UNIVERSIDAD CARLOS III DE MADRID

ESCUELA POLITÉCNICA SUPERIOR

GRADO EN INGENIERÍA INFORMÁTICA

TRABAJO FIN DE GRADO

SEGURIDAD Y CUMPLIMIENTO NORMATIVO EN EL CLOUD COMPUTING

AUTOR: Alexandra Tiemblo Moreno
TUTOR: Arturo Ribagorda Garnacho

Leganés, 15 de junio de 2012

Agradecimientos,

En primer lugar a mis padres, por su comprensión en los malos momentos y enfados a lo largo de la carrera, porque sus consejos siempre me han ayudado, porque sin ellos esto no sería posible. Y por supuesto al resto de mi familia.

A Don Arturo Ribagorda Garnacho por haberme dirigido este trabajo fin de grado. Por todas las atenciones, por su tiempo y su apoyo.

A todos mis profesores desde el colegio hasta la universidad. A mis compañeros y amigos.

Y a Javier por sus ánimos y su apoyo y porque siempre está ahí cuando más se necesita.

Gracias.

Índice de Contenidos

Índice de Ilustraciones

Índice de Tablas

1. Intoducción

El ritmo del cambio se está acelerando, la tendencia de querer hacer cualquier cosa a través de Internet en cualquier lugar y en cualquier momento ha logrado eliminar las barreras tradicionales. En los últimos años ha aumentado significativamente el uso de proveedores de servicios externos y la adopción de nuevas tecnologías como el Cloud Computing, pudiendo conectarse e interactuar de multitud de formas. Sin embargo, las nuevas tecnologías también implican nuevos riesgos. Una encuesta realizada por Ernest & Young en el año 2010 a empresas revela que el 46% de los encuestados respondieron que su inversión anual en la seguridad de la información aumenta con respecto al porcentaje total de los gastos, frente a un 6% que lo disminuye. Puede resultar un buen porcentaje, pero sólo un 30% de los encuestados aseguraron tener un programa de gestión de riesgos asociados a las nuevas tecnologías. Las empresas deberían establecer este tipo de programas de gestión de riesgos, ya que con el aumento de la inversión no se garantiza la protección.

El 23% de los encuestados estaban utilizando servicios de Cloud Computing, el 7% estaba evaluando su uso y el 15% iba a implantarlo en los siguientes 12 meses. Es un número bastante elevado teniendo en cuenta el desconocimiento sobre la fiabilidad y el nivel de seguridad de muchos servicios de Cloud Computing, por lo que otro dato, nada sorprendente pero sí relevante, de este sondeo es que el 50% de los encuestados planeaban gastar más dinero el siguiente año en procesos y tecnologías de prevención de fuga y pérdida de datos, ya que un 52% de ellos identificó la fuga de datos como un riesgo cada vez mayor, asegurando que la seguridad en la privacidad y la protección de información personal es la tercera actividad con mayor importancia en su empresa seguida del cumplimiento de las regulaciones y la protección de la reputación.

Por todo ello, y considerando al Cloud Computing como la herramienta "necesaria" y que su seguridad es un pilar fundamental, se hablará de la seguridad y el cumplimento normativo en el Cloud Computing.

1.1. ¿Qué es Cloud Computing?

La informática ha evolucionado mucho durante los últimos años, a principios de los 60, los ordenadores eran máquinas con un precio muy elevado, complicadas de utilizar y difíciles de mantener. Eran de uso empresarial, diseñados para trabajar con un número muy grande de datos y no estaban conectados a la red.

Sin embargo, entre los años 70 y 80 su uso se generalizó y no fue hasta finales de los 80 cuando comenzaron a usarse ordenadores personales en los puestos de trabajo, eran menos potentes pero también más baratos. A pesar de ello seguían existiendo las máquinas potentes que controlaban las aplicaciones que necesitaban más recursos y los datos sensibles. Estos últimos fueron denominados servidores y los menos potentes clientes. Así comenzó la arquitectura cliente-servidor. Finalmente en los años 90

adoptamos Internet a gran escala, esto hizo posible tanto pasar a otro mundo más allá de nuestros ordenadores navegando por la *world wide web* como poder conectar a los ya definidos cliente y servidor. En esa misma década aparecieron tanto el *hosting*[1] y como su modalidad *housing*, dedicada principalmente a grandes empresas y empresas de servicios web, pudiendo ser considerados como precedentes del Cloud Computing.

En los últimos años estamos asistiendo al surgimiento y desarrollo del Cloud Computing, traducido al español como computación en la nube, servicios en la nube, informática en la nube, nube de cómputo, nube de conceptos o simplemente "la nube". Gracias a ello podemos, entre otras cosas, almacenar todos los recursos de información en servidores de terceros y acceder a ellos a través de Internet desde cualquier punto.

La definición de **Cloud Computing** que generalmente se usa como base es la del NIST[2], *"Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable and reliable computing resources (network, servers, storage, applications, services) that can be rapidly provisioned and released with minimal consumer management effort or service provider interaction»"*, que traducida al castellano vendría a ser: Cloud Computing es un modelo para habilitar un acceso conveniente, bajo demanda y a través del acceso de red a un conjunto compartido de recursos informáticos o computacionales (redes, servidores, almacenamiento, aplicaciones, servicios) que pueden ser rápidamente provisionados y publicados con un mínimo esfuerzo de administración o de interacción con el proveedor de servicios. Cabe destacar que la definición anterior del Cloud Computing es la misma que establece ISO en su documento "*ISO/IEC WD 17788, Cloud Computing – Vocabulary*" del 7 de Marzo de 2012, el cual está en estado de borrador. De este mismo documento pueden obtenerse las cinco características esenciales que definen el Cloud Computing, auto-servicio bajo demanda, acceso amplio a la red, agrupación de recursos, rápida elasticidad y servicio medible y supervisado:

1. Auto-servicio bajo demanda: un usuario puede abastecerse de capacidades como tiempo de servidor y almacenamiento en red, sin necesidad de pedirlo expresamente al proveedor del servicio. Como por ejemplo Windows Live Hotmail.

2. Acceso amplio a la red: se puede acceder a ésta desde diferentes redes y dispositivos heterogéneos, pesados o livianos, como el ordenador o un teléfono móvil. Por ejemplo, en el caso de Dropbox es posible tener documentos almacenados en la nube y consultarlos desde cualquiera de los dos dispositivos anteriormente citados.

3. Agrupación de recursos: existen un conjunto de recursos computacionales (tanto físicos como virtuales) del proveedor que se habilitan para servir a múltiples consumidores de acuerdo con sus necesidades puntuales, lo que implica que se asignen y reasignen continuamente según varíen las necesidades de los clientes y en función de la demanda. Un buen ejemplo sería Windows Live SkyDrive.

[1] Servicio que provee a los usuarios de Internet un sistema para poder almacenar información, imágenes, vídeo, o cualquier contenido accesible vía web.

[2] Instituto Nacional de Estándares y Tecnologías, una agencia del US Departmen of Commerce, creada en 1901.

4. Rápida elasticidad: las capacidades pueden ser rápida y elásticamente aprovisionadas, en algunos casos de manera automática, para escalar hacia fuera y también rápidamente liberadas para escalar hacia dentro. La escalabilidad consiste en aumentar la capacidad de atender usuarios o volumen sin perder calidad en los servicios ofrecidos. La escalabilidad hacia fuera u horizontal consiste en aumentar en número de nodos y la escalabilidad hacia dentro o vertical en añadir más recursos a uno de los nodos en particular. Con esto se consigue que el cliente puede acceder a los recursos de manera inmediata e ilimitada.

5. Servicio medible y supervisado: se controla y optimiza de una manera automática el uso de recursos pudiéndose conocer así en todo momento el nivel de recursos utilizado de una manera transparente tanto para el proveedor como para el cliente.

Tres eventos importantes en la historia del Cloud Computing han sido:

- En 1961, John McCarthy dijo que "algún día la computación se organizaría como un servicio público". [3]

- En los años 90, en Amazon constataron que sólo utilizaban un 10-15% de la capacidad de sus infraestructuras informáticas, por lo que barajaron la posibilidad de ofrecer el espacio sobrante a usuarios. Finalmente en 2006 presentaron los Servicios Web de Amazon. [4]

- Entre los años 2007 y 2008, algunas universidades norteamericanas, la primera fue la Universidad de Washintong, seguida de Carnegie Mellon University, Massachusets Institute of Technology, Stanford University, University of California at Berkeley y la Universidad de Maryland se unieron a ciertas empresas como Google, Microsoft o IBM para comenzar una investigación sobre el Cloud Computing.

Estas importantes inversiones por parte de las grandes empresas que dominan el terreno tecnológico, junto con los avances tanto en la capacidad de procesamiento, como en la conexión a internet y los dispositivos móviles, han conseguido que el Cloud Computing haya tenido y esté teniendo una rápida evolución e implantación, tanto que muchos usuarios disfrutan del Cloud Computing sin darse cuenta. Ofrece una gran cantidad de beneficios como unos bajos costes, seguridad, alto rendimiento y escalabilidad.

Gracias al modelo Cloud Computing se ha cambiado completamente la forma de utilización y entendimiento de las aplicaciones informáticas, se aprovechan al máximo

[3] McCarthy, J., "Centennial Keynote Address", MIT, 1961

[4] En inglés, Amazon Web Services (AWS) http://aws.amazon.com/

las ventajas de internet, los dispositivos móviles y los ordenadores personales. Además implica un ahorro de costes.

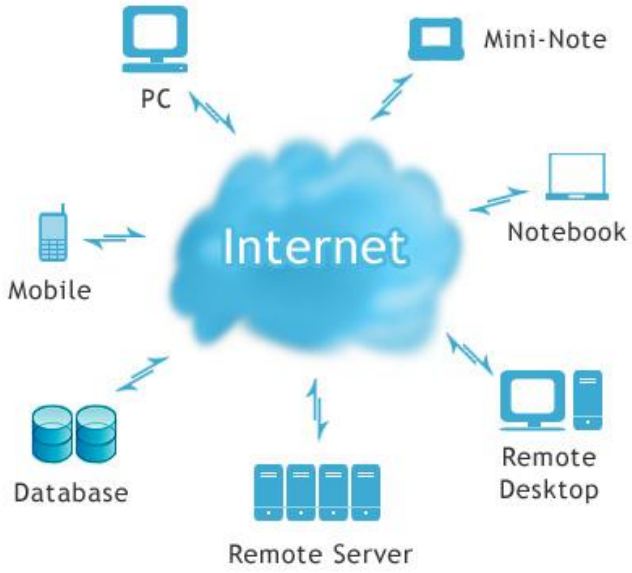

Ilustración 1 - Conexiones del Cloud Computing

1.1.1. Tipos de servicios

Dentro del Cloud Computing existen tres niveles o tres tipos de servicios:

- Software como servicio/*Software as a Service* (Saas): se encarga de suministrar el software como un servicio a través de Internet sin tener que pagar por licencias. El proveedor de la nube proporciona una aplicación al usuario, como por ejemplo, Dropbox o Google Docs. Está dirigido sobre todo a los usuarios finales, los cuales no tienen por qué ser informáticos.

- Plataforma como servicio/*Platform as a Service* (PaaS): es el nivel intermedio. Se encarga de dar una plataforma de procesamiento completa al usuario de manera que este no tenga que comprar ni mantener hardware o software de base y pueda desarrollar aplicaciones o servicios sobre la plataforma. Por ejemplo Google App Engine,[5] que se dirige a los informáticos que crean programas.

- Infraestructura como servicio/*Infastructure as a Service* (IaaS): se trata del nivel más bajo. En este caso trata de suministrar una infraestructura completa, en este entorno los usuarios pueden ejecutar cualquier software, sistemas operativos y aplicaciones en el equipo del proveedor del servicio de Cloud Computing, que por cualquier motivo no quiere instalarlos en su máquina local. Como por

[5] http://code.google.com/intl/es/appengine/docs/whatisgoogleappengine.html

ejemplo EC2 de Amazon,[6] que está dirigido prioritariamente a las grandes empresas.

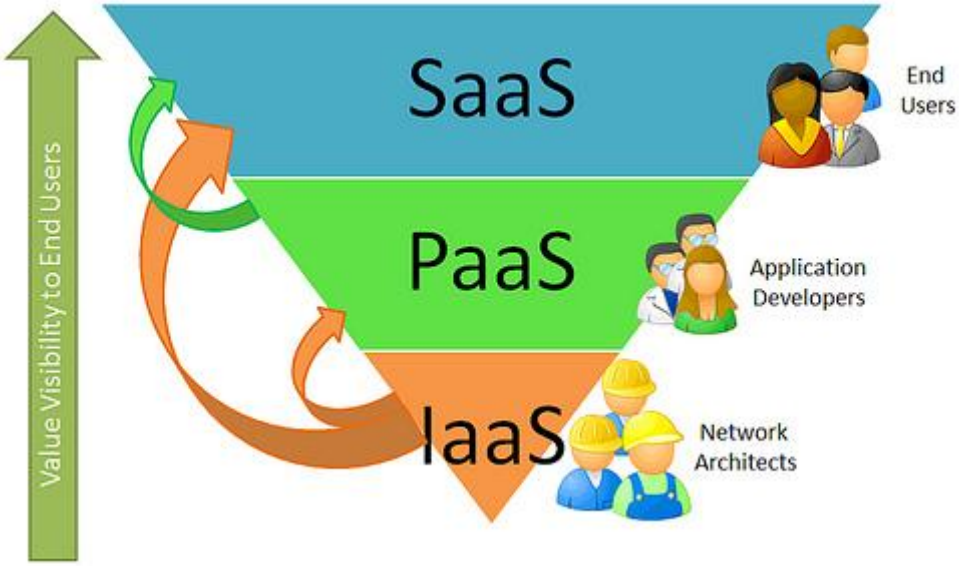

Ilustración 2 - Tipos de Servicio del Cloud Computing

1.1.2. Tipos de infraestructura

En cuanto a modelos de despliegue los sistemas de Cloud Computing se pueden agrupar en diferentes categorías:

- Nubes privadas: son aquellas operadas por una sola organización, la cual decide dónde y cómo se ejecutan los procesos dentro de la nube.

- Nubes de la comunidad: nube de infraestructuras compartidas por varias organizaciones y que forman una comunidad específica con intereses comunes. Puede ser gestionada por la propia comunidad o por un tercero, pero la política de seguridad y privacidad es común. Es una variación de la nube privada.

- Nubes públicas: aquellas en las que todo está en manos de terceros. Muchos usuarios utilizan servicios a través de Internet, que son propiedad de un proveedor que gestiona la infraestructura y los servicios que se ofrecen, y pueden compartir espacio en disco u otras infraestructuras de red con otros usuarios.

- Nubes híbridas: son aquellas en las que se usan varias nubes de las anteriormente descritas por separado pero unidas mediante una portabilidad de datos y aplicaciones. Por ejemplo, una empresa tiene su servidor web en la nube pública

[6] http://aws.amazon.com/es/ec2/

pero el servidor de bases de datos en su propia nube privada. De esta manera la nube pública y la nube privada se mantienen conectadas, los datos sensibles permanecen controlados por la empresa pero el servidor web lo controla un tercero.

TIPO	VENTAJAS	INCONVENIENTES
PRIVADAS	- Mayor control sobre los recursos y los datos sensibles que en la nube pública. - Se asegura que se cumplen con las políticas internas.	- Coste elevado.
COMUNIDAD	- Se asegura que se cumplen con las políticas internas. - Reducción de costes con respecto a la nube privada.	- La seguridad depende del administrador de la infraestructura.
PUBLICAS	- Escalabilidad. - Ahorro de coste y tiempo.	- Se comparte con más usuarios. - La seguridad depende de un tercero. - Poca transparencia para el cliente. - Permite un menor control que cualquier otro tipo de nube.
HIBRIDAS	- Menor complejidad y coste que en la nube privada. - Las ventajas de las nubes que se utilicen.	- Los inconvenientes de las nubes que se utilicen.

Tabla 1 - Ventajas e inconvenientes de los tipos de Cloud.

Fuente: Elaboración Propia.

A continuación se muestra una ilustración como resumen de los tipos de servicio e infraestructura del Cloud Computing.

Ilustración 3 - Conceptos generales del Cloud Computing según la definición de NIST

1.1.3. Desde el punto de vista técnico

Desde un punto de vista más técnico el Cloud Computing tiene que ver con la virtualización, su crecimiento y evolución van de la mano de aquella. Con la virtualización se consigue la creación, a través de software, de una versión virtual de algún recurso tecnológico, como puede ser una plataforma de hardware, un sistema operativo, un dispositivo de almacenamiento u otros recursos de red, es decir, se consigue optimizar la provisión de servicios de TI, y con el Cloud Computing conseguimos desplegar las infraestructuras para que los usuarios o clientes finales puedan disfrutar de los servicios. El Cloud Computing aprovecha al máximo las arquitecturas virtualizadas. Se ha conseguido que el modelo un equipo una aplicación, cambie hacia el modelo de un equipo muchas aplicaciones de una manera en la que los recursos estén disponibles de una manera eficiente y con una mayor flexibilidad. No hay que confundir la virtualización con el Cloud Computing, la virtualización es una tecnología que posibilita la computación en la nube.

Con el Cloud Computing conseguimos una serie de claras ventajas:

- Escalabilidad.
- Reducción de costes debido al "pago por uso".
- Acceso muy rápido a recursos hardware sin inversión inicial por parte de los usuarios.
- Mayor agilidad (*business agility*).

1.1.4. Desde el punto de vista legal

Independientemente de las cuantiosas ventajas del Cloud Computing y de lo mucho que facilita la vida tanto para empresas como para los ciudadanos de a pie, existen ciertas incertidumbres desde el punto de vista legal.

En lugar de tener los datos almacenados en nuestros propios ordenadores o, en el caso de las empresas, en bases de datos propias, se encuentran en "la nube", en cualquier parte del mundo, por lo que la ubicación y procesamiento de estos se convierten en conceptos difíciles de definir. Es más, estos datos pueden trasladarse de un país a otro en un instante. Esto suscita problemas en cuanto a la seguridad de los datos, principalmente la privacidad, la protección de la propiedad intelectual y más aspectos que se verán más tarde detenidamente.

2. Aspectos Técnicos

El uso del Cloud Computing da un cambio en la seguridad informática, ya no se tienen los servidores de una empresa localizados en una sala del edificio a la que sólo pueden acceder las personas autorizadas, sino que ahora la seguridad recae también sobre la empresa suministradora de los servicios en la nube.

Como se ha visto el Cloud Computing brinda numerosas ventajas tanto a las empresas como a los usuarios, pero también ofrece un gran número de oportunidades a los piratas informáticos. Los ataques como robo de contraseñas mediante el *password cracking*[7], envío de spam o ataques de denegación de servicio, son mucho más sencillos y baratos dando un gran cambio en la seguridad informática de grandes empresas.

2.1 Riesgos

Los riesgos más importantes, bien por su frecuencia o por el daño que puedan causar son:

- **Agotamiento de recursos:** como el Cloud Computing es un servicio bajo demanda y, a pesar de que sus infraestructuras están destinadas a producir un alto nivel de servicio y disponibilidad, existe un nivel de riesgo calculado en la asignación de de los recursos, ya que estos se asignan mediante procesos estadísticos. El modelado incorrecto del uso de recursos, la inadecuada provisión

[7] Proceso informático por el cual se consiguen descrifrar las contraseñas de aplicaciones para obtener un acceso no autorizado.

de los mismos e inversiones en infraestructuras, o simplemente un descenso en el rendimiento o un fallo puntual puede conducir, desde la perspectiva del proveedor del servicio, a:

- Falta de disponibilidad de servicio: fallos en ciertos escenarios de aplicaciones muy específicos los cuales se usan un recurso particular muy intensivo.
- Control de acceso comprometido: en algunos casos puede ser posible forzar a un sistema a un "fallo de apertura" en caso de agotamiento de recursos.
- Pérdidas económicas y de reputación debido a los fallos para satisfacer la demanda de los clientes.
- La estimación inexacta por exceso puede llevar a la creación de una infraestructura de gran tamaño que podría llevar a pérdidas económicas y de rentabilidad.

El tiempo de recuperación en los tres primero casos debe estar recogido en el plan de contingencia del proveedor y este deberá de disponer de infraestructuras de respaldo o tener un contrato o acuerdo con otro proveedor para prestar servicio a los clientes.

Desde el punto de vista del cliente la falta de recursos podría conducir a:

- Fallos en la entrega o disminución del rendimiento de los servicios a tiempo real.
- Poner la confidencialidad e integridad de los datos en situación de riesgo.

Según NIST se producen 4,38 horas de caída en un año (siendo la probabilidad de que esté caído de un 0,05%). Una buena práctica sería asegurarse de que las operaciones más críticas se puedan reanudar de una manera casi inmediata y el resto de operaciones lo hagan en un tiempo prudencial.

Este riesgo es reconocido por la ENISA [8] en su informe *Cloud Computing. Benefits, risks and recommendations for information security.*

- **Fallos de aislamiento:** los recursos compartidos y el concepto multi-propietario son dos características del Cloud Computing, ya que el almacenamiento, la red y la capacidad de computación se comparten entre los usuarios. Los proveedores prestan sus servicios de manera escalable con infraestructura compartida, pero a menudo los componentes que forman parte de esta infraestructura no están diseñados para ofrecer las fuertes propiedades de aislamiento que requiere este tipo de arquitectura multi-propietario. Los datos deberían estar debidamente protegidos tanto cuando se encuentran en el lugar donde se almacenan como en el tránsito y su acceso debe ser controlado. La transferencia de los datos se puede proteger mediante la criptografía usando estándares de comunicaciones

[8] European Network and Information Security Agency

seguras, pero la seguridad en el lugar de almacenamiento no es tan sencilla, debido por una parte a los problemas de autenticación de los usuarios y por otra parte a que los procedimientos de almacenamiento no están claros a causa del concepto multi-propietario. La probabilidad de que esto ocurra es mayor en el caso de las nubes públicas que en las nubes privadas y el impacto que tendría sería una pérdida de datos valiosos o sensibles lo que provocaría una pérdida de reputación de los proveedores del servicio. Es recomendable una buena estrategia de defensa, la cual debería incluir computación, almacenamiento y la vigilancia y monitorización de las redes. Las acciones de un usuario no deben afectar a las operaciones de otros usuarios que estén siendo ejecutadas por el mismo proveedor de servicios, por ello la compartimentación debe ser fuerte. Además los clientes no deberían tener acceso a los datos de cualquier otro cliente ni al tráfico de red.

Dentro de este tipo de riesgos se incluyen los ataques de SQL injection que consisten en infiltrar código intruso en una aplicación para realizar consultas en una base de datos, se consigue utilizando vulnerabilidades informáticas en las validaciones de las entradas de texto, por lo tanto ese tipo de ataque afecta a las aplicaciones tipo SaaS. El diseño de la base de datos en la arquitectura multi-propietario que utiliza SaaS consiste en el almacenamiento de todos los usuarios en la misma tabla identificados por el ID de cada usuario que actúa como clave primaria, por ejemplo en el caso de una aplicación SaaS que permita a una empresa llevar un registro de todos sus empleados de manera que todos ellos tengan una cuenta de resgistro asociada y puedan añadir, borrar, modificar o consultar sus datos, una de las posibles tablas sería la que almacenase todos los empleados con sus respectivos datos. Si la aplicación es vulnerable a ataques de SQL injection el atacante podría acceder a los datos de cualquier cliente introduciendo una consulta SQL en el campo de registro.

Este riesgo es citado por la ENISA en su informe *Cloud Computing. Benefits, risks and recommendations for information security*, por Gartner[9] en el informe *Assessing the Security Risks of Cloud Computing* y por la CSA[10] en un informe publicado en 2010, *Top Threats to Cloud Computing V1.0*, que recoge este riesgo dentro de los problemas derivados de las tecnologías compartidas.

- **Empleados desleales:** los empleados que tienen acceso a información privilegiada pueden realizar actividades maliciosas con ellas y esto podría tener un impacto en la confidencialidad, la integridad y la disponibilidad de todo tipo de datos y servicios, y por tanto, indirectamente sobre la reputación de la organización y la confianza del cliente. Por ejemplo los administradores o los auditores de los sistemas.

  Los empleados pueden ser una amenaza desencadenando incidentes de seguridad. Incluso el propio proveedor gestionando las altas y bajas puede crear

[9] Gartner S.A. es una compañía de investigación y consultoría de tecnologías de la información, con sede en Stamford, Connecticut, Estados Unidos. Se conocía como Grupo Gartner hasta 2001.

[10] Cloud Security Alliance se define como una organización internacional sin ánimo de lucro para promover el uso de mejores prácticas para garantizar la seguridad en cloud.

agujeros si este no es informado debidamente de las bajas del personal en la empresa.

Este riesgo está contemplado en el informe *Cloud Computing. Benefits, risks and recommendations for information security* de la ENISA y en el informe *Top Threats to Cloud Computing V1.0* de la CSA. También Gartner en su informe sobre los principales riesgos del Cloud Computing, *Assessing the Security Risks of Cloud Computing*, reconoce que el acceso de usuarios con privilegios puede ser un riesgo, por lo tanto propone como obligatorio consensuar con el proveedor los usuarios que tendrán acceso a los datos para minimizar los riesgos de que haya usuarios con elevados privilegios que no deberían tener acceso a los mismos.

- **Abuso de las ventajas de registro y uso malintencionado:** los proveedores de servicios de Cloud Computing ofrecen a los clientes un registro muchas veces gratuito, para el que no se necesitan demasiados datos, y una capacidad ilimitada de almacenamiento, provocando que cualquier persona puede registrarse y utilizar los servicios que estos proveedores ofrecen. Esto incita que los piratas informáticos abusen de esta facilidad y anonimato relativo que produce este tipo de registros para llevar a cabo sus actividades maliciosas. Según la CSA los proveedores de PaaS han sido tradicionalmente los que más ataques de este tipo han sufrido, pero los piratas informáticos han comenzado a dirigirse también a los proveedores de IaaS. Muchos *botnet*[11] han utilizado los servidores de IaaS para las funciones de difusión y control, por ejemplo los servidores de IaaS han ofrecido alojamiento al *botnet* Zeus, el cual realizaba ataques de *phisingh*[12] mandado emails a las víctimas para que estos siguiesen los enlaces a webs maliciosas que en ellos se mandaban. El pasado 26 de marzo de 2012 tuvo lugar una acción de desmantelamiento por parte del FBI pero esto no implica la detención por completo de la actividad de Zeus. Otro problema que persiste es el *spam*, como medida de defensa han sido publicados bloques enteros de direcciones de red IaaS en la lista negra (*blacklist*) para impedir la llegada de correos masivos.

  Mediante este tipo de ataques no sólo se consigue obtener beneficio económico de los clientes del servicio sino también del propio proveedor, cuanto más crece el uso del Cloud Computing los trabajadores se convierten en un blanco más atrayente para los cibercriminales.

  En el informe sobre las siete mayores amenazas de la infraestructuras cloud *Top Threats to Cloud Computing V1.0*, realizado por la CSA, se proponen soluciones como que el registro inicial y los procesos de validación sean más estrictos, realizar introspecciones exhaustivas del tráfico de clientes de la red, añadir a las *blacklist* bloques de direcciones de la propia red y hacer un seguimiento de las mismas.

[11] Término que hace referencia a un conjunto de robots informáticos o bots, que se ejecutan de manera autónoma y automática pudiendo controlar todos los ordenadores/servicios infectados de forma remota.
[12] Estafa cibernética cometida mediante el uso de un tipo de ingeniería social y caracterizada por intentar adquirir información confidencial de forma fraudulenta.

- **Interceptación de datos en tránsito:** al tratarse de una arquitectura distribuida los datos en tránsito son mucho mayores que en cualquiera de las infraestructuras tradicionales, ya que por ejemplo los datos deben ser transferidos para sincronizar los clientes remotos con las infraestructuras en la nube. La información debe recorrer diferentes nodos para llegar a su destino, cada uno de ellos son un foco de inseguridad. Si se utilizan protocolos seguros, HTTPS por ejemplo, la velocidad total disminuiría debido a la sobrecarga que estos requieren. El entorno de conexión debería ser mediante una red privada virtual, VPN (*Virtual Private Network*) pero esta práctica no siempre se sigue. Por lo que sniffing, spoofing, ataques man-in-the-middle o ataque de repetición pueden ser posibles amenazas. Por otra parte, y en algunos casos, los proveedores de los servicios no ofrecen clausulas de confidencialidad o no la divulgan lo suficiente como para garantizar el respeto por la información secreta del ciente y el "quien sabe lo que circula por la nube" *("know-how" that will circulate in the "cloud").*

  Este riesgo es mencionado en el informe *Cloud Computing. Benefits, risks and recommendations for information security* de la ENISA.

- **Fuga o pérdida de datos:** en la nube el riesgo de que los datos se vean comprometidos incrementa a causa de las numerosas iteraciones que estos sufren debido a la propia arquitectura de la misma. La eliminación o modificación de datos sin una copia de seguridad es un ejemplo obvio, además del almacenamiento en medios poco fiables. Como en la interceptación de datos en tránsito, la fuga de datos tiene el mismo riesgo pero aplicado a la transferencia de datos entre el usuario y el proveedor de servicios de Cloud Computing, desencadenando pérdidas de información. Esto provocaría la pérdida de reputación a la compañía suministradora y de confianza por parte de los clientes. La pérdida o corrupción de claves de cifrado también puede ocasionar una destrucción efectiva de los datos ya que no podrían ser descifrados. Este último caso está reconocido como un riesgo por la ENISA, no sólo por la pérdida de los datos sino por su posible robo si estas claves de cifrado llegan a manos de terceros con intenciones deshonestas.

  Este riesgo está reconocido tanto por la ENISA como por la CSA en los informes *Cloud Computing. Benefits, risks and recommendations for information security* y *Top Threats to Cloud Computing V1.0* respectivamente. Esta última propone remedios como cifrar y proteger la integridad de los datos en tránsito, copias de seguridad de las claves. Otra posible medida para evitar este riesgo podría ser el establecimiento de políticas de seguridad para la generación de claves, almacenamiento, gestión y prácticas de destrucción de las mismas.

  La probabilidad de que este tipo de riesgo ocurra es bastante baja pero su impacto podría llegar a ser alto.

- **Interfaces y APIs[13] poco seguras:** generalmente los proveedores de servicios en la nube ofrecen una serie de interfaces y APIs (cada proveedor ofrece las suyas propias) para el aprovisionamiento, gestión, coordinación y seguimiento, para controlar e interactuar con los recursos, desde arrancar o parar los servicios en la nube hasta aumentar o disminuir los mismos, de tal manera que todo se realiza a través de estas. De una manera general la seguridad y la disponibilidad de servicios del Cloud Computing dependen de la seguridad de estas APIs por lo que son un punto crítico de la seguridad y la privacidad.

  Este riesgo es referenciado por la CSA en su informe *Top Threats to Cloud Computing V1.0*, exponiendo a los proveedores de servicios de computación en la nube a una serie de problemas de seguridad relacionados con la confidencialidad, integridad, disponibilidad y responsabilidad. Los remedios que propone esta organización son analizar el modelo de seguridad, asegurar la implementación de una fuerte autenticación y controles de acceso en sintonía con una transmisión cifrada y la correcta comprensión de la cadena de dependencia asociada con la API.

- **Borrado incorrecto de datos:** este riesgo es difícil de controlar, ya que cuando se solicita el borrado de algún recurso o datos personales en la nube estos se encuentran en soportes en los que también están almacenados los datos de otros clientes y para que su eliminación sea completa sólo sería posible destruyendo dicho soporte, ya que la sobreescritura no es capaz de conseguirlo en dispositivos no regrabables ni ópticos como los CD, DVD o Blu-ray Disc, en caso de que los datos o recursos que se quieren borrar no se encuentren en ninguno de estos tres soportes, el riesgo sería nulo ya que la sobreescritura es totalmente efectiva, sin embargo si hay que utilizar la destrucción física existen ciertas desventajas como la necesidad de transportar los equipos a una ubicación externa o la dificultad de certificación del proceso así como la necesidad de un sistema de destrucción para cada soporte. Esto implica que los datos pueden estar disponibles más allá de la vida útil especificada en las políticas de seguridad de la empresa suministradora.

  Este riesgo se menciona en el informe *Cloud Computing. Benefits, risks and recommendations for information security* de la ENISA.

- **Secuestro de sesión:** si los atacantes obtienen las credenciales de un usuario pueden no solo acceder a actividades y transacciones sino también manipular datos, poner información falseada en lugar de la verdadera. Existen numerosos métodos de ataque como el *phisihing*, citado anteriormente, el fraude la explotación de vulnerabilidades de software (SQL injection) o redirecciones a webs falsas o maliciosas (*pharming).* Este último método de ataque permite al atacante redirigir un nombre de dominio a una máquina distinta, de manera que el usuario que acceda a ese dominio en realidad será redirigido a la página web

[13] Application Programming Interface. Conjunto de funciones y procedimientos para ser utilizado por otro software como una capa de abstracción.

que el atacante haya especificado para ese dominio. Generalmente la técnica de *pharming* es utilizados para realizar ataques de *phishing*.

Algunas de las buenas prácticas para evitar este riesgo son la realización de políticas de seguridad para prohibir compartir credenciales entre usuarios y servicios, aplicar técnicas de autenticación de doble factor siempre que sea posible o monitorizar las sesiones en busca de actividades inusuales.

Riesgo recogido por la ENISA en el informe *Cloud Computing. Benefits, risks and recommendations for information security* y en el informe *Top Threats to Cloud Computing V1.0* realizado por la CSA .

- **Ataque distribuido de denegación de servicio (DDoS):** es un tipo de DoS de manera coordinada entre varios equipos. Se genera un gran flujo de información desde varios puntos de conexión consiguiendo agotar el ancho de banda o la capacidad de procesamiento de la víctima. Un tipo de ataque de denegación de servicios son los ataques EDoS (*Economic Denial of Service*), en un ataque DDoS lo único que se persigue es el colapso mediante peticiones recurrentes y masivas de manera que el servidor no sea capaz de responder a todas las peticiones solicitadas, sin embargo la finalidad de los ataques EDoS no es la caída de los servicios si no un cierre forzado debido a la imposibilidad de hacer frente a los gastos por el uso de los recursos. La ventaja del escalado dinámico del Cloud Computing que permite optimizar el gasto en infraestructura, hace que se puedan solicitar mayor cantidad de recursos si son necesarios o liberarlos en caso de que ya no lo sean. Justamente esta ventaja es lo que aprovechan los ataques DDoS para solicitar masivamente recursos, el servicio sigue funcionando correctamente pero provoca un gasto desorbitado para el proveedor de dicho servicio. Para evitar este tipo de ataques son necesarias las políticas de seguridad para limitar el uso de recursos o tener un empleado capaz de gestionar esto sin dejar que el escalado dinámico se encargue por sí solo.

  En el informe *Cloud Computing. Benefits, risks and recommendations for information security*, realizado por laENISA, se contempla dicho riesgo.

- **Desastres naturales:** el riesgo de que los desastres naturales afecten a las empresas de Cloud Computing es, en general, menor que en comparación a las estructuras tradicionales, ya que los proveedores de los servicios en la nube suelen ofrecer varios sitios redundantes y rutas de red por defecto. Su probabilidad es muy baja pero sin embargo su impacto sería muy alto por lo que su nivel de riesgo es medio. Los principales desastres naturales son inundaciones e incendios.

- **Acceso físico no autorizado:** al concentrarse los recursos en centros de datos grandes y, a pesar de que los controles físicos perimetrales son más fuertes que anteriormente, el impacto que produce la vulneración de los procedimientos de seguridad física es cada vez mayor. Hay que considerar el robo de equipamiento y la pérdida o robo de copias de seguridad. Se vería afectado el hardware físico,

los datos personales y sensibles, la reputación de la empresa y la confianza del usuario entre otros. Para que tanto el acceso físico no autorizado como el robo de equipamiento y copias de seguridad ocurra, los atacantes se aprovechan de las vulnerabilidades de procedimientos inadecuados de seguridad física (pueden incluir la falta de control físico en el perímetro como tarjetas de autenticación a la entrada). Se debería de disponer del servicio de seguridad o protocolo AAA (autenticación, autorización y registro; del inglés *authentication, authorization and accounting*) sin el cual se facilita el acceso no autorizado a recursos e imposibilita el rastreo del uso indebido de los incidentes de seguridad.

- **Problemas con la red:** errores de conexión, congestión en la red o el uso no óptimo son los problemas que pueden ocurrir con las redes, estos problemas pueden explotar las vulnerabilidades del sistema, de la falta de recursos de aislamiento, de la falta de planes de recuperación o de configuración errónea provocada por ejemplo por error humano. También se debe considerar dentro de estos problemas la modificación del tráfico de red, lo que provocaría retrasos en la sincronización, además de que en esta situación las credenciales son vulnerables a la interceptación y reproducción, cabiendo la posibilidad de la lectura de los datos en tránsito.

La siguiente tabla muestra el riesgo, impacto y probabilidad de cada uno de los riesgos anteriormente citados:

	RIESGO	**IMPACTO**	**PROBABILIDAD**
Agotamiento de recursos	Medio	Incapacidad de proporcionar capacidad adicional: Medio/Bajo Incapacidad de proporcionar la capacidad acordada: Alto	Incapacidad de proporcionar capacidad adicional: Media Incapacidad de proporcionar la capacidad acordada: Baja

Fallos de aislamiento	Alto	Muy Alto	Nube privada: Baja Nube pública: Media
Empleados desleales	Alto	Muy Alto	Media
Abuso de las ventajas de registro y uso malintencionado	Alto	Muy Alto	Media
Interceptación de datos en tránsito	Medio	Alto	Media
Fuga o pérdida de datos	Medio	Alto	Media
Interfaces y APIs poco seguras	Medio	Alto	Baja
Borrado incorrecto de datos	Medio	Muy Alto	Media
Secuestro de sesión	Medio	Alto	Media
Ataque distribuido de denegación de servicio (DDos)	Medio	Cliente: Alto Proveedor: Muy Alto	Cliente: Media Proveedor: Baja
Desastres naturales	Medio	Alto	Baja
Acceso físico no autorizado	Alto	Alto	Media
Problemas con la red	Medio	Alto	Media

Tabla 2 - Riesgos Técnicos (Riesgo, impacto y probabilidad).

Fuente: ENISA y Elaboración Propia.

2.2. Medidas de seguridad

De una manera general los proveedores de servicios de Cloud Computing deben encargarse de garantizar la seguridad, impidiendo que personas no autorizadas entren en sus centros de procesamientos de datos y manteniendo los equipos en buen estado y actualizados para poder enfrentarse a las amenazas existentes en Internet. Para reforzar la seguridad se deberían utilizar tanto la deslocalización como la segmentación de datos, permitiendo así poder recuperar la actividad en caso de fallo rápidamente teniendo copias de seguridad prácticamente a tiempo real, además de mantener un control de usuarios, borrar cuentas que no se utilicen o revisar el software para comprobar que no tiene vulnerabilidades. A continuación se explicarán las medidas de seguridad más importantes:

- **Análisis de riesgos:** consiste en estudiar los activos y sus vulnerabilidades, las amenazas y su probabilidad para identificar los riesgos de seguridad, determinar su magnitud e identificar las áreas que requieren implantar medidas de seguridad. Con ello se consigue conocer el impacto de un fallo de seguridad y la probabilidad de que este ocurra. Para la realización del análisis de riesgos existe una guía para la gestión de riesgos de seguridad de la información, la norma ISO/IEC 27005:2008.

- **Plan de seguridad:** las empresas dedicadas al Cloud Computing deben estar preparadas para gestionar correctamente las incidencias y el efecto de las mismas. Partiendo de la premisa de que la seguridad absoluta no existe y si existiese, el coste sería inabordable, la elaboración de un plan de seguridad para una empresa tiene como medios principales:

    - Determinación de activos y procesos.
    - Nivel de seguridad: Actual y deseable.
    - Planificación de la continuidad de negocio.
    - La implementación: de la teoría a la práctica.
    - Obligaciones legales.
    - Métricas: Cuantificando las decisiones.
    - Políticas de seguridad: A partir del plan de seguridad derivan posteriormente las diferentes políticas de actuación de distintos departamentos o situaciones, como puede ser el plan de acción ante el fuego o la política de destrucción de documentos.[14]

  La definición de un buen plan de seguridad es una de las medidas más importantes de seguridad, para poder elaborarlo primero necesitaríamos realizar un análisis de riesgos tal y como ya se ha expuesto, como se ha explicado las diferentes políticas de seguridad pueden aplicarse a distintos departamentos y situaciones por lo que dicha medida de seguridad es eficaz para todos y cada uno de los riesgos anteriormente mencionados. La norma ISO/IEC 17799

[14] INTECO. El plan de seguridad.

(denominada también como ISO 27002) es un estándar de buenas prácticas que puede usarse de ayuda para la realización del plan de seguridad.

- **Infraestructuras de respaldo:** un centro de respaldo es un centro de procesamiento de datos (CPD) diseñado para tomar el control de otro CPD principal en caso de contingencia. El centro de respaldo debería estar en una localización totalmente distinta a la del CPD principal con el objetivo de que no se vean afectados por la misma contingencia simultáneamente, además el centro de respaldo tiene que ser compatible con el centro de procesamiento de datos principal. Existen dos tipos dependiendo de su equipamiento, hot site cuando dicho equipamiento es exactamente igual al del CPD principal, siendo su disponibilidad inmediata, y cold site cuando se trata de un local vacío de material informático pero sí con la infraestructura (aire acondicionado, falso suelo, comunicaciones…)

  La existencia de centros de respaldo sirve como medida de seguridad para riesgos como el agotamiento de recursos, ya que se asegurarían la reanudación de las operaciones más críticas casi de inmediato y el resto en un tiempo prudencial. También es importante en caso de desastres naturales y robo, para evitar la pérdida total de los datos.

- **Planes de contingencia:** la anterior medida de seguridad por sí sola no basta para hacer frente a un riesgo grave, por lo que es necesario disponer de un plan de contingencia, cuya definición formal sería "acciones a realizar, recursos a utilizar y personal a emplear caso de producirse un acontecimiento intencionado o accidental que inutilice o degrade los recursos informáticos o de transmisión de datos de una organización"[15]. Al plan de contingencia también se le conoce como plan de recuperación de desastres o plan de continuidad de negocios, el cual debe contener las medidas técnicas, humanas y organizativas necesarias para asegurar la continuidad de las actividades de la empresa suministradora. El plan de contingencia debe expresar claramente la amenaza, el impacto, los activos e interdependencias que se verían afectados, las medidas organizativas necesarias, así como los recursos materiales necesarios así como el personal encargado del cumplimiento del plan y sus responsabilidades de una manera concreta. Los objetivos principales de un plan de contingencia son minimizar el impacto, limitar la extensión de los daños, facilitar una degradación controlada, adiestrar al personal, proporcionar alternativas y permitir una rápida restauración. Generalmente consta de tres subplanes, el plan de respaldo, el cual recoge las medidas para prevenir que una amenaza se convierta en un desastre, el plan de emergencia cuya finalidad es disminuir los efectos que provoca una amenaza al materializarse, es decir las medidas necesarias durante e inmediatamente después de su materialización y el plan de recuperación el cual se encarga de restaurarlo todo tal y como se encontraba antes de que se produjese el desastre.

[15] A. Ribagorda, Glosario de Términos de Seguridad de las T.I., Ediciones CODA, 1997

El plan de contingencia es uno de los elementos, si no el más importante que compone el plan de seguridad:

Ilustración 4 - Componentes del plan de seguridad. INTECO

Esta medida de seguridad es importante para todos y cada uno de los riesgos mencionados anteriormente, la falta de planes de contingencia supone una gran vulnerabilidad.

- **Seguridad del personal:** es importante que las políticas incluyan controles previos al inicio de la relación laboral (identidad, nacionalidad o situación, historia y referencias de empleo, antecedentes, curso de acogida, cláusula de confidencialidad, asunción de responsabilidades, aceptación del manual de seguridad o código de uso…), tras la conclusión de la relación (revocación de derechos, persistencia de responsabilidades legales y devolución de recursos) y durante la vigencia de la relación laboral de manera general la política de seguridad para el personal debe contener: asignación y administración de responsabilidades, reporte de incidencias, información de cambios de las normas de seguridad, planes de formación y concienciación, campañas de mentalización, perfiles de usuarios y política de control de accesos y manuales de seguridad, los cuales deben ser claros, concisos y permanentemente actualizados.

  Aplicando ciertas medidas, como por ejemplo especificar clausulas legales y de confidencialidad en los contratos laborales y determinar los posibles problemas en los procesos de notificación, se podría minimizar el impacto e incluso evitar ciertos riesgos como la existencia de empleados desleales. Con las

políticas de control de acceso se minimizaría el riesgo de que haya usuarios con elevados privilegios que no deberían tener acceso a los mismos.

- **Compartimentación:** se define como el "aislamiento del sistema operativo, programas y ficheros de datos en los dispositivos de almacenamiento (memoria principal y secundarias), para protegerles de accesos concurrentes o no autorizados".[16] El principio básico para la compartimentación es que cuanta menos cantidad de personas conozcan los detalles, menor será el riesgo de que la información pueda ser robada, comprometida o usada de manera malintencionada. Una compartimentación fuerte es una buena medida de seguridad contra fallos de aislamiento.

  El almacenamiento en sí es muy importante para la seguridad, en función de la duración y el valor de los datos estos se guardarán de manera diferente, por ejemplo, de manera local, en servidores de almacenamiento en red, dispositivos externos… cualquiera que sea el sistema de almacenamiento se deben especificar las políticas que todos los usuarios deben seguir para evitar que la capacidad aumente de manera desordenada con su consiguiente falta de control y posible pérdida de información. Los aspectos más importantes que se deben seguir son entre otros, la ubicación de los archivos dentro del árbol de directorios, qué sistemas de cifrado se utilizará, el tipo de información almacenada, las personas encargadas de la actualización, modificación, borrado y adición de datos, si se realizarán copias de seguridad o qué procedimientos de borrado se utilizarán, estos últimos dos aspectos se explicarán a continuación.

- **Borrado seguro:** existen varios métodos de destrucción de información, entre ellos por ejemplo la desmagnetización, la cual consiste en la exposición de los soportes de almacenamiento a un campo magnético eliminando así los datos almacenados en ellos. La destrucción física como por ejemplo la trituración, a través de la cual se inutiliza el soporte que guarda la información y la sobre-escritura, que consiste en la escritura de un patrón de datos sobre los datos ya contenidos en los soportes de almacenamiento. Sin embargo estos métodos tienen inconvenientes. La desmagnetización al igual que la destrucción física requiere una configuración del sistema para cada soporte y es necesario transportar los equipos a una ubicación externa, pero esta además posee una desventaja añadida, sólo es válida para dispositivos de almacenamiento magnético, mientras que la destrucción física es un método de borrado adecuado para cualquier tipo de dispositivo. Por otro lado la sobre-escritura ofrece grandes ventajas respecto a la desmagnetización y la destrucción física, ya que con una única solución para todos los dispositivos se elimina de forma segura la información y los dispositivos se pueden reutilizar tras este proceso, sin embargo no es efectiva para dispositivos no regrabables ni ópticos como CD's, DVD's, Blu-ray Disc's o pen drive's.

  Métodos como el formateo o los comandos de borrado del sistema operativo no destruyen la información de forma segura.

[16] A. Ribagorda, Glosario de Términos de Seguridad de las T.I., Ediciones CODA, 1997.

- **Copias de seguridad:** es conveniente establecer un procedimiento con el fin de sistematizar la realización de copias de seguridad. Se debe identificar en todo momento qué datos requieren de copias de seguridad, su frecuencia, la frecuencia con la que estas se realicen dependerá de la importancia de la información que se esté almacenando, ubicar estas copias de seguridad en un establecimiento diferente de la información original, probar el sistema de forma exhaustiva, definir la vigencia de las copias o planificar su restauración son algunos de los requisitos que debe cumplir la planificación de copias de seguridad. De esta manera podría evitarse riesgos como la fuga o pérdida de datos.

- **Acceso limitado a los clientes:** no todas las cuentas de los clientes tendrán el mismo sistema de privilegios, algunas por ejemplo sólo tendrán acceso a la operación de lectura y otras sin embargo a escritura y borrado, no sólo eso sino que los clientes no deberían tener acceso a los datos de cualquier otro cliente ni al tráfico de red. Es recomendable que exista un "administrador" para gestionar los cambios en el acceso, por ejemplo cambio de roles, adición de nuevos usuarios o existencia roles con privilegios en casos extraordinarios de emergencias. Con esto conseguiríamos reducir riesgos como el fallo de aislamiento, el acceso físico no autorizado, el secuestro de sesión o el abuso de las ventajas de registro y uso malintencionado.

- **Registro y procesos de validación estrictos:** se deberían realizar controles sobre la identidad de las cuentas de usuario en el registro, además de la existencia de diferentes niveles de controles de identidad basados en los recursos necesarios.

- **Autenticación:** debe existir autenticación mutua, es decir tanto cliente como proveedor deben autenticarse, para operaciones que requieren de alta seguridad sería conveniente realizar una autenticación de doble factor, es decir, aquel tipo de autenticación que requiere dos o más de los tres factores da autenticación (algo que el usuario sabe, algo que el usuario tiene y algo que el usuario es), de esta manera podrían evitarse riesgos como el secuestro de sesión, el acceso físico no autorizado, las interfaces y API's poco seguras y los fallos de aislamiento.

- **Cifrado:** debe utilizarse el cifrado de datos no sólo en los almacenados o en reposo sino en los datos en tránsito, para ello se dispondrá de una política de cifrado de claves para definir qué y que no debe ser encriptado, quien tiene acceso a esas claves y con qué algoritmos será cifrada. Gracias al cifrado de datos pueden evitarse riesgos tales como la interceptación de datos en tránsito y la fuga o pérdida de los mismos, además afecta de manera indirecta a otros tipos de riesgos como el acceso no autorizado, el secuestro de sesión o empleados desleales puesto que si se consiguiesen datos estos estarían cifrados por lo que no supondría una amenaza para los mismos.

- **API's seguras:** es necesario que tanto API's como interfaces estén diseñadas de una manera segura, esto junto con un fuerte control de acceso a las API's sirve como media de seguridad para evitar los problemas de seguridad como acceso y robo a la información, tanto intencionados (ataques de malware para que se realicen acciones para las que no fueron programadas) como accidentales.

- **Medidas para evitar ataques SQL Injection:** las maneras más comunes para evitar ataques de SQL injection son:

    - Parametrización: un error muy común es utilizar el valor introducido en los campos de entrada sin validar previamente que el tipo de dato que se está esperando es el mismo que ha sido recibido, por ejemplo y volviendo al caso anterior de la aplicación en la que se almacenan todos los empleados puede que el nombre de usuario sea un número asociado al empleado y sin embargo sea ese campo donde se escriba la consulta SQL, si se controla el tipo que debe recibir esto no ocurriría, por ello se deben parametrizan las sentencias SQL pudiendo especificar el tipo que se espera para cada parámetro.

    - Validación de entradas: la mayoría de los ataques de SQL injection pueden prevenirse con la adecuada validación de tipo y formato de los campos de entrada que tiene que rellenar el usuario.

  Además de estos pasos generales anteriores existen remedios concretos para las aplicaciones SaaS, por ejemplo mantener con valor oculto el identificador de los usuarios en las consultas o en caso de error en la base de datos nunca mostrar los nombres de las tablas o sus valores en el mensaje de error.

- **Seguridad física:** al igual que con la seguridad personal muchos de los posibles problemas surgen debido a que la infraestructura está bajo el control de un tercero, por ejemplo en el caso de la externalización, por lo que una violación de la seguridad física puede llegar a tener un gran impacto en los clientes, para ello se debe tener muy claro quiénes a parte del personal autorizado tiene acceso a las infraestructuras por ejemplo personal de limpieza, consultores, etc y cada cuanta frecuencia lo hacen, además estos accesos deberían estar controlados bien mediante el personal de vigilancia o bien que dichos accesos sean automatizados, por ejemplo mediante un lector de tarjetas o de huellas digitales. Existen numerosas vías para mantener una buena seguridad física como realizar un inventario de los elementos, proteger los equipos portátiles del personal, realizar auditorías… Todo ello ayudaría a reducir el riesgo de un acceso no autorizado y la posterior pérdida de datos.

- **Controles ambientales:** toda empresa debería tener métodos para evitar daños por incendio e inundaciones y dependiendo de la localización geográfica los demás métodos variarían en función del riesgo de terremotos, etc. Como anteriormente se ha citado se debería disponer de un plan de seguridad para poner en marcha en caso de un accidente de este tipo. Además podría controlarse la temperatura y la humedad en los centros de datos, proteger a los edificios de descargas de rayos, disponer de equipos de continuidad eléctrica en caso de corte del suministro eléctrico, revisar dichos generadores con frecuencia además de los extintores y demás medidas. Es importante disponer de controles ambientales y mantenerlos en buen estado para mitigar daños producidos por desastres naturales y/o un simple pico de tensión.

Por otro lado el cliente también puede adoptar ciertas medidas de para reforzar su seguridad como son:

- **Control perimetral:** la forma básica sería mediante la instalación y configuración de un firewall o cortafuegos, para monitorizar las comunicaciones que se realizan entre el equipo y la red y permitiéndolas o rechazándolas dependiendo de las reglas del administrador del sistema. Un escalón por encima estarían el IDS (*Intrusion Detection System* o Sistema de Detección de Intrusiones) que además de bloquear o permitir las conexiones las analiza siendo capaz de detectar si alguna de ellas transporta contenido malicioso categorizándolo mediante una lista de reglas y heurísticas e informando al administrador del sistema. El control perimetral es uno de los pilares de la seguridad informática.

- **Criptografía:** es recomendable que los clientes cifren los archivos con un nivel adecuado a los datos que estén almacenando en la nube de tal manera que si un tercero accede a ellos no pueda leer el contenido si no dispone de la clave de cifrado. Además utilizando los protocolos SSL[17] (*Secure Sockets Layer* o capa de conexión segura) y TLS[18] (*Transpor Layer Security* o seguridad en la capa de transporte) los datos que viajan desde el servidor en la nube hasta el cliente lo harán cifrados evitando que terceros malintencionados o no puedan acceder a ellos. En el caso de los administradores del sistema de Cloud Computing y desarrolladores de aplicaciones deberán usar SSH[19] (*Secure Shell* o intérprete de órdenes segura) y VPN[20] (*Virtual Private Network* o red privada virtual) para que la comunicación con los sistemas en la nube sea segura.

[17] Protocolo criptográfico que proporciona autenticación y privacidad de la información entre extremos sobre Internet mediante el uso de criptografía.
[18] Protocolo criptográfico que proporciona comunicaciones seguras a través de Internet basado en SSL que cifra los segmentos de las conexiones de red que se encuentran por encima de la capa de transporte usando criptografía asimétrica para el intercambio de claves, cifrado simétrico para la privacidad y códigos de autenticación para la integridad del mensaje.
[19] Protocolo y programa que sirve para accede a máquinas remotas a través de una red utilizando técnicas de cifrado que hacen que la información viaje de manera no legible. Permite copiar datos de forma segura, gestionar claves y pasar los datos de cualquier otra aplicación por un canal seguro.
[20] Tecnología de red que permite una extensión de la red local sobre una red pública o no controlada como es Internet.

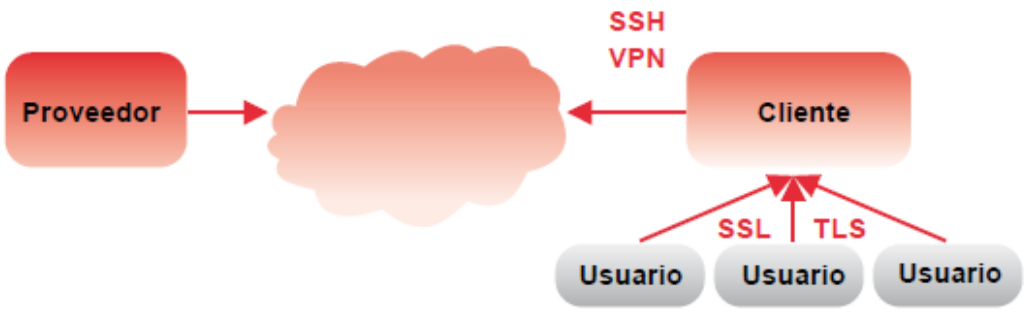

Ilustración 5 - Ejemplo de participantes en el Cloud Computing (INTECO)

- **Gestión de logs o archivos de registro de eventos:** los clientes pueden llevar un control de los logs a los que tenga acceso como por ejemplo el registro de las conexiones peligrosas detectadas por el IDS y por el cortafuegos o la lista de usuarios que acceden a la aplicación, realizando frecuentemente copias de seguridad de ellos y/o almacenándolos en un equipo distinto.

Como se ha visto anteriormente, uno de los objetivos principales de la seguridad en el Cloud Computing es la protección de los datos que abastecen los sistemas y aplicaciones, para ello la CSA propone establecer la Gestión del Ciclo de Vida de la Información y que consta de seis fases: crear, almacenar, utilizar, compartir, archivar y destruir .

Para finalizar con los aspectos físicos se adjunta una tabla con las medidas de seguridad por parte de los proveedores y los diferentes riesgos a los que pueden ser aplicadas:

RIESGOS / MEDIDAS DE SEGURIDAD	Agotamiento de recursos	Fallos de aislamiento	Empleados desleales	Abuso de las ventajas de registro y uso malintencionado	Intercepción de datos en tránsito	Fuga o pérdida de datos	Interfaces y APIs poco seguras	Borrado incorrecto de datos	Secuestro de sesión	Ataque distribuido de denegación de servicio (DDos)	Desastres naturales	Acceso físico no autorizado	Problemas con la red
Análisis de riesgos	X	X	X	X	X	X	X	X	X	X	X	X	X
Plan de seguridad	X	X	X	X	X	X	X	X	X	X	X	X	X
Infraestructuras de respaldo	X		X			X			X		X	X	
Planes de contingencia	X	X	X	X	X	X	X	X	X	X	X	X	X
Seguridad del personal			X										
Compartimentación		X											

Borrado seguro								X					
Copias de seguridad						X					X		
Acceso limitado a clientes		X		X					X			X	
Registro y procesos de validación estrictos			X	X			X					X	
Autenticación		X					X		X			X	
Cifrado			X		X	X			X			X	
API's seguras						X	X						
Medidas para evitar SQL injection		X							X				
Seguridad Física											X	X	
Controles ambientales											X		

Tabla 3 - Relación de los riesgos y sus medidas de seguridad.

Fuente: Elaboración Propia.

3. Aspectos Legales

Como se ha adelantado anteriormente a pesar de sus innumerables ventajas el Cloud Computing entraña ciertos riesgos en cuanto a la protección de datos o la confidencialidad. La computación en la nube podría considerarse tanto un amigo como un enemigo.

Teniendo en cuenta la reducción de los costes y la flexibilidad que aporta muchas PYMES están incorporando el modelo de computación en la nube, sin embargo una encuesta realizada por la ENISA a dichas PYMES asegura que las mayores preocupaciones de estas son la privacidad y la disponibilidad de los datos y servicios así como la confidencialidad y la falta de responsabilidad por parte de los proveedores en caso de que ocurriese algún incidente de seguridad.

What are your main concerns in your approach to Cloud Computing?

Answer Options	Answer Options	Not Important	Medium Importance	Very Important	Showstopper	Rating Average	Response Count
Privacy		0	7	28	31	3,36	66
Availability of services and/or data		3	9	28	26	3,17	66
Integrity of services and/or data		0	9	28	27	3,28	64
Confidentiality of corporate data		1	3	17	43	3,59	64
Repudiation		1	24	25	7	2,67	57
Loss of control of services and/or data		2	14	29	17	2,98	62
Lack of liability of providers in case of security incidents		1	15	25	19	3,03	60
Inconsistency between trans national laws and regulations		8	25	15	12	2,52	60
Unclear scheme in the pay per use approach		10	26	14	9	2,37	59
Uncontrolled variable cost		4	21	26	7	2,62	58
Cost and difficulty of migration to the cloud (legacy software etc...)		7	31	14	6	2,33	58
Intra-clouds (vendor lock-in) migration		5	21	20	10	2,63	56
Other (please specify)							3
					answered question		**73**
					skipped question		**1**

Ilustración 6 - Encuesta de la ENISA a PYMES sobre el Cloud Computing[21]

[21] Survey - An SME Perspective on Cloud Computing

Con respecto a la preocupación sobre la protección de los datos en el Cloud Computing existen regulaciones legales que se explicarán a continuación, partiendo de la base de que en Europa la protección de datos personales está considerada como un derecho fundamental.

La Ley Orgánica de Protección de Datos (LOPD), es una Ley Orgánica española que tiene por objeto proteger y garantizar, en lo que respecta al tratamiento de los datos personales, los derechos fundamentales de las personas físicas, especialmente su honor, intimidad y privacidad. El objetivo de la LOPD se establece en el Artículo 1 *"La presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derecho fundamentales de las personas físicas y especialmente de su honor e intimidad personal y familiar"* y en el Artículo 2 el ámbito de aplicación que más tarde abordaremos. En el ámbito de la Unión Europea La Directiva 95/46/CE sobre protección de datos [22] (a partir de ahora referido como DPD) tiene por objeto lograr el equilibrio entre un alto grado de protección de la vida privada de las personas y la libre circulación de datos personales dentro de la Unión Europea, en concreto el preámbulo del artículo 3 apunta lo siguiente: *"Considerando que el establecimiento y funcionamiento del mercado interior, dentro del cual está garantizada, con arreglo al artículo 7 A del Tratado, la libre circulación de mercancías, personas, servicios y capitales, hacen necesaria no sólo la libre circulación de datos personales de un Estado miembro a otro, sino también la protección de los derechos fundamentales de las personas;".* Esta directiva intenta conservar el equilibrio entre intereses encontrados, por una parte la privacidad de las personas y por otra los intereses por prestar servicios para los que los datos personales son fundamentales. Con la DPD se establecieron unos principios básicos de privacidad que deben cumplirse en el caso del procesamiento de datos personales como puede verse en el Artículo 2(a) *"«datos personales»: toda información sobre una persona física identificada o identificable (el «interesado»); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social;"*. En lo que respecta al Cloud Computing en muchos casos se procesan datos personales, las direcciones de correo electrónico por ejemplo serían un caso de datos personales, además según el Grupo de Trabajo sobre Protección de Datos[23] del Artículo 29 adoptado el año 2007, también las direcciones IP de los equipos utilizados son consideradas datos personales: *"El Grupo de trabajo considera las direcciones IP como datos sobre una persona identificable. En ese sentido ha declarado que «los proveedores de acceso a Internet y los administradores de redes locales pueden identificar por medios razonables a los usuarios de Internet a los que han asignado direcciones IP, pues registran sistemáticamente en un fichero la fecha, la hora, la*

[22] Directiva 95/46/CE del Parlamento Europeo y del Consejo de la Unión Europea, del 24 de octubre de 1995, relativa a la protección de las persona físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, DO Nº L281 del 23 de noviembre de 1995.

[23] El Grupo de Trabajo del Artículo 29 (GT 29) creado por la Directiva 95/46/CE tiene carácter de órgano consultivo independiente y está integrado por las Autoridades de Protección de Datos de todos los Estados miembros, el Supervisor Europeo de Protección de Datos y la Comisión Europea - que realiza funciones de secretariado-. Asimismo, los Estados candidatos a ser miembros de la Unión y los países miembros del EEE acuden a las reuniones del GT 29 en condición de observadores. La Agencia Española de Protección de Datos forma parte del mismo desde su inicio, en febrero de 1997.

duración y la dirección IP dinámica asignada al usuario de Internet. Lo mismo puede decirse de los proveedores de servicios de Internet que mantienen un fichero registro en el servidor HTTP. En estos casos, no cabe duda de que se puede hablar de datos de carácter personal en el sentido de la letra a) del artículo 2 de la Directiva »[24].

Especialmente en aquellos casos en los que el tratamiento de direcciones IP se lleva a cabo con objeto de identificar a los usuarios de un ordenador (por ejemplo, el realizado por los titulares de los derechos de autor para demandar a los usuarios por violación de los derechos de propiedad intelectual), el responsable del tratamiento prevé que los «medios que pueden ser razonablemente utilizados» para identificar a las personas pueden obtenerse, por ejemplo, a través de los tribunales competentes (de otro modo la recopilación de información no tiene ningún sentido), y por lo tanto la información debe considerarse como datos personales."

En el año 2009 el Grupo de Trabajo sobre Protección de Datos del Artículo 29 estableció que no sólo se deben cumplir los requisitos de la legislación de la UE en cuanto a la protección de datos con los usuarios cuyos datos se procesan o almacenan, sino también aquellos que se encuentran en el contenido de redes sociales, como por ejemplo en comentarios o etiquetas y en las imágenes que retratan individuos identificables. Pero en este último caso existe controversia, en algunos Estados miembros de la UE las imágenes son consideradas como datos sensibles ya que podrían ser utilizadas para conocer el origen racial o para deducir sus creencias religiosas o datos relativos a la salud (los datos sensibles en la Ley Orgánica de Protección de Datos son: ideología, afiliación sindical, creencias religiosas, origen racial, salud y vida sexual), aún así el Grupo de Trabajo, de manera general, no lo considera como datos sensibles.

De igual manera el artículo 2b de la Directiva sobre Protección de Datos considera que el tratamiento de los datos personales es: *"cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción."*

Existe una excepción en cuanto a la aplicabilidad de la DPD, se trata del caso de las actividades domésticas, esta posee una condición en el artículo 3 apartado 2 para la aplicación de dicha Directiva en la que dice que *"Las disposiciones de la presente Directiva no se aplicarán al tratamiento de datos personales […] efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas."* Esa excepción es relevante, ya que afecta a los usuarios que usan la nube de manera exclusivamente personal, como por ejemplo en el caso de la correspondencia. El Grupo de Trabajo del Artículo 29 en el año 2009 destaca que un gran número de usuarios de las redes sociales funcionan en un ámbito personal, familiar o doméstico y por ello considera que no se aplica la normativa que regula a los responsables del tratamiento de datos y se aplica la <<exención doméstica>>. No se aplicaría la exención si el usuario utilizase las redes sociales actuando en nombre de una empresa o asociación con fines comerciales, políticos o sociales, si el acceso a la información del perfil fuese pública,

[24] Documento de trabajo WP 37: Privacidad en Internet: - Enfoque comunitario integrado de la protección de datos en línea adoptado el 21.11.2000.

es decir, si todos los miembros de la red social pueden acceder a dicho perfil o cuando los motores de búsqueda puedan indexar los datos, dicho usuario asumirá la plena responsabilidad del tratamiento de datos.

Hasta aquí se ve de manera muy clara que el Cloud Computing procesa muchos datos personales y ha de regirse por estas leyes, pero ¿quién es el responsable del tratamiento de datos? La Ley Orgánica de Protección de Datos describe tanto el concepto de responsable de tratamiento como de encargado de tratamiento, en los artículos 3d y 3g respectivamente *"d)Responsable del fichero o tratamiento: persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento" " g)Encargado del tratamiento: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento."* Por otra parte el Grupo de Trabajo del Artículo 29 en el año 2010 definió también los conceptos de responsable del tratamiento y encargado del tratamiento, ya que su concepto e iteración entre ellos libran un papel fundamental a la hora de aplicar la Directiva 95/46/CE. En cuanto a la definición del responsable del tratamiento la Directiva pone de manifiesto tres componentes fundamentales: *"el aspecto personal («la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo»); la posibilidad de un control plural («que solo o conjuntamente con otros»); los elementos esenciales para distinguir al responsable del tratamiento de otros agentes («determine los fines y los medios del tratamiento de datos personales»)."* Así mismo el responsable del tratamiento puede delegar todas o parte de las actividades del tratamiento a una organización externa, la cual sería la encargada del tratamiento, siempre y cuando se cumpla lo establecido por el RLOPD en el artículo 21.

Parece muy sencillo descubrir en un caso concreto quien sería el encargado y quien el responsable, pero esto no es así ya que pueden existir situaciones complejas en las que los responsables y encargados del tratamiento actúen solos o conjuntamente y con distintos grados de autonomía y responsabilidad. En cualquier caso para que las normas de protección de datos puedan garantizarse es necesario asignar las responsabilidades.

Es muy importante determinar el papel exacto de todas las partes implicadas con respecto al tratamiento de datos personales, ya que con ello se puede determinar qué ley debe aplicarse y a quien o quienes hay que reclamarles responsabilidades. Con esto surge un nuevo tema, la aplicabilidad:

Como se ha citado anteriormente el artículo 2 de la LOPD trata el ámbito de aplicación de la misma a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por sectores público y privado. Establece se regirá por la LOPD todo tratamiento de datos de carácter personal:

a) Cuando el tratamiento sea efectuado en el territorio español en el marco de las actividades de un establecimiento del responsable de tratamiento.
b) Cuando al responsable del tratamiento no establecido en territorio español, le sea de aplicación la legislación española en aplicación de normas de Derecho Internacional público.

c) Cuando el responsable del tratamiento no esté establecido en el territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en el territorio español, salvo que tales medios se utilicen con fines de tránsito.

En el artículo 3 del reglamento de desarrollo de la LOPD, aprobado por el Real Decreto 1720/2007, de 21 de diciembre (RLOPD) se aportan nuevos elementos con respecto al ámbito territorial de aplicación, tales como:

- Si el responsable de tratamiento no se encontrase en territorio español pero existiese un encargado del tratamiento ubicado en España, a este último se le aplicarían las medidas de seguridad en el tratamiento de datos de carácter personal (Título VIII del reglamento).
- Si el responsable del tratamiento no se encuentra establecido en la Unión Europea y utilizase medios situados en España (a excepción de que estos sean utilizados con fines de tránsito) deberá existir un representante establecido en el estado español.
- Se entiende por establecimiento cualquier instalación estable que permita el ejercicio efectivo y real de una actividad, con independencia de su forma jurídica.

Ahora bien, hay que tener en cuenta al encargado de tratamiento y no sólo al responsable, ya que si aquel entra en juego estaríamos hablando de un tratamiento de los datos por cuenta de terceros, por lo que se consideraría que no hay comunicación de datos. En este caso obligatoriamente debe existir un contrato o relación jurídica donde se especifique la actividad que llevará a cabo el encargado de tratamiento bajo el mandato del responsable del tratamiento y su vinculación. En el artículo 12 de la LODP se regula el tratamiento de datos personales por parte de terceros. *"[…] 2. La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas. En el contrato se estipularán, asimismo las medidas de seguridad a que se refiere el artículo 9 de esta Ley que el encargado del tratamiento está obligado a implementar.*

3. Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento. […]"

En estas situaciones en las que exista un tercero prestando servicios de Cloud Computing, y sea de aplicación la LOPD, también hay que aplicar lo previsto en el capítulo III, encargado de tratamiento, del RLOPD (arts.20, 21 y 22). Una de las obligaciones que se estipula en estos artículos, en concreto en el artículo 20 es que el responsable de tratamiento deberá velar por que el encargado de tratamiento reúna las garantías para el cumplimiento de lo dispuesto en el Reglamento. En el artículo 21 se regula la posibilidad de subcontratación de los servicios, el encargado de tratamiento no podrá subcontratar la realización de ningún tratamiento que se le hubiera encomendado por parte del responsable del tratamiento, excepto que este último hubiera dado

autorización para ello, pero existen situaciones en las que el encargado del tratamiento podrá subcontratar sin necesidad de autorización:

- Que en el contrato de servicios que se realizó entre el encargado y el responsable del tratamiento se especifiquen los servicios que puedan ser objeto de subcontratación indicando, si es posible, la empresa con la que se vaya a subcontratar. En el caso de que no se indicase la empresa de subcontratación el encargado del tratamiento indique al responsable los datos que la identifiquen antes de proceder a la subcontratación.
- Que el tratamiento de datos de carácter personal por parte del subcontratista se ajuste a las instrucciones del responsable del fichero.
- Que el encargado del tratamiento y la empresa subcontratista formalicen un contrato, en este caso el subcontratista será tratado como encargado del tratamiento.

Y por último el artículo 22, conservación de los datos por parte del encargado del tratamiento, en el que se especifica que una vez cumplida la prestación, los datos de carácter personal deberán ser destruidos o devueltos (no procederá la destrucción de los datos cuando exista una previsión legal que exija su conservación, en cuyo caso deberá procederse a la devolución de los mismos garantizando la conservación del fichero por parte del responsable del mismo) al responsable del tratamiento, al igual que cualquier soporte o documentos en los que conste cualquier dato de carácter personal.

La Directiva de Protección de Datos también define el derecho nacional aplicable, se determina en el artículo 4:

"Artículo 4
Derecho nacional aplicable
1. Los Estados miembros aplicarán las disposiciones nacionales que haya aprobado para la aplicación de la presente Directiva a todo tratamiento de datos personales cuando:
a) el tratamiento sea efectuado en el marco de las actividades de un establecimiento del responsable del tratamiento en el territorio del Estado miembro. Cuando el mismo responsable del tratamiento esté establecido en el territorio de varios Estados miembros deberá adoptar las medidas necesarias para garantizar que cada uno de dichos establecimientos cumple las obligaciones previstas por el Derecho nacional aplicable;
b) el responsable del tratamiento no esté establecido en el territorio del Estado miembro, sino en un lugar en que se aplica su legislación nacional en virtud del Derecho internacional público;
c) el responsable del tratamiento no esté establecido en el territorio de la Comunidad y recurra, para el tratamiento de datos personales, a medios, automatizados o no, situados en el territorio de dicho Estado miembro, salvo en caso de que dichos medios se utilicen solamente con fines de tránsito por el territorio de la Comunidad Europea.
2. En el caso mencionado en la letra c) del apartado 1, el responsable del tratamiento deberá designar un representante establecido en el territorio de dicho Estado miembro, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento."

Según este artículo de la DPD y, por supuesto, según la LOPD, pueden diferenciarse 3 circunstancias, y así lo hace la ENISA en el informe "*Cloud Computing. Benefits, risks and recommendations for information security.* Catteddu y Hogben*"*:

1. El responsable esté físicamente en un estado miembro. Cuando el mismo se establece en el territorio de varios estados miembros se deben tomar las medidas necesarias para garantizar que todos y cada uno de estos establecimientos cumple las obligaciones establecidas por la legislación nacional aplicable.
2. El responsable no esté físicamente en un estado miembro y además se rija por las leyes internacionales.
3. El responsable del tratamiento no esté en el territorio de un estado miembro pero recurra para el tratamiento de datos a medios situados en él, a menos que los medios empleados en el territorio de la Comunidad Europea se utilicen únicamente para los fines de tránsito. Esto se contempla en el Artículo 4c de la DPD: *"el responsable del tratamiento no esté establecido en el territorio de la Comunidad y recurra, para el tratamiento de datos personales, a medios, automatizados o no, situados en el territorio de dicho Estado miembro, salvo en caso de que dichos medios se utilicen solamente con fines de tránsito por el territorio de la Comunidad Europea."*. Así como en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos Personales, en el artículo 2.1 c) también está presente lo citado anteriormente: *"Se regirá por la presente Ley Orgánica todo tratamiento de datos de carácter personal: […] c) Cuando el responsable del tratamiento no esté establecido en territorio de la Unión Europea y utilice en el tratamiento de datos medio situados en el territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito."*

Para este último caso un ejemplo claro sería el siguiente: un usuario dentro de la Unión Europea introduce sus datos en un formulario de la web, la DPD no sería aplicable puesto que el ordenador se usaría meramente con un fin de tránsito. Pero si las empresas suministradoras de servicios de Cloud Computing utilizasen, por ejemplo, cookies, código Flash o JavaScript la DPD sí sería aplicable. El Grupo de Trabajo del Artículo 29 en el año 2008 dice sobre esto que: *"La utilización de cookies y de programas informáticos similares por un prestador de servicios en línea puede también considerarse como un recurso a medios en el territorio de un Estado miembro, invocándose así la aplicación del Derecho en materia de protección de datos de dicho Estado miembro."* Por lo tanto si los proveedores de servicios de Cloud Computing utilizan cookies (o similares) estarían incluidos en la jurisdicción de la DPD, pero si no lo hacen quedarían fuera del ámbito de aplicación de la DPD.

En el artículo 5.3 de la Directiva 2002/58/CE, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, encontramos que: *"Los Estados miembros velarán por que únicamente se permita el almacenamiento de información, o la obtención de acceso a la información ya almacenada, en el equipo terminal de un abonado o usuario, a condición de que dicho abonado o usuario haya dado su consentimiento después de que se le haya facilitado información clara y completa, en particular sobre los fines del tratamiento de los datos, con arreglo a lo dispuesto en la Directiva 95/46/CE. Lo anterior no impedirá el posible almacenamiento o acceso de índole técnica al solo fin de efectuar la transmisión de una comunicación a través de una red de comunicaciones electrónicas, o en la medida de lo estrictamente necesario a fin de que el proveedor de un servicio de*

la sociedad de la información preste un servicio expresamente solicitado por el abonado o el usuario." Con esto se pretende proteger a los usuarios de los estados miembros, ya que es el usuario el que decide si sus datos se almacenarán o no (mediante cookies o similares), pero a la vez lo que consigue es que si los usuarios rechazan las cookies toda esta protección anteriormente citada (artículo 4.1 c) desaparece, ya que como hemos visto antes si no se utilizan cookies, los ordenadores de los clientes serían utilizados y considerados exclusivamente para la transmisión y no cumplirían el requisito para que la DPD sea aplicable.

Con esto se llega a la conclusión de que la aplicabilidad de la DPD depende de una manera muy relevante del lugar donde se encuentre establecido el responsable del tratamiento o en su defecto el encargado del mismo. Por ello en la Directiva 2000/31/CE, en concreto en el considerando 19, se especifica que: *"Se debe determinar el lugar de establecimiento del prestador de servicios a tenor de los dispuesto en la jurisprudencia del Tribunal de Justicia, según la cual el concepto de establecimiento implica la realización efectiva de una actividad económica a través de un establecimiento fijo durante un periodo indefinido.[…] cuando se trata de una sociedad que proporciona servicios mediante un sitio Internet, dicho lugar de establecimiento no se encuentra allí donde está la tecnología que mantiene el sitio ni allí donde se puede acceder al sitio, sino el lugar donde se desarrolla la actividad económica."*

El lugar en donde esté establecido el responsable del tratamiento es relevante para la aplicabilidad de la DPD, pero el lugar de ubicación del "cliente" o persona a la que pertenezcan los datos tratados no son pertinentes a este respecto. Esto también se afirma en el informe de la ENISA de Catteddu y Hogben nombrado anteriormente.

Parece que una vez que tenemos claro que lo importante es tener establecido el rol de responsable del tratamiento ya lo tendríamos todo resuelto, pero no es tan sencillo, primero vamos a ver, en concreto en el caso de España, cual serían esos países miembros de hemos estado hablando. En el título V de la LOPD Artículo nº33 se dice que *"no se podrán realizar transferencias temporales ni definitivas de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogido para someterlos a dicho tratamiento con destino a países que no proporcionen un nivel de protección equiparable al que presta la presente Ley"*. En general tanto el título V de la LOPD como el título VI del Real Decreto por el que se aprueba la Ley Orgánica de Protección de datos (RLOPD) se trata el movimiento internacional de datos, y como dice el artículo nº33 especificado anteriormente, se establece como principio general que no se pueden hacer transferencias de datos personales a países que no proporcionen un nivel de protección equiparable al de la LOPD. Además de los Estados Miembros de la Unión Europea, Islandia, Liechtenstein, y Noruega, la relación de países cuyo nivel de protección se considera equiparable por la Agencia Española de Protección de Datos, según lo establecido en el art. 67 del Reglamento de desarrollo de la LOPD, es la siguiente:

- Suiza, de acuerdo con la Decisión de la Comisión 2000/518/ CE, de 26 de julio de 2000.
- Canadá respecto de las entidades sujetas al ámbito de aplicación de la ley canadiense de protección de datos, de acuerdo con la Decisión 2002/2/CE de la Comisión de 20 de diciembre de 2001.
- Argentina, de acuerdo con la Decisión 2003/490/CE, de la Comisión de 30 de junio de 2003.

- Guernsey, de acuerdo con la Decisión 2003/821/CE de la Comisión, de 21 de noviembre de 2003.
- Isla de Man, de acuerdo con la Decisión 2004/411/CE de la Comisión, de 28 de abril de 2004.
- Jersey, de acuerdo con la Decisión 2008/393/CE de la Comisión, de 8 de mayo 2008.
- Islas Feroe, de acuerdo con la Decisión 2010/146/UE de la Comisión de 5 de marzo de 2010.
- Andorra, de acuerdo con la Decisión 2010/625/UE, de la Comisión de 19 de octubre de 2010.
- Israel, de acuerdo con la Decisión de la Comisión de 31 de enero de 2011 de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo.
- Las entidades estadounidenses adheridas a los principios de "Puerto Seguro" (Safe Harbor), de acuerdo con la Decisión 2000/520/CE de la Comisión de 26 de julio de 2000. En EEUU no existe ninguna legislación que exija una regulación del procesamiento de datos similar a la Directiva e Protección de datos 95/46/CE en la Unión Europea, por lo que el departamento de comercio de los Estados Unidos (*U.S. Department of Commerce*) junto con la Unión Europea el programa Safe Harbor que permite a empresas estadounidenses, Google por citar un ejemplo, que cumplan con los requisitos exigidos por la Directiva adherirse a dicho programa. El Acuerdo de "Puerto Seguro" consta de siete principios básicos, referidos a la notificación (información a los afectados), opción (posibilidad de oposición de los afectados), transferencia ulterior a terceras empresas, seguridad, integridad de los datos (principios de finalidad y proporcionalidad), derecho de acceso y aplicación (procedimientos para la satisfacción de los derechos de los afectados).

A continuación se muestran dos imágenes en las que puede verse un mapa global de las leyes de protección de todo el mundo:

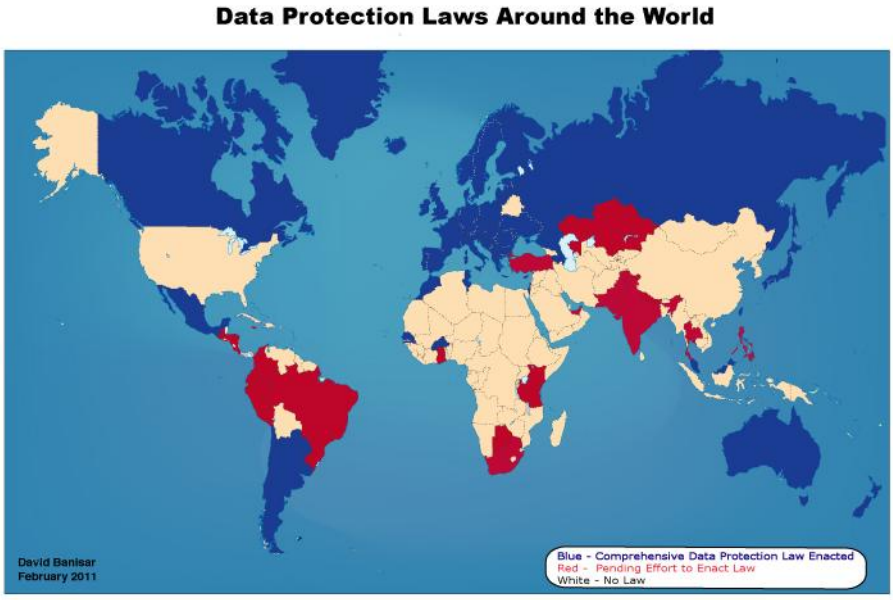

Ilustración 7 – Mapa global de leyes de protección de datos de Privacy International (Febrero 2011)

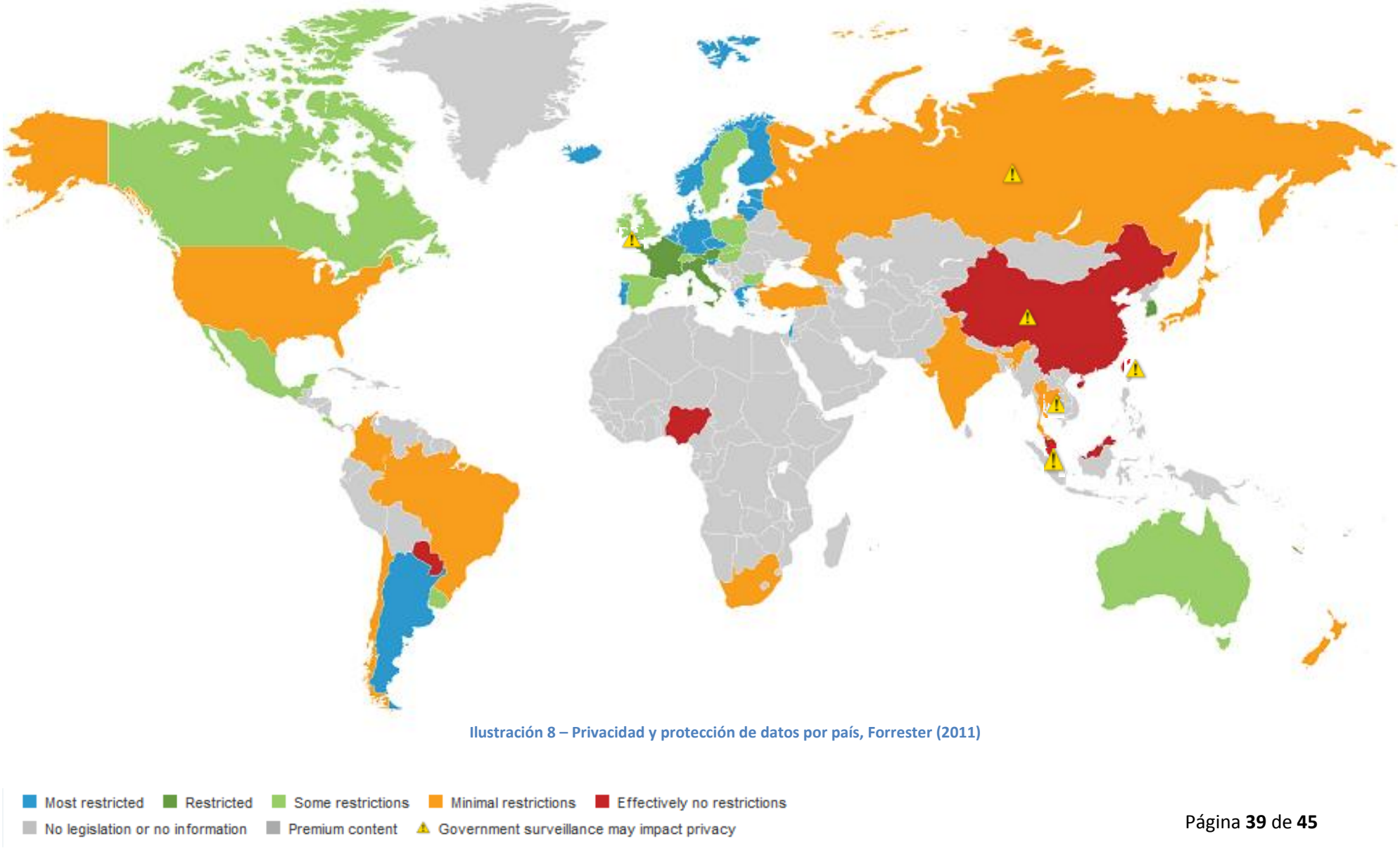

Ilustración 8 – Privacidad y protección de datos por país, Forrester (2011)

Esta última ilustración es muy poco fiable ya que España en concreto es uno de los países con leyes más restrictivas en cuanto a la protección de datos personales, sin embargo Forrester decide calificarla con el nivel 3 de 6 en su escala, siendo su nivel de privacidad y protección de datos "Algo restrictivos". Además de las leyes españolas mencionadas anteriormente cabe destacar la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI). Sin duda los servicios de computación en la nube son servicios de prestación de servicios de la Sociedad de la Información, pero estos, de conformidad con el artículo 6 de la LSSI, no requieren de autorización previa. Sin embargo, los proveedores de servicios de Cloud Computing deberán comunicar al Registro Mercantil al menos un nombre de dominio o dirección de Internet en la que prestan sus servicios con el fin de permitir su identificación, por consiguiente quedan obligados a suministrar determinada información, especificada en el artículo 10 de la LSSI, a los destinatarios y a los órganos que resultarán competentes de forma permanente, fácil, directa y gratuita, entre la que se encuentra *"su nombre o denominación social; su residencia o domicilio, o en su defecto, la dirección de uno de sus establecimientos permanentes en España; su dirección de correo electrónico o cualquier otro dato que permita establecer con él una comunicación directa y efectiva"* , la información correspondiente en el caso de que se ejerciese una profesión regulada o *"las normas profesionales aplicables al ejercicio de su profesión y los medios a través de los cuales se puedan conocer, incluidos los electrónicos."*

Las responsabilidades que exige la LSSI a los suministradores de servicios de la Sociedad de la Información hacen que estas adopten medidas oportunas para evitar tener acceso a la información de terceros que almacenan, lo que implica al no tener conocimiento efectivo eludirían responsabilidades sobre el mismo, pero esto supondría una ventaja en relación con la seguridad para el propio destinatario de sus servicios.[25]

A pesar de las especificaciones de Ley Orgánica de Protección de Datos como de las Directiva 95/46/CE y debido a la evolución de las redes y tecnologías existen incertidumbres en cuanto a la asignación de responsabilidades en el tratamiento de los datos de carácter personal y en cuanto al alcance de las legislaciones nacionales aplicables. A causa de ello el Grupo de Trabajo sobre Protección de Datos del Artículo 29 ha tratado de aprobar dictámenes en los que se tratan específicamente temas que debido a la velocidad de vértigo con la que ha cambiado la sociedad estos últimos años no están contemplados en la Directiva 95/46/CE, por ejemplo en 2009 se aprobó el dictamen que habla sobre las redes sociales y en 2010 se aprobó el Dictamen que trata los conceptos de responsable del tratamiento y encargado de tratamiento con una mención directa al Cloud Computing. Por todo ello la Comisión Europea ha propuesto un proyecto normativo, publicado el 25 de enero de 2012, para unificar las distintas normas de protección de datos de los Estados miembros, que sustituirá a la actual Directiva 95/46/CE, y por la cual los Estados podrán sancionar a las empresas que cometan violaciones graves de la privacidad o negligencias en la custodia de información con multas de hasta el 2% de los ingresos mundiales de dichas empresas. La propuesta de la Comisión incluye algunos cambios como la notificación por parte de las empresas toda violación de datos grave, tanto a las autoridades como a los usuarios, a ser posible en un plazo de 24 horas, el "derecho al olvido" que ayudará a los usuarios a borrar sus datos cuando no existan razones legítimas para conservarlos, el acceso más

[25] Cloud Compilance Report. Versión 1 – mayo 201. CSA

fácil a los propios datos o la transferencia de los datos personales propios con mayor facilidad de un proveedor de servicios a otro.

Con respecto a la responsabilidad por incumplimiento de las leyes españolas anteriormente citadas, es necesaria la mención al Código Penal. A través del Cloud Computing y al tratarse de un entorno tan amplio podrían incurrirse numerosos artículos del Código Penal, aunque en concreto se analizará el delito de estafa. El 23 de diciembre de 2010 entró en vigor la reforma del Código Penal por la que se incorpora por primera vez la responsabilidad penal de las personas jurídicas. En el artículo 248 se regula el delito de estafa estableciendo que:

"1. Cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno.

2. También se consideran reos de estafa:

a. *Los que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro.*
b. *Los que fabricaren, introdujeren, poseyeren o facilitaren programas informáticos específicamente destinados a la comisión de las estafas previstas en este artículo.*
c. *Los que utilizando tarjetas de crédito o débito, o cheques de viaje, o los datos obrantes en cualquiera de ellos, realicen operaciones de cualquier clase en perjuicio de su titular o de un tercero."*

Las sanciones por delitos de estafa varían en función de la cantidad defraudada variando desde seis a tres años de cárcel, siempre y cuando esta exceda los 400 euros.

En concreto, el ámbito del Cloud Computing resulta muy aconsejable que las empresas dispongan de sistemas de prevención, medidas de vigilancia y control sobre sus empleados, ya que si cualquiera de estos comete hechos delictivos por no haberse ejercido sobre ellos el "debido control", la empresa también será penalmente responsable tal y como se indica en la Ley Orgánica 5/2010, de 22 de junio, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal: *"Para la fijación de la responsabilidad de las personas jurídicas se ha optado por establecer una doble vía. Junto a la imputación de aquellos delitos cometidos en su nombre o por su cuenta, y en su provecho, por las personas que tienen poder de representación en las mismas, se añade la responsabilidad por aquellas infracciones propiciadas por no haber ejercido la persona jurídica el debido control sobre sus empleados, naturalmente con la imprescindible consideración de las circunstancias del caso concreto a efectos de evitar una lectura meramente objetiva de esta regla de imputación"*

Artículo 6.1 del Código Civil: "La ignorancia de las leyes no excusa de su cumplimiento"

4. Conclusiones

Las empresas deben garantizar que sus sistemas son seguros y que los riesgos están gestionados, estas deben poseer mecanismos y herramientas de auditoría para determinar cómo se almacenan los datos, se protegen y se utilizan tanto para validar los servicios como para verificar el cumplimiento de las políticas, teniendo en cuenta su ubicación geográfica por los riesgos que pueden conllevar, ya citados anteriormente. Estas auditorías deberían ser tanto internas como externas para una mayor fiabilidad. Deben poner en marcha un programa de gestión de riesgos que sea suficientemente flexible como para adaptarse al entorno de riesgos variables y en continua evolución al que se somete el Cloud Computing, prestando especial atención a los roles y responsabilidades involucrados en dicha gestión y, no sólo a estos sino a todos los empleados incluyendo políticas de seguridad con el personal. En estas políticas deben estar muy claras las responsabilidades de cada empleado y qué ocurriría en todos y cada uno de los casos de incumplimiento.

El Cloud Computing puede usarse para que los cuerpos y fuerzas de seguridad ejerzan un mayor control sobre la población pudiendo proteger a los ciudadanos de actos violentos vinculados a la seguridad pública y a la seguridad de los estados. Pero también para mal, pues ¿donde quedaría la intimidad? Por ejemplo, es sabido que en Estados Unidos debido a la ley antiterrorista, USA Patriot Act, está permitido a las autoridades norteamericanas inspeccionar los datos que albergan las compañías de sus países aunque los servidores estén físicamente localizados en otros países. A causa de esto el gobierno francés va a invertir 135 millones de euros al proyecto Andrómeda, que consiste en crear su propio sistema de Cloud Computing para que los datos sensibles de empresas francesas no se alojen en otros países, en este proyecto participan empresas como Orange, Thales oDassault.

5. Futuras líneas de trabajo

Este trabajo fin de grado abre futuras líneas de trabajo. Las más significativas son las siguientes:

- **Normalizar/estandarizar:** aún no existen estándares definidos para facilitar la interoperabilidad o portabilidad entre otros, por lo que se recomienda el establecimiento de estándares tecnológicos, así como de términos y condiciones generales para su uso. IEEE (Institute of Electrical and Electronics Engineers) en un comunicado en 2011 aseguraba que el Cloud Computing crecería de una manera espectacular pero “sin un marco común y flexible de interoperabilidad, la innovación podría resentirse, dejando a los usuarios en un ecosistema aislado”. IEEE por su parte tiene dos grupos de trabajo, P2301 y P2302 que trabajarán en la estandarización de la gestión y la portabilidad y en la interoperabilidad entre clouds respectivamente.

- **Armonización legal internacional:** ajustar el marco legal para la protección de datos del Cloud Computing mundialmente, eliminando así riesgos comentados anteriormente cuando se mueven datos fuera de la Unión Europea. Con esto se lograrían eliminar las barreras técnicas legales y de esta manera promover que tanto ciudadanos como empresas se beneficien del uso del Cloud Computing en un ambiente idóneo para desarrollos técnicos futuros.

6. Bibliografía

CATTEDDU, D., & HOGBEN, G. (2009). *Cloud Computing. Benefits, risks and recommendations for information security.* Heraklion: ENISA.

Comité Económico y Social Europeo. (26 de octubre de 2011). Dictamen del Comité Económico y Social Europeo sobre el tema «La computación en nube (cloud computing) en Europa» (Dictamen de iniciativa).

CSA. (mayo de 2011). Cloud Compilance Report. *Capítulo Español de Cloud Security Alliance. Versión 1* .

CSA. (marzo de 2010). Top Threats to Cloud Computing V1.0.

Deutsch, D. R. (27 de noviembre de 2011). ISO Focus Article on Cloud Computing.

Directiva 2000/31/CE del parlamento europeo y consejo. (8 de junio de 2000). Relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico).

Directiva 2002/58/CE del parlamento europeo y del consejo. (12 de julio de 2002). Relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas).

Directiva 95/46/CE del parlamento europeo y del consejo. (24 de octubre de 1995). Relativa a la protección de las personas físicas en lo que respecta al tratamientode datos personales y a la libre circulación de estos datos.

Documento de trabajo. Privacidad en Internet: Enfoque comunitario integrado de la protección de datos en línea. (21 de noviembre de 2000). *WP 37* .

ENISA. (2009). *An SME perspective on Cloud Computing. Survey.*

Ernst & Young. (2010). Borderless security. *Global Information Security Survey* .

Garnacho, A. R. (1997). *Glosario de Términos de Seguridad de las T.I.* Madrid: CODA S.L.

Gartner. (2008). *Assessing the Security Risks of Cloud Computing.*

Grupo de Trabajo sobre Protección de Datos del Artículo 29. (4 de abril de 2008). Dictamen 1/2008 sobre cuestiones de protección de datos relacionadas con motores. *WP 148* .

Grupo de Trabajo sobre Protección de Datos del Artículo 29. (16 de febrero de 2010). Dictamen 1/2010 sobre los conceptos de «responsable del tratamiento» y «encargado. *WP 169* .

Grupo de Trabajo sobre Protección de Datos del Artículo 29. (20 de junio de 2007). Dictamen 4/2007 sobre el concepto de datos personales. *WP 136* .

Grupo de Trabajo sobre Protección de Datos del Artículo 29. (12 de junio de 2009). Dictamen 5/2009 sobre las redes sociales en línea. *WP 163* .

Grupo de Trabajo sobre Protección de Datos del Artículo 29. (30 de mayo de 2002). Documento de trabajo relativo a la aplicación internacional de la legislación comunitaria sobre protección de datos al tratamiento de los datos personales en Internet por sitios web establecidos fuera de la UE. *WP 56* .

INTECO. (octubre de 2011). Guía para empresas: seguridad y privacidad del cloud computing.

INTECO-CERT. (marzo de 2011). Riesgos y Amenazas en el Cloud Computing.

ISO. (7 de Marzo de 2012). ISO/IEC WD 17788, Cloud Computing - Vocabulary.

Jansen, W., & Grance, T. (enero de 2011). Guidelines on Security and Privacy in Public Cloud Computing. *Draft NIST Special Publication* .

Ley orgánica 10/1995 del Código Penal. (23 de noviembre de 1995).

Ley Orgánica 5/2010 por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. (23 de junio de 2010).

LOPD. Ley Orgánica 15/1999 de Protección de Datos de Caracter personal. (13 de diciembre de 1999).

Mell, P., & Grance, T. (Septiembre de 2011). The NIST Definition of Cloud Computing. *NIST Special Publication 800-145* .

RLOPD. Real Decreto por el que se aprueba el reglamento de desarrollo de la Ley Orgánica 15/1999 de Protección de Datos de Caracter Personal. (19 de enero de 2008).