Luis Joyanes Aguilar
Catedrático de Lenguajes y Sistemas Informáticos
Escuela de Ingeniería y Arquitectura
Universidad Pontificia de Salamanca

COMPUTACIÓN EN LA NUBE

Notas para una estrategia española en *CLOUD COMPUTING*

Nube, o Computación en la Nube (términos para definir *Cloud Computing*)*, es un concepto tecnológico *(buzzwords*) cada vez más utilizado. Las organizaciones ven en esta tecnología la solución a muchos problemas, económicos o de infraestructuras tecnológicas.

La adopción de la computación en la nube (**SaaS, PaaS** e **IaaS)** está creciendo a gran velocidad y los modelos de entrega o despliegue de la nube (**privada, pública, híbrida y comunitaria)** ofrecidos por multitud de proveedores**, se han hecho** habituales en la terminología de las estrategias empresariales o centros de investigación

En este artículo se pretende analizar estos modelos, *casi* estándares en la industria; sus ventajas e inconvenientes y la problemática de la computación en la nube: **seguridad, protección de datos** y **privacidad.**

Estados Unidos ha publicado ya su estrategia federal para la adopción de *cloud computing;* la Unión Europea trabaja en una estrategia similar.

* La traducción al español se está haciendo de dos formas: "computación en nube" y "computación en la nube" o bien "informática en nube" o "informática en la nube". No hay unanimidad y en España y Latinoamérica se utilizan ambos indistintamente. Sí hay unanimidad al considerar el término en organizaciones y empresas y medios de comunicación para representar en términos simples el nuevo modelo.

España debe sumarse a ese esfuerzo, hacia una estrategia europea. Se revisan en este trabajo las principales *estrategias,* y se proponen ideas para la necesaria implantación de la adopción de la nube por organizaciones, empresas y administraciones públicas.

agenda digital, *cloud computing*, IaaS, PaaS, SaaS, privacidad, protección de datos, seguridad.

Cloud Computing is one of the technological terms (buzzwords) most repeated in social media. Companies and organizations are seeing this technology in solving many problems, especially economic but also technological infrastructure.

The adoption of the services cloud computing (SaaS, PaaS and IaaS) are growing rapidly and models of delivery or deployment of the cloud (private, public, hybrid and community) offered by an endless supply of providers are beginning to be common in the terminology of business strategies and research centers.

This article aims to analyze in addition to the above models is almost standard in the industry, their advantages and disadvantages with the problems brought about by cloud computing: security, data protection and privacy.

United States has already published a federal strategy for the adoption of cloud computing; the European Union works in a similar strategy. Spain needs to work in the same direction, framed in that future European strategy. We review the strategies of U.S. and EU, and propose some ideas for the necessary implementation of a strategy for cloud adoption by organizations and enterprises.

digital agenda , cloud computing, IaaS, PaaS, SaaS, privacy, data prtection, security

1. ¿CÓMO HA LLEGADO *CLOUD COMPUTING*?

Casi todas las grandes empresas del sector TIC (tecnologías de la información y comunicación) han lanzado estrategias de *cloud computing* para la década. De igual modo, las principales operadoras de telecomunicaciones e internet, que son *per se* empresas de la nube.

Otros sectores, mientras, migran gradualmente.

Entre 2008 y 2009, surgió el nuevo paradigma tecnológico de la Nube, con todas sus tecnologías asociadas que, al poco tiempo, despegó con su llegada al gran público. Dos grandes cabeceras económicas mundiales, *Business Week* y *The Economist, ya* preveían en 2008 el advenimiento de esta arquitectura, y analizaron con detalle la computación en nube y su impacto en las corporaciones[1].

Estamos ante un cambio disruptivo, al que los departamentos de TI han de enfrentarse. Los directivos deben considerar el modo de adquirir y distribuir información en este entorno, protegiendo al mismo tiempo los intereses de la compañía. Las empresas innovadoras deben tomar ventaja de estos nuevos recursos y reinventarse en sus mercados. Aquellas que no lo consigan se pueden quedar rápidamente desactualizadas y, tal vez, fuera del negocio.

Sin embargo, *la computación en nube nos traerá grandes interrogantes y algunos problemas en asuntos controvertidos, como la protección de datos y la privacidad de los usuarios.* Otra pregunta planteada por analistas sociales y tecnológicos es *si desaparecerá el ordenador tal como hoy lo conocemos. O si será sustituido por el teléfono móvil, tabletas electrónicas, o por otros dispositivos.*

1 JOYANES, Luis . *Icade,* nº 76, enero-abril, 2009, p.96

¿Morirá el PC?[2] ***¿Morirá la Web?***[3] ***¿Entramos en la era Post-PC?, como, entre otros, anunciaba el genial Steve Jobs***.

Los datos y aplicaciones se reparten en nubes de máquinas, cientos de miles de servidores de computadores pertenecientes a los gigantes de Internet. Poco a poco, se extiende a cientos de grandes empresas, universidades, administraciones, que desean tener sus propios centros de datos a disposición de sus empleados, investigadores o doctorandos[4]. Las nubes de servidores han favorecido que el correo electrónico pueda ser leído y archivado a distancia en servidores. también es posible subir y descargar fotografías y video , o escuchar música en '*audiostreaming*'. O, en la gestión *empresarial*, utilizar un programa de software de CRM (gestión de relaciones con los clientes), ambos servicios previo pago de una cuota.

Por último mencionar algunas de las innovaciones tecnológicas asociadas a la "Nube", que producirán transformaciones sociales, además del impredecible cambio tecnológico: la ***Web en tiempo real, la geolocalización, la realidad aumentada*** la llegada de la ***telefonía móvil LTE de cuarta generación (4G)***, las tecnologías inalámbricas , códigos **QR (Bidi), NFC, RFID,** sensores inalámbricos, los estándares USB, Buetooth e implantación de redes inalámbricas *Wifi* y *WiMax,* que están configurando la ***Internet de las cosas.***

2. DEFINICIÓN DE CLOUD COMPUTING

No sólo es una frase de moda un '*buzzword*'. es un término que representa un nuevo modelo de informática, tenido por muchos analistas por una innovación tan relevante como lo fue internet en su momento. Además, es el mejor sinónimo de la propia Web. *Cloud Computing* es la evolución de un conjunto de tecnologías que afectan al enfoque de las organizaciones y empresas en la construcción de sus infraestructuras de TI. Al igual que ha sucedido con la evolución de la Web, con la Web 2.0 y la Web Semántica, la computación en nube no incorpora nuevas tecnologías. Se han unido tecnologías potentes e innovadoras, para construir este nuevo modelo y arquitectura de la Web.

Reese plantea que, "si bien Internet es un fundamento necesario, la nube es algo más que Internet. Es aquel lugar donde utilizar tecnología cuando se necesita, mientras se necesite, ni un minuto más". No se instala nada en su escritorio, ni se paga por la tecnología cuando no se utiliza.

La nube puede ser infraestructura o software, es decir, puede ser una aplicación a la que se accede a través del escritorio y se ejecuta inmediatamente tras su descarga, o

2 GOMEZ, Lee y BULEY, Taylor (2009). "The PC is Dead" en *Forbes, 28* de diciembre de 2009

3 ANDERSON, Chris (2010). "The Web is dead. Long live the internet" en *Wired* (ediciones en USA, Gran Bretaña e Italia), Octubre 2010, Gran Bretaña, pp. 125-131.

4 *Op. Cit.,* pp. 95-111.

bien un servidor al que se invoca cuando se necesita. En la práctica, la informática en nube proporciona un servicio de *software* o *hardware.*

No existe una definición aceptada universalmente; sin embargo, existen organismos internacionales cuyos objetivos son la estandarización de Tecnologías de la Información y, en particular, de *Cloud Computing.* Uno de los organismos más reconocidos es el National Institute of Standards and Technology (**NIST**)[5] y su Information Technology Laboratory, que define la computación en nube (*cloud computing*)[6] como:

> "Un modelo que permite el acceso bajo demanda a través de la Red a un conjunto compartido de recursos de computación configurables (redes, servidores, almacenamiento, aplicaciones y servicios) que se pueden aprovisionar rápidamente con el mínimo esfuerzo de gestión o interacción del proveedor del servicio"

La nube es un conjunto de *hardware* y *software*, almacenamiento, servicios e interfaces que facilitan la entrada de la información como un servicio. El mundo de la nube tiene un gran número de actores o participantes. Los grupos de intereses del mundo de la computación en nube son: los *vendedores o proveedores:* proporcionan las aplicaciones y facilitan las tecnologías, infraestructura, plataformas y la información correspondiente; los *socios de los proveedores:* crean *servicios* para la nube, ofreciendo servicios a los clientes; los *líderes de negocios*: evalúan los servicios de la nube para implantarlos en sus organizaciones y empresas; los *usuarios finales* utilizan los servicios de la nube, gratuitamente o con una tarifa.

Los servicios de la nube deben ser distribuídos (*multi-tenancy*); es decir, empresas diferentes comparten los mismos recursos fundamentales. Por esta razón las empresas comienza a encontrar nuevos valores, facilitando la eliminación de las complejas restricciones que supone el entorno informático tradicional; incluyendo espacio, tiempo, energía y costes.

2.2. Características de *cloud computing*

El modelo de la nube, según NIST, se compone de cinco características esenciales, tres modelos de servicio y cuatro modelos de despliegue. Las características fundamentales son:

5 El NIST es una Agencia del Departamento de Comercio de los Estados Unidos. Dentro del NIST, el Computer Security Resource Center (CSRC) se encarga de los estándares de las Tecnologías de la Información y, en concreto, de Cloud Computing

6 En octubre de 2009, Peter Mell y Tim Grance, investigadores del NIST publicaron la norma (*draft*) de la definición de *cloud computing* y una guía del mismo, realizada en colaboración con la industria y el gobierno y titulada: "Effectively and Securely Using the Cloud Computing Paradigm" y que puede ser descargada en en el sitio oficial del NIST : http://crsc.nist.gov/groups/SN/cloud-computing/cloud-computing-v25.ppt

Autoservicio bajo demanda. Un consumidor puede proveerse unilateralmente de tiempo de servidor y almacenamiento en red, a medida que lo necesite; sin requerir interacción humana con el proveedor del servicio.

- **Acceso ubicuo a la Red**. Se realiza mediante mecanismos estándares, que promueven el uso por plataformas de clientes delgados (teléfonos móviles, computadoras portátiles, PDAs, tabletas).
- **Distribución de recursos independientes de la posición**. Los recursos de computación del proveedor son agrupados *("pooled")* para servir a múltiples consumidores utilizando un modelo multi-distribuido ("*multitenant*") con diferentes recursos físicos y virtuales asignados y reasignados dinámicamente conforme a la demanda del consumidor. Existe una sensación de independencia de la posición, de modo que el cliente, normalmente, no tiene control ni conocimiento sobre la posición exacta de los recursos proporcionados. Pero podría especificarla a un nivel más alto de abstracción (país, región geográfica o centro de datos). Ejemplos de recursos incluyen almacenamiento, procesamiento, memoria, ancho de banda de la red y máquinas virtuales.
- **Elasticidad rápida**. Las funcionalidades ("*capabilities")* se pueden proporcionar de modo rápido y elástico, en algunos casos automáticamente. Sus características de aprovisionamiento dan la sensación de ser ilimitadas y pueden adquirirse en cualquier cantidad o momento.
- **Servicio medido**. Los sistemas de computación en la nube controlan y optimizan automáticamente el uso de recursos, potenciando la capacidad de medición en un nivel de abstracción apropiado al tipo de servicio (almacenamiento, procesamiento, ancho de banda y cuentas activas de usuario). El uso de recursos puede ser monitorizado, controlado e informado, proporcionando transparencia para el proveedor y para el consumidor.

3. MODELOS DE LA NUBE

El NIST clasifica los modelos de la computación en nube en dos grandes categorías:

- **Modelos de despliegue.** Se refieren a la posición (localización) y administración (gestión) de la infraestructura de la nube (Pública, Privada, Comunitaria, Híbrida)
- **Modelos de servicio.** Se refieren a los servicios específicos a los que se puede acceder en una plataforma de *computación en la nube* (Software, Plataforma e Infraestructura como Servicios).

Estas tecnologías ofrecen tres *modelos de servicios:*

1. ***Software***. Al usuario se le ofrece la capacidad de que las aplicaciones suministradas se desenvuelvan en una infraestructura de la *nube,* siendo las aplicaciones accesibles a través de un navegador web, como en el correo electrónico Web. Posiblemente, este es el ejemplo más representativo, por lo extendido, de este modelo de servicio. El usuario carece de cualquier control sobre la infraestructura o sobre las propias aplicaciones, excepción hecha de las posibles configuraciones de usuario o personalizaciones que se le permitan.

2. ***Plataforma***. Al usuario se le permite desplegar aplicaciones propias (adquiridas o desarrolladas por el propio usuario) en la infraestructura de la *nube* de su proveedor, que ofrece la plataforma de desarrollo y las herramientas de programación. En este caso, el usuario mantiene el control de la aplicación, aunque no de toda la infraestructura subyacente.

3. ***Infraestructura***. El proveedor ofrece recursos como capacidad de procesamiento, de almacenamiento o comunicaciones, que el usuario puede utilizar para ejecutar cualquier *software;* desde sistemas operativos hasta aplicaciones.

Los modelos de despliegue de las infraestructuras y servicios de la nube se clasifican en las siguientes categorías:

1. ***Nube* privada**. Los servicios no son ofrecidos al público en general. La infraestructura es íntegramente gestionada por una organización.

2. ***Nube* pública**. La infraestructura es operada por un proveedor que ofrece servicios al público en general.

3. ***Nube* híbrida**. Resultado de la combinación de dos o más *nubes* individuales que pueden ser privadas, compartidas o públicas. Permite enviar datos o aplicaciones entre ellas.

4. ***Nube* comunitaria** (*communiy*). Ha sido organizada para servir a una función o propósito común. Es preciso compartir objetivos comunes (misión, políticas, seguridad). Puede ser administrada bien por las organizaciones constituyentes, bien por terceras partes. Este modelo es el definido por el NIST, aunque la mayoría de organizaciones, proveedores y usuarios de la nube aceptan los tres modelos de despliegue: pública, privada e híbrida

5. MODELO DE NEGOCIOS EN LA NUBE

Está totalmente enfocado hacia las características clave de la computación en nube, realizado para potenciar sus conceptos (tecnologías y modelos de ingresos). Los modelos de negocios se pueden aplicar por igual a proveedores y consumidores de la nube. El

de proveedores se basa en el desarrollo de tecnologías y soluciones facilitadoras de la nube; incluye las siguientes soluciones[7]:

- *Los servicios de la nube* proporcionan la red e infraestructuras de computación mediante plataformas y soluciones. Los proveedores de servicios y soluciones de la nube son similares, y permiten desarrollar y proporcionar servicios y soluciones de la nube desde la perspectiva de los consumidores. Los proveedores de servicios de la nube incluyen organizaciones que operan con centros de datos propios y apoyados en servicios de virtualización. Los proveedores son variados y tienen gran implantación, aprovechando sus centros de datos y de su experiencia en alojamiento de datos y aplicaciones.
- *Proveedor de servicios de plataformas de la nube.* Proporcionan plataformas basadas en la nube, hospedados en entornos de sistemas e infraestructuras específicos, para que los desarrolladores puedan acceder a la plataforma, desarrollar una nueva aplicación de negocios y alojarlas en la plataforma basada en la nube.
- *Proveedores de tecnologías.* Desarrollan las herramientas y tecnologías que facilitan que la nube se establezca y se proporcione a los consumidores de recursos proporcionados por la nube. Ofrecen un amplio rango de herramientas, tecnologías, sistemas operativos para facilitar el despliegue de nubes públicas, privadas, híbridas y comunitarias.
- *Proveedores de soluciones.* Desarrollan aplicaciones o *suites* completas, para conseguir un amplio mercado de consumidores de la nube (otras operadoras de telefonía e internet)
- *Modelos de negocio para consumidores. Estas* empresas aplican conceptos de la nube a sus estrategias de negocios.

  Ofrecen soluciones para gestión empresarial.

5. LA NUBE MÓVIL: PRESENTE Y FUTURO

La computación en la nube móvil (o la nube móvil(se refiere a un modelo de procesamiento que se realiza en la nube. Los datos se guardan en la nube y el acceso se realiza mediante un dispositivo móvil que actúa como terminal de presentación o pantalla. Aunque el dispositivo móvil puede ser muy variado, suele referirse al teléfono inteligente (Smartphone). La facilidad de transporte y el tamaño de las tabletas ha hecho que sean estos dos terminales los más considerados al hablar de la nube móvil.

7 Eric A. Marks, Bob Lozano. Executive´s Guide to Cloud Computing. New Jersey : Wiley, 2010. (pp.82-83).

La nube móvil requiere una conexión fiable a la mayor velocidad de acceso posible y un buen ancho de banda (al menos teléfonos de generación 3G tales con protocolos HSDPA, HSUPA o HSPA+ o de cuarta generación, 4G, LT), un dispositivo móvil con acceso a Internet) y un navegador adaptado al dispositivo. Los servicios en la nube móvil experimentarán un enorme crecimiento en los próximos años.

Evidentemente, se enfrenta a grandes retos y oportunidades en el corto plazo. Las redes 3G y las ya inminentes 4G no tienen capacidad infinita. Además de la saturación, las operadores de telefonía y proveedores de contenidos se enfrentan a una necesaria y creciente especialización, y a la generación de nuevas líneas de negocio por la necesidad ineludible de implantar innovaciones tecnológicas eficientes y rentables.

Actualmente, es asunto clave en la nube móvil la sincronización[8], que permite a los usuarios enviar mensajes, realizar llamadas, acceder a todo tipo de contenidos con múltiples dispositivos y plataformas. Los servicios de música en streaming o de almacenamiento en la nube, y ya realizan estas tareas de sincronización. No solo con dispositivos, sino incluso con redes sociales.

El servicio de sincronización que ha revolucionado el mercado , llevando el consumo al gran público, es la plataforma *iCloud* de Apple. Aquí, puede subirse cualquier dato a la nube desde un dispositivo. Automáticamente, la nube lo sincroniza y lo pone al alcance de todos los dispositivos de la familia Apple, lo que hasta ahora no era posible en abierto. Otro ejemplo son los populares servicios de mensajería instantánea para móviles, que permiten enviar texto, fotografías, vídeos, audio…y que funcionan desde cualquier dispositivo o sistema operativo móvil.

En resumen, se trata de integrar la computación en la nube con la computación móvil en un nuevo término conocido como la nube móvil. La inteligencia de las computadoras, las aplicaciones y los datos están en la nube. Antes, sólo se guardaban en el disco duro de cada ordenador personal.

Gran parte del futuro empresarial pasa por la nube móvil.

6. LA SEGURIDAD: ¿UNA DEBILIDAD DE LA NUBE?

En una primera impresión, la abstracción del hardware que trae consigo la nube da la sensación de que el nivel de seguridad es inferior al de los modelos tradicionales. En algunos modelos de la nube, se pierde el control de seguridad sobre dichos servicios. Sin embargo, si las políticas de seguridad del proveedor están bien definidas, y el cliente las ejecuta fielmente, trabajar en la nube supondrá una mejora en la seguridad

8 Son numerosas las señales que apuestan a la sincronización como una de las características ya decisivas en la nube. Citemos un caso concreto. HTC, uno de los grandes fabricantes de teléfonos celulares y tabletas, compró en agosto de 2011, la compañía Dashwire, conocida por su plataforma de sincronización Dashworks, con la finalidad evidente de potenciar sus servicios de sincronización

El usuario no sabe exactamente dónde está almacenada la información, mientras que en la computación tradicional sí. Trasladar toda la información a la nube significa *"confiar la seguridad a terceros", lo que puede ser motivo de* preocupación. Así, se plantean preguntas clave en la estrategia de seguridad en la nube:

- ¿dónde estarán desplegados los datos?
- ¿con qué protección?
- ¿quién es responsable de ellos?

Los grandes proveedores tienen respuesta clara para la tercera pregunta: el responsable de los datos es el cliente. IBM llama a este tipo de seguridad "*Secure by design*" (seguridad personalizada). El concepto pretende que el entorno sea el resultado de la interacción entre proveedor y receptor de servicios.

La seguridad tiene que partir del cliente. Cuando una empresa quiere llevar sus datos a la nube, debe especificar sus preferencias. Conociéndolas, el proveedor diseña un servicio específico para la empresa.

Una de las críticas más negativas a La Nube es la relativa a la seguridad y el control de los datos. Aparentemente, las Organizaciones tienen un control más rígido sobre los datos almacenados en su propia infraestructura que si los traslada a la nube. Por otro lado, es necesario considerar los requerimientos legales. La nube puede ser incluso más segura que un centro de datos tradicional, si bien el método de reforzar la seguridad de la información si es radicalmente distinto.

La computación en nube tiene características específicas que requieren evaluación de los riesgos en áreas como integridad, recuperación y privacidad de los datos, así como en asuntos legales en áreas como normativa de regulación y Auditoría de los Sistemas de Seguridad de la Información.

La evaluación de riesgos y la revisión de la seguridad en la nube deben considerar en primer lugar las opciones de despliegue de la nube (pública, privada e híbrida) y modelos de entrega de servicios (SaaS, PaaS, IaaS). Estrechamente relacionados con los modelos anteriores, están los procesos relacionados con la virtualización y almacenamiento en los centros de datos. Como sucede en el Plan General de Seguridad de la Información, ninguna lista de controles de seguridad podrá cubrir todas las circunstancias, pero se deberá adoptar un enfoque basado en riesgos para moverse o migrar a la nube y seleccionar las opciones de seguridad. Los activos de despliegue en la nube se agrupan en dos grandes bloques: los datos y las aplicaciones.

7. OBJETIVOS DE LA SEGURIDAD DE LA INFORMACIÓN EN LA NUBE

El desarrollo del software seguro se basa en la aplicación de principios de diseño de software seguro que forman los principios fundamentales del aseguramien-

to del software. El aseguramiento del software se define[9] como: "los fundamentos que permiten tener confianza justificada de que el software debe tener todas las propiedades requeridas para asegurar que, cuando se ejecute, deberá operar de modo fiable, aun con fallos intencionales. Esto significa que debe ser capaz de resistir tantos ataques como sea posible, contener los daños y recuperar un nivel de ejecución normal.

Los principios que soportan el aseguramiento de los sistemas de información en la nube son similares a los establecidos para las Tecnologías de la Información, pero con las características de la Nube. Se consideran los siguientes: **confidencialidad, integridad** y **disponibilidad** (la Triada de la Seguridad); los principios complementarios son: autenticación, autorización, auditoría, responsabilidad (*accountability*) y privacidad.

7.1. Confidencialidad

Se refiere a la prevención de divulgación (revelación), intencionada o no, de información no autorizada.

La pérdida de la confidencialidad se puede producir de muchas formas. Algunos elementos de telecomunicaciones utilizados para garantizarla son:

- Protocolos de seguridad de redes
- Verificación de claves
- Cifrado (encriptación) de datos

En la nube, confidencialidad es la protección de datos durante la transferencia entre entidades. Una política de confidencialidad define los requisitos para asegurarla, previniendo la divulgación no autorizada de la información. Se debe especificar qué información o datos se pueden intercambiar. Los temas relacionados con la confidencialidad incluyen: derechos de propiedad intelectual, control de acceso, cifrado, inferencia, anonimato y canales de cobertura y análisis de tráfico.

7.2. Integridad

Es la garantía de que el mensaje enviado es recibido, de que no ha sido alterado. Esta integridad de los datos se debe garantizar en el tránsito y almacenamiento. También deben especificarse los medios de recuperación , a partir de errores detectados (borrados, inserciones o modificaciones). Estos incluyen políticas de control de acceso, quién puede transmitir y recibir datos, y qué información puede ser intercambiada.

Asimismo, es muy importante asegurar la integridad de sus datos. La confidencialidad no implica integridad, los datos pueden ser cifrados con propósitos de confidencialidad, pero el usuario puede carecer de un mecanismo para verificar su integridad. El cifrado

9 Software Security Assurance Report

sólo es suficiente para la confidencialidad. La integridad precisa también el uso de códigos de mensajes de autenticación.

El aspecto de la integridad de los datos es especialmente significativo en aplicaciones de almacenamiento en modelos IaaS.

Por otra parte, existen costes asociados a las transferencias cuando se mueven los datos hacia o desde la nube, así como la utilización de las redes, esencialmente los anchos de banda. El cliente querrá verificar que los datos permanecen en la nube, sin tener que descargar y volver a subirlos.

7.3. Disponibilidad

Cuando se ha conseguido mantener la confidencialidad y la integridad, se debe asegurar la disponibilidad de sus datos. La *disponibilidad* asegura el acceso fiable y a tiempo por el personal apropiado. Garantiza que los sistemas funcionen adecuadamente.

En definitiva, la disponibilidad alude a los elementos que crean fiabilidad y estabilidad en redes y sistemas. Asegura que la conectividad es accesible cuando se necesita y permite a los usuarios autorizados acceder a la red o sistemas.

Las amenazas a la disponibilidad incluyen intentos maliciosos para controlar, destruir o dañar recursos de computación y denegar acceso legítimo al sistema.

Una primera amenaza son los ataques en la red, como la denegación de servicio DoD (Denial-of-service) Otra es la propia disponibilidad del proveedor de servicios. Ningún proveedor garantiza la disponibilidad completa.

Los requisitos de disponibilidad deben garantizar que los recursos de computación estén disponibles, a los usuarios autorizados, cuando sean necesarios.

Los términos opuestos a confidencialidad, integridad y disponibilidad son la divulgación (revelación), alteración y destrucción.

Una tarea difícil de evaluar en disponibilidad es asegurar que los proveedores de almacenamiento en la nube permanecerán en el sector en el futuro; es un factor difícil de medir, por lo que debemos recurrir a proveedores solventes.

Consideraciones prácticas

Estos tres principios deben quedar reflejados en el contrato de servicios (SLA). Los acuerdos a nivel de servicios han evolucionado desde posiciones débiles. Pero consideramos que los grandes proveedores garantizarán el cumplimiento de cada SLA.

8. LA SEGURIDAD COMO SERVICIO (SecaaS)

La organización Cloud Security Alliance (CSA) publicó en 2011 un informe anunciando un grupo de trabajo denominado "Consejo de Seguridad como Servicio". Además, definía las categorías de seguridad consideradas servicios. Su propósito es identificar las definiciones de la Seguridad como Servicio y sus medios, para clasificar los diferentes tipos de seguridad como servicios y orientar a las organizaciones en la ejecución de buenas prácticas.

CSA clasifica los servicios de seguridad en las siguientes categorías:

- Gestión de identidades y acceso
- Prevención de perdida de datos
- Seguridad en la Web
- Seguridad para el correo electrónico
- Evaluación de la seguridad
- Gestión de intrusiones
- Seguridad de la información y gestión de eventos
- Cifrado
- Continuidad del negocio y recuperación de desastres
- Red de seguridad

9. PROTECCIÓN DE DATOS EN LA NUBE

En la Unión Europea, la Directiva 1995/46/EC[10], dedicada a la ***protección de datos***,https://www.privacyinternational.org/article/privacidad-y-proteccion-de-datos-en-la-uni%C3%B3n-europea - _ftn12 define los fundamentos de la protección de datos personales que los Estados Miembros de la UE deben trasladar a su legislación. Las disposiciones de la Directiva pueden ser invocadas en los tribunales nacionales contra las normas de protección de datos de los Estados Miembros, y derogar las normas que incumplan las directivas. En España, los organismos que protegen los datos personales y la privacidad son la Agencia Española de Protección de Datos y el Instituto INTECO.

10 Portal de síntesis de la legislación de la Unión Europea: http://europa.eu/legislation_summaries/information_society/data_protection/l14012_es.htm

Según la guía para empresas de Inteco[11]: "*El ciclo de vida de los datos procesados en la nube es el siguiente:*

- ***Los datos son preparados para adaptarse a la nube, cambiando** su formato o creando un fichero con toda la información necesaria.*

- ***Los datos "viajan" a la nube a través de una conexión a Internet,** mediante un correo electrónico, una aplicación específica o transfiriendo a la nube la copia de seguridad.*

- ***Los datos son procesados en la nube,** desde su almacenamiento hasta el cálculo de complejas operaciones matemáticas. Pueden almacenarse en copias de seguridad en la nube para facilitar futuros accesos.*

- ***Los datos finales "viajan" de vuelta al usuario.** Una vez terminado el procesamiento, deben volver al usuario con el valor añadido de la información generada en la nube. Al abandonar la organización, los datos pueden constituir un riesgo para la privacidad: Cualquier malintencionado podría interceptarlos mientras son transferidos. En todo caso, son almacenados y procesados en una infraestructura informática ajena al control del usuario".*

Los mecanismos para minimizar estos riesgos de privacidad son muy sencillos. Antes de migrar los datos a la nube, conviene preguntarse: "Es necesario que todos los datos de la organización pasen a la nube?". La guía Inteco menciona el caso de una empresa encargada de tramitar nóminas que decide utilizar servicios en la nube. Esta empresa tiene bases de datos de miles de trabajadores con información personal. Inteco recomienda no transferir datos sensibles a la nube, recomendando claves con correspondencia real en archivos depositados en servidores de la empresa.

La protección de datos y la privacidad son clave para operar en la nube. Las leyes, nacionales e internacionales, deben primar sobre cualquier otra consideración en los tratos acordados con los proveedores. Dado que la protección de datos está recogida en casi todas las legislaciones occidentales, nos centraremos en los problemas que plantea la privacidad en el uso de la nube y la necesidad de regularla; así como en las políticas imperantes.

11 Observatorio de la Seguridad de la Información, *Guía para empresas: seguridad y privacidad del cloud computing"*. León (España): INTECO. 2011.(observatorio.inteco.es; www.inteco.es). INTECO es el Instituto español de las Tecnologías de las Comunicaciones con sede en León y entre cuyos objetivos fundamentales es velar y ayudar a empresas, fundamentalmente PYMES, en sus políticas de seguridad y su implementación

10 PRIVACIDAD E IMPACTO EN LA NUBE

Un área muy afectada por la computación en nube es la privacidad (intimidad en español). La mayoría de los legisladores, también los distribuidores de soluciones de la nube, proporcionan normas para su protección. El impacto es tal, que un posible robo de identidad de la empresa puede producir no sólo la pérdida de la privacidad de la organización, sino un gran daño en su imagen y reputación. A corto plazo puede afectar a los resultados económicos; pero, a la larga, puede producir pérdidas de credibilidad, confianza y publicidad negativa.

En muchas ocasiones, la responsabilidad de controles de privacidad corresponde al departamento de TI. Pero son las unidades de negocio las que deben velar por su protección. Se debe estandarizar los procesos aplicados a la computación en nube, y o incumplimientos de la privacidad de la organización y de sus empleados.

El concepto privacidad –intimidad- varía entre países, culturas y jurisdicciones.

La privacidad[12] se define como Información de identificación personal (PII, Personally Identificable Information) y se refiere a la recopilación, uso, divulgación, almacenamiento y destrucción de datos personales. Se vincula al cumplimiento de la normativa legal y a la transparencia en el empleo de los datos personales. No existe consenso acerca de qué constituyen los datos personales. Consideraremos las definiciones de organismos internacionales relevantes.

La Organización para la Cooperación y Desarrollo Económico, OCDE define la privacidad como: Cualquier información relativa a un individuo identificable o identificado (relativo a datos); una persona identificable es aquella que puede ser identificada, directa o indirectamente, en particular por referencia a un número de identificación o uno o más factores específicos a su identidad física, psicológica, mental, económica, cultural o social"[13].

Existen opiniones divergentes sobre los responsables de la seguridad y privacidad. Suele asignarse a los proveedores de los servicios de la nube la responsabilidad mediante acuerdos contractuales como los de nivel de servicio (SLA); sin embargo, la empresa responsable de los datos no puede transferir su responsabilidad. A efectos jurídicos, los responsables de fallos en la seguridad cae en la organización propietaria o gestora de los datos. Esta situación se produce incluso si el usuario carece de capacidad técnica para asegurar los requisitos contractuales con el proveedor de servicios de la nube.

12 La Real Academia Española, , define privacidad como. ". Ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión" (www.rae.es).

13 www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00

La experiencia ha demostrado que los fallos en la seguridad y privacidad de los datos tienen un efecto en cascada[14]. Cuando una organización pierde el control de la información personal de los usuarios, éstos son los responsables (directa o indirectamente) de los daños posteriores. Se producen diferentes efectos: robo de identidad, invasión de la privacidad o solicitación no deseada.

Continuamente, aparecen nuevos y desconocidos riesgos. Por tanto, la protección de la privacidad es muy compleja en la nube y se enfrenta a grandes retos, si bien la privacidad puede ser protegida con igual o mayor garantía en los datos y aplicaciones alojados en la nube.

11. PRINCIPIOS DE PRIVACIDAD DE LA UNIÓN EUROPEA

La Unión Europea es una de las organizaciones internacionales más preocupadas por la protección de la privacidad en Internet. Por esta razón, ha definido principios protectores del individuo, que se encuentran entre los más avanzados del mundo. Una transferencia de información, desde la UE hacia otro país, queda anulada si se comprueba que no existen protecciones personales equivalentes en el receptor. Los principios de privacidad más sobresalientes de la unión Europea son los siguientes[15]:

- Los datos deben ser recopilados o coleccionados de acuerdo con las leyes
- La información recogida sobre una persona no puede ser divulgada a otras organizaciones o personas, a menos que sea autorizada por la ley o por consentimiento expreso del interesado.
- Los registros de datos personales deben ser precisos y actualizados
- Las personas tienen derecho a corregir los errores contenidos en sus datos
- Los datos deben ser utilizados sólo para los propósitos con los que fueron coleccionados y se deben utilizar solo por un periodo razonable de tiempo.
- Las personas tienen derecho a recibir un informe sobre la información que se tiene sobre ellas.
- La transmisión de información personal a lugares donde no se pueda asegurar una protección de datos equivalente a la existente en la UE se debe prohibir.

Las políticas de privacidad están enmarcadas dentro de la Directiva de la Unión Europea (EU Directive 95/46/EC) que regula la protección de las personas respecto

14 *Ibid,* p. 150

15 En el sitio Web oficial de la unión Europea http://europa.eu/index_es.htm podrá consultar las políticas de protección de datos y privacidad vigentes. Si quiere acceder a información legal le recomendamos utilice el buscador EUR-Lex en http://eur-lex.europa.eu/RECH_menu.do?ihmlang=es

al procesamiento de datos personales y al movimiento libre de tales datos (Directiva EU). Una proposición clave de la directiva de la UE es la restricción en la transferencia de datos personales fuera de la Unión Europea (o auqellos designados por la Unión Europea como países con estándares de protección de datos similares). El objetivo del regulador es prevenir a las organizaciones de que contravienen las reglas de privacidad transfiriendo datos a lugares donde no estén protegidos legalmente. Por esta razón, las organizaciones deben considerar las soluciones de la computación en nube con sumo cuidado, preocupándose de conocer previamente a la firma del contrato si los países donde van a residir sus datos están avalados por la Unión Europea y tienen leyes parecidas.

La directiva de la UE, cuyas actualizaciones se reflejan en el calendario de la Agenda Digital Europea, contiene diferentes principios para permitir la transferencia de datos; destacamos los siguientes:

- El interesado ha dado su consentimiento sin ambigüedad a la transferencia propuesta
- La transferencia es necesaria para el desempeño de un contrato entre el interesado y el controlador o la implementación de medidas precontractuales tomadas en función de la respuesta del interesado.
- La transferencia es necesaria para la conclusión o desempeño de un contrato concluido, según las necesidades del interesado, entre el controlador y una tercera parte.
- La transferencia es necesaria o se requiere legalmente en interés público o para el establecimiento, ejercicio o defensa de reclamaciones legales.
- La transferencia es necesaria para proteger los intereses vitales del interesado.

12. RIESGOS Y AMENAZAS EN CLOUD COMPUTING

La publicación del NIST (*National Institute of Standards and Technologies*) «*Guidelines on Security and Privacy in Public Cloud Computing*» pone de manifiesto, además de la actualidad de este nuevo modelo para la distribución de servicios y aplicaciones, la necesidad de difundir buenas prácticas de seguridad. Este no es el único documento que refleja la creciente preocupación por la seguridad en estas plataformas, como se refleja en informes de otras entidades de referencia.

El informe "*Riesgos y amenazas en el Cloud Computing*" realizado por INTECO[16] resume algunos de estos documentos con el propósito de facilitar una visión general

16 INTECO www.inteco.es. Este informe de INTECO se preparó en base a la publicación de ENISA (Agencia Europea de Seguridad) **Seguridad y resistencia en las nubes de la Administración Pública.** ENISA: www.enisa.europa.eu/

de amenazas, riesgos y aspectos claves en la seguridad en *cloud*. Este informe describe las infraestructuras y servicios *cloud*, analizando los distintos elementos que han de tenerse en cuenta para su seguridad, según los criterios y estándares internacionales. Las preocupaciones que derivan de estos informes se centran en la **gestión de los datos**, fundamentalmente en su propiedad y forma de operarlos y tratarlos. Con el análisis realizado en este informe, se obtiene una visión global de esta problemática y se extraen conclusiones comunes a todos los puntos de vista.

La **seguridad y la propiedad de los datos** es uno de los aspectos clave. Los informes muestran una gran preocupación por la propiedad y el tratamiento de los datos dado que estas infraestructuras pueden gestionarlos en múltiples países lo que puede generar conflictos en cuanto al marco legal en el que son tratados. También se plantea que estos entornos, al manejar gran cantidad de datos, pueden ser objeto de fugas de información, ya sean intencionadas o fortuitas.

El **cumplimiento normativo** también es uno de los pilares de la seguridad en entornos *cloud.* En este caso, el problema se presenta debido a la falta de transparencia de estas infraestructuras, por lo que es recomendable que el suscriptor del servicio se informe claramente de cómo se gestiona el entorno.

Para la creación de un servicio *cloud,* interviene una multitud de softwares de distintos proveedores. Al ser **entornos complejos, hay que vigilar** las posibles vulnerabilidades del mismo e implantar procedimientos de parcheado. Otro de los aspectos considerados importantes es la **identidad y el control de acceso**. Por lo general, la mayoría de las infraestructuras son compartidas por múltiples empresas o usuarios y su mala definición puede provocar accesos no autorizados a datos confidenciales. La definición de una buena política de identidad y control de acceso, basado en el mínimo privilegio, es esencial en entornos *cloud*.

Por último, los **contratos de acuerdo de servicio (SLA) son aquí un denominador común**. Todas las recomendaciones indican que deben ser revisados y creados específicamente, detallando los controles, normativas, medidas de protección, plazos de recuperación del servicio. ENISA, la agencia de seguridad de la Unión Europea, ha publicado recientemente una normativa específica para contratos en la nube.

13. EL *CLOUD COMPUTING* EN LA CASA BLANCA

El portal tecnológico *ReadWriteWeb*[17] publicó un informe sobre la iniciativa la *Casa Blanca* apoyando al *Cloud Computing*. Vivek Kundra, asesor tecnológico de Barak Obama, presentó ante el Congreso, en julio de 2010, el *cloud computing* como algo esencial en la infraestructura tecnológica del Gobierno.

17 *ReadWriteWeb.com*, 05/07/2010

Kundra insistió en cuatro puntos:

- La computación gubernamental está desfasada
- Los centros de datos federados ya suman más de 1.000. El mercado privado ahorra usando plataformas de *cloud computing* privadas, híbridas y servicios públicos.
- Los servicios de *cloud computing* mediante datos pueden ayudar a impulsar las políticas. Se requiere la interacción entre electores y participantes en agencias federales. La interoperabilidad entre agencias y plataformas requiere los servicios de *cloud computing* con conjuntos básicos de estándares.
- La transparencia es la capacidad de poder tener acceso a datos públicos a tiempo real.

El *cloud computing* permitirá interactuar con el gobierno federal usando los datos para generar ideas y transformar el debate sobre cuestiones de política pública. El servicio **data.gov,** basado en la nube, es un claro ejemplo. Otro servicio importante en la nube es **usaspeding.gov,** que busca la máxima transparencia.

13.1. Estrategia de *cloud computing* de la Casa Blanca

En 2011, lanzó su estrategia federal de Cloud Computing, guía para la adopción de este modelo tecnológico en las dependencias federales. El documento[18], coordinado por Kundra, define el concepto *cloud computing,* y el impacto en ahorro y niveles de servicio que producirá en la administración federal.

Es el resultado de las políticas puestas en marcha, desde 2010, orientadas a facilitar la migración de servicios en la administración norteamericana hacia la nube.

El Gobierno estadounidense exigirá a las agencias federales que utilicen servicios en la nube cuando exista una solución segura, factible y económicamente ventajosa. La estrategia indica que cada Agencia deberá ajustar sus presupuestos a la incorporación de la nube, revaluando todos los procesos que resulten ineficientes.

La estrategia señala que el Cloud Computing entrega beneficios intangibles a los ciudadanos, como: "visualizar el consumo de electricidad *online, con la* autorregulación del consumo privado; historiales médicos compartidos en diversos lugares y por distintas especialidades, etc.

18 El documento se puede descargar en: www.cio.com/documents/Federal-Cloud-Computing-Strategy.pdf

13.2. Iniciativa Federal de *Cloud Computing*

En mayo de 2011 , se publicó la Iniciativa Federal de Cloud Computing (FCCI). Como consecuencia, el Gobierno convocó una licitación *pública* para proveerse de servicios en la nube. La licitación afectaba a diferentes servicios:

- **EaaS** (email como servicio)
- Automatización de oficinas (software de ofimática)
- Servicios de almacenamiento en la nube (discos duros virtuales)
- Servicios profesionales

Considerando el despliegue de la nube, la licitación señala que los servicios se deben ofrecer en tres modalidades: nube privada del Gobierno Federal (Government Community Cloud), nubes privadas y públicas.

13.3. consideraciones prácticas para potenciar *cloud computing* en Estados Unidos

Vivek Kundra declaró[19], en 2011, que la migración de los servicios federales reducirá los gastos en computación del orden de miles de millones de dólares.

El Gobierno Federal es el comprador más grande de tecnologías de la información del mundo – gasta más de 80.000 millones de dólares al año – y planea cerrar el 40 por ciento de los centros de datos -800 de de 2000- en los próximos cuatro años para reducir el presupuesto de tecnología y modernizar el modo en que se utilizan los computadores para gestionar datos y proporcionar servicios a los ciudadanos. Según Kundra, la reducción de los centros de datos forma parte de una amplia estrategia para afrontar la computación en la era Internet; el gobierno se desplaza hacia la nube, donde los usuarios utilizan aplicaciones remotas como el correo electrónico. Estos servicios en la nube pueden ser proporcionados al gobierno por agencias o empresas tecnológicas externas. Aquí, el gobierno puede ahorrar 5.000 millones de dólares anuales al reducir la necesidad de compras de hardware y software por las agencias gubernamentales. El ahorro de costes por el cierre previsto de centros de datos se estima en 3,000 millones de dólares al año;

Como muestra de ese viraje hacia la nube, casi 140.000 empleados federales se han movido al correo electrónico basado en la nube, ahorrando unos 42 millones de dólares anuales.

19 Steve Lohr en entrevista publicada en el New York Times el 20 de junio de 2011. http://www.nytimes.com/2011/07/20/technology/us-to-close-800-computer-data-centers.html [consultado el 20-07-2011].

14. LA ESTRATEGIA DE *CLOUD COMPUTING* DE LA UNIÓN EUROPEA

La UE aprobó, en 2010, la Agenda Digital Europea[20]. Una de las tendencias estratégicas contempladas era *Cloud Computing*.

En la Declaración de Granada, se reconoce a *Cloud Computing* como un sector estratégico, donde Europa tiene un gran potencial de mercado. Hay una tendencia creciente en el empleo de *cloud computing*. La Comisión Europea estima que, en 2014, los servicios de la nube generarán ingresos de casi 35.000 millones de euros.

Tras varios anuncios oficiales, se realizó en Bruselas, en 2011, una consulta para recabar información con vistas al desarrollo de una estrategia europea de *cloud computing*. La idea de la comisaria Kroes era "involucrar a los principales usuarios, para un movimiento coordinado de estandarización que soporte la interoperabilidad y portabilidad de los datos".

El *cloud computing* constituye una importante oportunidad para la Administración Pública, ha manifestado Kroes reiteradamente.

ENISA, siguiendo con los planes para el lanzamiento de la estrategia europea de la nube, anunció en una nota de prensa el 2 de abril de 2012, la Guía para la supervisión de los contratos de computación en la nube, mediante un mejor conocimiento de los criterios de seguridad en los contratos de servicios.

15. CONSIDERACIONES PARA UNA ESTRATEGIA ESPAÑOLA DE CLOUD COMPUTING

La Agenda Digital Española, alineada con la estrategia de la UE, establecerá los objetivos, líneas de trabajo y medidas para impulsar el desarrollo de la Sociedad de la Información durante la legislatura. El Ministerio de Industria ha constituido un Grupo de Expertos de Alto Nivel para la Agenda Digital, cuya primera reunión se celebró en mayo de 2012. Debe proponer y tutelar las medidas para desarrollar la estrategia del Gobierno en telecomunicaciones y Sociedad de la Información, la Agenda Digital Española.

España partirá de unos objetivos generales, desarrollando cada uno en líneas de actuación prioritarias, plasmadas en medidas concretas. Según los últimos comunicados

20 La Agenda Digital Europea se publicó como conclusión de la Declaración de Granada en la reunión de ministros responsables de la Sociedad de la Información celebrada los días 18 y 19 de abril de 2010 en Granada. Esta agenda fue aprobada con posterioridad.

emitidos por Industria, las líneas de actuación prioritarios serán *smart cities* (ciudades inteligentes) y comercio electrónico.

Al igual que en la UE, proponemos que se contemple también una estrategia española para la computación en la nube, incorporando las directivas emanadas de la estrategia europea.

16. EL FUTURO CAMINARÁ POR LA NUBE

Los tres eventos anuales de relevancia mundial (Feria CES de Las Vegas, World Mobile Congress en Barcelona y CeBIT, feria de computación de Hannnover) marcan las tendencias a seguir por organizaciones y empresas, y predicen los cambios sociales y tecnológicos que se avecinan. 2012 no ha sido una excepción. Los tres eventos se han centrado en la nube como arquitectura tecnológica dominante. De igual forma, prestigiosos informes confirman la tendencia: *cloud computing* como aglutinador de los negocios, la industria, los medios de comunicación…

Asimismo, a la nube se incorporan servicios ofrecidos por grandes empresas, además de las PYMES, su hábitat natural.

La nube de servicios y datos será utilizada por organizaciones y empresas y consumidores particulares como medio para reducir los costes de infraestructuras y mantenimiento, al trasladar parte de su hardware y software a la nube. El almacenamiento físico dejará de estar, poco a poco, en unidades privadas, pasando también a la nube.

Por otra parte, la mejora de la escalabilidad (extensión de las necesidades tecnológicas de las empresas sin pérdida de calidad), unida a la popularización de los servicios de la nube, y el uso de aplicaciones móviles y medios sociales, conducirán gradualmente hacia la plena migración.

Los tres servicios más conocidos de la nube, IaaS, PaaS y SaaS, serán ofrecidos por multitud de proveedores, que facilitarán la toma de decisiones.

Queremos destacar el cambio de mentalidad que se producirá con el almacenamiento en la nube; sitios como iCloud, Amazon Drive, Dropbox, SugarSync, SkyDrive, Box.com, Strato y el futuro Google Drive, seguirán ofreciendo soluciones para facilitar la vida a las personas, organizaciones y empresas

Los proyectos de TI en la nube deberán velar, en cualquier forma***, por la seguridad***, la elección del proveedor, la escalabilidad, la evaluación (posibilidad de realizar pruebas previas antes de la contratación), la implantación de tarifas planas, el acuerdo previo de nivel de servicios (SLA), ***la protección y privacidad de los datos.***

Cloud Computing ha madurado, y podrá ya mantener un crecimiento constante. Las noticias relativas a la Nube no paran de aparecer y las publicaciones en prensa, radio y televisión propagan el modelo y sus principales manifestaciones. La computación en nube será, con toda probabilidad, el motor de la computación del futuro

Las tendencias predominantes serán la **movilidad** y la **ubicuidad**. Los usuarios de telefonía móvil llegarán pronto a los dos mil millones de teléfonos y cada día serán más inteligentes, y los usuarios de Internet en la década actual se espera lleguen a cinco mil millones. La gran mayoría se conectarán a la nube descargándose programas y aplicaciones web, desde cualquier lugar en cualquier momento y con cualquier dispositivo: "la ubicuidad se configurará como una utopía alcanzable gracias a Internet y la Web y, en particular, la Nube".

En conclusión, no es que "***el futuro ya no es lo que era***",, como diría mi siempre admirado Groucho Marx, sino que ha llegado, ya está aquí y este futuro pasará por la nube que se convertirá en el centro de atención del nuevo universo digital.

BIBLIOGRAFÍA

BANKINTER/ACCENTURE (2010). *Cloud computing. La tercera ola de las Tecnologías de la Información.* 2010. [disponible en: www.fundacionbankinter.org]

CIERCO, David. (2011). *Cloud Computing. Retos y oportunidades.* FUNDACIÓN IDEAS, 2011. [disponible en: www.fundacionideas.org]

NIST. *Guidelines en Security and Privacy in Public Cloud Computing*. NIST, 2011.

ENISA (2011). *Seguridad y resistencia en las nubes de la Administración Electrónica.* Brsuelas: Enisa, enero 2011. Traducción del documento original en ingles, por INTECO bajo la dirección de Daniele Catteddu. [disponible en www.inteco.es].

INTECO-CERT , (2011). . *Riesgos y amenazas en cloud computing*. Marzo 2011. [disponible en www.inteco.es].

JOYANES, Luis (2009*a*) "La Computación en Nube*(Cloud Computing)*: El nuevo paradigma tecnológico para empresas y organizaciones en la Sociedad del Conocimiento" en *ICADE,* nº 77, enero-marzo 2009, Madrid: Universidad Pontificia Comillas.

JOYANES, Luis. (2009*c*). *Seminario Empresa 2.0: Integración de la Web 2.0 y Cloud Computing en la empresa.* Madrid: Corenetworks [en línea: www.corenetworks.es].

KRUTZ, Ronald L. y DEAN VINES, Ruseell (2010). Cloud Security. A Comprehensive Guide to Secure Cloud Computing. Indianapolis: Wiley.

KUNDRA, Vivek, (2011). *Federal Cloud Computing Strategy.* Washington: The White House, february 2011.

MARKS, Eric A. y LOZANO, Bob. (2010). *Executive´s Guide Cloud computing*. New Jersey Wiley

MATHER Tim *et al*. (2009). *Cloud Security and Privacy.* Sebastopol: O´Reilly

NAHARI, Hadi y KRUTZ, Ronald L. (2011). Web Commerce Security. Design and Development. Indianapolis: Wiley.

OBSERVATORIO DE LA SEGURIDAD DE LA INFORMACIÓN, (2011). *Guía para empresas: seguridad y privacidad del cloud computing.* Marzo 2011. INTECO-CERT. [disponible en www.inteco.es].

VELTE, Anthony T. *et al* (2010). *Cloud Computing. A Practical Approach.* New York: McGraw-Hill