Escritos Contables y de Administración, ISSN 1853-2063, vol. 4, n° 1, 2013, págs. 109 a 147.

AUDITORÍA FINANCIERA EN ENTORNOS DE COMPUTACIÓN EN LA NUBE: REVISIÓN DEL ESTADO DEL ARTE

FINANCIAL AUDIT IN CLOUD COMPUTING: STATE OF THE ART REVIEW

María de los Ángeles López[1], Diana Ester Albanese[2], Regina Durán[3]

Fecha de recepción: 28/04/2014
Fecha de aceptación: 18/09/2014

RESUMEN

El uso de la Computación en la Nube (CN) en las organizaciones representa un nuevo desafío para los auditores financieros, dado que posee particularidades que deben ser revisadas por su impacto en el encargo de auditoría. El propósito de este trabajo consiste en realizar una revisión de la literatura y normativa vigente en la República Argentina respecto de los efectos de la CN sobre la auditoría financiera y plantear retos de investigación que resulta importante afrontar. Al respecto se abordan aspectos de la auditoría considerados relevantes en este entorno: el

[1] Consejo Nacional de Investigaciones Científicas y Técnicas (CONICET), Departamento de Ciencias de la Administración, Universidad Nacional del Sur, angeles.lopez@uns.edu.ar.
[2] Departamento de Ciencias de la Administración, Universidad Nacional del Sur, dalbanese@uns.edu.ar.
[3] Departamento de Ciencias de la Administración, Universidad Nacional del Sur, rduran@criba.edu.ar.

conocimiento del cliente; la identificación y evaluación de riesgos; la evaluación del sistema de control interno; las características específicas de las evidencias; las habilidades y competencias requeridas al auditor y el uso de especialistas. La investigación de estas temáticas permitirá fortalecer los conocimientos en esta área y contribuir en la elaboración de normas y recomendaciones que sirvan de guía para los profesionales en el ejercicio de su labor.

Palabras clave: Auditoría Financiera – Entornos de Computación en la Nube – Riesgos de la Computación en la Nube – Aspectos de auditoría potencialmente afectados

ABSTRACT

The use of Cloud Computing (CC) by organizations represents a new challenge for financial auditors since it has particularities that must be reviewed because of their impact in audit engagements. The objective of this paper is to review the literature and current standards in Argentina concerning the CC effects on financial audit, and to propose future research challenges that we must face. Among the relevant aspects that we consider are: entity understanding; risk identification and assessment; internal control evaluation; specific characteristics of the evidence; abilities and competencies required by the auditor, and use of specialists. Research on these areas will allow us to strengthen our knowledge about them and contribute to draw up norms and recommendations to help professionals do their work.

Key words: Financial Audit – Cloud Computing – Cloud Computing Risks – Audit aspects potentially affected.

JEL: M420

1. INTRODUCCIÓN

El uso de la tecnología de la información (TI) para la elaboración y el almacenamiento de la información contable ha tenido importantes efectos sobre la auditoría financiera, aun cuando su objetivo —brindar una seguridad razonable sobre la confiabilidad de la información contenida en los estados contables— no se ha visto alterado. Diversos autores han documentado cambios en las diferentes etapas del proceso de auditoría, así como en las habilidades exigidas a los profesionales para desarrollar una labor diligente y responsable.

En la actualidad ha cobrado importancia una nueva alternativa de TI para la gestión de los negocios de las organizaciones conocida como Computación en la Nube, cuya expansión se debe a la generalización del uso de la internet, la disminución de costos en el ancho de banda y otros avances tecnológicos (Mohamed, 2009), así como los diversos beneficios tangibles y mensurables que aporta (ISACA, 2009; Zhang, Cheng y Boutaba, 2010). Sin embargo, la complejidad y diversidad de la CN, junto con los riesgos que ella representa —pérdida del control sobre la información y los controles internos, interrupciones en la prestación de servicios, cambios de jurisdicción de localización de la información, entre otros, muchos de los cuales se han materializado en incidentes (Infobae, 2012; Kuranda, 2014)—, generan desafíos no solo para los entes usuarios, sino también para sus auditores (Blaskovich y Mintchik, 2011).

Actualmente la nube puede ser utilizada en distintas aplicaciones y procesos de negocio. Si bien difícilmente un ente podría delegar todo su sistema de TI a la nube, es posible que pueda trasladar parte de sus operaciones (Jansen y Grance, 2011), implementando por ejemplo paquetes de *software* de contabilidad y finanzas (Beal, 2013) o sistemas de *Enterprise Resource Planning* (ERP) que incluyan los módulos de contabilidad, ventas, gestión de clientes —como las opciones previstas por Oracle (2014) y SAP (2014)—, entre otros.

Este cambio en las técnicas de TI utilizadas por las empresas en la gestión representa un desafío para la auditoría externa como disciplina, proponiendo a los investigadores académicos temas a abordar que no

surgen tanto de estudios previos, sino más bien de la aparición de una arquitectura especifica (Blaskovich y Mintchnik, 2011) que requiere un avance desde la óptica del conjunto de conocimientos así como de la práctica profesional.

La *Cloud Security Alliance* (CSA) (2011) sugiere la necesidad de revisar de que manera se ve afectado el cumplimiento de los fines de la auditoría en este entorno. Nicolaou, Nicolaou y Nicolaou (2012) argumentan que la nube representa un nuevo contexto de trabajo con un impacto significativo en la auditoría, requiriéndose que los profesionales comprendan la tecnología y tomen las precauciones correspondientes para asegurar la calidad de su labor. Alali y Yeh (2012) destacan la necesidad de investigaciones acerca de la determinación del enfoque de auditoría, la evaluación de riesgos materiales, la evaluación de controles internos sobre los estados financieros y la forma en que los auditores financieros darán cumplimiento a los requerimientos de la regulación en entornos de CN.

Se presenta aquí una revisión de antecedentes de bibliografía y normas de auditoría y de encargos de aseguramiento vigentes en la República Argentina, y de estándares y recomendaciones emitidas por instituciones dedicadas a la investigación de la CN, con el objetivo de identificar avances que se han producido al respecto. Se examinan antecedentes referidos a la auditoría financiera en contextos de TI, a fin de proveer un marco para futuras investigaciones relacionadas a la CN como un nuevo entorno de TI particular en el que los auditores deben desarrollar su trabajo.

A la fecha, la mayoría de los estudios académicos en relación a la CN se refieren a aspectos técnicos (Kumar y Goudar, 2012) y en menor medida a su utilización por las organizaciones —beneficios, riesgos, factores de adopción (Yigitbasioglu, Mackenzie y Low, 2013)—. A su vez existen estudios referidos a los efectos de la TI y la tercerización de la TI sobre la auditoría (Minguillón, 2006; Astiz y Sole, 2008; Scutella y Barg, 2010; Pastor, 2011; Valencia y Tamayo, 2012; Bierstaker, Chen, Christ, Ege y Mintchik, 2013; entre otros). Sin embargo, existe una escasez de investigaciones académicas relacionadas a la auditoría de estados financieros en esta clase de ambientes tecnológicos complejos basados en tecnologías emergentes (Alali y Yeh, 2012).

Esta brecha presenta una oportunidad para el desarrollo de investigaciones académicas, pretendiéndose en este trabajo integrar la literatura de la auditoría financiera en entornos de TI con la referida a la CN, a fin de identificar los potenciales efectos que la CN tiene sobre los encargos de auditoría y los aspectos que necesitan mayor desarrollo en cuanto a conocimientos y normas, aportando a la teoría de la auditoría externa como disciplina.

La revisión se ha estructurado del siguiente modo: en primera instancia se realiza una revisión de los efectos de la TI sobre la auditoría financiera (sección 2), lo cual representa el cuerpo de literatura en el que se encuadra el problema de investigación. En la sección 3 se describen las particularidades de la CN como un caso particular de TI en el que pueden ejecutarse las auditorías, incluyendo las características consideradas relevantes a los efectos del tema tratado. En la sección 4 se incluye el análisis de diversos aspectos de la auditoría financiera que podrían verse específicamente afectados por un entorno de CN y que se pretende profundizar, a saber: el conocimiento del cliente; la identificación y evaluación de riesgos de auditoría; la evaluación del sistema de control interno; las características específicas de las evidencias de auditoría; y las habilidades y competencias requeridas al contador público y el uso de especialistas. Como conclusión se exponen las consideraciones finales junto con posibles retos de investigación que merecen atención.

2. AUDITORÍA FINANCIERA EN ENTORNOS DE TI

El uso de la tecnología de la información y comunicación ha cambiado la forma en que las empresas operan sus negocios (Brazel y Agoglia, 2007), en la medida en que se han modificado los procesos de registro, almacenamiento y comunicación de las transacciones comerciales y sus correspondientes informes financieros, alterándose los sistemas de contabilidad y control interno de las organizaciones (Pastor, 2011).

En consecuencia, ha sido inevitable que los auditores financieros reconozcan la TI en sus trabajos (Hunton, Bryant y Bagranoff, 2004a), dado que si bien el objetivo y alcance de una auditoría no se modifica a causa de

ella (Cerullo y Cerullo, 1997; Pastor, 2011; González, 2004), existen ciertas particularidades a las que se deben adaptar, tales como la existencia de registros electrónicos, transacciones virtuales, autorizaciones no escritas, entre otras.

Una auditoría se realiza en un entorno informatizado cuando está involucrada una computadora en el procesamiento, almacenamiento, transmisión o emisión de información financiera de importancia para la auditoría, ya sea que dicha computadora sea operada por la entidad o por un tercero (Scutella y Barg, 2010). Actualmente, en la mayoría de los casos, el auditor desarrolla su trabajo en entornos informatizados, siendo el uso de la CN un caso particular.

Diversos autores han documentado los efectos de la TI sobre la auditoría financiera. Cerullo y Cerullo (1997) destacan que si bien las etapas básicas de la auditoría son las mismas para un sistema de información manual o computadorizado, la ejecución de cada una de ellas requerirá de ciertas adecuaciones.

Avanzando en el tema, Astiz y Sole (2008) y Pastor (2011) plantean particularidades de cada una de las tres etapas principales de la auditoría (planificación, ejecución y reporte); por ejemplo, en la planificación se requiere profundizar el conocimiento del negocio del cliente y de la industria, para asegurar que se comprende la relevancia de los sistemas de información computadorizados. A partir de ello, en el análisis de riesgos se deben considerar aquellos derivados del uso de entornos informáticos, para poder elaborar el plan de auditoría en respuesta a los riesgos de error material, centrándose en la eficiencia y eficacia de los controles internos de los sistemas informáticos de contabilidad por sobre las pruebas sustantivas de los documentos y transacciones electrónicas. En la ejecución, cuando se hubiera optado por un enfoque de cumplimiento, resaltan los aspectos a evaluar en la validación de los controles internos informáticos y para el caso de un enfoque sustantivo, mencionan la ejecución de pruebas mediante el uso de técnicas de auditoría asistidas por computador (TAAC). Finalmente, en la etapa de conclusión y reporte, sugieren que el informe de recomendaciones sobre el control interno debería contener las observaciones pertinentes en relación a los controles de TI.

González (2004), Minguillón (2006) y Scutella y Barg (2010) abordan aspectos en los que el profesional debe tener en cuenta el uso que el ente auditado realiza de la TI en la planificación del trabajo, entre ellos: la forma en que se logrará el conocimiento, comprensión y evaluación de los sistemas de contabilidad y control interno; las consideraciones de los riesgos inherentes y de control a través de las cuales el auditor llega a la evaluación del riesgo de auditoría y finalmente, el diseño y aplicación de pruebas de control y procedimientos sustantivos apropiados para cumplir con el objetivo de la auditoría.

Sobre la definición del enfoque de auditoría, Hunton, Wright y Wright (2004b), Astiz y Sole (2008) y Casal (2010) plantean que, en virtud de la complejidad de los sistemas utilizados por las organizaciones, la tendencia a un enfoque basado en controles debería ser el proceso natural, dado que en entornos de TI difícilmente se pueda reducir el riesgo de auditoría y alcanzar la eficiencia utilizando únicamente un enfoque con procedimientos sustantivos.

Casal (2010) agrega que en la planificación se debe evaluar la necesidad de contar con la colaboración de especialistas de TI de acuerdo a la complejidad de los sistemas informatizados, incrementándose el carácter multidisciplinario del encargo de auditoría, y Hunton *et al.* (2004a) revelan de qué manera un auditor de sistemas puede colaborar con el auditor financiero en cada paso del encargo, si bien podría ejecutar él mismo dichas tareas en caso de tener los conocimientos y las habilidades necesarias.

Valencia y Tamayo (2012) resaltan que a partir de la incorporación de la TI se produce una evolución en las evidencias de auditoría que se convierten casi en su totalidad en digitales, careciéndose del acceso tradicional a la documentación de referencia, sea porque la información se encuentra almacenada solo en forma electrónica o está disponible solo por un periodo de tiempo limitado (Brazel y Agoglia, 2007; Pastor, 2011; *American Institute of Certified Public Accountants* (AICPA), SAS 80). Según Valencia y Tamayo (2012) ello conlleva la necesidad de un mejoramiento en las competencias de los profesionales para su adecuada obtención y tratamiento, debiendo acudir a las TAAC en forma complementaria a las técnicas manuales utilizadas tradicionalmente.

El cuadro 1 resume las consideraciones de diversos autores sobre la forma en que la TI afecta a la auditoría financiera. Los antecedentes disponibles presentan desarrollos conceptuales y análisis de normativa, existiendo una falta de trabajos empíricos basados en métodos como estudios de caso, encuestas o entrevistas. En la sección 4 de este trabajo se profundiza el análisis de la computación en la nube sobre cuatro de los aspectos de la auditoría considerados por los autores mencionados.

Cuadro 1: Resumen de Antecedentes acerca de Auditoría Financiera y TI

Referencia	País	Principales aportes
Cerullo y Cerullo (1997)	EE.UU.	Un sistema de procesamiento de la información automatizado no modifica el objetivo de la auditoría. Las fases de la auditoría son las mismas (planificación inicial, revisión y evaluación preliminar de la estructura de control interno, terminación de la revisión y testeo de controles, pruebas sustantivas y documentación y reporte), si bien la ejecución de cada una de ellas sufren modificaciones debido al uso de la TI por el ente auditado.
González (2004)	España	Importancia de los entornos informatizados sobre aspectos de la auditoría tales como la planificación, la evaluación de controles y de riesgos; énfasis en la relevancia de la evaluación de riesgos y los procedimientos diseñados en respuesta a ellos para obtener evidencia adecuada. Requisito de conocimientos mínimos por parte del auditor y asistencia de expertos.
Hunton *et al.* (2004a)	EE.UU.	Los sistemas de TI complejos requieren una evaluación de los sistemas de información como parte de la auditoría financiera. Un auditor de TI puede colaborar con el financiero en cada etapa de la auditoría contable, dependiendo su participación del nivel de contribución requerida por este último.
Minguillón (2006)	España	Importancia de la auditoría a través del ordenador, implementando técnicas y metodologías de auditoría adecuadas en particular en administraciones públicas que operan en entornos de TI cada vez más complejos. Efectos sobre diferentes aspectos de la auditoría. Relevancia de la formación del auditor y el trabajo multidisciplinario con especialistas de auditoría informática.
Astiz y Sole (2008)	España	En un entorno de TI complejo, una auditoría financiera eficiente y eficaz requiere un enfoque basado en la confianza en los controles, con una adecuada consideración de los riesgos tecnológicos que afectan la integridad y exactitud de los datos contables.
Scutella y Barg (2010)	Argentina	La existencia de sistemas de información computadorizados puede afectar la comprensión de los sistemas de contabilidad y control interno, la evaluación de riesgos inherentes y de control y el diseño y desarrollo de las pruebas de control y procedimientos sustantivos utilizados para la consecución del objetivo de auditoría.
Pastor (2011)	Perú	Efectos de la TI y la contabilidad *on-line* sobre el proceso de auditoría: la planificación de la auditoría (en particular la evaluación de los controles internos), las pruebas y la documentación. Importancia de la evaluación continua de la TI y las comunicaciones como forma de prevención y disuasión de errores en los estados financieros.
Valencia y Tamayo (2012)	Colombia	Importancia del uso de Técnicas de Auditoría asistidas por Computador a fin de obtener evidencias de auditoría digitales. Existencia de una escasa investigación académica en relación al tema.

Fuente: Elaboración propia.

3. LA COMPUTACIÓN EN LA NUBE

Se resaltan aquí conceptos referidos a la computación en la nube, a fin de caracterizar el nuevo entorno de TI al que pueden verse expuestos los auditores financieros.

El *National Institute of Standards and Technology* (NIST) (Mell y Grance, 2011:2) ha elaborado un concepto amplio para definir a la computación en la nube, refiriéndose a ella como:

> (…) un modelo que permite obtener, desde cualquier lugar y según las necesidades de la demanda, un cómodo acceso a través de una red a un conjunto compartido de recursos informáticos (redes, servidores, almacenamiento, aplicaciones y servicios) que pueden ser solicitados y provistos rápidamente, con un mínimo esfuerzo administrativo o interacción con el proveedor de los servicios.

Otros autores han elaborado conceptos y caracterizaciones que destacan distintos aspectos del servicio, como la escalabilidad del recurso y la valorización del servicio sobre una base de pago por uso (Vaquero, Rodero, Caceres y Lindner, 2009; Böhm, Leimeister, Riedl y Krcmar, 2011); la forma de provisión del servicio a través de internet (Joint, Baker y Eccles, 2009; Mowbray, 2009) y la independencia de localización entre el usuario y el proveedor del servicio de la nube (Buyya, Yeo, Venugopal, Broberg y Brandic, 2009).

Mell y Grance (2011) resumen un conjunto de características esenciales que definen la CN: autoservicio, acceso a través de la red, recursos compartidos por diversos usuarios, rápida escalabilidad y servicio medido. A su vez definen los modelos de provisión de *cloud computing*, incluyendo tres tipos de servicios (*Software*, Plataforma e Infraestructura como un Servicio) y cuatro de distribución (nubes públicas, privadas, comunitarias e híbridas). Cada uno de estos modelos implican diferentes niveles de responsabilidad del usuario y del proveedor sobre el control interno, la seguridad y la configuración del servicio (Liu *et al.*, 2011:9; *Committee of Sponsoring Organizations of the Treadway Commission* (COSO), 2012).

La prestación de estos servicios a través de internet requiere de una red de relaciones entre diferentes actores que conforman una cadena (Böhm *et*

al., 2011), cuya arquitectura comprende además del usuario y el prestador, a los denominados *broker, carrier* y el auditor de la nube, que ejecuta una evaluación independiente del servicio analizando a todos los miembros de la cadena (Liu *et al.*, 2011). La relación entre ellos se formaliza mediante lo que se conoce como *Service Level Agreement* (SLA) (Buyya *et al.*, 2009), que estipula, entre otras cuestiones, el tipo de servicio a prestar y los roles y responsabilidades de cada actor, siendo en algunos casos fruto de la negociación de ambas partes o en otros, simples contratos de adhesión.

Otra particularidad de la CN se refiere al cambio en la geografía de la computación (Hayes, 2008) derivado de la independencia de localización entre el usuario y el proveedor (Buyya *et al.*, 2009). Los proveedores buscan ubicar sus recursos en lugares donde existan bajos costos (Armbrust *et al.*, 2010), pudiendo crearse nubes con centros de datos localizados en distintos países (Zhang *et al.*, 2010). En algunos casos ocurre que el usuario desconoce la localización exacta de los datos propios almacenados en la nube (Mansfield, 2008).

Ello tiene dos consecuencias principales sobre la auditoría: a) los elementos a ser evaluados están físicamente en una o más instalaciones separadas geográficamente entre sí, siendo complejo y oneroso que el equipo de auditoría realice un trabajo presencial; b) se deben tener en cuenta los marcos jurídicos involucrados para evaluar su cumplimiento, considerando la distribución geográfica de los recursos (CSA, 2011:13).

Dada la configuración de la infraestructura y la forma de prestación del servicio tercerizado con una importante participación del proveedor, Rumitti y Falvella (2013) destacan que la auditoría en entornos de la nube debe orientarse en principio a la evaluación de riesgos y controles derivados de su uso por el ente auditado y al grado de seguridad (confidencialidad, integridad y disponibilidad) brindado para la elaboración de la información financiera.

En relación a los riesgos, se debe identificar únicamente aquellos que fueran relevantes para la auditoría financiera dentro del conjunto amplio de riesgos que representa la nube —algunos que le son propios y otros comunes a las alternativas de tercerización tradicional, pero que pueden verse potenciados en este entorno (Chow *et al.*, 2009)—.

Sobre la comprensión y prueba de los controles internos, es fundamental conocer aquellos implementados por el proveedor del servicio en relación a la información financiera importante del usuario (Arens, Elder y Beasley, 2007). Ello encuentra ciertas dificultades en el caso de la CN, considerando la complejidad de las cadenas de suministro, debiendo el auditor obtener satisfacción suficiente basada en la evaluación de riesgos y controles operacionales considerando a todos sus integrantes (CSA, 2011:113). A su vez, el acceso a los controles para su evaluación, probablemente se verá entorpecido por el proveedor del servicio para evitar las auditorías redundantes y sus potenciales perjuicios (Nicolaou *et al.*, 2012; Rumitti y Falvella, 2013) debiendo evaluarse la aplicación de métodos alternativos para la realización del trabajo.

Rumitti y Falvella (2013) mencionan respecto de la obtención de evidencias en la nube, que la posibilidad de aplicación de pruebas sustantivas y analíticas depende de la modalidad del servicio contratado por el ente, considerando que los servicios de tipo IAAS son más permeables a la auditoría que los de tipo SAAS.

Este cambio en el ambiente de TI a ser enfrentado por la auditoría como disciplina, demanda cierta capacidad de adaptación, pero hasta el momento no ha sido acompañado por una respuesta adecuada en el ámbito normativo profesional. Nicolaou *et al.* (2012) mencionan que los estándares de auditoría no se han desarrollado aún al punto de brindar una guía clara sobre cómo y qué testear en las operaciones de un cliente cuando depende de un proveedor de CN. No obstante, las organizaciones profesionales —como el AICPA, el *Canadian Institute of Chartered Accountants* (CICA) y la *Information Systems Audit and Control Association* (ISACA)— se encuentran trabajando en ello, resultando útiles los aportes que se puedan efectuar sobre el tema.

En función de las características descriptas, se denota que el uso de la CN como soporte de la generación de información contable representa un nuevo contexto para el trabajo del auditor financiero, con particularidades que la diferencian de otros entornos de provisión de servicios TI. En consecuencia, se requiere la revisión de la forma en que el auditor realizará la ejecución del encargo de auditoría en este ambiente, así como las herramientas, métodos,

pruebas de auditoría, las responsabilidades, la necesidad de colaboraciones de especialistas, entre otros (CSA, 2011).

En la próxima sección se describen ciertos aspectos de la auditoría financiera que se consideran particularmente afectados por este nuevo entorno.

4. ASPECTOS DE LA AUDITORÍA FINANCIERA POTENCIALMENTE AFECTADOS POR LA CN

Sobre la base de los antecedentes relevados respecto de la auditoría financiera en entornos de TI en la sección 2 y considerando las particularidades de la CN indicadas en la sección 3, se profundiza a continuación la revisión de antecedentes sobre los efectos que la implementación de esta tecnología por parte del ente auditado puede tener sobre determinados aspectos de la auditoría seleccionados, a saber: el conocimiento del cliente; la identificación y evaluación de riesgos; la evaluación de controles internos; la obtención de evidencias y las capacidades exigidas a los profesionales contadores públicos así como la colaboración de expertos para el desarrollo de trabajos de auditoría en estos ambientes.

Tal como se indicó en la introducción de este trabajo, la revisión efectuada se refiere a la literatura disponible, como también a la normativa de auditoría vigente en la República Argentina[4] aplicable a cada una de estas etapas (cuadro 2). Además se mencionan aspectos relacionados que se incluyen en diferentes documentos elaborados por organismos profesionales (cuadro 3), si bien estos no se refieren específicamente a la auditoría financiera. Los últimos no tienen carácter vinculante, siendo recomendaciones elaboradas sobre la base de la opinión y experiencia de profesionales que conforman los distintos organismos para guiar a las empresas y profesionales frente a los nuevos desafíos que la CN representa.

[4] En la República Argentina conviven normas de auditoría nacionales, como la RT 37 de la FACPCE (2013), y las normas internacionales de auditoría (NIA) y normas internacionales de encargos de aseguramiento de la IFAC, cuya adopción en Argentina ha sido resuelta por las Resoluciones Técnicas RT 32 (FACPCE, 2012) y RT 35 (FACPCE, 2012). En particular, las NIA son de aplicación obligatoria para las auditorías de estados financieros que deben ser emitidos aplicando las Normas Internacionales de Información Financiera y de aplicación opcional en el resto de los casos.

Cuadro 2: Normas Internacionales y Nacionales vinculadas al tema de investigación

	ORGANISMO EMISOR - NORMATIVA	NORMAS RELEVADAS
INTERNACIONALES	*International Federation of Accountants* (IFAC) - *International Standards on Auditing* (ISA) e *International Standard on Assurance Engagements* (ISAE)	NIA 315 (ACTUALIZADA) – Identificación y análisis de los riesgos de distorsiones significativas mediante la comprensión de la entidad y su entorno.
		NIA 402 – Consideraciones sobre auditorías relacionadas con entidades que utilizan organizaciones de servicios.
		NIA 500 – Elementos de juicio de las auditorías.
		NIA 620 – Uso del trabajo de un experto.
		ISAE 3000 – Encargos de aseguramiento distintos de las auditorías o revisiones de información financiera histórica.
		ISAE 3402 – Reporte de aseguramiento sobre los controles en una organización de servicios.
ARGENTINA	Federación Argentina de Consejos Profesionales de Ciencias Económicas (FACPCE) - Normas de auditoría y de encargos de aseguramiento	RESOLUCIÓN TÉCNICA 37 – Normas de Auditoría, Revisión, Otros Encargos de aseguramiento, Certificación y Servicios Relacionados.

Fuente: Elaboración propia.

Cuadro 3: Documentos y recomendaciones relacionados a la CN

ORGANISMO EMISOR	PAÍS/ REGIÓN	AÑO	ESTÁNDARES Y RECOMENDACIONES
Cloud Security Alliance	EE.UU.	2011	Cloud Compliance Report: Capítulo en Español de Cloud Security Alliance.
		2013	The Notorious Nine: Cloud Computing Top Threats in 2013.
		2013	CSA position paper on AICPA Service Organization Control Reports.
Committee of Sponsoring Organizations of the Treadway Commission (COSO)	EE.UU.	2012	Enterprise Risk Management for Cloud Computing.
European Network and Information Security Agency (ENISA)	Europa	2009	Cloud Computing - Benefits, risks and recommendations for information security.
Information Systems Audit and Control Association (ISACA)	Internacional	2011	IT control objectives for Cloud Computing.
		2012	Principios rectores para la adopción y el uso de la computación en nube.
National Institute of Standards and Technology (NIST)	EE.UU.	2009/ 2011	NIST SP 800-145 – The NIST Definition of Cloud Computing.
		2011	NIST SP 500-292 – NIST Cloud Computing Reference Architecture.
		2011	NIST SP 800-144 – Guidelines on Security and Privacy in Public Cloud Computing.

Fuente: Elaboración propia.

4.1. CONOCIMIENTO DEL CLIENTE

A los efectos de cumplir con el objetivo de la auditoría de estados financieros, el profesional auditor debe realizar un examen que comprende un proceso de investigación de tres etapas: planificación, ejecución y reporte (Fowler Newton, 2004:6). La planificación pretende prever los procedimientos que se aplicarán para obtener los elementos de juicio válidos para sustentar la opinión y los recursos necesarios para llevar a cabo dichos procedimientos (Slosse, Gordicz y Gamondés, 2007).

Un primer paso fundamental en la etapa de planificación, consiste en lograr un conocimiento integral del negocio del ente auditado y su entorno (Bell, Marrs, Solomon y Thomas, 1997), a partir de la comprensión en profundidad de la naturaleza de la actividad del ente, sus operaciones y su industria (Arens *et al.*, 2007; Casal, 2009), con el fin que el auditor pueda formarse una idea de ciertos riesgos a nivel global, pudiendo, sobre la base de ellos, evaluar la condición de auditabilidad *(auditability)* del ente y ejecutar una auditoría efectiva fundamentada en evidencias de auditoría más exhaustivas y relevantes.

Entre los factores que han incrementado la importancia del entendimiento del cliente y la industria, Arens *et al.* (2007:199-200) resaltan la incorporación de la TI en los procesos internos del auditado y en las comunicaciones con proveedores y clientes. Se debe identificar y entender los sistemas de contabilidad y control interno afectados por el ambiente de TI, enfocándose en la importancia y la complejidad de las actividades desarrolladas en dicho ambiente (Astiz y Sole, 2008; Scutella y Barg, 2010).

En este paso, el profesional debería tomar conocimiento del uso que la compañía auditada esté realizando de la computación en la nube. Una adecuada comprensión del modelo de servicio y de distribución adoptado por el ente será fundamental, dado que no solo poseen características propias, sino que en principio pueden representar diferentes tipos de riesgos (ENISA, 2009) que pueden afectar la información financiera. Además el profesional debe considerar que si el uso de la CN es significativa para la entidad y pertinente para la auditoría, deberá obtener una comprensión suficiente de la organización de servicios (el proveedor), su entorno y su

control interno, con el fin de identificar y analizar los riesgos de distorsiones significativas y diseñar procedimientos de auditoría en respuesta a ellos (IFAC, NIA 402, 7).

4.2. IDENTIFICACIÓN Y EVALUACIÓN DE RIESGOS

A partir del conocimiento obtenido, el profesional estará en condiciones de evaluar el riesgo de negocio del cliente[5]; esto implica comprender las condiciones —internas y del entorno— que amenazan la habilidad de la organización para ejecutar los procesos de negocio efectivamente y alcanzar sus objetivos. La gerencia del ente usuario es la responsable de identificar dichos riesgos y determinar respuestas para enfrentarlos —como prácticas de evaluación de riesgos efectivas y una dirección corporativa—; en consecuencia, el auditor evalúa dichos controles administrativos y determina los riesgos residuales de errores de importancia que se utilizan para clasificarlos mediante el modelo de reisgo en auditoría. (Arens *et al.*, 2007).

Dentro de los riesgos residuales, el profesional debe identificar los "riesgos significativos" (IFAC, NIA 315, 26), aquellos que representan riesgo de error material en los estados contables, en la medida en que no todo riesgo de negocio es relevante para el auditor. Los riesgos significativos deben ser evaluados en dos niveles: riesgos de declaración equivocada material a nivel de estado financiero (riesgos globales o generales) y a nivel de aserción para las clases de transacciones, saldos de cuentas y revelaciones (riesgos específicos o individuales) (IFAC, NIA 315, A98, A102; Fowler Newton, 2004:525; Casal, 2013).

El modelo de riesgo en auditoría comprende cuatro categorías (Arens *et al.*, 2007:241): riesgo inherente (RI), riesgo de control (RC), riesgo planeado de detección (RD) y riesgo aceptable de auditoría. La TI representa un nuevo

[5] La literatura actual así como las normas y estándares profesionales internacionales (en particular la NIA 315) guían a los auditores a considerar el riesgo de negocio del cliente cuando evalúan el riesgo de error material durante la fase de planificación de la auditoría financiera (Schultz, Bierstaker y Donell, 2010; Mantilla y Casal 2012); por el contrario, según Casal (2013), no se puede fundamentar que las normas argentinas (actual RT 37 y anterior RT 7) necesariamente provean lineamientos a ese fin.

factor en la medición de los riesgos inherente y de control, en la medida en que incorpora amenazas que no estaban presentes en los entornos manuales, tales como la ausencia de rastros de transacciones, la falta de segregación de funciones o la generación automática de transacciones y registraciones por el ordenador (Minguillón, 2006; Oggero, 2006). La NIA 315 reconoce ciertos riesgos específicos derivados de la informática en lo que respecta al control interno de la entidad y Presa (2013) menciona factores agravantes de cada tipo de riesgo derivados del uso de la TI. A su vez, el riesgo de auditoría es creciente conforme se incrementa la complejidad del entorno informatizado (Minguillón, 2006; Casal, 2013).

En la literatura, diversos autores han documentado los potenciales riesgos del uso de la CN siempre desde la perspectiva de la entidad usuaria. Entre ellos, ENISA (2009) elaboró un detalle de 35 riesgos clasificados en riesgos de política y organización (incluyendo riesgos de *lock-in* —que representan dificultades para la migración o cambio de proveedor—, pérdida de gobernanza, reputación compartida, viabilidad del proveedor), técnicos (por ejemplo, fallas de aislamiento, empleado malicioso, fallas en la protección de los datos), legales (riesgo de cumplimiento, de cambio de jurisdicción, de protección de datos y confidencialidad) y otros no específicos de la nube (problemas del uso de internet, acceso no autorizado a instalaciones, desastres naturales, robos de equipos de computación).

Svantesson y Clarke (2010) examinan, entre otros, los riesgos de *privacidad*, diferenciando entre las "nubes domésticas" y las "nubes transfronterizas", siendo estas últimas una amenaza para el cumplimiento de la normativa. Mansfield (2008), Mowbray (2009), Armbrust *et al.* (2010), Jansen y Grance (2011), ISACA (2012), entre otros tantos, también resumen riesgos similares a los mencionados por los otros autores.

Por su parte, el comité COSO (2012) ha elaborado un informe orientado a la gestión de riesgos empresariales en CN y la CSA (2013a) identificó nueve amenazas a la seguridad en la nube con el objeto de guiar decisiones de gestión de riesgo por parte de usuarios y proveedores. Yigitbasioglu *et al.* (2013: 111) destacan que los riesgos de seguridad son particularmente relevantes en relación a los datos financieros y contables almacenados en la nube. Sin embargo, no se han encontrado estudios o recomendaciones en

relación a qué riesgos de la CN son realmente "significativos" para la auditoría financiera en los términos de la NIA 315.

4.3. EVALUACIÓN DE CONTROLES INTERNOS

Una vez obtenido un adecuado conocimiento del cliente e identificados y valorados los riesgos significativos, el auditor debe evaluar los controles internos relevantes (IFAC, NIA 315, 28) que sirven para prevenir, detectar o corregir los errores en la información financiera (Casal, 2011; Presa, 2013), definir el riesgo de control y determinar el enfoque de auditoría a aplicar —de cumplimiento o sustantivo (Nannini et al., 2011)—.

Por ser la CN un entorno de TI con cierta complejidad, es importante la revisión del sistema de control interno en la planificación de la auditoría financiera, en la medida en que le permite al auditor considerar los riesgos tecnológicos de auditoría que pudieran afectar la integridad y exactitud de los datos (Astiz y Sole, 2008), a la vez que le genera economías en el desarrollo de la auditoría debido a la reducción del alcance del trabajo que se puede lograr a partir de la evaluación de los controles (Hunton *et al.*, 2004a).

En primer lugar, el auditor obtiene información referida al diseño e implementación de los controles y define el nivel de riesgo preliminar, en función del cual decide si es conveniente continuar con el testeo de los controles mediante pruebas que permiten evaluar su eficiencia operativa, aplicando un enfoque de cumplimiento si el riesgo de control es bajo (Fowler Newton, 2004; Minguillón, 2006, 2010; Presa, 2013) o aplicar un enfoque sustantivo o abandonar el encargo, cuando el riesgo de control es muy alto. Dicho análisis debe ser realizado para dos categorías de controles, los generales y los de aplicación (González, 2004; Arens *et al.*, 2007), evaluándolos en ese orden en la medida en que el mal funcionamiento de los primeros invalida los segundos, dando lugar a manifestaciones erróneas en los estados contables sin que sean detectadas.

Ahora bien, aun cuando las normas de auditoría brindan un marco para la evaluación de los sistemas de control interno, no existe normativa técnica general que guie la evaluación de en ambientes de TI complejos en una auditoría financiera (Minguillón, 2010), menos aún en entornos tan recientes

como lo es el de la CN, respecto del cual existe una falta de estándares específicos que guíen la labor del auditor (Nicolaou *et al.*, 2012).

El uso de una organización de servicios por el ente auditado –donde ciertas políticas, procedimientos y registros a su cargo pueden generar un impacto material en los procesos que componen el sistema de control interno del cliente– requiere que el auditor obtenga cierto nivel de seguridad sobre la eficacia del diseño y funcionamiento de los controles internos que residen en toda la cadena de provisión del servicio (Arens *et al.*, 2007; CSA, 2011:116).

Para estos casos, la NIA 402 prevé como alternativas la obtención de un informe sobre la descripción, diseño y, en su caso, eficacia operativa de los controles del prestador del servicio; el contacto del auditor financiero con el prestador para obtener información específica; visitas a la organización de servicios para aplicar procedimientos sobre los controles relevantes; recurrir a auditores del servicio independientes con el fin de que apliquen procedimientos que proporcionen la información necesaria sobre los controles.

Aun cuando la CSA (2011:117) recomienda que el prestador del servicio debe disponer los medios para facilitar los trabajos de auditoría, Joint *et al.* (2009:274) y Nicolaou *et al.* (2012) reconocen que es poco probable (sino imposible) que contractualmente se otorguen derechos a realizar auditorías a los usuarios —y sus auditores— que les permitan entrar en el proveedor para verificar el desempeño de los servicios y revisar los procedimientos, sea por la forma en que los datos están almacenados en la nube, el riesgo de que se interrumpa la prestación del servicio o de que se pongan en riesgo los datos de otros usuarios que se encuentran excluidos de la auditoría, pero que están alojados en los mismos equipos (CSA, 2013b; Rumitti y Falvella, 2013).

En consecuencia, el uso de informes de terceros independientes sobre los controles de la organización de servicios parece ser la opción viable, existiendo diversas alternativas previstas en las normas internacionales (IFAC, NIA 402, ISAE 3402 y 3000) más detalladamente en las normas estadounidenses (AICPA, SSAE 16 y AU Section 401) y recientemente incorporadas en las argentinas (FACPCE, RT 37) —sea informes sobre los controles de la empresa de servicios que son relevantes para el control interno

de entidades usuarias sobre los informes financieros (conocidos como reportes SOC1) o sobre controles relevantes para la seguridad, continuidad, integridad de procesamiento de un sistema o la confidencialidad o privacidad de la información procesada por el sistema (SOC2 o 3); y a su vez informe sobre controles puestos en operación o sobre controles puestos en operación y su eficacia operativa (Tipo I o II según las diversas normas)—.

En el SLA es donde debe definirse —si es posible la negociación— el tipo de informe que debe proveer el auditor del servicio contratado por el proveedor (SOC1, 2 o 3; Tipo I o II) y el periodo a cubrir, los dominios de control a evaluar (sean objetivos de control en SOC1 o principios determinados en SOC2/3), la existencia de subproveedores del servicio y si serán incluidos, o no, el alcance (métodos *cave-out* o *integrated* según ISAE 3402, 9) y la fecha esperada de entrega del reporte (KPMG, 2012).

En cuanto a la selección del tipo de informe, el AICPA (s.f.) reconoce que la emisión de un informe SOC2 resulta eficaz porque cubre tanto riesgos relativos a los estados financieros como otros riesgos operacionales, siendo que puede ser utilizado tanto por las organizaciones usuarias como por sus auditores. Según la CSA (2013b), el proveedor debe proporcionar un informe SOC1 si su servicio impacta sobre la elaboración de la información financiera de los usuarios; un informe SOC2 si no posee un efecto directo o relevante sobre los controles internos sobre el reporte financiero, pudiendo ser necesario que provea ambos para poder cubrir las expectativas de sus clientes. KPMG (2012) indica que en el caso de uso de la nube para servicios de tipo ERP (*Enterprise Resource Planning*) aplican los informes de tipo SOC1 en la medida en que provee un servicio de información financiera a los usuarios, pero reconoce que también podría emitirse un SOC2/3 referido a seguridad y continuidad/disponibilidad para responder a las necesidades específicas de los usuarios de los servicios. Por su parte, la NIA 402 plantea que el informe Tipo I puede resultar útil para comprender el control interno en la planificación de la auditoría, mientras que la RT 37 recomienda a los auditores financieros el uso del informe Tipo II.

Un problema adicional se refiere a qué marco debe ser utilizado para la evaluación de los controles en la nube, que definirá los controles a ser relevados e informados por el auditor del servicio. En general, las

auditorías de sistemas no relacionadas a una auditoría financiera, basadas en marcos como el COBIT, comprenden una gran cantidad de controles generales que no resultan relevantes desde el punto de vista de la auditoría financiera (Minguillón, 2010).

La CSA (2011:117) recomienda que para realizar el trabajo en la nube se utilicen marcos referidos a esta tecnología, los cuales están aún en desarrollo o en un estado incipiente de aplicación. En particular pretende que para la elaboración de informes SOC2, además de utilizar los principios y criterios propuestos por el AICPA, se aplique como criterio adicional la Matriz de Controles en la Nube (*Cloud Controls Matrix* (CCM)) para producir un reporte de aseguramiento que provea una evaluación más pertinente y comprensiva de los controles para usuarios de los servicios de CN (CSA, 2013b).

En consecuencia, en función del tipo de informe que le sea brindado y el marco utilizado para la evaluación de controles, el auditor financiero aún debe considerar si ha obtenido información suficiente y pertinente en relación a los controles que fueran relevantes según su propia evaluación de riesgos, dejando de lado otros controles respecto de los que hubiera obtenido información, pero cuya evaluación implica un trabajo innecesario e ineficiente. Si la comprensión obtenida a través de dichos informes resulta insuficiente, el auditor del usuario podría intentar utilizar el resto de los procedimientos propuestos por la NIA 402 indicados previamente, existiendo dudas acerca de su aplicabilidad en un entorno de CN por las restricciones mencionadas.

4.4. EVIDENCIAS DE AUDITORÍA EN CONTEXTOS DE CN

Las evidencias de auditoría comprenden toda la información utilizada por el auditor para alcanzar las conclusiones sobre las cuales se basa su dictamen e incluyen tanto la información contenida en los registros contables de los que se obtienen los estados financieros, como otra información (IFAC, NIA 500; AICPA, SAS 106). A través de ellas, el profesional pretende determinar si la información auditada se presenta de acuerdo con el criterio establecido y si los estados financieros se presentan con objetividad (Arens *et al.*, 2007:162). Entre los objetivos de su obtención

y su adecuada documentación en papeles de trabajo se encuentran los siguientes: a) facilitar el planeamiento de la auditoría; b) permitir la preparación del informe y respaldar la opinión del auditor; c) servir como respaldo de las comunicaciones y del trabajo realizado frente a posibles controversias legales/judiciales o disciplinarias (Fowler Newton, 2004).

Los antecedentes encontrados en relación a las evidencias en la CN se refieren a la obtención de evidencias digitales en la nube —considerando su función de repositorio de datos e información almacenados a ser analizados para la obtención de indicios— desde la perspectiva de la auditoría interna, la auditoría de TI (CSA, 2011:105-108) y de la informática forense (Taylor, Haggerty, Gresty y Hegarty, 2010; Taylor, Haggerty, Gresty y Lamb, 2011). Se recurre entonces a los antecedentes referidos a las evidencias digitales que surgen a partir de la incorporación de la TI en los procesos de negocio, de modo que los auditores deben recopilar y procesar información electrónica como evidencia de auditoría (Caldana, Correa y Ponce, 2007), volviéndose más escasa la evidencia física con la que habitualmente trabajan (Valencia y Tamayo, 2012).

Caldana *et al.* (2007:12) las definen como aquella información —texto, gráficos, imagen, audio, video, o cualquier otra— creada, transmitida, procesada, registrada y/o mantenida electrónicamente, que respalda el contenido de un informe de auditoría. Pueden ser clasificadas en dos categorías (Minguillón, 2006) que deben ser evaluadas en conjunto: a) los programas y elementos lógicos empleados en la gestión por el auditado, de donde el auditor externo obtiene evidencia sobre los controles internos; b) los datos e información contenidos en soportes electrónicos, que representan la versión intangible de muchas pistas visibles de transacciones que son rastreadas por los auditores, destacándose del resto de la evidencia documental por su característica de ilegibilidad.

Si bien el objetivo de la auditoría y la función de los elementos de juicio no se ven alteradas, las modificaciones significativas que se producen en las características de las evidencias a partir de la TI hacen que se requiera una forma diferente de obtenerlas, tratarlas y usarlas dentro del ciclo de auditoría (Valencia y Tamayo, 2012); en el caso de la CN se han detectado ciertas particularidades que merecen ser analizadas.

En primer lugar, no es posible la estandarización de procedimientos para la obtención, análisis y presentación de evidencias, debido al secreto de las arquitecturas de la nube pretendido por los proveedores —siendo que cada servicio es distinto a los demás— (CSA, 2011), debiéndose adaptar los programas y procesos de obtención de evidencias en cada caso en particular (Taylor *et al.*, 2010; Taylor *et al.*, 2011).

Al planificar la forma de obtención de las evidencias, el profesional deber evaluar la disponibilidad de la información a los fines de la auditoría y los riesgos específicos de su uso (Caldana *et al.*, 2007). La misma puede verse afectada por características propias de la TI como la falta de visibilidad de los registros de auditoría (Arens *et al.*, 2007) por la inexistencia de soporte documental tangible de los archivos electrónicos (IFAC, NIA 500).

A su vez, la CN introduce dificultades adicionales. La ubicación de la información auditada es un factor que determina la posibilidad de realizar el trabajo en las instalaciones del cliente o no (Pastor, 2011); en el caso de la nube pública, los datos se encuentran en instalaciones del proveedor y el ente accede a ellos a través de internet; ello representa ciertas dificultades para el auditor: la particularidad de los recursos compartidos impide el acceso irrestricto a los sistemas y datos por la necesidad de proteger a otros usuarios (CSA 2011b; Taylor *et al.*, 2011); la responsabilidad compartida implica que si bien los datos siguen siendo propiedad del usuario, las aplicaciones o servicios que gestionan los datos pueden ser propiedad del proveedor; la distribución geográfica de los datos y la falta de trazabilidad de su ubicación –salvo que se haya estipulado algo distinto al respecto– genera dificultades para su obtención íntegra por el desconocimiento de su ubicación (CSA, 2011) dada la indisponibilidad de un único dispositivo de almacenamiento que pueda ser aislado o copiado para contar con la totalidad de la evidencia; finalmente, la conservación de la evidencia está bajo control y voluntad del tercero involucrado.

Como consecuencia de lo anterior, la identificación de las evidencias suele ser más sencilla en una nube privada en la medida en que los datos residen en los sistemas del ente auditado o en los del proveedor de la nube y los servidores, aplicaciones o repositorios de datos, en los que potencialmente están los elementos de juicio, son identificables, pudiéndose cerrar los

servidores por un tiempo limitado para obtenerlos (Taylor *et al.*, 2011). Ello no resulta posible en la nube pública, dada la arquitectura más dispersa con presencia de otros usuarios que no deben verse perjudicados.

La existencia de los datos contables originales en un único momento o en un lapso de tiempo limitado puede afectar la naturaleza y oportunidad de ejecución de los procedimientos de auditoría (González, 2004; Arens *et al.*, 2007; Pastor, 2011; IFAC, NIA 500). En el caso de la nube, la evidencia es más etérea y dinámica, no habiendo prácticamente datos permanentes (los registros de ingresos o los archivos temporarios de internet pueden ser eliminados inmediatamente después que el usuario cierra su sesión, disminuyendo por ejemplo la cantidad de evidencia para la evaluación de controles) (Taylor *et al.*, 2010; Taylor *et al.*, 2011). A su vez, al estar los datos distribuidos en diferentes jurisdicciones, quedan sujetos a las normas vigentes en cada una de ellas en cuanto a plazo y forma de conservación. En estos casos el auditor debería ejecutar los procedimientos en el momento en que la información esté disponible o requerir al cliente la retención de cierta información para su evaluación (IFAC, NIA 500, 24; AICPA, SAS 106, 25), lo cual podría implicar que se incluya en el contrato de auditoría la obligación del ente de conservar esos datos para garantizar el cumplimiento.

Las medidas de seguridad adoptadas para garantizar la seguridad de la información pueden convertirse en una traba para el profesional; por ejemplo, la autenticación de los usuarios requiere que se prevea como accederán los miembros del equipo de auditoría a la información almacenada, creándose perfiles de usuario con las atribuciones necesarias para que puedan realizar su labor (Taylor *et al.*, 2010; Taylor *et al.*, 2011); a su vez se debe determinar si se podrán utilizar las herramientas TAAC que usualmente emplea en otros entornos de TI. Por otra parte, el uso del encriptado implica que el profesional no solo debe identificar las evidencias sino que además debe traducirlas o decodificarlas, requiriéndose que se provean las claves, tal como ocurriría en un caso de investigación forense (Taylor *et al.*, 2010).

La falta de disponibilidad de la información se puede producir también por la destrucción o modificación no autorizada de los archivos electrónicos originales con información que respalda los saldos y transacciones reflejados en los registros contables, lo cual es un riesgo de la CN mencionado por

diversos autores. Dicha alteración —intencional o no— puede ser más sencilla que en los documentos en papel sin que queden rastros de ella (AICPA, SAS 80), no pudiendo en muchos casos ser recuperadas salvo que el ente posea adecuados archivos de respaldo (Arens *et al.*, 2007; Casal, 2010) o hubiera previsto las medidas de seguridad adecuadas como el uso del encriptado. A partir de las conclusiones a las que hubiera arribado el auditor en la etapa de evaluación de controles internos, podrá determinar si el diseño, implementación y operatividad de los controles de seguridad y los automatizados son suficientes para prevenir los cambios no autorizados en los sistemas o en los registros contables. Según el resultado obtenido, determinará la necesidad de aplicar procedimientos adicionales tales como confirmaciones de terceros para evaluar la integridad y fiabilidad de la evidencia obtenida.

Además de la disponibilidad, el auditor deberá evaluar la confiabilidad de las evidencias electrónicas que usará como elementos de juicio (IFAC, NIA 500, 10; AICPA, SAS 106, 9), debiendo mantenerse escéptico en relación a la autenticidad de los registros brindados por sus clientes. Si bien el auditor no necesariamente es un especialista en la obtención y examen de evidencia informática para darse cuenta que la información proporcionada por los ordenadores no es fiable, él deberá arbitrar los medios que estén a su alcance para cerciorarse de ello, sea obteniendo evidencia corroborativa de lo que ha conocido de su cliente o teniendo en cuenta las conclusiones obtenidas de la comprensión y testeo de los controles informáticos, en la medida en que la suficiencia y adecuación de la evidencia dependerá de la efectividad de los controles internos existentes para asegurar la exactitud e integridad del registro electrónico de la información.

Por otra parte, al aplicar las técnicas para la obtención de las evidencias en formato electrónico, el auditor buscará garantizar la inalterabilidad de la información de origen, dado que nada impediría que sea este quién, accidental o intencionalmente, modifique los archivos soporte. Un alternativa consiste en utilizar *software* de auditoría con garantía de no modificación de datos de origen. Si ello no fuera posible, debería evaluar el uso de otros

medios para este fin, por ejemplo la aplicación de la firma digital, la electrónica o funciones de tipo *hash*.

Estas alternativas permitirían además garantizar el origen, la autoría y la integridad de los archivos y/o documentos digitales que obtiene. Así, en caso que la fuente de las evidencias electrónicas desapareciera de la nube una vez ejecutados los procedimientos y obtenidas los elementos de juicio por alguno de los riesgos que ella implica, quedando como única constancia de su existencia las copias que en sus papeles de trabajo conserva el auditor, este podría oponerlas como respaldo de su opinión y, en caso de que fuera necesario, utilizarlos como medio de prueba en instancias judiciales. Sin embargo, estas precauciones tienen el límite en el dinamismo de la información.

Una vez superadas las dificultades relacionadas a la obtención de las evidencias en la nube, se entiende que el procesamiento y evaluación de la información dependerá de las decisiones que adopte cada profesional atendiendo a las circunstancias y al plan de trabajo definido en el proceso de planificación de la auditoría, siempre aplicando los procedimientos sobre copias de los archivos originales contenidos en la nube, para evitar la alteración de estos últimos. Finalizado el procesamiento, el profesional evaluará si el alcance de su trabajo fue suficiente para cubrir todos los riesgos posibles, no existiendo riesgos residuales de no detección de errores materiales. En caso que continuara siendo un riesgo significativo, debería ajustar sus procedimientos o comprensión del proceso para contemplar las actividades que minimicen dicho riesgo.

Por último, el auditor deberá arbitrar los medios para garantizar la conservación de las evidencias, tanto de los datos obtenidos de su cliente como de los papeles de trabajo electrónicos que hubiera generado. Para ello deberá preservar los documentos digitales tomando medidas que prevengan su obsolescencia y destrucción, garantizado su disponibilidad futura, teniendo en cuenta que los plazos de conservación exigidos a los profesionales exceden con creces los ciclos cada vez más cortos de renovación tecnológica.

4.5. COMPETENCIAS PROFESIONALES. INTERVENCIÓN DE ESPECIALISTAS

En la medida en que se producen nuevos avances tecnológicos, los auditores necesitan expandir sus conocimientos y habilidades sobre sistemas de información contable complejos para poder desarrollar auditorías eficientes y eficaces (Brazel y Agoglia, 2007; Brazel, 2008).

Si bien no se espera que el profesional sea un experto en informática, el nivel de conocimientos alcanzado le debe permitir planificar, dirigir, supervisar y revisar el trabajo realizado (Minguillón, 2006), volviéndose más competente para comprender el grado de influencia que el uso de la TI tiene sobre los sistemas contable y de control interno de la entidad (González, 2004) y consecuentemente sobre la auditoría de estados financieros en general (SAS 94) y el propio enfoque de la auditoría en particular (González, 2004).

Según Brazel y Agoglia (2007), la pericia en sistemas de información contable permite al auditor sobreponerse a las dificultades que representan los entornos complejos respecto de la evaluación de riesgos específicos de los sistemas, la planificación de pruebas de control y procedimientos sustantivos, la confianza en los juicios de años anteriores como punto de partida, proveyendo las bases para ajustar los planes de auditoría para mitigar los riesgos potenciales específicos de los sistemas de información. Los autores destacan que la formación debe alcanzar a todos los miembros del equipo de auditoría; en la selección de sus miembros la pericia en sistemas de información complejos puede ser más valorada que la experiencia general en auditoría.

Los conocimientos del profesional deben comprender las normas relacionadas, las características de los entornos informatizados, una profundización en la evaluación de los controles internos generales y de aplicación, la evidencia informática, uso de las principales TAAC y papeles de trabajo electrónicos, así como conceptos básicos sobre auditoría de sistemas de información (Minguillón, 2006).

Presa (2013) reconoce que frente al avance constante y rápido de la tecnología, es posible que existan temas relacionados a la TI que excedan los conocimientos y habilidades del profesional a cargo del encargo de auditoría. A partir de la consideración de la propia competencia, el auditor

debe evaluar la necesidad o conveniencia de contar con el asesoramiento oportuno de especialistas con conocimientos adicionales o más profundos de los que él mismo posea en algún área de sistemas (González; 2004; Presa, 2013). Brazel (2008) destaca que la mayor complejidad de los sistemas de TI adoptados por las empresas, han incrementado el rol de los auditores de TI en los acuerdos de auditoría, más aún cuando el profesional contable no cuenta con el nivel de conocimientos adecuados.

Los factores que pueden propiciar dicha intervención comprenden: la complejidad de los sistemas; el uso de tecnologías emergentes; la significatividad de la evidencia de auditoría que solo esté disponible en formato electrónico; la existencia de conexiones remotas al sistema y el acceso simultáneo de usuarios a las aplicaciones y bases de datos, lo que incrementa el riesgo de integridad de la información de la entidad, entre otros (Astiz y Sole, 2008; Presa, 2013).

La participación de los especialistas puede ser útil en diversos aspectos, como la obtención de un conocimiento adecuado de los sistemas contable y de control interno afectados por el entorno informatizado (incluyendo la TI, los datos e información y los sistemas de comunicación) (Hunton *et al.*, 2004b); la determinación del efecto del entorno informatizado en la evaluación del riesgo global y el riesgo a nivel de saldos y de tipos de transacciones; la realización de pruebas de controles, el diseño y aplicación de procedimientos sustantivos; el uso de TAAC para la extracción y análisis de datos, asociado a la reunión de evidencias y la realización de pruebas para ciertos objetivos de auditoría; la realización de recomendaciones a la gerencia, en la medida en que el auditor de TI podría detectar fallas en controles que valiera la pena informar para que sean subsanadas (Hunton *et al.*, 2004a; Minguillón, 2006). Para la evaluación, los auditores de TI realizan un estudio detenido de documentación relevante, entrevistas, así como el ingreso y manipulación de los datos contenidos en las computadoras (Hunton *et al.*, 2004b).

La intervención de los expertos puede darse al menos de tres modos: 1) que sean incorporados en el equipo de auditoría; 2) que sean contratados por el auditor a efectos de que emitan un informe independiente sobre alguna materia específica que luego será tenido en cuenta en el examen profesional,

siendo de aplicación la NIA 620; 3) en casos de uso de organizaciones de servicio de TI por parte del ente auditado, el especialista puede ser el tercero independiente que realice la emisión del informe sobre los controles de la organización para uso de terceros.

Aún en estos casos, un mínimo de conocimientos en TI y sistemas de información complejos se exige al auditor para no resignar el liderazgo en el trabajo a realizarse (González, 2004), dado que la responsabilidad por la dirección de la auditoría de estados contables no puede ser delegada (Presa, 2013). El contador debe evaluar si el experto tiene la competencia, la capacidad, la objetividad y la independencia necesarias para sus fines, dependiendo del riesgo involucrado (FACPCE, RT 37) y la labor y los resultados alcanzados por el experto. Los conocimientos obtenidos le permitirán, por ejemplo, lograr una mayor comprensión de cuáles son los controles del sistema que el auditor de TI ha testeado (o no), así como responder a las deficiencias en las competencias de los auditores de TI expandiendo el alcance de las pruebas sustantivas para incluir sus propios tests del sistema, compensando dichas debilidades (Brazel, 2008). Brazel y Agoglia (2007) estudian mediante un experimento como se dan las relaciones entre auditores financieros y de TI, indicando que éstas se ven influenciadas por la pericia del auditor de TI tanto como por el nivel de pericia en sistemas de información complejos del auditor financiero.

Rumitti y Falvella (2013) consideran que la realización de auditorías en entornos de la nube necesariamente requerirá de equipos de trabajo multidisciplinarios —proponiéndose la inclusión de especialistas en sistemas por sus competencias en seguridad lógica y aspectos funcionales de los servicios contratados, así como de asesores legales especializados en derecho informático y derecho internacional privado—. Sin embargo aclaran que la coordinación de la auditoría continúa siendo competencia del contador público, por su incumbencia en auditoría y su formación específica en sistemas de información, que trasciende lo técnico e incluye los aspectos legales.

5. CONSIDERACIONES FINALES Y RETOS E INVESTIGACIÓN

La computación en la nube está siendo adoptada paulatinamente en diversos aspectos de la actividad empresarial. Académicamente es incipiente la investigación desde la perspectiva organizacional y escasa desde la auditoría financiera, contando con algunos trabajos que plantean interrogantes más que respuestas. Ello representa una oportunidad para fortalecer los conocimientos en esta área y brindar bases para la elaboración de normas y recomendaciones que sirvan de guía para los profesionales al momento de ejecutar encargos de auditoría en la nube.

El presente trabajo pretende contribuir a la literatura existente brindando un marco teórico para la realización de futuras investigaciones en el área de la auditoría financiera en entornos de TI y el uso de organizaciones de servicio por el ente auditado, dando respuestas a la demanda de mayores estudios sobre el efecto de tecnologías emergentes sobre la auditoría.

En su mayoría los trabajos sobre computación en la nube y auditoría financiera en entornos de TI poseen un enfoque técnico o conceptual. La realización de estudios empíricos, basados en la experiencia y conocimiento de profesionales así como en el estudio de casos, podría ayudar a identificar nuevos aspectos de la auditoría que requieran ser investigados y a capitalizar el conocimiento adquirido en el ejercicio profesional de encargos ejecutados en estos entornos.

Importantes avances se requieren en relación a la etapa de planificación del encargo. Respecto del conocimiento del cliente, a fin de lograr una adecuada comprensión del sistema de información basado en la nube, sería interesante identificar los tipos de servicio en la nube y los aspectos particulares que deberían ser indagados por el profesional en relación al uso de la organización de servicios. La consideración del tipo de industria que hace uso del servicio (de acuerdo al nivel de regulación vigente, tamaño de usuario, etc.) son factores que también debieran ser considerados.

Por otra parte, investigaciones futuras debieran orientarse a examinar los factores de riesgo significativos para la auditoría financiera que introduce el uso de la CN por el ente auditado, basándose en las categorías definidas por la literatura existente. Ello considerando que no todos los riesgos derivados

del uso de la nube —descriptos en los antecedentes desde la perspectiva del usuario del servicio— son relevantes para la auditoría financiera.

En consecuencia, serán necesarios estudios que indaguen acerca de los controles claves para el auditor en este tipo de entornos. El surgimiento de nuevos estándares de control interno podría requerir una ampliación o modificación de los controles a ser considerados. Teniendo en cuenta las dificultades que podría introducir la CN, debiera evaluarse la adecuación de las técnicas previstas en la normativa para la identificación, comprensión y evaluación de los controles de la organización de servicios así como el nivel de satisfacción que los informes de auditores independientes previstos pueden brindar al auditor externo.

Resulta importante indagar el efecto del uso de la CN sobre las características de las evidencias digitales. En relación al proceso de obtención, debería considerarse la aplicabilidad y eficiencia de las herramientas y técnicas de auditoría vigentes. Por otra parte se debieran considerar las restricciones a la auditabilidad y evaluación de controles que podría suponer el entorno, afectando la evaluación de la confianza que puede depositar el profesional en la información procedente de los sistemas informáticos de terceros.

Estudios futuros basados en información de encargos de auditoría ejecutados en ambientes de CN permitirían determinar en qué medida los estados contables de los usuarios son más propensos a tener errores materiales o evidencias de fraudes y la naturaleza y alcance de dichos errores, así como las causas de los mismos, a fin de establecer si efectivamente el uso de la CN genera un potencial de error en la información.

Finalmente, se podría inferir que quiénes cuentan con las capacidades y conocimientos para afrontar estos desafíos y liderar los trabajos de auditoría en la nube son los contadores públicos. Resulta importante identificar el nivel de conocimiento actual así como las capacidades específicas que debieran poseer para el desarrollo de encargos en estos ambientes de TI y otros igualmente complejos, con el fin de garantizar que son capaces de conducir los encargos en forma responsable y utilizar de manera diligente el trabajo realizado por especialistas.

Frente a la necesidad de un trabajo multidisciplinario en un entorno de CN, donde el contador público profesional seguramente necesitará de la colaboración de los auditores informáticos, resulta interesante indagar la forma en que ambos profesionales colaboran entre sí en entornos más sencillos, distinguiendo entre grandes y pequeños estudios de auditoría, a fin de evaluar si se encuentran preparados para trabajar en estos ambientes más complejos y definir los roles y responsabilidades de cada uno de ellos.

6. BIBLIOGRAFÍA

Alali, F. y Yeh, C. (2012). "Cloud Computing: Overview and Risk Analysis". *Journal of Information Systems,* vol. *26*, n° 2, págs. 13-33.

American Institute of Certified Public Accountants (AICPA). *Statement on Auditing Standards.* Consultado el 10/04/2014. Disponible en http://www.aicpa.org/research/standards/auditattest/pages/sas.aspx.

American Institute of Certified Public Accountants (AICPA). *Statements on Standards for Attestation Engagements.* Consultado el 10/04/2014. Disponible en: http://www.aicpa.org/research/standards/auditattest/pages/ssae.aspx.

American Institute of Certified Public Accountants (AICPA) (s.f.). *Top 11 Tips for CPAs Engaging in a Service Organization Control (SOC) Reporting Project.* Consultado el 25/10/2013. Disponible en www.aicpa.org/IMTA.

Arens, A. A.; Elder, R. J. y Beasley, M. S. (2007). *Auditoría. Un enfoque Integral.* Aída Gabriela Valladares Franyuti (traductora). 11° edición. Mexico: Pearson Education.

Armbrust, M.; Fox, A.; Griffith, R.; Joseph, A. D.; Katz, R.; Konwinski, A.; Lee, G.; Patterson, D.; Rabkin, A.; Stoica, I. y Zaharia, M. (2010). "A view of cloud computing", *Communications of the ACM*, vol. *53*, n° 4, págs. 50-58.

Astiz F., F. J. y Sole B., M. (2008). "La auditoría de cuentas anuales en entornos informatizados", *Partida Doble*, n° 202, págs. 70-81.

Beal, V. (2013). *5 Top Picks for Small Business Cloud-Based Accounting*. Consultado el 19/08/2014. Disponible en: http://www.cio.com/article/2388062/small-business/5-top-picks-for-small-business-cloud-based-accounting.html.

Bell, T.; Marrs, F. O.; Solomon I. y Thomas H. (1997). "Auditando organizaciones mediante una perspectiva estratégica de sistemas", en: Bell, T.; Peecher, M. E.; Solomon, I.; Marrs, F. O. y Thomas, H. (2007). *Auditoría basada en riesgos. Perspectiva estratégica de sistemas.* Trad. Samuel A. Mantilla Blanco. Bogotá: Ecoe Ediciones.

Bierstaker, J.; Chen, L.; Christ, M.; Ege, M. y Mintchik, N. (2013). "Obtaining Assurance for Financial Statement Audits and Control Audits When Aspects of the Financial Reporting Process Are Outsourced", *AUDITING: A Journal of Practice & Theory*, vol. *32*, n° 1, págs. 209-250.

Blaskovich, J. y Mintchick, N. (2011). "Information Technology Outsourcing: A taxonomy of prior studies and direction for future research", *Journal of Information Systems*, vol. *25*, n° 1, págs. 1-36.

Böhm, M.; Leimeister, S.; Riedl, C. y Krcmar, H. (2011). "Cloud Computing – Outsourcing 2.0 or a new Business Model for IT Provisioning?", en: Keuper, F.; Oecking, C. y Degenhardt, A. (editores), *Application Management. Challenges - Service Creation - Strategies* (2011), Alemania: Gabler.

Brazel, J. F. (2008). "How do financial statement auditors and IT auditors work together?", *The CPA Journal,* vol. *78* n° 11, págs. 38-41.

Brazel, J. F. y Agoglia, C. P. (2007). "An examination of auditor planning judgements in a complex accounting information system environment", *Contemporary Accounting Research,* vol. *24* n° 4, págs. 1059-1083.

Buyya, R.; Yeo, C. S.; Venugopal, S.; Broberg, J. y Brandic, I. (2009). "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility", *Future generation computer systems,* vol. *25* n° 6, págs. 599-616.

Caldana, D.; Correa, R. y Ponce, H. (2007). "Competencias de los auditores gubernamentales chilenos para la obtención de evidencia electrónica de auditoría", *Revista Contaduría y Administración,* n° 223, págs. 9-31.

Casal, A. M. (2009). *Tratado de Informes de Auditoría, revisión, otros aseguramientos y servicios relacionados.* 1° edición. Buenos Aires: Errepar.

Casal, A. M. (2010). *Gobierno Corporativo: dirección, administración y control de organizaciones de forma ética y responsables*. 1° edición. Buenos Aires: Errepar.

Casal, A. M. (2011). "La identificación y valoración de los riesgos en la auditoría de estados financieros", *D&G Profesional y Empresaria*, vol. *XII*, n° 140, págs. 539-550.

Casal, A. M. (2013). "La auditoría basada en riesgos y las nuevas normas de la Resolución Técnica (FACPCE) 37", *D&G Profesional y Empresaria*, vol. XIV, n° 168, págs. 955-978.

Cerullo, M. J. y Cerullo, M. V. (1997). "Conducting a financial audit in an automated environment", *Computer Audit Update,* vol. *1997*, n° 9, págs. 8-16.

Chow, R.; Golle, P.; Jakobsson, M.; Shi, E.; Staddon, J.; Masuoka, R. y Molina, J. (2009). C*ontrolling data in the cloud: outsourcing computation without outsourcing control*, Proceedings of the 2009 ACM workshop on Cloud computing security, ACM, New York Disponible en http://markus-jakobsson.com/papers/jakobsson-ccsw09.pdf.

Cloud Security Alliance (2011). *Cloud Compliance Report – Capítulo Español de Cloud Security Alliance - Version 1.0*. Consultado el 29/11/2012. Disponible en http://www.consejotransparencia.cl/consejo/site/artic/20110614/asocfile/20110614163116/des144_cloud_compliance_report_csa_es_v_1_0_1.pdf.

Cloud Security Alliance (2013a). *The Notorious Nine: Cloud Computing Top Threats in 2013*. Consultado el 25/10/2013. Disponible en: https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf.

Cloud Security Alliance (2013b). *CSA position paper on AICPA Service Organization Control Reports.* Consultado el 08/08/2013. Disponible en https://cloudsecurityalliance.org/download/csa-position-paper-on-aicpa-service-organization-control-reports.

Committee of Sponsoring Organizations of the Treadway Commission (2012). *Enterprise Risk Management for Cloud Computing*. Consultado el 4/12/2012. Disponible en http://www.coso.org/documents/Cloud%20Computing%20Thought%20Paper.pdf.

European Network and Information Security Agency (2009). *Cloud Computing - Benefits, risks and recommendations for information security*. Consultado el 20/01/2010. Disponible en: http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment.

Federación Argentina de Consejos Profesionales en Ciencias Económicas. *Resoluciones Técnicas.* Consultado el 15/02/2014. Disponible en: http://www.facpce.org.ar:8080/infopro/categorias.php?categoria=3.

Fowler Newton, E. (2004). *Tratado de Auditoría.* 3era. edición. Buenos Aires: La Ley.

González, I. J. (2004). "La auditoría de cuentas en entornos informatizados: Norma Técnica de Auditoría", *Partida Doble*, n° 156, págs. 48-53.

Hayes, B. (2008). "Cloud Computing", *Communications of the ACM,* vol. *51*, n° 7, págs. 9-11.

Hunton, J. E.; Bryant, S. M. y Bagranoff, N. A. (2004a). *Core concepts of Information Technology Auditing*. Estados Unidos: John Wiley and Sons Inc.

Hunton, J. E.; Wright, A. M. y Wright, S. (2004b). "Are Financial Auditors Overconfident in Their Ability to Assess Risks Associated with Enterprise Resource Planning Systems?", *Journal of Information Systems*, vol. *18* n° 2, págs. 7-28.

INFOBAE (01/08/2012). *Advierten a clientes por ataque a Dropbox*. Consultado el 25/06/2014. Disponible en: http://www.infobae.com/2012/08/01/662244-advierten-clientes-ataque-dropbox.

International Federation of Accountants (IFAC). "Normas Internacionales de Auditoría", en Consejo Profesional de Ciencias Económicas de la Cuidad Autónoma de Buenos Aires (traductor) (2009), *Normas Internacionales de Auditoría*. Federación Argentina de Consejos Profesionales en Ciencias Económicas, 1ra edición. Buenos Aires.

International Federation of Accountants (IFAC) (2011). *International Standard on Assurance Engagements (ISAE) 3402 – Assurance Reports on Controls at a Service Organization.* Consultado el 15/02/2014. Disponible en: http://www.ifac.org/sites/default/files/downloads/b014-2010-iaasb-handbook-isae-3402.pdf.

International Federation of Accountants (IFAC) (2013). *International Standard on Assurance Engagements (ISAE) (Revised) - Assurance Engagements Other than Audits or Reviews of Historical Financial Information.* Consultado el 15/02/2014. Disponible en: https://www.ifac.org/sites/default/files/publications/files/ISAE%203000%20Revised%20-%20for%20IAASB.pdf.

Information Systems Audit and Control Association (ISACA) (2009). *Cloud computing – Business Benefits with security, governance and assurance perspectives.* Consultado el 19/01/2010. Disponible en: http://www.isaca.org/Knowledge-Center/Research/Documents/Cloud-Computing-28Oct09-Research.pdf.

Information Systems Audit and Control Association (ISACA) (2011). *IT control objectives for Cloud Computing.* Consultado el 25/06/2014. Disponible en: http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/IT-Control-Objectives-for-Cloud-Computing-Controls-and-Assurance-in-the-Cloud.aspx.

Information Systems Audit and Control Association (ISACA) (2012). *Principios rectores para la adopción y el uso de la computación en nube.* Consultado el 13/06/2012. Disponible en http://www.isaca-bogota.org/Documentos/Cloud-Computing.pdf.

KPMG (2012). *Effectively using SOC1, SOC 2, and SOC 3 reports for increased assurance over outsourced operations.* Consultado el 08/08/2013. Disponible en:http://www.kpmg.com/US/en/IssuesAndInsights/Articles Publications/Documents/SOCWhitepaper.pdf.

Kumar, S. y Goudar, R. (2012). "Cloud Computing – Research Issues, Challenges, Architecture, Platforms and Applicatios: A Survey". *International Journal of Future Computer and Communications*, vol. *1*, n° 4, págs. 356-360.

Kuranda, S. (2014). *The 10 Biggest Cloud Outages Of 2013*. Consultado el 25/06/2014. Disponible en: http://www.crn.com/slide-shows/cloud/240165024/the-10-biggest-cloud-outages-of-2013.htm.

Jansen, W. y Grance, T. (2011). *Guidelines on Security and Privacy in Public Cloud Computing. NIST SP 800-144.* Consultado el 02/08/2012. Disponible en http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf.

Joint, A.; Baker, E. y Eccles, E. (2009). "Hey, you, get off of that cloud?", *Computer Law and security review*, vol. *25*, n° 3, págs. 270-274.

Liu, F.; Tong, J.; Mao, J.; Bohn, R.; Messina, J.; Barger, L. y Leaf, D. (2011). *NIST Cloud Computing Reference Architecture. NIST SP 500-292.* Consultado el 06/08/2013. Disponible en http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909505.

Mansfield, D. S. (2008). "Danger in the clouds", *Network security,* vol. *2008*, n° 12, págs. 9-11.

Mell, P. y Grance, T. (2011). *The NIST Definition of Cloud Computing. NIST SP800-145.* Consultado el 02/08/2012. Disponible en http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

Minguillón R., A. (2006). "La fiscalización en entornos informatizados", *Auditoría pública,* n° 40, págs. 117-128.

Minguillón R., A. (2010). "La revisión de controles generales en un entorno informatizado", *Auditoría Pública,* n° 52, págs. 125-136.

Mohamed, A. (2009). "A history of cloud computing", *Computer Weekly*. Consultado el 15/08/2014. Disponible en: http://www.computerweekly.com/feature/A-history-of-cloud-computing.

Mowbray, M. (2009). "The Fog over the Grimpen Mire: Cloud Computing and the Law", *Scripted Journal of Law, Technology and Society,* vol. *6*, n° 1, págs. 132-146.

Nannini, M. S.; Español, G.; González, S.; Giménez, M.; Puyó, V.; Padovan, A.; Stefanon, G. y Villani, S. (2011). *El enfoque de riesgo en la auditoría*, Anales de las 16° Jornadas de Investigaciones en la Facultad de Ciencias Económicas y Estadísticas, Universidad Nacional de Rosario. Rosario, Argentina.

Nicolaou, C. A.; Nicolaou, A. I. y Nicolaou, G. D. (2012). "Auditing in the cloud: Challenges and opportunities", *The CPA Journal,* vol. *82*, n° 1, págs. 66-70.

Oggero, P. B. (2006). *Riesgos de auditoría y su relación con el trabajo del auditor externo de estados contables en un ambiente de tecnología informática*, Anales del 16° Congreso Nacional de Profesionales en Ciencias Económicas, Rosario, Argentina.

Oracle (2014). Consultado el 19/08/2014. Disponible en: https://www.oracle.com/applications/enterprise-resource-planning/erp-cloud-midsize-companies.html.

Pastor C., C. A. (2011). "Responsabilidad del contador público en la evaluación continua de las TIC en empresas con contabilidad on-line", *Quipukamayoc,* vol. *19*, n° 36, págs. 185-194.

Presa, R. (2013). *Cuaderno Profesional Nro. 65: Efectos de la Tecnología de Información sobre el control interno.* Consejo Profesional de Ciencias Económicas de la Ciudad Autónoma de Buenos Aires, Buenos Aires.

Rumitti, C. y Falvella, M. (2013). "La Nube – Mitos y Realidades2, en: Slosse, Carlos (compilador) (2013), *Contabilidad IV. Auditoría.* (E-book). La Plata: Edulp.

SAP (2014). Consultado el 19/08/2014. Disponible en: http://www.sap.com/latinamerica/pc/tech/cloud/software/cloud-applications/enterprise-suite.html.

Scutella, J. y Barg, V. (2010). *Riesgos de uso de ambientes computarizados*, Anales del 18° Congreso Nacional del Profesionales en Ciencias Económicas, Buenos Aires, Argentina.

Slosse, C. A.; Gordicz, J. C. y Gamondés, S. F. (2007). *Auditoría.* Buenos Aires: La Ley.

Svantesson, D. y Clarke, R. (2010). "Privacy and consumer risks in cloud computing", *Computer law and security review*, vol. *26*, n° 4, pp. 391-397.

Taylor, M.; Haggerty, J.; Gresty, D. y Hegarty, R. (2010). "Digital evidence in cloud computing systems", *Computer law & security review,* vol. *26*, n° 3, págs. 304-308.

Taylor, M., Haggerty, J., Gresty, D. y Lamb, D. (2011). "Forensic investigation of cloud computing systems". *Network Security,* vol. 2011, n° *3*, págs. 4-10.

Valencia D., F. J. y Tamayo A., J. A. (2012). "Evidencia digital y técnicas de auditoría asistidas por computador", *Ventana Informática*, n° *26*, págs. 93-110.

Vaquero, L. M.; Rodero M., L.; Caceres, J. y Lindner, M. (2009). "A break in the clouds: towards a cloud definition", *ACM Sigcomm Computer Communication Review,* vol. *39*, n° 1, págs. 50-55.

Yigitbasioglu, O.; Mackenzie, K. y Low, R. (2013). "Cloud Computing: How does it differ from IT outsourcing and what are the implications for practice and research?", *The International Journal of Digital Accounting Research*, vol. *13*, págs. 99-121.

Zhang, Q.; Cheng, L. y Boutaba, R. (2010). "Cloud computing: state-of-the-art and research challenges", *Journal of Internet Services and Applications,* n° *1*, págs. 7–18.