GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

INTECO
Instituto Nacional de Tecnologías de la Comunicación

Guía para empresas: seguridad y privacidad del *cloud computing*

OBSERVATORIO DE LA **SEGURIDAD** DE LA **INFORMACIÓN**

Edición: Octubre 2011

La "Guía para empresas: seguridad y privacidad del cloud computing" ha sido elaborada por el equipo del Observatorio de la Seguridad de la Información de INTECO:

Pablo Pérez San-José (dirección)

Cristina Gutiérrez Borge (coordinación)

Susana de la Fuente Rodríguez

Laura García Pérez

Eduardo Álvarez Alonso

El **Instituto Nacional de Tecnologías de la Comunicación (INTECO)** (http://www.inteco.es), sociedad estatal adscrita al Ministerio de Industria, Turismo y Comercio a través de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, es una plataforma para el desarrollo de la Sociedad del Conocimiento a través de proyectos del ámbito de la innovación y la tecnología. La misión de INTECO es aportar valor e innovación a los ciudadanos, a las pymes, a las Administraciones Públicas y al sector de las tecnologías de la información, a través del desarrollo de proyectos que contribuyan a reforzar la confianza en los servicios de la Sociedad de la Información en nuestro país, promoviendo además una línea de participación internacional. Para ello, INTECO desarrollará actuaciones en las siguientes líneas: Seguridad, Accesibilidad, Calidad TIC y Formación.

El **Observatorio de la Seguridad de la Información** (http://observatorio.inteco.es) se inserta dentro de la línea estratégica de actuación de INTECO en materia de Seguridad Tecnológica, siendo un referente nacional e internacional al servicio de los ciudadanos, empresas, y administraciones españolas para describir, analizar, asesorar y difundir la cultura de la seguridad y la confianza de la Sociedad de la Información.

INTECO quiere agradecer la colaboración de la **Asociación Profesional Española de Privacidad (APEP)** (http://www.apep.es) en la elaboración de esta guía, en especial a su presidente Ricard Martínez por su aportación personal:

Índice

1. Introducción al *cloud computing*

En los últimos años las organizaciones asisten con expectación al surgimiento y desarrollo del *cloud computing* o paradigma de computación en la nube (también llamada "la nube"), según el cual, todos los recursos de información pueden ser almacenados en servidores de terceros y accesibles a través de Internet. Los proveedores disponen de centros de proceso de datos para dar servicio a múltiples usuarios. A cambio, los clientes reciben un soporte flexible a las necesidades y particularidades de su actividad en cada momento.

Este modelo ofrece grandes posibilidades para empresas y entidades, tanto en términos de inversión como en economías de escala, deslocalización, acceso a la información desde cualquier lugar, etc. Si bien no existen datos concluyentes de la adopción de la nube en España, se identifican una serie de factores[1] que pueden propiciar su extensión en los sectores público y privado: desarrollo del sector TIC, tejido empresarial dominado por la PYME, disposición geográfica de la población y potencial del sector público, entre otros.

El presente documento ofrece una aproximación al modelo *cloud computing* para todo tipo de organizaciones, deteniéndose en las principales implicaciones en cuanto a seguridad y privacidad, claves para asegurar el éxito en la utilización de servicios en la nube.

A lo largo de la presente guía, el lector encontrará las denominaciones entidad, empresa, organización, cliente, contratista, o usuario en función del papel que tome en la situación concreta que se esté tratando en cada apartado.

1 Fundación para la Innovación Bankinter *(2010). Cloud Computing. La tercera ola de las Tecnologías de la Información.*

1.1. CLOUD COMPUTING COMO EVOLUCIÓN DE TECNOLOGÍAS

Cloud computing, o informática "en la nube", es una propuesta tecnológica o modelo que permite ofrecer servicios informáticos a través de Internet en el que los recursos, el software y los datos se ofrecen bajo demanda. El objetivo de este nuevo modelo es que la empresa o el usuario final no tengan que preocuparse por los detalles técnicos y puedan utilizar cualquier aplicación con su navegador web.

Cloud computing es la **suma de la evolución de varias tecnologías**:

- **Aumento de la capacidad de procesamiento**. Desde el origen de la informática, la capacidad de cómputo de los ordenadores personales se ha ido incrementando de forma vertiginosa.

- **Conexión a Internet**. La Red se ha convertido en una herramienta casi indispensable en la vida cotidiana de las personas. Su evolución implica aumento en la velocidad de conexión y en el número de conexiones en los hogares y en el trabajo.

- **Dispositivos móviles**. La miniaturización de los componentes informáticos ha permitido la aparición de dispositivos móviles que permiten la conexión permanentemente a Internet. Hoy en día, en un negocio es necesario poderse conectar con los recursos de la empresa, tanto desde ordenadores fijos como desde dispositivos portátiles, convirtiéndose la ubicuidad y movilidad en requisitos de gran importancia.

En cuanto a la **historia de la computación en la nube**, destacan los siguientes eventos:

- En 1961, John McCarthy sugirió que los avances en la informática y las comunicaciones conducirían a que "algún día la computación se

organizaría como un servicio público" (*utility*), igual que el modelo de negocio del agua o la electricidad.

- A finales de los años 90, los técnicos de Amazon se dieron cuenta que tenían una gran infraestructura informática pero que apenas utilizaban el 10-15% de su capacidad. Vieron las posibilidades de ofrecer estos servicios a usuarios y en 2006 presentaron los Servicios Web de Amazon[2].

- Durante los años 2007 y 2008, grandes empresas como Google o IBM se unieron a universidades norteamericanas para iniciar una investigación a gran escala sobre el *cloud computing*. Como resultado de esta investigación, enero de 2009 apareció Eucalyptus, una plataforma de código abierto que permitía la creación de sistemas en la nube compatibles con los servicios web de Amazon[2].

En conclusión, los avances en los tres campos mencionados anteriormente (capacidad de procesamiento, conexión a Internet y dispositivos móviles) junto a las importantes inversiones realizadas por las grandes empresas que dominan el panorama tecnológico mundial han propiciado la rápida evolución e implantación del *cloud computing*. Hasta tal punto que muchos usuarios ya disfrutan los servicios en la nube sin darse cuenta.

1.2. EL LUGAR DEL *CLOUD COMPUTING* EN EL DESARROLLO INFORMÁTICO

La evolución de la informática en los últimos años se puede simplificar en los siguientes hitos:

- ***Mainframes***. A principios de los años 60, los ordenadores eran dispositivos muy caros, difíciles de mantener y de utilizar. Las empresas

2 En inglés, *Amazon Web Services* (AWS) http://aws.amazon.com/

tenían grandes ordenadores, conocidos como *mainframes*, para hacer las tareas más críticas y complicadas. Generalmente, estos no estaban conectados a la Red y se utilizaban para manejar grandes cantidades de datos como censos o transacciones económicas.

- **Arquitectura cliente-servidor**. Entre los años 70 y 80, se generalizó el uso de ordenadores personales en los puestos de trabajo, menos costosos y potentes, pero que permitían realizar tareas básicas. Además disponían de un determinado número de ordenadores más potentes que se encargaban de mantener los datos más sensibles así como las aplicaciones que necesitaban más recursos. Estos ordenadores con mayores capacidades de proceso se denominaron servidores, mientras que las máquinas con recursos más limitados de cada puesto de trabajo pasaron a llamarse clientes. Nació la arquitectura cliente-servidor.

- **Arquitecturas colaborativas y distribuidas**. La complejidad de las aplicaciones informáticas ha ido creciendo con el tiempo, lo que ha obligado a crear sistemas más complejos para solucionar de forma eficiente todas las nuevas necesidades. Por ejemplo, la *computación grid* utiliza un número variable de ordenadores trabajando de forma colaborativa para solucionar problemas complejos para los que individualmente no tienen suficientes recursos. Por otra parte, la arquitectura *peer-to-peer* o p2p es una arquitectura distribuida en la que todos los nodos hacen a la vez de consumidores y suministradores de información. Estas arquitecturas son ampliamente utilizadas en la actualidad.

El **modelo *cloud computing*** no sustituye a las arquitecturas anteriores, pero consigue cambiar radicalmente la forma en la que se utilizan y entienden las aplicaciones informáticas, gracias a que permite aprovechar al máximo los puntos fuertes de Internet, los dispositivos móviles y los ordenadores personales.

1.3. NIVELES DEL SERVICIO

Para comprender el funcionamiento del *cloud computing* es fundamental comprender los tres niveles en que puede ser proporcionado el servicio.

1. **Infraestructura como Servicio** (IaaS, de sus siglas en inglés *Infrastructure as a Service)*. Se trata del nivel más alto de servicio. Se encarga de entregar una infraestructura de procesamiento completa al usuario bajo demanda. El usuario dispone de una o varias máquinas virtuales en la nube con las que, por ejemplo, puede aumentar el tamaño de disco duro en unos minutos, obtener mayor capacidad de proceso o enrutadores[3] y pagar solamente por los recursos que utilice. Este nivel puede ser visto como una evolución de los Servidores Privados Virtuales que ofrecen actualmente las empresas de *hosting*[4].

2. **Plataforma como Servicio** (PaaS, de sus siglas en inglés *Platform as a Service*). Se trata del nivel intermedio, se encarga de entregar una plataforma de procesamiento completa al usuario, plenamente funcional y sin tener que comprar y mantener el hardware y software. Por ejemplo, un desarrollador web necesita un servidor web que sirva sus páginas, un servidor de bases de datos y un sistema operativo. Este nivel se encarga de proporcionar todos estos servicios.

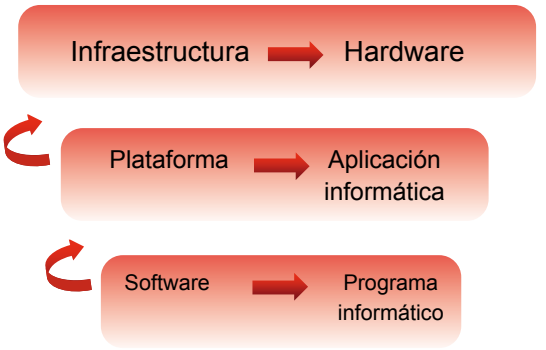
3. **Software como Servicio** (SaaS, de sus siglas en inglés *Software as a Service*). Este nivel se encarga de entregar el software como un servicio a través de Internet siempre que lo demande el usuario. Se trata del nivel más bajo que permite el acceso a la aplicación

3 Enrutador o *router*: Dispositivo que distribuye tráfico entre redes.

4 *Hosting:* Servicio ofrecido por empresas consistente en prestar alojamiento dentro de sus servidores a las páginas web de otras empresas, con la finalidad de que almacenen información, videos, fotografías o cualquier tipo de datos que desean tener accesible en la Red.

utilizando un navegador web, sin necesidad de instalar programas adicionales en el ordenador o teléfono móvil. Las suites ofimáticas a las que se puede acceder online son un buen ejemplo de este nivel.

Ejemplos de servicios entregados en cada nivel de *cloud computing*



1.4. MODELOS DE DESPLIEGUE DE SERVICIOS

Se pueden agrupar los sistemas de *cloud computing* en las siguientes categorías principales:

- Las **nubes públicas** son aquellas en las que todo el control de los recursos, procesos y datos está en manos de terceros. Múltiples usuarios pueden utilizar servicios web que son procesados en el mismo servidor, pueden compartir espacio en disco u otras infraestructuras de red con otros usuarios.

- Las **nubes privadas** son aquellas creadas y administradas por una única entidad que decide dónde y cómo se ejecutan los procesos dentro de la nube. Supone una mejora en cuanto a la seguridad y privacidad de los datos y procesos, ya que los datos sensibles permanecen en la infraestructura informática de la entidad, mientras que controla qué usuario accede a cada servicio de la nube. Sin embargo, la entidad sigue siendo la encargada de comprar, mantener y administrar toda la infraestructura hardware y software de la nube.

- En las **nubes híbridas** coexisten los dos modelos anteriores. Por ejemplo, una empresa hace uso de una nube pública para mantener su servidor web mientras que mantiene su servidor de bases de datos en su nube privada. De este modo, se establece un canal de comunicación entre la nube pública y privada mediante el cual los datos sensibles permanecen bajo estricto control mientras que el servidor web es administrado por un tercero. Esta solución disminuye la complejidad y coste de la nube privada.

- Se apunta además un cuarto modelo de despliegue de servicios, las **nubes comunitarias**, que son compartidas entre varias organizaciones que forman una comunidad con principios similares (misión, requerimientos de seguridad, políticas y cumplimientos normativos). Puede ser gestionada por la comunidad o por un tercero. Este modelo puede ser visto como una variación en el modelo de *cloud* privada.

1.5. TIPOLOGÍA DE PROVEEDORES

El panorama actual dirige a los usuarios hacia dos posibles soluciones. La primera sería contratar un *cloud* hosting y la segunda sería utilizar los servicios específicos de *cloud computing* ofertados por grandes empresas.

1. **Los servicios de *cloud hosting*** son similares a los servicios ofrecidos por empresas de *hosting* tradicional. La diferencia principal es que en un servicio en la nube se paga por lo que se utiliza y se pueden ampliar o disminuir los recursos del sistema en cuestión de minutos. En un sistema de *hosting* tradicional es necesario saber qué capacidad de procesamiento se va a necesitar e incluso qué versión del sistema operativo se va a utilizar antes de contratar los servicios.

2. **Los servicios de *cloud computing*** ofertados por las grandes empresas del sector informático permiten obtener una mayor personalización en la solución informática contratada. Dado que esta opción brinda más funcionalidades también requiere un mayor conocimiento técnico por parte del contratante para aprovechar al máximo sus características.

Existen herramientas y funcionalidades de *cloud computing* que se ofrecen de forma gratuita en la Red, como páginas y plataformas colaborativas en la Web 2.0.

2. Características principales del *cloud computing*

2.1. ACCESO UBICUO A LOS DATOS

¿Con *cloud computing* se puede trabajar desde cualquier lugar?

La principal característica del *cloud computing* es el acceso ubicuo (desde cualquier lugar) a los datos. Solo se necesita un navegador web y conexión a Internet para disfrutar de los servicios en la nube, no hace falta tener un sistema operativo determinado o instalar un software específico en cada cliente. Se puede utilizar un portátil, un teléfono móvil o una videoconsola conectado a la Red para acceder a las aplicaciones de la nube en cualquier momento.

Actualmente, las tecnologías móviles son una parte importante dentro del modelo de negocio de una empresa. La combinación de dispositivos móviles y fijos crea nuevas oportunidades en el desarrollo de la actividad empresarial permitiendo plena operatividad.

Esta característica supone una gran ventaja frente a otras tecnologías, aunque es importante puntualizar que existen limitaciones: no es posible utilizar las aplicaciones en la nube si no hay conexión a Internet. Además, la calidad y la velocidad de la conexión deben ser altas para poder utilizar el servicio de forma correcta. Por norma general, las aplicaciones de escritorio (aquellos programas que están instalados en un ordenador) tienen un rendimiento mayor que las aplicaciones web debido a que aprovechan mejor todos los recursos del equipo.

2.2. ASPECTOS ECONÓMICOS

¿Es necesario llevar a cabo una gran inversión para implantar el modelo en la organización?

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.

2.3. ESCALABILIDAD Y FLEXIBILIDAD

¿Cuánto tiempo puede pasar desde que se detecta que son necesarios más recursos hasta que están disponibles?

La sencillez con la que se pueden añadir o eliminar recursos también supone una ventaja frente al modelo tradicional. Fuera de la nube, cuando un administrador del sistema necesita instalar una unidad de disco duro adicional, debe elegir el producto y seguir un protocolo para realizar la compra, recibir, instalar y configurar el equipo para su puesta a punto. Si transcurrido un tiempo el volumen de usuarios desciende o varían las funcionalidades del sistema, ya no se podrá dar marcha atrás.

Debido a la gran escalabilidad y flexibilidad del *cloud computing*, todos los proveedores de servicios ofrecen la posibilidad de añadir o eliminar recursos en cuestión de minutos, aumentando el almacenamiento o el número de procesadores sin que la aplicación se vea afectada. No hay que instalar nada en el sistema operativo, ni configurar unidades de hardware adicionales. Del mismo modo, si pasado un tiempo se detecta que el servicio en la nube no requiere tanta capacidad de procesamiento, se pueden disminuir sus recursos para adecuarlos al volumen de trabajo necesario en cada momento.

2.4. DESLOCALIZACIÓN DE DATOS Y PROCESOS

¿Sabe la empresa dónde está su información?

En un sistema informático tradicional, el administrador del sistema conoce en qué máquina se almacena cada dato y qué servidor es el encargado de cada proceso. El modelo en la nube hace uso de distintas tecnologías de virtualización para poder ofrecer todas las funcionalidades necesarias, por lo que se pierde el control sobre la localización. Esto no significa que los datos o procesos estén perdidos en Internet, puesto que el cliente mantiene el control sobre quién es capaz de acceder o modificar esta información.

La 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. 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.

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.

2.5. DEPENDENCIA DE TERCEROS

¿Pierde la empresa el control sobre su información y sus procesos?

Tanto si se trabaja con una nube pública como con una nube híbrida, existirá una empresa contratada para proveer los servicios necesarios. Los beneficios de contar con estas empresas es que se encargan de todo el mantenimiento del hardware, recintos especializados para los centros de procesamiento de datos, suministro eléctrico y conectividad a Internet, etc.

Los proveedores de servicio en la nube no solo hospedan un servidor web (como ocurre en el *hosting* tradicional), sino también todos los procesos y datos que están en la nube, además de las copias de seguridad. Es decir, que comparten parte de su control con el usuario u organización.

El establecimiento de un nivel adecuado de transparencia en el mercado a la hora de negociar los términos y condiciones en los contratos es fundamental para contrarrestar la falta de control derivada de la dependencia de terceros.

3. Marco legal

El *cloud computing* tiene su principal fundamento en la gestión remota de la información. Las organizaciones transfieren gran cantidad de información, en algunos casos sensible, en servidores pertenecientes a terceros.

Esto conlleva numerosas implicaciones jurídicas, más aún en el caso de que los datos se alojen en servidores de otro país, en la medida en que convergen dos o más jurisdicciones y surge la necesidad de determinar aspectos como la Ley aplicable, los tribunales competentes o las condiciones exigibles para que la transferencia de los datos a los sistemas del proveedor pueda ser viable y en su caso autorizada por la autoridad nacional de protección de datos. Al firmar el correspondiente contrato o términos de uso, el cliente o contratante se vincula a aceptar una jurisdicción concreta.

En el caso europeo, el marco general en cuanto a protección de datos y libre circulación de los mismos lo fija la **Directiva 95/46/CE**, en adelante la Directiva[5]. La trasposición nacional operada por cada Estado miembro obliga a tener en cuenta la Ley nacional como criterio rector.

Asimismo, existen Decisiones y Comunicaciones de la Comisión Europea y documentos adoptados por los principales actores a nivel europeo en la materia, como es el caso de la Agencia Europea de Seguridad de las Redes y de la Información (ENISA)[6] de los que se deduce el carácter fundamental del marco legal aplicable.

---

5 Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

6 Fuente: ENISA (2011). *Security and Resilience in Governmental Clouds.*

3.1. REGULACIÓN DE LA LOPD

La **Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal (LOPD)** regula los aspectos relativos al tratamiento de los datos personales y la libre circulación de los datos. La **Agencia Española de Protección de Datos (AEPD)**[7] es el órgano de control que se encarga de garantizar el cumplimiento de esta normativa dentro del territorio español[8].

En primer lugar, tanto la empresa contratante de servicios como la proveedora deben tener en cuenta la definición de dato personal que establece el artículo 3 de la LOPD: *un dato personal es cualquier información concerniente a personas físicas identificadas o identificables*.

- Si los datos con los que se va a trabajar en la nube pertenecen a esta categoría, la empresa que los trate debe cumplir con carácter previo con el conjunto de obligaciones previstas en la LOPD: la inscripción de ficheros, deberes relacionados con la información en la recogida, el consentimiento y la calidad de los datos, garantía de los llamados derechos ARCO (Acceso, Rectificación, Cancelación y Oposición) o la adopción de medidas de seguridad[9].

- Si los datos con los que se va a trabajar en la nube no son datos personales (son, por ejemplo, complejas operaciones matemáticas, cálculos físicos o químicos, etc.), se puede proceder sin que la LOPD señale impedimento alguno.

---

7 Más información: https://www.agpd.es/

8 Existen además otras Agencias de Protección de Datos de carácter autonómico, en las Comunidades Autónomas de Madrid, Cataluña y en el País Vasco.

9 Más información: Agencia Española de Protección de Datos (2008) *Guía del responsable de ficheros*.

Además, 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.**

Prestación de servicios por terceros ajenos al responsable

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 (RDLOPD)[10] 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**.

Se define un encargado del tratamiento como *la persona física o jurídica, pública o privada, u órgano administrativo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento o del responsable del fichero, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio* (artículo 5 RDLOPD).

En la siguiente tabla se recogen los principios básicos que deben reunir las cláusulas contractuales relacionadas con **el *acceso a los datos por cuenta de terceros y la seguridad de los datos***, así como la figura a quien se dirige dicha cláusula.

10 Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal o RLOPD.

Aspectos a contemplar	Artículos implicados	Contenido de las cláusulas contractuales
Acceso a los datos por cuenta de terceros	Artículo 12 LOPD Artículos 20, 21 y 22 RDLOPD	**El responsable deberá:** • Supervisar que el encargado reúne las garantías para el cumplimiento de lo dispuesto por el RDLOPD. • Incluir una descripción del conjunto de instrucciones que el encargado aplica para tratar los datos. • Establecer las medidas de seguridad que el encargado del tratamiento está obligado a implantar.
		El encargado deberá: • Utilizar los datos exclusivamente para los fines contratados. En caso contrario, se convierte en responsable y debe responder por la infracción cometida. • No comunicar esta información a terceros, ni siquiera para su conservación. • Estar autorizado por el responsable para subcontratar[11] y cumplir todos los requisitos de la LOPD y el RLOPD en esta materia. • Destruir o devolver la información tratada al responsable una vez finalizado el contrato. Cabe cumplir la obligación de devolución mediante la migración de los datos a un nuevo proveedor.
Seguridad de los datos	Artículo 9 LOPD Título VIII RDLOPD	**El responsable deberá:** • Adoptar las medidas técnicas y organizativas necesarias para garantizar la seguridad de los ficheros. • Evitar que la información se pierda o que sea accedida o tratada por personal no autorizado. • Establecer medidas de prevención frente los distintos riesgos a los que se encuentran sometidos los datos, ya provengan de la acción humana, sean tecnológicos o dependan del entorno físico o natural.

11 Se admite la subcontratación. No se considera comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento.

Debe tenerse en cuenta que la existencia del contrato regulado por el artículo 12 de la LOPD excluye la aplicación de la regulación prevista para las comunicaciones de datos personales y facilita, por tanto, el despliegue de servicios basados en el cloud computing.

La figura del encargado es contemplada de modo muy específico por el Título VIII del RDLOPD. El artículo 82 señala la necesidad de que las medidas que se fijen en el contrato tengan en cuenta de modo muy preciso la naturaleza de la prestación, si esta se desarrolla en los locales del responsable o en los del encargado y las condiciones de seguridad que afecten a un acceso remoto.

El conjunto de medidas de seguridad previstas por la ley y su reglamento tiene por objeto garantizar la integridad y la seguridad de los ficheros en los centros de tratamiento, locales, equipos y programas y de la disponibilidad de la información[12].

¿Cómo afectan el artículo 9 y 12 de la LOPD al cloud computing?

El proveedor de servicios en la nube se encarga de mantener la seguridad en sus centros de proceso de datos. Habitualmente no será posible una inspección de sus medidas de seguridad por el cliente interesado en contratar sus servicios. 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**. Por ello será fundamental para el cliente cerciorarse de que el proveedor de servicios se compromete a respetar y cumplir las obligaciones contenidas en la LOPD y la Directiva y

12 Véase la *Guía de Seguridad de Datos* (2010) y la herramienta EVALUA de la Agencia Española de Protección de Datos que permiten identificar el conjunto de medidas de seguridad previstas y testear su cumplimiento.

en especial, en lo relativo a la seguridad de los datos y el acceso a los datos por cuenta de terceros.

La dificultad en estos casos reside en que en la práctica se puede alcanzar el resultado previsto por la legislación mediante un método distinto al habitual. De acuerdo con la Ley, al aceptar los términos de uso el proveedor se convierte en encargado del tratamiento y únicamente puede tratarlos de acuerdo a las instrucciones del responsable del tratamiento (el cliente), sin aplicarlos o utilizarlos con fin distinto al establecido, ni comunicarlos a otras personas. Sin embargo, puesto que en realidad los proveedores del sector utilizan condiciones generales será necesario verificar previamente que estas se ajustan a las previsiones de la Ley española y el grado de disposición del propio proveedor a incorporar en su caso cláusulas adicionales, escogiendo entre aquellas ofertas que garanticen este cumplimiento.

Por otra parte, la adopción de medidas de seguridad y la garantía de la confidencialidad, integridad, y disponibilidad de los datos no solo tiene una dimensión relacionada con el cumplimiento normativo sino también con el prestigio y la reputación de la organización. Cuando el proveedor se encuentre sometido a la Ley española deberá garantizar el cumplimiento de la normativa, esto es el RDLOPD y, en su caso, si el cliente es una administración pública, los requisitos que deriven de los Esquemas Nacionales de Seguridad[13] e Interoperabilidad[14]. Cuando el proveedor no esté sometido a la normativa española, salvo que se trate de un país que se rija por lo dispuesto por el artículo 17 de la Directiva, es conveniente verificar que las medidas de seguridad previstas por aquél responden a los principios y objetivos de nuestra regulación.

13 Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

14 Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

Traspaso de fronteras de los datos

¿Qué debe hacer la empresa cuando los datos almacenados en la nube se encuentren en otros países?

El artículo 33 y el artículo 34 del Título V de la LOPD sobre *Movimiento Internacional de Datos y el RDLOPD* responden a este interrogante. El mercado del *cloud computing* es global, puesto que es habitual que los datos se ubiquen fuera de España e incluso en varios países distintos.

La transferencia internacional de datos se define como el *tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo, bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español.*

En el caso en el que el encargado se encuentre establecido y/o usando medios para el tratamiento de datos en un Estado miembro, el responsable debe aplicar las obligaciones de seguridad tal como las define la legislación del Estado miembro del encargado, con independencia de los pactos alcanzados por ambas partes[15].

La transferencia internacional de datos obliga a distinguir entre los países integrados en el Espacio Económico Europeo y terceros estados ajenos a éste ámbito geográfico. En el primer caso, rigen las reglas ordinarias sobre el encargado del tratamiento. En caso de que la prestación se realice en países ajenos al Espacio Económico Europeo, operará el régimen previsto por los artículos 33 y 34 de la LOPD.

15 Conforme al artículo 17.3 de la Directiva **95/46/CE** (en relación con su artículo 4).

Artículos implicados	Contenido del artículo
Artículo 33 LOPD	No se permite la trasferencia temporal ni definitiva de datos de carácter personal a otros países que no brinden un nivel de protección equiparable al de la LOPD.
Artículo 34 LOPD	En ocasiones se permite esta transferencia previa autorización administrativa del Director de la Agencia Española de Protección de Datos (AEPD)[16]. Dicha autorización no es necesaria: • En los supuestos excepcionales del artículo 34.a al 34.j de la LOPD. • En el caso de los países respecto de los que la Comisión ha declarado que considera adecuado el nivel de protección de datos personales[17].

Cuando no se den estas circunstancias será necesario obtener la autorización del Director de la AEPD siguiendo el procedimiento previsto por la Sección Primera, del Capítulo V del Título IX del RDLOPD. Es muy importante tener en cuenta que cuando el contrato siga los criterios fijados en los distintos modelos de cláusulas contractuales tipo establecidas mediante Decisiones de la Comisión Europea[18], el artículo 70.2 del RDLOPD apunta que *se considerará que establecen las adecuadas garantías*.

16 Según el procedimiento previsto en la Sección Primera, del Capítulo V del Título IX del RDLOPD.

17 Estos son: Suiza, Argentina, Guernsey, Isla de Man, Jersey, Islas Feroe, Andorra, Israel. Existen dos países con ciertas particularidades. Canadá en el que se consideran seguras las organizaciones sometidas a la ley canadiense de protección de datos, y Estados Unidos, respecto de las empresas que hayan suscrito *"Safe Harbour"*, esto es los principios de Puerto Seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de los Estados Unidos.

18 En concreto, las Decisiones de la Comisión Europea aludidas son:

- Decisión 2001/497/CE de la Comisión, de 15 de junio de 2001, relativa a 'Cláusulas contractuales tipo para la transferencia de datos personales a un tercer país previstas en la Directiva 95/46/CE.
- Decisión 2002/16/CE de la Comisión, de 27 de diciembre de 2001, relativa a 'Cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE. (queda derogada a partir de 15 de mayo de 2010).
- Decisión 2010/87/UE de la Comisión, de 5 de febrero de 2010, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo.

3.2. REGULACIÓN DE LA LSSI

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.

3.3. REGULACIÓN DEL CÓDIGO PENAL

El abanico de cuestiones que plantea en un entorno de *cloud* puede ser muy complejo, si bien en este apartado se analiza de forma particular el delito de estafa.

Las características del modelo en la nube, como la deslocalización y la transferencia a terceros de datos y procesos, pueden invitar a posibles estafadores a crear sitios web falsos en la nube para apropiarse de información sensible volcada por los usuarios o distribuir malware en este entorno para llevar a cabo ataques de fraude online.

El Código Penal regula el delito de estafa en el artículo 248 (reformado recientemente según la **Ley Orgánica 5/2010, de 22 de junio**) y en concreto establece que:

1. Cometen estafa los que, engañen a otro con ánimo de lucro, induciéndole a realizar un acto en perjuicio propio o ajeno.

2. Igualmente se consideran estafadores:

    a. Los que, con ánimo de lucro y valiéndose de alguna manipulación informática o similar, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro, incluyendo la información dentro de esta categoría.

    b. Los que fabriquen, introduzcan, posean o faciliten programas informáticos específicamente destinados a la comisión de fraude.

    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.

En función del importe de lo defraudado, el quebranto económico causado a la víctima, las relaciones entre esta y el defraudador, los medios empleados por éste y el resto de posibles circunstancias que sirvan para valorar el hecho, se imponen diferentes sanciones al estafador, como recoge dicho texto legal.

3.4. EL SISTEMA JURÍDICO DE LOS PAÍSES DE DESTINO

La elección del país de destino de los datos que sean objeto de una prestación basada en el *cloud computing* no solo debe tener muy en cuenta las normas que regulan las tecnologías de la información y las comunicaciones, sino el conjunto del Ordenamiento jurídico. La Constitución Española y los Tratados de la Unión Europea se enmarcan en una tradición constitucional que salvaguarda los derechos fundamentales de las personas.

Por ello, ubicar los datos en un país en el cual estos derechos no resulten garantizados contraviene de algún modo el espíritu del modelo constitucional español y del modo de concebir los derechos humanos. Precisamente por ello, el artículo 37.1.f y el artículo 70.3 RDLOPD **permiten denegar o suspender temporalmente una transferencia** cuando *la situación de protección de los derechos fundamentales y libertades públicas en el país de destino o su legislación impidan garantizar el íntegro cumplimiento del contrato y el ejercicio por los afectados de los derechos que el contrato garantiza*.

Por otra parte, en ocasiones los países de destino pueden conferir facultades extraordinarias a sus servicios de inteligencia, o a sus fuerzas y cuerpos de seguridad, para el acceso a la información contenida en servidores bajo su jurisdicción.

Con independencia de que en la mayor parte de las ocasiones probablemente se trate de medidas perfectamente reguladas y conformes con nuestros

valores constitucionales**, la posible intensidad de las mismas debería ser contemplada en el análisis de riesgos previo a la ubicación no ya solo de datos personales, sino también de aquella información y recursos que la organización desee salvaguardar frente a cualquier acceso externo** (Ver apartado 5.2 *Seguridad por parte del cliente*).

4. Riesgos del *cloud computing*

Como toda tecnología, el *cloud computing* no está exento de riesgos. Cuanto más compleja es la infraestructura informática utilizada, más posibles vulnerabilidades aparecen. A continuación se describen los principales riesgos de seguridad y privacidad que pueden generar un impacto en los recursos en la nube[19]:

4.1 ABUSO Y USO MALINTENCIONADO

El *cloud computing* ofrece un gran número de ventajas y oportunidades que también están siendo aprovechadas por los piratas informáticos. Ataques como el robo de contraseñas[20], envío de spam, granjas de *captchas*[21] o ataques de denegación de servicio distribuido[22] se vuelven mucho más sencillos y baratos.

Los ciberdelincuentes pueden planear sus ataques contratando servicios en la nube para posteriormente ejecutarlos en cuestión de horas. Además, los recursos que utilicen se borrarán una vez concluya el ataque, lo que dificulta mucho su persecución.

Del mismo modo, pueden contratar servicios de almacenamiento en la nube para guardar datos maliciosos o robados. De esta forma, dificultan que las

---

19 Fuente: Banegas, M. (Telefónica España Grandes Clientes) Presentación *Seguridad en Cloud Computing*. ENISE 4 (2010).

20 El *password cracking* es un proceso informático que consiste en descifrar la contraseña de determinadas aplicaciones para conseguir un acceso no autorizado.

21 *Captcha* es el acrónimo de *Completely Automated Public Turing test to tell Computers and Humans Apart* (Prueba de Turing pública y automática para diferenciar máquinas y humanos). Se trata de una prueba desafío-respuesta utilizada en computación para determinar cuándo el usuario es o no humano.

22 En inglés, *Distributed Denial of Service* (DDOS). La denegación de servicio distribuida consiste en atacar a un sistema informático para consumir todos sus recursos (por ejemplo el ancho de banda) impidiendo el acceso a usuarios legítimos.

autoridades puedan acceder a esta información (por la complejidad que supone) para actuar contra los atacantes.

4.2. FUGAS INTERNAS DE INFORMACIÓN

La amenaza también puede provenir de la propia empresa, bien por errores humanos, bien por acciones deliberadas de los usuarios del *cloud*. Estos incidentes desencadenan pérdidas de información, con los consiguientes daños en la imagen de la empresa y las posibles consecuencias legales y/o jurídicas. Para evitar estas situaciones, las organizaciones utilizan medidas como la incorporación de cláusulas de confidencialidad en los contratos laborales o el establecimiento de políticas de seguridad.

4.3. APIS INSEGURAS

Las APIs[23] son el único punto de interacción con los programas que se están ejecutando en la nube. Al ser las puertas de entrada hacia los servicios en la nube, se convierten en un punto crítico de la seguridad y privacidad del sistema.

Cada proveedor de servicios en la nube ofrece sus propias APIs de conexión que permiten desde arrancar o parar los servicios en la nube hasta aumentar o disminuir los recursos de los mismos.

Sin una correcta política de seguridad, las APIs pueden sufrir ataques de malware para que realicen acciones adicionales o diferentes para las que originalmente fueron programadas. Con ello, los atacantes persiguen el robo y/o acceso a la información de la víctima.

---

23 *Application Programming Interface.* Una interfaz de programación de aplicaciones es el conjunto de funciones y procedimientos que ofrecen las bibliotecas para ser utilizados por otro software como una capa de abstracción.

4.4 SUPLANTACIÓN DE IDENTIDAD

La suplantación de la identidad es un riesgo presente tanto en los sistemas informáticos tradicionales como en el modelo de *cloud computing*. Sin embargo, tiene una especial relevancia en éste último.

En la mayoría de los sistemas informáticos es necesario identificarse antes de realizar cualquier tarea. Habitualmente, esta identificación se produce mediante la combinación del nombre de usuario y una clave secreta o *password*.

Dependiendo del uso que se esté haciendo del *cloud computing*, esta combinación tradicional de usuario y contraseña puede no resultar lo suficientemente robusta. Es necesario investigar otros sistemas mucho más seguros para evitar la suplantación de identidad en la Red.

Una solución para incrementar la seguridad es la utilización del DNI electrónico como mecanismo de identificación, ya que incluye medidas criptográficas y biométricas como complemento a las tradicionales medidas de seguridad.

Imagen DNI electrónico

4.5. DESCONOCIMIENTO DEL PERFIL DE RIESGO

La gestión de la seguridad en los entornos informáticos tradicionales se ha estudiado durante mucho tiempo. Es relativamente sencillo aplicar soluciones informáticas para aumentar la seguridad, dificultando las entradas no autorizadas o disminuyendo las vulnerabilidades del sistema.

Sin embargo, el *cloud computing* entraña una evolución no conocida anteriormente. Ofrece nuevas funcionalidades e incrementa las oportunidades de negocio, pero a su vez es un modelo que puede ser explotado por nuevas amenazas en la Red.

Esto no significa que sea menos seguro que los modelos anteriores, simplemente que hay menos experiencia de ataques y los expertos en seguridad estudian los nuevos *modus operandi* de los usuarios malintencionados a la vez que los posibles fallos de diseño.

De entre estas preocupaciones, los expertos destacan **el uso de tecnologías compartidas**[24]. Especialmente, en cuanto al aislamiento necesario de la información de diferentes usuarios en una misma infraestructura. Ante esto, los proveedores de servicios *cloud* deben mantener sus esfuerzos para asegurar un servicio sin fisuras en el que cada usuario tenga acceso únicamente a su propia información.

24 Fuente: INTECO-CERT (2011). *Riesgos y amenazas en cloud computing*.

5. Seguridad en la nube

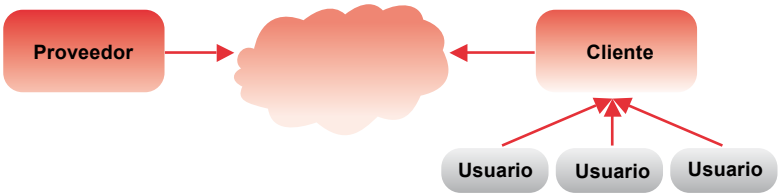
Utilizar los servicios en la nube conlleva un cambio en la forma de entender la seguridad informática. Deja de existir la imagen tradicional en la que todos los servidores de la empresa están en el sótano del edificio donde solo pueden acceder los administradores informáticos. Al hacer uso del *cloud computing* una parte importante de la seguridad del sistema recae sobre la empresa que provee los servicios en la nube.

Para entender el modelo de seguridad de la información aplicado en este modelo es necesario conocer los distintos actores que participan en él:

- **Proveedor de servicios en la nube**: empresa que dispone de la infraestructura informática necesaria para hospedar los programas siguiendo el modelo de *cloud computing*.

- **Cliente**: persona, organización o empresa que contrata los servicios en la nube. El cliente es quien paga cierta cantidad de dinero para beneficiarse de las prestaciones de la computación en la nube. El usuario final, o la persona o grupo de personas que utiliza el programa, puede ser distinto al cliente. Por ejemplo, una empresa puede contratar servicios en la nube para hospedar un servidor web al que accederán sus empleados, como se muestra en la siguiente imagen.

Ejemplo de participantes en el *cloud computing*



Los mecanismos de seguridad que se pueden aplicar para proteger los datos alojados en la nube deben considerarse como un **trabajo colaborativo entre las dos partes (proveedor de servicios en la nube y cliente**), ya que ambas deben asumir unas responsabilidades. La realización de auditorias de seguridad conjuntas es una buena práctica para revisar que todo el sistema está protegido frente a posibles amenazas.

5.1. SEGURIDAD POR PARTE DEL PROVEEDOR DE *CLOUD COMPUTING*

El proveedor de servicios en la nube se encarga de garantizar la seguridad física en sus centros de procesos de datos. Deberá impedir que personas no autorizadas entren en dichos edificios para, por ejemplo, robar sus equipos. Del mismo modo, deberá mantener sus equipos actualizados tanto a nivel hardware como software para hacer frente a las amenazas existentes en Internet.

El proveedor utiliza mecanismos como la virtualización y la segmentación de datos para reforzar la seguridad de sus servicios en la nube.

- La **virtualización** puede ser vista como una forma de aumentar la seguridad de los procesos que se ejecutan en la nube. Varias máquinas virtuales pueden ser ejecutadas en un único servidor pero cada máquina virtual ejecuta un sistema operativo de forma aislada. El espacio de memoria y disco están controlados por un hipervisor[25]

25 Hipervisor: plataforma de virtualización que permite utilizar, al mismo tiempo, diferentes sistemas operativos.

que impide que los procesos ejecutados en distintas máquinas virtuales puedan interactuar entre ellos.

El mayor riesgo al que debe enfrentarse el proveedor de servicios en cuanto a este mecanismo es el control y eliminación del software malintencionado que pretenda burlar las protecciones del hipervisor para tener acceso a otras máquinas virtuales o incluso al sistema anfitrión.

- La deslocalización de los datos es una característica que también puede ser explotada como un mecanismo de seguridad en sí misma. La **segmentación de datos** permite que los datos de un cliente residan en diferentes servidores, incluso en diferentes centros de datos. De esta forma se protegen dichos datos frente a un hipotético robo en las instalaciones del proveedor de servicios.

  Además, al poder mantener los datos en varias localizaciones de forma simultánea, se dispone de un sistema de copias de seguridad prácticamente en tiempo real. Así, ante fallos de seguridad, se puede recuperar rápidamente la actividad, permitiendo la continuidad del negocio.

5.2. SEGURIDAD POR PARTE DEL CLIENTE

Por su parte, el cliente es responsable de mantener el sistema operativo actualizado e instalar los parches de seguridad que aparezcan. Igualmente es necesario mantener políticas de seguridad tradicionales como el control de usuarios, el borrado de cuentas de usuario que ya no se utilizan, o la revisión del software para comprobar que no tiene vulnerabilidades, entre otras.

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.

- Por parte del cliente, uno de los pilares de la seguridad informática es el **control perimetral**. Para llevarlo a cabo, es recomendable la instalación y configuración de un firewall o cortafuegos, aplicación informática que se encarga de monitorizar todas las comunicaciones que se realizan desde o hacia el equipo o la red y decide si las permite dependiendo de las reglas establecidas por el administrador del sistema.

  Para añadir otro nivel de seguridad de red, es igualmente recomendable la instalación y configuración de un *Intrusion Detection System* o IDS[26]. Un IDS es aquella aplicación informática que no solo bloquea o permite conexiones sino que analiza dichas conexiones para detectar si alguna de ellas es portadora de contenido peligroso para el equipo o para la red. Además es capaz de categorizar las distintas amenazas e informar al administrador del sistema siguiendo una lista de reglas y heurísticas.

- La **criptografía** es otro de los mecanismos que va a jugar un papel protagonista en el uso de los servicios en la nube. La criptografía proporciona un nivel superior de seguridad en tres aspectos principales:

  1. **Protección de las conexiones de Red entre los usuarios y las aplicaciones en la nube.** El uso de *Secure Sockets*

26 *Intrusion Detection System* o Sistema de Detección de Intrusiones.

Layer (SSL)[27] y *Transport Layer Security* (TLS)[28] permiten que todos los datos que viajen desde el servidor en la nube hasta el usuario estén cifrados impidiendo su acceso a terceras personas incluso cuando se utiliza una red Wi-Fi no segura.

Certificado SSL de *Amazon.com*

2. **Protección de las conexiones entre los administradores del sistema y los servicios de la nube**. En este caso, el uso de *Secure Shell* (SSH)[29] y *Virtual Private Network* (VPN)[30] permitirá a los administradores del sistema o desarrolladores de las aplicaciones mantener una canal seguro de comunicación con los sistemas en la nube.

---

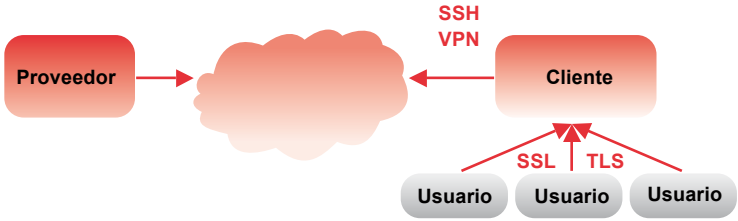
27 *Secure Sockets Layer:* Protocolo de Capa de Conexión Segura. Proporciona autenticación y privacidad de la información entre extremos sobre Internet mediante el uso de criptografía.

28 *Transport Layer Security:* Seguridad de la Capa de Transporte. Consiste en un protocolo criptográfico que proporciona comunicaciones seguras a través de Internet. TLS es un protocolo independiente que permite a los protocolos de niveles superiores actuar por encima de él de manera transparente. Basado en SSL de Netscape 3.0, TLS supone la evolución de su predecesor, si bien no son operables entre sí.

29 *Secure Shell:* Intérprete de órdenes segura. Es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red.

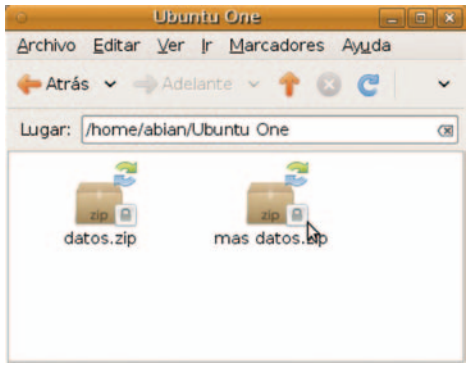
30 *Virtual Private Network:* Una Red Privada Virtual. Es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet.

Ejemplo de participantes en el *cloud computing*



3. **Protección de los datos utilizando criptografía**. Si se utiliza la nube como un sistema de almacenamiento de datos es muy recomendable utilizar un nivel de cifrado adecuado para aquellos datos sensibles que vayan a ser depositados allí. De esta forma, si algún usuario no autorizado intercepta los datos o tiene acceso al sistema de ficheros de la nube, no podrá leer el contenido allí depositado sin conocer la clave de cifrado.

Utilización de archivos cifrados en Ubuntu One



- La única manera de comprobar la actividad informática, detectar incidentes y formular un plan de acción para evitar que vuelvan a suceder en el futuro es **gestionar los logs[31] del sistema**. Aunque es muy posible que no se tenga acceso a toda la información sobre los eventos del sistema, el cliente debe almacenar y revisar todos los logs que estén bajo su responsabilidad. Por ejemplo, el registro de usuarios que acceden a la aplicación, manipulan o borran ficheros en la máquina virtual, o el registro de conexiones potencialmente peligrosas detectadas por el IDS y por el cortafuegos.

  Además, es recomendable realizar copias de seguridad frecuentes de estos logs e incluso almacenarlos en una máquina distinta ya que si un atacante se hace con el control del sistema en la nube podría destruir los ficheros de registro borrando así sus huellas.

31 Log: fichero de texto en el que queda recogida toda la actividad que tiene lugar en un determinado ordenador, permitiendo para ciertos programas que su propietario o administrador detecte actividades ilícitas e identifique, por medio de su dirección IP, al usuario correspondiente..

6. Privacidad en la nube

La información es el activo más importante de las organizaciones. Asegurar la privacidad de la información durante su ciclo de vida es crucial a la hora de utilizar servicios de *cloud computing*.

6.1. PROTECCIÓN DE DATOS

El ciclo de vida que siguen los datos que son procesados en la nube es el siguiente:

- **Los datos son preparados para poder adaptarse a la nube** adaptando su formato o creando un fichero que contenga toda la información necesaria.

- **Los datos "viajan" a la nube a través de una conexión a Internet,** mediante un correo electrónico, una aplicación específica para importarlos o la transferencia a la nube de la copia de seguridad obtenida de un servidor en la organización.

- **Los datos son procesados en la nube,** desde su almacenamiento hasta el cálculo de complejas operaciones matemáticas. Es importante mencionar que los datos 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, el resultado debe volver al usuario con el valor añadido de la información generada en la nube.

El mero hecho de que los datos abandonen la organización pueden constituir un riesgo desde el punto de vista de la privacidad: un usuario malintencionado podría interceptar los datos mientras están siendo transferidos por Internet. Incluso si no son interceptados, están siendo

almacenados y procesados en una infraestructura informática ajena al control del usuario.

> El hecho de que los datos abandonen la organización puede constituir un riesgo desde el punto de vista de la privacidad.

Los mecanismos para minimizar estos riesgos de privacidad son muy sencillos. Antes de migrar los procesos a la nube conviene preguntarse: "¿Es realmente necesario que todos los datos de la organización pasen a estar en la nube?". El siguiente ejemplo aclara este interrogante.

Una empresa encargada de tramitar las nóminas de empleados decide utilizar servicios en la nube. Esta empresa tiene bases de datos de miles de trabajadores con DNI, nombre, dirección postal, sueldo bruto, puesto de trabajo, porcentaje de retenciones, número de horas trabajadas, etc. La operación matemática que esta empresa desea realizar en la nube es el cálculo del sueldo neto que debe ser entregado a cada empleado a final de mes. ¿Es necesario que todos los datos de los empleados sean migrados a la nube? ¿Realmente se necesita el DNI de un empleado para descontarle el porcentaje de IRPF?

Una solución segura es enviar a la nube solo los datos necesarios para realizar el cálculo del salario que son el sueldo bruto y el porcentaje de retenciones. En lugar de enviar a la nube el nombre o el DNI para identificar al trabajador, se crea un nuevo identificador (por ejemplo un número) que permite asignar correctamente el nuevo valor a cada trabajador. De este modo, se impide a un posible atacante que intercepte las comunicaciones traducir esos datos. Además, el proveedor de servicios en la nube nunca tendrá datos sensibles en sus sistemas, solo contendrá valores matemáticos sin saber a quién pertenecen o qué contienen.

6.2. INTEGRIDAD

Mantener una correcta integridad de los datos significa que estos permanecen idénticos durante las operaciones de transferencia, almacenamiento o recuperación. En el ámbito del *cloud computing*, la integridad de los datos es especialmente crítica: los datos están siendo transferidos constantemente entre los servicios en la nube y los distintos usuarios que acceden a ellos.

Debido a las características de la computación en la nube, varios usuarios pueden estar accediendo simultáneamente y modificando determinada información. Por ello, deben implementarse los mecanismos que garanticen la correcta integridad de los datos.

La mayor amenaza para la integridad de los datos en la nube es que los datos se acaben corrompiendo debido a errores en su manipulación. Si no se detecta que ha habido un problema en la transferencia y los datos se almacenan erróneamente, la próxima vez que el usuario quiera acceder a ellos no podrá utilizarlos.

Para evitar que los datos en la nube no puedan utilizarse o que no estén disponibles se utilizan principalmente tres mecanismos: control de integridad, gestión de cambios y copias de seguridad.

- **El control de integridad** hace uso de funciones matemáticas (funciones resumen o *hash*) para verificar que los datos no han sufrido modificaciones durante su traslado. El proceso consiste en obtener un valor para la función *hash* antes de mover el dato y otro cuando se ha terminado de mover. Si dichos valores no coinciden es que ha habido un problema en la transacción y debe ser repetida. En el caso del *cloud computing* no se utilizan funciones resumen solo para ficheros, sino también para máquinas virtuales completas o para las copias de seguridad.

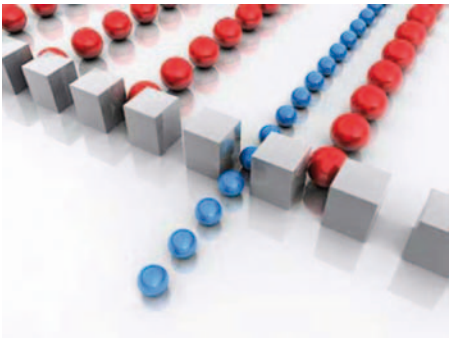
- **La gestión de cambios** mantiene un historial de modificaciones de los datos o ficheros almacenados en la nube. Cada modificación lleva asociada un sello de fecha y el usuario que lo produjo. Si se detecta que varios usuarios han modificado el recurso a la vez se puede analizar el sello de fecha para comprobar qué versión tiene validez. Del mismo modo, si se detecta un error de integridad en el recurso se puede volver a una versión anterior que sea correcta.

- **Las copias de seguridad** son la última línea defensiva para garantizar la integridad de los datos. Utilizando adecuadamente las herramientas en la nube se pueden programar copias de seguridad cada cierto tiempo. Si se detecta un fallo de integridad a nivel general, la única forma de solucionarlo es volver a una versión anterior del sistema almacenada en la copia de seguridad.

6.3. CONTROL DE ACCESO

Igual que sucede con las arquitecturas tradicionales, el control de acceso también juega un papel importante en el *cloud computing*. Aunque esta tecnología se represente informalmente como una nube a la que se conecta todo el mundo desde sus equipos (tanto fijos como dispositivos móviles), no significa en absoluto que cualquier persona pueda acceder a cualquier dato o proceso en la nube.

Es necesario distinguir claramente entre los servicios que se ofrecen de forma libre y gratuita en la nube y la utilización de recursos en la nube para fines personales o empresariales.



Se pueden utilizar sistemas de correo electrónico en la nube, como Gmail o MSN Hotmail, y eso no significa que cualquier persona pueda leer el correo de otra libremente. Aunque tal vez el ejemplo más completo para hablar del control de acceso en la nube sea Picasa. Picasa es un sistema de almacenamiento y organización gratuito de fotos en la nube. Cuando se va a crear un nuevo álbum de todos, el usuario tiene la posibilidad de elegir si esas fotos serán públicas y visibles para todo el mundo, solo podrán ser vistas por un conjunto de personas o si es una galería privada a la que solo el usuario tendrá acceso. En este caso concreto, es el usuario de Picasa el que establece la política de control de acceso utilizando el sistema como un expositor de imágenes para todo el mundo o como un sistema de backups privado de fotos.

Extendiendo el ejemplo anterior, cuando una empresa o entidad utiliza las capacidades de la computación en la nube, necesita que el administrador del sistema establezca un correcto control de acceso ***para garantizar que los usuarios solo utilizan los datos o procesos para los que han sido autorizados.***

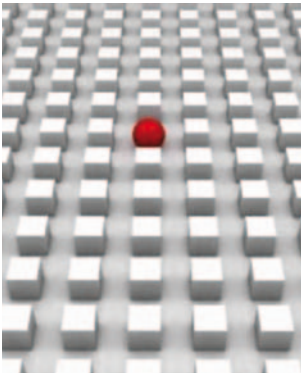
6.4. PREVENCIÓN FRENTE A PÉRDIDA

Uno de los mayores riesgos a los que se enfrenta todo sistema informático es la pérdida de datos, ya sea porque un usuario ha borrado información accidentalmente, porque haya un fallo en algún dispositivo hardware o por culpa de un ataque informático. Perder los datos no solo significa tener que rehacer parte del trabajo realizado, sino que en muchos casos puede significar cuantiosas pérdidas económicas. La solución a este problema se enfoca desde dos puntos de vista principales.

- Por un lado, una correcta **política de seguridad** limita la libertad de los usuarios para borrar elementos del sistema, protege los equipos ante el ataque de software malintencionado y además impide que personas ajenas a la organización accedan o corrompan los datos. El proveedor de servicios se encarga de solucionar todos los problemas relacionados con los componentes electrónicos. Si detecta un fallo en uno de los equipos dentro de sus instalaciones, automáticamente lo aísla y todos los procesos que se ejecutan en él se migran a otra máquina que no tenga problemas. Este proceso puede durar tan solo unos minutos e incluso realizarse sin cortar el servicio, permitiendo una disponibilidad ininterrumpida de los servicios en la nube.

- Por otra parte, una correcta **política de copias de seguridad** permite recuperar los datos aún cuando todas las medidas de seguridad han fallado o cuando se produce una avería en un componente hardware. Todos los proveedores de servicios en la nube ofrecen sistemas de copias de seguridad de forma completamente transparente para el usuario. Tan solo es necesario seleccionar los activos que se quieren proteger y la periodicidad con la que se desean estas copias. La recuperación frente a un ataque puede ser tan sencilla como la restauración de un *snapshot* (copia instantánea de volumen) anterior de la máquina virtual.

Las características anteriormente expuestas permiten disponer de un sistema robusto preparado para realizar una correcta recuperación frente a desastres, es decir, **asegurando la continuidad del negocio**.

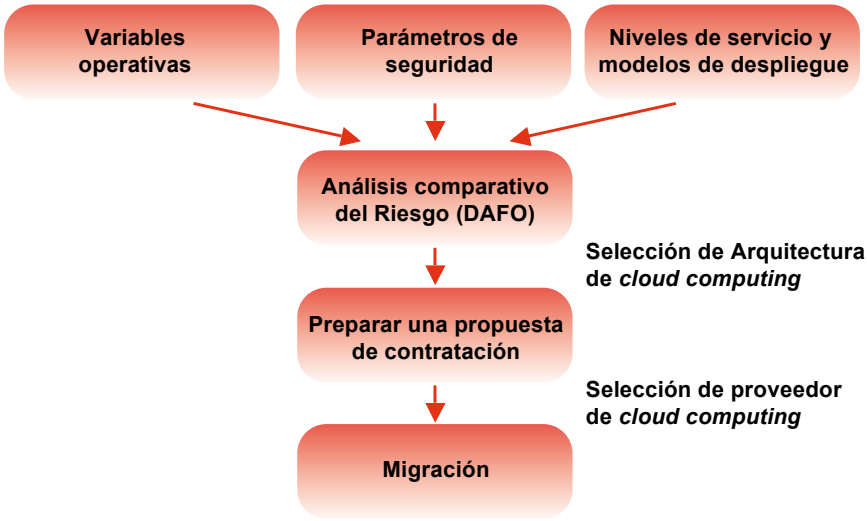


Por último, existe otra ventaja relativa a los dispositivos portátiles, cada vez más utilizados en las empresas y desde los que se accede a la información de la organización: ordenadores portátiles, USBs, móviles, etc. Estos dispositivos pueden ser robados u olvidados exponiendo grandes cantidades de datos a personas completamente ajenas a la organización. Si se utilizan sistemas en la nube, aunque se pierda un teléfono móvil o alguien robe un portátil, la información permanecerá inaccesible para terceros.

7. Pasos para entrar en la nube

Una vez que se ha entendido cómo funciona el *cloud computing* y las distintas posibilidades que ofrece, es el momento de pensar en si realmente la empresa o entidad se pueden beneficiar de ellos. Un posible esquema para la toma de decisiones es el siguiente[32]:

Esquema de toma de decisiones



Los siguientes apartados incluyen los distintos pasos que se deben seguir para "dar el salto" a la nube:

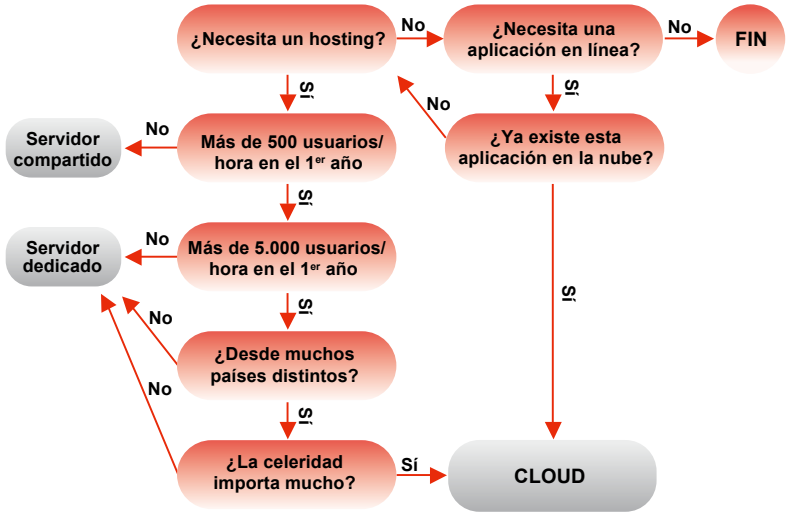
32 Ver nota al pie 6.

7.1. ANÁLISIS DE NECESIDADES Y OPORTUNIDADES

En primer lugar, la empresa o entidad debe observar:

- **Las características de su actividad:**
  - Áreas de negocio adecuadas para la migración.
  - Conjunto de usuarios que se aprovecharán de las oportunidades del *cloud computing*. Por ejemplo, personas que trabajan en remoto o usuarios que viajan mucho. Se debe tener en cuenta las necesidades de dicho grupo de usuarios y las posibilidades de que se adapten bien a las soluciones basadas en la nube.

Ejemplo de valoración de variables operativas



- Presupuesto: utilizando las aplicaciones en la nube se puede ahorrar una cantidad importante de dinero en la compra de licencias de software. Por lo tanto, un buen punto de partida podría ser la utilización de suites ofimáticas en la nube en lugar de comprar e instalar una suite ofimática por cada equipo de la organización.

- **Los parámetros de seguridad y tolerancia a fallos** que cada organización debe definir en su modelo ideal de *cloud computing* se estructuran en cuatro categorías:

  - Preparación de la organización para proporcionar un nivel aceptable de servicio a la vez que protegen la confidencialidad e integridad de la información.

  - Entrega del servicio: capacidad de los sistemas para proporcionar los servicios de acuerdo con los requisitos establecidos en el acuerdo de servicio.

  - Respuesta y recuperación: criterios para medir la capacidad del sistema para restaurarse en caso de incidentes o fallos.

  - Cumplimiento legal y normativo específico.

- **Niveles de servicio y modelos de despliegue.** En base a los apartados 1.3 *Niveles del servicio* y 1.4 *Modelos de despliegue de servicios.*

En base a los parámetros establecidos, se lleva a cabo un **análisis DAFO**, para identificar las debilidades, amenazas, fortalezas y oportunidades de cada modelo de nube para la organización. Este análisis debe ser un mínimo que la entidad puede complementar con métodos más exhaustivos, como el análisis de riesgos.

Con este análisis, la organización debe obtener la información para identificar el modelo de nube más apropiado para cada circunstancia.

7.2. OFERTA DE SERVICIOS EN LA NUBE

Si se decide que las características del negocio o entidad requieren una solución basada en el *cloud computing*, el siguiente paso obligatorio es estudiar cuidadosamente las distintas opciones existentes en el mercado.

Hay muchas empresas especializadas en servicios de *cloud hosting* que llevan años trabajando con esta tecnología, mientras que hay empresas de *hosting* tradicional que empiezan a ofertar distintos paquetes de funcionalidades en la nube. Por otra parte, las grandes multinacionales del software como Microsoft, Amazon o Google disponen de una gran oferta de servicios en la nube que pueden ser aplicados rápidamente a las necesidades concretas del cliente.

7.3. RESPONSABILIDAD Y TÉRMINOS DE USO

Como en todo acuerdo empresarial, la relación entre el proveedor de servicios en la nube y el cliente (en este caso, el contratante) debe estar regulada por un contrato. Este **contrato** debe definir claramente la posición de cada una de las partes así como sus responsabilidades y obligaciones.

Los **términos de uso** se encargan de definir las especificaciones técnicas más importantes relacionadas con la entrega y la calidad del servicio. Estas últimas establecen los niveles de rendimiento y disponibilidad garantizados por el proveedor.

Es importante puntualizar que en otro tipo de acuerdos comerciales, los contratos siempre se negocian. En el caso de los proveedores de servicios en

la nube no existe tal acercamiento de posiciones. Estas empresas muestran claramente las condiciones en las que prestan su servicio y **es el cliente el que debe estudiar cuidadosamente** cada una de ellas hasta encontrar la que mejor satisface sus necesidades.

Las partes del contrato en las que el cliente debe centrar su atención son las siguientes:

- **Acuerdos de Nivel de Servicio** *(Service Level Agreements, SLAs)* con sus correspondientes informes periódicos.

- **Confidencialidad:** fundamentalmente en las operaciones de traslado de datos y almacenamiento en servidores.

- **Disponibilidad**. Esta cláusula especifica el nivel de disponibilidad que el proveedor de servicios se compromete a mantener. Normalmente todos los proveedores de servicio mantienen un nivel de disponibilidad cercano al 100%, aunque es probable que alguno lo muestre en horas mensuales.

- **Rendimiento**. Este apartado asegura que se alcanzan los niveles de potencia de cálculo, almacenamiento y ancho de banda contratados con el proveedor de servicios.

- **Seguridad**. El proveedor de servicios se compromete a mantener un nivel de seguridad suficiente en sus instalaciones para albergar sus datos y procesos, por lo que debe dar al cliente una lista de las medidas de seguridad que está aplicando en sus sistemas. El cliente debe prestar especial atención a esta sección porque tiende a ser algo vaga por parte de los proveedores de servicio, pero debe contener una Política de gestión de copias de seguridad y Gestión de Incidentes. Es conveniente que el proveedor cuente con un

Plan de Continuidad de Negocio y Recuperación ante desastres operativo y actualizado.

- **Pagos**. Esta sección contiene los detalles de los pagos que debe realizar el cliente para disfrutar de los servicios contratados. Debe incluir claramente la cantidad y la periodicidad de dichos pagos.

- **Suspensión del servicio**. Esta cláusula está más relacionada con los contratos en los que solo existe un único servidor. En el caso del *cloud computing* se podría eliminar, pero las grandes empresas lo mantienen para indicar al cliente que es posible que se suspenda momentáneamente el servicio debido a actualizaciones en su infraestructura informática.

- **Servicios de soporte**. Esta sección contendrá los compromisos del proveedor de servicios en cuanto al soporte prestado al cliente. Es importante que el contrato especifique el tiempo que el proveedor requiere para recuperar el sistema cuando se ha producido un error.

- **Terminación o modificación**. Las características del *cloud computing* permiten una gran flexibilidad a la hora de modificar los servicios que el cliente necesita. El acuerdo legal debe contener claramente las opciones de modificación del contrato o terminación del mismo, sobre todo en lo relativo a recuperación y borrado de la información.

- **Privacidad y cumplimiento normativo**. Esta cláusula define el nivel de compromiso del proveedor de servicios con el cumplimiento de las leyes propias de su territorio y de ajustarse a las normas vigentes en el territorio español o europeo, en especial las relativas a la privacidad y protección de datos. En cualquier caso, el contenido del contrato debe permitir establecer con precisión los compromisos de cumplimiento normativo que asume el proveedor

7.4. UTILIZACIÓN DE MECANISMOS DE MIGRACIÓN

Lo más importante a la hora de utilizar los servicios en la nube es tener claro qué parte de los activos informáticos van a ser transferidos. Para ello, conviene hacer un estudio de las implicaciones de migrar todos los datos y procesos a la nube. En dicho estudio se debe sopesar la cantidad y sensibilidad de los datos manejados. Siempre se debe procurar que los datos más sensibles estén sometidos al más estricto control para evitar que sean accedidos por personas sin la debida autorización.

El proceso de migración puede ser secuencial:

- Durante los primeros momentos de uso del *cloud computing*, una opción recomendable es **no migrar a la nube los datos o procesos más sensibles**, mientras que las aplicaciones más pesadas se trasladan a la nube. Por ejemplo, se puede instalar el servidor web y correo en la nube pero mantener el servidor de bases de datos en local.

- 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. Cada uno de los proveedores de servicios en la nube tiene un sistema propio de migración. En algunos es suficiente enviar un email a una dirección concreta con los

datos que se desean migrar para que todo funcione correctamente mientras que en otros casos hay una interfaz web en la que se realiza la configuración.

- Para permitir la correcta continuidad de negocio es muy importante **mantener una copia completa del sistema en el modelo tradicional durante un tiempo**. En caso de que se detecten problemas después de realizar la migración a la nube, se puede volver al modelo tradicional. De esta forma, se puede trabajar en la correcta integración de las aplicaciones en el nuevo modelo de forma trasparente para los usuarios.

OBSERVATORIO INTECO

Síguenos a traves de:

Web **http://observatorio.inteco.es**

Perfil Facebook ObservaINTECO
http://www.facebook.com/ObservaINTECO

Perfil Twitter ObservaINTECO:
http://www.twitter.com/ObservaINTECO

Perfil Scribd ObservaINTECO:
http://www.scribd.com/ObservaINTECO

Canal Youtube ObservaINTECO:
http://www.youtube.com/ObservaINTECO

Blog del Observatorio de la Seguridad de la Información:
http://www.inteco.es/blogs/inteco/Seguridad/BlogSeguridad

Envíanos tus consultas y comentarios a:

observatorio@inteco.es

Instituto Nacional
de Tecnologías
de la Comunicación