colegio oficial
ingenieros de telecomunicación

Guía de Iniciación a Actividad Profesional

Migración de Pymes a Entornos de Cloud Computing

Grupo de Nuevas Actividades Profesionales
Colegio Oficial de Ingenieros de Telecomunicación

Grupo de Nuevas Actividades Profesionales del COIT (Grupo NAP)

En acuerdo de Junta de Gobierno del COIT desde julio de 2009, el Grupo de trabajo de "Nuevas Actividades Profesionales" (NAP), se enmarca dentro del Grupo de trabajo de Ejercicio Profesional, que queda conformado por los Grupos NAP y ELP (Ejercicio Libre Profesional).

Este Grupo de Trabajo nació en el 2003 con el objetivo de ocuparse de detectar nuevas actividades que surjan, analizarlas, evaluar su impacto y, en su caso, promocionarlas. Una resultante de esta misión es promover, en su caso, la conveniencia o la obligatoriedad de contar con la redacción de un proyecto técnico de telecomunicaciones en estas nuevas áreas de actividad, ya sea por su grado de complejidad, porque soporten servicios de telecomunicación de uso público, porque deban quedar garantizados unos requisitos mínimos de calidad y de seguridad o bien porque se deba hacer un uso eficaz y eficiente de ciertos recursos públicos limitados en un régimen de mercado liberalizado.

Este documento se enmarca dentro de una nueva serie de estudios breves denominados "Guías de Iniciación a Actividades Profesionales" que pretenden dar respuesta a todas aquellas cuestiones que puedan plantearse de manera práctica y didáctica a aquellos que quieran adentrarse en nuevas actividades profesionales.

Esperamos que sea de vuestro de interés
Cayetano Lluch Mesquida
Vicedecano del COIT

Agradecimientos

En la redacción de esta guía se ha contado con la valiosa ayuda y experiencia de nuestro compañero David Calles y la empresa Softec-Internet a los que agradecemos desde estas líneas su colaboración.

Índice

1 Objetivos 10
2 Introducción 10
3 Servicios que es posible migrar a la Nube 11
4 Argumentario para la Migración de Empresas a la Nube 11
5 Guía para la migración de entornos de Pymes a la Nube 13
6 Aspectos a tener en cuenta para la migración 19
7 La elección del proveedor de Servicios de Cloud Computing 21
8 Mercado objetivo 22
9 Valoración económica 23
10 Razones para desarrollar esta actividad 23
11 Bibliografía y Enlaces de interés 23

1 Objetivos

En esta guía pretendemos orientar a aquellos ingenieros de telecomunicación que quieran iniciarse en actividades de asesoramiento e implantación de servicios de cloud computing en PYMEs, dotándoles de una perspectiva general del sector del cloud, presentando algunos de los condicionantes técnicos, económicos y jurídicos que hay que tener en cuenta en el paso a servicios cloud y orientándoles sobre los clientes potenciales a los que los ingenieros se pueden dirigir.

2 Introducción

El tejido empresarial español se compone básicamente de PYMEs. Éstas han adoptado las TICs (Tecnologías de la Información y la Comunicación) como parte de su vida diaria y cada vez más, son conscientes de la importancia que tienen estas para el aumento de la productividad y las posibilidades de crecimiento económico de las empresas. Sin embargo, muchas no pueden dedicar mucho tiempo ni recursos a su mantenimiento, corriendo el riesgo de perder el tren de la oportunidad que las Tics suponen.

Paralelamente, tanto los ciudadanos como las empresas nos hemos habituado a la utilización de servicios on-line en nuestra vida cotidiana (e-mail, redes sociales, información web,…) aplicaciones todas ellas que residen en la red.

El Cloud Computing o computación en la nube surge para dar respuesta a este tipo de problemática. Según la definición del NIST *(National Institute of Standards and Technologies),* Cloud computing o computación en la nube es un "modelo que permite, de forma práctica y desde cualquier ubicación, el acceso bajo demanda a una serie de recursos informáticos configurables compartidos (redes, servidores, sistemas de almacenamiento, aplicaciones y servicios), que pueden ser rápidamente dotados y puestos en funcionamiento con un mínimo esfuerzo de gestión e interacción con el proveedor de servicios". Es decir un servicio al que se accede a través de la red.

Hay aplicaciones informáticas que son relevantes para el desarrollo y la gestión de las PYMES y son susceptibles de utilizar a través de servicios en la nube: Herramientas de Productividad, Herramientas de Trabajo en Grupo, CRM y ERP. Igualmente a nivel hardware, los servidores por ejemplo también son susceptibles de migrarlos a la nube.

Básicamente, existen tres tipos de servicios de cloud computing o de "nube" como popularmente se conoce:

- **Cloud público o nube pública**: son servicios ofrecidos por terceros en los que múltiples usuarios acceden a la infraestructura de la nube. De este modo muchos usuarios utilizan servicios web que son procesados en el mismo servidor, pueden compartir espacio en disco u otras infraestructuras de red con otros usuarios.

- **Cloud privado o nube privada:** servicio utilizado por un solo cliente que controla qué aplicaciones deben correr y dónde. Este tipo de nube es adecuada para aquellas compañías que necesitan una alta protección de los datos.

- **Cloud híbrida o nube híbrida:** Son combinaciones de modelos de nubes públicas y privada. La organización usuaria es propietaria de una parte pero también comparte otras.

Por último, existe un cuarto modelo: las nubes comunitarias. Son nubes compartidas por varias organizaciones que pueden ser gestionadas por la propia comunidad o por un tercero.

3 Servicios que es posible migrar a la Nube

En el ámbito del "cloud computing" los servicios que se prestan se estructuran en niveles o capas, como si de la torre OSI se tratara, en los que se sitúan conceptualmente diferentes recursos "as a service": "infraestructure as a service" (IaaS), "platform as a service" (PaaS), "software as a service" (SaaS), y todo lo que admita funcionar "as a service".

Software como servicio: aplicación completa ofrecida como un servicio bajo demanda, lo que en la práctica significa una sola instancia del software que corre en la infraestructura del proveedor y sirve a múltiples organizaciones de clientes. Algunos ejemplos populares son Google Apps y Microsoft Office 365.

Plataforma como servicio: en este servicio se proporciona al usuario una plataforma completa de procesamiento sin necesidad de tener que comprar y mantener hardware y software. Los ejemplos comerciales incluyen Google App Engine, que sirve aplicaciones de la infraestructura Google, y también Windows Azure, de Microsoft, una plataforma en la nube que permite el desarrollo y ejecución de aplicaciones codificadas en varios lenguajes y tecnologías como .NET, Java y PHP. Servicios PaaS tales como éstos permiten gran flexibilidad, pero puede ser restringida por las capacidades que están disponibles a través del proveedor.

Infraestructura como servicio: se denomina también en algunos casos "hardware as a service", se trata del servicio que proporciona almacenamiento y capacidad de cómputo. Servidores, sistemas de almacenamiento, conexiones, routers y otros sistemas se concentran a través de lo que se denomina "virtualización".

4 Argumentario para la Migración de Empresas a la Nube

A continuación se enumeran las ventajas e inconvenientes de los servicios de cloud computing:

Ventajas	Inconvenientes
Escalabilidad	*Se comparte la infraestructura con más organizaciones.*
Eficiencia de los recursos mediante los modelos de pago por uso	*Poca transparencia para el cliente, ya que no se conoce el resto de servicios que comparten recursos, almacenamiento, etc.*

Gran ahorro de tiempo y costes *No se necesitan grandes inversiones iniciales*	*Dependencia de la seguridad de un tercero.*

5 Guía para la migración de entornos de Pymes a la Nube

Describimos en este apartado los pasos a seguir en el proceso de migración de una PYME a los servicios de cloud computing.

El cliente tendrá asociada una suscripción de los servicios contratados, tales como un plan que contenga alojamiento (hosting), correo electrónico, u otros servicios particulares que el cliente desee migrar.

Existen muy diversas opciones para las plataformas y los planes asociados, pero básicamente pueden darse tres casuísticas diferentes en cuanto al tipo de hosting y básicamente tres entornos de sistemas operativos.

En cuanto al hosting podemos identificar:

1. **Servidores compartidos.** Se hace uso de una misma máquina para una serie de alojamientos. Todos los alojamientos de los diferentes clientes disponen de acceso a los mismos recursos de la máquina, pudiendo en determinados momentos ser este punto un cuello de botella importante. Además, aunque no deberían interferirse, lo cierto es que las aplicaciones de diferentes clientes se ejecutan en paralelo, y esto podría llegar a ser una fuente de riesgo para datos sensibles. Puede entenderse que es la solución más económica de las tres, siendo difícil garantizar en cualquier caso una calidad de servicio.

2. **Servidores dedicados virtuales.** Son máquinas que tienen alojado algún software que permite independizar diferentes partes de la misma (RAM, Procesador, Espacio en Disco, Ancho de Banda de Internet…), de tal modo que un cliente disponga de una porción de la máquina acorde con las necesidades que haya definido, y que vaya definiendo en cada momento. Es el sistema más usado para el Cloud Computing, ya que otorga flexibilidad, incluso pudiendo programar aumentos de alguno de los parámetros dependiendo de las circunstancias externas temporales, y al mismo tiempo minimiza los costes, al ser estos compartidos por otros clientes, sin que exista interferencia entre los datos, ni riesgos de intrusión. Esta solución, siendo más cara que la de los servidores compartidos, permite garantizar una calidad de servicio al cliente final.

3. **Servidores dedicados.** Son máquinas destinadas al servicio de un único cliente. Suelen ser gestionadas directamente por estos, y la ventaja de disponer de un alojamiento de este tipo estriba en que se ubica en un entorno controlado y con ancho de banda potencialmente ilimitado. Es la solución más costosa, y salvo casos puntuales muy concretos de seguridad, no es la mejor solución debido a que cualquier ampliación en los parámetros del servicio requiere de una manipulación física de la máquina para desarrollar las ampliaciones oportunas.

Al respecto de los sistemas operativos que se ofertan, básicamente son:

1. **Sistemas Windows.** Esta opción es más cara pero su mantenimiento es más sencillo. No es la más elegida en el entorno de Cloud Computing, debido a los costes asociados, si bien puede ser una opción más interesante, si no se dispone de los conocimientos adecuados para manejar otras alternativas. Además en la actualidad todas las plataformas importantes orientadas a dar servicios web tienen su opción de instalación en Windows.

2. **Sistemas Linux.** Claramente la opción más económica debido a los costes de licencias que se evitan. Sin embargo, debe cuidarse el hecho de que son sistemas más especializados, que requieren de conocimientos previos importantes por parte de los encargados que deban manipular los entornos de desarrollo. Se dispone de todas las herramientas necesarias para el despliegue de cualquier entorno de Cloud Computing.

3. **Sistemas Mac.** Esta solución presume de ser muy estable, aunque tiene los dos inconvenientes de las otras dos plataformas, el coste de las licencias, y la especialización de los gestores de las máquinas. Es un sistema residual para este tipo de entornos, salvo cuando sobre ellos se instalan máquinas virtuales que emulen los sistemas Windows o Linux, en cuyo caso estaríamos en los puntos anteriores.

Para independizar al cliente del sistema operativo, se crean diferentes plataformas compatibles normalmente con todas ellas, o al menos con las dos principales (Windows y Linux) que permiten la gestión de los recursos de las máquinas, de forma que el proceso sea transparente tanto para el distribuidor de Sistemas Cloud, como para los usuarios que manejan las plataformas para configurar o acceder a las características contratadas a través las mismas.

Existen varias plataformas que realizan la función anterior, como VMWare o Parallels Plesk, plataformas que operan en los dos sistemas operativos, y que permiten un control total por parte del operador del hosting, o del revendedor del servicio o VAR (Value Added Reseller) que opera con este. En algunos casos, estas plataformas permiten aplicaciones muy diversas que pueden instalarse dentro del entorno, de tal manera que se permita a un cliente desplegar en la nube las actividades que antes desarrollaba en local.

Entrando de lleno en la elección del plan para el cliente, se debe considerar que esta no siempre es libre, sino que puede venir de algún modo condicionada por el anterior hosting que dispusiera dicho cliente, o por la decisión económica o de facilidad de manejo.

1. Alta del cliente con sus datos en el Sistema Cloud

En este punto lo que se hace es dar de alta al cliente con todos los datos necesarios en la plataforma.
Se puede hacer de forma manual, si son pocos clientes a dar de alta, o de forma programada para grandes volúmenes de clientes.

2. Alta de la suscripción asociado a los planes del cliente

En esta fase al cliente hay que asociarle las suscripciones de los servicios contratados (un plan que contenga hosting, correo…)
Para el ejemplo se ha estimado un plan de hosting compartido Linux.

3. Proceso de Replicación de Datos de Origen

Segmentamos por una parte la replicación de datos de la web y del correo electrónico

WEB

Fase 1: Recogida de datos

Deben obtenerse los siguientes datos:

- Obtención de datos de configuración DNS e IPs de origen
- Verificación del tipo de programación: versiones de PHP, ASP, etc...
- Librerías especiales utilizadas
- Aplicaciones web si las hubiere: Joomla, Mambo, Wordpress, PHPBB, etc...
- Obtención de datos de usuarios y contraseñas FTP del origen.
- Obtención de información sobre certificados SSL del origen si los hubiere.
- Obtención de información sobre Bases de Datos. Nombre de la base de datos, usuarios, tipo de base de datos

Fase 2: Réplica de datos

Una vez recogidos los datos, se dan de alta en el plan asociado respetando todo lo posible los datos de origen para que la migración sea trasparente. En caso de que algún dato no sea posible replicar (ejemplo: contraseña que contenga caracteres inválidos en el Sistema Cloud o que no cumpla la política de seguridad establecida) será puesto por defecto o acordado con el cliente y se le informará.

CORREO ELECTRÓNICO

Fase 1: Recogida de datos

Deberán obtenerse los siguientes datos:

- Cuentas de correo, usuarios y contraseñas válidos en el sistema de origen.
- Existencia o no de elementos externos. Ejemplo: filtros antispam tipo spamina.
- Alias de correo.
- Redirecciones de cuentas.
- Autorespondedores de correo electrónico.
- Listas de correo.
- Grupos de correo.
- Libretas de direcciones y agendas. Revisando la compatibilidad con webmail.
- Filtros webmail, listas blancas y negras.

Fase 2: Réplica de datos

Una vez recogidos los datos, se dan de alta en el plan asociado respetando todo lo posible los datos de origen para que la migración sea trasparente. En caso de que algún dato no sea posible replicarlo (ejemplo: contraseña que contenga caracteres inválidos en el Sistema Cloud o que no cumpla la política de seguridad establecida) será puesto por defecto o acordado con el cliente.

Puede ocurrir que hay procesos manuales (caso de la réplica de datos de la web) que pudieran programarse "automáticos" si contempláramos grandes volúmenes, pero no es el caso.
Por otro lado, sí que existen procesos programados como es la réplica de las cuentas de correo en función del número de buzones de correo que tenga la PYME.

4. Migración de datos

En esta fase se pasa a replicar los contenidos del anterior alojamiento del cliente en la nueva plataforma.

Para ello los pasos que se dan son:

- Replicar los registros DNS actuales en la configuración del Sistema Cloud actualizando los datos de los registros que van a cambiar con la migración y dando de alta los nuevos registros que sean necesarios.
- Migración del contenido web de origen y subiéndolo a la nueva plataforma usando el mismo sistema para conservar los permisos y usuarios.
- Migración del contenido de las bases de datos usando un "dump" de la base de datos de origen y restaurada posteriormente en el Sistema Cloud.
- Instalación de certificados de seguridad si los hubiere.
- Comprobación de funcionamiento de la WEB. Es posible que haya que modificar en código enlaces a la IP o nombre de la máquina antigua si existieran en la programación. Será necesario escanear los ficheros en busca de patrones que hagan referencia al antiguo servidor.
- Insertar en el entorno webmail los datos sobre las direcciones de correos; agendas, filtros, listas blancas y negras.
- Migración de los contenidos del correo para lo que usaremos una sincronización mediante el protocolo IMAP que mantiene todas las características del correo.
- Revisión de los contenidos migrados y funcionamiento del entorno de correo.

La duración de esta fase depende en exclusiva del volumen de contenidos y correos a migrar y su "peso" ya que se hace directamente por la red entre los dos servidores (antiguo y nuevo).

5. Puesta en marcha del nuevo entorno en producción

Este es punto de inflexión donde realmente el cliente es consciente realmente de la migración. Hasta este punto todas las acciones han sido transparentes para el cliente.
Para poner en marcha el nuevo sistema sólo hay que cambiar el direccionamiento de las DNS. Para ello se pueden modificar los registros actuales o cambiar los servidores de nombres y utilizar los asignados a la nueva plataforma.
El tiempo de propagación del cambio de DNS es de 24/48 horas aproximadamente por lo que es conveniente realizarlo en viernes o fin de semana para minimizar el impacto de la resincronización de contenidos posterior.

IMPORTANTE: El cambio de las DNS es el punto donde asumimos que no hay vuelta atrás al proceso de migración.

6. Resincronización de contenidos

Durante el tiempo de propagación de 48 horas parte de la información puede ir indistintamente a ambas plataformas. Para solventar esa situación realizaremos una resincronización de los contenidos del correo y de las modificaciones en las bases de datos que se hayan producido durante ese período.
Esta acción no supone parada del servicio y es transparente para el usuario final.
La duración de esta fase depende del volumen de correos (y su tamaño) a resincronizar pero no debiera pasar de una o dos jornadas.

7. Formación

Si fuera necesario, el proveedor de cloud, podría realizar una formación al cliente.

Resumimos de manera gráfica el esquema de pasos para la migración:

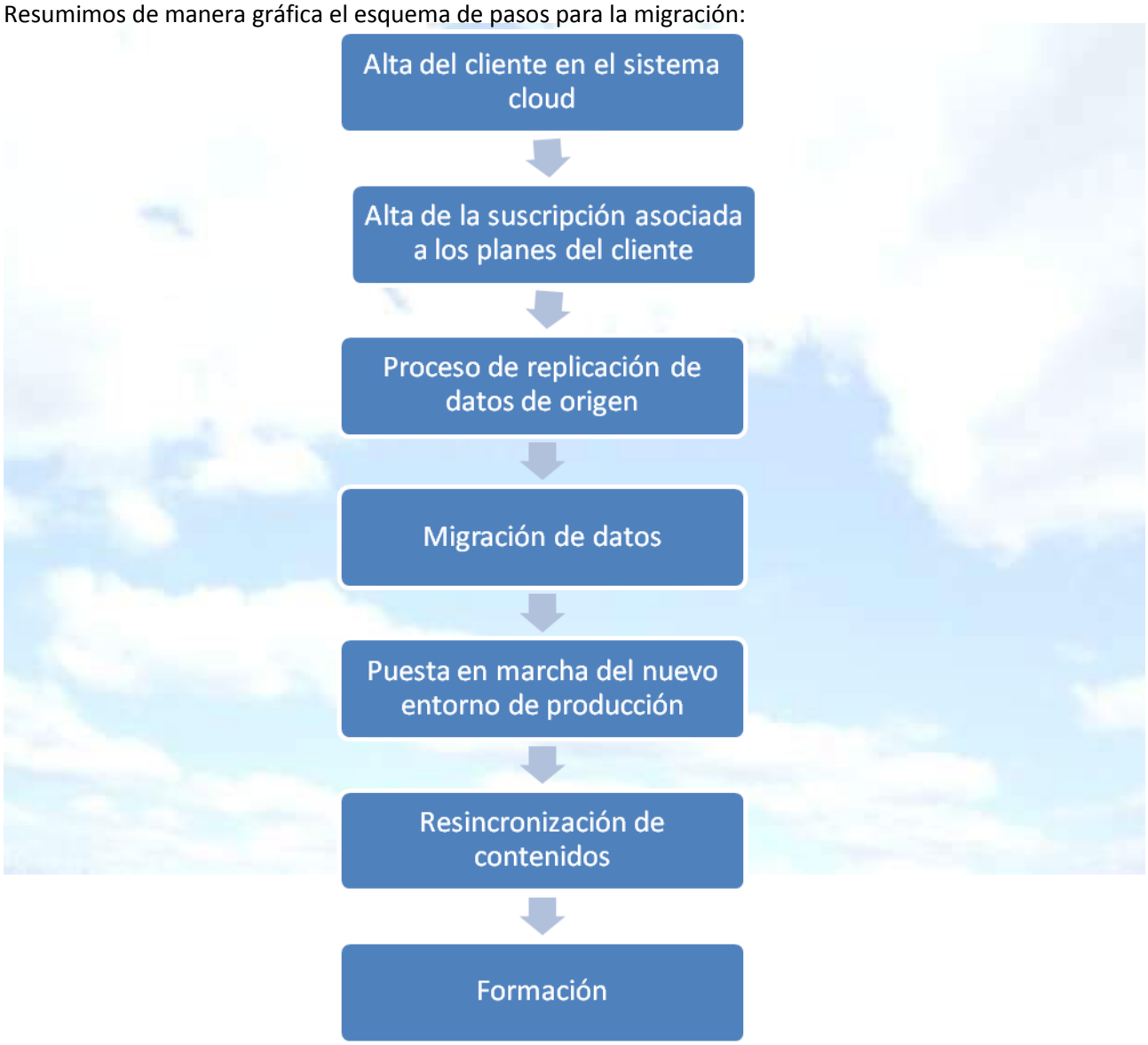

Figura 1. Esquema de pasos en la migración a cloud

Una posible planificación de proceso en tiempo sería:

Id	Nombre de tarea	Duración	Comienzo	Fin
1	ALTA DEL CLIENTE CON SUS DATOS EN EL SBC	0,5 días	mar 30/11/10	mar 30/11/10
2	ALTA DE LA SUSCRIPCIÓN ASOCIADO A LOS PLANE	0,5 días	mar 30/11/10	mar 30/11/10
3	**PROCESO DE REPLICACIÓN DE DATOS DE ORIGEN**	**2 días**	**mar 30/11/10**	**jue 02/12/10**
4	WEB	0,5 días	mar 30/11/10	mar 30/11/10
5	CORREO	2 días	mar 30/11/10	jue 02/12/10
6	**MIGRACIÓN DE DATOS**	**1 día**	**jue 02/12/10**	**vie 03/12/10**
7	WEB	0,5 días	jue 02/12/10	jue 02/12/10
8	CORREO	1 día	jue 02/12/10	vie 03/12/10
9	PUESTA EN MARCHA DEL NUEVO ENTORNO EN PRO	0,5 días	vie 03/12/10	vie 03/12/10
10	RESINCRONIZACIÓN DE CONTENIDOS	0,5 días	lun 06/12/10	lun 06/12/10

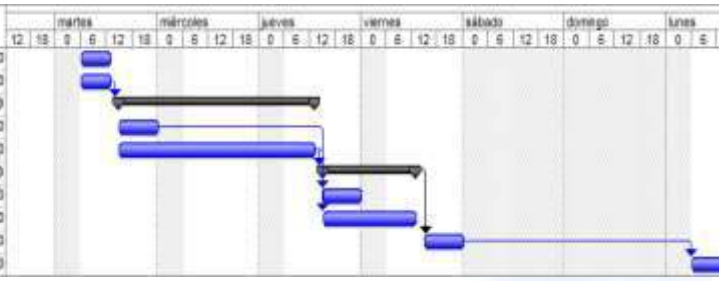

Figura 2. Ejemplo de planificación temporal del proceso

6 Aspectos a tener en cuenta para la migración

Para dar el paso a cloud computing hay que tener en cuenta una serie de aspectos tanto de índole económica, técnica y jurídica:

Aspectos Técnicos

Un aspecto esencial y que a veces pasa desapercibido es tener en cuenta es que no es posible utilizar servicios de cloud computing si no hay una buena conexión a Internet. La calidad de conexión y su velocidad deben ser altas para que las prestaciones y experiencia del servicio sean las adecuadas.

Otro asunto que no conviene olvidar es la deslocalización de datos. La localización de los datos puede incidir significativamente en el régimen jurídico aplicable y en las condiciones del contrato. En determinados casos podría requerirse cumplir con los requisitos previstos para las transferencias internacionales de datos personales. Como ventaja es que se pueden llevar tanto los datos como los procesos al lugar más conveniente para la organización. Por ejemplo, se pueden utilizar múltiples copias de un servidor y repartirlas por centros de proceso de datos en distintos puntos del planeta para mejorar los tiempos de acceso de los usuarios. Esto además, facilita el mantenimiento de copias de seguridad no solo de los datos sino del servidor entero, del sistema operativo y los programas instalados en él.

Durante los primeros momentos de uso del cloud computing, una opción recomendable es **no migrar a la nube los datos o procesos más sensibles.** Para vencer los miedos iniciales, puede comenzarse por sistemas poco críticos para el negocio, o poco confidenciales, e ir avanzando en función de la experiencia. En cualquier caso conviene prestar atención a los *backups* y a la recuperación frente a desastres.

Una vez comprobada si la fórmula funciona se puede realizar una **migración total a la nube**, utilizando los mecanismos de apoyo que proporcionan los proveedores de servicios y así reducir significativamente la complejidad de la tarea.
Para permitir la correcta continuidad de negocio es muy importante **mantener una copia completa del sistema en el modelo tradicional durante un tiempo**.

Deben evaluarse de las facilidades de dar marcha atrás con el proveedor elegido y de cambio de proveedor de Cloud.

Los mecanismos específicos que puede adoptar el cliente para reforzar la seguridad en la nube engloban el control perimetral, la criptografía y la gestión de logs o archivos de registro de eventos.

Aspectos Jurídicos

Es importante tener en cuenta que igualmente hay que cumplir con la Ley Orgánica de Protección de Datos (LOPD). Cuando el proveedor se encuentre sometido a la Ley española deberá garantizar el cumplimiento de la normativa (LOPD y su reglamento de desarrollo) y, en su caso, si el cliente es una administración pública, los requisitos que deriven de los Esquemas Nacionales de Seguridad e Interoperabilidad.

En el caso de datos de carácter personal, de acuerdo con la normativa española de protección de datos, el cliente que contrata servicios de cloud computing para el tratamiento de datos de carácter personal (fuera de la excepción de actividades personales o domésticas) asume las obligaciones inherentes al de responsable de fichero. Por su parte, el proveedor del servicio, en la medida en que efectúa el tratamiento por cuenta del responsable, desempeñaría el rol de encargado del tratamiento.

No obstante, las posiciones relativas de cliente y prestador de servicios de computación en nube presentan unas características peculiares. En la prestación de servicios de *cloud computing* por terceros ajenos a la organización responsable se produce lo que la LOPD y su Reglamento de Desarrollo denominan un *encargo del tratamiento*. Esto es, una prestación de servicios en la que los datos son objeto de algún tipo de tratamiento por parte del prestador/proveedor, quien pasa a ser el **encargado del tratamiento**.

Dependiendo del tipo de servicio en nube que se contrate y de los perfiles del cliente y del proveedor variará sensiblemente la posibilidad de que el cliente-responsable pueda impartir al prestador las instrucciones sobre el modo de tratar los datos a que se refiere la legislación. En el caso del cloud computing es fundamental revisar las condiciones del contrato a fin de garantizar una adecuada previsión de las cuestiones relacionadas con la **presencia de un encargado del tratamiento** y/o una **transferencia internacional de datos personales.**

Por otra parte, salvo en casos muy específicos, la contratación se realiza a través de **condiciones generales**,-esto es, de contratos que responden a un modelo general para una categoría de clientes y adicionalmente pueden preverse **políticas de privacidad**.

Los prestadores de servicios de la sociedad de la información (servicios de alojamiento de datos en la nube y acceso a Internet), deben cumplir con los requisitos establecidos en la **Ley 34/2002, de Servicios de la Sociedad de la Información y del Comercio Electrónico (LSSI)**:

En concreto, los proveedores de servicios establecidos en España están obligados a informar a sus clientes de forma permanente, fácil, directa y gratuita sobre:

- Los medios técnicos aplicados para aumentar la seguridad de la información (como programas antivirus, antiespías y filtros de correo).
- Las medidas de seguridad que aplican en la provisión de los servicios.
- Las herramientas existentes para el filtrado y restricción del acceso a determinados contenidos y servicios en Internet no deseados o que puedan resultar nocivos para la juventud y la infancia.
- En el caso de los proveedores de acceso a Internet, además deben comunicar a los usuarios las responsabilidades en que pueden incurrir por el uso ilícito de la Red.

Además de los citados preceptos legales la **Ley 32/2003 General de Telecomunicaciones** también vela por el cumplimiento de las obligaciones en el secreto de las comunicaciones y protección de datos personales, así como de los derechos y obligaciones de carácter público vinculados con las redes y servicios de comunicaciones electrónicas, imponiendo a su vez las correspondientes sanciones por su incumplimiento.

Aspectos económicos

A la hora de desplegar un nuevo servicio, el modelo informático basado en *cloud computing* permite reducir costes con respecto al modelo tradicional, ya que los recursos que la entidad debe destinar son

menores, tanto directos (en cuanto a hardware, mantenimiento, personal, etc.) como indirectos (instalaciones, suministros, etc.), de tal forma que parte de los costes fijos pasan a ser variables.

A la vez, las entidades pueden contratar un servicio en la nube por una cantidad al mes y en función de cómo evolucionen sus necesidades, aumentar o disminuir los recursos de procesamiento, sabiendo que se va a pagar por uso efectivo.

7 La elección del proveedor de Servicios de Cloud Computing

Una vez un cliente ha decidido que quiere migrar su sistema a la Nube, es conveniente revisar las diferentes políticas internas por si estas condicionasen jurídicamente, el proveedor del Sistema Cloud que va a contratarse.

Por otra parte, aunque pueden existir diversas circunstancias en las condiciones del servicio que deban tratarse directamente en el contrato con el proveedor, hay unos mínimos de exigencia que deberían garantizar todos los proveedores de Cloud. Una de estas es seguir la **normativa internacional ISO 27001**, que reúne las últimas tecnologías de seguridad para garantizar la máxima disponibilidad, integridad y estabilidad de los servicios alojados.

De hecho la principal desventaja que se le reprocha al Cloud es la potencial falta de seguridad de los datos. Para evitar que una amenaza pueda hacer realidad este argumento, es necesario garantizar sistemas de protección contra dichas amenazas. Dependiendo del tipo de amenaza pueden aplicarse las siguientes medidas:

- **Medidas lógicas:** se refiere a la protección de la información almacenada y transportada. Para garantizarlas, se deben establecer diversas políticas de control de accesos, de instalación, copia de software, copias de seguridad, uso de criptografía, uso de cortafuegos, definición de una política de monitorización (logging) y auditoría (auditing). Entre estas medidas también se incluyen medidas humanas (definición de funciones, relaciones y responsabilidades de los distintos usuarios: administrador del sistema, usuarios, personas relacionadas con el sistema pero sin necesidad de usarlo, y personas ajenas al sistema).

- **Medidas físicas**: se aplican mecanismos para impedir el acceso directo o físico no autorizado al sistema. Se definen ciertos controles tales como el control de las condiciones medioambientales, prevención de catástrofes, vigilancia, sistemas de contingencia, sistemas de recuperación y control de la entrada y salida de material.

- **Medidas administrativas**: son aquellas que deben ser tomadas por las personas encargadas de definir la política de seguridad para ponerla en práctica, hacerla viable y vigilar su correcto funcionamiento. Las fundamentales son:

    - Documentación y publicación de la política de seguridad y de las medidas tomadas para ponerla en práctica
    - Establecimiento de un plan de formación del personal

- Información de los usuarios que deben conocer la política de seguridad de la empresa y las medidas de seguridad tomadas para ponerla en práctica, además tienen que ser conscientes de las consecuencias de un mal uso del mismo.

- **Medidas legales:** sirven para disuadir al posible atacante o para aplicarle algún tipo de castigo a posteriori. Son fijadas por instituciones gubernamentales, e incluso por instituciones internacionales. Destaca la LOPD: Ley Orgánica de Protección de Datos de Carácter Personal, que vincula a todas las entidades que trabajen con datos de carácter personal definiendo las medidas de seguridad de carácter técnico para su protección y las penas a imponer en caso de incumplimiento. También son importantes la LSSSI (Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico) y la Directiva Europea de Protección de Datos.

Así pues para controlar los riesgos de seguridad, es importante que las aplicaciones que se usen en Cloud, fundamentalmente cuando estas requieran de confidencialidad, incorporen sistemas de cifrado y protocolos de seguridad.

Todos los elementos anteriores, deben ser exigibles a un proveedor de Cloud, y nos permitirá valorar la calidad del servicio que puede ofrecer a la Pyme. El cumplimiento de los parámetros expuestos, redundará en una mayor garantía de seguridad y estabilidad del sistema Cloud elegido.

8 Mercado objetivo

A modo de guía, y sin descartar otras consideraciones, indicamos algunas de las empresas que podrían ser clientes potenciales de servicios de cloud computing y que por tanto necesitan tanto de labores de asesoramiento como de la propia migración.

1) Empresas nuevas, que tienen sistemas nuevos o migraciones ya previstas de sistemas obsoletos.

2) Empresas que necesiten utilizar entornos de pruebas, o que precisen nuevos procesos de negocio que ofrecen dudas sobre su rentabilidad o cuya demanda es poco previsible. Como ventaja en Cloud Computing equivocarse sale barato porque se paga por uso, no hay grandes inversiones iniciales.

3) Empresas que no reúnen condiciones óptimas para alojar sistemas de información: salas no adaptadas, sin refrigeración, vulnerables a fallos eléctricos, entornos físicamente inseguros, etc.

4) Empresas que dedican muchos recursos económicos y tiempo al mantenimiento de sus TIC más que a innovar en ellas y con ellas, es decir, empresas que no obtienen ventajas competitivas por operar sus propias TIC.

5) Empresas que dispongan de aplicaciones en las que importe menos el rendimiento que la accesibilidad desde cualquier lugar. Pensar en la velocidad habitual de navegación por Internet con una línea ADSL y evaluar si ese rendimiento es suficiente.

6) Empresas en la que existen dispersión geográfica entre sistemas o aplicaciones con mucha intercomunicación pueden evitar la dispersión geográfica entre sistemas o aplicaciones con mucha intercomunicación, pues esto degrada el rendimiento y genera nuevos puntos de fallo.

7) Aplicaciones en las que un navegador web es interfaz adecuado. Si se va a acceder desde diversos dispositivos (ordenadores, *tablets*, *smartphones*, etc.) es de suponer que sí lo es.

9 Valoración económica

Recomendamos que una vez analizadas las necesidades de cliente, se facturen las labores de asesoramiento e implantación en función del número de horas de trabajo.

10 Razones para desarrollar esta actividad

En un entorno de crisis económica en el que nos encontramos, donde la restricciones presupuestas, la reducción de costes y el incremento de la productividad será la tónica general, los servicios de cloud computing, y por tanto, las labores de asesoramiento, consultoría e implantación de servicios cloud a clientes representan una oportunidad de actividad profesional para los Ingenieros de Telecomunicación.

Según NEC, en el plano tecnológico, el cloud computing y la eficiencia energética se constituirán en los pilares principales para la optimización de costes.

La firma Gartner asegura que para el año 2015 el crecimiento del cloud alcanzará los 21.300 millones de dólares.

Para IBM que coincide con NEC, los servicios de cloud computing serán claves para los CIOs de las empresas en la reingeniería de procesos para optimizar costes, destacando además que las empresas españolas se están sumando a la tendencia de subirse a la nube, apostando que el 57 % de las empresas españolas pretender adoptar cloud en los próximos 5 años.

Esto son sólo algunas de los análisis que las grandes firmas tienen previstos para el mercado de cloud computing, cuyo potencial de crecimiento es fuerte.

11 Bibliografía y Enlaces de interés

CSA, 2010, Top Threats to Cloud Computing V1.0

Gartner, 2008, Assessing the Security Risks of Cloud Computing

NIST, 2011, Guidelines on Security and Privacy in Public Cloud Computing

ENISA, 2011, SWOT analysis, Risk Assessment (Public Administration) and Privacy

ENISA, 2009, Computer Assurance

ENISA, 2009, Risk Assessment

CSA, Security Guidance

CSA, Identity and Access Management:

World Privacy Forum Report

Inteco, Riesgos y Amenazas en Cloud Computing 2011

Inteco. Guia para empresas: seguridad y privacidad del cloud computing

Agencia Española de Protección de Datos