bases de datos o entornos de programación en las que el usuario puede desarrollar sus propias soluciones.
- **SAAS (Software as a Service):** podemos hablar de una Nube de Software cuando el usuario encuentra en la nube las herramientas finales con las que puede implementar directamente los procesos de su organización: una aplicación de contabilidad, de correo electrónico, un *worlkflow*, un programa para la gestión de expedientes, etc.



CUMPLIMIENTO BASADO EN EL RIESGO

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.

- **Falta de transparencia y control.** El cliente transfiere el control al proveedor de servicios.
- **Ubicación de los datos.** Es necesario acordar con el proveedor para que el procesamiento de los datos esté sujeto al marco legal del país.
- **Cumplimiento normativo.** Seguridad e integridad de los datos.
- **Aislamiento de datos.** El cliente transfiere el control al proveedor de servicios.
- **Portabilidad y viabilidad a largo plazo.** Implicaciones en la migración de datos.
- **Acceso de usuarios con privilegios.** Acordado con el proveedor para usuarios de soporte.
- **Recuperación.** Política de recuperación de datos en caso de desastre.
- **Monitorización.** La monitorización y vigilancia son actividades muy dependientes de los mecanismos ofrecidos por el proveedor de servicios.

Para identificar los riesgos de la forma más sencilla posible se ha de tener en cuenta los aspectos que ya hemos analizado, desde el tipo de computación en nube que se contrata hasta el tipo de servicio que nos presta el proveedor.

Tal y como se ha mencionado, en este proceso de computación en nube, la información pasa a estar en formato virtual accesible desde una web. Esto conlleva una serie de riesgos, que se han de tener en cuenta para implementar medidas de seguridad que garantiza la seguridad de la información.

En las administraciones públicas se tratan infinidad de datos personales por lo que resulta de aplicación el **REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos** y por el que se deroga la Directiva 95/46/CE (en adelante, "RGPD").

El **artículo 32 del RGPD** establece que teniendo en cuenta el estado de la técnica, los costes de aplicación, y

Uno de los mayores riesgos para las administraciones públicas a la hora de contratar este servicio en la nube es la pérdida de control y las trabas que pueden encontrarse cuando pretenden pedir la portabilidad*

- ***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.***

- ***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'.***

la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo.

El problema que todos conocemos es que a pesar de exigir que se implementen medidas de seguridad no existe un catálogo de medidas a implementar para cumplir con el RGPD.

Para resolver este asunto, lo habitual es acudir a la **Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales** (en adelante, "LOPDGDD"), en concreto, a la disposición adicional primera sobre medidas de seguridad en el ámbito del sector público, donde se determina que las administraciones públicas han de aplicar a los tratamientos de datos personales las medidas de seguridad que correspondan de las previstas en el Esquema Nacional de Seguridad, así como impulsar un grado de implementación de medidas equivalentes en las empresas o fundaciones vinculadas a los mismos sujetas al Derecho privado.

En los casos en los que el tercero preste un servicio en régimen de concesión, encomienda de gestión o contrato, como puede ser la computación en nube, las medidas de seguridad se corresponderán con las de la Administración pública de origen y se ajustarán al Esquema Nacional de Seguridad.

A la hora de contratar un servicio de computación en la nube se han de tener en cuenta los riesgos para derechos y libertades de los titulares de los datos personales. En administraciones públicas recobra mayor importancia lo siguiente:

1. Establecer medidas para cumplir con el Capítulo V del RGPD sobre las transferencias internacional de datos.
2. Firmar contrato de encargado con el proveedor para garantizar que se implementan las medidas de seguridad necesarias.
3. Facilitar información al ciudadano sobre donde se almacenan sus datos y la cesión a terceras partes.
4. Realizar análisis de riesgos teniendo en cuenta las amenazas a la que los datos se exponen por tenerlos alojados en la nube.

ESQUEMA NACIONAL DE SEGURIDAD

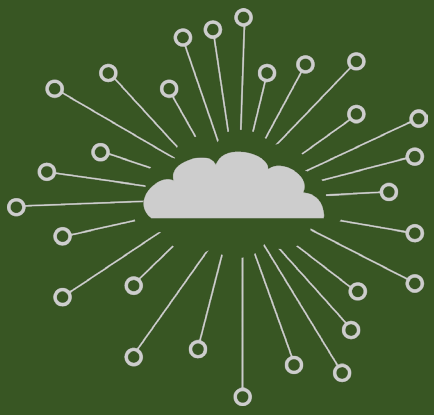
El pasado mes de mayo entró en vigor el **Real Decreto 311/2022**, de 3 de mayo, por el que se regula el nuevo Esquema Nacional de Seguridad (en adelante, "ENS") y que sustituye al anterior Real Decreto 3/2010, de 8 de enero, por el que se regula el ENS en el ámbito de la Administración Electrónica.

Entre las **novedades** que trae consigo esta nueva versión del ENS, cabe destacar lo siguiente:

- **Incorporación de la figura del perfil de cumplimiento:** el objetivo es alcanzar una adaptación al ENS más eficaz y eficiente, racionalizando recursos requeridos sin menoscabo de la protección perseguida y exigible.
  Se trata de enumerar un conjunto de medidas de seguridad, comprendidas o no el en Anexo II del ENS que, como consecuencia del preceptivo análisis de riesgos, resulten de aplicación a una entidad o sector de actividad concreta y para una determinada categoría de seguridad.
  Se persigue introducir la capacidad de ajustar los requisitos del ENS a necesidades específicas, entre otras, a determinados ámbitos tecnológicos como el servicio en nube.

- **Nuevo sistema de codificación de los requisitos de las medidas de seguridad:** el objetivo es facilitar de manera proporcionada la seguridad de los sistemas de información, su implantación y su auditoría.
  Se han codificado los requisitos de medidas y se han organizado de la siguiente forma:
  1. Requisitos base.
  2. Posibles refuerzos de Seguridad (R) alineados con el nivel de seguridad perseguido, que se suman a los requisitos base de la medida, pero que no siempre son incrementales entre sí; de forma que en ciertos casos, se puede elegir entre aplica un refuerzo u otro.

"Para el caso que nos ocupa nos centraremos en las medidas del Marco Operacional, en concreto la nueva incorporada al catálogo sobre servicios en la nube (op.nub)."



Esquema Nacional de Seguridad

Decálogo de recomendaciones para la utilización de servicios en la nube:

1. Determinar la categoría del sistema (BÁSICA, MEDIA o ALTA) que soportará la solución en la nube, según el ANEXO I del nuevo ENS.
2. Elaborar la declaración de aplicabilidad, según el ANEXO II del nuevo ENS.
3. Realizar un análisis de riesgos, para identificar requisitos adicionales de seguridad, que se reflejarán en la declaración de aplicabilidad.
4. Acogerse a un Perfil de Cumplimiento Específico (en caso de que sea de aplicación).
5. Establecer las condiciones contractuales, con carácter previo a la contratación, en los pliegos y/o peticiones de oferta.
6. En las condiciones contractuales, además de las relativas al cumplimiento de requisitos legales, detallar aspectos relativos al servicio, su infraestructura, el dimensionamiento, los registros de actividad, la gestión de incidentes, copias de seguridad, etc. y establecer condiciones relativas a la finalización del servicio.
7. Supervisar el cumplimiento, por parte del CSP, de los requisitos legales establecidos en las condiciones de contratación.
8. Realizar un seguimiento periódico del cumplimiento de los Acuerdos de Nivel de Servicio (SLA), establecidos con el CSP.
9. Planificar revisiones periódicas de la información, que el CSP proporciona a través de diversos mecanismos, como por ejemplo los registros de actividad, la capacidad, el almacenamiento, etc.
10. Elabora una normativa de seguridad específica para los usuarios de la nube.

MEDIDA DE SEGURIDAD

Para el caso que nos ocupa nos centraremos en las medidas del Marco Operacional, en concreto la de servicios en la nube (op.nub):

Requisitos:

- **[op.nub.1.1]** Los sistemas que suministran un servicio en la nube a organismos del sector público deberán cumplir con el conjunto de medidas de seguridad en función del modelo de servicio en la nube que presten: SaaS, PaaS e IaaS.
- **[op.nub.1.2]** Cuando se utilicen servicios en la nube suministrados por terceros, los sistemas de información que los soportan deberán ser conformes con el ENS o cumplir con las medidas desarrolladas en una guía CCN-STIC que incluirá, entre otros, requisitos relativos a:

1. Auditoría de pruebas de penetración (pentesting).
2. Transparencia.
3. Cifrado y gestión de claves.
4. Jurisdicción de los datos.

Refuerzo R1 - Servicios certificados.

- **[op.nub.1.r1.1]** Cuando se utilicen servicios en la nube suministrados por terceros, estos deberán estar certificados bajo una metodología de certificación reconocida por el Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las Tecnologías de la Información.[op.nub.1.r1.2] Si el servicio en la nube es un servicio de seguridad deberá cumplir con los requisitos establecidos en [op.pl.5].

Refuerzo R2 - Guías de Configuración de Seguridad Específicas.

- **[op.nub.1.r2.1]** La configuración de seguridad de los sistemas que proporcionan estos servicios deberá realizarse según la correspondiente guía CCN-STIC de Configuración de Seguridad Específica, orientadas tanto al usuario como al proveedor.

MATERIAL COMPLEMENTARIO

- Esquema Nacional de Seguridad. Consulta este enlace.
- Guía cloud clientes AEPD. Consulta este enlace.
- Guía de seguridad Cloud CCN. Consulta este enlace.
- Guía orientaciones para prestadores de servicios de Cloud Computing. Consulta este enlace.

NOTICIAS

- **La AEPD impone sanción de apercibimiento por infracción del artículo 32 RGPD "seguridad del tratamiento".** El reclamante expone que se impuso sin consentimiento el uso de unas cuentas personales de correo electrónico, alojado en la plataforma GOOGLE SUITE. En la página 19 se aclara que El Cloud *"es un disco duro virtual en donde guardar y compartir carpetas y archivos que permite la edición ofimática de manera colaborativa".* De la información trasladada, la AEPD considera que la reclamada ha infrinjido el artículo 32 RGPD, relativo a la seguridad del tratamiento. Consulta la Resolución en este enlace.

- **La AEPD impone sanción de apercibimiento por infracción de diversos artículos del RGPD y de la LOPDGDD.** La AEPD, tras las noticias que aparecieron en los medios de comunicación sobre la implantación de una app de rastreo de posibles infectados de COVID-19. En la resolución queda patente que los datos del sistema RADAR COVID eran almacenados en los servidores de AWS ubicados en la zona geográfica de Irlanda. Aportan el documento "Arquitectura AWS Cloud: Definición de Servicios". Sin embargo, la AEPD considera – entre otras infracciones descritas en el documento – la infracción del artículo 28 RGPD, por entender que no estaba debidamente articulada la relación entre responsable y encargado del tratamiento. Consulta la Resolución en este enlace.