UNIVERSIDAD DE SALAMANCA

FACULTAD DE TRADUCCIÓN Y DOCUMENTACIÓN

GRADO EN INFORMACIÓN Y DOCUMENTACIÓN

Trabajo de Fin de Grado

GESTIÓN DE DOCUMENTOS ELECTRÓNICOS EN LA NUBE

VNiVERSiDAD D SALAMANCA

Beatriz Pena Rodríguez

Manuela Moro Cabero

Salamanca, 2017

UNIVERSIDAD DE SALAMANCA

FACULTAD DE TRADUCCIÓN Y DOCUMENTACIÓN

GRADO EN INFORMACIÓN Y DOCUMENTACIÓN

Trabajo de Fin de Grado

GESTIÓN DE DOCUMENTOS ELECTRÓNICOS EN LA NUBE

Beatriz Pena Rodríguez

Manuela Moro Cabero

Salamanca, 2017

To my family on both sides of the Atlantic,

specially to my Francis Family,

for all the support, love, friendship and happy moments I'll never forget.

[Asiento catalográfico]

Pena Rodríguez, Beatriz

Gestión de documentos electrónicos en la nube / Beatriz Pena Rodríguez, María Manuela Moro Cabero. Salamanca: Universidad de Salamanca, 2017

44 p; x cm.

I. Título. 1. Moro Cabero, María Manuela. 2. Universidad de Salamanca

[Resumen]

El presente trabajo de fin de grado estudia la gestión documental en la nube, siendo su objetivo principal establecer estrategias para afrontar la gestión documental. Mediante una revisión teórica se analizan los riesgos a los que se expone la documentación. Como resultado, se aporta una clasificación de los mismos y se proponen las estrategias para combatirlos.

[Palabras clave]: computación en la nube, gestión documental, seguridad de información, gestión de riesgos.

[Abstract]:

This bachelor's thesis studies the management of information in the cloud, being its main objective to establish strategies for facing record management. It analyzes a theoretical review in order to expose the risks which the documentation is sensitive to. As a result, it's provided a classification of risks and a strategy plan to face them.

[Key words]: cloud computing, record management, information security, risk management.

Tabla de contenido

Índice de ilustraciones

0. Introducción

Justificación del trabajo:

La intención de este trabajo es estudiar la computación en la nube desde el punto de vista documental, contemplando tanto la gestión como la seguridad de la información almacenada en este tipo de servicios.

Debido a la reducción de costes que supone, actualmente, tanto las empresas privadas como las administraciones públicas están apostando cada vez más por la computación en la nube y, en la mayoría de los casos, no son conscientes del riesgo que eso supone. En este momento de auge, resulta esencial analizar estos riesgos, así como, una vez identificados y priorizados, proponer estrategias para una gestión de la documentación adecuada.

Formulación del problema

Tanto las personas físicas como las jurídicas (empresas, instituciones, administraciones) confían sus archivos personales o de trabajo a empresas de las cuales, habitualmente, no conocen en qué condiciones y lugares almacenan, traspasan o utilizan la información y datos que les proporcionan y, por tanto, tampoco los peligros a los que se exponen

En la mayoría de los casos, las organizaciones no son conscientes de todos los peligros que eso implica y de las posibles consecuencias de efectuar una inadecuada decisión. Así mismo, sería preciso disponer de un protocolo de actuación en el que se recopilen las estrategias más significativas de utilidad para las organizaciones que afrontan la gestión de documentos en entornos de *Cloud Computing*.

Objetivos:

Objetivo general: Establecer una batería de estrategias que permitan afrontar la gestión de documentos en entornos de *Cloud Computing.*

Para el logro de este objetivo, se proponen las siguientes acciones:

Vinculadas al conocimiento del entorno o/y contexto de *Cloud Computing:*

- Definir qué es la nube y cómo funciona
- Describir los diferentes tipos de servicios ofertados

Vinculadas a los requisitos de gestión documental

- Identificar los riesgos más comunes desde el enfoque documental
- Analizar los riesgos, priorizando los mismos
- Proponer estrategias de actuación

Metodología:

La investigación es de naturaleza descriptiva basada en el análisis de la literatura editada sobre el objeto investigado, así como sobre las experiencias que los archiveros han difundido mediante actividades tales como jornadas, informes y contenidos webs.

Resultados esperados:

Se espera que este trabajo sea útil para que las organizaciones públicas o privadas sean conscientes de los riesgos que conllevan los servicios en la nube y sean capaces de exigir en sus contratos una serie de condiciones que aseguren la protección de los datos y cumplan con todas las normativas vigentes.

1. El *Cloud Computing*

Estado de la cuestión:

La idea de trabajo mediante la computación en la nube no es nueva. Ya en la década de los 60, John Mc Carthy, en su discurso en el centenario del MIT, predijo que en el futuro la informática se convertiría en una "utilidad pública" [Wheeler y Waggener, 2009].

El concepto de servicios electrónicos globales comenzó a gestarse con investigadores como Joseph C.R. Licklider, que 1963, en un memorándum para ARPA4, quien contempló las ventajas que proporcionaría una infraestructura de red que permitiese compartir servicios. Esta idea evolucionó en la red ARPANet, que a su vez dio origen a lo que hoy conocemos como Internet.

El avance de Internet y las nuevas tecnologías han impulsado su evolución, gracias al aumento de capacidad de procesamiento y almacenamiento, así como al desarrollo de estándares para la interoperabilidad entre dispositivos. Las formas de almacenar y trabajar la información han cambiado radicalmente. El paso del soporte analógico al digital ha superado las expectativas, siendo mayor al incremento experimentado, respecto a los soportes físicos, debido a sus numerosas ventajas (accesibilidad, reducción de costes, flexibilidad, etc.). Estos factores, han provocado que en la actualidad se use la nube para muchas actividades corrientes que antes se ejecutaban en un entorno local, como ver contenido multimedia como series o películas (Netflix), escuchar música (Spotify), consultar el correo (Gmail) y hasta el almacenamiento masivo de información (Dropbox, Drive), etc.

En cuanto al término “nube”, se comenzó a utilizar en varios contextos en los años noventa, pero no fue hasta más tarde cuando Eric Schmidt, CEO de Google, utiliza la palabra “nube” para describir el modelo de negocio de Servicios de Internet a través de Internet en 2006, produciendo que el término ganara en popularidad.

Sin embargo, también hay que tener en cuenta que las TIC y concretamente la computación en la nube suponen numerosos riesgos que se deben tener en cuenta, especialmente en los casos en los que se trata información personal o sensible. Con anterioridad a su investigación, pasamos a reflexionar sobre los interrogantes básicos definitorios y delimitadores de este entorno de trabajo, tales como: ¿Qué es la nube? ¿Cuáles son sus principales características y modelos? ¿Quién interviene?, ¿Qué tipos de nube se conocen? ¿Qué modalidades de servicio se ofertan? Entre otros.

¿Qué es la nube?

Según el NIST (National Institute of Standards and Technology), la computación en la nube se define como un modelo de servicio que consiste en la oferta de recursos informáticos entre los que se incluyen redes, servidores, almacenamiento, aplicaciones y servicios).

El *Cloud computing* es una solución que permite al usuario optimizar los procesos y reducir el coste de los recursos con respecto al tratamiento y gestión de la información. No hay necesidad de hacer grandes inversiones en infraestructura, sino que el proveedor la presta. Incluso, en aquellos casos que fuera adecuado, se permiten opciones intermedias, en las que el contratante puede actuar con responsabilidades de desarrollador.

Desde la óptica de un Archivo, la nube aporta un modelo de servicio para facilitar comunicación, Software, infraestructura tal como red, sistemas operativos, etc. para la gestión de los ficheros, espacio de almacenamiento para disponer de e-depósitos casi ilimitados; así como opciones de rentabilizar costes, al evitar compra de infraestructuras; formación tecnológica, al proporcionar sistemas y software; disponibilidad compartida, al proporcionar infraestructura distribuida de red con accesos diversos, incluso seguridad, al disponer de mejores expertos en seguridad de la información y de estándares específicos, como veremos, etc.

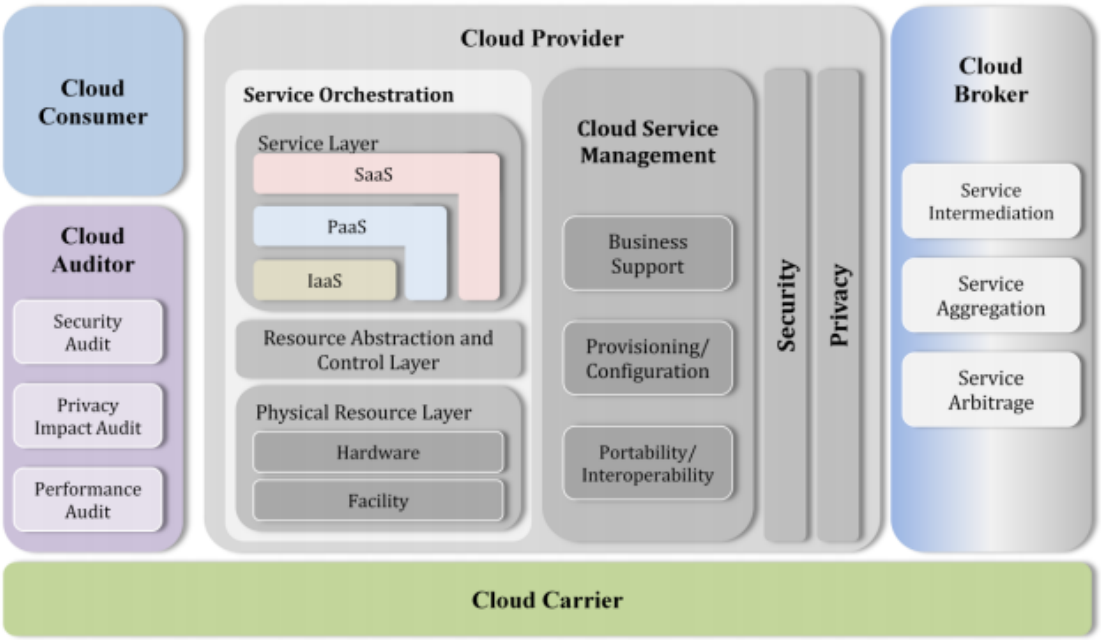

Ilustración 1. Modelo de referencia de nube. Fuente: NIST.

En la nube se reconocen y delimitan el servicio las siguientes características esenciales:

1. Autoservicio bajo demanda:

El consumidor puede proveer unilateralmente capacidades de computación, tales como tiempo del servidor y almacenamiento en red, según sea necesario automáticamente, sin necesidad de interacción humana con cada proveedor de servicios.

Desde la perspectiva de un Archivo, esta característica favorece su contratación, dado que las particularidades de cada Archivo se ajustan mediante esta opción.

2. Amplio acceso a la red:

Todas las capacidades están disponibles a través de la red y se accede a través de mecanismos estándar que promueven el uso por las diferentes plataformas de clientes, por ejemplo, teléfonos móviles, tablets, portátiles, etc.
Desde un enfoque de cliente/atención ciudadana, el Archivo dispone de opciones de gestión distribuida de la información en un marco de servicio dirigido a la ciudadanía, o en el caso de entidades privadas, se facilita la disposición de los documentos con geolocalización distribuida, favoreciendo modelos de gestión de negocio acordes con la economía digital.

3. Puesta en común de recursos

Los recursos informáticos del proveedor se agrupan para servir a varios consumidores. Se utiliza un modelo de múltiples inquilinos, con diferentes recursos físicos y virtuales asignados dinámicamente y reasignados de acuerdo a la demanda del consumidor.

Existe una sensación de independencia de ubicación en que el cliente generalmente no tiene control o conocimiento sobre la ubicación exacta de los recursos proporcionados, pero puede especificar la ubicación en un nivel de abstracción más alto (por ejemplo, país, estado o centro de datos). Ejemplos de recursos incluyen almacenamiento, procesamiento, memoria y ancho de banda de la red.

La puesta en común de recursos para centros con bajo nivel presupuestario es el único modo de asegurar servicios de calidad sostenibles. Este hecho, se percibe en los Archivos pequeños y medios en los que los presupuestos pueden calificarse de modestos o reducidos.

4. Elasticidad rápida.

Las capacidades pueden ser suministradas elásticamente y liberadas, en algunos casos automáticamente, para escalar rápidamente hacia el exterior y hacia el interior de acuerdo con la demanda. Para el consumidor, las capacidades disponibles para el aprovisionamiento a menudo parecen ser ilimitadas y se pueden apropiar en cualquier cantidad en cualquier momento.

La flexibilidad de estos entornos favorece la adaptación y empleo de servicios para los Archivos, dadas sus particularidades, atendiendo a la naturaleza y uso de los fondos que gestionan, tanto en el momento de la creación de los documentos como a lo largo de su ciclo de vida o situación multidimensional.

5. Servicio medido.

Los sistemas de nube controlan y optimizan automáticamente el uso de recursos aprovechando una capacidad de medición en algún nivel de abstracción apropiado al tipo de servicio (por ejemplo, almacenamiento, procesamiento, ancho de banda y cuentas de usuario activas). El uso de recursos puede ser monitoreado, controlado y reportado, proporcionando transparencia tanto para el proveedor como para el consumidor del servicio utilizado.

Un servicio medido implica un gasto medido. Desde un enfoque de rentabilidad y sostenibilidad en el Archivo, un servicio medido supone un apoyo para la gestión presupuestaria y contable.

Estas características son importantes para delimitar el concepto de servicio en la nube, aunque también para aproximarnos a los riesgos que el archivero debe de afrontar, pues, aun con las ventajas que conllevan, incluyen igualmente, riesgos vinculados. Ejemplo, la idea de servicio medido conlleva, igualmente la necesidad de conocer cómo se mide y de establecer nuevos presupuestos para considerar los costes de gestionar y preservar los documentos. La elasticidad, por ejemplo, favorece modelos adaptados, aunque también, la necesidad de controlar los modelos de nube y de servicio que se ofrecen y que serán objeto de contratación, etc.

Agentes

Es necesario tener claro los diferentes roles en el contrato *Cloud*. Para tal fin, vamos a intentar definir e identificar cada uno de ellos. Además, aunque en la mayoría de los casos sólo se hable de cliente y proveedor, hay más implicados que pueden jugar un papel importante en el proceso.

Siguiendo la guía *Cloud* se establecen tres tipos de agentes:

- Clientes: usuarios que hacen uso de los recursos proporcionados
- Proveedor de servicios de *Cloud computing* o proveedor de la nube: es quién proporciona los recursos
- Socios o *partners*: crean y soportan servicios en la nube que venden al usuario final, por ejemplo, creando una aplicación de marketing que se ejecuta en la nube a partir de servicios más básicos de la misma

El NIST amplía la relación de agentes que intervienen, tal y como se aprecia en la siguiente enumeración:

- Consumidor: persona u organización que mantiene una relación de negocio y utiliza servicios de un proveedor *Cloud.*
- Proveedor: persona, organización o entidad encargada de abastecer servicios a las partes interesadas en ellos.
- Auditor: agente que puede conducir asesoramiento independiente sobre los servicios en la nube, operaciones en sistemas de información, actuación y seguridad de la implementación
- Broker (Corredor): entidad que maneja el uso, actuación y entrega de servicios en la nube y negocia las relaciones entre proveedores y consumidores.
- Carrier (Operador/Transportista): intermediario que provee conectividad y transporte de los servicios Cloud de los proveedores a los consumidores

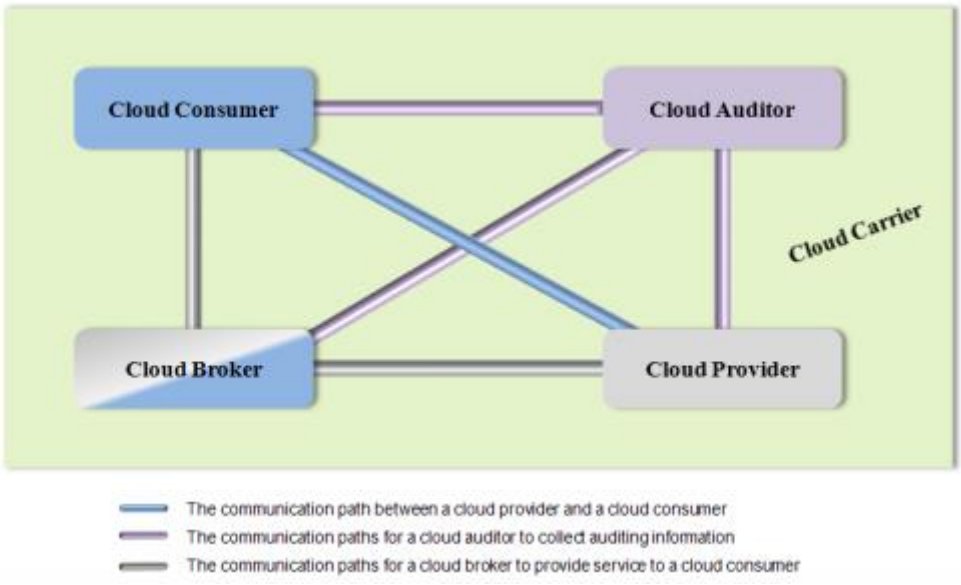

Ilustración 2. Agentes y relaciones entre ellos en Cloud Computing. Fuente: NIST.

Tipología

Una vez aclarado el concepto de nube es necesario precisar que existen diferentes tipos de nube. Seguimos en este caso la clasificación que propone la Guía Cloud para empresas, donde se reconocen los siguientes tipos de nube.

- Pública

Las nubes públicas son aquellas en las que todo el control de los recursos, procesos y datos está en manos de terceros. Es lo que se entiende por computación en la nube en el sentido tradicional, pues los recursos se suministran dinámicamente de manera precisa y vía Internet a través de aplicaciones web / servicios web desde un proveedor externo.

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. Es el modelo menos seguro, pues no todas las aplicaciones y datos están protegidos de ataques maliciosos.

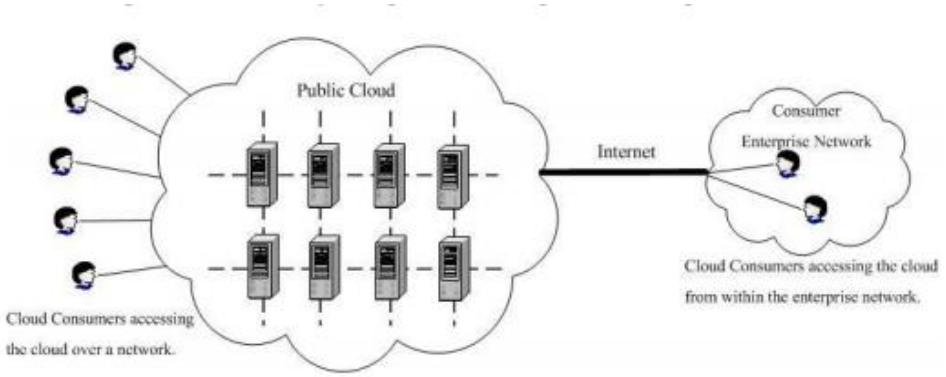

Ilustración 3. Nube pública. Fuente: NIST

- Privada

Las nubes privadas son las creadas por una entidad (no necesariamente la misma que la va a utilizar) que se encarga también de su gestión y administración. Supone una mejora con respecto a la seguridad y privacidad de los datos, pues se puede controlar qué usuario accede a cada servicio de la nube.

Se utiliza en grandes entidades como administraciones públicas o corporaciones.

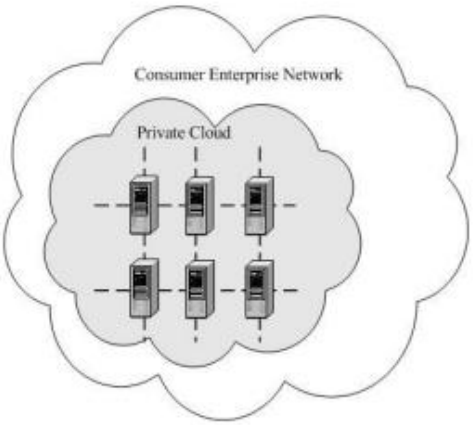

Ilustración 4. Nube privada. Fuente: NIST

- Nube comunitaria

Son servicios *Cloud* que se comparten entre varias organizaciones formando una comunidad. En esencia, este modelo es una ampliación del modelo de *Cloud* privada, sólo que en este caso el peso está repartido entre la comunidad y no recae solamente sobre una única organización.

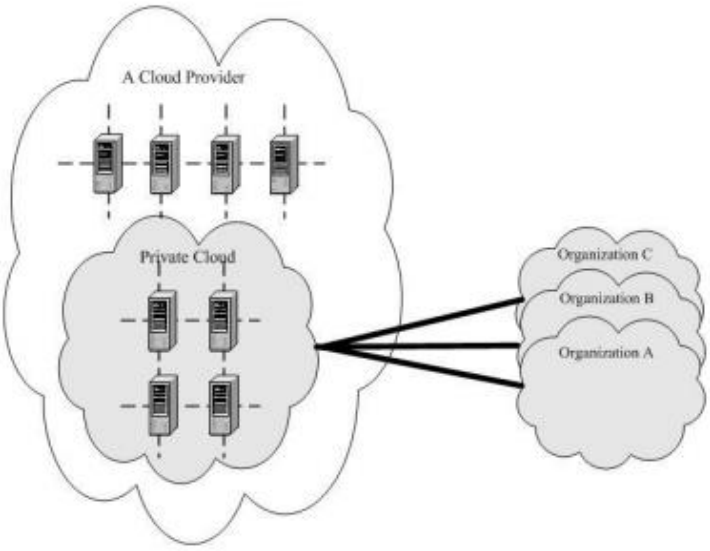

Ilustración 5. Nube comunitaria. Fuente: NIST

- Nube híbrida

Como su propio nombre indica, las nubes híbridas combinan el modelo de la nube pública y privada. 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 ejerce mayor control sobre los datos sensibles, aunque el servidor lo gobiernen terceros.

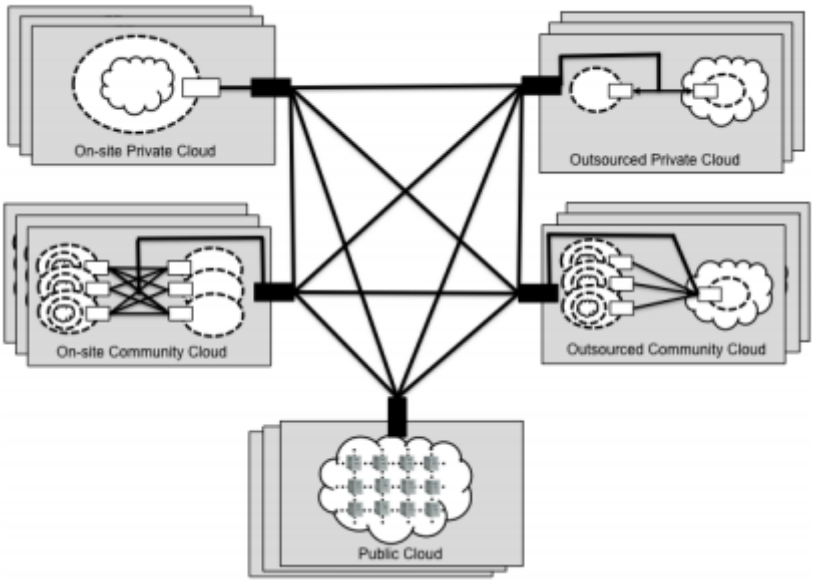

Ilustración 6. Nube híbrida. Fuente: NIST

Niveles de servicio

Los diferentes niveles de servicio se pueden agrupar en las siguientes categorías:

- Infraestructura como Servicio (Infrastructure as a Service = IaaS)

Es el nivel más alto pues entrega una infraestructura completa al usuario, es decir, proporciona hardware y software.

Tal vez se pueda decir que éste es el modelo más primitivo de *nube*, que se inició con los sitios de Internet que proporcionaban capacidad de almacenamiento masivo a través de la red y los servidores de alojamiento web.

Garantiza el acceso a servicios estandarizados en los que el proveedor ofrece almacenamiento, procesamiento, redes y equipos para manejar tipos específicos de cargas de trabajo del cliente. (Herrera, 2001)

- Plataforma como servicio (PaaS = Platform as a Service= PaaS)

Es el nivel intermedio. Proporciona una plataforma sin necesidad de comprar ni mantener hardware o software. Por ejemplo, proporciona utilidades como bases de datos, un servidor web, sistema operativo, etc.

- Software como servicio (Software as a Service=SaaS)

Es el nivel más bajo ya que simplemente entrega el software a través de internet siempre que el usuario lo necesite. Se accede desde el navegador web, sin necesidad de instalar programas y suele emplearse con el fin de resolver u ocuparse de un proceso: una aplicación de contabilidad, de gestión documental, de correo electrónico, etc.

Ilustración 7. Modelos de servicio, de mayor a menor nivel

En la tabla que seguidamente se incluye, se muestran las modalidades de servicios de forma resumida y comparada:

	Infraestructura como servicio (IaaS)	Plataforma como servicio (PaaS)	Software como servicio (SaaS)
Nivel de servicio	alto	intermedio	bajo
Nivel de *Cloud*	hardware	aplicación informática	programa informático
Ejemplos	Amazon Web Services (AWS), Cisco Metapod, Microsoft Azure, Google Compute Engine (GCE)	Amazon SimpleDB, Caspio, MS Azure	Google Apps, Microsoft Office, Dropbox, NetDocuments

Ilustración 8. Tabla de niveles de servicio

Tras establecer estos conceptos básicos con respecto a la nube, se clasifican a continuación, atendiendo a la guía Cloud de los archivos de Reino Unido, los aspectos esenciales según presentan ventajas o inconvenientes.

Ventajas:

- Disponible cuando se necesita (bajo demanda) sin necesidad de prolongadas compras y procesos de adquisición
- Disponible en redes estándar como internet, sin requerimientos especiales de protocolos o hardware
- Elasticidad, es decir, tener la habilidad de ofrecer capacidad adicional si la demanda crece y menos en caso de que baje.
- Posibilidad de acceder a herramientas y procedimientos específicos para la preservación digital a través de vendedores especializados

Inconvenientes

- La flexibilidad y el cambio constante son dos trazos básicos de la nube, lo cual supone un importante contraste con la naturaleza a largo plazo de los archivos.
- La nube puede ser más barata en un principio, pero a menudo necesita que las organizaciones manejen el presupuesto de forma diferente, además de costos de entrenamiento al personal y en muchos casos de reclutamiento o asesoría.
- Obliga a cumplir todos los requisitos legales
- Cuestiones con respecto al copyright y derechos de la información, especialmente con respecto a los permisos de acceso a los datos.
- Riesgos de seguridad en el caso de la información personal
- El contrato con el servidor de *Cloud* es una gran responsabilidad y supone un trabajo y esfuerzo que no todas las empresas o centros de información pueden asumir, especialmente los de pequeño tamaño.
- Implica definir estrategias y establecer auditorías periódicas
- Es complicado conocer dónde está ubicada la información y hasta donde llevan los contratos con terceros y las subcontrataciones.

Seguidamente, y para completar el detalle descriptivo de estos entornos se incluye información sobre la localización del proceso y de los datos.

Localización del proceso y de los datos:

Los archiveros muestran, tal y como veremos, dudas ante la geolocalización de los datos y el control sobre dónde se están llevando a cabo los procesos de almacenamiento y/o de gestión de los mismos. La pérdida de este control les preocupa enormemente, dado que su rol se identifica como el desempeño de asegurar fiabilidad o aportar fiabilidad a la información que se gestiona, almacena y usa. Es necesario aclarar una serie de conceptos vinculados a la geolocalización para comprender de forma completa el ecosistema del Cloud Computing. Estos se relacionan con la subcontratación, la localización y transparencia y están directamente vinculados a los principales riesgos a los que se expone la documentación.

Subcontratación:

Es el proceso económico que se produce en el ámbito empresarial cuando se delegan responsabilidades y tareas a una entidad externa. En el caso de la nube, este rol lo cumplen los *partners*. En numerosos casos, la relación no es directa con los proveedores, sino que estos externalizan parte de los servicios (por ejemplo el almacenamiento, hardware, comunicaciones, etc.). Incluso estos terceros pueden subcontratar de nuevo parte del servicio, formando una cadena de sucesivas subcontrataciones. [Para el Archivo, el rol de fiabilidad de los datos pareciera que se pierde. De ahí que resulte importante saber hasta dónde llegan todos los tentáculos]

Localización:

Este concepto se refiere a la ubicación de los servidores. Como ya hemos comentado es esencial tener localizada la información, especialmente si está fuera del Espacio Económico Europeo. A la hora de contratar, se debe exigir conocer no sólo la sede del proveedor, sino también la ubicación de todos los recursos físicos, especialmente si se encuentran subcontratados a terceros.

Transparencia:

Aplicada a la computación de la nube, transparencia significa que el proveedor debe ofrecer información precisa y detallada de todo lo que hace con los datos en todo momento. Esta obligación debe quedar constatada en el acuerdo y contrato de servicio resultante. El archivero debe de controlar este aspecto o al menos, asesorar al respecto.

Tras este capítulo podemos afirmar conocer el funcionamiento básico de la nube, así como los tipos y niveles de servicio, además de identificar los agentes implicados y los principales conceptos que conforman el ecosistema *Cloud*. A continuación, necesitaremos conocer un elemento más que influye en el sistema, la legislación aplicable.

2. Marco legislativo

Debido a la importancia de controlar aspectos como privacidad y seguridad de información, la legislación está intentando abarcar y regular los aspectos clave de la nube. En este apartado se reseñan las normas más importantes que afectan al *Cloud computing* desde el punto de vista de la gestión y seguridad de la documentación, clasificadas según su alcance.

Nivel nacional

1. Ley de Protección de datos: Ley orgánica 15/1999 de 13 de diciembre y Reglamento de Desarrollo (RDLOPD)- aprobado por R.D. 1720/2007

La ley establece en el art. 3 que "un dato personal es cualquier información concerniente a personas físicas identificadas o identificables." Es vital diferenciar si la información entra dentro de la categoría de dato personal, pues en caso de no serlo (si se trata por ejemplo de operaciones matemáticas, cálculos físicos o químicos, etc.), la LOPD no aplica.

La información almacenada en la nube pertenece, en la mayoría de los casos, a esta categoría. Por tanto el proveedor del servicio debe cumplir con el conjunto de obligaciones establecidas por la propia ley, como son la inscripción de ficheros, el consentimiento y calidad de datos, garantía de derechos ARCO (Acceso, Rectificación, Cancelación y Oposición), la adopción de medidas de seguridad, además de los deberes relacionados con la recogida de información.

La ley establece una serie de obligaciones con respecto al acceso a los datos por cuenta de terceros y la seguridad de los datos. En el caso del acceso, cabe destacar que el encargado debe cumplir todos los requisitos de la LOPD y el RDLOPD, incluyendo la devolución o destrucción de la información tratada una vez finalice el contrato.

Además, no puede comunicar esta información a terceros, ni siquiera con fines de conservación (Artículos 20, 21 y 22 RDLOPD)

Teniendo en cuenta que el principal riesgo es el desvío de información a terceros, es de vital importancia la transparencia, especialmente si los datos con los que se está trabajando son de carácter personal.

También con respecto a la seguridad, el Artículo 9 LOPD Título VIII RDLOPD establece que el **responsable deberá:** *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.*

Podemos concluir diciendo que la ley cubre el riesgo de terceros y de seguridad, pero no ofrece garantías con respecto a las copias de la información almacenada, especialmente a la hora de destruir la información una vez terminado el contrato.

Cabe destacar también el papel de la Agencia Española de Protección de Datos (AEPD), el organismo encargado de garantizar el cumplimiento de la LOPD en el territorio español, así como el Esquema Nacional de Interooperabilidad (ENI) y el Esquema Nacional de Seguridad (ESN) y sus políticas destinadas a la protección e intercambio de información.

2. Ley 34/2002, de Servicios de la Sociedad de la Información y del Comercio Electrónico (LSSI):

Esta normativa regula determinados aspectos de los servicios de la sociedad de la información, en particular, el comercio electrónico en el mercado interior. La ley juega un papel crucial dado que regula la transferencia de datos en este tipo de actividades comerciales, entre las cuales se incluyen los servicios en la nube.

3. Código penal

Aunque el Código Penal abarca muchos aspectos y delitos diferentes, en el caso de la nube se considera incluido dentro de los delitos de estafa. Este caso se puede dar fácilmente cuando no hay transparencia al contratar servicios y estos se deslocalizan o se producen transferencias de información a terceros.

Nivel europeo:

A nivel de Europa, cabe destacar las siguientes regulaciones:

- Directiva EU 2016/1148 del 6 de Julio de 2016

Debido a la importancia que tienen los sistemas de información en las actividades económicas y sociales es necesario asegurar su seguridad y confiabilidad. Esta directiva pretende responder a los desafíos de seguridad, así como cubrir los riesgos más relevantes, aplicado tanto a los operadores de servicios como a los proveedores de servicios digitales.

Con respecto al Cloud Computing, la directiva señala en el punto 56 que:

> "Cuando las administraciones públicas de los Estados miembros utilicen los servicios ofrecidos por los proveedores de servicios digitales, en particular los servicios de cloud computing, deben exigir a los proveedores de dichos servicios medidas adicionales de seguridad más allá de lo que los prestadores de servicios digitales normalmente ofrecerían de conformidad con los requisitos de la presente Directiva. Deben ser capaces de fijar esto mediante obligaciones contractuales."

- EU Data Protection directive 95/46/CE

El objeto de esta normativa es proteger los derechos que respecta al tratamiento de los datos personales. Según sus premisas, para que el tratamiento sea considerado lícito deben de cumplirse la siguiente condición: ora el interesado debe dar consentimiento ora el tratamiento de los datos debe ser un ejercicio necesario (bien para cumplir un contrato, intereses vitales del interesado o bien una obligación legal o de interés público)

La calidad de los datos debe ser garantizada en todo momento. Deben ser tratados de manera legal y lícita, recogidos con un fin determinado, deben ser adecuados, exactos y si es posible, actualizados. El dueño de los datos puede exigir en todo momento sus derechos de propiedad, de acceso, y de oposición: Por tanto puede exigir conocer en todo momento la ubicación y estado de los datos y negarse a que estos sean objeto de tratamiento si así lo considera.

Nivel internacional:

El principal organismo regulador a nivel internacional es el comité ISO (International Organisation for Standardisation). Con base en Ginebra, la ISO es un organismo independiente y no gubernamental, que ha desarrollado 21.684 estándares internacionales y documentos relacionados con diversas industrias, desde la tecnología a la alimentación, agricultura, salud, tráfico, etc. Con respecto a la seguridad de la información y en concreto a la gestión de la documentación se destacan

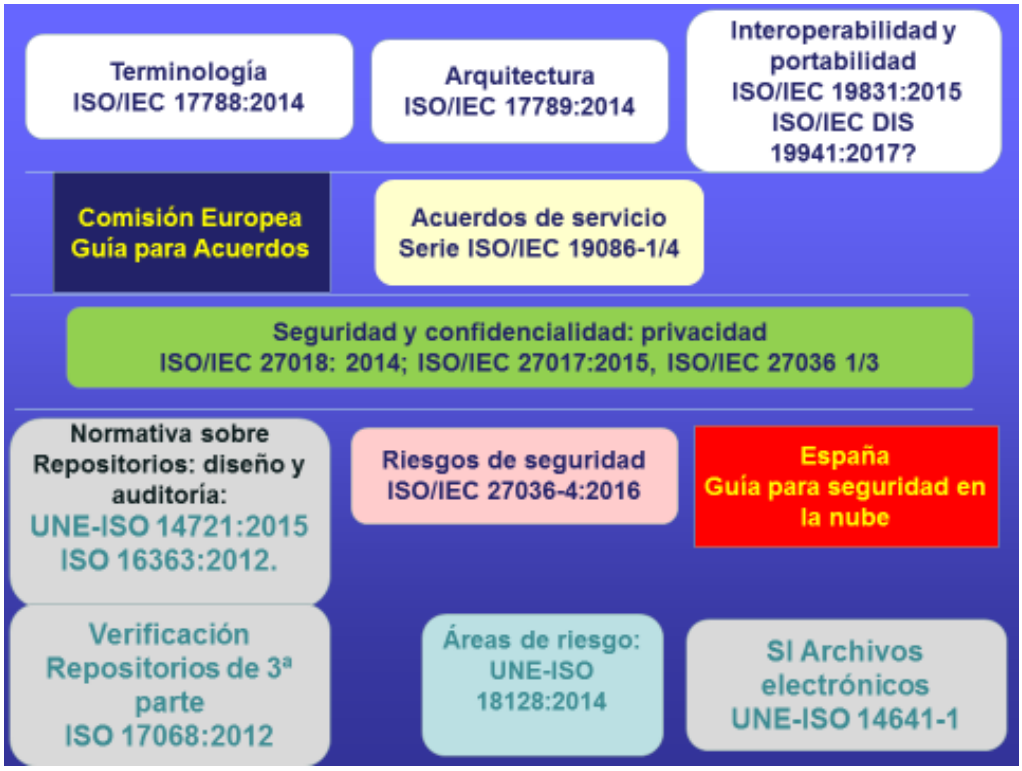

Ilustración 9. Road Map para la normalización del entorno de Cloud Computing desde el enfoque de gestión documental. Fuente: Contenidos disciplina Preservación digital. Máster SID. USAL.Salamanca, Curso 2017, tema 5.

- Norma ISO 14641-1:2012

Esta norma introduce especificaciones para el almacenamiento y acceso de documentos electrónicos, lo cual garantiza legibilidad, integridad *y trazabilidad de los documentos durante la duración de su conservación.*[1]

[1] ISO 14641-1:201. Electronic archiving — Part 1: Specifications concerning the design and the operation of an information system for electronic information preservation. Fuente: https://www.iso.org/obp/ui/#iso:std:iso:14641:-1:ed-1:v1:en

De esta norma es indicativo de las preocupaciones de controlar el almacenamiento de información por parte de terceros. Así, la norma regula en el apartado 13, las actuaciones de tercera parte de confianza prestadora de servicios de Archivo.

También vela por asegurar el cumplimiento de los requisitos de confidencialidad, seguridad, etc. Así mismo, incluye un modelo de contrato de servicio en el que se señala un contenido muy preciso.

Apartado 13

- **Actividades de la tercera parte** de confianza prestadora de servicios de Archivo (cumplimiento de requisitos, políticas compatibles y procedimientos de seguridad)
- Además de la implementación de un modelo de archivo electrónico en el que se cumplan requisitos debe asegurar **confidencialidad, identificar a cada cliente, proporcionar certificados de depósito y trazabilidad del archivo**, además de efectuar todas las eliminaciones
    - Anexo C- principios para condiciones generales de servicio
    - **Modelo de contrato de servicio.** Se normaliza: **contenido, duración, calidad, periodo de conservación, seguridad y protección de datos, información y mantenimiento, transferencia y continuidad, transferibilidad, confidencialidad y datos personales, restitución, seguro profesional, subcontratación, evaluación…**

En el apartado 14 igualmente se trabaja el acuerdo del subcontratista, el contenido del contrato del subcontratista y la transferencia de datos.

Apartado 14

- **Acuerdo del subcontratista** y verificación de confirmación de cumplimiento requisitos de la norma ISO 14641-1, procedimientos, seguridad, políticas compatibles…
- **Contenido del Contrato** del subcontratista…
- **Transferencia de datos** mediante redes de telecomunicaciones abiertas, condiciones

- ISO / IEC 17788: 2014

Esta ISO proporciona una visión general del cloud computing además de definir la terminología básica. Esta expresa conceptos conocidos y trabajados a diario por los archiveros, tales como:

- disponibilidad, confidencialidad,
- seguridad,
- integridad
- interoperabilidad,
- capacidad de portabilidad, reversibilidad,
- auditoría,
- almacenamiento de datos,
- Etc.

- ISO 27001 y 27002

La familia ISO/IEC 2700 ayuda a las organizaciones a gestionar la seguridad y mantener su información protegida. En nuestro caso particular nos centraremos en dos normas en lo que a *Cloud computing* compete.

La ISO / IEC 27001 es el estándar más conocido en la familia que proporciona los requisitos para un Sistema de Gestión de la Seguridad de la Información (ISMS).[2]

Por su parte, la ISO / IEC 27002: 2013 proporciona directrices para las normas de seguridad de la información organizacional y las prácticas de gestión de la seguridad de la información, incluyendo la selección, implementación y administración de controles teniendo en cuenta el entorno de seguridad de la información de la organización.[3]

Según aclara el propio comité, este estándar está diseñado para ser utilizado por organizaciones que tienen la intención de implementar modelos de control para la seguridad de información o bien desarrollar sus propias directrices.

[2] ISO/IEC 27002:2013 Preview Information technology -- Security techniques -- Code of practice for information security controls. Fuente:
[3] https://www.iso.org/standard/54533.html

- ISO/IEC 27017:2015

Esta nueva norma se basa en las normas de seguridad de la información existentes, incluyendo ISO/IEC 27001 e ISO/IEC 27002. Publicada en 2015, proporciona directivas para el control de la seguridad, aplicado a la provisión y uso de servicios cloud proveyendo[4]:

- Guías de Implementación adicional para controles relevantes especificados en la 27002
- Controles adicionales específicamente relacionados con servicios -*Cloud*

Estas recomendaciones funcionan tanto como para los proveedores como para los clientes *Cloud*.

- ISO/IEC 27018:2014

Esta norma establece controles y directrices para implementar medidas de protección de Información de Identificación Personal (PII) de acuerdo con los principios de privacidad en ISO / IEC 29100 para el entorno de *Cloud computing* público. [5]

Está basada en ISO / IEC 27002, la norma anteriormente comentada, pues tiene en cuenta los requisitos reglamentarios para la protección de la información personal que podrían ser aplicables en el contexto del entorno de seguridad de la información de un proveedor de servicios públicos servicios en la nube.

Es además aplicable a todos los tipos y tamaños de organizaciones, incluyendo empresas públicas y privadas, entidades gubernamentales y organizaciones sin fines de lucro que proveen servicios de procesamiento de información como procesadores PII a través de *Cloud computing* bajo contrato con otras organizaciones.

[4] ISO/IEC 27017:2015 Information technology –Security techniques –Code of practice for information security controls based on ISO/IEC 27002 for cloud services. Fuente: http://www.iso.org/iso/catalogue_detail?csnumber=43757

[5] ISO/IEC 27018:2014 Tecnología de la información. Técnicas de seguridad. Código de práctica para la protección de información personal identificable (IPI) en nubes públicas que actúan como encargados del tratamiento. Fuente: http://www.iso.org/iso/catalogue_detail.htm?csnumber=61498

La ISO/IEC 27018 tiene los siguientes objetivos principales[6]:

- Ayuda a los proveedores de servicios en el cloud que procesan datos personales a hacer frente a las obligaciones legales aplicables, así como a las expectativas del cliente
- Habilita la transparencia para que los clientes puedan elegir servicios en el cloud bien gobernados
- Facilita la creación de contratos de servicios en el cloud
- Proporciona a los clientes en el cloud un mecanismo para garantizar que los proveedores del cloud cumplan con las obligaciones legales y otras

En resumen, la norma ISO/IEC 27018 proporciona una base práctica para inducir la confianza en la industria del *Cloud,* centrándose especialmente en la privacidad.

Como hemos podido comprobar en este apartado, la necesidad de regulación en esta materia está cubierta por las normas y estándares anteriormente destacados. Cabe también destacar que aparte de los estándares internacionales, es habitual que los países en concreto cuenten con legislación específica, como es el caso de España. Este hecho es importante en el caso de que la compañía o sus subcontrataciones se encuentren localizados en un país ajeno al propio.

Es importante que el Archivero conozca y maneje estas directivas a la hora de asesorarse, para así conocer sus derechos y obligaciones como cliente y de esta forma exigir un contrato seguro y beneficioso para su centro.

Tras el análisis general y la revisión de las principales normas, es momento de entrar en materia de riesgos y estrategias.

[6] Isofocus, la la revista de la Organización Internacional de Normalización. Enero-febrero 2015.

3. Riesgos y estrategias

Riesgos

Los riesgos se pueden dividir en diferentes tipos de grupos y clasificaciones atendiendo a varios autores. Seguidamente se revisan algunas propuestas:

Según el documento de trabajo de la Guía Cloud, se deben considerar los siguientes aspectos:

- Precios: Planes de precios, bienestar de los usuarios, factores de precios y precios colaborativos
- Adopción: Costes, especificaciones no funcionales, operativas y socio-técnicas
- Mercados: Colaboración, bienestar, estrategia y diseño
- Sourcing: Costo, seguridad y privacidad

Los archivos de Australia establecen la siguiente clasificación de riesgos en lo que respecta a la computación en la nube:

Alcance	Tener en cuenta de forma cuidadosa la información que se almacena y su valor: *"Cuanto mayor sea el valor del material, más controles deben ser implementados para asegurar la integridad, autenticidad y confiabilidad de la información."*
Propiedad	Es necesario mantener la propiedad de la información que se almacena y maneja en la nube
Conformidad	El proveedor del servicio debe cumplir con la regulación vigente y las políticas y estándares adecuadas
Ubicación de almacenamiento	Es necesario especificar la ubicación de almacenamiento como un requisito *sine qua non* antes de adquirir un modelo de servicio en la nube o negociar contratos con un proveedor, dado que esto puede afectar a la legislación que lo regula y puede influir en el contrato y el servicio.
Preservación	La información almacenada debe ser preservada para que pueda ser accesible durante tanto tiempo como se necesite, por ello es necesario asegurar la continuidad de los documentos

	atendiendo a los aspectos de conservación necesarios (formato, interoperabilidad, etc.)
Retención y eliminación	Los proveedores de servicios en la nube sólo deben disponer de información comercial, incluidas copias, bajo instrucción de su agencia.
Habilidades	Esta gestión debe contar con especialistas en administración de información en la planificación e implementación de cloud computing que sean profesionales capaces de hacer el trabajo.

Con respecto a la autenticidad y precisión:

Almacenamiento	Conocer la ubicación de su información en todo momento.
Audit logs (AL)	Los logs tienen mucho valor dado que registran los accesos (hora, ubicación) y también los usuarios. La empresa debe de darte acceso
Seguridad de los sistemas ICT	La seguridad física y virtual asegura que la información remains auténtica, accurate y confiable. Importante políticas y manuales para ello

-En cuanto a seguridad de accesos inautorizados y borrado de información:

Viabilidad del proveedor del servicio de la nube	Si el proveedor cesa el negocio, el acceso se puede perder el acceso a la información de forma temporal o en algunos casos permanentemente. Por ello en caso de que ocurra es necesario avisar con antelación para contar con el tiempo necesario para elaborar estrategias.
Riesgo de destrucción incompleta de información de negocio	A menudo y como medida de prevención se crean copias de seguridad de la información. Es importante que en caso de eliminar la información y sus copias se eliminen realmente en todos los casos (incluyendo backups, etc.)

Contratación de terceros	Es frecuente que los servicios en la nube cuenten con subcontratos. Esto debe especificarse siempre y el cliente debe tenerlo claro.

-Fiabilidad y legibilidad

Legibilidad y usabilidad de la información de negocio corporativa	Si no se puede leer, la información carece de valor. Considerar riesgos de aceptar software y formatos que imponga el proveedor puede llevar a incompatibilidades y perder información
Impacto de la información corporativa corrupta	Siempre hay un riesgo de que la información digital se corrompa y sea irrecuperable.
Metadatos compatibles para identificar y recuperar la información de la agencia corporativa	Los metadatos son imprescindibles para que la información pueda ser completa e utilizable. Para ello debe seguir las normas de metadatos aplicables a la hora de describir el documento.
Impacto del bloqueo del vendedor	Un proveedor de la nube puede exigir usar su propio software y hardware. En ese caso, hay que tomar precauciones porque el proveedor puede bloquear la posibilidad de recuperar la información en un formato migrable a otro proveedor o incluso a los propios servidores. El valor de la información en esos casos se reduce severamente.

-Relacionados con otra información corporativa relevante

Mantenimiento y manejo de metadatos	Los metadatos deben estar actualizados y normalizados. A poder ser, deberían conservarse en caso de conversión.
Relación entre la información corporativa almacenada en la nube y en local	Es importante que ambas estén relacionadas y las conexiones sean claras. Es vital además evitar duplicados o versiones desactualizadas o diferentes porque puede causar serios problemas a la hora de recuperar información.

Según Paquette et al. se establecen estos grupos de riesgo según los siguientes aspectos referidos a la computación en la nube:

a) Riesgos tangibles

- Acceso: Sólo para usuarios identificados y se debe requerir login y tracking.

- Disponibilidad: La importancia de estar funcionando 24/7.

Puede haber fallos en el sistema si no se calcula bien la capacidad de almacenamiento en base a la demanda. Lo cual es complicado delimitar, porque si se contrata en exceso supone una pérdida de dinero, pero de menos puede provocar *overloads* que impidan el acceso o hagan que el sistema se caiga, lo cual deriva en una pérdida de dinero y confianza. También puede haber caídas por ataques maliciosos de los hackers, especialmente en el caso de grandes compañías.

Además, también se debe tener en cuenta la disponibilidad del vendedor en sí, ya que puede suceder que la empresa quiebre o que se produzca una compra o fusión por parte de otra compañía.

- Infraestructura: debe ser flexible y escalable.

Hay que tener en cuenta los posibles costes de mejorar la infraestructura en caso de que el diseño no sea flexible o escalable.

Las TIC cambian constantemente y evolucionan a nivel vertiginoso, por lo cual se debe estar preparado para futuras restricciones y debe ser fácil y práctico hacer cambios.

Además, debido a la falta de estándares es complicado de diseñar un modelo y casi imposible hacerlo compatible, pues cada vendedor tiene uno diferente. Además, en la

mayoría de los casos este se mantiene privado y confidencial para sacarle rentabilidad, por lo que no dejan en abierto su diseño.

- Integridad

Es necesario asegurar una serie de características de los datos, entre las cuales se encuentran la validación, la calidad, la seguridad y la durabilidad.

b) Intangibles

- Garantizar el acceso y uso de la nube cuando y donde se quiera sin interrupciones,
- Confianza en la nube,
- Servicio continuado,
- Seguridad para la prevención de accesos inautorizados,
- Mecanismos de seguridad para con el proveedor: restricción de monotorizar o rastrear,
- Confidencialidad y privacidad,
- Preservación y conservación a largo plazo,
- Clara definición de responsabilidad si algo grave sucede,
- Regulación y control de la información creada y modificada,
- Interoperabilidad de la tecnología (software),
- Portabilidad de datos y recursos entre diferentes partes de la nube,
- Capacidad de ser autodidacta, y
- Localización de la jurisdicción legal.

A continuación, se incluye otra propuesta de clasificación de riesgos (López et. al.)

1. Riesgos **estratégicos**: relacionados con el proceso de gestión y con los requerimientos del sistema
2. Riesgos **reputacionales**
3. Riesgos **legales**: como son el incumplimiento de obligaciones y de las normas
4. Riesgos **operacionales**: fraudes (internos y externos), relaciones laborables y seguridad en el puesto de trabajo, alteraciones o fallos tecnológicos, ejecución, gestión y cumplimiento del plazo de los procesos.

Por su parte, la Guía *Cloud* para empresas establece los siguientes riesgos:

- Abuso y uso malintencionado: sensible a ataques de piratas informáticos y a malware
- Fugas internas de información
- APIs inseguras
- Suplantación de identidad
- Desconocimiento del perfil de riesgo

Este documento aporta puntos de vista totalmente diferentes a las anteriores propuestas de riesgos que hemos repasado antes. Especialmente en lo que respecta al segundo apartado, las fugas de información, pues lo habitual es centrarse en el proveedor y olvidar que los riesgos también pueden fácilmente ocurrir en la propia empresa, bien por errores humanos o por acciones malintencionadas.

Tras el análisis de las diversas aportaciones de los autores, ofrecemos ahora una propuesta de clasificación de riesgos, tal y como se muestra en la siguiente tabla, donde se incluyen principales riesgos vistos y aquellos aspectos que deberían ser controlados.

Generales	Acceso	Infraestructura y diseño	datos
Costo	24/7	Costo económico	Seguridad
Pérdida de control	Autenticado	Debe ser dinámico	Integridad
Cambios en el *workflow* y en los procesos	Controlado para terceros	Interoperabilidad	Privacidad
Necesidad de actualización constante		Auditorías periódicas	Eliminación
Ataques hacker o desastres naturales		Debe ser seguro y fiable	Portabilidad
			Propiedad
			Ubicación

Ilustración 10. Propuesta de riesgos.

No todos los riesgos anteriores se recogen en la tabla, ya que la mayoría de ellos simplemente se engloban dentro de la categoría general a la que pertenecen pretendiendo hacer una clasificación general de los aspectos más destacados.

Además, hay que señalar la importancia que tienen los *backups* o copias de seguridad, pues permiten recuperar la información en caso de pérdida o catástrofe. Es preciso asegurar que el proveedor cuenta con varias copias de respaldo. Así mismo, esta gestión implica disponer de una opción de almacenamiento de seguridad para servidores y e-depósitos.

Estrategias

Antes de considerar la migración de servicios y aplicaciones a entornos *Cloud* es preciso realizar un análisis de riesgos que determine las indicaciones y los pasos a seguir. Estos deben establecerse en función de la naturaleza de los datos y exponer de forma clara los niveles asumibles de riesgos.

Previamente a comenzar un contrato con un proveedor cloud, es necesario asegurar los siguientes aspectos:

- Informarse de los tipos de nube y modelos de servicio para elegir el más conveniente en el caso particular del Archivo en concreto.
- Definir el tipo de datos a almacenar (nivel de sensibilidad de la misma)
- Conocer la legislación vigente en materia de *Cloud computing* para saber la normativa que afecta en este caso.
- Solicitar a la compañía información detallada sobre la compañía y sus actividades, especialmente los servicios a terceros que tienen contratados.
- Conocer y exigir las medidas de seguridad pertinentes
- Asegurar confidencialidad
- Exigir garantías (en el caso de pérdida de información, de destrucción, derechos ARCO, etc.)

Es importante que una vez se hayan definido todos estos puntos, el Archivo elabore un análisis de riesgos (utilizando un análisis DAFO, por ejemplo) y para ello cuente con asesoría tanto externa (informáticos, abogados, otros profesionales del mismo campo, etc.) como interna (el propio personal/entidad responsable).

El archivero/gestor documental cumple un rol fundamental en el manejo y la gestión de la documentación dentro de la unidad y es una parte imprescindible en el proceso de migración. Por tanto, debe estar presente en todas las decisiones y se debe considerar asesor en el proceso de elaboración de todas las políticas y planes estratégicos.

La Guía Cloud para empresas recomienda no migrar toda la información de golpe, al menos evitar la más sensible, ya que seguramente no sea necesario almacenar la totalidad de los datos en la nube. Además, sobre todo al principio, se recomienda mantener una copia completa del modelo tradicional hasta que no se esté completamente seguro del nuevo sistema y de que la información no es dañada o corrompida.

El NIST reseña los siguientes aspectos que es necesario controlar, clasificados en tres grandes grupos:

Técnicos	**Operacionales**	**Gestión**
Control de acceso	Entrenamiento	Certificación y validación de la información
Auditoría y rendición de cuentas	Planes de contingencia	Planes de acción
Identificación y autenticación	Planes de respuesta en caso de incidente	Gestión de riesgos
Protección el sistema	Mantenimiento	Adquisición de servicios
	Protección de la información	
	Protección física y medioambiental	
	Seguridad personal	
	Integridad del sistema y la información	

Ilustración 11. Criterios de control. Fuente: NIST

Cabe destacar también sus recomendaciones generales con respecto a diferentes aspectos del *Cloud*:

A) Management

- **Migrar los datos a la nube y de la nube**: con respecto a ciertos servicios (tales como el correo electrónico, repositorios compartidos, etc.) el cliente debe desarrollar un plan para migrar los datos e interactuar con ellos una vez que residan en la nube, (incluyendo las descargas). Además, se recomienda formalizar la devolución de los documentos en el caso de cese de contrato o de la migración entre nubes.

- **Continuidad de las operaciones:** en caso de que la pérdida de acceso a una aplicación suponga costes severos y no abordables, se recomienda siempre realizar el trabajo en local a menos que el proveedor esté dispuesto a refundar los servicios. Se debe además asegurar que el proveedor cuenta con planes de continuidad y procedimientos para actualización de servicios del sistema y de modificaciones de las aplicaciones. En caso de interrupción por error de su parte, el proveedor debe asumir en todo caso reembolsar los daños derivados de esto.

- **Conformidad**: El NIST también aconseja determinar si las capacidades para definir los controles necesarios existen dentro del proveedor en particular, si estos controles están siendo implementados de forma apropiada y también de

que estos estén documentados y correctamente examinados (que hayan sido objeto de una auditoría, que cumplan certificaciones de calidad como estándares ISO, etc.).

- **Personal de administración**: asegurar que los procesos se puedan compartimentar entre la administración del proveedor y del cliente.

- **Legalidad**: exigir soporte legal, especialmente garantías en lo que a preservación de datos respecta

- **Políticas operacionales**: destacan en este apartado dos aspectos, en primer lugar establecer políticas en caso de respuesta de incidente para recuperar procesos/prácticas y destinadas para vetar usos privilegiados, tales como al proveedor o a administradores de red.

- **Aceptación de políticas de uso**: Se debe asumir la responsabilidad de asegurar que todos los empleados y usuarios han leído y comprenden completamente las políticas de uso y las consecuencias en caso de incumplimiento. Aunque este punto parezca muy básico *a priori*, es un muy importante.

- **Licencias**: comprobar que todas las licencias de uso y propiedad del software están en regla

- **Gestionar los parches**: en caso de contar con parches de software instalados para trabajar con la aplicación sin conexión.

B) Gobernanza de datos:

- **Estándares de acceso a los datos**: asegurar la capacidad de portabilidad y/o interoperabilidad entre los datos.
- **Separación**: en función del nivel de sensibilidad de la información, el NIST recomienda dividirla en diferentes niveles o incluso en diferentes nubes.
- **Integridad**: mantener la integridad, utilizando por ejemplo *cheksums* y técnicas de replicación
- **Regulaciones**: asesorarse y asegurar que se cumplen todas las leyes
- **Disposición**: requerir mecanismos de eliminación y de prueba en caso de que esa eliminación se produzca.
- **Recuperación**: examinar las capacidades del proveedor con respecto a backups, almacenamiento y recuperación.

C) Seguridad y confiabilidad

- **Vulnerabilidades del cliente**: minimizar las posibles vulnerabilidades a ataques hacker o infección de malware promoviendo buenas prácticas entre los empleados y reforzando los antivirus y medidas de seguridad con el equipo informático.
- **Encriptación :** se recomienda exigir encriptación lo más fuerte posible tanto para las transferencias como para el almacenamiento.
- **Seguridad física**: el contratante debe exigir o en su defecto elaborar por sí mismo planes de seguridad para con los servidores físicos, especialmente en lo que a desastres naturales u otros problemas.
- **Autenticación**: se deben considerar formas avanzadas de autenticación para evitar riesgos de intrusiones.
- **Identificación y control de acceso**: pedir herramientas para ingresar y mantener autorizaciones para usuarios de las aplicaciones del proveedor.
- **Requisitos de actuación:** comprobar siempre el rendimiento de las aplicaciones antes de implementarlas.
- **Visibilidad**: requerir total transparencia en las operaciones

D) Máquinas virtuales

- **Vulnerabilidades**: deben estar protegidas de ataques por parte de otras máquinas virtuales, del *host* y de la red.
- **Migración**: se debe formular una estrategia para la migración entre máquinas virtuales

E) Software y aplicaciones

- **Software de tiempo crítico**: debido al prejuicio que pueden reponer lentas respuestas en caso de que la aplicación sufra retrasos inesperados o inevitables.
- **Software de seguridad crítica**: no se recomiendan aplicaciones de seguridad crítica en este momento, dado a la falta de capacidad para evaluar todos los subsistemas que componen una nube.
- **Herramientas de desarrollo de la aplicación**: se debe preferir servicios que proporcionen herramientas para mitigar la vulnerabilidad y que permitan mejorarla.
- **Soporte de ejecución:** asegurar la funcionalidad y rendimiento de las aplicaciones antes de implementarlas.

- **Configuración**: la aplicación debe poder configurarse de forma segura y además debe permitir integrar las políticas de seguridad de la empresa/archivo.
- **Lenguajes de programación**: deben ser estándares.

A parte de todo lo anterior, se recomienda también:

- Mantener siempre el sistema actualizado y el software en su última versión, especialmente para contar con los últimos parches de seguridad.
- Encriptar el acceso o establecer una identificación más compleja que simplemente usuario y contraseña, para complicar más
- Exigir al proveedor contar con un registro de *logs* para saber quién accede a la aplicación, modifica o borra los ficheros. De hecho, a ser posible, se deberían almacenar esos registros e incluso tener copias de seguridad de los mismos.
- Realizar auditorías periódicas

4. Conclusiones

Las nuevas tecnologías sólo están comenzando su trayectoria y aún queda mucho por investigar y mucho potencial que explotar. Con este trabajo también se pretende desmitificar que las nuevas tecnologías no son seguras, simplemente son una forma diferente de trabajar, lo cual supone que sea necesario estudiar y analizarlas con cuidado, pero sin duda sus ventajas compensan los inconvenientes.

En el caso particular de la nube hemos comprobado que, aunque a priori parezca una solución atractiva para los centros de información, implica una gran cantidad de trabajo previo a la realización de la migración. Tras conocer el funcionamiento básico de la nube y el marco legislativo que la ampara, se ha propuesto una relación de riesgos y estrategias, el cual es el objetivo principal de este trabajo. Es importante conocer la localización del proveedor y sus terceros para saber bajo qué legislación están amparados. También se debe intentar usar modelos normalizados y así permitir la interoperabilidad de la información. Además, cabe destacar la importancia de realizar *backups* y almacenarlos en diferentes lugares, incluido en local.

Además, es necesario insistir y destacar la importancia del archivero en todo el proceso migratorio. Su asesoría debe de tenerse siempre en cuenta, pues es la persona más familiarizada con la gestión de la documentación independientemente del formato en que esta se encuentre.

<u>Desafíos y futuras líneas de investigación:</u>

Todavía es necesario trabajar e investigar mucho en este ámbito, especialmente con respecto a los desafíos de privacidad y seguridad. Este trabajo sólo pretende ser una breve introducción a la gestión documental en la nube, especialmente para concienciar a los Archivos/Unidades de información a la hora de realizar migraciones. Por lo tanto, deja muchos frentes abiertos a la hora de investigar y ampliar la materia.

5. Bibliografía

- Adjei, J. K. (2015). Explaining the role of trust in cloud computing services. Info, 17 (1) págs. 54 – 67. Disponible en: http://dx.doi.org/10.1108/info-09-2014-0042
- Agencia Española De Protección De Datos (2013) Guía para clientes que contraten servicios de Cloud Computing. Disponible en: https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_Cloud.pdf
- Bager, L. Grance, Patt-Corner. R., Voas, J.(2012). Cloud Computing Synopsis and Recommendations: Recommendations of the National Institute of Standards and Technology. National Institute of Standards and Technology, Special Publication 800-146. Disponible en: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-146.pdf
- Beagrie, N., Charlesworth, A., Miller, P. (2014). How Cloud Storage can address the needs of public archives in the UK. The National Archives Guidance on Cloud Storage and Digital Preservation. Disponible en: http://www.nationalarchives.gov.uk/documents/archives/cloud-storage-guidance.pdf
- Can, Liu. (2016). Gestión de la información en la nube: un enfoque preservador. Universidad de Salamanca.
- Fernández, C. M., Recio, M. (2015). Privacidad elevada a la nube. Aenor, 309. ISSN: 2255-2111. Disponible en: http://www.aenor.es/revista/pdf/nov15/20nov15.pdf
- Herrera Bravo, R. (2011). Cloud computing y seguridad: despejando nubes para proteger los datos personales. Revista de Derecho y Ciencias Penales, 17, págs. 43-58, ISSN 0718-302X.
- Instituto Nacional de Tecnologías de la Comunicación (2011) Guía para empresas: seguridad y privacidad del cloud computing. Disponible en: http://www.leonoticias.com/adjuntos/fichero_63594_20111026.pdf

- Johnson, V. Ranade, S., Thomas,. D (2014),"Size matters", Records Management Journal, 24 (3) págs. 224 – 237. Disponible en: http://dx.doi.org/10.1108/RMJ-01-2014-0004
- López, M. de A., Albanese, D. E., Sánchez, M. A. (2014) Gestión de riesgos para la adopción de la computación en nube en entidades financieras de la República Argentina, Contaduría y Administración, 59(3), págs 61-88, ISSN 0186-1042. http://dx.doi.org/10.1016/S0186-1042(14)71266-5
- National Archives of Australia (2014). Cloud computing and information management. Australian Government.
- Ojala, A., Tyrväinen, P. (2011),"Value networks in cloud computing", Journal of Business Strategy, Vol. 32 (6) págs. 40 – 49. Disponible en: http://dx.doi.org/10.1108/02756661111180122
- Oppenheim, C. (2012). Cloud law and contract negotiation. El profesional de la información, 21 (5), págs. 453-457. Disponible en: https://doi.org/10.3145/epi.2012.sep.02
- Saim Ul Haq Quddusi , (2014),"Document management and cloud computing", The TQM Journal, Vol. 26(2) pp. 102 – 108. Disponible en: http://dx.doi.org/10.1108/TQM-06-2012-0038
- Sowmya Karunakaran Venkataraghavan Krishnaswamy Sundarraj Rangaraja P , (2015). Business view of cloud, Management Research Review, Vol. 38 (6) pp. 582 – 604. Disponible en: http://dx.doi.org/10.1108/MRR-01-2014-0021
- Stancic,. H., Rajh, A., Brzica, H. (2015). Archival Cloud Services: Portability, Continuity and Sustainability Aspects of Long-term preservation of Electronically signed records. The Canadian Journal of Information and Library Science, 39(2), págs. 210-228
- Svantesson, D., Clarke, R. (2010). Privacy and consumer risks in cloud computing, 26, págs. 391-397.