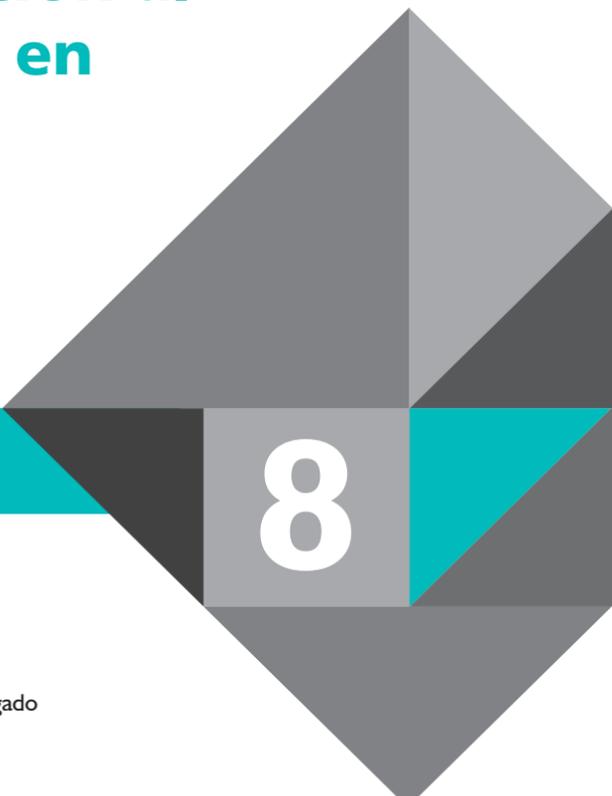


Introducción al cómputo en la nube



8

Traducción al español:
Alicia Barnard, Alejandro Delgado
y Juan Voutssás



**Cuadernos
Digitales de
Archivística**

Serie: Temas
fundamentales de
preservación digital

ARCHIVO GENERAL DE LA NACIÓN

Dirección General: Mercedes de Vega

Dirección General Adjunta de Administración: Alba Alicia Mora Castellanos

Dirección de Publicaciones y Difusión: María Fernanda Treviño Campero

Departamento de Publicaciones: Esther Pérez Guzmán

Coordinación Editorial: Esther Pérez Guzmán

Diseño y formación: Alejandro Amaro Rosas

Diseño de portada: Alejandro Amaro Rosas

Corrección de estilo: Ma. del Carmen Gutiérrez Haces y Francisco J. González Ruiz

Asistencia editorial: Roberto del Vecchyo Calcáneo

Introducción al cómputo en la nube

Traducción al español: Alicia Barnard, Alejandro Delgado y Juan Voutsás

D.R. © a la edición en inglés

ICA/InterPARES

D.R. © Primera edición en español

Archivo General de la Nación

Eduardo Molina núm. 113

Col. Penitenciaría

Deleg. Venustiano Carranza, C.P. 15350

Ciudad de México

Primera edición: octubre de 2016

DERECHO DE USO

Se permite la reproducción, publicación, transmisión, difusión en cualquier modo o medio de cualquier parte del material contenido en el archivo (únicamente texto sin imágenes) sin alterar o modificar el original, con fines de referencia y/o reproducción, académicos o educacionales, con excepción de los personales o comerciales, citando la fuente de referencia y otorgando el crédito correspondiente al autor y al editor.

Contenido

Agradecimientos	6
Prefacio a la edición en inglés	7
Prefacio a la edición en español	8
Acerca de ICA e InterPARES	9
Público objetivo	11
Cómo usar la serie	11
Objetivos	12
Arquitectura modular del programa	13
Alcance.....	15
Introducción	16
Objetivos y metas de este módulo	17
Alcance.....	17
Aprendizajes esperados	18
Panorama.....	19
Características esenciales.....	19
Definición de cómputo en la nube.....	19
Modelos de servicio	20
Modelos de despliegue	21
Puntos clave en la adopción de cómputo en la nube	23
Escalabilidad	23
Flexibilidad y confiabilidad del servicio	24
Eficiencia y facilidad de uso	26
Costos	26
Interoperabilidad e integración.....	27
Cumplimiento y hallazgo electrónico.....	28
Continuidad de negocio y recuperación ante desastre.....	30

Privacidad y confidencialidad	30
Propiedad intelectual y derechos de autor	31
Integridad de la información	32
Pérdida de gobernanza	32
Propiedad de los datos	33
Recuperación y destrucción de información	33
Disposición para el cómputo en la nube: evaluación y preparación.....	35
Marco de referencia para la toma de decisiones en la nube.....	35
Recopilación de datos.....	38
Evaluación de la organización.....	38
Selección del modelo de servicio en la nube y modelo de despliegue	42
Análisis y evaluación de riesgos.....	43
Proyecto piloto/Implementación en la nube.....	44
Operación en la nube	44
Estrategia de salida y retorno a la organización	45
Actividades de revisión	46
Recursos adicionales	47
Referencias	49
Apéndice A: Las 10 preguntas fundamentales para contratar un tercero en la migración hacia la nube	52
Apéndice B: Análisis contextual.....	54
Apéndice C: Análisis de documentos de archivo	56

Agradecimientos

Muchas personas contribuyeron a la creación de los ocho módulos que integran esta serie, en particular, los estudiantes de doctorado de la Universidad de la Columbia Británica, Elizabeth Shaffer, Corinne Rogers, Donald Force y Elaine Goh, quienes elaboraron los borradores de los contenidos basados en los trabajos de InterPARES 1 y 2, así como los casos de estudio desarrollados en InterPARES 3.

También agradecemos a los numerosos asistentes de investigación quienes elaboraron casos de estudio para todos los módulos así como al equipo de InterPARES en Canadá, a un sinnúmero de investigadores internacionales involucrados con este proyecto y, por supuesto, a su directora, Luciana Duranti.

Finalmente, nuestra gratitud a todos aquellos que revisaron y comentaron los módulos, con una mención especial a los investigadores John McDonald, consultor de administración de información (módulos 1, 2, 7 y 8), Jim Suderman, director del despacho de acceso a la información de Toronto (módulo 3), Evelyn McLellan, archivista de sistemas de Artefactual Systems, Inc. y Paul Hebbard, archivista administrador de documentos de archivo de la Universidad Simon Fraser (módulo 6).



Digital Records Pathways: Topics in Digital Preservation es una iniciativa educativa desarrollada en conjunto por el International Congress on Archives (ICA) y The International Research on Permanent Authentic Records in Electronic Systems (InterPARES) con el propósito de ofrecer capacitación a archivistas y profesionales que manejan documentos en cuanto a la producción, la administración y la preservación de documentos de archivo digitales auténticos, fiables y usables. El programa asume que el lector cuenta con una sólida base en cuanto a los conceptos fundamentales de la administración de archivos y en la teoría archivística, y sobre esa suposición se elaboró esta serie modular.

La serie está formada por ocho módulos más un glosario en donde se ha conjuntado terminología de acuerdo con la base de datos del ICA. Ésta aborda los conocimientos teóricos y prácticos necesarios para establecer el marco de referencia, la estructura de gobernanza y los sistemas requeridos para administrar y preservar documentos de archivo digitales, a través de su ciclo de vida. Cada módulo se refiere, específicamente, a un tema relevante para la administración o la preservación de los documentos de archivo. Todos los módulos se han diseñado de tal manera que pueden ser estudiados en forma independiente o en conjunto.



Prefacio a la edición en español

Desarrollar materiales educativos con el fin de apoyar las tareas de preservación digital en instituciones y organizaciones fue uno de los objetivos del Proyecto de Investigación Internacional para la Preservación de Documentos de Archivo Electrónicos, InterPARES 3 (2007-2012), el cual dio como resultado la serie en inglés de ocho módulos de capacitación con el título *Digital Records Pathways: Topics in Digital Preservation*.

No obstante que los archivos digitales –también llamados electrónicos–, se producen en la actualidad en volúmenes insospechables, el conocimiento de los archivistas y gestores de documentos en cuanto a la producción, conservación y preservación de los mismos aún es limitado, entre otros factores, a causa de la escasez de materiales de capacitación en idioma español.

Lo anterior fue el motivo para que Alicia Barnard y Juan Voutssás, miembros del Team México que formó parte del Proyecto InterPARES 3, junto con Alejandro Delgado, de España, se dieran a la tarea de traducir a nuestro idioma los ocho módulos de la citada serie, los cuales fueron publicados inicialmente en formato electrónico por el Proyecto InterPARES 3.

El Archivo General de la Nación se une a este esfuerzo para lograr una mayor difusión de temas y tópicos sobre la preservación de archivos digitales en el entorno de los archivos de nuestro país y de aquellos de habla española en Latinoamérica, y presenta una nueva versión electrónica en español de los módulos de la mencionada serie, en espera de que coadyuven a la mejor comprensión y entendimiento de la preservación de archivos digitales y el ambiente donde los mismos se producen, conservan y preservan.

Mercedes de Vega



The International Council on Archives (ICA) y The International Research on Permanent Authentic Records in Electronic Systems (InterPARES) tienen el compromiso de crear materiales didácticos para la educación continua de archivistas y administradores de documentos de archivo, construir conocimiento básico, diseminar los nuevos hallazgos y dotar a los archivistas y profesionales de los documentos de archivo del conocimiento y las competencias especializados necesarios para la administración y la preservación de documentos de archivo digitales.

El 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 y su representación, por medio de profesionales en 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 los archivos y asegurar su acceso por medio de la asesoría, el establecimiento de estándares, el desarrollo profesional y el impulso del diálogo entre archivistas, líderes, productores y usuarios de archivos.

El ICA es una organización neutral, no gubernamental; sus miembros 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 registrado, para producir estándares reconocidos, buenas prácticas e impulsar el diálogo, el intercambio y la diseminación del conocimiento y experiencia más allá de fronteras internacionales. Con aproximadamente





mil quinientos miembros en 195 países y territorios, el credo del Consejo ha sido aprovechar la diversidad cultural de sus integrantes para entregar soluciones eficaces y una profesión flexible e imaginativa.

El proyecto InterPARES (www.interpares.org), pretende desarrollar conocimiento original y esencial para la conservación, a largo plazo, de documentos de archivo producidos y almacenados en formatos digitales, así como proveer una base sólida para estándares, políticas, estrategias y planes de acción capaces de asegurar la longevidad de los materiales documentales y la capacidad de sus usuarios para confiar en su autenticidad. InterPARES se ha desarrollado en tres etapas:

- InterPARES 1 (1999-2001). Esta etapa se enfocó en el desarrollo de la teoría y los métodos que pudiesen asegurar la preservación de la autenticidad de los documentos de archivo producidos y 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). Se 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 conservación 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 sobre la base de los hallazgos de las primeras dos etapas en conjunto con otros proyectos de preservación digital de distintas partes del mundo. Se llevó la teoría a la



práctica al trabajar con archivos y unidades archivísticas dentro de organizaciones que tuvieran recursos humanos y financieros limitados, con el fin de implementar en ellas programas sólidos de gestión y preservación de archivos.

Público objetivo

El público objetivo para el cual está destinado este programa se compone de archivistas, gestores documentales y profesionales de la gestión archivística, interesados en ampliar sus capacidades en la administración de documentos de archivo 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.

Cómo usar la serie

Cada módulo de la serie está formado por conocimiento teórico y metodológico, así como por aplicaciones prácticas ilustradas en casos de estudio y escenarios modelo. Si bien los módulos fueron desarrollados por el equipo canadiense de InterPARES y, por tanto, ejemplificados en un contexto propio a aquél, son adaptables a un dominio específico o ámbito jurídico. Para una mayor aplicabilidad se han traducido a los idiomas de los miembros del ICA.

Los módulos pueden estudiarse por separado o en conjunto, de acuerdo con cada necesidad o interés, pues abarcan un rango amplio de competencias requeridas; pueden ser estudiados individualmente u ofrecerse a grupos como asociaciones profesionales o instituciones de capacitación laboral. Algunos de los módulos incluyen formularios



que pueden adaptarse a universidades o asociaciones profesionales para el desarrollo de cursos curriculares, o como materiales de capacitación para estudiantes y profesionales de la gestión o preservación documental digital. Las universidades y asociaciones profesionales son libres de adaptar los materiales para desarrollar sus propios cursos curriculares o de capacitación. Se sugieren recursos adicionales en la web que se identifican a lo largo de los módulos con el icono:



o bien, cuando se trata de información complementaria ubicada en anexos o en los mismos módulos de la serie, se distinguen con la figura:



Objetivos

Los módulos tienen los siguientes objetivos:

- Aportar recursos educativos basados en investigación actual sobre temas de administración de archivos digitales para beneficio de miembros de asociaciones profesionales relacionadas con esa temática.
- Proporcionar a los profesionales de archivos, con conocimiento teórico y procedimental, habilidades estratégicas necesarias para desarrollar, implementar y supervisar un sistema de gestión o de preservación documental.
- Ilustrar conceptos teóricos con aplicaciones prácticas mediante ejemplos reales extraídos de casos de estudio, asociados con contextos administrativos y tecnológicos específicos.

- Proporcionar contenidos y estructura a programas educativos universitarios para implementar cursos sobre administración o preservación de archivos.

Arquitectura modular del programa

Los primeros dos módulos presentan los fundamentos de todo programa de preservación de documentos de archivo digitales; proporcionan los conocimientos propedéuticos sobre los demás módulos. Los siguientes tres módulos tratan temas generales contemporáneos que competen a la preservación digital: el papel de la cultura organizacional, una visión general de los metadatos y de la valoración en el contexto de la administración de documentos de archivo fuera del sistema de gestión documental Electronic Recordkeeping Management System (ERMS). En los tres últimos módulos se abordan temas específicos de interés contemporáneo: la administración de correos electrónicos, la preservación de documentos de archivo en ambientes web, y los temas emergentes acerca del creciente auge del cómputo en la nube (tabla 1).

Tabla 1 Arquitectura modular del programa

Tema del módulo	Aspecto
1. Un marco de referencia para la preservación digital. 2. Desarrollo de políticas y procedimientos para la preservación digital.	Fundamentos
3. Cultura organizacional y sus efectos en la administración de archivos 4. Breviario de metadatos. 5. Control de los documentos de archivo digitales.	Generalidades
6. Correo electrónico. 7. Documentos de archivo en ambientes web. 8. Cómputo en la nube.	Específico
Base de datos internacional, terminología.	Fundamentos



Cada módulo contiene todos o algunos de los siguientes elementos:

- Panorama del tema y alcance del módulo.
- Objetivos y aprendizajes esperados del módulo.
- Metodología o procedimientos para la aplicación y desarrollo del módulo.
- Formularios (cuando apliquen) para facilitar la implementación del módulo.
- Ejemplos, casos de estudio o escenarios (cuando apliquen) con situaciones reales acerca del tema.¹
- Ejercicios de los puntos clave del aprendizaje.
- Preguntas de revisión que optimicen la comprensión y entendimiento del tema.
- Recursos adicionales.
- Lecturas, estándares y otros recursos de referencia.

Cuando se ha considerado apropiado, se hace la distinción de la administración y preservación de documentos de archivo activos en contraste con las responsabilidades relativas a éstos que ya no son requeridos para actividades cotidianas de la organización y que serán preservados por su productor o por un tercero de confianza.

¹ Los ejemplos y casos de estudio citados en los módulos provienen de casos reales de InterPARES 3 y tienen como propósito apoyar la experiencia de aprendizaje del módulo. Si bien reflejan los hallazgos de investigación del proyecto, no necesariamente deben ser tomados como plantillas para ser aplicadas a pie juntillas en todos los casos. Cada organización (productor o preservador) es diferente y la preservación de sus documentos de archivo debe tomar las mejores prácticas desde una perspectiva práctica en cuanto a la viabilidad de una cierta implementación.



Alcance

La serie comprende los siguientes ocho módulos:

Módulo 1. Un marco de referencia para la preservación digital.

Módulo 2. Desarrollo de políticas y procedimientos para la preservación digital.

Módulo 3. Cultura organizacional y sus efectos en la administración de archivos.

Módulo 4. Breviario de metadatos.

Módulo 5. Estrategias 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.

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 archivos la cual refleja los usos habituales y prácticos en 16 idiomas. Esta base, desarrollada conjuntamente por el ICA e InterPARES está disponible en www.web-denizen.com/. Dicho recurso dinámico continuará creciendo y desarrollándose en la medida en que los miembros de la comunidad archivística mundial puedan participar agregando o enriqueciendo las definiciones usadas en su región de práctica. Pueden verse ciertos términos específicos, en breves glosarios existentes en cada módulo, aún no incluidos en la base de datos.



Introducción

El cómputo en la nube² consiste en una serie de servicios de cómputo bajo demanda, entregados a través de internet desde una ubicación remota o por medio de los servidores de una organización. Dado que aún se considera un concepto emergente, el cómputo en la nube es un reflejo del cambio en el modelo cliente-servidor hacia el modelo de red, a partir de entornos aislados hasta la red mundial; lo cual 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 empresa u organización –desde el almacenamiento y la colaboración hasta el procesamiento y la comunicación–, se pueden desplazar hacia la nube. Esencialmente, el cómputo en la nube es un servicio o conjunto de servicios prestados por medio de internet, bajo demanda del usuario y desde una ubicación remota, en lugar de residir en un equipo de escritorio, una laptop o los servidores de la organización. Así, las organizaciones contratan a un proveedor de servicios que ofrezca almacenamiento, procesamiento y aplicaciones a través de la web. Los recursos del cómputo en la nube están disponibles bajo demanda para acceder a información, aplicaciones y procesamiento, independientemente de la ubicación y de los dispositivos de acceso.

El cómputo en la nube ofrece flexibilidad y comodidad porque los usuarios pueden trabajar cuando y donde quieran sin importar de dónde vienen los datos que ven en pantalla –siempre y cuando haya acceso a internet–. Además, para ese propósito el cómputo en la nube permite a los proveedores utilizar centros de datos distantes.

² También llamado computación en la nube.



Así, el cómputo en la nube se está adoptando rápidamente por las organizaciones públicas y privadas debido a los potenciales beneficios percibidos, como la relación costo-beneficio, la escalabilidad, el rendimiento y la comodidad. Sin embargo, los riesgos potenciales de esta adopción deben ser plenamente comprendidos por las organizaciones con el fin de tomar decisiones bien informadas respecto de su utilización.

Objetivos y metas de este módulo

- 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 en la organización.
- Preparar el terreno para ayudar a los usuarios en el desarrollo de una estrategia de cómputo en la nube e identificar los documentos de archivo y procesos que son candidatos potenciales para el manejo por subcontratación con terceros en la nube.
- Ayudar a los usuarios a identificar los problemas relacionados con el uso del cómputo en la nube al momento de seleccionar procesos, aplicaciones y documentos de archivo que se pretendan mover hacia ese entorno, así como los requerimientos de negocio, las reglas y los marcos normativos que deben ser examinados en los términos que plantea el cómputo en la nube.

Alcance

En este módulo se proporciona una introducción al cómputo en la nube, a los problemas asociados con la gestión documental y a los desafíos que deben considerarse 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.

Aprendizajes esperados

Al término de este módulo, usted 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 a su determinación.
- Saber dónde encontrar información adicional y recursos que faciliten la comprensión e implementación de la tecnología del cómputo en la nube.



Definición de cómputo en la nube

El National Institute of Standards and Technology, NIST (Instituto Nacional de Estándares y Tecnologías) proporciona la definición más amplia y adoptada acerca del cómputo en la nube. Esta definición identifica cinco características esenciales 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 acceso conveniente, ubicuo y bajo demanda, vía internet, a un conjunto compartido de recursos de cómputo configurables (por ejemplo, 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.

Características esenciales

Autoservicio bajo demanda: los usuarios pueden proveerse de capacidades computacionales (por ejemplo, tiempo en servidor o redes, almacenamiento, etcétera) conforme las requieran, sin asistencia por parte del proveedor de esos servicios.

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

Conmutación de recursos: modelo multipropietario 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: uso de los recursos cuantificado, controlado y reportado, lo que facilita a los usuarios pagar con base en el consumo de cada tipo de servicio (por ejemplo, almacenamiento, proceso, ancho de banda, etcétera).

Modelos de servicio

Software como servicio (*software as a service, SaaS*). Capacidad provista al usuario para emplear los programas y las aplicaciones del proveedor ejecutados en la infraestructura de la nube. Tales aplicaciones son accesibles desde diferentes dispositivos a través de una interfaz de cliente ligera como un navegador web (por ejemplo, el correo electrónico basado en la web). El usuario no administra ni controla la infraestructura de nube subyacente como la red, los servidores, sistemas operativos, almacenamiento o incluso capacidades de aplicaciones individuales, con la posible excepción de algunas limitadas configuraciones específicas que le son permitidas.

Plataforma como servicio (*plataform as a service, PaaS*). 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 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, IaaS*). Capacidad ofrecida al usuario para proveerle procesamiento, almacenamiento, redes y otros recursos



informáticos fundamentales donde el usuario es capaz de instalar y ejecutar software a voluntad, como sistemas operativos y aplicaciones. El usuario no administra ni controla la infraestructura de la 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).

Modelos de despliegue

Nube privada. La infraestructura de nube es operada únicamente por una organización. Puede ser manejada por la misma organización o por un tercero dentro o fuera de las instalaciones de ésta.

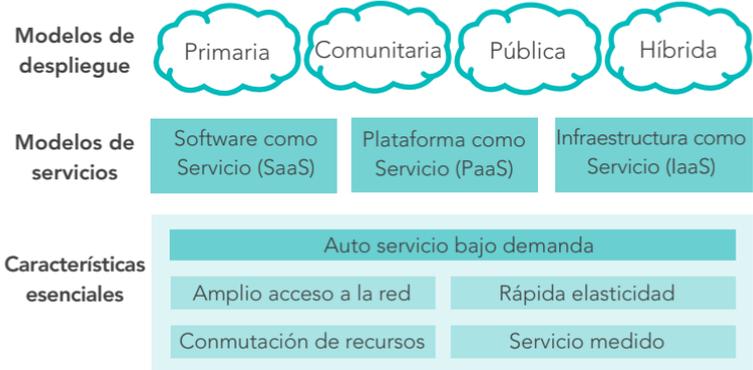
Nube comunitaria. La infraestructura de nube es compartida por varias organizaciones y apoya a una comunidad específica que comparte ciertas afinidades (por ejemplo, la misión, los requisitos de seguridad, políticas u objetivos). Puede ser administrada por la organización o por un tercero, y puede estar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

Nube pública. La infraestructura de la nube pertenece a una organización que vende sus servicios en la nube; está disponible al público en general o a un gran grupo industrial.

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 unidas 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).



Figura 1. Cómputo en la nube



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



Puntos clave en la adopción de 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 elegidos. Migrar información y servicios a la nube no está exento de riesgos y desafíos. Por lo general, las cuestiones de seguridad y disponibilidad son preocupaciones comunes en este tema; otros desafíos dependerán del entorno de nube y servicios elegidos por el usuario.

Aquellos usuarios que consideran la posibilidad de migración de información y servicios hacia la nube deben comprender totalmente los beneficios y riesgos asociados con el cómputo en la nube y disminuir las contingencias 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.

Escalabilidad

El empleo del cómputo en la nube permite a las organizaciones aprovechar la infraestructura compartida y beneficiarse con las economías de escala. “El cómputo en la nube lleva la economía de las Tecnologías de la Información y la Comunicación (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 proyección de usos predeterminados, escalando los servicios que requiere la organización cuando están en su máximo y reduciéndolos durante periodos con menos demandas.

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 “tipos de servicios públicos” puede proporcionar beneficios a las organizaciones por medio 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, en las cuales esos cambios en los requerimientos de recursos pueden variar desde poca o ninguna a la necesidad de manejar grandes cantidades de datos o de procesamientos. Los beneficios de escalabilidad se pueden garantizar siempre que el uso del cómputo en la nube se controle y, si es necesario, se regule por las organizaciones para asegurar que la relación costo-beneficio es adecuada (Convery, 2010).

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 ellos poseen grandes recursos de computación, cuando una eventual falla en su servidor afecta los servicios prestados a los usuarios, las aplicaciones y servicios pueden ser automáticamente redirigidos a otros servidores. Además, 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 interrupción o caída de un centro.

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 o Service Level Agreements (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 de nivel de servicio.

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 almacenar 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, gmail 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, por tanto, deben ser capaces de responder ante tales amenazas con rapidez y eficacia. Si bien los acuerdos SLA proporcionan 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 se produce en un momento crítico, esa compensación podría significar poco en comparación con 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; subestimarlos por parte del proveedor puede dar como resultado la reducción o interrupción del 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, los proveedores de cómputo en la nube están sujetos a condiciones



de mercado, adquisiciones y absorciones de empresas, etcétera. 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 en las organizaciones que utilizan sus servicios y aplicaciones, incluyendo la pérdida de datos, interrupciones en las operaciones comerciales y atención al cliente, entre otros. 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.

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 tradicional de compra, instalación y despliegue de equipo y programas. Dado que los servicios y aplicaciones se encuentran en la nube, los usuarios pueden tener acceso a ellos desde prácticamente cualquier lugar en donde haya acceso a internet. Además, el cómputo en la nube permite a las organizaciones probar los servicios y aplicaciones cuando así lo decidan sin grandes gastos y con una mínima pérdida financiera. El entorno de la nube puede permitir a algunos usuarios usar soluciones tecnológicas nuevas y económicas que de otra forma no serían viables, y la eficiencia proporcionada por la nube puede permitir esta reasignación de los recursos de TIC a otras tareas.

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; asimismo puede implicar una reducción del gasto en TIC ya que



las organizaciones no están obligadas a hacer grandes gastos porque pueden emplear un modelo de compra bajo demanda, es decir, adquirir sólo los recursos informáticos que necesitan para desarrollar su negocio en cualquier momento.

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 costos operativos mediante la reducción o reasignación del personal de TIC dentro de la empresa, utilizando así más eficazmente los recursos humanos. Ventajas adicionales en los costos provienen de la reducción del consumo de energía, de la pérdida de tiempo debido a retrasos en las operaciones computacionales y de la del desperdicio de recursos como un servidor sin usar.

A pesar de estos ahorros aparentes, las organizaciones deben calcular el costo 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 hacer un análisis de la relación costo-beneficio para identificar los verdaderos costos antes de mudar los documentos de archivo y servicios a la nube.

Interoperabilidad e integración

El cómputo en la nube es una industria emergente. Actualmente existe una falta de normalización,³ 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

³Existen iniciativas tales como www.cloud-standards.org tendientes a estandarizar APIs y procedimientos.



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 mitigar el hecho de quedar anclados con un determinado proveedor. A pesar de la subcontratación de aplicaciones y servicios, el nivel de gestión y mantenimiento por parte de la organización puede fluctuar dependiendo del modelo de nube elegido.

La integración de los servicios en la nube en una organización donde ya existe un entorno de servicios de TIC debe considerar 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 que se tienen en la organización. Los servicios de cómputo en la nube pueden limitar las posibilidades de personalizar 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 para asegurar que se han considerado los obstáculos técnicos.

Cumplimiento y hallazgo electrónico

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

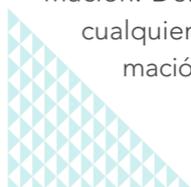
La información almacenada a lo largo de varias jurisdicciones puede ser susceptible de divulgación y de incautación por



parte de gobiernos extranjeros o dependencias 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 multipropietario, 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 EUA, la ley de seguridad nacional, y demás legislaciones relacionadas con la seguridad, junto con complicadas tecnologías electrónicas de recopilación de información, permiten a los gobiernos tener acceso a la información electrónica en prácticamente cualquier contexto” (Jaeger, Lin y Grimes, 2008).

Varios asuntos legales pueden 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 y Grimes, 2008), de igual manera la información sensible de una organización inocente puede quedar incautada en una investigación (Jaeger, Lin y Grimes, 2008). Los usuarios de la nube deben estar conscientes de sus requerimientos jurídicos y reglamentarios relacionados con 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 sin dañar la autenticidad e integridad de esa información. Debido a la naturaleza dinámica de la nube, en cualquier momento dado puede ser difícil localizar la información 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 y, por tanto, pueden afectar la certificación y fiabilidad por parte de los usuarios.

Ejercicios:

1. Identifique los marcos legislativo y normativo que apliquen a los documentos de archivo de su organización.
2. Conteste: ¿Qué tanto impactaría el potencial almacenamiento de sus documentos de archivo en la nube con la capacidad de su organización para cumplir con estas leyes y regulaciones?

Continuidad de negocio y recuperación ante desastre

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

Las interrupciones en el servicio de internet pueden afectar la funcionalidad de 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. Con el fin de cumplir con las obligaciones de rendimiento puede incurrirse en costos adicionales con motivo de servicios de supervisión y seguridad necesarios. La continuidad del negocio y la planificación de recuperación en casos de desastre deben ser planeadas, probadas y documentadas.

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 “impredicibles marcos jurídicos y de ejecución” lo cual puede implicar que los datos personales sean susceptibles al acceso no autorizado por parte de terceros. En ese tipo de entornos la responsabilidad de mantener segura la información se transfiere al proveedor de la nube; sin embargo, la responsabilidad de salvaguardar la información personal y confidencial recae siempre en la organización usuaria de la nube ya que fue quien recabó la información.

Puede ser difícil para la organización usuaria de la nube controlar eficazmente el manejo de los datos y las técnicas de procesamiento de los proveedores de la nube para asegurar que sean conservados legalmente y de acuerdo con las necesidades de la organización. Como “controlador” de la información, el usuario es responsable de la seguridad de la información personal y confidencial que recaba, 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.

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 pueden ser un gran problema y más difícil de abordar cuando la información almacenada en la nube se encuentra en servidores remotos. Diversos cuestionamientos surgen acerca de la cuestión de qué 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 industriales puede ser un problema para las organizaciones que almacenan información en la nube.

Integridad de la información

La mayoría de las arquitecturas de nube carecen de estándares formales que administren la manera en que los datos se almacenan y manipulan, y muchas aplicaciones no tienen las funciones de gestión documental comunes, por lo que es difícil para las organizaciones usuarias cumplir con los requisitos de gestión documental.

La autenticidad y la 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 dicho entorno. 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 consecuencia de que haya interceptación durante la transferencia en redes no seguras, combinado con datos en entornos de multipropietarios, y la destrucción ineficaz de éstos.

Pérdida de gobernanza

El incremento del cómputo en la nube aumenta la necesidad de gobernanza. “La gobernanza implica el control y la supervisión de las políticas, procedimientos y estándares para el desarrollo de aplicaciones, así como el diseño, la implementación, las pruebas y la supervisión de los servicios desplegados” (Jansen y Grance, 2011). Debido a la naturaleza del cómputo en la nube, y la capacidad



de los usuarios (empleados) para contratar fácilmente servicios informáticos, es posible que la organización pierda el control de este entorno de la nube. Las responsabilidades de seguridad de la información almacenada en la nube se transfieren al proveedor. El nivel de control que tiene un usuario 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 de cumplir con los requerimientos legales y regulatorios así como a una incapacidad para demostrar la autenticidad y fiabilidad de la información que tienen almacenada en la nube (Convery, 2010).

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 pueden ser víctimas de acuerdos de servicios ambiguos. Las organizaciones deben asegurarse de mantener sus derechos de propiedad a toda costa y de que el proveedor de la nube no adquiera derechos de propiedad, concesión de licenciamientos ni uso sobre la información de la organización.

Recuperación y destrucción de información

Las prácticas de administración de archivos requieren que la destrucción sistemática de éstos se realice con el fin de cumplir con la tabla de retención de la organización. En el entorno de la nube, el cumplimiento eficaz de la destrucción de documentos de archivo puede ser difícil de lograr. En la nube, la eliminación de datos insegura o incompleta es un problema pues



la “eliminación de datos adecuada y oportuna puede ser imposible” debido a la falta de disponibilidad de copias adicionales almacenadas o porque el modelo multipropietario de la nube puede tener los datos de los clientes en un modelo de espacio de disco compartido (Enisa, 2009). Las organizaciones pueden facilitar 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 replicar la información en varios lugares de la nube como método de redundancia puede beneficiar a las organizaciones, cumplir las leyes acerca de acceso a la información y protección de la privacidad requiere que las organizaciones estén al tanto de la cantidad de copias que se tienen de su información y dónde residen éstas con el fin de cumplir con dicha legislación.

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



Véase en el Apéndice A, las diez preguntas centrales para plantearse en el momento de contratar servicios de un tercero para migrar hacia la nube.

Disposición para el cómputo en la nube: evaluación y preparación

El cómputo en la nube es una herramienta que necesitará adaptarse en la estrategia global de la organización puesto que auxilia en el logro de 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 en cuanto al 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 migrados 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

El empleo de un marco de referencia para la toma de decisiones para evaluar el grado de disposición de la organización en el entorno de nube cuando se quiere migrar documentos de archivo y servicios hacia ella, ayudará a identificar cualquier problema, así como cuáles son los documentos y procesos más adecuados para ese entorno.

Marco de referencia para la 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 tipo de negocio de su organización, su gobernanza y los requisitos de cumplimiento.
4. Realizar una evaluación de riesgos para los documentos de archivo, aplicaciones y procesos en caso de traslado hacia 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 al mudar registros, aplicaciones y procesos identificados 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, garantizar que los procedimientos para obtener información de los sistemas del proveedor de nube son adecuados y pueden ser transferidos a otro proveedor de servicios o de vuelta hacia la organización.

El marco de referencia para la toma de decisiones en la nube consta de una serie de pasos, algunos de los cuales son iterativos y pueden ocurrir simultáneamente (Fig. 2). En los apartados siguientes se explicarán estos pasos.



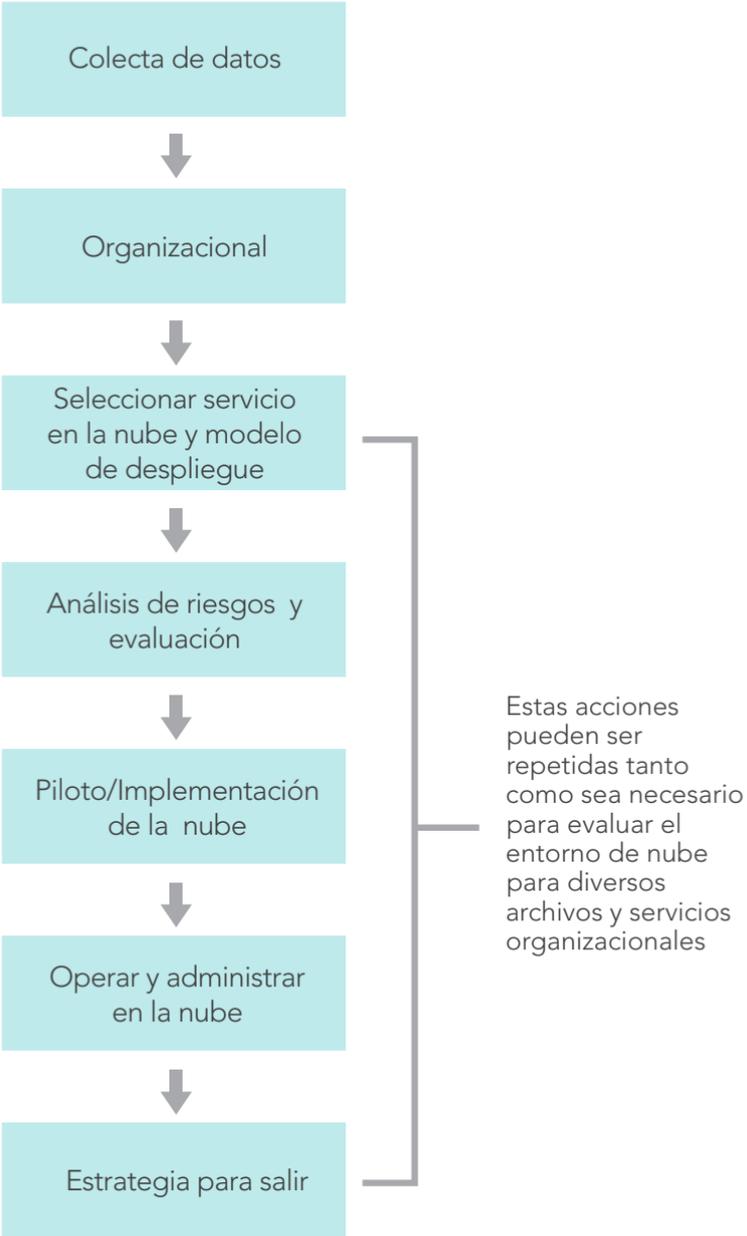


Figura 2: Marco de Referencia de Toma de Decisiones en la Nube.



Recopilación de datos

El marco de referencia de toma de decisiones en la nube 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 o talleres y la plática con los proveedores de servicios serán de gran ayuda para quienes quieren tener un conocimiento profundo del cómputo en la nube y sus diferentes modelos. Es importante asegurarse de que no sólo el personal de TIC sea informado del funcionamiento del cómputo en la nube, sino que los tomadores de decisiones también deben ser orientados al respecto.

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

Ejercicio:

De los tomadores de decisiones y desarrolladores de políticas dentro de su organización, ¿quiénes serían candidatos para capacitarse acerca del cómputo en la nube?

Evaluación de la organización

A fin de obtener ventajas 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 mudarse.

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



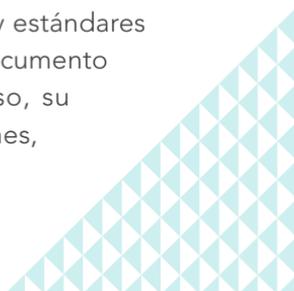
pueden tener un marco de referencia existente que ya utilicen para evaluar posibles proyectos de tercerización, el cual puede ser adecuado para esta tarea. Además, la recopilación interna de los datos ayudará a las organizaciones a evaluar aquellos activos adecuados para el entorno de nube.

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. Éstos abarcan:

- Correo electrónico.
- Gestión documental.
- Herramientas de colaboración.
- Herramientas de productividad (por ejemplo, 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 sólo en el contexto de una función de negocio o una subunidad.

El análisis contextual recopila información sobre toda 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 mediante 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 cuadro de clasificación de la organización puede ayudar a identificar los documentos de archivo y la 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	Mantener las 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 catastrofico sobre las operaciones, activos e individuos de la organización.
Integridad	Vigilar que no se cometan acciones de modificación o destrucción no autorizada de información, lo que implica que se asegure la autenticidad y el 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 catastrofico 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 catastrofico 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 dentro de su organización pudieran migrar hacia la nube? ¿Por qué estarían mejor ubicados allí?

Selección del modelo de servicio 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 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 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 (CSA, 2009):

- 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.

Las razones organizacionales para la migración de documentos de archivo, aplicaciones y procesos hacia 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.

Análisis y evaluación de riesgos

Implica 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 se esté 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 hacia la nube y ayudará en la preparación para la adopción eficaz del cómputo en ésta.





El marco de referencia de seguridad de información de Enisa (Cloud Computing 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 plantear a un proveedor de la nube con el fin de garantizar efectivamente que protegerán la información confiada a ellos (éstas tienen el propósito de servir como base y deben ser ampliadas de acuerdo con las necesidades particulares de cada organización). Disponibles en: <http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-information-assurance-framework>

Proyecto piloto/Implementación en la nube

Lleve a cabo un proyecto piloto migrando documentos de archivo, aplicaciones y procesos identificados hacia ese entorno. La supervisión cercana de ese piloto asegurará que los problemas imprevistos sean reconocidos y tratados oportunamente en el proceso. El proceso de pilotaje puede repetirse varias veces hasta que se tenga confianza en la plataforma elegida y el servicio puede ser establecido cuando se considere que cumple con todos los requisitos necesarios.

Operación en la nube

Una vez trasladados los documentos a la nube, deben tenerse en cuenta y prever una serie de aspectos que deben realizarse en la gestión documental como aplicaciones y procesos que se realizan cotidianamente, incluyendo esa gestión documental y su clasificación, el cumplimiento, seguimiento y auditoría, la seguridad y el acceso permanente.



Estrategia de salida y retorno a la organización

Antes de migrar los documentos de archivo, aplicaciones o procesos a la nube, las organizaciones deben asegurarse de contar con los procedimientos 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.



Actividades 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. Conteste:
 - ¿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?
 - ¿Cómo se puede utilizar el entorno de cómputo en la nube de forma rentable para las organizaciones?
5. Enumere cinco beneficios para las organizaciones en la migración de aplicaciones y servicios hacia la nube.
6. Mencione cinco riesgos para las organizaciones en la migración de aplicaciones y servicios hacia la nube.



Autor: Australian Government, Department of Finance and Deregulation

Título: *Cloud Computing Strategic Direction Paper*

Fecha de Publicación: enero 2011

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 instituciones 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 para las dependencias. La estrategia del gobierno se divide en tres corrientes: orientación y documentación para los organismos; adopción de la nube en servicios "no clasificados" y el estudio de sus riesgos, y fomento de 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 de 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 investigan cómo optar por el cómputo en la nube en sus organizaciones.

** Nota del traductor: Además del material que se recomienda en la versión en inglés, en español hay obras disponibles que ha elaborado la Benemérita Universidad Autónoma de Puebla.



Autor: Wyld, David C.

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

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

Fecha de publicación: 2009

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*

Fuente/editor: Enisa

Fecha de publicación: enero de 2011

URL: <https://www.enisa.europa.eu/publications/security-and-resilience-in-governmental-clouds>

Autor: Cloud Security Alliance

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

Fuente/editor: Cloud Security Alliance

Fecha de publicación: diciembre de 2009

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.



- Askhoj, J., Sugimoto, S., & Nagamori, M. *Preserving Records in the Cloud*, preprints.
- Armbrust, M. et al. (2009), "Above the Clouds: A Berkeley View of Cloud Computing", en *Technical Report ucb/eecs-2009*, 28, University of California at Berkeley.
- Australian Government, Department of Finance and Deregulation (abril de 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 (octubre de 2011), *Cloud Computing – Opportunities and Challenges*, it Industry Innovation Council.
- Ball, C. (febrero de 2011), Facebook Feature Could Ease Cloud-Based, eddltn Law Technology News.
- Bradshaw, S., Millard, C. y Walden, I. (2010), "Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services", en *Paper*, núm. 63, Queen Mary School of Law Legal Studies Research.
- BSA. (2011). *Cloud Computing Policy Agenda for Europe*.
- Cloud Computing Explained* by Rosalyn Metz, en *Educause Quarterly*, disponible en: <http://www.educause.edu/EDUCAUSE+Quarterly/EDUCAUSEQuarterlyMagazineVolum/CloudComputingExplained/206526>



- Cloud Security Alliance (CSA). (marzo de 2010), *Top Threats to Cloud Computing* v.1.0. Disponible en <https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf>
- Convery, Nicole (26 de agosto de 2010). *Cloud Computing Toolkit: Guidance for Outsourcing Information Storage to the Cloud*. Disponible en http://www.archives.org/images/documents/Cloud_Computing_Toolkit-2.pdf
- Digital Agenda Assembly (2011), "Towards a Cloud Computing Strategy for Europe: Matching Supply and Demand", en *Report from Workshop*, 18.
- Enisa (Noviembre de 2009). *Cloud Computing: Benefits, Risks and Recommendations for Information Security*.
- Jaeger, P. T., Lin, J., y Grimes, J. M. (2008), "Cloud Computing and Information Policy: Computing in a Policy Cloud?", en *Journal of Information Technology & Politics*, 5(3), pp. 269-283.
- Maxwell, W. y Wolf, C. (mayo de 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", en *Hogan Lovells White Paper*.
- NIST (2010), *Definition of Cloud Computing v15*. Online, disponible en <http://src.nist.gov/groups/SNS/cloud-computing/>
- O'Brien, K. J. (19 de septiembre de 2010), "Cloud Computing Hits Snag in Europe", en *New York Times*.
- Office of the Information and Privacy Commissioner of British Columbia (febrero de 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. y Bromage, D. (2010), "Current State of Play: Records Management and the Cloud", en *Records Management Journal*, 20(2), pp. 217-225.

Wylde, D. C. (2010), "The Cloudy Future of Government it: Cloud Computing and the Public Sector around the World", en *International Journal of Web & Semantic Technology*, 1(1).



Apéndice A: Las 10 preguntas fundamentales para contratar un tercero en la migración hacia la nube⁴

Nicole Convery provee una útil lista acerca de las diez preguntas centrales que deben hacerse los usuarios que contemplan la posibilidad de contratar a un tercero como proveedor de aplicaciones y servicios en la nube:

- ¿Cuáles procesos, aplicaciones e información pueden moverse a la nube para ganar eficiencia y rentabilidad al tiempo que se satisfaga la seguridad y los requisitos de cumplimiento de la organización?
- ¿Cómo resultaría dañada la organización si personas no autorizadas tuvieran acceso a los sistemas, aplicaciones, servicios de la organización y la información se pusiera a disposición del público?
- ¿Cómo protege el proveedor de servicios en la nube la información y los sistemas contra el acceso no autorizado (por ejemplo, piratería, intromisión, usos inadecuados)?
- ¿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?

⁴ Nicole Convery, *Cloud Computing Toolkit: Guidance for Outsourcing Information Storage to the Cloud*, Reino Unido e Irlanda, Department of Information Studies, Aberystwyth University. Archives & Records Association, 26 de agosto de 2010.



- ¿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, licencias, etcétera)?
- ¿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?



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 los 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, obtenga y proporcione toda 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, obtenga y proporcione 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 materiales

Resuma la información acerca del contexto material en el que su organización opera, incluyendo información relevante acerca de 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, obtenga y proporcione 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

- Elabore una lista de 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

- Elabore una lista de 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 semiactivos.

Requerimientos y restricciones tecnológicas

- Identifique y describa todo el equipo usado en su organización:
 - Arquitectura (por ejemplo, topología de la red, infraestructura, equipos de cómputo).
 - Herramientas de producción o entrada (por ejemplo, programas, cámaras, micrófonos).
 - Herramientas de proceso (por ejemplo, programas, consola).
- Identifique y describa los tipos de documentos producidos (por ejemplo, gráficos, textos, audio).
- Liste los formatos utilizados (por ejemplo, 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.

