López, María de los Ángeles; Albanese, Diana

RIESGOS DERIVADOS DEL USO DE LA COMPUTACIÓN EN LA NUBE QUE IMPACTAN EN LA AUDITORÍA DE ESTADOS FINANCIEROS

Audit.ar

2021, vol. 1, no. 1, pp. 1-8

López, M.A., Albanese, D. (2021). Riesgos derivados del uso de la computación en la nube que impactan en la auditoría de estados financieros. Audit.ar. En RIDCA. Disponible en: https://repositoriodigital.uns.edu.ar/handle/123456789/5640

VOL. 1, NRO. 1
MAYO - OCTUBRE 2021

ISSN 2718-8647

AUDIT.AR
REVISTA DE AUDITORÍA

ARTÍCULO DE INVESTIGACIÓN

RIESGOS DERIVADOS DEL USO DE LA COMPUTACIÓN EN LA NUBE QUE IMPACTAN EN LA AUDITORÍA DE ESTADOS FINANCIEROS

RISKS ARISING FROM THE USE OF CLOUD COMPUTING THAT IMPACT FINANCIAL STATEMENT AUDITS

María de los Ángeles López
Profesora adjunta de Auditoría, Departamento de Ciencias de la Administración, Universidad Nacional del Sur. Argentina.
angeles.lopez@uns.edu.ar

Diana Albanese
Profesora Titular de Auditoría, Departamento de Ciencias de la Administración, Universidad Nacional del Sur. Argentina.
dalbanese@uns.edu.ar

RESUMEN

En los ultimos años el uso de la Computación en la Nube (CN) ha tenido un fuerte crecimiento en procesos de organizaciones públicas y privadas, con una mayor expansión debido a la implementación de la administración electrónica a causa de la pandemia provocada por el covid-19. Ello ha incrementado la importancia de esta tecnología para el desarrollo de las auditorías financieras, particularmente en la etapa de evaluación de riesgos. El objetivo de este trabajo consiste en analizar los riesgos de la CN vinculados a procesos que deben ser evaluados por los auditores, en la medida en que tienen impacto en la información financiera objeto de su examen. Se pretende identificar aquellos con mayor relevancia, tanto por su probabilidad de ocurrencia como por su potencial impacto. A través del análisis bibliográfico como técnica de recolección de datos, se propone una clasificación y descripcion de diversos factores de riesgo. Del análisis surge que este ambiente de tecnología de información (TI) no necesariamente es mas riesgoso que otros, y que los riesgos mas significativos para el auditor son los relacionados con la seguridad de la información, el control interno y los legales.

ABSTRACT

The use of cloud computing (CC) has grown considerably over the last years in processes carried out by public and private organizations, and has been promoted especially due to the implementation of electronic management systems driven by the Covid-19 pandemic. This expansion has increased the importance of this technology for developing financial audits, particularly for risk assessment. The purpose of this study is to analyse the risks of cloud computing linked to processes that must be assessed by the auditors, to the extent that these risks impact the financial information under examination. This work aims to identify the most relevant risks, due not only to their occurrence probability but also to their potential impact. A classification and description of several risk factors are proposed through a bibliographic research as a data collection technique. From the analysis, it arises that this IT environment is not necessarily more risky than others, and that the most significant risks for auditors are those related to information security, internal control and legal matters.

PALABRAS CLAVE
auditoría de estados financieros, computación en la nube, riesgos.

KEYWORDS
financial statement audit, cloud computing, risks.

RIESGOS DERIVADOS DEL USO DE LA COMPUTACIÓN EN LA NUBE QUE IMPACTAN EN LA AUDITORÍA DE ESTADOS FINANCIEROS

AUTORAS:
María de los Ángeles López
Diana Albanese

RECIBIDO:
12 de diciembre, 2020

APROBADO:
15 de abril, 2021

AUDITAR
PRIMERA REVISTA ARGENTINA EXCLUSIVA SOBRE AUDITORÍA

DOI: https://doi.org/10.24215/27188647e001
CÓDIGO JEL: M42
ISSN: 2718-8647
http://revistas.unlp.edu.ar/auditar

ENTIDAD EDITORA:
Instituto de Investigaciones y Estudios Contables, Facultad de Ciencias Económicas, Universidad Nacional de La Plata

INTRODUCCIÓN

La computación en la nube (CN) o *cloud computing* es una forma de provisión de servicios tecnológicos cuya utilización por parte de las organizaciones ha ido creciendo sistemáticamente; su expansión se aceleró con la implementación de la administración electrónica. Actualmente, la crisis provocada por el covid-19 en el mundo ha incrementado la externalización de sistemas de información (Minguillón y Pinar, 2020).

Si bien esta tecnología ha traído beneficios a los usuarios, se generaron nuevos riesgos y se intensificaron otros preexistentes (Yau-Yeung et al., 2020). La bibliografía referida a las nuevas tecnologías en general analiza los factores de riesgos que las organizaciones deben considerar al momento de decidir su implementación. A su vez, el auditor de estados financieros (en adelante el auditor) debe adaptarse al nuevo escenario al momento de evaluar los riesgos del negocio y riesgos de los procesos. Tal es así que los Órganos de Control Externos Autonómicos (OCEX) de España aprobaron en mayo de 2020 las Consideraciones de auditoría relativas a la utilización de una organización de servicios proveedora de CN (Minguillón y Pinar, 2020). En consecuencia, el objetivo del presente trabajo consiste en analizar los riesgos vinculados a la CN que el auditor debe evaluar al momento de planificar un encargo.

El trabajo se estructura de la siguiente manera: en primer lugar se describe la importancia de la tecnología de la información (TI) en el modelo de auditoría basada en riesgos; a continuación se introduce el concepto de CN y se realiza un analisis de los factores de riesgo vinculados describiendo su importancia para la auditoría; finalmente se presentan las consideraciones finales.

LA AUDITORÍA BASADA EN RIESGOS Y LA TECNOLOGÍA DE INFORMACIÓN

En el modelo de Auditoría Basada en Riesgos (ABR), a partir del conocimiento del cliente, el auditor toma conocimiento de los riesgos del negocio, que comprenden aquellos eventos negativos que podrían dificultar la ejecución de procesos y la consecución de los objetivos de la organización. Entre ellos, el contador debe evaluar aquellos riesgos que resultan ser significativos, definidos por la NIA 315 (Revisada), como aquellos riesgos de incorrección material que, a juicio del auditor, requieren una consideración especial en la auditoría.

Esos riesgos deben ser evaluados en dos niveles: riesgos de declaración equivocada material a nivel de estados financieros y a nivel de afirmaciones correspondientes a transacciones, saldos contables e información a revelar (Casal, 2013; NIA 315 (Revisada), A.25). El riesgo de auditoría se refiere al riesgo de emitir una opinión equivocada, y comprende cuatro categorías, identificadas por Arens et al. (2007, p. 241) como riesgo inherente, riesgo de control, riesgo planeado de detección y riesgo aceptable de auditoría.

La tecnología de la información es un factor relevante al momento de evaluar los riesgos inherentes y de control, debido a que pueden surgir amenazas propias de estos entornos, tales como ausencia de pistas de transacciones, falta de segregación de funciones o la generación automática de transacciones y registraciones (Minguillón, 2006).

La NIA 315 (Revisada) (A. A40, A64, Anexo 2) identifica un conjunto de riesgos específicos derivados de la informática que pueden afectar el control interno, como errores en el procesamiento de datos, accesos y cambios no autorizados en los datos, los archivos maestros o los programas; pérdida potencial de datos o incapacidad de acceder a ellos del modo requerido, entre otros. La presencia de algunos de ellos podría derivar en incorrecciones significativas en los estados financieros.

Por su parte, Presa (2013) propone factores que agravan cada uno de los riesgos vinculados al uso de la tecnología, mientras que Casal (2013) y Minguillón y Pinar (2020) resaltan que el riesgo de auditoría aumenta en la medida en que el entorno informatizado se vuelve más complejo.

Fronti de García y Suárez Kimura (2008) resumen tres grupos de riesgos asociados a la TI: a) *riesgos de infraestructura de* tecnología, relacionados con la seguridad de la información; b) *riesgos de las aplicaciones*; c) *riesgos vinculados con los procesos de negocio*. El auditor deberá considerarlos, evaluando la significatividad de deficiencias de control y sus consecuencias patrimoniales.

Los entornos tecnológicos actualmente son muy variados. A continuación, se presenta un análisis de riesgos relevantes para el auditor vinculados a uno en particular: la computación en la nube.

RIESGOS DE LA COMPUTACIÓN EN LA NUBE

> Según *The National Institute of Standards and Technology* (NIST), se entiende por computación en la nube a 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. (Mell y Grance, 2011, p. 2)
>
> Este modelo de distribución de software (Saas), plataformas (Paas) o infraestructuras (Iaas) como servicios posee características esenciales, que incluyen: autoservicio a solicitud del usuario; acceso a través de una red; rápida escalabilidad; recursos computacionales compartidos por diferentes usuarios; forma de medición del uso de los servicios (Mell y Grance, 2011).

En distintos estudios se encuentran descripciones de los riesgos potenciales de la CN desde el punto de vista del usuario, según se describen mas adelante. El propósito es evaluarlos a efectos de garantizar resultados satisfactorios derivados de su uso y la sostenibilidad en el tiempo (Islam et al., 2017). Incluso *The Committee of Sponsoring Organization* (COSO, 2012) ha elaborado un conjunto de pautas para identificar los riesgos que conlleva el uso de la CN y evaluar su impacto en las organizaciones, colaborando con la gestion de los ejecutivos.

Sin embargo, los estudios relacionados a la auditoría financiera en entornos de CN son escasos. En López (2017), se realiza un análisis de las particularidades de diversas etapas del proceso de la auditoría financiera cuando ésta es desarrollada en estos ambientes de TI, mediante un estudio exploratorio con un enfoque cualitativo basado en entrevistas a auditores financieros y de sistemas de los grandes estudios de Argentina.

Se considera que algunos riesgos podrían tener un fuerte impacto sobre la auditoría, pudiendo llegar a imposibilitar la ejecución del encargo; al respecto, Yigitbasioglu et al. (2013) reconocen que en los casos en que los datos financieros y contables se encuentran almacenados en la nube, los riesgos de seguridad son relevantes. En otros casos, se trata de riesgos posibles pero con probabilidades de ocurrencia baja o impacto cercano a cero para la auditoría externa. Aun así, no existe acuerdo acerca de si una auditoría ejecutada en un ambiente de CN es necesariamente mas riesgosa que aquella realizada en un entorno de TI tradicional.

A continuación se amplía la descripción de categorías de riesgos vinculadas al uso de la CN y su relevancia para la auditoría de estados financieros.

RIESGOS DERIVADOS DEL PROCESO DE IMPLEMENTACIÓN DE LA NUBE

Se incluye en esta categoría los riesgos por falta de planificación del proceso de implementación. Citando a Svantesson y Clarke (2010, p. 395), puede suceder que los sistemas de información y tecnologías contratados no respondan a las necesidades de la organización o no se alinen con sus planes estratégicos, derivando en niveles de riesgos desconocidos. Otra situación de riesgo podría ser que algunos integrantes del ente contraten y utilicen servicios en la nube sin solicitar autorización a superiores o para actividades no autorizadas, evitando procedimientos tradicionales de revisión y aprobación (COSO, 2012, p. 13), o que se produzcan fallas en la adecuación de la estructura organizacional para la implementación de CN, resultando en el fracaso de la implementación del servicio (Brender y Markov, 2013; COSO, 2012, p. 5). Es altamente probable que en una auditoría de estados financieros el contador requiera la intervención de un auditor de sistemas para evaluar este tipo de riesgos.

En López (2017) se analiza esta categoría de riesgos, y se obtienen un conjunto de conclusiones al respecto, según se

describe a continuación.

Por un lado, se encuentra que la falta de planificación por parte del auditado posee una baja probabilidad de ocurrencia en empresas grandes; es de esperar que los administradores solo migren a la nube una vez que estén convencidos respecto de la seguridad y se hayan cumplido los correspondientes procesos de implementación de TI. Sin embargo, la falta de planificación y un proceso de implementación inadecuado representarían deficiencias de control con efecto en la definición del enfoque de auditoría.

Respecto del riesgo de uso no autorizado de la nube, se debe analizar el efecto sobre el circuito contable. Resulta improbable que un sistema de gestión completo, que genera y procesa hechos y operaciones que deben ser registrados en el sistema contable, fuera implementado en la nube sin autorizacion previa. Por otro lado, el resguardo de información en la nube sin autorización –sea con una intención maliciosa o no– no tendría efecto sobre las transacciones. En definitiva, este riesgo pareciera no tener alta probabilidad o alto impacto a los fines de la auditoría financiera (López, 2017).

Para prevenir este tipo de riesgos, es importante la intervención del auditor –de sistemas o financiero– en todo el proceso de evaluación, selección e implementación de la CN para garantizar que se cumplan todas sus etapas y que se analicen no solo aspectos funcionales al desarrollo del negocio del ente, sino también al control interno y la auditoría; cabe aclarar que, si bien esta es una situación deseable, no siempre ocurre en la realidad (López, 2017).

RIESGOS PROPIOS DE LA TERCERIZACIÓN

El modelo de CN se basa en la tercerización de un servicio. Las empresas renuncian a cierto nivel de control que debe verse compensado por la confianza que le merecen los sistemas y los proveedores de la nube y la posibilidad de verificación de los procesos y eventos (López, 2017).

Un riesgo relacionado es la pérdida de gobernabilidad por parte del usuario sobre ciertos procesos, información y partes del sistema, pudiendo verse afectada la seguridad de la información, la calidad y eficiencia de los procesos y el cumplimiento de requisitos y expectativas del usuario respecto de los controles internos (Ali et al., 2015; Brender y Markov, 2013; Caldarelli et al., 2016; COSO, 2012; European Network and Information Security Agency [ENISA], 2009; Jamil y Zaki, 2011).

Otro riesgo derivado del uso de la CN podría ser la falta de transparencia, dado que no es habitual que los proveedores difundan información referida a sus sistemas, controles y medidas de seguridad, generando problemas al usuario a la hora de evaluar el control interno y las prácticas de gestión de datos, al impedir la ejecución de pruebas de confiabilidad, tests sobre controles y monitoreo de actividades (COSO, 2012; ENISA, 2009; Jamil y Zaki, 2011).

Ambos riesgos impactan significativamente sobre la auditoría. Si existe externalización de sistemas y/o procesos, el conocimiento y la evaluación de riesgos y controles se extiende al prestador del servicio, requiriéndose información del tercero involucrado que podría ser obtenida, por ejemplo, de los informes de control interno de las organizaciones de servicios (López, 2017; Minguillón y Pinar, 2020; Rumitti y Gómez, 2019; RT37).

Se incluye tambien el riesgo de *lock-in*, es decir, la dependencia con el proveedor elegido, de modo que resulta complejo poder migrar a otro prestador o retornar al entorno de TI propio. Este riesgo no pareciera afectar al auditor, en la medida en que su preocupación es que la información se encuentre disponible para ser auditada –salvo que implique un riesgo de negocio importante para el auditado (López, 2017)–.

Otros factores de riesgo dentro de esta categoría incluyen que el usuario pierda una certificación obtenida como consecuencia del uso de la CN, la interrupción del servicio por falta de viabilidad del proveedor y la reputación compartida con el prestador. Estos eventos afectan al auditado y deben ser gestionados, pero tampoco parecieran ser relevantes para la auditoría.

RIESGOS TÉCNICOS

Esta categoría comprende los riesgos de continuidad y los riesgos de seguridad.

Los primeros están asociados a la disponibilidad del servicio y la información, el resguardo *(back up)* y las medidas de recuperación ante desastres de un sistema (Hunton et al., 2004, p. 50). Eventuales interrupciones del servicio, sean temporarias o permanentes, originadas en fallas de los sistemas, pueden dificultar el acceso a la información, así como generar errores o problemas en el procesamiento de las transacciones (Brender y Markov, 2013).

Este tipo de riesgo puede originarse, por ejemplo, en las fallas en la conexión a internet y sus vulnerabilidades (ENISA, 2009; Jansen y Grance, 2011, p. 11; Yigitbasioglu, 2015). Según el estudio de López (2017), no es específico de la nube, pero posee alta probabilidad e impacto, considerando las deficiencias de infraestructura en algunas regiones de Argentina. Debe ser gestionado por el usuario, quien es responsable del traslado de la información desde la compañía hasta el proveedor.

Los riesgos de continuidad son relevantes para la auditoría, poseen alta probabilidad de ocurrencia e impacto y deben ser gestionados por el usuario y por el proveedor mediante políticas de *back up* seguras. En la evaluación del control interno será importante analizar las medidas tomadas por el cliente al respecto, de manera de garantizar la integridad de la información y efectuar recomendaciones a la gerencia (López, 2017).

Por su parte, los riesgos de seguridad estan vinculados al acceso a los datos por terceros no autorizados (Hunton et al., 2004, p. 50), comprometiendo la seguridad y privacidad de la información y los sistemas, generando riesgo de pérdida o modificación no autorizada de datos, registro de transacciones no autorizadas, inexistentes o inexactas (Arens et al., 2007; ENISA, 2009; NIA 315 (Revisada) (A. A64)).

En general los factores de riesgo específicos se refieren a empleados maliciosos; fuga o interceptación de datos en tránsito, eliminación de datos insegura o no efectiva (disponibles más allá de los plazos pretendidos por el usuario de acuerdo a sus políticas de seguridad), acceso de la información a través de navegadores de uso generalizado y problemas de gestión de la identidad y claves de encriptado (Ali et al., 2015; Brender y Markov, 2013; COSO, 2012; ENISA, 2009; Jamil y Zaki, 2011).

La elaboración de los estados financieros depende en gran medida de los datos procesados, de modo que los riesgos vinculados a la seguridad poseen alto impacto en la auditoría, debiéndose evaluar las políticas de control implementadas por el cliente y el proveedor del servicio para minimizar estos riesgos. Como medida de prevención debería impedirse cualquier posibilidad de asiento manual, o niveles claros de autorización para realizarlo, mediante la gestión de perfiles, roles y funcionalidad. A su vez son importantes las políticas preventivas que hubiera adoptado el proveedor del servicio en la nube, como *firewalls* adecuados y medidas para la detección inmediata de sujetos que estuvieran intentando ingresar a los sistemas (López,2017).

RIESGOS LEGALES

Referidos al incumplimiento de la normativa aplicable al ente auditado, estos riesgos suelen verse afectados en el caso de cambios en las tecnologías debido al desfase temporal entre la actualización de la normativa y los avances tecnológicos (Suárez Kimura, 2007). Aun cuando un ente tercerice ciertos procesos, es responsable de cumplir las leyes y normas que le son aplicables. Su incumplimiento da lugar a sanciones significativas con impacto en los estados financieros en caso de multas, litigios y otros (NIA 250 (Revisada), A.2, A.3). Estos riesgos son relevantes en los entornos de CN (Yau-Yeung et al., 2020).

Por una parte, deben considerarse los riesgos derivados del marco jurídico del lugar donde está alojada la información (Caldarelli et al., 2016; González y Piccirilli, 2013), que puede ser diferente a la ubicación del ente usuario (nubes transfronterizas) y no siempre conocida por éste. Si bien pareciera ser más relevante para el auditado que para el auditor, podrán mitigarse mediante la negociación de las condiciones de prestación del servicio, intentando definir una ubicación geográfica de la información que sea favorable para el ente (cuando esto fuera posible) y la lectura detallada de los contratos (López, 2017).

Por otro lado, se consideran los riesgos de incumplimiento de la normativa que rige al ente auditado en su locación. Aquí los auditores se focalizan principalmente en las normas

referidas a los sistemas de información contable, analizados también por Suárez Kimura y Escobar (2015), que comprenden en general la obligación de llevar los libros de acuerdo a las exigencias legales y mantener la información en la sede de la compañía que corresponda, según lo establecido por el Código Civil y Comercial de la Nación (CCCN) y la Ley General de Sociedades.

Una de las principales dificultades se relaciona a la obtención de autorización para llevar libros en medios mecánicos (Ley 19.550, art.61) cuando la información contable se transnacionaliza y se desconoce su ubicación al estar alojada fuera de Argentina, debido a que la labor de los entes de contralor se ve obstaculizada. Es posible que se requiera al auditado que identifique la ubicación física de los servidores y la información, a fin de cumplir con sus tareas de revisión, y, si el servidor está localizado en extraña jurisdicción[1], se garantice el acceso a la información, así como también que exista una réplica de la base de datos en la sede social de la compañía (López, 2017).

Otro tema controvertido en entornos de CN, analizado en López (2017), se refiere a la ubicación de los registros contables y la información que les da soporte. Si bien estos deben permanecer en el domicilio del titular (CCCN, art. 325), este requisito podría no ser cumplido en el caso del uso de la CN, considerando que los datos están alojados en la sede del proveedor del servicio. Incluso la ubicación de los datos podría modificarse sin conocimiento del usuario de acuerdo a las necesidades y conveniencia del proveedor. Los usuarios deberán prever soluciones que serán evaluadas por el auditor, tales como realizar copias locales de información alojada en la nube, trayéndola al país para cumplir las disposiciones.

Los riesgos de incumplimiento de normas referidas a la confidencialidad de los datos o la protección de la propiedad intelectual podrían dar lugar a situaciones litigiosas contingentes que deberían afrontar las entidades. Son muy difíciles de evaluar desde el punto de vista de la auditoría, dado que son eventos posibles, pero cuya probabilidad de ocurrencia e impacto contable es muy difícil de estimar *a priori* (López, 2017).

Frente a su ocurrencia, corresponde analizar el grado de responsabilidad atribuible al ente auditado por el incumplimiento de las leyes. Aun si el ente pudiera demostrar que adoptó las medidas de seguridad adecuadas y requeridas por la normativa que le fuera aplicable, y que sufrió un jaqueo o robo de información, es posible que el ente contratante de la nube también sea responsabilizado (López, 2017). En general los auditores financieros evalúan dichos eventos cuando la infracción ya ha ocurrido; la NIA 250 (Revisada) (A.19) postula que si toman conocimiento de un incumplimiento –o habiendo obtenido indicios sobre el mismo–, deberán indagar sobre el hecho en cuestión y el contexto en el que se produjo, evaluándolo junto con cualquier otra información que permita evaluar el posible efecto del mismo sobre los estados financieros.

RIESGOS CONTRA LA SEGURIDAD FÍSICA

Incluye el riesgo de acceso físico no autorizado a instalaciones y edificios y los desastres naturales. Según se describe en López (2017), estos factores de riesgo no son exclusivos de los entornos de CN; sin embargo, deben ser considerados por el usuario y su auditor, teniendo en cuenta la ubicación geográfica de los servidores del proveedor del servicio –en caso de que esta fuera conocida–, su infraestructura y las medidas de seguridad del proveedor y del auditado.

CONSIDERACIONES FINALES

Las organizaciones han obtenido importantes ventajas con el uso de la CN pero también surgieron riesgos relacionados con la seguridad, el control interno y legales que son significativos para el auditor porque impactan potencialmente en la información financiera. Dichos riesgos fueron descriptos a lo largo del presente trabajo.

A modo de conclusión se puede decir que la utilización de la CN por el auditado no necesariamente resulta más riesgosa

[1] Incluyen países de alto riesgo donde los gobiernos pueden aprobar legislación que les permita acceder a todos los datos dentro de sus fronteras (Brender y Markov, 2013) o calificados como países con legislación permisiva.

para el auditor que otros entornos tecnológicos. Los riesgos dependen principalmente del proveedor que se contrate, de las previsiones y recaudos que adopte el cliente al momento de contratar el servicio y de los controles que se implementen.

El mundo post covid-19 trae aparejado una aceleración del uso de la administración electrónica y el uso de la CN se constituye en una herramienta útil para la gestión. Este cambio afecta el trabajo del auditor, quien deberá adaptarse y evaluar nuevos factores de riesgo al momento de planificar su trabajo, a la vez que requerirá de un trabajo multidisciplinario con especialistas en sistemas que colaboren en la tarea de evaluación de riesgos y la aplicación de procedimientos de control.

Frente al permanente avance de la tecnología, resulta conveniente en el futuro realizar este tipo de análisis vinculados a riesgos propios de otros ambientes tecnológicos, aportando tanto al desarrollo de la disciplina como a la labor de los profesionales en el ejercicio de encargos de auditoría en ambientes de TI diversos.

REFERENCIAS

Ali, M., Khan, S. U. y Vasilakos, A. V. (2015). Security in cloud computing: Opportunities and challenges. *Information Sciences, 305*(2015), 357-383.

Arens, A. A., Elder, R. J. y Beasley, M. S. (2007). *Auditoría. Un enfoque Integral.* (11ª ed., Trad. A. G. Valladares Franyuti). Pearson Education.

Brender, N. y Markov, I. (2013). Risk perception and risk management in cloud computing: Results from a case study of Swiss companies. *International Journal of Information Management, 33*(2013), 726-733.

Caldarelli, A., Ferri, L. y Maffei, M. (2016). Expected benefits and perceived risks of cloud computing: an investigation within an Italian setting. *Technology Analysis & Strategic Management.* https://doi.org/10.1080/09537325.2016.1210786

Casal, A. M. (2013). La auditoría basada en riesgos y las nuevas normas de la Resolución Técnica (FACPCE) 37. *Revista Desarrollo y Gestión, XIV*(168), 955-977.

Committee of Sponsoring Organizations of the Treadway Commission (2012). *Enterprise Risk Management for Cloud Computing.* https://www.coso.org/Documents/Cloud-Computing-Thought-Paper.pdf

European Network and Information Security Agency (ENISA) (2009). *Cloud Computing - Benefits, risks and recommendations for information security.* https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment

Federación Argentina de Consejos Profesionales de Ciencias Económicas (2013). Resolución Técnica 37 - *Normas de Auditoría, Revisión, Otros Encargos de Aseguramiento, Certificación y Servicios Relacionados.*

Fronti de García, L. y Suárez Kimura, E.B. (2008). Aportes tecnológicos al Sistema de Control Interno. *Contabilidad y auditoría, 14*(27), 53-73.

González A., J. C. y Piccirilli, D. (2013). Consideraciones Legales Relativas a la Privacidad en Proyectos de Cloud Computing en el Exterior de Argentina. *Revista Latinoamericana de Ingeniería de Software, 2*(1), 77-90.

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

International Federation of Accountants (2013). Norma Internacional de Auditoría 315 (Revisada) – Identificación y valoración de los riesgos de incorrección material mediante el conocimiento de la entidad y su entorno. En IFAC (2018), *Manual de Pronunciamientos Internacionales de Control de Calidad, Auditoría, Revisión, Otros Encargos de Aseguramiento, y Servicios Relacionados, Edición 2018, Volumen I,* (pp.307-367).

International Federation of Accountants (2017). Norma Internacional de Auditoría 250 (Revisada) – Consideración de las disposiciones legales y reglamentarias en la auditoría de estados financieros. En IFAC (2018), *Manual de Pronunciamientos Internacionales de Control de Calidad, Auditoría, Revisión, Otros Encargos de Aseguramiento, y Servicios Relacionados, Edición 2018, Volumen I,* (pp.227-247).

Islam, S., Fenz, S., Weippl, E. y Mouratidis, H. (2017). A Risk Management Framework for Cloud Migration Deci-

sion Support. *Journal of Risk and Financial Management, 10*(2), 10.

Jamil, D. y Zaki, H. (2011). Cloud computing security. *International Journal of Engineering Science and Technology, 3*(4), 3478-3483.

Jansen, W. y Grance, T. (2011). NIST Special Publication 800-144 - *Guidelines on Security and Privacy in Public Cloud Computing.* https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf

Ley Nro. 19550. Ley General de Sociedades. Boletín Oficial, Buenos Aires, 25/04/1972.

Ley Nro. 26.994. Código Civil y Comercial de la Nación. Boletín Oficial, Buenos Aires, 08/10/2014.

López, M. A. (2017). Particularidades de la auditoría financiera cuando la entidad utiliza computación en la nube. Análisis basado en la experiencia de auditores de la República Argentina [Tesis de doctorado]. Universidad Nacional del Sur, Bahía Blanca, Argentina.

Mell, P. y Grance, T. (2011). *NIST Special Publication 800-145 - The Nist Definition of Cloud Computing.* http://faculty.winthrop.edu/domanm/csci411/Handouts/NIST.pdf

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

Minguillón, R. A. y Pinar, L.P. (2020). Auditoría y Gestión de los fondos públicos. *Auditoría pública,* (75), 35-44.

Presa, R. (Coord.) (2013). *Cuaderno Profesional Nro. 65: Efectos de la Tecnología de Información sobre el control interno* (1ª ed.). Consejo Profesional de Ciencias Económicas de la Ciudad Autónoma de Buenos Aires.

Rumitti, C. y Gómez, P. (2019). Organizaciones de servicios... un ¿nuevo? desafío para los contadores. *Enfoques*, 12.

Suárez Kimura, E. B. (2007). Medios digitalizados en el procesamiento de datos contables: repercusión en la actividad del contador público. *Contabilidad y auditoría, 13*(26), 221-251.

Suárez Kimura, E. B. y Escobar, D. S. (2015). *El sistema contable en la nube - Diagnóstico actual y desafíos con la unificación de códigos.* XXXVII Simposio Nacional de práctica profesional. http://www.economicas.uba.ar/wp-content/uploads/2016/06/CECONTA_T2015_149_SUAREZKIMURA_SISTEMA_CONTABLE_NUBE.pdf

Svantesson, D. y Clarke, R. (2010). Privacy and consumer risks in cloud computing. *Computer and security review, 26*(4), 397-397.

Yau-Yeung, D., Yigitbasioglu, O. y Green, P. (2020). Cloud accounting risks and mitigation strategies: evidence from Australia. *Accounting Forum, 44*(4), 421-446. https://doi.org/10.1080/01559982.2020.1783047

Yigitbasioglu, O. M. (2015). External auditors' perceptions of cloud computing adoption in Australia. *International Journal of Accounting Information Systems, 18,* 46-62.

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, 13,* 99-121.