

Los Caminos de los Documentos de Archivo Digitales: Tópicos en Preservación Digital

Módulo 8: Introducción al Cómputo en la Nube

InterPARES / ICA
Primera Versión en Español
Octubre, 2013
Traducción del inglés a cargo de:
Alicia Barnard, Alejandro Delgado y Juan Voutssás

Tabla de Contenido

Los Caminos de los Documentos de Archivo Digitales: Tópicos en Preservación Digital 4

1	Prefacio	4
1.1	Acerca del ICA e InterPARES	4
1.2	Público Objetivo.....	6
1.3	Cómo Usar los Módulos.....	6
1.4	Objetivos	6
1.5	Alcance.....	7
1.6	Base de Datos Internacional de Terminología.....	8
	Módulo 8 – Introducción al Cómputo en la Nube	8
2	Introducción.....	8
2.1	Objetivos y Metas.....	9
2.2	Alcance	9
2.3	Resultados del Aprendizaje Esperados.....	9
3	Resumen	10
3.1	Definición de Cómputo en la Nube	10
3.1.1	<i>Características Esenciales</i>	10
3.1.2	<i>Modelos de Servicio</i>	10
3.1.3	<i>Modelos de Despliegue</i>	11
4	Tópicos Clave en la Adopción de Cómputo en la Nube	13
4.1	Escalabilidad	13
4.2	Flexibilidad y Confiabilidad del Servicio.....	13
4.3	Eficiencia y Facilidad de Uso.....	14
4.4	Costos	15
4.5	Interoperabilidad e Integración.....	15
4.6	Cumplimiento y Hallazgo Electrónico	16
4.7	Continuidad de negocio y Recuperación Ante Desastres	17
4.8	Privacidad y Confidencialidad	17
4.9	Propiedad Intelectual y Derechos de Autor.....	18
4.10	Integridad de la Información	18
4.11	Pérdida de Gobernanza.....	18
4.12	Propiedad de los Datos	19
4.13	Recuperación y Destrucción de Información	19
5	Disposición Para el Cómputo en la Nube – Evaluación y Preparación	20
5.1	Marco de Referencia de Toma de Decisiones en la Nube	20
5.2	Colecta de Datos.....	22
5.3	Evaluación Organizacional.....	22
5.4	Selección de los Modelos de Servicio y de Despliegue en la Nube	25
5.5	Análisis de Riesgos y Evaluación.....	25
5.6	Piloto /Implementación en la Nube	26

5.7	Operación en la Nube	26
5.8	Estrategia de Salida	26
6	Preguntas de Revisión	27
7	Recursos Adicionales.....	27
8	Referencias	30
	Apéndice A: Las 10 Preguntas Centrales Para Tercerizar hacia la Nube	32
	Apéndice B: Análisis Contextual	33
	Apéndice C: Análisis de Documentos de Archivo.....	34

Tabla de Figuras

Figura 1: Cómputo en la Nube.....	12
Figura 2: Marco de Toma de Decisiones para el Cómputo en la Nube	21

Los Caminos de los Documentos de Archivo Digitales: Tópicos en Preservación Digital

1 Prefacio

Los Caminos de los Documentos de Archivo Digitales : Tópicos en Preservación Digital es una iniciativa educativa desarrollada conjuntamente por el Consejo Internacional de Archivos –ICA- y el Proyecto InterPARES, - “The International Research on Permanent Authentic Records in Electronic Systems” o “Proyecto de Investigación Internacional en Preservación de Documentos de Archivo Permanentes en Sistemas Electrónicos. Su propósito es ofrecer entrenamiento a archivistas y profesionales de los documentos de archivo en la producción, administración y preservación de documentos de archivo digitales auténticos, fiables y usables. El programa presupone que el lector cuenta con una sólida base en los conceptos fundamentales de la administración de archivos y en la teoría archivística, y sobre ese conocimiento se construye ese documento

“*Los Caminos de los Documentos de Archivo Digitales*” está conformado por ocho módulos. Trata conocimiento teórico y práctico necesario para establecer el marco de referencia, estructura de gobernanza y sistemas requeridos para administrar y preservar documentos de archivo digitales a través de su “ciclo de vida”. Cada módulo trata específicamente un tema relevante para la administración o la preservación de los documentos de archivo. El programa completo se ofrece sin costo en el sitio web del ICA en: <http://www.ica.org>

1.1 Acerca del ICA e InterPARES

El ICA e InterPARES tienen el compromiso de crear materiales educativos para la educación continua de archivistas y administradores de archivos, construir conocimiento básico, diseminar los nuevos hallazgos y dotar a los archivistas y profesionales de los documentos de archivo con el conocimiento y las competencias especializados necesarios para la administración y preservación de documentos de archivo digitales.

El Consejo Internacional de Archivos (ICA) (www.ica.org) está dedicado al manejo eficaz y a la preservación de documentos de archivo, así como al cuidado y uso del patrimonio archivístico mundial a través de su representación por medio de los documentos de archivo y sus profesionales a lo largo de todo el planeta. Los archivos son un recurso increíble: son un subproducto documental del quehacer humano y por tanto testigos irremplazables de eventos pasados, puntales de la democracia, de la identidad de individuos y comunidades, así como de los derechos humanos. Pero también son frágiles y vulnerables. El ICA se esfuerza por proteger a los archivos y asegurar su acceso a través de la asesoría, el establecimiento de estándares, el desarrollo profesional y el impulso del diálogo entre archivistas, tomadores de decisiones, productores y usuarios de archivos.

El ICA es una organización neutral no gubernamental, fundada por sus miembros, los cuales operan por medio de las actividades propias de cada membresía. Por más de sesenta años el ICA ha unido a instituciones archivísticas y practicantes a lo largo del mundo para asesorar acerca de la buena administración archivística y la protección física del patrimonio así registrado, para producir estándares reconocidos y buenas prácticas e impulsar el diálogo, el intercambio y la diseminación de ese conocimiento y experiencia más allá de fronteras internacionales. Con aproximadamente 1500 miembros en 195 países y territorios, el credo del consejo ha sido aprovechar esa diversidad cultural de sus integrantes para entregar soluciones eficaces y una profesión flexible e imaginativa.

El Proyecto InterPARES - The International Research on Permanent Authentic Records in Electronic Systems o Proyecto de Investigación Internacional en Preservación de Documentos de Archivo Permanentes en Sistemas Electrónicos - (www.interpares.org) pretende desarrollar conocimiento original y esencial para la preservación a largo plazo de documentos de archivo producidos y conservados en formatos digitales, así como proveer una base sólida para estándares, políticas, estrategias y planes de acción capaces de asegurar la longevidad de esos materiales documentales y la capacidad de sus usuarios para poder confiar en su autenticidad. El proyecto InterPARES se ha desarrollado en tres etapas:

InterPARES 1 (1999-2001) el cual se enfocó en el desarrollo de teoría y métodos que pudiesen asegurar la preservación de la autenticidad de los documentos de archivo producidos y/o conservados en bases de datos y sistemas de gestión de documentos de archivo durante el curso de las actividades propias de su administración. Los hallazgos de esta etapa presentaron el punto de vista del preservador de los documentos de archivo.

InterPARES 2 (2002-2007) continuó investigando acerca de temas relativos a la autenticidad, fiabilidad y exactitud durante todo el ciclo de vida de los documentos de archivo, desde su producción hasta su preservación permanente. Se enfocó en aquellos documentos de archivo producidos en entornos digitales dinámicos e interactivos a lo largo de actividades artísticas, científicas y gubernamentales.

InterPARES 3 (2007-2012) se construyó con base en los hallazgos de las primeras dos etapas en conjunto con otros proyectos de preservación digital de otras partes del mundo. Llevó la teoría a la práctica trabajando con archivos y unidades archivísticas dentro de organizaciones que tuvieran recursos humanos y/o financieros limitados con el fin de implementar en ellas programas sólidos de administración y preservación archivística.

1.2 Público Objetivo

El público objetivo para el cual está destinado este programa consiste en archivistas y profesionales de la gestión documental y la información interesados en ampliar sus competencias en la administración de archivos digitales. En conjunto, los módulos conforman todo un paquete de recursos documentales para la educación continua de profesionales, con especial énfasis en aquellos temas que impactan en la preservación de documentos de archivo auténticos, fiables y exactos.

1.3 Cómo Usar los Módulos

Cada módulo está conformado por conocimiento teórico y metodológico, así como aplicaciones prácticas ilustradas a través de casos de estudio y escenarios modelo. Si bien los módulos fueron desarrollados por el *Team* Canadá de InterPARES y por tanto ejemplificados con un contexto canadiense, cada uno es adaptable a un dominio específico o contexto jurídico. Para una mayor aplicabilidad, han sido traducidos a los idiomas de los socios del ICA.

Los módulos pueden ser estudiados individualmente o como un conjunto de acuerdo con cada necesidad o interés, y abarcan un rango muy amplio de competencias requeridas. Pueden ser auto-estudiados por personas u ofrecidos por medio de asociaciones profesionales o capacitación laboral. Algunos de los módulos incluyen plantillas que pueden ser adaptadas por universidades o asociaciones profesionales para el desarrollo de cursos curriculares específicos, o como materiales de capacitación específicos para estudiantes y profesionales de la gestión o preservación documental digital. Las universidades y asociaciones profesionales son libres de hacer esas adaptaciones de los materiales y de desarrollar sus propios cursos curriculares o de capacitación con su propio contexto.

1.4 Objetivos

Los módulos tienen los siguientes objetivos:

- Proporcionar recursos educativos basados en investigación actual acerca de temas de documentos de archivo digitales para beneficio de miembros de asociaciones profesionales relacionadas con esa temática;
- Proporcionar a los profesionales de archivos conocimiento teórico y procedimental así como habilidades estratégicas necesarias para desarrollar, implementar y supervisar un sistema de gestión o de preservación de archivos;
- Ilustrar conceptos teóricos con aplicaciones prácticas a través de ejemplos reales extraídos de casos de estudio, asociados a contextos administrativos y tecnológicos específicos;
- Proporcionar contenidos y estructura a programas educativos universitarios para implementar cursos sobre administración o preservación de archivos.

1.5 Alcance

Los Caminos de los Documentos de Archivo Digitales : Tópicos en Preservación Digital consta de los siguientes módulos:

Módulo 1: Introducción – Un Marco de Referencia Para la Preservación Digital

Módulo 2: Desarrollo de Política y Procedimientos Para la Preservación Digital

Módulo 3: Cultura Organizacional y sus Efectos en la Administración Archivística

Módulo 4: Un Resumen de Metadatos

Módulo 5: De Ad Hoc a Regulado– Estrategias de Valoración para Lograr el Control de los Documentos de Archivo Digitales en Ambientes de Red Distribuidos

Módulo 6: Administración y preservación de Correo Electrónico

Módulo 7: Administración y Preservación de Documentos de Archivo en Ambientes Web

Módulo 8: Introducción al Cómputo en la Nube

Cada módulo contiene algunos o todos los siguientes componentes:

- **Resumen** del tema y alcance del módulo;
- **Objetivos de Aprendizaje** y nivel esperado de conocimiento al final del módulo;
- **Metodología** o procedimientos para la aplicación y desarrollo del módulo;
- **Plantillas (cuando apliquen)** para facilitar la implementación del módulo;
- **Ejemplos, Caso(s) de Estudio o Escenarios (cuando apliquen)** con situaciones reales acerca de los temas del módulo;
- **Ejercicios** de los puntos clave del aprendizaje;
- **Preguntas de Revisión** que optimicen la comprensión y entendimiento del tema
- **Recursos Adicionales** para cada tópico, lo cual incluye **lecturas, estándares** y otras plantillas para referencia.

Resumen del Programa en Conjunto			
1. Un Marco de Referencia para la Preservación Digital			Fundamentos
2. Desarrollo de Políticas y Procedimientos para la Preservación Digital			
3.Cultura Organizacional	4. Resumen de Metadatos	5. Estrategias de Valoración	Generalidades
6. Correo Electrónico	7. Sitios Web	8. Cómputo en la Nube	Específico
Base de Datos Internacional de Terminología			Fundamentos

1.6 Base de Datos Internacional de Terminología

La terminología utilizada en los módulos es la que se usa comúnmente por las comunidades que practican la administración archivística. Para asegurar un entendimiento generalizado y reducir un potencial riesgo de confusión que pudiese surgir de prácticas regionales o jurisdiccionales, estos módulos están apoyados por una base de datos de administración de documentos alimentada internacionalmente. Está disponible en www.web-denizen.com/. Pueden verse ciertos términos específicos aún no incluidos en la base de datos en breves glosarios existentes en cada módulo.

Módulo 8 – Introducción al Cómputo en la Nube

2 Introducción

El “cómputo en la nube” –también llamado “computación en la nube”–, consiste en una serie de servicios de cómputo entregados bajo demanda a través de internet desde una ubicación remota o por medio de los servidores de una organización. Siendo todavía un concepto emergente, es un reflejo del cambio en el modelo cliente-servidor hacia el modelo de red, partiendo de entornos aislados hasta la red mundial; permite una perspectiva independiente de la plataforma y ubicación para la comunicación, la colaboración, el almacenamiento y la producción.

La idea básica detrás de “*la nube*” es que todo lo que pueda hacerse en los sistemas informáticos en una organización, –desde el almacenamiento y la colaboración hasta el procesamiento y la comunicación–, se pueden desplazar a la nube. Esencialmente, el cómputo en la nube es un servicio o conjunto de servicios prestados a través de internet, bajo demanda del usuario y desde una ubicación remota, en lugar de residir en un computador de escritorio, una laptop o los servidores de la organización. Así, las organizaciones contratan con un proveedor de servicios que ofrezca almacenamiento, procesamiento y /o aplicaciones a través de la web. Los recursos del cómputo en la nube están disponibles bajo demanda, independientemente de la ubicación y de los dispositivos del usuario, al momento que este los requiera y desde cualquier lugar para acceder a información, aplicaciones y procesamiento.

El cómputo en la nube ofrece flexibilidad y comodidad– siempre y cuando haya acceso a la web; los usuarios pueden trabajar cuando y donde quieran, y a ellos les tiene sin cuidado de dónde vienen los datos de la pantalla, ya que el cómputo en la nube permite a los proveedores utilizar centros de datos distantes para ese propósito.

El cómputo en la nube está siendo rápidamente adoptado por las organizaciones públicas y privadas debido a los potenciales beneficios percibidos, como la relación costo-beneficio, la escalabilidad, rendimiento y comodidad. Sin embargo, los riesgos potenciales de la adopción del cómputo en la nube deben ser plenamente comprendidos

antes de su adopción por las organizaciones con el fin de tomar decisiones bien informadas en torno a su utilización.

2.1 Objetivos y Metas

- El propósito de este módulo es definir las características del cómputo en la nube y explicar sus modelos de servicio y de despliegue, delinear una metodología e identificar las herramientas para el análisis de riesgos cuando se emplea la nube dentro de la organización;
- Este módulo prepara el terreno para ayudar a los potenciales usuarios en el desarrollo de una estrategia de cómputo en la nube y la identificación de los documentos de archivo y procesos que son candidatos potenciales para la subcontratación con terceros –tercerización– en la nube;
- En este módulo ayuda a los usuarios en la identificación de los problemas relacionados con el uso del cómputo en la nube al momento de seleccionar procesos, aplicaciones y documentos de archivo que se pretenda mover hacia ese entorno, así como los requerimientos de negocio, las reglas y los marcos normativos que deben ser examinados en los términos que el cómputo en la nube plantea.

2.2 Alcance

Este módulo proporciona una introducción al cómputo en la nube, a los problemas asociados con la gestión documental y a los desafíos que deben ser considerados antes de que una organización migre sus documentos de archivo y /o servicios a la nube. No tiene la intención de actuar como una herramienta de análisis de riesgos o de desarrollo de políticas; pretende ayudar a los usuarios en el desarrollo de una estrategia organizacional para el cómputo en la nube.

2.3 Resultados del Aprendizaje Esperados

Al término de este módulo, el alumno será capaz de:

- Identificar y comprender las características esenciales del cómputo en la nube;
- Identificar y comprender los tres modelos de servicio del cómputo en la nube;
- Identificar y comprender los cuatro modelos de despliegue del cómputo en la nube;
- Entender los potenciales beneficios del cómputo en la nube;
- Entender los riesgos potenciales y problemas relativos al uso del cómputo en la nube;
- Entender las estrategias para identificar los riesgos en el uso del cómputo en la nube por parte de su organización y hacer preguntas clave que ayuden en el establecimiento de esos;
- Saber dónde encontrar información y recursos adicionales que faciliten la comprensión e implementación de la tecnología del cómputo en la nube.

3 Resumen

3.1 Definición de “Cómputo en la Nube”

El Instituto Nacional de Estándares y Tecnologías –National Institute of Standards and Technology (NIST)– provee actualmente la definición más amplia y adoptada acerca del cómputo en la nube. Esta definición identifica cinco características esenciales acerca de este tema, así como tres “modelos de servicio” y cuatro “modelos de despliegue”. De acuerdo con la definición del NIST:

El Cómputo en la Nube es un modelo para crear vía la red acceso conveniente, ubicuo y bajo demanda a un conjunto compartido de recursos de cómputo configurables (por ej., redes, servidores, almacenamiento, aplicaciones y servicios), los cuales pueden ser rápidamente asignados y provistos con un mínimo de gestión administrativa e interacción con el proveedor. Este modelo promueve la disponibilidad; tiene cinco características esenciales, tres modelos de servicio y cuatro modelos de despliegue.

3.1.1 Características Esenciales

Auto servicio bajo demanda: Los usuarios pueden proveerse de capacidades computacionales (por ej., tiempo en servidores o redes, almacenamiento, etc.) conforme las requieran, sin asistencia por parte del proveedor de esos servicios.

Amplio acceso a la red: la disponibilidad de la red con acceso a internet usando dispositivos estándares (por ej., teléfonos, móviles, laptops, etc.)

Conmutación de recursos: un modelo multi-propietario que conmuta recursos a varios usuarios.

Rápida elasticidad: capacidad de los usuarios para aumentar o disminuir rápidamente las capacidades demandadas a la nube.

Servicio medido: el consumo de los recursos es cuantificado, controlado y reportado, permitiendo así a los usuarios pagar con base a su consumo de cada tipo de servicio (por ej., almacenamiento, proceso, ancho de banda, etc.)

3.1.2 Modelos de Servicio

Software como Servicio (Software as a Service o SaaS): La capacidad ofrecida al usuario para usar los programas y aplicaciones del proveedor y que son ejecutadas en la infraestructura de la nube. Tales aplicaciones son accesibles desde diferentes dispositivos del cliente a través de una interfaz ligera de cliente como un navegador web (por ejemplo, el correo electrónico basado en la web). El usuario no administra ni controla la infraestructura de nube subyacente tales como la red, servidores, sistemas operativos,

almacenamiento o incluso capacidades de aplicaciones individuales, con la posible excepción de algunas limitadas configuraciones específicas del usuario que le son permitidas.

Plataforma como Servicio (Platform as a Service o PaaS): La capacidad ofrecida al usuario para desplegar sobre la infraestructura de nube aplicaciones desarrolladas o adquiridas con lenguajes y herramientas de programación aportados por el proveedor. El consumidor no gestiona ni controla la infraestructura de nube subyacente tales como redes, servidores, sistemas operativos, o de almacenamiento, pero tiene control sobre las aplicaciones desplegadas y posiblemente las configuraciones de entorno del alojamiento de esas aplicaciones.

Infraestructura como Servicio (Infrastructure as a Service o IaaS): La capacidad ofrecida al usuario de proveerle procesamiento, almacenamiento, redes y otros recursos informáticos fundamentales donde el usuario es capaz de instalar y ejecutar software a voluntad, tales como sistemas operativos y / o aplicaciones. El usuario no administra ni controla la infraestructura de nube subyacente pero tiene el control de los sistemas operativos, almacenamiento, aplicaciones desplegadas y algún control limitado de componentes de red seleccionados (por ejemplo, cortafuegos de servidores).

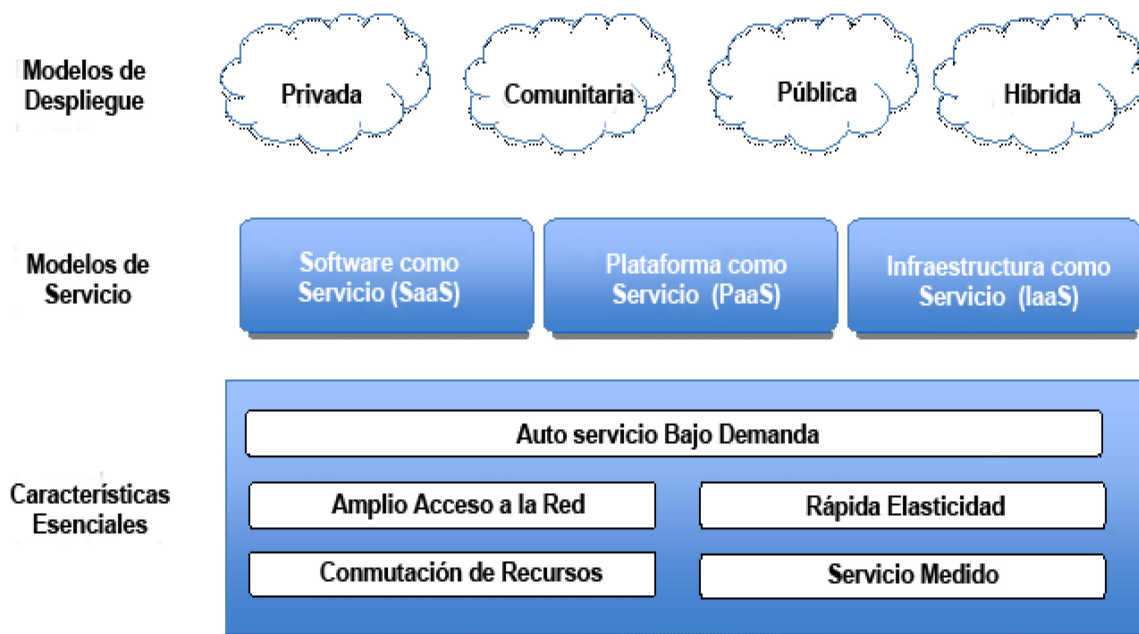
3.1.3 Modelos de Despliegue

Nube Privada: La infraestructura de nube es operada únicamente por una organización. Puede ser manejada por la organización en sí o por un tercero dentro o fuera de las instalaciones.

Nube Comunitaria: La infraestructura de nube es compartida por varias organizaciones y apoya a una comunidad específica que comparte ciertas afinidades (por ejemplo, la misión, los requisitos de seguridad, políticas u objetivos). Puede ser administrada por las organizaciones o por un tercero, y puede existir en las instalaciones o fuera de ellas.

Nube Pública: La infraestructura de nube se hace disponible al público en general o a un gran grupo industrial, y pertenece a una organización que vende esos servicios en la nube.

Nube Híbrida: La infraestructura de nube es una agregación de dos o más tipos de nubes (privada, comunitaria o pública) las cuales siguen siendo entidades únicas, pero están unidos por tecnología estandarizada o propietaria que permite la portabilidad de datos y aplicaciones (por ejemplo, dispersión de recursos dentro de la nube para balancear la carga entre ellas).



Adaptado de NIST. (2009). *Presentación en "Effectively and Securely Using the Cloud Computing Paradigm v26"*. Disponible en <http://csrc.nist.gov/groups/SNS/cloud-computing/> y en: Nicole Convery. "Cloud Computing Toolkit: Guidance for Outsourcing Information Storage to the Cloud". Disponible en: www.archives.org.uk/images/documents/Cloud_Computing_Toolkit-2.pdf

Figura 1: Cómputo en la Nube

4 Tópicos Clave en el Cómputo en la Nube

Los beneficios potenciales para una organización en una eventual migración de su información y procesos de negocio hacia la nube son numerosos; sin embargo, mucho depende del contexto organizacional en el que los servicios en la nube se implementan y la elección de los servicios y modelos de despliegue elegidos. Migrar información y servicios a la nube no está exento de riesgos y desafíos. Si bien por lo general las cuestiones de la seguridad y la disponibilidad son preocupaciones comunes en el cómputo en la nube, un cierto número de otros desafíos dependerá del entorno de nube y servicios elegidos por el usuario. Aquellos que consideran la posibilidad de migración de información y servicios hacia la nube deben obtener una comprensión completa de los beneficios y riesgos asociados con el cómputo en la nube y mitigar así los riesgos mediante la adopción de un enfoque basado en el riesgo y una planificación que considere cuáles de sus registros y / o procesos son los más adecuados para el ambiente de la nube.

4.1 Escalabilidad

El empleo del cómputo en la nube permite a las organizaciones aprovechar la infraestructura compartida y ganar con las economías de escala. “El cómputo en la nube lleva la economía de las TIC a la cabeza, debido a una elasticidad de recursos sin precedentes” (Wyld, 2009). Los usuarios pueden proveerse de recursos computacionales bajo demanda, eliminando el requisito de pronósticos de uso predeterminados, escalando los servicios que requiere la organización cuando están en su máximo y reduciéndolos durante periodos menos demandantes. La escalabilidad es “la capacidad de un sistema informático para crecer con relativa facilidad en respuesta a una creciente demanda” (Langley, 2008). Este cambio en las TIC como modelo de consumo “tipo servicios públicos” puede proporcionar beneficios a las organizaciones a través del intercambio de recursos agregados a lo largo de plataformas y puede eliminar grandes inversiones en infraestructura y aplicaciones dentro de la empresa. Las soluciones de cómputo en la nube son ideales en situaciones que experimentan picos en la demanda de recursos informáticos - tanto en el sector público como en el privado- y donde esos cambios en la demanda de recursos puede variar desde poca o ninguna demanda a la necesidad de manejar grandes cantidades de datos o de procesamiento. Los beneficios de escalabilidad se pueden garantizar siempre que el uso del cómputo en la nube se controle y, -si es necesario-, sea regulado por las organizaciones para asegurar que la relación costo-beneficio sea adecuada (Convery, 2010).

4.2 Flexibilidad y Confiabilidad del Servicio

Los proveedores de cómputo en la nube pueden ofrecer a menudo una mayor confiabilidad con respecto a servicios considerados tradicionales dentro de una empresa de servicios de TIC. Debido a que los proveedores de cómputo en la nube poseen grandes recursos de computación, la eventual falla en su servidor raramente afecta a los servicios prestados a los usuarios, ya que aplicaciones y servicios pueden ser automáticamente redirigidos a otros servidores. La información de un usuario se almacena por lo general de forma redundante en varios servidores en múltiples ubicaciones lo que ayuda en la

prevención de pérdida de información en caso de una interrupción o caída de un centro de datos. Esta idea de que no exista un único punto con posibilidad de falla proporciona a los usuarios un alto grado de flexibilidad en los recursos informáticos. Los proveedores de servicios de cómputo en la nube con frecuencia garantizan un cierto punto de referencia de la disponibilidad de los servicios en lo que se conoce como “Acuerdo de Nivel de Servicio” (Service Level Agreement o SLA), a menudo hasta un máximo de 99,99 % del tiempo posible, (lo cual se traduce a sólo 52 minutos o menos de inactividad del servicio al año. La adición de más “nueves” en el porcentaje de tiempo garantizado operativo tiene un impacto considerable en los costos del acuerdo.

A pesar del alto nivel de garantía de servicio de los proveedores de cómputo en la nube, la mayoría de las organizaciones son reacias a utilizar la nube para el almacenamiento de datos e información de “misión crítica”, independientemente de los posibles beneficios financieros y de eficiencia. Los proveedores de cómputo en la nube llegan a tener interrupciones (por ejemplo, G-mail tuvo un corte de 100 minutos en septiembre de 2009), las cuales están fuera del control del usuario. Además, los proveedores de la nube son más propensos a intrusos maliciosos o personal interno malintencionado y deben por tanto ser capaces de reaccionar ante tales amenazas con rapidez y eficacia. Si bien los acuerdos SLA abonan por lo general una indemnización en caso de una caída del sistema, la responsabilidad por los daños causados por la interrupción del servicio recaerá en el usuario y si tal interrupción se produce en un momento crítico, esa compensación podría significar poco a la luz de las pérdidas comerciales de reputación y futuras pérdidas con motivo de dicha interrupción (Convery, 2010). La asignación de recursos por parte del proveedor de la nube también puede afectar a la fiabilidad del servicio para los usuarios. Una subestimación por parte del proveedor puede dar lugar a una lentificación o interrupción en el servicio a los usuarios.

El cómputo en la nube se encuentra todavía en una relativa infancia, y por lo mismo, no existen normas o directrices generales reguladas para la interacción con los usuarios. Como modelo de negocio con fines de lucro, los proveedores de cómputo en la nube están sujetos a condiciones de mercado, adquisiciones y absorciones de empresas, etc. Si un proveedor de cómputo en la nube deja de operar súbitamente o es comprado por otra compañía, pueden ocurrir inesperadamente cambios en los servicios lo cual puede tener un efecto negativo sobre las organizaciones que utilizan sus servicios y aplicaciones – incluyendo la pérdida de datos, interrupciones en las operaciones comerciales y / o servicios al cliente, etc. Las organizaciones deben investigar la reputación, historia y sostenibilidad potencial de un proveedor de la nube antes de tomar la decisión de asociarse con él.

4.3 Eficiencia y Facilidad de Uso

La naturaleza del cómputo en la nube permite el acceso fácil y casi inmediato a los servicios y aplicaciones, en comparación con el modelo de organización más tradicional de compra, instalación y despliegue de equipo / programas. Dado que los servicios y aplicaciones se encuentran “en la nube”, los usuarios pueden tener acceso a ellos desde prácticamente cualquier lugar en el que puedan acceder a internet. Además, el cómputo en la nube permite a las organizaciones “probar” los servicios y aplicaciones cuando así

lo decida sin grandes gastos y con una mínima pérdida financiera. El entorno de nube puede permitir a algunos usuarios el uso de nuevas soluciones tecnológicas y / o económicos que de otra forma no le serían viables, y la eficiencia proporcionada por la nube puede permitir esta reasignación de los recursos de TIC a otras tareas.

4.4 Costos

Debido a que los recursos de infraestructura se comparten entre un gran número de aplicaciones y usuarios, el cómputo en la nube puede disminuir o eliminar en gran medida la compra de infraestructura organizativa y los costos de mantenimiento. El cómputo en la nube puede implicar una reducción del gasto en TIC ya que con él las organizaciones no están obligadas a hacer grandes gastos, ya que pueden emplear un modelo de compra bajo demanda, con sólo la compra de los recursos informáticos que necesitan para realizar su negocio en cualquier momento dado. Las organizaciones pueden tratar las aplicaciones y servicios de cómputo en la nube como gasto operativo y no como gasto de capital. El uso organizacional de los recursos de cómputo en la nube reduce los costes operativos mediante la reducción o reasignación del personal de TIC dentro de la empresa, utilizando así más eficazmente los recursos humanos. Eficiencias adicionales en los costos provienen de la reducción del consumo de energía, la reducción de la pérdida de tiempo debido a retrasos en las operaciones computacionales, y la reducción en el desperdicio de recursos tales como el espacio de un servidor sin usar. A pesar de estos ahorros de costes aparentes, las organizaciones deben calcular el coste total en que se incurrirá al mover documentos de archivo y servicios a la nube (incluyendo un examen y evaluación de la estructura de precios de los proveedores de estos servicios), y llevando a cabo un análisis de la relación costo-beneficio para identificar los verdaderos costos antes de mover los documentos de archivo y servicios a la nube.

4.5 Interoperabilidad e Integración

El cómputo en la nube es una industria emergente. Hay una falta actual de normalización,¹ y el uso de interfaces propietarias y de software en la industria de la nube está orientado hacia los mejores intereses de sus proveedores, ya que trabaja para mantener a los clientes cautivos (Convery, 2010). Esta falta de interfaces estandarizadas y procedimientos pueden obstaculizar la capacidad de una organización para combinar con eficacia una variedad de servicios en la nube e intercambiar información entre múltiples proveedores de ese entorno. Las organizaciones deben emplear estrategias de estándares abiertos, interoperabilidad y portabilidad de la información con el fin de evitar y / o mitigar el hecho de quedar anclados con un cierto proveedor. A pesar de la tercerización de aplicaciones y servicios, el nivel de gestión y mantenimiento por parte de la organización puede fluctuar dependiendo del modelo de nube elegido.

¹ Existen iniciativas tales como www.cloud-standards.org tendientes a estandarizar APIs y procedimientos.

La integración de los servicios en la nube en una organización donde ya existe un entorno de servicios de TIC debe tener en cuenta que ambos ambientes deben ser integrados. La migración hacia la nube impacta sobre la arquitectura existente, en particular en las nuevas aplicaciones y servicios en la nube que interactúan con los sistemas ya existentes en la organización. Los servicios de cómputo en la nube pueden limitar las posibilidades de personalización de aplicaciones y servicios, incrementando la complejidad de la integración de éstos en los sistemas existentes. Antes de mudarse a la nube es necesaria una evaluación del impacto en los procesos de negocio existentes para asegurar que los obstáculos técnicos son considerados.

4.6 Cumplimiento y Hallazgo Electrónico

El almacenamiento de la información en la nube debe tomar en consideración el cumplimiento de la normativa de protección de datos aplicable al contexto jurídico de la organización involucrada. Los temas relativos a dónde se almacena la información, las medidas de seguridad para protegerla, la capacidad de accederla y la capacidad para asegurar su autenticidad son cuestiones que deben ser tomadas en cuenta por las organizaciones usuarias de la nube.

La información almacenada a lo largo de varias jurisdicciones puede ser susceptible de divulgación y de incautación por parte de gobiernos extranjeros o agencias cuya legislación pueda estar en conflicto con la de la organización de origen. Dado que los servicios en la nube operan bajo el principio de ambientes compartidos multi-propietario, la información almacenada en la nube puede estar en peligro de ser divulgada o incautada debido a su proximidad con la información de otros usuarios que sean perseguidos en una acción legal. “La Ley Patriota de los E.U.A., la Ley de Seguridad Nacional, y demás legislaciones relacionadas con la seguridad, junto con sofisticadas tecnologías electrónicas de recopilación de información, permiten a los gobiernos tener acceso a la información electrónica en prácticamente cualquier contexto” (Jaeger, Lin & Grimes, 2008). Una variedad de asuntos legales puede surgir con respecto a la información almacenada en servidores remotos incluyendo la recopilación de datos que es decomisada en “grados diversos” al sujeto al que se persigue (Jaeger, Lin & Grimes, 2008), así como información sensible de una organización inocente puede quedar atrapada en una investigación (Jaeger, Lin & Grimes, 2008). Los usuarios de la nube deben estar conscientes de sus requerimientos jurídicos y reglamentarios relacionados a su jurisdicción y asegurar que la información almacenada en la nube cumple con ellos.

En caso de litigio, los usuarios de aplicaciones y servicios en la nube deben ser capaces de localizar y obtener información de la nube con eficacia durante el proceso de búsqueda de hallazgo electrónico –e-hallazgo– sin dañar la autenticidad e integridad de esa información. Debido a la naturaleza dinámica de la nube, la localización de la información en cualquier momento dado puede ser difícil e impactar sobre su recuperación oportuna.

La relativa novedad de los servicios del cómputo en la nube implica que la mayoría de los estándares de cumplimiento y seguridad no fueron diseñados para ese entorno de nube y pueden por tanto afectar la certificación y fiabilidad por parte de sus usuarios.

Ejercicios:

- Identifique los marcos legislativo y normativo que apliquen a los documentos de archivo de su organización.
- ¿Qué tanto impactaría el potencial almacenamiento de sus documentos de archivo en la nube con la capacidad de su organización para cumplir con ese marco legislativo?

4.7 Continuidad de Negocio y Recuperación en Casos de Desastre

El cómputo en la nube puede proporcionar a las organizaciones estrategias de continuidad de negocio y de recuperación ante desastres eficazmente y a bajo costo. Las organizaciones pueden utilizar la infraestructura de nube para facilitar la redundancia de la información almacenada fuera del sitio, lo que reduce enormemente los costos de equipo asociado con el respaldo tradicional y los modelos de recuperación ante desastres.

Las interrupciones en el servicio de internet pueden afectar a los servicios en la nube y perturbar la continuidad del negocio. La naturaleza dinámica de la nube puede implicar que la información almacenada no esté disponible de inmediato en caso de un desastre. Puede llegar a incurrirse en costos adicionales con motivo de servicios de supervisión y seguridad necesarios con el fin de cumplir con las obligaciones de rendimiento. La continuidad del negocio y la planificación de recuperación en casos de desastre deben ser planeadas, probadas y documentadas.

4.8 Privacidad y Confidencialidad

El acceso no autorizado a datos privados y confidenciales es un problema de privacidad de la información que existe en la nube. Los datos de un usuario pueden residir en múltiples jurisdicciones que por lo mismo presuponen riesgos para la seguridad de esos datos personales y confidenciales. Los centros de datos que residen en ubicaciones consideradas de “alto riesgo” pueden estar sujetos a “impredecibles marcos jurídicos y de ejecución” lo cual puede implicar que datos personales sean susceptible a acceso no autorizado por parte de terceros. La responsabilidad de mantener segura la información se transfiere al proveedor de la nube en ese tipo de entornos; sin embargo, la responsabilidad de salvaguardar la información personal y confidencial recae siempre en la organización usuaria de la nube ya que fue el colector de la información.

Puede ser difícil para los usuarios de la nube controlar eficazmente el manejo de los datos y las técnicas de procesamiento de los proveedores de la nube para asegurar que los datos sean manejados legalmente y de acuerdo con las necesidades de la organización usuaria. Como “controlador” de la información, el usuario de la nube es responsable de la seguridad de la información personal y confidencial que recoge, aun si existiese mal manejo de los datos de carácter personal y confidencial por parte del proveedor de la nube. Asegurar que los proveedores de servicios cumplan con los requisitos de la legislación sobre privacidad, el empleo de un “régimen robusto de acceso y gestión de

autenticación” y un buen cifrado de datos (Convery, 2010) pueden ayudar a garantizar la protección de la información personal y confidencial que reside en la nube.

4.9 Propiedad Intelectual y Derechos de Autor

Debido a que internet traspasa los dominios internacionales, la aplicación de las leyes de propiedad intelectual y derechos de autor puede ser un problema todavía más amplio y más difícil de navegar cuando la información se almacena en la nube en servidores remotos. Preguntas difíciles surgen acerca de cuáles leyes se aplican a esta información y cuáles son las responsabilidades de la organización que crea y posee esta información.

La divulgación no autorizada de secretos comerciales puede ser un problema para las organizaciones que almacenan este tipo de información en la nube.

4.10 Integridad de la Información

La mayoría de las arquitecturas de nube carecen de estándares formales que rijan la manera en que los datos se almacenan y manipulan, y muchas aplicaciones en la nube carecen de las funciones de gestión documental comunes en las aplicaciones típicas de ese corte, por lo que es difícil para las organizaciones usuarias de la nube cumplir con los requisitos de gestión documental.

La autenticidad y fiabilidad de la información están vinculadas a la capacidad de demostrar su cadena de custodia. Gran parte de la responsabilidad del almacenamiento y procesamiento de información en el entorno de la nube reside con el proveedor de ese servicio en ese entorno. El mantener la autenticidad (o la apariencia de autenticidad) puede ser difícil de implementar en un entorno de nube, ya que es más susceptible a acceso no autorizado como resultado de la interceptación a través de la transferencia en redes no seguras, combinado con datos en entornos de multi-propietarios, y la destrucción ineficaz de ellos.

4.11 Pérdida de Gobernanza

El incremento del uso del cómputo en la nube uso aumenta la necesidad de gobernanza. “La gobernanza implica el control y supervisión de las políticas, procedimientos y estándares para el desarrollo de aplicaciones, así como el diseño, implementación, pruebas y supervisión de los servicios desplegados” (Jansen & Grance, 2011). Debido a la naturaleza del cómputo en la nube, y la capacidad de los usuarios (empleados) para contratar fácilmente servicios en ese entorno, el llegar fácilmente a la falta de control por parte de la organización es una posibilidad real en el entorno de la nube. Las responsabilidades de seguridad de la información para aquella almacenada en la nube se transfieren al proveedor de la nube. El nivel de control que un usuario de la nube tiene sobre su seguridad a menudo depende del modelo de servicio de nube elegido –que puede ir desde poco o ningún control sobre un proveedor de infraestructura de SaaS, hasta un mayor control de las aplicaciones y sistemas en un entorno IaaS.

La pérdida de gobernanza puede llevar a las organizaciones a una incapacidad e cumplir con los requerimientos legales y regulatorios así como a una incapacidad de poder

demostrar la autenticidad y fiabilidad de la información que tienen almacenada en la nube (Convery, 2010).

4.12 Propiedad de los Datos

El claro establecimiento de la propiedad de una organización sobre su información almacenada en la nube es un componente esencial del contrato de servicio. Como lo ilustran los datos que residen en muchos sitios de redes sociales, la propiedad de los datos y los derechos de privacidad puede ser víctimas de acuerdos de servicios ambiguos. Las organizaciones deben asegurarse a toda costa de mantener sus derechos de propiedad y de que el proveedor de la nube no adquiera derechos de propiedad, concesión de licenciamientos ni uso sobre la información de la organización.

4.13 Recuperación y Destrucción de la Información

Las prácticas de administración de archivos requieren que la destrucción sistemática de estos se produzca con el fin de cumplir con la tabla de retención de la organización. El cumplimiento eficaz de la destrucción de documentos de archivo puede ser difícil de lograr en el entorno de la nube. La eliminación de datos insegura o incompleta es un problema existente en el entorno de la nube en donde la “eliminación de datos adecuada y oportuna puede ser imposible” debido a la falta de disponibilidad de copias adicionales almacenadas o porque el modelo multi-propietario de la nube puede tener los datos de los clientes en un modelo de espacio de disco compartido (ENISA, 2009). Las organizaciones pueden describir las claves de cifrado y otros métodos para ayudar en el logro de una destrucción eficaz de los documentos de archivo almacenados en la nube.

Si bien la replicación de la información en varios lugares de la nube como método de redundancia puede beneficiar a las organizaciones, el cumplimiento de las leyes acerca de libertad de la información y de acceso y protección de privacidad requiere que las organizaciones estén muy al tanto de la cantidad de copias de su información que existen y dónde residen con el fin de cumplir con dicha legislación.

“Si la extracción de la información requiere un cambio de formato de la información, ello puede tener graves consecuencias para la autenticidad y fiabilidad de los documentos de archivo corporativos e impactar sobre su admisibilidad legal” (Convery, 2010).



Véase el Apéndice ‘A’ acerca de diez preguntas centrales para hacer al momento de tercerizar hacia la nube.

5 Disposición Para el Cómputo en la Nube – Evaluación y Preparación

El cómputo en la nube es una herramienta que necesitará ser acomodada dentro de la estrategia general de la organización; ayuda en el apoyo a la misión y la estrategia general de negocio de la organización. La tercerización del almacenamiento de documentos de archivo y procesos de la organización en el entorno de nube puede beneficiar a las organizaciones a través del ahorro de costos, escalabilidad y conveniencia. La evaluación por parte de la organización debe tener en cuenta las necesidades de negocio de la organización, el riesgo y los marcos normativos en los cuales los documentos de archivo, procesos y aplicaciones puedan ser efectivamente migradas a la nube (Convery, 2010).



Véase “Cloud Computing Toolkit: Guidance for Outsourcing Information Storage to the Cloud” en:
www.archives.org.uk/images/documents/Cloud_Computing_Toolkit-2.pdf

La utilización de un marco de decisión para evaluar el grado de disposición de su organización en el entorno de nube para preparar y migrar documentos de archivo y servicios hacia la nube ayudará a identificar cualquier problema así como cuáles de esos documentos y procesos son los más adecuados para el entorno de la nube.

5.1 Marco de Referencia de Toma de Decisiones en la Nube

El *Marco de Referencia de Toma de Decisiones en la Nube* se divide en las fases siguientes:

1. Recolectar datos sobre los servicios de cómputo en la nube y modelos de despliegue, así como de los proveedores de servicios en la nube;
2. Llevar a cabo una evaluación de la organización para identificar cuáles documentos de archivo, aplicaciones y procesos son potenciales candidatos para migración al entorno de nube;
3. Determinar cuáles servicios en la nube y modelos de despliegue son aptos para el modelo de negocio de su organización, su gobernanza y los requisitos de cumplimiento;
4. Llevar a cabo una evaluación de riesgos para los documentos de archivo, aplicaciones y procesos en caso de trasladarse a la nube, incluyendo la identificación, análisis y desarrollo de un plan de respuesta al riesgo;
5. Llevar a cabo un proyecto piloto en la nube para la organización, moviendo los registros identificados, aplicaciones y procesos hacia el entorno de nube;
6. Tomar en cuenta la serie de cuestiones que deben preverse para la continua administración de archivos, aplicaciones y procesos ya trasladados a la nube - incluyendo la gestión documental y la clasificación, el cumplimiento, el seguimiento y la auditoría, la seguridad y el acceso permanente;
7. Antes de mover los documentos de archivo, aplicaciones o procesos a la nube, las organizaciones deben garantizar que los procedimientos son adecuados

para obtener información de los sistemas del proveedor de nube y ser transferidos a otro proveedor de servicios o hacia la organización.

El *Marco de Referencia de Toma de decisiones en la Nube* es una serie de pasos, algunos de los cuales son iterativos y puede ocurrir simultáneamente. Las siguientes subsecciones amplían cada fase del marco.

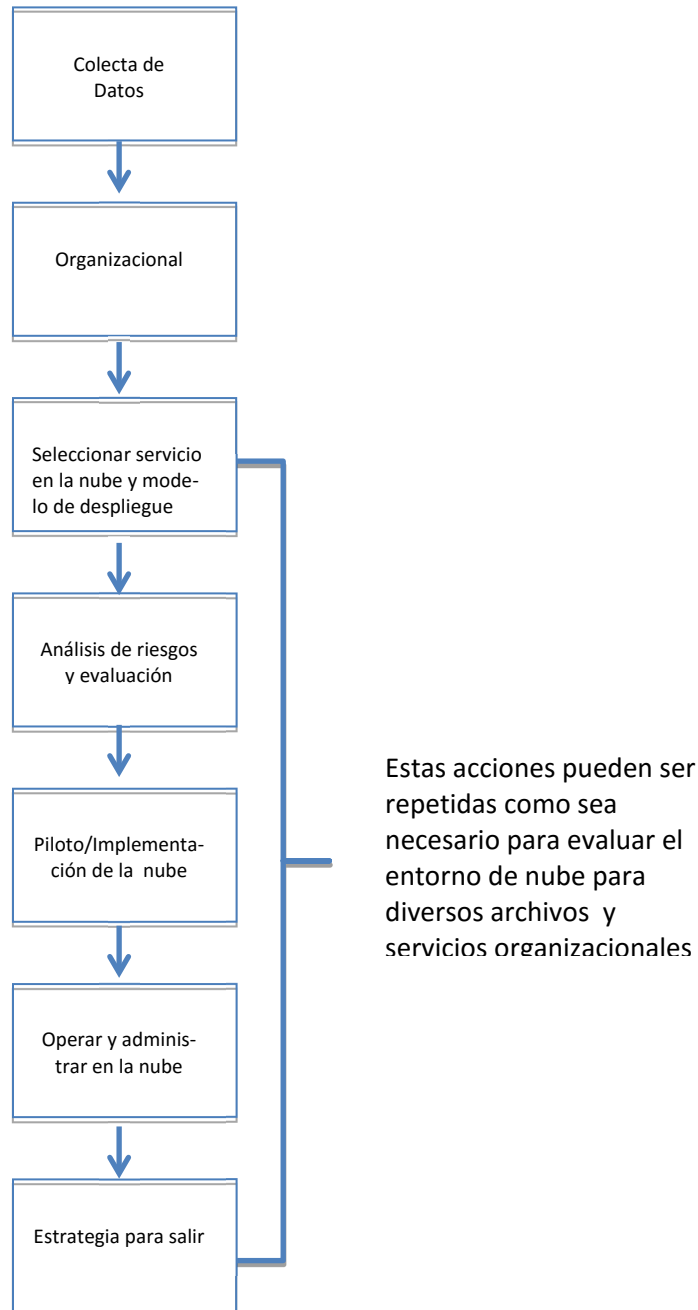


Figura 2: Marco de Referencia de Toma de Decisiones en la Nube

5.2 Recolección de Datos

El marco de referencia para la toma de decisiones comienza con el aprendizaje de los fundamentos del cómputo en la nube. La lectura de las definiciones y los recursos disponibles, la asistencia a seminarios y / o talleres y la plática con los proveedores de cómputo en la nube serán de gran ayuda para las personas a fin de obtener un conocimiento profundo del cómputo en la nube y sus diferentes modelos. Es importante asegurarse de que no sólo el personal de TIC sea educado en el funcionamiento del cómputo en la nube, ya que también los tomadores de decisiones deben estar informados.

Existen varios recursos disponibles enumerados en la sección seis los cuales ayudarán a los usuarios a profundizar en el conocimiento del cómputo en la nube y los temas principales involucrados en su adopción. Muchos de esos recursos comprenden bibliografías que a su vez llevan a una red más amplia de recursos.

Ejercicio:

- Identifique a los tomadores de decisiones y desarrolladores de políticas dentro de su organización quienes serían candidatos para educación acerca de cómputo en la nube.

5.3 Evaluación de la Organización

A fin de tomar ventaja con éxito de los beneficios de la migración de documentos de archivo, aplicaciones y procesos hacia la nube, las organizaciones deben identificar cuáles de esos documentos y procesos de su organización son adecuados para la mudanza.

El nivel de detalle en el que las organizaciones realizan evaluaciones acerca de cuáles activos se podrían trasladar a la nube puede variar dependiendo de sus requerimientos de negocio y los marcos regulatorios y de cumplimiento. Las organizaciones pueden tener un marco de referencia existente que ya utilicen para evaluar posibles proyectos de tercerización, el cual puede ser adecuado para esta tarea específica. Alternativamente, la recolección interna de datos ayudará a las organizaciones a evaluar aquellos activos adecuados para el entorno de nube.

(Convery, 2010) identifica una serie de aplicaciones y procesos organizacionales que con frecuencia se adaptan a la migración hacia el entorno de la nube debido al ahorro de costos y una mayor eficiencia o la funcionalidad. Estos abarcan:

- Correo electrónico;
- Gestión documental;
- Herramientas de colaboración;
- Herramientas de Productividad (por ej., sistemas de nómina);

- Almacenamiento a largo plazo de información inactiva.

La realización de un análisis contextual ayudará a identificar los documentos de archivo, aplicaciones y procesos que se pueden trasladar a la nube. Tal análisis puede llevarse a cabo a nivel de toda la organización o podría llevarse a cabo en el contexto de una función de negocio o una sub-unidad organizativa. El análisis contextual recoge información sobre la organización, su estructura administrativa, sus obligaciones legales y reglamentarias con respecto a sus documentos de archivo; las normas y estándares que influyen en la producción del documento de archivo; su mantenimiento y uso, su elaboración y gestión; sus limitaciones, incluyendo la cultura empresarial de la organización; las limitaciones de personal y las limitaciones tecnológicas.



Véase el Apéndice 'B': Análisis Contextual

Obtenga un conocimiento exhaustivo de las prácticas actuales de producción y gestión documental dentro de su organización a través de entrevistas a los productores de los documentos y el análisis de las políticas pertinentes que rigen y limitan la gestión de estos documentos. Examine todos los estándares y mejores prácticas relevantes a su contexto organizacional.



Véase el Apéndice 'C': Análisis de Documentos de Archivo

Un marco de referencia del esquema de clasificación de la organización puede ayudar en la identificación de los documentos de archivo y / o información que se pretende transferir, procesar y almacenar en la nube. Una vez que la información ha sido identificada debe evaluarse en términos de posibles amenazas a la confidencialidad, integridad y disponibilidad con el fin de identificar los parámetros de riesgo aceptables de la información de la organización una vez almacenada en la nube (Convery, 2010).

Objetivos de la Seguridad	Impacto Potencial		
	Bajo	Moderado	Alto
Confidencialidad Preservar restricciones autorizadas acerca del acceso a la información y su divulgación, incluyendo los medios para proteger la privacidad personal y la propiedad de la información. [44 U.S.C., SEC. 3542]	La divulgación no autorizada de información tendría un efecto adverso limitado sobre las operaciones, activos e individuos de la organización.	La divulgación no autorizada de información tendría un efecto adverso serio sobre las operaciones, activos e individuos de la organización.	La divulgación no autorizada de información tendría un efecto adverso severo o catastrófico sobre las operaciones, activos e individuos de la organización.
Integridad Vigilar contra modificación o destrucción no autorizada de información, lo que implica su autenticidad y no repudio. [44 U.S.C., SEC. 3542]	La modificación o destrucción no autorizada de información tendría un efecto adverso limitado sobre las operaciones, activos e individuos de la organización.	La modificación o destrucción no autorizada de información tendría un efecto adverso serio sobre las operaciones, activos e individuos de la organización.	La modificación o destrucción no autorizada de información tendría un efecto adverso severo o catastrófico sobre las operaciones, activos e individuos de la organización.
Disponibilidad Asegurar acceso y uso oportuno y confiable de la información. [44 U.S.C., SEC. 3542]	La interrupción del acceso o uso de la información tendría un efecto adverso limitado sobre las operaciones, activos e individuos de la organización.	La interrupción del acceso o uso de la información tendría un efecto adverso serio sobre las operaciones, activos e individuos de la organización.	La interrupción del acceso o uso de la información tendría un efecto adverso severo o catastrófico sobre las operaciones, activos e individuos de la organización.

(Convery, 2010, adaptado de: *Categorization of federal information and information systems from NIST* (2008) Information security. Vol. 1: Guide for mapping types of information and information system categories. NIST SP800-60. Disponible en-línea en: http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800_Vol1-Rev1.pdf)

Ejercicios:

- ¿Existen documentos de archivo en su organización que puedan ser migrados eficazmente hacia la nube? Identifíquelos.
- ¿Cuáles documentos de archivo de su organización consideraría usted que no deben moverse hacia la nube? ¿Por qué?
- ¿Cuáles aplicaciones y / o servicios actualmente realizados dentro de su organización pudieran ser migrados hacia la nube? ¿Por qué estarían mejor ubicados ahí?

5.4 Selección del Modelo de Servicio de Cómputo en la Nube y Modelo de Despliegue

Una vez que se ha identificado a los documentos de archivo, aplicaciones y procesos que se pueden migrar a la nube, es necesario determinar cuál modelo de servicio en la nube y modelo de despliegue conviene a los principios, gobernanza y requisitos de cumplimiento de su organización (Convery, 2010).

El empleo de un análisis FODA para identificar las fortalezas, oportunidades, debilidades y amenazas para cada modelo de nube puede ser un método eficaz para determinar cuál combinación de despliegue en la nube y modelos de servicio se adaptan mejor a las necesidades de su organización (ENISA, 2011).

Existen importantes ventajas y desventajas en cada modelo de servicio con respecto a las funciones integradas, la complejidad frente a la apertura (extensibilidad) y la seguridad.

- SaaS proporciona la funcionalidad más integrada con la menor extensibilidad y un nivel relativamente alto de seguridad integrada;
- PaaS tiende a ser más extensible que SaaS a costa de características y capacidades “ya preparadas para el cliente”, pero tiene más flexibilidad para construir seguridad adicional;
- IaaS ofrece pocas o ninguna de las características semejantes a las de las aplicaciones, pero tiene gran extensibilidad. Implica que la seguridad está menos integrada más allá de la protección de la infraestructura. Los sistemas operativos, aplicaciones y contenidos son gestionados y asegurados por el usuario.

(CSA, 2009)

Las razones organizacionales para la migración de documentos de archivo, aplicaciones y / o procesos a la nube deben ser informadas a la estrategia global de la organización para el cómputo en la nube, teniendo en cuenta el tipo de negocio de la organización y sus estrategias de TIC (Convery, 2010). La selección de los modelos de servicio y de despliegue en la nube también debe tener en cuenta el grado de control que una organización tendrá sobre la seguridad y el riesgo.

5.5 Análisis y Evaluación de Riesgos

Realizar una evaluación de riesgos de los documentos de archivo aplicaciones y procesos a ser migrados hacia la nube, e incluir la identificación, análisis y desarrollo de un plan de respuesta ante desastres.

Es importante comprender el valor de la información dentro de la organización y los documentos de archivo así como el sistema que usted está considerando para migrar a la nube. La realización de un análisis del contexto de riesgo específico ayudará a las organizaciones a evaluar el riesgo de migrar archivos y procesos a la nube y ayuda en la preparación para la adopción eficaz del cómputo en la nube.



El “marco de referencia de seguridad de información de ENISA” - “ENISA Information Assurance Framework” es un recurso excelente para evaluar el riesgo en la adopción del cómputo en la nube, para comparar a los proveedores de nube, y para la preparación de una adopción eficaz. El marco ofrece una serie de preguntas que una organización puede hacer a un proveedor de la nube a fin de garantizar efectivamente que están protegiendo la información confiada a ellos (estas tienen el propósito de servir como base y deben ser ampliadas de acuerdo con las necesidades particulares de cada organización). Disponible en:
<http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-information-assurance-framework>

5.6 Piloto / Implementación en la Nube

Lleve a cabo un proyecto piloto de su organización en la nube, migrando documentos de archivo, aplicaciones y procesos identificados hacia ese entorno. La supervisión cercana de ese piloto asegurará que los problemas imprevistos son identificados y tratados oportunamente en el proceso. El proceso piloto inicial puede repetirse varias veces hasta que la confianza en la plataforma elegida y / o servicio puede ser establecida y se considere que ya cumple con todos los requisitos necesarios.

5.7 Operación en la Nube

Deben tenerse en cuenta y preverse una serie de cuestiones que deben realizarse en la cotidiana gestión documental, aplicaciones y procesos una vez trasladados a la nube – incluyendo esa gestión documental y su clasificación, el cumplimiento, seguimiento y auditoría, su seguridad y acceso permanente.

5.8 Estrategia de Salida

Antes de migrar los documentos de archivo, aplicaciones o procesos a la nube, las organizaciones deben asegurarse de poseer procedimientos disponibles para recuperar la información de los sistemas del proveedor de nube y poder transferirlos a otro proveedor de esos servicios o de regreso a la organización.

6 Preguntas de Revisión

1. Nombre las cinco características del cómputo en la nube.
2. Identifique y explique los tres modelos de servicios en la nube.
3. Identifique y explique los cuatro modelos de despliegue en la nube.
4. ¿Cuáles son los beneficios y riesgos de la utilización de los efectos de la nube para mejorar la continuidad del negocio y recuperación ante desastres?
5. ¿Cómo se puede utilizar el entorno de cómputo en la nube de forma rentable para las organizaciones?
6. Enumere cinco beneficios para las organizaciones en la migración de aplicaciones y servicios hacia la nube.
7. Enumere cinco riesgos para las organizaciones en la migración de aplicaciones y servicios hacia la nube.

7 Recursos Adicionales

Autor: Australian Government, Department of Finance and Deregulation

Título: *Cloud Computing Strategic Direction Paper*

Fecha de Publicación: Enero 2011

URL: <http://www.finance.gov.au/e-government/strategy-and-governance/cloud-computing.html>

En este trabajo (en inglés) se describe la posición del gobierno australiano acerca del cómputo en la nube. La estrategia del gobierno australiano permite a las agencias elegir servicios basados en la nube si demuestran conveniencia financiera, son aptos para su propósito y son suficientemente seguros. El documento también proporciona una guía sobre lo que es cómputo en la nube e identifica problemas y beneficios del cómputo en la nube para las agencias. La estrategia del gobierno se divide en tres corrientes - Orientación y documentación para las agencias; adopción de la nube en servicios "no clasificados" y el estudio de sus riesgos; y fomentar enfoques estratégicos para el cómputo en la nube.

Autor: Convery, Nicole

Título: *Cloud Computing Toolkit: Guidance for Outsourcing Information Storage to the Cloud*

Fecha de Publicación: Agosto, 2010

URL: www.archives.org.uk/images/documents/Cloud_Computing_Toolkit-2.pdf

Un recurso excelente; este extenso trabajo de investigación (en inglés) es indispensable para los profesionales de la información y los documentos de archivo que están investigando optar por el cómputo en la nube en sus organizaciones.

Autor: Wyld, David c.

Título: *Moving to the Cloud: An Introduction to Cloud Computing in Government*

Fecha de Publicación: 2009

Fuente/Editor: IBM Center for The Business of Government: E-Government Series

URL: <http://www.businessofgovernment.org/report/moving-cloud-introduction-cloud-computing-government>

Un examen del estado del arte del cómputo en la nube en las organizaciones del gobierno estadounidense y los posibles beneficios e inconvenientes de la utilización gubernamental de estos servicios. Proporciona una introducción general a la terminología del cómputo en la nube, modelos y marcos de referencia.

Autor: ENISA

Título: *Security & Resilience in Government Clouds: Making an Informed Decision*

Fecha de Publicación: Enero, 2011

Fuente/Editor: ENISA

URL: <http://www.enisa.europa.eu/act/rm/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds>

Autor: Cloud Security Alliance

Título: *Security Guidance for Critical Areas of Focus in Cloud Computing*

Fecha de Publicación: Diciembre 2009

Fuente/Editor: Cloud Security Alliance

URL: <https://cloudsecurityalliance.org/guidance/>

Este reporte investiga los temas relevantes a la seguridad en la nube, y provee un método de análisis y una guía para decisiones acerca de la seguridad en ese entorno.

8 Referencias

- Askhoj, J., Sugimoto, S., & Nagamori, M. *Preserving Records in the Cloud*. Preprint.
- Armbrust, M., et al.. (2009). Above the Clouds: A Berkeley View of Cloud Computing.
- Australian Government Department of Finance and Deregulation. (April, 2011). *Cloud Computing Strategic Direction Paper*. Disponible en <http://www.finance.gov.au/e-government/strategy-and-governance/cloud-computing.html>
- Australian Government, Department of Innovation, Industry, Science and Research. (October, 2011). IT Industry Innovation Council. *Cloud Computing - Opportunities and Challenges*
- Ball, C. (February, 2011). Facebook Feature Could Ease Cloud-Based EDDL TN Law Technology News.
- Bradshaw, S., Millard, C. & Walden, I.. (2010). *Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services*, Queen Mary School of Law Legal Studies Research Paper no. 63.
- BSA. (2011). *Cloud Computing Policy Agenda for Europe*.
- Cloud Computing Explained* by Rosalyn Metz. Educause Quarterly. Disponible en: <http://www.educause.edu/EDUCAUSE+Quarterly/EDUCAUSEQuarterlyMagazineVolume/CloudComputingExplained/206526>
- Cloud Security Alliance (CSA). (March, 2010) *Top Threats to Cloud Computing v.1.0*. Disponible en <https://cloudsecurityalliance.org/research/projects/top-threats-to-cloud-computing/>
- Convery, Nicole. (August 26, 2010). *Cloud Computing Toolkit: Guidance for Outsourcing Information Storage to the Cloud*. Disponible en http://www.archives.org.uk/images/documents/Cloud_Computing_Toolkit-2.pdf
- Digital Agenda Assembly. (2011). Report from Workshop 18: *Towards a Cloud Computing Strategy for Europe: Matching Supply and Demand*.
- ENISA (November, 2009). *Cloud Computing: Benefits, Risks and Recommendations for Information Security*.
- Jaeger, P. T., Lin, J., & Grimes, J. M. (2008). *Cloud Computing and Information Policy: Computing in a Policy Cloud?*, Journal of Information Technology & Politics, 5(3), 269-283.
- Maxwell, W. & Wolf, C. (May, 2012). *A Global Reality: Governmental Access to Data in the Cloud: A comparative analysis of international jurisdictions Governmental access to data stored in the Cloud – including cross-border access –exists in every jurisdiction*. Hogan Lovells White Paper.
- NIST (2010) *Definition of Cloud Computing v15*. Online. Disponible en <http://csrc.nist.gov/groups/SNS/cloud-computing/>
- O'Brien, K. J. (Sept. 19, 2010). New York Times. *Cloud Computing Hits Snag in Europe*.

Office of the Information and Privacy Commissioner of British Columbia. (February, 2012). Cloud Computing Guidelines for Public Bodies. Disponible en http://www.oipc.bc.ca/news/2012Releases/CloudComputing_Announcement.pdf

Pew Internet and American Life Project. (2010). *The Future of Cloud Computing*.

Stuart, K. & Bromage, D. (2010). *Current state of play: records management and the cloud*. Records Management Journal. 20(2), 217-225.

Wyld, D. C. (2010). *The Cloudy Future of Government IT: Cloud Computing and the Public Sector around the world*. International Journal of Web & Semantic Technology, 1(1).

Apéndice 'A': Las 10 Preguntas Centrales Para Tercerizar Hacia la Nube²

Nicole Convery provee una útil lista acerca de las diez preguntas centrales que deben hacerse los usuarios que contemplan la posibilidad de tercerizar aplicaciones y servicios hacia la nube:

- ¿Cuáles procesos, aplicaciones e información pueden moverse a la nube para ganar eficiencia y rentabilidad al tiempo que satisface la seguridad y los requisitos de cumplimiento de la organización?
- Cómo puede la organización sufrir daños si los sistemas, aplicaciones, servicios e información fueran accedidos por personas no autorizadas y la información se pusiera a disposición del público?
- ¿Cómo están protegidos la información y los sistemas por el proveedor de servicios en la nube contra el acceso no autorizado (por ejemplo, piratería, interceptación, mal uso del usuario)?
- ¿Cómo puede la organización garantizar la integridad, autenticidad y fiabilidad de su información almacenada en la nube?
- ¿Cuáles son las responsabilidades de la organización con respecto a la seguridad de la infraestructura y de la información en la nube dentro de los modelos de servicio y de despliegue elegidos?
- ¿Cómo puede la organización aplicar sus programas de gestión de la información (por ejemplo, clasificación, retención) en el entorno de la nube?
- ¿Cuál es el impacto de la tercerización de servicios e información en la nube respecto de los requisitos legislativos y reglamentarios de la organización (por ejemplo, protección de datos personales, derecho a la información, transparencia, hallazgo electrónico, derechos de autor, licenciamientos, etc.)?
- ¿Cómo debe la organización auditar y controlar los servicios en la nube y establecer en consecuencia los acuerdos de nivel de servicio?
- ¿Puede negociar la organización con el proveedor contratos y acuerdos que se ajusten a su evaluación de riesgos y entorno de cumplimiento?
- ¿Cuáles son los costos totales de la puesta en marcha y la gestión cotidiana de los servicios en la nube?

² Nicole Convery. "Cloud Computing Toolkit: Guidance for outsourcing information storage to the cloud." Department of Information Studies, Aberystwyth University. Archives & Records Association UK & Ireland. 26 August 2010.

Apéndice 'B': Análisis Contextual

El análisis contextual reúne datos sobre la organización y sus marcos regulatorios y legales. Incluye información acerca de la estructura administrativa de la organización, sus obligaciones legales y reglamentarias con respecto a sus documentos de archivo; normas y estándares que influyen en la producción, mantenimiento y uso de esos documentos de archivo; los requisitos para su creación y mantenimiento; sus limitaciones, incluyendo las del personal y tecnológicas; y la cultura de negocios de la organización. Un análisis contextual proporciona la siguiente información.

Posicionamiento Legal y Regulatorio

Identifique y provea la información acerca de todas las leyes, reglamentos, estándares legales o códigos de conducta que gobiernen o afecten la elaboración y mantenimiento de documentos de archivo de su organización, así como los requerimientos para su retención y disposición.

Normas

Identifique y provea la información acerca de los estándares, metodologías, códigos o regulaciones no legales que gobiernen o afecten la elaboración y mantenimiento de documentos de archivo de su organización, así como los requerimientos para su retención y disposición.

Recursos (Físicos)

Resuma la información acerca del contexto físico en el que su organización opera, incluyendo información relevante sobre equipo e infraestructura.

Gobernanza

Documente la estructura de gobernanza de su organización y el proceso de toma de decisiones en lo relativo a administración archivística.

Documente los principios, misión, y su evolución a lo largo del tiempo.

Políticas

Identifique y provea la información acerca de todas las políticas existentes relativas a documentos de archivo; su producción, mantenimiento, retención, disposición y preservación a largo plazo.

Funciones

Liste todas las funciones mayores que lleva a cabo su organización y que resultan en la producción de documentos de archivo.

Apéndice ‘C’: Análisis de Documentos de Archivo

Actividades que generan documentos y documentos de archivo

- Liste los tipos de actividades generales dentro de su organización que desembocan en la producción de documentos y documentos de archivo.
- Identifique a los productores de esos documentos.

Documentos y documentos de archivo resultantes de las actividades

- Liste los tipos principales de documentos y documentos de archivo que resultan de esas actividades.

Existencia de un programa o plan de administración de archivos

- Describa las actividades llevadas a cabo en la organización actualmente y que se relacionan con la gestión documental.
- Analice las políticas que el productor tenga y que rigen la producción y gestión documental.

Individuos responsables del mantenimiento de los documentos de archivo

- Identifique a las personas responsables de administrar los documentos de archivo después de su producción (mantenimiento de documentos de archivo). Pueden ser el personal designado de documentos de archivo, su productor, o ambos.

Existencia de estrategias para el mantenimiento

- Identifique el conjunto de medios prácticos, ya sea formalmente articulados o informalmente implementados, que conforman la gestión documental; esto abarca:
 - La ubicación donde los documentos de archivo son guardados,
 - El medio / soporte en el que son almacenados,
 - Una descripción acerca de cómo están organizados,
 - Una breve descripción acerca de todos los métodos usados para mantenerlos,
 - Una breve descripción acerca de todos los métodos usados para contrarrestar la obsolescencia tecnológica mientras están activos o semi-activos.

Requerimientos y Restricciones Tecnológicas

- Identifique y describa todo el equipo usado en su organización:
 - Arquitectura (por ej., topología de la red, infraestructura, equipos de cómputo),
 - Herramientas de producción o entrada (por ej., programas, cámaras, micrófonos),
 - Herramientas de proceso (por ej., programas, consola).
- Identifique y describa los tipos de documentos producidos (por ej., gráficos, textos, audio).
- Liste los formatos utilizados (por ej., .pdf, .doc, .jpg) e identifique los retos particulares relativos a su mantenimiento y preservación.

- Identifique y describa de qué forma las limitaciones tecnológicas relevantes impactan la producción, forma, contenido, identidad, integridad, organización y preservación de los documentos de archivo.