UNIVERSIDAD NACIONAL DEL SUR

TESIS DE DOCTOR EN CIENCIAS DE LA ADMINISTRACIÓN

Particularidades de la auditoría financiera cuando la entidad utiliza computación en la nube.

Análisis basado en la experiencia de auditores de la República Argentina

María de los Ángeles López

BAHÍA BLANCA ARGENTINA

2017

PREFACIO

Esta Tesis se presenta como parte de los requisitos para optar al grado Académico de Doctor en Ciencias de la Administración, de la Universidad Nacional del Sur y no ha sido presentada previamente para la obtención de otro título en esta Universidad u otra. La misma contiene los resultados obtenidos en investigaciones llevadas a cabo en el ámbito del Departamento de Ciencias de la Administración durante el período comprendido entre el 10 de agosto de 2010 y el 19 de junio de 2017, bajo la dirección de la Mg. Regina Durán.

María de los Ángeles López

UNIVERSIDAD NACIONAL DEL SUR
Secretaría de Posgrado y Educación Continua

La presente tesis ha sido aprobada el …./…./….. mereciendo la calificación de ……
(…….)

A Santiago,
y nuestros hijos, Jazmín, Bastian e Iñaki.

AGRADECIMIENTOS

Al Consejo Nacional de Investigaciones Científicas y Técnicas (CONICET) de la República Argentina y al Departamento de Ciencias de la Administración de la Universidad Nacional del Sur, por brindarme esta posibilidad de formarme y desarrollar mi carrera de investigación y docencia.

A quienes me acompañaron y dirigieron en este proceso. Mg. Regina Durán, gracias por tu confianza, por ayudarme a enfocarme en el norte y por las oportunidades que me has brindado. Mg. Diana Albanese, gracias por creer en mí, por tu apoyo y tu dedicación. Gracias por orientarme y motivarme no solo en el trabajo académico, sino también en lo personal.

A todos los profesionales que han participado de la investigación, sea como revisores, entrevistados, intermediados para la obtención de contactos, por su buena voluntad y enorme generosidad en compartir sus experiencias y su tiempo para que este trabajo fuera posible.

A los profesores del Doctorado, por todo lo aprendido, en especial a aquellos que se interesaron y me brindaron su tiempo y recomendaciones para poder avanzar.

A mis compañeros de postgrado, con quienes comencé este camino. En especial Diego Schneider, por compartir tantos trabajos, charlas y recomendaciones, por motivarme tantas veces cuando no era sencillo continuar.

A mis amigos, mis compañeros de cátedra y los becarios, por estar siempre presentes, por su ayuda y por alegrar este camino como tesista.

A mi familia, mis padres y hermanos, por su apoyo y porque con ustedes aprendí a esforzarme para ser mejor y perseguir mis objetivos.

A mamá, porque gracias vos y tu permanente amor, consejos y ayuda esto ha sido posible.

Muy especialmente, a Santiago y nuestros hijos: son la razón por la que culmino el proceso. Gracias por su amor, su paciencia, porque se alegraron con cada logro y compartieron día a día, durante años, los pasos que tuve que dar para llegar. Y principalmente porque son parte del enorme crecimiento personal que representó para mi hacer esta tesis.

Finalmente a Dios, por darme esta oportunidad y acompañarme en cada momento.

RESUMEN

La auditoría financiera se ha visto afectada de manera significativa a partir del uso de la tecnología de la información (TI) para la elaboración y el almacenamiento de la información contable. En particular, el surgimiento de nuevas soluciones como la computación en la nube (CN) representa un desafío para el avance de la disciplina, tanto desde la perspectiva académica como de la práctica profesional.

Esta tesis tiene como objetivo general analizar las particularidades de la auditoría financiera cuando el ente auditado utiliza la computación en la nube en procesos que afectan a la información contable. Se realiza un estudio exploratorio, con un enfoque cualitativo, obteniendo datos mediante entrevistas en profundidad a auditores financieros y de sistemas pertenecientes a los grandes estudios de auditoría de la República Argentina.

En primer lugar, se describe el nivel de utilización de la CN por las empresas argentinas. Si bien se encuentra en un estado incipiente de evaluación e implementación, existen expectativas de crecimiento, incluso en procesos con impacto en los estados financieros. En este marco, la auditoría contable y la de sistemas necesitan adaptarse al nuevo entorno.

A continuación se analizan las particularidades de diversas etapas de la auditoría financiera en el ambiente de TI bajo estudio. En la planificación, el proceso de conocimiento del cliente y su entorno es considerado especialmente importante. Se describen un conjunto de aspectos que el auditor necesitaría conocer a fin de lograr una adecuada comprensión de los sistemas de información del ente y una discusión sobre los procedimientos que se podrían aplicar a dicho efecto, considerando ciertas limitaciones impuestas por la tecnología analizada.

Posteriormente se abordan los diversos factores de riesgo derivados del uso de la CN identificados por la literatura, haciendo énfasis en aquellos con potencial impacto en la auditoría financiera. Luego de su tratamiento, se elabora una *risk breakdown structure*, herramienta útil a los fines de simplificar y sistematizar la evaluación de riesgos en estos encargos.

En relación a la evaluación del sistema de control interno en entornos de CN, se describen controles del usuario y del proveedor del servicio cuyo diseño, implementación y funcionamiento interesan al auditor financiero. A partir del análisis de esta alternativa de tercerización de TI, se propone una selección de los procedimientos aplicables al entorno específico para el cumplimento de este paso de la planificación del encargo.

Respecto de la etapa de ejecución, los resultados sugieren que no existen cambios importantes en el proceso de obtención, procesamiento y conservación de las evidencias de auditoría, salvo algunas precauciones que deben tomarse, vinculadas principalmente a los riesgos de falta de disponibilidad futura de la información.

Finalmente se destaca la necesidad de que se profundicen aspectos vinculados a la TI en la formación de los contadores públicos para llevar adelante auditorías financieras en el entorno tecnológico actual, como también la relevancia del trabajo interdisciplinario, incorporando especialistas en sistemas a los equipos de auditoría.

De la presente investigación resulta que la utilización de la computación en la nube en procesos vinculados a la elaboración de información contable tiene un potencial impacto en la auditoría de estados financieros sobre cada uno de los puntos analizados, planteando la posibilidad de realizar nuevos estudios para el avance de la disciplina.

ABSTRACT

Financial audit has been significantly affected by the use of information technology (IT) for the processing and storage of accounting information. Particularly, the emergence of new solutions such as cloud computing (CC) represents a challenge for the development of the discipline, both from an academic perspective and professional practice.

This thesis aims to analyze the features of financial auditing when the audited entity uses cloud computing in processes that affect financial information. An exploratory study is carried out with a qualitative approach, obtaining data through in-depth interviews to financial and systems auditors belonging to the great audit firms of the Argentine Republic.

Firstly, the level of utilization of the CC by Argentine companies is described. Although it is in an early stage of evaluation and implementation, there are expectations of growth, even in processes with an impact on financial statements. In this framework, accounting and systems audits need to adapt to the new environment.

Next, an analysis is proposed on the various stages of the financial audit in the IT environment under study. In planning, the process of understanding the entity and its environment is considered especially important. A description is made about a set of aspects that the auditor would need to know in order to achieve an adequate understanding of the information systems of the entity, and a discussion on the procedures that could be applied to that effect, considering certain limitations imposed by the technology analyzed.

Subsequently, the various risk factors derived from the use of CC and identified by the literature are addressed, with emphasis on those with a potential impact on financial auditing. After its treatment a risk breakdown structure is elaborated, useful tool in order to simplify and systematize the risk assessment in these engagements.

In relation to the evaluation of the internal control system in CC environments, there is a description of user and service provider controls, whose design, implementation and operation can interest the financial auditor. Based on the analysis of this IT outsourcing alternative, it is proposed a selection of the procedures applicable to the specific environment for the fulfillment of this planning stage.

Regarding the execution stage, the results suggest that there are no significant changes in the process of obtaining, processing and preserving audit evidence, except for some precautions that must be taken, mainly related to the risks of future unavailability of the information.

Finally, it is underlined the need to deepen aspects related to IT in the training of public accountants to carry out financial audits in the current technological environment, as well as the relevance of interdisciplinary work, incorporating system specialists to the audit teams.

The present research shows that the use of cloud computing in processes linked to the preparation of accounting information has a potential impact on the audit of financial statements on each of the analyzed points, suggesting the possibility of further studies for the development of the discipline.

ÍNDICE

LISTADO DE FIGURAS

LISTADO DE CUADROS

LISTADO DE ABREVIATURAS

AICPA: *American Institute of Certified Public Accountants*

BCRA: Banco Central de la República Argentina

CI: Controles internos

CN: Computación en la nube

COSO: *Committee of Sponsoring Organizations of the Treadway Commission*

CSA: *Cloud Security Alliance*

EEFF: Estados financieros

ERP: *Enterprise Resource Planning*

ERS: *Enterprise Risk Services*

ENISA: *European Network and Information Security Agency*

FACPCE: Federación Argentina de Consejos Profesionales de Ciencias Económicas

IAASB: *International Auditing and Assurance Standards Board (IFAC)*

IESBA: *International Ethics Standards Board for Accountants (IFAC)*

IFAC: *International Federation of Accountants*

IFRS: *International Financial Reporting Standards*

IGJ: Inspección General de Justicia

ISA: *International Standards on Auditing* (en español, Normas Internacionales de Auditoría)

ISAE: *International Standards on Assurance Engagements* (en español, Normas Internacionales de Encargos de Aseguramiento)

IES: *International Education Standards* (en español, Normas Internacionales de Formación)

ISACA: *Information Systems Audit and Control Association*

NIA: Norma Internacional de Auditoría

NIEA: Normas Internacionales de Encargos de Aseguramiento

NIF: Normas Internacionales de Formación

NIST: *National Institute of Standards and Technology*

OS: Organización de Servicios

RBS: *Risk Breakdown Structure*

RT: Resolución Técnica

SIC: Sistema de información contable

SLA: *Service Level Agreement*

SAS: *Statements on Auditing Standards* (Normas de Auditoría de Estados Unidos)

SSAE: *Statements on Standards for Attestation Engagements* (Normas para Encargos de Aseguramiento de Estados Unidos)

TAACs: Técnicas de Auditoría Asistidas por Computadora

TI: Tecnología de Información

TIC: Tecnología de Información y Comunicación

VPN: *Virtual Private Network*

1. INTRODUCCIÓN

1.1. TEMA ABORDADO Y SU RELEVANCIA

El crecimiento explosivo de las soluciones de tecnología de la información (TI) y el deseo de las empresas de obtener ventajas competitivas ha llevado a un incremento sustancial del uso de sistemas de TI para generar, procesar, almacenar y comunicar información. Existen pocas compañías que no confíen en la TI para cumplir sus objetivos de reporte financiero, operativos y de cumplimiento (Tucker, 2001).

La contabilidad en particular se ha visto enriquecida por el avance tecnológico; la posibilidad de generar información contable en forma ágil aporta a su objetivo de brindar apoyo a quienes deben tomar decisiones, tanto a nivel interno como externo de las organizaciones (Suárez Kimura, 2007).

En consecuencia, el uso de la tecnología de la información para la elaboración y el almacenamiento de la información contable ha tenido importantes efectos sobre la auditoría de estados financieros (o auditoría financiera) (Rîndasu, 2016). 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 importantes en las diferentes etapas del proceso de auditoría, así como en las habilidades exigidas a los profesionales para desarrollar una labor diligente y responsable.

A decir de Brandas, Stirbu y Didraga (2013) y Janvrin, Bierstaker y Lowe (2008), siendo que la TI ha modificado dramáticamente el proceso de auditoría, son necesarios estudios que se ocupen de estas cuestiones.

En particular, Curtis, Jenkins, Bedard y Deis (2009:81-82) en su síntesis de literatura sobre los efectos de los nuevos ambientes de sistemas de información sobre el proceso de auditoría, destacan que: a) la contabilidad y el reporte financiero dependen cada vez más de la tecnología implementada por las organizaciones, de modo que muchos controles automatizados permiten reducir el riesgo de errores y fraudes en los estados financieros, a la vez que agregan el riesgo de un eventual mal funcionamiento; b) la utilización de sistemas integrados, como los *Enterprise Resource Planning* (ERP), hace que se integren al proceso de elaboración de información a clientes y proveedores, modificándose los límites de la definición de cliente auditado para el auditor financiero; c) la actual tendencia a la tercerización de procesos críticos del sistema de información contable genera que en muchos casos los auditores financieros no tengan acceso a los sistemas de información alojados en los proveedores de los servicios tercerizados, produciéndose modificaciones en diversos aspectos del proceso de auditoría, como por ejemplo, obligándolos a utilizar reportes sobre el control interno de la organización de servicios que no siempre brindarán satisfacción a sus necesidades.

Este último punto ha cobrado especial importancia a partir de aparición de una alternativa de tercerización de TI que se ha denominado *Computación en la Nube* (CN), la cual ha surgido en los últimos años y toma cada vez más relevancia en el mundo empresarial para la gestión de los negocios de las organizaciones.

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 & Grance, 2011) implementando, por ejemplo, paquetes de *software* de contabilidad y finanzas (Beal, 2013; Yigitbasioglu, 2015) o sistemas de *Enterprise Resource Planning* que incluyan los módulos de contabilidad, ventas, gestión de clientes –como las opciones previstas por Oracle (2014) y SAP (2014) –, entre otros.

Su 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 (*Information Systems Audit and Control Association* (ISACA), 2009; Yigitbasioglu, 2015; Zhang, Cheng & 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 (Ali, Khan & Vasilakos, 2015; Brender & Marjov, 2013; CSA, 2010, 2013a; ENISA, 2009)–, muchos de los cuales se han materializado en incidentes (Agrawal, 2017; Infobae, 2012; Kuranda, 2014; Tsidulko, 2016), generan desafíos no sólo para los entes usuarios, sino también para sus auditores (Blaskovich & Mintchik, 2011).

Este cambio en las soluciones de TI utilizadas por las empresas en la gestión representa un reto para la auditoría de estados financieros 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 específica (Blaskovich & Mintchnik, 2011) que requiere un avance desde la óptica del conjunto de conocimientos así como de la práctica profesional.

La *Cloud Security Alliance* (CSA) (2011b) sugiere la necesidad de revisar de qué manera se ve afectado el cumplimiento de los fines de la auditoría en este entorno, en particular en lo que se refiere a la evaluación de controles que afecta a la auditoría financiera, considerando las características específicas que posee la nube frente a otras alternativas de TI. 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 pertinentes 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 y de los controles internos sobre los estados financieros y la forma en que los auditores darán cumplimiento a los requerimientos de la regulación en entornos de CN.

A la fecha, la mayoría de los estudios académicos en relación a la CN se refieren a aspectos técnicos y en menor medida a aspectos vinculados a su utilización por las organizaciones –factores de adopción, riesgos, beneficios– aun cuando su impacto sobre las entidades usuarias es significativo y requiere de investigaciones al respecto (Bayramustra & Nasir, 2016; Kumar & Goudar, 2012; Yigitbasioglu, Mackenzie & Low, 2013). A su vez existen estudios referidos a los efectos de la TI y la tercerización de la TI sobre la auditoría (Astiz & Sole, 2008; Bierstaker, Chen, Christ, Ege & Mintchik, 2013; Minguillón, 2006; Pastor, 2011; Scutella & Barg, 2010; Valencia & Tamayo, 2012; entre otros).

Sin embargo, se ha detectado una escasez de investigaciones académicas relacionadas a la auditoría de estados financieros en este tipo de ambientes tecnológicos complejos basados en tecnologías emergentes (Alali & Yeh, 2012); esta brecha representa una oportunidad para el desarrollo de este trabajo de investigación, en el que se pone énfasis en los efectos sobre el proceso de auditoría de los estados financieros emitidos por un ente que utiliza la CN para elaborar la información contable.

1.2. ESTADO DE IMPLEMENTACIÓN DE LA CN EN LA REPÚBLICA ARGENTINA

La presente investigación se contextualiza en la República Argentina, razón por la que resulta necesario analizar antecedentes sobre el estado de utilización de la computación en la nube en este país.

Investigaciones desarrolladas por consultoras durante los años 2013 y 2014 (ORACLE-MERCADO, 2013; USUARIA 2013, 2014) han documentado las características de la implementación de la nube por parte de empresas argentinas, así como las previsiones futuras al respecto. Sin embargo no se han encontrado a la fecha investigaciones académicas en el país que se orienten en este sentido.

La primera, desarrollada por ORACLE y MERCADO (2013), consiste en una investigación *on-line* entre ejecutivos de distintas áreas de empresas argentinas sobre la percepción que poseen acerca de la nube. Las realizadas por USUARIA (2013; 2014) son investigaciones sobre la utilización de la nube por medianas y grandes empresas argentinas, de diversos sectores económicos (finanzas, servicios, industria, comercio, gobierno) en los años 2012 y 2013, mediante entrevistas personales a los profesionales de TI. Un resumen de los resultados obtenidos en estos trabajos se presenta en el Cuadro 1.

Cuadro 1 - Utilización de la CN por empresas argentinas

ASPECTOS	USUARIA		ORACLE -MERCADO
	AÑO 2012	AÑO 2013	AÑO 2013
Cantidad de empresas relevadas	81	83	265
Porcentaje de adopción a la fecha del estudio	26.8%	28.8%	42.3%

Nivel de adopción esperado en los siguientes 24 meses	33.8%	40%	
Modelos de distribución utilizados mayormente	Nube privada de gestión interna.	Nube pública. Nube privada de gestión externa.	Nube privada de gestión interna. Nube pública.
Servicios adoptados	*Hosting* de aplicaciones.	Infraestructura (*hosting* de servicios y/o aplicaciones) Servicios a usuarios (mensajería, colaboración, ofimática).	Almacenamiento de contenidos. Aplicaciones *web*. Herramientas de colaboración.
Servicios a ser adoptados en los siguientes 24 meses	Servicios a usuarios (mensajería, colaboración, ofimática).	ERP. Payroll.	
Principales beneficios percibidos	Reducción de costos. Flexibilidad y escalabilidad.	Aporte a la agilidad del negocio. Flexibilidad y escalabilidad de los recursos de TI. Reducción de costos.	
Principales inhibidores para la implementación	Seguridad de la información. Cultura de la compañía. Pérdida de control de la infraestructura de TI.	Cultura de la compañía. Seguridad de la información.	Inseguridad que genera subir información sensible para la compañía. La empresa no está preparada internamente para el concepto de soluciones en la nube.

Fuente: Elaborado con base en USUARIA (2013), USUARIA (2014) y ORACLE-MERCADO (2013).

A la fecha de realización de dichas investigaciones, el desconocimiento sobre el valor de la herramienta implicaba que los tiempos de implementación se extiendan (ORACLE-MERCADO, 2013), pero con un incremento en el nivel de adopción de un año a otro, con esperanzas de fuerte crecimiento para los siguientes 24 meses, considerando los planes declarados por las organizaciones (USUARIA, 2014). Según Marino (2014) los especialistas prevén que todo pasará por la nube en los próximos años; su aplicación es una decisión estratégica de mediano y largo plazo. Conocer casos de éxito de empresas que hubieran implementado soluciones en la nube puede ser un factor que incremente el nivel de uso (ORACLE-MERCADO, 2013:190).

A través del tiempo se observa que existe un aumento en el nivel de adopción de modelos de distribución que suponen la tercerización de la gestión de la nube (modelos público y privado de gestión externa), lo cual puede deberse a una mayor madurez alcanzada por los servicios ofrecidos por los proveedores. El estudio de ORACLE-MERCADO (2013) reconoce que las grandes empresas crean y administran entornos de nube privada para servicios de infraestructura básica, plataformas de desarrollo e incluso aplicaciones enteras, mientras que las empresas medianas acceden a ofertas de nube pública dado que carecen de escala para instalar sus propias nubes.

Como se puede apreciar, los principales beneficios percibidos por las empresas no se refieren a la reducción de costos –punto sujeto a discusión en la teoría–, sino al aporte al negocio –focalización de los recursos en los procesos de valor de la compañía y agilidad en el despliegue de nuevos procesos, productos y servicios– y la flexibilidad y escalabilidad.

Los inhibidores principales para la implementación de esta tecnología se mantuvieron en el tiempo. Se refieren a la cultura organizacional y la seguridad de la información y del gobierno de datos. Este inhibidor se relaciona a riesgos identificados tales como: localización de los datos (poder acceder a ellos en cualquier momento); protección de la información (confidencialidad en un entorno de recursos compartidos); recuperación de la información (en caso de desastres o de extinción de la relación contractual); marco legal (cumplimiento de normas de protección y seguridad independientemente de la localización); responsabilidad del propietario de la información (referida a la localización, protección y recuperación de los datos) (USUARIA, 2013, 2014). A su vez, existen inhibidores menos importantes vinculados al proveedor del servicio (oferta inmadura y marco legal) (USUARIA, 2014), que se verán superados con el transcurrir del tiempo.

Según Marino (2014), cualquier industria puede hacer uso de la CN; algunas lo hacen para conectarse con los clientes –cuando poseen presencia *web* con alta concurrencia–; otras para desarrollar sus sistemas operativos. Dichas industrias incluyen los sectores de consumo masivo y venta minorista, el sector financiero –sea para poner a disposición de los clientes recursos de *home banking* o para montar allí su infraestructura interna con gran flexibilidad y reducción de costos– e incluso el sector público para desarrollar su relación con los ciudadanos.

Un estudio publicado en el año 2016 por BSA –que realiza un seguimiento regular del cambio en las políticas (marco legal y regulatorio) para la implementación de la nube sobre 24 países que representan el 80% del mercado mundial de TI– demuestra que a nivel mundial el panorama sigue mejorando. En particular, ubica a la República Argentina en el lugar 16 de las 24 economías líderes en tecnología de la información en relación a la preparación para la computación en la nube. Esto demuestra que el contexto se encuentra en evolución y que es de esperar que se vuelva favorable para un incremento en el nivel de uso de esta tecnología en el futuro por parte de las empresas.

1.3. OBJETIVOS DE LA INVESTIGACIÓN

Para el desarrollo de esta investigación se ha planteado un objetivo general y 6 objetivos específicos:

- **Objetivo General**

Analizar las particularidades de la auditoría financiera cuando el ente auditado utiliza la computación en la nube en procesos que afectan a la información contable.

- **Objetivos Específicos**

1. Indagar respecto de la utilización de la CN por las empresas argentinas.

2. Identificar los principales aspectos del uso de la CN que el auditor deberá considerar para obtener un acabado conocimiento del cliente y su entorno.

3. Identificar y describir los riesgos derivados del uso de la computación en la nube para la elaboración de información contable relevantes para la auditoría de estados financieros.

4. Determinar las particularidades de la evaluación del sistema de control interno en entornos de CN para la planificación de la auditoría financiera.

5. Indagar las posibles consecuencias sobre el proceso de obtención, procesamiento y conservación de las evidencias de auditoría que surjan en el contexto de la nube.

6. Analizar la formación y las habilidades requeridas al contador público y la eventual colaboración de especialistas en TI para el desarrollo de encargos de auditoría financiera en entornos de TI complejos, en particular los basados en la computación en la nube.

1.4. DESCRIPCIÓN DEL APORTE

A partir del desarrollo de la presente tesis se pretende realizar los siguientes aportes:

- A la academia, y la disciplina auditoría en particular: realizar un aporte en un área en el que no se encuentran muchas publicaciones en el contexto de la investigación, utilizando el método científico a través de una metodología cualitativa para la obtención de resultados empíricos que respalden las conclusiones. Esta es una disciplina relevante por la confiabilidad que brinda a la información financiera para la toma de decisiones por parte de sus diversos usuarios. Sin embargo, las investigaciones en esta área son escasas, siendo necesario ampliar e innovar en las temáticas sobre las que se investiga.
- A la actividad docente, para la formación de profesionales en el área de auditoría: exponer temas y nuevos ambientes de TI sobre los cuales pueda ser necesario formar a los alumnos.
- A la profesión de contadores públicos: acercar las experiencias de los grandes estudios; llamar la atención sobre nuevas realidades que afectan a la profesión y respecto de las cuales se requiere capacitación; facilitar un marco de referencia para el estudio del tema propuesto; resaltar cuestiones que requieren ser analizadas por quienes están a cargo de la emisión de normas.

1.5. ESTRUCTURA DE LA TESIS. LOS PRÓXIMOS CAPÍTULOS

A fin de dar cumplimiento a los objetivos planteados en esta tesis, la misma está integrada por cuatro partes principales: marco teórico, metodología, resultados y consideraciones finales. Cada una de ellas es dividida en apartados para facilitar la exposición.

En primer lugar, en el **Capítulo 2** se desarrolla el referencial teórico que da sustento a la investigación. En un primer apartado se resumen los antecedentes referidos a auditorías financieras en entornos de tecnología de información. Seguidamente se describe el caso particular de la computación en la nube, destacando los conceptos principales requeridos para su comprensión. A continuación, se incluyen cinco apartados referidos a cada uno de los aspectos de la auditoría de estados financieros que se consideran principalmente afectados por la TI y que serán estudiados en esta tesis, de acuerdo a los objetivos específicos propuestos.

El **Capítulo 3** describe la metodología utilizada en la investigación. En el mismo se presentan las justificaciones de las elecciones realizadas a través de la teoría y una descripción de los diversos aspectos y detalles operacionales. La utilización de un enfoque cualitativo, a través de la realización de entrevistas en profundidad a expertos, resultó ser la opción elegida para la obtención de datos del campo que permitieran dar cumplimiento a los objetivos.

En el **Capítulo 4** se expone un resumen del perfil de cada uno de los profesionales entrevistados. La presentación de este contenido –previo a la exposición de los resultados– resulta útil para conocer las características de los informantes y tener un marco que permita evaluar los datos.

A continuación, en el **Capítulo 5** se exponen los resultados obtenidos. El mismo está dividido en apartados, uno por cada objetivo específico a cumplir. En primer lugar, se describen las particularidades de la utilización de la computación en la nube por las empresas argentinas, de acuerdo a la experiencia de los entrevistados, permitiendo ubicar la investigación en el contexto actual. En los siguientes apartados, se detallan los efectos de la tercerización de TI, en particular el caso de la CN, sobre cada uno de los aspectos de la auditoría financiera definidos como relevantes en el marco teórico. Se describen aspectos y procedimientos relevantes para el conocimiento del cliente y su entorno, etapa fundamental en una auditoría financiera en un ambiente de CN. Luego, se realiza una evaluación de los diferentes factores de riesgo, identificando aquellos relevantes para la auditoría de estados contables, proponiendo para ello una herramienta denominada estructura de desglose de riesgos. Vinculado a ello, en el siguiente apartado se analizan las particularidades que implica la evaluación de controles internos en la nube para la planificación de la auditoría. Seguidamente se expresan algunas consideraciones en relación a las evidencias digitales en la nube. Finalmente, se resumen conceptos relevantes respecto de la formación requerida a los contadores públicos para la realización de auditorías en entornos de TI cambiantes y cada vez más complejos, así como la importancia del trabajo interdisciplinario, utilizando la colaboración de expertos del área de sistemas.

Por último, en el **Capítulo 6** se resumen las consideraciones finales derivadas de esta tesis, acompañadas de una descripción de las limitaciones del estudio y futuras líneas de investigación.

2. REVISIÓN DE LA LITERATURA[1]

El desarrollo del marco conceptual mediante la revisión de la literatura sirve al planteamiento del problema cualitativo inicial (Hernández Sampieri, Fernández & Baptista, 2010) a la vez que resulta útil a efectos de organizar el conocimiento en un conjunto de relaciones que permiten ver las variables que actúan en el problema y definir los métodos destinados a reunir la información necesaria (Vázquez, Bongianino, Sosisky & Albano, 2006). Se busca establecer relaciones entre el problema de investigación y el cuerpo más amplio de conocimientos.

En el presente capítulo se desarrolla el marco teórico de esta investigación elaborado a partir de una revisión de antecedentes de bibliografía académica y de normas de auditoría vigentes en la República Argentina –nacionales e internacionales–, así como de estándares y recomendaciones emitidas por instituciones dedicadas a la investigación de la CN, con el objetivo de identificar los avances que se han producido al respecto.

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 (Apartado 2.1.), lo cual representa el cuerpo de literatura en el que se encuadra el problema de investigación. Luego 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 (Apartado 2.2.). En la sección siguiente (Apartado 2.3.) 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 y su entorno; la identificación y evaluación de riesgos de auditoría; la evaluación del sistema de control interno; las características específicas de las evidencias de auditoría; las habilidades y competencias requeridas al contador público y el uso de especialistas.

2.1. AUDITORÍA FINANCIERA EN ENTORNOS DE TECNOLOGÍA DE LA INFORMACIÓN

El uso de tecnologías de la información y comunicación (TICs) ha cambiado la forma en que las empresas operan sus negocios (Brazel & 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 tecnología de información (TI) en sus trabajos (Hunton, Bryant & Bagranoff, 2004), dado que si bien el objetivo y alcance de una auditoría no se modifica a causa de ella (Cerullo & Cerullo, 1997; González,

[1] Un resumen del apartado del referencial teórico fue publicado en coautoría con la Mg. Diana Albanese y la Mg. Regina Durán. Véase López, Albanese y Durán (2013).

2004; Pastor, 2011), 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 una tercera parte (Scutella & Barg, 2010). Actualmente, en la mayoría de los casos el auditor financiero desarrolla su trabajo en entornos informatizados debido al uso generalizado de la TI que realizan sus clientes, siendo 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 vinculados al reporte financiero. Ello incluye una amplia comprensión del flujo de transacciones y actividades efectuadas en forma electrónica y los controles relacionados para asegurar la validez y fiabilidad de la información en un entorno sin papel. A partir de ello, en el análisis de riesgos se deben considerar aquellos derivados del uso de entornos informáticos, para 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 hubiere 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 computadora (TAACs). Finalmente, en relación a 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.

En relación a la definición del enfoque de auditoría, 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. (2004) 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 sólo en forma electrónica o porque está disponible solo por un período de tiempo limitado (Brazel & Agoglia, 2007; NIA 500; Pastor, 2011). Según plantean, ello conlleva la necesidad de un mejoramiento en las competencias de los profesionales para su adecuada obtención y tratamiento, debiendo acudir a las TAACs en forma complementaria a las técnicas manuales utilizadas tradicionalmente.

Janvrin et al. (2008) realizan una investigación basada en la opinión de auditores de estudios de diverso tamaño de USA, desde firmas locales de una sola oficina hasta de las internacionales conocidas como las *BIG-4*. Describen que el nivel de uso y la importancia otorgada a la TI en el proceso de auditoría varían significativamente de acuerdo al tamaño de la firma de auditoría. Esto se debe principalmente a dos cuestiones: a) los grandes estudios poseen mayores recursos que les permiten adquirir soluciones de TI costosas y contar con la colaboración de especialistas en sistemas (pudiendo resultar en auditorías de mejor calidad), lo cual está más limitado para los pequeños y medianos estudios nacionales, regionales o locales; b) los grandes estudios poseen clientes de mayor tamaño o que hacen uso de alternativas de TI más complejas.

Brandas et al. (2013) plantean que el uso de la TI en los procesos financieros y contables en las organizaciones requiere de la integración de la auditoría financiera con la auditoría de sistemas, para asegurar la integridad, exactitud, realidad y disponibilidad de la información de los estados contables. El enfoque en riesgos y controles para la evaluación de los sistemas de información contables en ambientes de TI es fundamental en dichos encargos.

El Cuadro 2 resume las consideraciones de los diversos autores en relación a la forma en que la TI afecta a la auditoría financiera. Los antecedentes disponibles presentan desarrollos conceptuales y análisis de normativa, demostrando una falta de trabajos empíricos basados en métodos como estudios de caso, encuestas o entrevistas. En la *Sección 2.3.* de este trabajo se

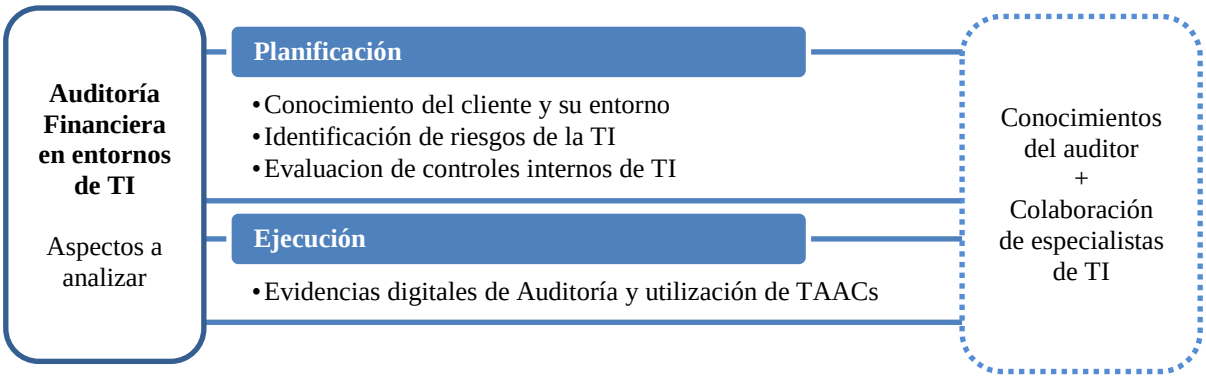
profundiza el análisis de la computación en la nube sobre cinco de los aspectos de la auditoría, considerados por los autores mencionados y que han sido seleccionados para ahondar en los efectos que esta solución de TI produce sobre los mismos. La Figura 1 expone el esquema conceptual que resume dicha elección.

Cuadro 2 - Resumen de antecedentes acerca de auditoría financiera y TI

REFERENCIA	PAÍS	PRINCIPALES APORTES
Cerullo & Cerullo (1997)	USA	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 sufre 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 riesgos y de controles; 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. (2004)	USA	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 & 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.
Janvrin et al. (2008)	USA	El nivel de uso y la importancia otorgada a la TI varía significativamente de acuerdo al tamaño de la firma de auditoría.
Scutella & 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 (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 & 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.
Brandas et al. (2013)	Rumania	Necesidad de integración de auditoría de TI con auditoría financiera. Propuesta de un modelo con enfoque integrado en riesgos, controles y pruebas de auditoría de los sistemas de información contable.

Fuente: Elaboración propia.

Figura 1 - Esquema conceptual para la investigación

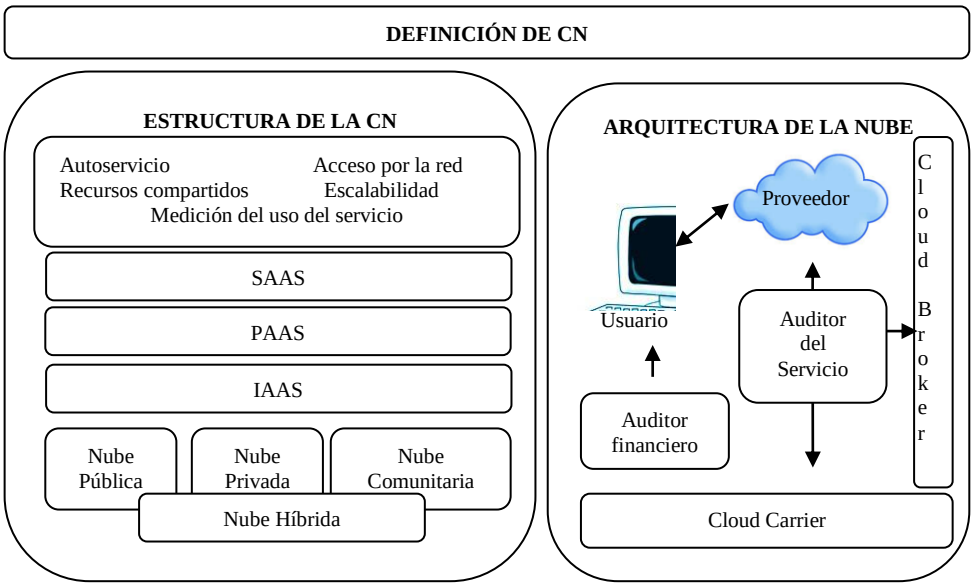


Fuente: Elaboración propia.

2.2. LA COMPUTACIÓN EN LA NUBE COMO AMBIENTE DE TI PARA LA REALIZACIÓN DE AUDITORÍAS DE ESTADOS FINANCIEROS

El presente apartado describe 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, y que es objeto de estudio de esta tesis. En la Figura 2 se resumen los conceptos a desarrollar.

Figura 2 - Resumen de conceptos referidos a la CN



Fuente: Elaboración propia.

2.2.1. Definición de la CN

El *National Institute of Standards and Technology* (NIST) (Mell & 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.

Por su parte, Vaquero, Rodero, Caceres y Lindner (2009) analizaron 20 enunciados utilizados en reportes científicos que describen la CN, y elaboraron un concepto que pretende ser comprensivo de las diversas características que la definen. Entre ellas, establecen que las nubes consisten en grandes reservas de recursos virtualizados, fácilmente utilizables, tales como *hardware*, desarrollo de plataformas y/o servicios. Estos recursos pueden ser reconfigurados de un modo dinámico para ajustarse a un nivel de carga variable, llamado escala, permitiendo su utilización óptima. Esta reserva de recursos es típicamente explotada por el modelo de pago por uso, en el cual las garantías son ofrecidas por el proveedor de la infraestructura, por medio de los acuerdos, conocidos como Acuerdos de Prestación de Servicios (*Service Level Agreements – SLAs)*.

Böhm, Leimeister, Riedl y Krcmar (2011) elaboraron una definición basada en su revisión de la literatura y su percepción de la nube, focalizándose en la distribución de recursos y aplicaciones más que en la descripción técnica. Definen entonces:

> (…) cloud computing como un modelo de distribución de TI, basado en la virtualización, donde los recursos, en términos de infraestructura, aplicaciones y datos, son distribuidos a través de Internet como un servicio provisto por uno o varios prestadores. Estos servicios son escalables a demanda y pueden ser valorizados sobre una base de pago por uso.

Otros autores han elaborado conceptos y caracterizaciones que destacan distintos aspectos del servicio, como la forma de provisión del servicio a través de Internet (Joint, Baker & Eccles, 2009; Miller, 2008; Mowbray, 2009) y la independencia de localización entre el usuario y el proveedor del servicio de la nube (Buyya, Yeo, Venugopal, Broberg & Brandic, 2009).

Es importante resaltar este último aspecto: mediante el uso de la red, se logra la permanente conexión entre recursos de *hardware*, que pueden estar ubicados en diversos lugares, inclusive en diferentes países. Si bien el usuario normalmente desconoce la ubicación exacta de los recursos y de sus datos, en algunos casos puede tener la opción de elegir las localizaciones preferidas para sus centros de datos; esto puede ser útil, por ejemplo, para las organizaciones sujetas a regulaciones que las obligan a mantener los datos personales de sus clientes en ciertas localizaciones geográficas (Sultan, 2011:273). La determinación puede referirse a un nivel superior de abstracción, indicando el país, estado o centro de datos donde pretende que la información sea almacenada y procesada.

Autores como Joint et al. (2009) y Mowbray (2009) realizan una comparación entre los sistemas tradicionales de utilización de servicios de tecnología y la CN, resumida en el Cuadro 3,

que permite definir y comprender esta opción de tercerización de TI. Como se puede apreciar, el concepto no es totalmente nuevo, en la medida en que los correos electrónicos basados en la *web* son casos simples de uso de *cloud computing*.

Cuadro 3 - Comparación entre sistemas tradicionales de TI y CN

SISTEMAS TRADICIONALES DE TI	COMPUTACIÓN EN LA NUBE
• El sistema operativo -por ejemplo Windows-, las aplicaciones -como Microsoft Word- y los datos están almacenados en una computadora personal o en servidores privados. • En el ambiente empresarial, los usuarios utilizan *hardware* y copias de *software* que les pertenecen, y los datos se almacenan en servidores a los que tienen acceso los miembros de la organización.	• La información, el *software* o cualquier otro servicio, es almacenado y utilizado en los servidores de un tercero, a través de Internet, y no en la computadora personal o en los servidores privados. • Los datos se almacenan en servidores a los que tiene acceso el prestador del servicio y otros usuarios de los recursos compartidos.

Fuente: Elaborado a partir de Joint et al. (2009) y Mowbray (2009).

2.2.2. Beneficios del uso de la CN que justifican la implementación por parte de las organizaciones

Para las organizaciones, la computación en la nube es atractiva desde perspectivas tecnológicas, prácticas y financieras (Mansfield, 2008), y es el conocimiento de sus beneficios lo que motiva su utilización (ISACA, 2012).

La ventaja más relevante consiste en la eficiencia lograda mediante la tercerización de parte de la gestión de la información y de las operaciones de TI, permitiendo a la organización focalizarse en cuestiones estratégicas de su negocio, mejorando procesos, aumentando la productividad e innovando, mientras el proveedor de la nube se encarga de las actividades operativas de TI más inteligentemente, más rápido y de modo más económico (ISACA, 2009).

Existen otros beneficios, que son descriptos por diversos autores y se resumen en el Cuadro 4.

Cuadro 4 - Beneficios derivados de la utilización de la CN

BENEFICIO	DESCRIPCION	AUTORES
Reducción de costos y flexibilidad	Debido a su modelo de pago por uso, justificado en diversas razones: a) se reemplaza la adquisición de *hardware* y *software*, evitando las inversiones iniciales en infraestructura; b) limita los costos de funcionamiento, actualización y mantenimiento de TI; c) se reemplazan las inversiones de capital por gastos operativos, evitándose las pérdidas generadas por recursos inmovilizados por capacidad ociosa y las erogaciones de licencias de pago único, reemplazadas por pagos periódicos por uso (mensual o anual). Requiere un análisis de los costos ocultos relacionados.	Armbrust et al. (2010); Grossman (2009); Hernández Bravo (2009); ISACA (2012); Marino (2014); McAfee (2012); Rao (2012); Tarmidi, Rasid, Alrazi & Roni (2014); Yigitbasioglu (2015)

Agilidad y rapidez en la contratación y desarrollo de los negocios	Los servicios pueden ser utilizados en el momento en que se los necesita, evitando las demoras originadas por el desarrollo, configuración y operación de los proyectos de TI tradicionales.	ISACA (2009); Yigitbasioglu (2015); Zhang et al.(2010)
Escalabilidad	Garantiza la disponibilidad de recursos, brindando capacidad de almacenamiento y uso ilimitado. Ofrece mayor flexibilidad, permitiendo la cobertura de los picos de demanda, evitando los recursos ociosos, mediante la provisión de servicios *on demand*.	ENISA (2009); Hernández Bravo (2009); ISACA (2009); Yigitbasioglu (2015); Zhang et al. (2010)
Mantenimiento y actualización constante de los sistemas	Dado que el proveedor de *cloud computing* tiene acceso a los nuevos sistemas, los actualiza y los pone a disposición de sus clientes de inmediato y a un menor costo que el que ellos deberían pagar para obtenerlos.	Abdulelah (2014); ENISA (2009); Miller (2008); Zhang et al. (2010)
Expertos a disposición	El personal del proveedor del servicio brinda su conocimiento profesional y se especializa en cuestiones de seguridad, privacidad y otras áreas de interés para los usuarios. La experiencia y conocimiento se logra en parte por la prestación de un servicio a gran escala. Difícilmente podrían ser contratados por las empresas, principalmente las medianas y pequeñas.	Zhang et al. (2010)
Acceso a tecnologías	Fundamentalmente en el caso de las pequeñas y medianas empresas, que pueden acceder a aquellas soluciones tecnológicas que antes sólo estaban disponibles para grandes compañías, debido a su alto costo.	ISACA (2012); Marino (2014); Tarmidi et al. (2014)

Fuente: Elaboración propia.

Aun cuando la CN puede bridar múltiples beneficios que motivarían su utilización, existe un conjunto de riesgos y amenazas a la seguridad de la información del ente usuario que también deben ser tenidos en consideración. Éstos han sido documentados por diversos autores y serán descriptos más adelante en esta tesis.

2.2.3. Estructura de la Computación en la Nube

Mell y Grance (2011) han definido lo que denominan la estructura de la CN, que comprende un conjunto de características esenciales y modelos de provisión y distribución del servicio, que resulta interesante describir. Dichos conceptos han sido tomados y complementados por diversos autores (ISACA, 2009, 2012; Vaquero et al., 2009; CSA, 2011a; Svantesson & Clarke, 2010), en la medida en que ayudan a la definición de los servicios en la nube.

Las características esenciales de la CN identificadas por los autores comprenden:

a) Autoservicio a solicitud: el usuario se provee de herramientas de computación, unilateral y automáticamente en función de sus requerimientos (naturaleza "bajo demanda"), sin necesidad de interacción humana con cada uno de los proveedores de los servicios.

b) Acceso a través de la red: los servicios son distribuidos y están disponibles a través de una red de telecomunicaciones, existiendo amplio acceso a los datos a través de diversos

dispositivos, tales como *laptops*, teléfonos móviles y *personal digital assistants* - PDAs, en la medida en que se posea conexión a Internet.

c) Rápida escalabilidad: los servicios brindados son ilimitados, pudiendo ser utilizados en cualquier momento y cantidad. La escala de prestación es flexible, de manera que puede verse incrementada o disminuida en función del nivel de actividad del usuario en cada instante. El aprovisionamiento rápido de los recursos funciona en forma predictiva (no reactiva) previéndose los picos de demanda y actuando en forma automatizada a priori (Hernández Bravo, 2009).

d) Recursos compartidos: los recursos computacionales del proveedor son compartidos, de manera que sirven a múltiples usuarios –de una misma o de diferentes organizaciones. Ello se logra por medio de una dinámica asignación y reasignación de los recursos físicos y virtuales entre ellos, en función de su nivel de demanda.

Según la CSA (2011a:14-15) en el caso de una nube pública –definida a continuación– son distintas personas u organizaciones las que acceden a los recursos en la nube; en el caso de nubes privadas, si bien existe una organización propietaria, los diversos usuarios con los que comparte pueden comprender a consultores externos y contratantes, o inclusive diversas unidades de negocio usuarias del servicio como entidades por separado.

e) Medición del uso de los servicios: Se realiza un control y optimización del servicio, mediante un monitoreo continuo sobre su uso, brindando transparencia tanto para el proveedor como para el usuario. Los recursos utilizados son medidos por cliente y aplicación, por día, semana, mes y/o año.

Por otra parte, se definen los modelos de provisión de *cloud computing*, incluyendo tres tipos de servicios que varían de acuerdo a los requerimientos de los usuarios (Mell & Grance, 2011; Vaquero et al., 2009):

a) ***Infraestructura como un servicio (Infraestructure as a Service - IAAS):*** en el que el proveedor brinda como servicio los recursos de *hardware*, como el almacenamiento, y de *computing power*, incluyendo CPU y memoria, y el usuario puede desplegar y ejecutar *software*, incluyendo sistemas operativos y aplicaciones; los recursos son alquilados, sin necesidad de realizar inversiones en servidores y equipamiento de redes. Si bien el usuario no controla ni maneja la infraestructura subyacente, tiene el control sobre sistemas operativos, y posiblemente control limitado en la selección de componentes para la creación de redes. Las previsiones de seguridad, más allá de la infraestructura básica, son ejecutadas principalmente por el usuario del servicio.

b) ***Plataforma como un servicio (Platform as a Service - PAAS):*** el proveedor ofrece una plataforma que comprende el *hardware* y los sistemas operativos, con facilidades para el desarrollo de aplicaciones, incluyendo el diseño, implementación, testeo, operación y soporte de aplicaciones *web* y servicios en Internet. El usuario tiene control sobre las aplicaciones pero no sobre la infraestructura. La finalidad consiste en brindar un ambiente de desarrollo para la generación de aplicaciones, no estando definido para procesos operativos (Rumitti & Falvella, 2013).

c) ***Software como un servicio (Software as a Service - SAAS*)**: las aplicaciones de *software* son ofrecidas como servicios en Internet para el usuario, quien no necesita adquirir paquetes y licencias para uso propio a ser instalados en sus computadoras. El *software* provisto por un tercero está disponible en el momento en que es requerido, y el usuario carece de control tanto sobre la infraestructura como sobre las aplicaciones que utiliza.

En Liu et al. (2011) se describen los usuarios que se verían satisfechos por cada uno de estos modelos, así como los servicios prestados por el proveedor en cada supuesto, junto con ejemplos de servicios aplicables en cada caso. En el Cuadro 5 se describe también –a partir del trabajo de dichos autores– cuáles son las actividades a cargo de usuarios y proveedores en cada uno de los niveles de servicio.

Como se puede apreciar, existe una relación inversa entre el nivel de control que poseen el consumidor y el proveedor sobre los recursos (aplicaciones, *middleware* y sistemas operativos); esto es, en cada una de las alternativas de servicio, cuanto mayor es el control del usuario, menor es el del proveedor. Por ejemplo, en el caso de un servicio SAAS el alcance del control del usuario llega sólo al nivel de las aplicaciones, mientras que el *middleware* y el sistema operativo están bajo el control del proveedor. Su comprensión permite determinar hasta donde llega la responsabilidad de cada una de las partes involucradas.

Cuadro 5 - Actividades de usuario y proveedor en cada estrato de aplicaciones de acuerdo al tipo de servicio

	SAAS	PAAS	IAAS
APLICACIONES - Incluye las aplicaciones de *software* dirigidas a usuarios finales o programas	Consumidor: utiliza las aplicaciones. Proveedor: instala/gestiona/mantiene las aplicaciones.	Consumidor: instala/gestiona/mantiene las aplicaciones.	Consumidor: instala/gestiona/mantiene las aplicaciones.
MIDDLEWARE - Incluye los bloques de creación de *software* para desarrollar aplicaciones en la nube (librerías, bases de datos, etc.)	Oculto para el consumidor.	Consumidor: los utiliza. Proveedor: instala/gestiona/mantiene las aplicaciones.	Consumidor: instala/gestiona/mantiene las aplicaciones.
SISTEMAS OPERATIVOS (SO) - Incluye los sistemas operativos y drivers	Oculto para el consumidor.	Oculto para el consumidor.	Consumidor: asume responsabilidad por el SO alojado. Proveedor: controla el SO.

Fuente: Adaptado de Liu et al. (2011).

Asimismo, existen cuatro formas de distribución del servicio que hacen a la definición de la estructura de la CN:

a) Nubes públicas: en las que la estructura está disponible para el público en general, o al menos para un grupo industrial amplio; los recursos son provistos sobre la base de autoservicio a través de Internet, desde un sitio externo al usuario, perteneciente al proveedor, que factura los

servicios en función del nivel de consumo. Existen tres tipos: a) servicios gratuitos, soportados por publicidad, en general limitados para uso no comercial; b) servicios pagos, de bajo costo, dado que existe un contrato donde los términos del servicio no son negociables y pueden ser modificados unilateralmente por el proveedor; c) servicios pagos donde los términos del servicio son negociados entre usuario y proveedor, con un costo mayor (Jansen & Grance, 2011:6).

b) Nubes privadas: en las que la nube es creada según los principios de *cloud computing*, pero operada para una sola organización, pudiendo ser gestionada por la propia organización o por un tercero, y ser local o no.

c) Nubes comunitarias: donde la infraestructura es compartida por diferentes organizaciones, dando soporte a una comunidad que tiene preocupaciones compartidas, tales como su misión, requerimientos de seguridad, políticas y consideraciones de conformidad. El proveedor brinda el servicio a un número limitado y bien definido de usuarios. Dado que la cantidad de participantes es más limitada que en una nube pública, los costos son más elevados, pero puede ofrecer mayores niveles de privacidad, seguridad y/o cumplimiento de políticas.

d) Nubes híbridas: donde la infraestructura es una composición de dos o más nubes, privadas, públicas o comunitarias, que se mantienen como entidades únicas, pero que se unen por la estandarización o propiedad de la tecnología que permite portar los datos y aplicaciones.

Cada modelo posee características distintivas en relación al gerenciamiento, la propiedad, la localización y el acceso y utilización del servicio, determinando la combinación de estas cualidades el tipo de nube que debe ser adoptada (Sobragi, 2012), según surge del Cuadro 6.

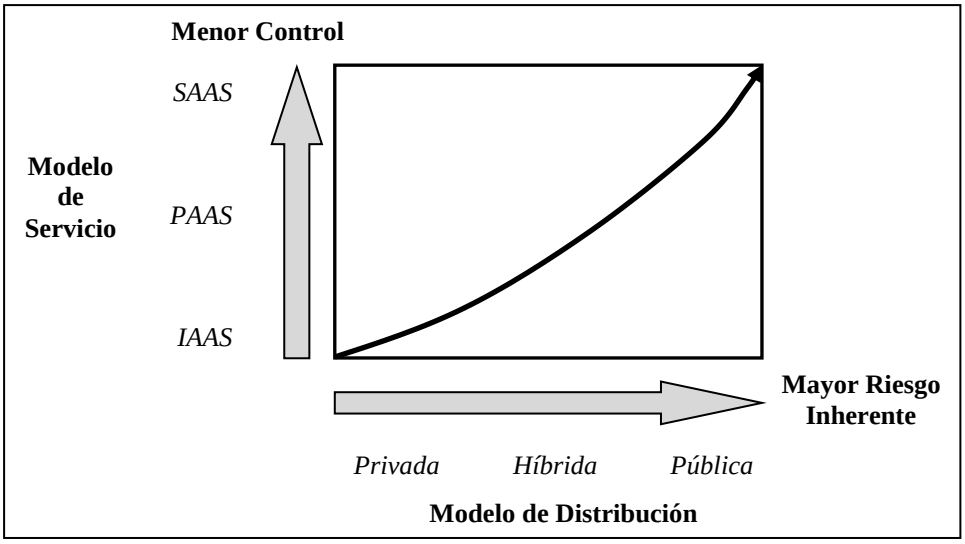
Cuadro 6 - Características de las formas de distribución de la CN

Tipo de Nube	Gerenciamiento	Propiedad	Localización	Acceso y utilización
Pública	Proveedor externo.	Proveedor del servicio.	Externa.	Compartido.
Privada	Organización y proveedor externo.	Organización.	Interna.	Privado.
Comunitaria	Organizaciones.	Comunitaria.	Externa e Interna.	Compartido.
Híbrida	Organización y proveedor externo.	Compartida.	Externa e Interna.	Compartido y Privado.

Fuente: Sobragi (2012).

La comprensión de los distintos modelos es fundamental, en la medida en que cada uno de ellos implica diferentes niveles de responsabilidad del usuario y del proveedor sobre el control interno, la seguridad y la configuración del servicio (*Committee of Sponsoring Organizations of the Treadway Commission* (COSO), 2012; CSA, 2013a; ISACA, 2012; Liu et al., 2011:9). Tal como se puede visualizar en la Figura 3, un servicio de IAAS privado será aquel que implique el mayor nivel de control por parte del usuario y el menor nivel de riesgo inherente; en el polo opuesto se encuentran los servicios de tipo SAAS públicos (COSO, 2012).

Figura 3 - Nivel de control directo por el usuario y riesgo inherente en relación a los modelos de CN



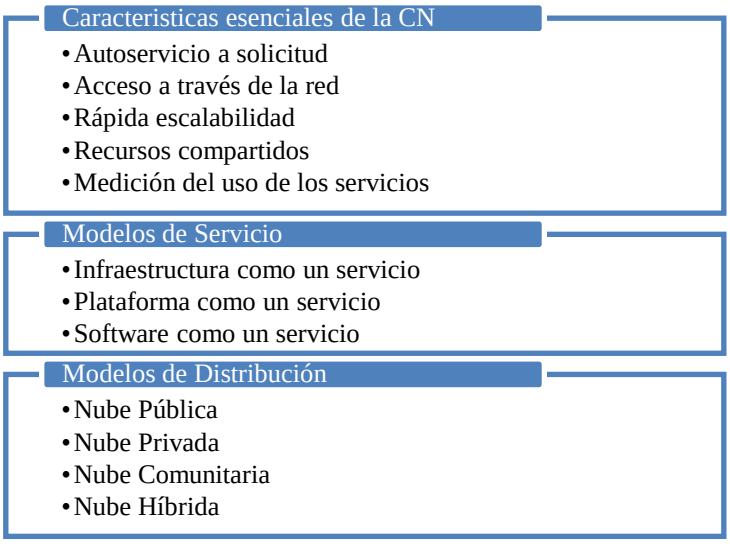
Fuente: COSO (2012:7).

Desde el punto de vista del usuario, la implementación y la selección del modelo a utilizar implica no solo un análisis de las necesidades y objetivos del ente y los costos relacionados, sino también de las responsabilidades inherentes al rol de proveedor y usuario respectivamente y de la posibilidad de supervisión de los procesos del proveedor, para garantizar que se alinean con las prácticas de gobernanza de la organización y las medidas implementadas para garantizar la seguridad de la información (Grossman, 2009; Jansen & Grance, 2011: 43).

Desde la perspectiva del auditor externo, la comprensión de las características de los servicios le permitirá evaluar a priori los riesgos inherentes y de control asociados al tipo de servicio adoptado por su cliente al momento de planificar la auditoría. A su vez, le otorga la posibilidad de brindar su opinión en caso que su asesoramiento fuera solicitado antes de la implementación del servicio.

A modo de resumen se exponen en la Figura 4 los componentes de la estructura de la CN descriptos previamente.

Figura 4 - Estructura de la CN



Fuente: Elaboración propia.

2.2.4. Arquitectura de la CN y acuerdos de prestación de servicios

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). Liu et al. (2011) han definido una arquitectura de la CN, donde son identificados los cinco actores principales, sus roles y responsabilidades clave. Los actores representan una entidad (persona u organización), que participan en una transacción o proceso y/o ejecutan tareas en la nube. Los dos actores principales y que se priorizarán en esta investigación son los siguientes:

- **Usuario:** individuo u organización que adquiere y utiliza productos y servicios de *cloud computing*. En este caso sería el ente auditado.
- **Proveedor:** pone los servicios a disposición de las partes interesadas; brinda los productos y servicios.

Tal como fue indicado previamente, de acuerdo al tipo de servicio (SAAS, PAAS, IAAS) el nivel de responsabilidad de usuario y proveedor sobre el control, seguridad y configuración del servicio puede variar.

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. Dichos acuerdos son, en algunos casos, fruto de la negociación de ambas partes, o en otros, simples contratos de adhesión donde el proveedor determina las pautas, y el usuario acepta o no las condiciones. El nivel de negociación dependerá del tipo de servicio contratado y del poder que posean cada uno de los actores. Los niveles de servicios contratados dependerán de las necesidades de los usuarios, dando lugar a los distintos modelos de distribución.

Otros actores relevantes en la prestación de servicios en la nube son los que siguen:

- **Auditor de la nube:** ejecuta una evaluación del servicio, de las operaciones del sistema de información, del desempeño y la seguridad de la implementación de la nube. Su función resulta valiosa dada su actuación independiente y la supervisión que realiza de la seguridad. Realiza su evaluación del servicio analizando a todos los miembros de la cadena; debe comunicarse no sólo con el proveedor, sino también con usuarios y *brokers* para poder recopilar la información de auditoría.
- ***Broker*:** actúa como intermediario entre el consumidor y el proveedor, gestionando el uso, desempeño y distribución de la nube. Puede ayudar a los usuarios en virtud de la complejidad de los servicios de la nube ofrecidos. A su vez, puede generar servicios de la nube con un valor añadido.
- ***Carrier*:** es la organización responsable de la conexión y transporte de los servicios entre los usuarios y proveedores de la nube; está a cargo de la transferencia de los datos (como si fuera el distribuidor de energía para la red eléctrica).

2.2.5. CN como alternativa de tercerización con efectos en la auditoría financiera

Se resumen en el siguiente apartado antecedentes referidos a consecuencias e interrogantes que surgen para la auditoría de estados financieros cuando el ente auditado utiliza servicios de computación en la nube.

Existe en los modelos de prestación de servicios a través de la nube un 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 para 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, 2011b: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) 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 & Beasley, 2007). Ello encuentra ciertas dificultades en el caso de la CN, dada 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 los prestadores de servicio subcontratados por el proveedor de la nube (CSA, 2011b: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 & Falvella, 2013) debiendo considerar procedimientos alternativos para la realización del trabajo.

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

Este cambio en el ambiente de TI que debe enfrentar 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 *American Institute of Certified Public Accountants* (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, 2011b).

2.3. ASPECTOS DE LA AUDITORÍA FINANCIERA POTENCIALMENTE AFECTADOS POR LA COMPUTACIÓN EN LA NUBE

Con base en los antecedentes relevados sobre la auditoría financiera en entornos de TI en la *Sección 2.1.*, y considerando las particularidades de la CN indicadas en la *Sección 2.2.*, 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 aspectos específicos de la auditoría

como: el conocimiento del cliente y su entorno; la identificación y evaluación de riesgos; la evaluación de controles internos; las evidencias digitales de auditoría; las competencias exigidas a los profesionales contadores públicos y la colaboración de expertos en estos ambientes.

Tal como se indicó en la introducción de este trabajo, la revisión efectuada se refiere no sólo a la literatura disponible, sino también a la normativa de auditoría vigente en la República Argentina aplicable a cada uno de estos aspectos a analizar, la cual se resume en el Cuadro 7.

La Argentina es uno de los pocos países en los cuales rigen diferentes normas para un mismo servicio profesional (Español & Subelet, 2013). Por un lado la Resolución Técnica (RT) Nro. 37 de la Federación Argentina de Consejos Profesionales de Ciencias Económicas (FACPCE) sobre Normas de auditoría, revisión, otros encargos de aseguramiento, certificación y servicios relacionados, y por otra parte, los pronunciamientos emitidos por la *International Federation of Accountants* (IFAC) por medio del *International Ethics Standards Board for Accountants* (IESBA) y el *International Auditing and Assurance Standards Board* (IAASB), que fueron aprobados mediante las RT 32 a 35 por la FACPCE y son de aplicación obligatoria en la auditoría de estados financieros emitidos obligatoriamente bajo *International Financial Reporting Standards* (IFRS) o encargos de revisión sobre estados financieros intermedios de ejercicios anuales auditados con normas internacionales. Para el resto su aplicación es optativa.

Cuadro 7 - 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 o NIA en español), *International Standard on Assurance Engagements* (ISAE o NIEA en español) *e International Education Standard* (IES o NIF en español)	NIA 250 – Consideración de las disposiciones legales y reglamentarias en la auditoría de estados financieros.
		NIA 265 – Comunicación de las deficiencias en el control interno a los responsables del gobierno y a la dirección de la entidad.
		NIA 300 – Planificación de la auditoría de estados financieros.
		NIA 315 (Revisada) – Identificación y valoración de los riesgos de incorrección material mediante el conocimiento de la entidad y su entorno.
		NIA 330 – Respuestas del auditor a los riesgos valorados.
		NIA 402 – Consideraciones de auditoría relativas a una entidad que utiliza una organización de servicios.
		NIA 500 – Evidencia de auditoría.
		NIA 620 – Utilización del trabajo de un experto del auditor.
		NIEA 3000 – Encargos de aseguramiento distintos de la auditoría o de la revisión de información financiera histórica.
		NIEA 3402 – Informes de aseguramiento sobre los controles en las organizaciones de servicios.
		NIF 8 - Competencias profesionales para los socios del encargo responsables por la auditoría de estados financieros.
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.

En el Cuadro 8 se detallan documentos elaborados por organismos profesionales, que si bien no se refieren específicamente a la auditoría financiera y no tienen carácter de vinculante, son recomendaciones elaboradas con base en la opinión y experiencia de profesionales para guiar a las empresas y profesionales frente a los nuevos desafíos que presenta la CN y se reconocen como antecedentes relevantes.

Cuadro 8 - Documentos y recomendaciones relacionadas a la CN considerados en esta tesis

ORGANISMO EMISOR	PAÍS/ REGIÓN	AÑO	ESTÁNDARES Y RECOMENDACIONES
Cloud Security Alliance	USA	2010	*Top Threats to Cloud Computing – Version 1.0.*
		2011a	*Security Guidance for Critical Areas of Focus in Cloud Computing - Version 3.0*
		2011b	*Cloud Compliance Report*: Capítulo en Español de Cloud Security Alliance.
		2013a	*The Notorious Nine: Cloud Computing Top Threats in 2013.*
		2013b	*CSA position paper on AICPA Service Organization Control Reports.*
Committee of Sponsoring Organizations of the Treadway Commission (COSO)	USA	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)	Internacio-nal	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)	USA	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.

2.3.1. CONOCIMIENTO DEL CLIENTE Y SU ENTORNO

A efectos de cumplir con el objetivo de la auditoría de estados financieros, el auditor lleva a cabo un proceso de investigación, destinado a formarse una opinión sobre la razonabilidad de la información contenida en los estados contables, que comprende tres etapas: planificación, ejecución y reporte (Fowler Newton, 2004:6). En la etapa de planificación se definen los procedimientos a aplicar para obtener los elementos de juicio válidos y suficientes que permitan sustentar la opinión y los recursos necesarios para llevar a cabo dichos procedimientos (Slosse, Gordicz & 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 & 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) así como de sus controles internos (NIA 315 (Revisada)), a fin de que el auditor pueda formarse una idea de ciertos riesgos a nivel global, pudiendo evaluar la condición de auditabilidad *(auditability)* del ente (Cansler, Elissondo, Godoy & Rivas, 2007) y ejecutar una auditoría efectiva, fundamentada en evidencias de auditoría más exhaustivas y relevantes (Eilifsen, Knechel & Wallage, 2001).

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, que, si bien puede mejorar la calidad y oportunidad de la información contable, puede generar nuevos riesgos que deben ser evaluados. Se deben identificar y entender los sistemas de contabilidad y control interno[2] (CI) afectados por el ambiente de TI, enfocándose en la importancia y la complejidad de las actividades desarrolladas en dicho ambiente (Astiz & Sole, 2008; Scutella & Barg, 2010).

La importancia del ambiente de sistemas de información computarizados se relaciona con la significatividad de las afirmaciones de los estados contables que se encuentran vinculados al referido proceso (Cansler et al., 2007). La complejidad[3] está determinada por factores como el uso de sistemas desarrollados a medida o con un nivel importante de modificaciones, número significativo de interfaces entre sistemas, sistemas ERP, infraestructuras tecnológicas complejas, operaciones en entornos multinacionales (Astiz & Sole, 2008), aplicación extendida del intercambio electrónico de transacciones con otras organizaciones (EDI), operaciones de negocio implementadas a través del uso de aplicaciones vía *WEB* (por Internet o por redes privadas – intranet/extranet) que implican una fuerte interacción con clientes y proveedores, descentralización

[2] Los sistemas de información relevantes para la información financiera –que incluyen al sistema contable– comprenden, entre otras áreas, los procedimientos y registros, relativos tanto a las tecnologías de información como a los sistemas manuales, mediante los que las transacciones se inician, registran, procesan, corrigen en caso necesario, trasladan al mayor e incluyen en los estados financieros (NIA 315 (Revisada), Apartado 18(b), A89).

[3] El avance de la tecnología es permanente; continúan surgiendo alternativas cada vez más complejas de acuerdo a los criterios mencionados, como es el caso de *blockchain*, definida como un conjunto de ordenadores (o servidores) llamados 'nodos' que, conectados en red utilizan un mismo sistema de comunicación (protocolo) con el objetivo de validar y almacenar la misma información registrada en una red P2P. Si bien su desarrollo es reciente, tiene potencial para ser aplicado en diferentes industrias y sectores económicos. Se espera que su implementación beneficie a la contabilidad, reemplazando la doble contabilización -basada en la documentación respaldatoria de transacciones- por registros compartidos entre las partes, de difícil falsificación o destrucción. Representa en consecuencia un nuevo desafío para la auditoría, requiriéndose una reflexión de sus potenciales efectos no solo desde el punto de vista tecnológico –en la medida en que permitirá verificar grandes cantidades de datos relevantes automáticamente y disminuir tiempos y costos de los encargos, orientándose a otras actividades que agreguen mayor valor– sino también desde los valores, en la medida en que su desarrollo se justifica en parte en la búsqueda de mayor transparencia y trazabilidad de las operaciones (Benitez, 2017; Deloitte, 2016). Existe aquí una nueva oportunidad para el desarrollo de investigaciones referidas a la auditoría financiera en entornos de TI emergentes.

importante de las actividades del sistema de información contable, alta proporción de procesos sustanciales de la organización que se encuentran tercerizados (Cansler et al., 2007), la estructura organizacional y el grado de concentración o segregación de funciones a partir del procesamiento por PC, y la disponibilidad de los datos para su uso a los fines de la auditoría.

La NIA 300 (en su Anexo) menciona que el auditor para planificar el encargo y establecer la estrategia global de auditoría, debe tener en cuenta, entre otras cuestiones, el "efecto de las tecnologías de la información en los procedimientos de auditoría, incluida la disponibilidad de datos y la utilización prevista de técnicas de auditoría asistidas por ordenador".

En esta instancia de evaluación del nivel de informatización del auditado, el contador auditor debería tomar conocimiento del uso que la compañía auditada esté realizando de la computación en la nube, considerando la incidencia que su aplicación pudiera tener sobre los procesos del negocio vinculados a los estados financieros.

De acuerdo a su habilidad y juicio profesional, podrá focalizarse solo en aquella información específica referida al uso de la CN que resulte relevante para su trabajo de auditoría de estados financieros, evitando la recolección de datos innecesarios (Fraser, 2011). Es por ello que considerando la amplitud de aplicaciones que tiene la CN dentro de un ente, es importante detectar en qué casos el uso de la nube por parte del auditado debe llamar la atención del auditor y cuáles son las cuestiones que deben ser evaluadas.

La utilización de servicios en la nube es un caso de utilización de una organización de servicio[4] (OS). Según la NIA 402 (A.1-3), es en la etapa de conocimiento de la entidad y su entorno cuando el auditor debe determinar la importancia de las actividades de la empresa de servicio para la entidad auditada y la relevancia para la auditoría. La Resolución Técnica 37 de la FACPCE (Segunda parte, Sección III.A.i) también se refiere a ello de la siguiente forma:

> **3.** Para poder emitir su opinión sobre los estados contables de un ente o abstenerse de emitirla, el contador debe desarrollar su tarea siguiendo los pasos que se detallan a continuación:
> **3.1.** Obtener un conocimiento apropiado de la estructura del ente, sus operaciones, sistemas, su control interno, las normas legales que le son aplicables y las condiciones económicas propias y las del ramo de sus actividades. **Este conocimiento tiene que permitir identificar, de ser aplicable, el uso de organizaciones de servicios para llevar a cabo total o parcialmente los procesos que tienen un impacto en la información fuente de los estados contables.** (el resaltado es propio)

En este sentido, según la norma internacional, los factores a ser indagados en esta etapa pueden incluir, entre otros:

[4] Una organización externa que presta a la entidad usuaria auditada un servicio que forma parte del sistema de información relevante para su información financiera (Español & Subelet, 2013). Ciertas políticas, procedimientos y registros a cargo de dicha organización pueden tener un impacto material en los procesos que componen el sistema de control interno del cliente y ser pertinentes para la auditoría de estados contables.

- la naturaleza del servicio suministrado y su significatividad para la entidad usuaria. Incluye la contratación de servicios de aplicaciones informáticas que permiten a los clientes procesar transacciones financieras y operativas. En el caso de la nube, una adecuada comprensión del modelo de servicio y distribución adoptado por el ente será fundamental, dado que no solo poseen características propias, sino que pueden representar diferentes tipos de riesgos (ENISA, 2009) que podrían afectar la información financiera;
- la naturaleza y la importancia relativa de las transacciones procesadas, o las cuentas o los procesos de información financiera afectados por la organización de servicios, que determinan la necesidad de obtener conocimiento de los controles de la OS relacionados a las mismas;
- el grado de interacción entre las actividades de la organización de servicios y las de la entidad usuaria; esto es, la medida en que esta última puede implementar controles eficaces sobre el procesamiento realizado por la organización de servicios y decide hacerlo;
- la naturaleza de la relación entre la entidad usuaria y la organización de servicios, incluyendo las condiciones del contrato aplicables a las actividades realizadas por la OS (NIA 402, A. 9, A3, A6, A7, A8).

De los puntos anteriores se deriva que si el auditor concluye que el uso de la CN es significativo para la entidad y pertinente para la auditoría, deberá obtener conocimiento suficiente de la naturaleza y significatividad de los servicios prestados por la organización de servicios (el proveedor) y de su efecto sobre los controles internos de la entidad usuaria que sean relevantes para la auditoría, para identificar y valorar los riesgos de incorrección material, y en consecuencia, diseñar y aplicar procedimientos de auditoría para responder a dichos riesgos (NIA 402, A. 7).

En general, los procedimientos utilizados para obtener un adecuado conocimiento del cliente, su entorno y el control interno que permitan identificar y analizar riesgos significativos comprenden: indagaciones a personas relevantes (la gerencia y otros miembros de la entidad, a criterio del auditor); observación e inspección de procesos y documentación; además del desarrollo de procedimientos analíticos de información financiera y no financiera (Arens et al., 2007; Fraser, 2011; NIA 315 (Revisada), Apartado (A.) 6).

Considerando la intervención de la organización de servicio y su potencial efecto sobre la información financiera, la NIA 402 (IFAC, A.12) prevé procedimientos específicos para el conocimiento de la misma, incluyendo en esta etapa la obtención de los informes sobre el sistema de control interno de la empresa de servicios, así como el contacto y eventual visita a ella.

Tal como fue expresado, en esta etapa el auditor debe comprender el control interno y determinar según su juicio profesional si un control, individualmente o en combinación con otros, es relevante o no para el desarrollo de su trabajo. Cabe destacar que la NIA 315 (Revisada) (A. 13) menciona que cuando se recaba información en relación a los controles internos, el auditor debe evaluar su diseño y si han sido implementados, realizando otros procedimientos además de las

indagaciones al personal de la entidad. Estos aspectos serán analizados en profundidad en el apartado *2.3.3. Evaluación del sistema de control interno*, debido a la importancia que poseen en el caso del ambiente de TI en la nube.

A su vez, el conocimiento del contexto de TI que el auditor obtenga en esta etapa le permitirá determinar si cuenta con los conocimientos específicos requeridos para la realización del encargo, y en caso de que fuera así, estar en condiciones de diseñar el plan de auditoría, dirigirlo o ejecutarlo, y finalmente evaluar el trabajo desarrollado (Cansler et al., 2007). De lo contrario, en esta etapa debe considerar la necesidad de incorporar expertos al equipo de auditoría que lo complementen en las materias específicas que estén fuera de su alcance. Estas cuestiones serán tratadas en el apartado *2.3.5. Competencias profesionales del auditor financiero. Intervención de expertos en tecnología de la información.*

El Cuadro 9 resume los conceptos introducidos en este apartado, proponiendo el conjunto de categorías consideradas para la elaboración del instrumento de recolección de datos –tal como se describe en el *Capítulo 3. Metodología* – y para el análisis de los resultados producidos por la tesis en relación al tópico de Conocimiento del cliente y su entorno. Se complementa el esquema conceptual para la investigación propuesto en la Figura 1, ampliando los conceptos relevantes.

Cuadro 9 - Conocimiento del cliente y su entorno

<table>
<tr><th>TÓPICO</th><th>CATEGORÍAS</th><th colspan="2">SUBCATEGORÍAS</th></tr>
<tr><td rowspan="8">CONOCIMIENTO DEL CLIENTE Y SU ENTORNO

Uso de una organización de servicios para la prestación de servicios de TI</td><td rowspan="6">ASPECTOS</td><td rowspan="5">CLIENTE Y SU ENTORNO</td><td>Sistemas de Contabilidad y CI afectados por la TI (importancia y complejidad)</td></tr>
<tr><td>Naturaleza y significatividad del servicio contratado a la OS
• Modelo de servicio de CN
• Modelo de distribución de CN</td></tr>
<tr><td>Naturaleza e importancia de transacciones/cuentas/procesos afectados por la OS</td></tr>
<tr><td>Grado de interacción entre actividades de la OS y entidad auditada (controles complementarios)</td></tr>
<tr><td>Naturaleza de la relación y condiciones de la contratación con la OS</td></tr>
<tr><td>CONTROL INTERNO</td><td>Tratado en el apartado 2.3.3.</td></tr>
<tr><td rowspan="5">PROCEDIMIENTOS</td><td colspan="2">Indagaciones a personas relevantes</td></tr>
<tr><td colspan="2">Observación e inspección de procesos</td></tr>
<tr><td colspan="2">Observación e inspección de documentación</td></tr>
<tr><td colspan="2">Procedimientos analíticos sobre la información</td></tr>
<tr><td colspan="2">Contacto y eventual visita a la OS</td></tr>
</table>

Fuente: Elaboración propia.

2.3.2. IDENTIFICACIÓN Y VALORACIÓN DE RIESGOS

A) La evaluación de riesgos en la auditoría de estados financieros.

A partir del conocimiento del cliente, el auditor financiero estará en condiciones de evaluar el riesgo de negocio[5], que implica comprender las condiciones –internas y del contexto– que amenazan la habilidad de la organización para ejecutar los procesos y alcanzar sus objetivos.

El siguiente paso consiste en realizar una evaluación preliminar del riesgo de *auditability*, que puede estar dado por las características del ente, por la naturaleza del negocio, deficiencias graves de control interno, o imposibilidad de planear y ejecutar su trabajo de manera tal de obtener una seguridad razonable de que los estados financieros no contengan errores o irregularidades.

Dentro del conjunto de riesgos del negocio, el profesional debe identificar los *riesgos significativos*, esto es, aquellos que representan posibles errores materiales en los estados financieros y requieren una consideración especial de auditoría (NIA 315 (Revisada), A. 25, 27).

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) (Casal, 2013; Fowler Newton, 2004:525; NIA 315 (Revisada), A.25). El modelo de riesgo en auditoría (riesgo de emitir una opinión profesional distinta a la que correspondería) 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.

En la medición de los riesgos inherente y de control se debe considerar a la tecnología de información como un factor importante, en la medida en que incorpora amenazas que no estaban presentes en los entornos manuales, tales como ausencia de rastros de transacciones, falta de segregación de funciones o la generación automática de transacciones y registraciones por el ordenador (Minguillón, 2006; Oggero, 2006).

La NIA 315 (Revisada) (A. A39, A63, Anexo 2) reconoce ciertos riesgos específicos derivados de la informática para el control interno de la entidad, agregando riesgos de confianza en sistemas que procesan datos de manera inexacta y/o datos inexactos, accesos no autorizados a los datos, cambios no autorizados en los datos de archivos maestros o en los sistemas, pérdida potencial de los datos o incapacidad de acceder a ellos del modo requerido, entre otros. Todos ellos pueden indicar la existencia de riesgos de incorrección material en los estados financieros.

---

[5] La literatura actual así como las normas y estándares profesionales internacionales (en particular la NIA 315 (Revisada)) 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 (Mantilla Blanco & Casal, 2012; Schultz, Bierstaker & Donell, 2010); por el contrario, según Casal (2013) no se puede afirmar que las normas argentinas (actual RT 37 y anterior RT 7) necesariamente provean lineamientos a ese fin.

Por su parte, 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 (Casal, 2013; Minguillón, 2006).

Fronti de García y Suárez Kimura (2008) resumen tres grupos de riesgos asociados a la TI con los cuales podrá enfrentarse el auditor externo: a) *riesgos de infraestructura de tecnología* (adecuación de la misma para el procesamiento de información desde el punto de vista de la seguridad: inadecuadas políticas vinculadas a robos de información, accesos no autorizados, vulnerabilidad a riesgos físicos, inadecuados procedimientos de resguardo de la información); b) *riesgos de las aplicaciones* (errores, cambios no documentados, mal diseño de controles de entrada/procesamiento/salida de información, etc.); c) *riesgos vinculados con los procesos de negocio* (referidos a las definiciones propias del negocio, vinculados a una falta de integración de los sistemas puestos en marcha en la empresa, interfaces deficiente entre los sistemas vinculados, inexistencia de una secuencia trasparente en el manejo de los datos). Todos ellos afectan la labor del auditor, quien deberá evaluar la significatividad de los problemas de control detectados y sus consecuencias patrimoniales.

B) Los riesgos de la computación en la nube. Diseño de una *Risk Breakdown Structure* para la auditoría de estados financieros en entornos de CN.

En la literatura diversos autores han documentado los potenciales riesgos del uso de la CN, siempre desde la perspectiva de la entidad usuaria. Esto resulta importante, dado que al momento de considerar la utilización de la computación en nube (u otras infraestructuras y tecnologías de información) es imprescindible realizar un análisis adecuado de los riesgos asociados a su implementación, de modo de garantizar resultados satisfactorios como consecuencia de su uso y la sostenibilidad de su utilización dentro de una organización en el tiempo (Holzmann & Spiegler, 2011; Islam, Fenz, Weippl & Mouratidis; 2017).

Entre la bibliografía disponible, ENISA (2009) elaboró un detalle de 35 riesgos clasificados en riesgos de política y organización (incluyendo riesgos de *lock-in* –que representa 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 (2010, 2013a) identificó 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.

Brender y Markov (2013), resumen los principales riesgos de la nube desde una perspectiva de la gestión, considerando fuentes de riesgos vinculados a la seguridad de la información, el cumplimiento de la regulación, la localización de los datos, soporte a investigaciones, *lock-in* y recuperación de desastres. A su vez, en su estudio sobre cinco empresas suizas encuentran que existe un nivel adecuado de concientización sobre los riesgos involucrados en la migración a la nube, y profundizan en el análisis de factores de riesgo a ser considerados.

A partir del relevamiento realizado en la literatura, se resumen a continuación los principales factores de riesgo vinculados a la utilización de la CN, mediante una herramienta denominada *Risk Breakdown Structure* (RBS) (Hillson, 2002a, 2002b; Holzmann & Spiegler, 2011; Project Management Institute (PMI), 2008), conocida en español como Estructura de Desglose de Riesgos[6].

Consiste en un método de identificación de riesgos estructurado que permite el reconocimiento de patrones de exposición a eventos contingentes que podrían afectar a una organización en el cumplimiento de sus objetivos o proyectos. Los mismos son categorizados de acuerdo a sus fuentes, realizándose una descripción jerárquica que facilita la identificación, evaluación y comprensión global de los riesgos. Cada nivel inferior dentro de la estructura representa una definición con un creciente grado de detalle (Hillson, 2002a). El *Project Management Institute* (2008) la define como una descripción jerárquica de riesgos, organizados por categorías y subcategorías que identifican las distintas áreas de posibles eventos contingentes.

En la elaboración de la RBS se siguió la propuesta de Holzmann y Spiegler (2011) de utilizar una metodología *bottom-up* (en oposición a la denominada *top-down*), agrupando los riesgos individuales identificados en la bibliografía en áreas que incluyan los que corresponden a una misma fuente. Para elaborar el modelo se realizó una revisión bibliográfica a partir de la cual han sido obtenidas descripciones de riesgos desarrolladas por múltiples organismos y autores. Los principales aportes se obtuvieron de los trabajos de Armbrust et al. (2009), Brender y Markov

[6] El trabajo de López, Albanese y Sanchez (2014) presenta el diseño de una *Risk Breakdown Structure* para la identificación y descripción jerárquica de las fuentes de riesgos vinculados con la implementación de la computación en nube en entidades financieras de la República Argentina. En el mismo se consideran las categorías de riesgos definidas por la normativa del Banco Central de la Republicar Argentina (Comunicación A4609): estratégicos, reputacionales, legales, operacionales.

(2013), CSA (2010), ENISA (2009), Holzmann y Spiegler (2011), ISACA (2009), Montahari et al. (2009), Mowbray (2009), Svantesson y Clarke (2010), entre otros.

La organización de los riesgos se realizó sobre la base de la *Risk Breakdown Structure* expuesta en el Cuadro 10. En el proceso de categorización, existe un nivel superior, el Nivel Cero, en el cual todo riesgo es simplemente Riesgo de la utilización de la CN. Luego, en el Nivel Uno, se determinan las categorías de fuentes de riesgo relevantes, en las que se incluyeron riesgos derivados del proceso de implementación aplicado por el ente; riesgos derivados de la tercerización; riesgos técnicos; riesgos legales; riesgos contra la seguridad física. Cada una de ellas puede a su vez subdividirse en subcategorías con mayor grado de detalle en el Nivel Dos, y así sucesivamente en niveles inferiores, llegando a la definición de cada uno de los factores de riesgos identificados.

A continuación se justifica la selección de las fuentes de riesgos consideradas:

- **Riesgos derivados del proceso de implementación aplicado por el ente:** la implementación de un servicio en la nube para la gestión del negocio, y para la elaboración de información financiera en particular, requiere de un proceso de decisión y adecuación, que considere no solo los potenciales beneficios que el uso de la nube reportaría para el ente, sino también los riesgos asociados, debiendo respetarse los procedimientos previstos en el ente para la implementación de nuevos sistemas. La falta de dicho proceso, así como de la autorización del uso por parte de los niveles adecuados, puede implicar el riesgo de que los sistemas de información y tecnologías asociadas no respondan a las necesidades de la entidad o no se encuentren alineados con los planes estratégicos de la misma (BCRA, 2006).

Sin planes definidos que respondan a las contingencias y los objetivos de largo plazo de la organización, con aporte y consentimiento de los sujetos involucrados, y adecuados presupuestos y cronogramas de ejecución, es muy difícil que se logre aprovechar el potencial de la arquitectura para la gestión de la información. A su vez es fundamental la definición previa de la estructura organizativa, con una identificación clara de los roles y responsabilidades involucrados en el proceso. Una incorrecta separación y definición de funciones, las incompatibilidades entre ellas y la inexistencia de controles por oposición de intereses pueden llevar al fracaso del proceso de implementación (López et al., 2014).

- **Riesgos propios de la tercerización:** la abstracción entre la infraestructura física y la información de la organización, propia de la computación en la nube (a diferencia de los modelos tradicionales, en los que el propietario de los datos tiene el control de la componente informática que los puede afectar) indica que está dividida la responsabilidad entre el usuario y el prestador del servicio, ya que las empresas transfieren el control de la infraestructura y de los procesos de seguridad a terceros, debiendo implementarse medidas efectivas para el aseguramiento (Sepúlveda, Salcedo & Gómez Vargas, 2010).

A medida que las empresas trasladan sus ambientes informáticos a la nube, 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 (RSA, 2009). El control compartido plantea interrogantes sobre la responsabilidad. Siendo la información el activo más preciado del núcleo de negocios de las organizaciones, es necesario que se tomen las medidas necesarias para evitar inconvenientes derivados de la tercerización.

- **Riesgos técnicos:** resulta de especial interés para el auditor la utilización de archivos adecuados y seguros que permitan la reconstrucción de la historia y el reproceso de las transacciones importantes (Fowler Newton, 2004). Sin embargo, la guarda de información en archivos electrónicos genera un riesgo de pérdida de información que podría aumentar las posibilidades de error en los estados financieros, e incluso la organización podría verse expuesta a serias interrupciones en el negocio (Arens et al., 2007). Se incluyen aquí dos grupos de factores de riesgos:

a) riesgos de continuidad: riesgos asociados a la disponibilidad, resguardo (*back up*) y medidas de recuperación ante desastres de un sistema (Hunton et al., 2004:50). La disponibilidad se refiere a que los sistemas de información sean accesibles para los usuarios; de modo que las fallas de los sistemas que generan interrupciones en la prestación del servicio –temporarias o permanentes– afectan el acceso a la información cuando es requerida, generando interrupciones, errores o dificultades para el procesamiento de las operaciones. La disponibilidad de los servicios en la nube es esencial, principalmente para los procesos de negocio críticos (Brender & Markov, 2013). Los procedimientos de *back up* y recupero de desastres aseguran que, en caso de interrupción del servicio, existen las medidas que permitan recuperar los datos y operaciones;

b) riesgos de seguridad: incluyen los riesgos asociados al acceso a los datos y la integridad (Hunton et al., 2004:50). Se refiere a las fallas en la seguridad que permiten el acceso a los datos por parte de terceros, comprometiéndose la seguridad y privacidad de la información y los sistemas, corriéndose riesgo de pérdida o modificación no autorizada de datos (ENISA, 2009).

Con frecuencia los sistemas de contabilidad basados en TI permiten el acceso en línea a la información en archivos maestros y otros registros guardados electrónicamente; el ingreso a través de Internet en forma remota incrementa la posibilidad de un acceso ilegítimo, de modo que si no existen restricciones apropiadas, como contraseñas e identificaciones de usuarios, se podrían emprender actividades no autorizadas, generando cambios inapropiados en los programas de *software* y los archivos maestros, además de la posibilidad de que se obtenga información de carácter confidencial sin permiso (Arens et al., 2007).

Este riesgo está previsto en la NIA 315 (Revisada) (A. A63), la cual reconoce que el acceso no autorizado a la información puede provocar destrucción de datos, cambios inapropiados, incluso el registro de operaciones no autorizadas o inexistentes, o el registro inexacto de operaciones, pudiendo surgir riesgos específicos si múltiples usuarios tienen acceso a una base de datos común.

Los daños pueden darse por ataques directos orientados a un blanco de información sensible concentrada en la nube, o indirectamente, como daño colateral por ataques a la información de otros usuarios alojada en el mismo lugar que la del ente en cuestión.

Desde el punto de vista de las organizaciones, la seguridad es una preocupación importante respecto de la nube (Brender & Markov, 2013), llegando a ser uno de los principales obstáculos para su implementación generalizada (Ali et al., 2015).

Los datos en la nube son más vulnerables a los riesgos en términos de confidencialidad, integridad y disponibilidad en comparación a los modelos convencionales de TI (Ali et al., 2015). Siendo que los datos son el principal insumo para la elaboración de estados financieros, objeto del trabajo del auditor externo, se espera que éste se interese especialmente en las medidas de control que se apliquen sobre estos riesgos.

- **Riesgos legales:** comprenden, entre otros aspectos, la exposición a sanciones, penalidades u otras consecuencias económicas y de otra índole por incumplimiento de normas y obligaciones contractuales (BCRA, 2008). Dichas sanciones podrían provenir de las mismas normas incumplidas, de las pautas de contratos o de sentencias dictaminadas por jueces frente a demandas o juicios que se hubieran iniciado en contra de la entidad y cuyas resoluciones hubieran resultado adversas a sus intereses. El marco normativo al que está sujeta una entidad comprende un conjunto de disposiciones legales y reglamentarias con efectos muy variados sobre los estados financieros; en algunos casos las consecuencias pueden ser materiales, por ejemplo si dan lugar a multas, litigios y otros similares (NIA 250, A. 2).

Éste es uno de los riesgos que usualmente se ven afectados por el uso de la TI, referido al incumplimiento de la normativa aplicable al ente en cuestión, y que suele ser preocupante en el caso de aplicación de nuevas tecnologías, como lo es la computación en la nube. En parte esto se debe a que, aun cuando existen esfuerzos por adaptar la normativa a los avances tecnológicos, en general ocurre un desfase temporal y una desarticulación entre lo que la normativa acepta y lo que los nuevos medios tecnológicos ofrecen para el procesamiento electrónico de datos (Suárez Kimura, 2007).

A pesar de la implementación de la tercerización, la responsabilidad última de cumplimiento de las leyes y normas es del usuario (NIA 250, A. 3), siéndole aplicables las sanciones por incumplimiento (Brender & Markov, 2013). En consecuencia, las organizaciones deben estar atentas para revisar las obligaciones de cumplimiento de la regulación tanto local como de los países donde se procesarán los datos en caso de uso de la CN (Gonzalez & Piccirilli, 2013).

Esta es una cuestión a la que el auditor financiero no escapa en la ejecución de su labor. Él debe procurar identificar las incorrecciones materiales en los estados financieros como consecuencia de incumplimientos de la normativa, si bien no es responsable de prevenirlos, a la vez que es posible que no los detecte en su totalidad (NIA 250, A. 4).

En relación a la CN, en su trabajo deberá evaluar, por ejemplo, el correcto cumplimiento de lo impuesto en relación a la formalidad de los libros de comercio y los medios de procesamiento permitidos por la normativa Argentina, incluyendo el Código Civil y Comercial de la Nación (arts. 322, 323, 325), la Ley General de Sociedades Comerciales (art.61) y normas específicas de entes reguladores como ser la Inspección General de Justicia en Capital Federal, el Banco Central de la República Argentina, entre otros.

- **Riesgos contra la seguridad física:** se incluyen aquí los riesgos de acceso no autorizado de tipo físico (Hunton et al., 2004:50), dado que el de tipo lógico se incluyó en los riesgos técnicos vinculados a la seguridad. A su vez, los riesgos relacionados a desastres naturales diversos que podrían afectar a los recursos físicos que dan soporte al servicio en la nube. Aun cuando la probabilidad de estos eventos es baja, en la medida en que los recursos físicos generalmente están bien protegidos, su impacto puede ser alto (Brender & Markov, 2013).

En general, se entiende que los riesgos de desastres naturales cuando se implementa *cloud computing* son menores comparados con las infraestructuras tradicionales, porque los proveedores ofrecen sitios redundantes para las aplicaciones y el almacenamiento de información. Finalmente, las condiciones ambientales inadecuadas no solucionadas por el proveedor son fuentes de potenciales daños y pueden afectar la integridad de los activos físicos (López et al., 2014).

Tal como puede apreciarse, en este caso se propone una *RBS Genérica*, aplicable a cualquier tipo de organización. La propuesta de esta herramienta se considera interesante dado que en algunos casos la visualización de los riesgos a un solo nivel – en un listado, por ejemplo –no brinda información útil para la toma de decisiones y para la evaluación de riesgos de una auditoría en particular. Es por ello que el ordenamiento en tantos niveles como sean necesarios siguiendo una estructura como la descripta brinda la flexibilidad necesaria para realizar distintos tipos de análisis.

Sin embargo, aún es necesario realizar un análisis acerca de la importancia que cada uno de esos factores de riesgos tienen para la auditoría financiera, en la medida en que no se han encontrado estudios o recomendaciones en relación a qué riesgos de la CN –dentro del conjunto aquí descripto– son realmente *significativos* en los términos de la NIA 315 (Revisada).

En consecuencia, se requeriría analizar cada uno de los *riesgos inherentes* a la utilización de la nube e identificar cuáles tienen mayor relevancia para la auditoría de los estados financieros. A su vez, en el caso de una auditoría en particular, a partir de la revisión de los controles implementados por la organización se deberá evaluar el *riesgo de control*, para en definitiva estimar el riesgo de auditoría y la condición de auditabilidad del ente, en función de lo cual se debe decidir si se está en condiciones de realizar el trabajo o si ante las importantes fallas en los controles debe ser rechazado porque no es posible llevar adelante la auditoría. Una vez contratado, esta evaluación servirá al auditor para la planificación del trabajo a realizar, en la definición del enfoque a aplicar.

Cuadro 10 - Riesgos de la CN

TÓPICO	CATEGORÍAS	SUBCATEGORÍAS	
NIVEL 0	**NIVEL 1 - FUENTES DE RIESGO**	**NIVEL 2 - FACTORES DE RIESGO**	**AUTORES**
RIESGO DE LA UTILIZACIÓN DE LA CN	**RIESGOS DERIVADOS DEL PROCESO DE IMPLEMENTACIÓN DE LA CN POR EL ENTE**	**Falta de planificación en el proceso de implementación (*Due Dilligence* insuficiente):** Aplicación de soluciones de CN sin una adecuada planificación, comprensión e investigación del servicio y sus características, considerando sólo sus potenciales beneficios. Ello conlleva el riesgo de que los sistemas de información y tecnologías aplicados no respondan a las necesidades de la entidad o no se alineen a sus planes estratégicos, siendo difícil aprovechar el potencial de la arquitectura para la gestión de la información, asumiéndose niveles de riesgo desconocidos para la entidad.	CSA (2013a); Svantesson & Clarke (2010: 395)
		Actividad no autorizada en la nube: las unidades de negocio o empleados del ente pueden contratar y utilizar servicios en la nube sin solicitar autorización a superiores o para actividades no autorizadas, evitando procedimientos tradicionales de revisión y aprobación. Ello es posible debido a que las adquisiciones de servicios CN representan gastos operativos de bajo monto en vez de inversiones en capital.	COSO (2012:13); ISACA (2012:8)
		Falla en la adecuación de la estructura organizacional: el ente omite adecuar la estructura para la aplicación de la nube; el uso de esta alternativa de TI puede requerir reducción del personal del área de TI, capacitación del personal, redefinición de roles y responsabilidades, separación de funciones, aplicación de controles por oposición de intereses; puede generar el fracaso del proceso de implementación, confusión de roles, problemas de privacidad y protección de la información, demoras en proyectos, costos más elevados, suministro de información incompleta a directivos para la toma de decisiones, falta de claridad en la determinación de roles y responsabilidades del proveedor, afectación de la moral y dedicación del personal del área de TI remanente.	Brender & Markov (2013); COSO (2012:5); ISACA (2012:8)
	RIESGOS PROPIOS DE LA TERCERIZACIÓN	**Pérdida de gobernabilidad por parte del usuario:** transferencia al proveedor (y sus subcontratados) del control sobre ciertas actividades, procesos, información, activos y componentes del sistema. Puede afectar la seguridad de la información, la calidad y eficiencia con que los procesos son llevados a cabo, el cumplimiento de requisitos y expectativas del usuario respecto de sus	Ali et al. (2015); Brender & Markov (2013); COSO (2012:14); ENISA (2009); Jamil & Zaki (2011: 3479); Jansen & Grance (2011: 12);

		controles internos.	Montahari et al. (2009)
		Viabilidad del proveedor: la interrupción de las operaciones del proveedor (cierre o quiebra) o la restructuración del servicio (fusión o absorción del proveedor, redefinición de la oferta de servicios) pueden generar una interrupción del servicio utilizado por el ente o modificación de las condiciones originales de contratación. Puede implicar para el ente usuario la pérdida o deterioro del rendimiento y calidad del servicio obtenido, la pérdida de la inversión realizada para la implementación, el deterioro de su capacidad para cumplir con sus funciones y obligaciones con sus propios clientes y empleados, pudiendo generarle responsabilidad contractual por negligencia del proveedor.	Armbrust et al. (2010:54); Brender & Markov (2013), COSO (2012: 5); ENISA (2009); Montahari et al. (2009)
		Vinculación al proveedor (*Lock in*): una vez contratado el servicio se genera cierta dependencia con el proveedor elegido, existiendo dificultades para migrar los datos y programas de un prestador a otro o volver al entorno de TI interno (propio de la entidad). Puede implicar cambios unilaterales en las condiciones contratadas por parte del proveedor, no sujetas a negociación, por ser él quien posee el control de los datos (por ejemplo, ajustes unilaterales a las tarifas)	Armbrust et al. (2010); Brender & Markov (2013); COSO (2012:4); ENISA (2009); Jamil & Zaki (2011:3479); Mowbray (2009:11); Nicoloau et al. (2012); Sultan (2011); Svantesson & Clarke (2010)
		Falta de transparencia: el proveedor no suele divulgar información detallada sobre sus sistemas, procesos, operaciones, controles y medidas de seguridad. Ello implica que el cliente encuentra dificultades para verificar los sistemas, comprobar de manera eficaz las prácticas de gestión de datos del proveedor, con la posible imposibilidad de realizar evaluaciones de confiabilidad, *tests* sobre controles, monitoreo de actividades.	COSO (2012:4,13); ENISA (2009); Jamil & Zaki (2011:3479); Mowbray (2009)
		Incumplimiento de requisitos de certificaciones: el ente usuario podría perder una certificación obtenida si el proveedor no está en condiciones de prestar un servicio adecuado a los requerimientos de dicha certificación (sea porque no los cumple o porque los cumple pero no permite su verificación).	ENISA (2009)

		Reputación compartida: la existencia de recursos compartidos (recursos físicos y virtuales, que pertenecen al proveedor y que sirven a muchos usuarios a partir de su asignación dinámica de acuerdo a su nivel de demanda) implica que cualquier error o actividad malintencionada cometida por el proveedor u otros usuarios puede tener efectos negativos sobre el desempeño e imagen del ente.	Armbrust et al. (2010:58); Brender & Markov (2013); COSO(2012:4); ENISA (2009)
	RIESGOS TÉCNICOS	**Insuficiencia de recursos (sub-aprovisionamiento):** interrupción temporal en la prestación del servicio, sea por imposibilidad del proveedor de brindar en nivel de servicio comprometido (por ejemplo, por errores en las proyecciones estadísticas utilizadas para la asignación de recursos a demanda de los usuarios) o por acciones de un atacante que impidan el uso del servicio otorgando niveles finitos de recursos (memoria, espacio en disco, ancho de banda) insuficientes para la demanda del usuario.	Armbrust et al. (2010: 54); COSO (2012:4); CSA (2013a); ENISA (2009); Mowbray (2009:5-6)
		Fallas de la conexión a Internet: vulnerabilidades de la red (pérdida de conexión, uso no óptimo, baja velocidad o congestión en la transferencia de datos): pueden generar interrupciones, errores o dificultades para el procesamiento de operaciones, inutilizando el servicio, con consecuencias sobre la eficiencia y productividad del negocio.	ENISA (2009); Jansen & Grance (2011:11); Miller (2008) ; Yigitbasioglu (2015)
		Fallas de los mecanismos de aislamiento de la información: error de la separación lógica de los usuarios, generando una pérdida de identificación de los datos ubicados en los recursos compartidos. Puede verse comprometida la seguridad por la confusión de información de diversos usuarios, la exposición al acceso de terceros no autorizados, la pérdida de datos sensibles, la interrupción del servicio. Algunos servicios ofrecidos prevén un aislamiento completo de los datos asegurando la privacidad, a diferencia de la nube de primera generación, en la que los datos de diferentes empresas coexistían en la misma base de datos.	Ali et al. (2015); Brender & Markov (2013); CSA (2010); ENISA (2009); ISACA (2009); Jansen & Grance (2011:11); Mansfield (2008:10); Mercado, (2013:191); Mowbray (2009)
		Empleado malicioso: abuso de una situación de privilegio por parte de empleados del proveedor (o de sus subcontratados), administradores de sistemas, auditores, entre otros, mal utilizando su posibilidad de acceso a los sistemas y datos de los usuarios. Pueden generar daños en la confidencialidad, integridad o disponibilidad de la información o los sistemas, daños a la imagen, pérdidas financieras, alteraciones de producción, etc.	Brender & Markov (2103); CSA (2010, 2013a); ENISA (2009); Mowbray (2009:12);
		Fuga/Interceptación de datos en tránsito:	Brender &

		siendo la computación en nube una arquitectura distribuida, implica que existe una mayor cantidad de datos en tránsito que en las infraestructuras tradicionales para que puedan ser transferidos ente los servidores de la nube y los clientes *web* remotos. Tal nivel de movilización incrementa los riesgos de interceptación de datos en tránsito y la fuga de datos, pudiendo la información del ente caer en manos de terceros, comprometiendo la confidencialidad, privacidad e integridad.	Markov (2013); CSA (2010, 2013a); COSO (2012:5); ENISA (2009); Montahari et al. (2009); Mowbray (2009:12)
		Eliminación de datos insegura o no efectiva: la información del ente puede estar disponible más allá de la vida útil especificada en sus políticas de seguridad, en la medida en que la eliminación de datos solicitada puede no ser completa, sea por imposibilidad práctica o por interés del proveedor en conservar dicha información para algún otro fin.	Ali et al. (2015); Brender & Markov (2013); ENISA (2009); Jamil & Zaki (2011:3480)
		Acceso a través de navegadores de Internet conocidos: las debilidades de los navegadores *web* son conocidas, pudiendo darse ataques convencionales sobre los servicios basados en la nube.	Ali et al. (2015); Brender & Markov (2013); Kaufman (2009); Mansfield (2008)
		Problemas de gestión de la identidad y claves de encriptado: las contraseñas**,** claves secretas o datos de encriptado pueden ser divulgadas, corrompidas, robadas o perdidas, impidiendo el acceso del ente usuario a su propia información; a su vez, si caen en manos de terceros, estos pueden hacer un uso indebido de ellas para la autenticación y el no repudio (firma digital), permitiéndoles afectar las actividades del usuario, manipular o falsificar datos, re-direccionar a los clientes del usuario a sitios ilegítimos, convirtiendo la cuenta del ente en una base para la realización de sus fraudes. Se compromete la confidencialidad, integridad y disponibilidad de los servicios y la información.	Ali et al. (2015); CSA (2010, 2013a:8,9); ENISA (2009)
	RIESGOS LEGALES	**Cambio de jurisdicción:** el posible desconocimiento de la localización exacta de los datos y su posible localización en jurisdicciones con marcos jurídicos inestables y normativas impredecibles que no respeten acuerdos internacionales, puede implicar que éstos queden sujetos a divulgación forzada, sean objeto de incursiones de las autoridades locales o secuestro por la fuerza.	Ali et al. (2015); Brender & Markov (2013); COSO, (2012: 14,19); ENISA (2009); Mowbray, (2009:5); Svantesson & Clarke (2010); Yigitbasioglu (2015)
		Determinación de la legislación y autoridad competente en caso de conflicto: usuario y proveedor del servicio pueden residir en jurisdicciones diferentes. La	Ali et al. (2015); Brender & Markov (2013)

		determinación de una corte en la localización del usuario facilita el conocimiento de la legislación, pero una de la localización del proveedor facilita la aplicabilidad de la resolución judicial (a riesgo de desconocer la normativa aplicable al ente y los procedimientos judiciales aplicables).	
		Confiscación judicial: el secuestro de *hardware* físico por orden judicial (incluso cuando fuera legítima) implica un perjuicio para los usuarios que no son objeto de las acciones represivas, como interrupción del servicio o revelación de sus datos a personas no deseadas.	Armbrust et al. (2010:58); COSO (2012:19); ENISA (2009); Mowbray (2009:4)
		Requisitos de los sistemas de información: incumplimiento de normas vigentes en la jurisdicción asiento del usuario que impongan condiciones que fueran incompatibles con el uso de la CN para el procesamiento o almacenamiento de información contable (por ejemplo por exigir la identificación de los servidores donde se encuentran los datos de un ente lo cual puede no ser posible).	COSO, (2012); ENISA (2009); ISACA (2009); Kaufman (2009:65); Mowbray (2009:9); Svantesson & Clarke (2010)
		Revelación de cuestiones sobre controles internos: incumplimiento de obligaciones de entidades públicas que deben revelar cierta información sobre sus controles y se ven imposibilitadas de hacerlo en caso de falta de información sobre los controles del proveedor.	COSO (2012)
		Protección de datos y confidencialidad: la eventual divulgación de datos personales, sea por negligencia o dolo del proveedor, incumpliendo normas de seguridad, confidencialidad y privacidad de la información, incluso sin que sea conocido por el usuario, lo expone a potenciales situaciones litigiosas y sanciones por su carácter de responsable y controlador de los datos.	CSA (2010, 2013a); COSO (2012:5,14); ENISA (2009); Gonzalez & Piccirilli, (2013); ISACA (2009); Mansfield (2008:10); Sultan (2011); Svantesson & Clarke (2010); Yigitbasioglu (2015)
		Protección de la propiedad intelectual: riesgo de falta de protección de aplicaciones originales creadas y ejecutadas en la nube por el usuario.	ENISA (2009); ISACA (2009)
	RIESGOS CONTRA LA SEGURIDAD FÍSICA	**Acceso físico no autorizado a instalaciones y edificios:** falla en la seguridad física aplicada por el proveedor que permite el acceso a instalaciones y el consecuente robo o destrucción de equipamiento, *software*, información, copias de seguridad, etc.	Brender & Markov (2013); ENISA (2009)

		Desastres naturales: terremotos, incendios, inundaciones y otro tipo de eventualidades de naturaleza similar que pueden afectar la integridad de los activos físicos propiedad del proveedor del servicio en donde se encuentran alojados los sistemas e información del ente.	Brender & Markov (2013); ENISA (2009)

Fuente: Elaboración propia.

2.3.3. EVALUACIÓN DEL SISTEMA DE CONTROL INTERNO

El entendimiento de la entidad y su entorno para la identificación y valoración de riesgos de incorrección material, incluye, de acuerdo a lo indicado por la NIA 315 (Revisada) (A. 1), la comprensión del control interno de la entidad. El auditor debe tomar conocimiento del *control interno relevante para la auditoría*, esto es, aquellos que a su criterio son necesarios para hacer frente a los riesgos de distorsiones significativas en las afirmaciones de los estados contables; el hecho de que un control sea o no relevante para la auditoría es una cuestión de juicio profesional (NIA 315 (Revisada), A. 12, A67 a A71). En particular se debe comprender la manera en que el ente ha dado respuesta a los riesgos derivados de la TI.

El auditor debe entonces evaluar los controles que sirven para prevenir, detectar o corregir los errores en la información financiera (Casal, 2011; Presa, 2013), definir el riesgo de control –la probabilidad de que errores contenidos en los estados financieros no sean evitados o detectados por el sistema de control interno del ente (Cansler et al., 2007)– y determinar, de acuerdo al nivel de confianza que pueda depositar en el sistema de control interno, el enfoque de auditoría a aplicar – de cumplimiento o sustantivo (Nannini et al., 2011; NIA 330).

A partir de la incorporación de la TI en los sistemas de contabilidad de las organizaciones, los sistemas de control interno se han optimizado por diversas razones: complementando o reemplazando a los controles manuales; mejorando la oportunidad, disponibilidad, calidad y razonabilidad de la información; incrementando la posibilidad de lograr una efectiva segregación de funciones mediante la implementación de controles de seguridad en aplicaciones, bases de datos y sistemas operativos (Arens et al., 2007; Pastor, 2011).

En consecuencia, en entornos informatizados se incrementa la importancia de la revisión del sistema de control interno para la auditoría financiera (Hunton et al., 2004). En la etapa de la planificación esto implicará considerar los riesgos tecnológicos que pudieran afectar la integridad y exactitud de los datos (Astiz & Sole, 2008) y los controles que los mitiguen. Si es posible confiar en dichos controles, se logran economías en el desarrollo de la auditoría debido a la reducción del alcance del trabajo (Hunton et al., 2004). En un entorno de TI basado en la CN esto pareciera ser sumamente relevante.

En primer lugar, se debería realizar una evaluación preliminar de la estructura de control interno, para identificar y comprender los controles clave para la auditoría financiera. En esta

instancia, se obtiene información referida al funcionamiento teórico de los controles, esto es, su diseño e implementación, y se define el nivel de riesgo preliminar, considerando el grado de confianza que el profesional podría depositar en el sistema de control interno (Fowler Newton, 2004; Minguillón, 2006). La consideración del diseño implica verificar si un control, individualmente o en conjunto con otros sería capaz de prevenir o detectar y corregir distorsiones significativas de manera efectiva, mientras que la implementación significa que el control existe y que la entidad lo está utilizando; el diseño es evaluado en primer lugar, dado que no resulta útil evaluar la implementación de un control que no sea eficaz (NIA 315 (Revisada), A.13, A73).

En función de ello, el auditor decide si es conveniente continuar con el testeo de los controles para verificar su funcionamiento real, mediante pruebas que permitan evaluar su eficacia operativa para prevenir, detectar y corregir errores materiales en los estados financieros (Fowler Newton, 2004; NIA 315 (Revisada), A. A75; NIA 330, A. 7-17; Pastor, 2011).

Ejecutadas las pruebas de controles el auditor obtendrá evidencia comprobatoria relativa a la eficiencia y eficacia de los controles y su real funcionamiento, y determinará el nivel de riesgo de control, resolviendo si decide confiar en ellos o no. Si el mismo es bajo podrá aplicar un enfoque de confianza en los controles, elaborándose el programa de auditoría estableciendo el riesgo de detección planificado (Cerullo & Cerullo, 1997; Fowler Newton, 2004; Minguillón, 2006, 2010; Presa, 2013). Siempre esta evaluación se considerará de carácter provisorio, porque cualquier prueba de validación de saldos podría poner en evidencia deficiencias de los controles (Nannini et al., 2011). Si las debilidades son materiales, el profesional concluirá que los controles internos no son eficaces y deberá replantearse su estrategia de auditoría, dando un mayor énfasis a las pruebas sustantivas para minimizar el riesgo final de auditoría (Minguillon, 2010), o decidir abandonar el encargo.

En los casos de auditorías recurrentes dicho proceso podría verse simplificado, dado que se deben identificar los cambios importantes que se hubieran producido en los controles y la evaluación de sus posibles consecuencias (Mora, Mauro & Villacorta, 2001; NIA 330, A. 13-14).

Todo el proceso descripto de evaluación del sistema de control interno en un ambiente de TI debe ser realizado para dos categorías de controles, los generales y los de aplicación (Arens et al., 2007; González, 2004; NIA 315 (Revisada), A. A104-A105).

Los *Controles Generales* se refieren al conjunto de políticas y procedimientos que se aplican a la totalidad o gran parte de los sistemas de información de una entidad, afectando al entorno informatizado en su conjunto, que ayudan a asegurar su correcto funcionamiento (González, 2004; Minguillón, 2010). Presa (2013:13-14) los divide en cuatro grupos: control de acceso (físico y lógico, solo permitido a personal autorizado); administración de cambios en los sistemas (adquisición, desarrollo y modificaciones dentro de un proceso formal, con cambios debidamente autorizados); operaciones de computación (operaciones en centros de procesamiento de datos y redes por personal capacitado, planes de resguardo de archivos y continuidad del negocio); y

controles organizacionales (ambiente de control, segregación de funciones e independencia de la función de sistemas respecto de los usuarios).

Los *Controles de Aplicaciones* son aquellos manuales o automáticos, diseñados en los propios sistemas informáticos empleados en el procesamiento de operaciones individuales mediante validaciones de entrada, procesamiento y salida, que incluyen controles de totalidad y exactitud; de validez, pertinencia y autorización; de actualizaciones, acumulación y almacenamiento de información; de confidencialidad y disponibilidad de la información (Arens et al., 2007; González, 2004; Minguillon, 2010; Presa, 2013).

La evaluación se realiza en el orden en que fueron expuestos, en la medida en que el mal funcionamiento de los primeros invalida a los segundos, dando lugar a manifestaciones erróneas en los estados contables sin que sean detectadas (Arens et al., 2007; Minguillon, 2010; Presa, 2013). En consecuencia, se puede concluir en forma desfavorable en relación al sistema de control interno sin necesidad de probar los controles de aplicaciones (lo cual es más complejo y costoso) (Presa, 2013:21), debiéndose adoptar un enfoque basado en procedimientos sustantivos (Minguillon, 2010).

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 guíe la evaluación de controles en entornos de TI complejos en una auditoría financiera (Minguillón, 2010), menos aún en entornos tan recientes como lo es el de la CN, en relación al 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, como es el caso del proveedor del servicio de CN, 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, 2011b:116; RT 37, Segunda parte, Sección III, A.i. 3.5.1.).

Cuando el cliente utiliza una OS, el auditor considera evidencias y procedimientos diferentes para la evaluación del riesgo de control (Bierstaker et al., 2013). La NIA 402 (A. 12) 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 la OS para obtener información específica; visitas a la OS para aplicar procedimientos sobre los controles relevantes; recurrir a los auditores del servicio independientes con el fin de que apliquen procedimientos que proporcionen la información necesaria sobre los controles.

Aun cuando la CSA (2011b: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 los usuarios –y sus auditores– a realizar auditorías 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 interrupción de la prestación del servicio o por

protección de datos de otros usuarios que se encuentran excluidos de la auditoría, pero que están alojados en los mismos equipos (CSA, 2013b; Rumitti & Falvella, 2013).

En consecuencia, el uso de informes de terceros independientes sobre los controles de la organización de servicios parece ser la opción viable para la evaluación del CI. Es decir, el proveedor del servicio en la nube contrata un *auditor independiente* (considerado en la arquitectura propuesta por Liu et al. (2011) expuesta previamente) quien realiza una evaluación objetiva de su sistema de control interno, y emite un informe, dando satisfacción a las necesidades de los usuarios y sus auditores, sin tener que dar respuesta a las peticiones individuales de cada uno de ellos, evitando costos (de tiempo y dinero) y resguardando la información de los múltiples usuarios de los recursos compartidos del prestador del servicio. Dichas auditorías buscan garantizar la seguridad de los servicios en la nube, y en particular la relacionada con los datos almacenados y los procesos que se ejecutan en ella (CSA, 2011b).

La confianza que brindan los auditores del servicio se debe a su independencia respecto del proveedor auditado (la cual debería ser garantizada a pesar de que son contratados por este último) y al conjunto de conocimientos y recursos que poseen para efectuar estas auditorías y realizar verificaciones periódicas de, por ejemplo, la integridad de los datos almacenados en la nube, algo que no podrían realizar los usuarios (CSA, 2011b:116).

Si el auditor financiero decide utilizar dicho informe debe realizar indagaciones sobre la competencia profesional y la reputación del auditor en el contexto de la tarea específica asumida, así como de la adecuación de las normas conforme a las cuales se emitió el informe (Arens et al., 2007; NIA 402, A. 13). La calidad y alcance del trabajo ejecutado por el auditor del servicio, su competencia y objetividad son determinantes críticos a ser considerados por el auditor del usuario para calificar la fiabilidad del informe obtenido (Bierstaker et al., 2013).

La NIA 402 y la RT 37 (Segunda parte, Sección III.A) brindan una guía para el uso de estos informes de controles de la OS por parte del auditor de estados financieros del usuario del servicio.

Existen diversos tipos de informe, según su alcance:

a) informes sobre los *controles de la empresa de servicios que son relevantes para el control interno de entidades usuarias relacionados con la información financiera* (conocidos como reportes SOC1); su caracterización y las guías para su elaboración por parte del auditor del servicio están previstas en la norma internacional NIEA 3402, en la estadounidense SSAE 18 AT Section 320 –reemplazando recientemente al SSAE 16 que a su vez sustituía al antiguo SAS 70– y la RT 37, Segunda Parte, Sección V.C.;

b) informes sobre controles de una OS distintos de los anteriores, como ser aquellos relevantes para la *seguridad, continuidad, integridad de procesamiento de un sistema o la confidencialidad o privacidad de la información por él procesada* (SOC2). Éstos pueden ser realizados por el auditor de la OS bajo la guía general de la NIEA 3000, la norma estadounidense

AT Section 101, y no siendo previsto específicamente por la RT 37, resulta aplicable lo establecido en la Segunda parte, Sección V.A. - *Otros encargos de aseguramiento en general.*

Ambos tipos de informe son descriptos con más detalle en el Cuadro 11 a continuación.

Cuadro 11 - Informes sobre CI de organizaciones de servicio según su alcance

Informe de Controles en una Empresa de Servicios que son relevantes para el Control Interno de las Entidades Usuarias sobre los Informes Financieros
• Se limita a procesos y sistemas *relevantes para el informe financiero*, focalizándose en los controles vigentes en la organización de servicios que se presumen relevantes para el control interno de las organizaciones usuarias, en la medida en que se relacionan con la preparación de su información contable, dejando de lado otros controles y tópicos, como recuperación de desastres o privacidad. Se aplica en general cuando el servicio se relaciona a procesamiento de transacciones financieras o al soporte de sistemas de procesamiento de transacciones (liquidaciones de sueldos, gestión de activos, etc.). • El público objetivo son los usuarios del servicio y sus auditores de estados financieros. Su uso es restringido. • Atiende únicamente al objetivo de control interno de suficiencia y confiabilidad de la información financiera (KPMG, 2012). • Siendo un tipo de encargo basado en afirmaciones (NIEA 3402, A.2), la organización de servicios es responsable de describir su sistema, identificando: el servicio prestado, el período o fecha a la cual se refiere la descripción, los objetivos de control y los controles que son relevantes para los usuarios porque impactan sobre el reporte financiero. En caso de corresponder, debiera describir los controles de organizaciones subcontratadas y controles complementarios de la entidad usuaria, según se describe más adelante. • El trabajo del auditor se basa en la aseveración realizada por la organización de servicio, que se incluye o adjunta a la descripción que ella misma realiza sobre su sistema, evaluando si los controles diseñados e implementados son adecuados para lograr el cumplimiento de los objetivos planteados en la descripción del sistema. • El dictamen del profesional brinda una opinión positiva (de seguridad razonable), con una conclusión orientada directamente sobre la materia a tratar y el criterio (NIEA 3402, A.2).
Informe de controles en una Empresa de Servicios que son Relevantes para la Seguridad, Continuidad, Integridad de Procesamiento de un sistema o la Confidencialidad o Privacidad de la información procesada por el sistema
• Pueden ser aplicado a cualquier sistema o proceso, en la medida en que brinda aseguramiento de los controles operacionales aplicados en la empresa de servicio relacionados con los dominios (de seguridad, continuidad, integridad de procesamiento, confidencialidad o privacidad) en los sistemas utilizados para procesar la información. • Su público objetivo son los usuarios, sus auditores y otros usuarios determinados (socios comerciales y otras partes interesadas). Su uso es restringido. • Los proveedores del servicio podrían negarse a revelar información sensible (por ejemplo, información detallada sobre los controles de seguridad de la información) (KPMG, 2012), dificultando la emisión de los informes. • Existe un mayor nivel de estandarización, dado que el proveedor selecciona el o los dominios que deben ser cubiertos por el informe de acuerdo a sus necesidades y las de los usuarios, y se utilizan para su evaluación los "Principios y Criterios de Confianza" elaborados conjuntamente por AICPA y CICA que se encuentran predefinidos (en vez de objetivos de control específicos de cada servicio). Dichos Criterios de Confianza son el estándar que utiliza el ente para preparar su descripción del sistema de control interno y por el auditor para evaluarlo. • Atiende a tres objetivos de control: suficiencia y confiabilidad de la información financiera, efectividad y eficiencia de las operaciones, cumplimiento de las leyes y regulaciones aplicables (KPMG, 2012).

Fuente: Elaboración propia con base en la normativa.

A su vez, los informes pueden referirse únicamente a los controles puestos en operación (diseño e implementación) o a los controles puestos en operación y su eficacia operativa (diseño, implementación y eficacia) (Tipo I o II según las diversas normas). En ambos, la organización de servicio prepara la descripción del sistema, y:

a) en el TIPO I, *informe sobre controles puestos en operación*, el profesional expresa una opinión positiva acerca de si, en todos los aspectos significativos, con base en criterios idóneos, la descripción propuesta por la OS representa razonablemente el sistema a una fecha determinada, si el control interno está debidamente diseñado para alcanzar los objetivos de control o criterios y si se han implementado los controles internos a partir de una determinada fecha;

b) en el TIPO II el dictamen del profesional contiene las mismas opiniones que el tipo I, pero además el auditor dictamina si los controles han funcionado de manera eficaz en un período especificado de acuerdo a los resultados de las pruebas de controles por él realizadas. El profesional debe identificar las pruebas de controles realizadas y los resultados obtenidos (KPMG, 2012; NIA 402 A. 8(c)(ii); NIEA 3402, A. 54; RT 37, Segunda Parte, Sección V.C.ii.2.2.3.).

Un tema adicional a ser considerado, y en particular en el caso de servicios en la nube, es la posibilidad de que la organización prestadora utilice servicios de una organización subcontratada (NIEA 3402, A. 9 (a) y (g); RT 37). En este caso, existen dos métodos para tratar los controles internos de dicha organización:

a) Método Exclusivo (*Carve-out*), donde la descripción del sistema realizada por la organización de servicio incluye la naturaleza de los servicios prestados por la organización subcontratada; sin embargo, los objetivos de control y los controles relacionados relevantes son excluidos de la descripción del sistema realizada por la OS y del alcance del encargo del auditor del servicio; éstos si incluyen los controles que la OS hubiera establecido para monitorear la efectividad de los de la organización subcontratada, lo que puede incluir la evaluación de un reporte de aseguramiento sobre ellos;

b) Método Integrado (*Integrated*): la descripción de los sistemas de la organización del servicio incluye la naturaleza de los servicios prestados por la organización subcontratada, sus objetivos de control y controles relevantes, los cuales están alcanzados por el encargo del auditor del servicio.

En el informe del auditor del servicio debe indicarse el método utilizado en relación a los controles de la organización subcontratada (NIEA 3402, A. 53 (c) (iv); RT 37, Segunda Parte, Sección V.C.ii.1.1.4.). La NIA 402 (A. 18, A40) prevé que si el informe del auditor del servicio excluye los servicios de la OS subcontratada, y estos son relevantes para la auditoría de estados financieros de la usuaria, el auditor financiero de ésta última deberá aplicar los requerimientos de la norma con respecto a la organización de servicios subcontratada. Cabe analizar si en entornos de CN esto resultaría posible, dadas las dificultades de comunicación con la OS y su subcontratada.

A su vez puede ocurrir que la descripción elaborada por la organización de servicios incluya ciertos controles complementarios de la organización usuaria, esto es, aquellos que la organización de servicios asume que la organización usuaria implementará (ISAE 3402, A. 9 (b); NIA 402, A. 8(a)); en caso de que estos fueran relevantes para el cumplimiento de los objetivos de control, su inclusión en la descripción es imperativa (NIEA 3402, A. 21 (c)).

Sin embargo el auditor del servicio en su informe debiera declarar que su opinión no los incluye y que la efectividad de los controles de la OS está sujeta a la de dichos controles complementarios (NIEA 3402, A. 53 (c) (iii); RT 37, Segunda Parte, Sección V.C.ii.1.1.3.). En estos casos, el auditor de la usuaria deberá evaluar su diseño e implementación (NIA 402, A. 10), pudiendo realizar pruebas que le permitan concluir que los controles de la entidad usuaria están operando eficazmente con respecto a algunas o a todas las afirmaciones correspondientes, con independencia de los controles implantados en la organización de servicios.

En un servicio de CN, es en el SLA en donde debe definirse –si es posible la negociación– el tipo de informe a ser provisto por el auditor del servicio contratado por el proveedor y el período a ser cubierto, los dominios de control a ser evaluados (sean objetivos de control en SOC1 o principios determinados en SOC2), la existencia de sub-proveedores del servicio y si serán incluidos o no el alcance (métodos *carve-out* o *integrated*), y la fecha esperada de entrega del reporte (KPMG, 2012). En dichas elecciones se debiera tener en consideración no solo las necesidades del usuario del servicio, sino también las de su auditor financiero, dado que el informe le será una fuente de información importante.

En cuanto a la selección del tipo de informe**,** en lo que respecta al alcance del mismo, 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 por las organizaciones usuarias así como por sus auditores. Según la CSA (2013b) el proveedor del servicio en la nube debe evaluar si su servicio impacta sobre la elaboración de la información financiera de los usuarios, debiendo proveer un informe SOC1 (en aquellos casos en los que el servicio implique el inicio, autorización, registro, procesamiento o reporte de transacciones financieras que son incluidas en los estados contables del usuario), o si no posee un efecto directo o relevante sobre los controles internos sobre el reporte financiero, debiendo aportar un SOC2, 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 aplican los de tipo SOC1 en la medida en que proveen un servicio de información financiera a los usuarios, pero reconoce que también podría emitirse un SOC2 referido a seguridad y continuidad/disponibilidad para responder a las necesidades específicas de los usuarios de los servicios.

Por otro lado, la NIA 402 (A. A22) plantea que tanto el informe Tipo I como el Tipo II pueden facilitar al auditor la obtención de conocimiento suficiente con el fin de identificar y valorar los riesgos de incorrección material, sin embargo, un informe Tipo I, no le proporciona evidencia alguna de la eficacia operativa de los controles relevantes. La RT 37 (Segunda Parte, Sección V.C.i.4) considera el informe Tipo II como el más útil para los auditores de las organizaciones usuarias.

En su caso, los auditores externos deberán evaluar los SLA para determinar el alcance de los testeos que pueden ejecutar *in-house* (en el ente usuario) versus el nivel y tipo de aseguramiento que necesitaran recibir del auditor del servicio (Nicoloau et al., 2012).

Debe considerarse además el marco de referencia a ser utilizado para la evaluación de los controles en la nube, que definirá los controles que serán relevados e informados por el auditor del servicio. Por ejemplo, la CSA (2011b:117) recomienda que para realizar la evaluación en la nube se utilicen marcos referidos a esta tecnología, los cuales aún están 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.

Sin embargo, 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. En consecuencia, y tal como se expresó al comienzo de este aparatado, el auditor financiero deberá ser capaz de identificar los *controles relevantes* al momento de planificar su trabajo, o sea, los referidos a sistemas y aplicaciones que previamente se hayan definido como significativos a efectos de la información financiera sujeta a auditoría (Minguillon Roy, 2010: 133), dejando de lado otros controles que la empresa utiliza para la gestión de sus negocios, sobre los que hubiera obtenido información pero cuya evaluación implica un trabajo innecesario e ineficiente (Fraser, 2011).

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 relevantes según su propia evaluación de riesgos. 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 (A. 12) indicados previamente, y en caso de necesitar complementar la evaluación de la eficacia operativa podría intentar realizar pruebas de controles sobre los establecidos por la entidad usuaria en relación a las actividades de la empresa de servicios, así como visitar al proveedor para realizar sus propias pruebas de controles.

Finalmente, a partir de las tareas de auditoría realizadas el profesional podría identificar debilidades significativas en el diseño, la implementación y/o el mantenimiento de los controles internos, que merezcan la atención de los responsables de gobierno de la entidad. En este caso, debería comunicar a la gerencia que tenga un nivel de responsabilidad apropiado y a quienes tengan la responsabilidad de la dirección, siendo aplicable la *NIA 265 – Comunicación de las deficiencias en el control interno a los responsables del gobierno y a la dirección de la entidad.*

El Cuadro 12 resume los aspectos de la evaluación del sistema de control interno que completan el esquema conceptual de la Figura 1.

Cuadro 12- Evaluación del sistema de control interno en entornos de CN

TÓPICO	CATEGORÍAS	SUBCATEGORÌAS	
EVALUACIÓN DEL SISTEMA DE CONTROL INTERNO	**CONTROLES INTERNOS DE TI RELEVANTES PARA EL AUDITOR**	**Controles Generales**	• De los sistemas de información del proveedor • Del cliente sobre las actividades del proveedor del servicio
		Controles de las Aplicaciones	
	PROCEDIMIENTOS APLICABLES	**Informes de CI de la organización prestadora del servicio**	• Alcance: SOC1 O SOC2 • Tipo: I o II • Método Inclusivo o *Carved Out*
		Contacto con el prestador del servicio	• Consultas • Visitas para aplicar procedimientos sobre controles relevantes
		Solicitud al auditor del servicio	Indicaciones para evaluación de controles o solicitud de información específica

Fuente: Elaboración propia.

2.3.4. LAS EVIDENCIAS DE AUDITORÍA[7]

Las evidencias de auditoría comprenden todos los elementos de juicio utilizados por el auditor para fundamentar su opinión e incluyen tanto la información contenida en los registros contables de los que se obtienen los estados financieros, como otra información (NIA 500, A. 5(c)).

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), encontrándose entre los objetivos de su obtención y su adecuada documentación en papeles de trabajo los siguientes: a) facilitar la planificación 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).

Respecto de la CN, los antecedentes encontrados se refieren a la obtención de evidencias digitales en la nube –considerando su función de repositorio para el almacenamiento de datos e información a ser analizados para la obtención de indicios– desde la perspectiva de la auditoría interna y la auditoría de TI (CSA, 2011b:105-108) y de la informática forense (Taylor, Haggerty, Gresty & Hegarty, 2010; Taylor, Haggerty, Gresty & Lamb, 2011).

Las *evidencias digitales* 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 (Caldana,

[7] El presente apartado ha sido elaborado con base en el trabajo realizado en coautoría con la Mg. Diana Albanese y el Cr. Carlos Alberto Rumitti. Véase López, Rumitti y Albanese (2013).

Correa & Ponce, 2007), volviéndose más escasos los elementos de juicio físicos con los que habitualmente trabajan (Valencia & 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 & Tamayo, 2012); en el caso de la CN, algunas cuestiones son similares a otras alternativas de tercerización de TI, a la vez que existen ciertas particularidades que merecen ser analizadas.

En primer lugar, no sería 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, 2011b), 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 debe 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 (datos contables y otra información disponible solo en formato electrónico) (NIA 500, A. A12).

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, 2011b), 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 las evidencias son identificables, pudiéndose cerrar los servidores por un tiempo limitado para obtenerlas (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 (Arens et al., 2007; González, 2004; NIA 500, A12-A13; Pastor, 2011). 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 de 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 puede considerar necesario ejecutar los procedimientos en el momento en que la información esté disponible o requerir al cliente la conservación de cierta información para su revisión (NIA 500, A. A13), 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 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 TAACs que usualmente se emplean 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 le provean las claves, tal como ocurriría en un caso de investigación forense (Taylor et al., 2010).

La falta de disponibilidad de la información puede producirse 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, 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 debe evaluar la fiabilidad de las evidencias electrónicas que usará como elementos de juicio (NIA 500, A. 7), debiendo mantenerse escéptico en relación a la autenticidad de los registros brindados por sus clientes –la evidencia de auditoría obtenida directamente por el auditor es más fiable que la obtenida indirectamente o por inferencia (NIA 500, A. A31). 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 confiable, 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 éste 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* (López, Rumitti & Albanese, 2013).

Estas alternativas permitirían además garantizar el origen, la autoría y la integridad de los archivos y/o documentos digitales que obtiene. Así, si la fuente de las evidencias electrónicas desapareciera de la nube una vez ejecutados los procedimientos y obtenidos 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, éste 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 de que continuara siendo un riesgo significativo, debería ajustar sus procedimientos o comprensión del proceso para contemplar las actividades que minimicen dicho riesgo (López et al., 2013).

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.

El Cuadro 13 resume los principales conceptos que complementan el esquema conceptual en referencia al tópico tratado en este apartado.

Cuadro 13 - Evidencias de auditoría digitales en la nube

TÓPICO	CATEGORÍAS	SUBCATEGORÌAS	
EVIDENCIAS DIGITALES DE AUDITORÍA	**OBTENCIÓN**	**Procedimientos para la obtención**	Autenticación de usuarios de auditoría Uso de TAACs Inalterabilidad de información de origen
		Disponibilidad de la información	Ubicación de la información Temporalidad de los datos Destrucción o modificación no autorizada
		Fiabilidad de la información	Autenticidad de registros Evaluación de controles internos
	PROCESAMIENTO	Procesamiento y evaluación de las evidencias de auditoría obtenidas No alteración de datos originales. Uso de copias de archivos digitales	
	CONSERVACIÓN	**De evidencias y papeles de trabajo**	Disponibilidad futura • Obsolescencia • Destrucción Plazos de conservación según la normativa

Fuente: Elaboración propia.

2.3.5. COMPETENCIAS PROFESIONALES DEL AUDITOR FINANCIERO. INTERVENCIÓN DE EXPERTOS EN TECNOLOGÍA DE LA INFORMACIÓN

La *competencia profesional* es la habilidad de ejercer un rol según un estándar definido; consiste en la integración y aplicación de competencia técnica, habilidades profesionales y valores, ética y actitudes. Comprende el conocimiento de principios, estándares, conceptos, hechos y procedimientos (Norma Internacional de Formación (NIF) 8, A. A2).

Según Nearon (2005), se refiere a la habilidad técnica de un auditor para descubrir los errores materiales en los estados financieros, y resulta de la combinación de la educación, el

entrenamiento y la experiencia. Permite al auditor recolectar la evidencia para respaldar su informe y evaluar si la misma es suficiente y confiable.

En lo que respecta a la normativa, la IFAC a través de los *International Education Standards* (Normas Internacionales de Formación (NIF), en español) brinda lineamientos para el desarrollo de las competencias profesionales. La formación del contador prevé un Desarrollo Profesional Inicial (DPI), en el que deben adquirirse conocimientos en diversas cuestiones vinculadas a la contabilidad, incluyendo las áreas de Auditoría y Tecnología de Información (NIF 2).

Luego, se propone que los contadores públicos que hubieran completado dicho nivel deben realizar un proceso de Desarrollo Profesional Continuo (DPC) (NIF 7), que les permita mantener y actualizar las competencias profesionales para proveer servicios de calidad y fortalecer la confianza pública en la profesión. Esto considerando: a) que el cambio es una característica del ambiente en el que trabajan los contadores, requiriéndose el desarrollo y mantenimiento de la competencia; b) que las aptitudes requeridas se modifican a lo largo de la carrera profesional en la medida en que se modifican los roles ejercidos (IFAC, 2015).

En lo que respecta específicamente al auditor, mediante la NIF 8 (A. 7) la IFAC establece los requisitos de competencia que deberían desarrollar y mantener los contadores cuando se desempeñan como *auditores profesionales* en el rol de socios del encargo (*engagement partners),* esto es, responsables por la auditoría de estados financieros.

El contenido temático de su formación incluye diversas áreas, entre ellas la tecnología de información. Los resultados del aprendizaje (*learning outcomes,* en inglés) en este punto deberían permitirle al profesional evaluar el entorno de TI para identificar controles relacionados a los estados financieros y determinar su impacto sobre la estrategia de auditoría. Esta área se complementa con una descripción completa de muchos otros puntos a ser cubiertos mediante la capacitación del auditor (NIF 8, Tabla A).

Finalmente, en relación con los conocimientos de los miembros del equipo de auditoría y cualquier experto del auditor que no forme parte del equipo, la NIA 220, referida al *Control de calidad de la auditoría de estados financieros*, establece que el socio debe satisfacerse respecto a que reúnan en conjunto la competencia y capacidad adecuadas para realizar el encargo de auditoría, de conformidad con las normas profesionales y los requerimientos legales y reglamentarios aplicables, y para poder emitir un informe que sea adecuado en función de las circunstancias (NIA 220, A. 14).

En la Argentina, esta situación se encuentra regulada en el Código de Ética Unificado de la FACPCE (2001), que en su artículo 5 establece:

> **COMPETENCIA. CAPACITACION CONTINUA**
> Artículo 5º: Los profesionales deben atender los asuntos que les sean encomendados con responsabilidad, diligencia, competencia y genuina preocupación.
> Tienen la obligación de mantener un alto nivel de idoneidad profesional, para lo cual deben capacitarse en forma continua.

En lo que respecta a los estudios académicos, existen diversos trabajos que tratan sobre las competencias profesionales que deben desarrollar los contadores que se desempeñan como auditores financieros. A los efectos de esta tesis, interesan particularmente aquellos referidos a la formación que deben adquirir en relación a la tecnología de la información.

Sánchez, Sálas y Rodríguez (2006) realizaron una investigación con 76 profesionales de estudios de auditoría de la ciudad de Santiago de Chile. El trabajo reveló que los principales conocimientos técnicos requeridos a los auditores se referían a cuestiones y normativa contable, de auditoría financiera y tributaria. Del mismo resulta que los conocimientos requeridos en relación a la tecnología se referían principalmente al uso de herramientas básicas, como procesadores de texto, planillas electrónicas y bases de datos, no requiriéndose –salvo en el caso de los *seniors*– el manejo de programas ERP o específicos de auditoría.

Sin embargo, otros autores como Gomes da Silva y Pimenta (2001) consideran que en un ambiente de cambios, en donde la tecnología está presente en todas las áreas de una organización y permanentemente se producen nuevos avances, los auditores deben adaptarse a las nuevas TI, siendo la capacidad de lidiar con ellas un requisito esencial en la formación de estos profesionales. Así, en opinión de Curtis et al. (2009), quienes no posean conocimientos extensos en sistemas pueden tener dificultades para comprender la tecnología compleja utilizada en los procesos de negocio de sus clientes.

En consecuencia, los auditores necesitan expandir sus conocimientos y habilidades sobre sistemas de información contable complejos para poder desarrollar auditorías eficientes y eficaces (Brazel, 2008; Brazel & Agoglia, 2007; Presa, 2013).

Tal como se expuso previamente, las normas como la NIF 8 reconocen que el auditor financiero puede requerir habilidades especializadas en sistemas de información y control computadorizados para el desarrollo de la auditoría financiera, pero no brindan una guía para los profesionales respecto de cuáles son los conocimientos requeridos para cumplir dichas tareas (Curtis et al., 2009; Rîndasu, 2016). De hecho, la norma Argentina vigente (RT37) no hace referencia a estos aspectos específicamente.

De acuerdo a la literatura, 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 auditada y consecuentemente sobre la auditoría de estados financieros en general y el propio enfoque de la auditoría en particular (González, 2004). Según Curtis et al. (2009), el entrenamiento y experiencia en sistemas de información puede ser tan importante como la formación y experiencia en contabilidad para una evaluación de control interno efectiva.

Brazel y Agoglia (2007) proponen que la pericia en sistemas de información contable

(SIC) proveen al auditor de habilidades de auditoría sofisticadas tales que le permiten 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 integrantes, la pericia en sistemas de información complejos puede ser más valorada que la experiencia general en auditoría.

Minguillón (2006) plantea que los conocimientos del profesional vinculados a la TI deben comprender diversos aspectos, tales como:

a) las normas aplicables relacionadas;

b) las características de los distintos entornos informatizados;

c) una profundización en la evaluación de los controles internos generales y de aplicación, su efecto en el riesgo de auditoría y en los procedimientos de auditoría aplicables;

d) la evidencia informática;

e) los ERP y su impacto en los procedimientos de auditoría;

f) uso de las principales técnicas de auditoría asistidas por computadora (TAACs) - ventajas, requisitos y limitaciones - y papeles de trabajo electrónicos;

g) uso de al menos un programa de análisis y extracción de datos (como ACL o IDEA);

h) conceptos básicos sobre auditoría de sistemas de información.

Adicionalmente, Rîndasu (2016) plantea la necesidad de que los auditores financieros posean conocimientos sólidos sobre TI que les permitan comprender como funcionan los sistemas de información de la organización y como se mantiene su seguridad, considerando el impacto que tiene esta última sobre los objetivos y las actividades de las organizaciones, dando lugar a nuevos factores de riesgo. Ya no es suficiente que se enfoquen en los estados financieros y en los flujos de datos a través de los sistemas; deben ser capaces de validar la existencia de controles eficientes sobre la seguridad de la información. Según su estudio en Rumania, los jóvenes y próximos auditores reconocen la importancia de este aspecto.

González (2004:53) menciona que, en su intento por alcanzar los conocimientos mínimos necesarios para trabajar en entornos informatizados, el profesional debe realizar un esfuerzo de formación importante no solo en aspectos teóricos sino con un componente práctico significativo para contar con experiencia aplicada especializada.

Curtis et al. (2009) en su trabajo de revisión citan diversos autores, quienes plantean que son necesarias modificaciones en los planes de estudio para la formación universitaria de contadores públicos que se desempeñen como auditores financieros, en pos de satisfacer los requerimientos de formación en sistemas de información (y TI) impuestos por los ambientes actuales (por ejemplo,

Arens & Elder, 2006; Arnold & Sutton, 2007) y que los educadores deben formar a los estudiantes para la comprensión de los aspectos tanto manuales como electrónicos del sistema contable (Carmichael, 2004).

Recientemente, Pan y Seow (2016) llegan a conclusiones similares mediante una revisión de literatura sobre los efectos de la TI sobre la contabilidad; sugieren que es necesaria una revisión de la formación universitaria brindada a los futuros contadores, en la medida en que el avance permanente de la TI y su uso en funciones de contabilidad y auditoría demanda nuevas capacidades a los profesionales. Entre los aspectos a fortalecer se encuentran la formación en controles y auditoría de TI.

A su vez, Borthick, Curtis y Sriram (2006) indican que la falta de experiencia en sistemas de información de los auditores puede ser compensada mediante ciertos tipos de entrenamiento direccionado; esto es, puede ser necesario que los propios estudios de auditoría brinden entrenamiento a sus auditores en áreas que no fueran cubiertas por la formación universitaria.

Ahora bien, aun cuando el profesional contable convertido en auditor financiero puede y debe profundizar sus conocimientos de la TI, Presa (2013) reconoce el conocimiento que puede alcanzarse es finito dado el avance constante y rápido de la tecnología, de modo que es posible que existan temas relacionados a la TI que excedan los conocimientos y habilidades del profesional a cargo del encargo de auditoría.

Es así que, a partir de la consideración de la propia competencia, el auditor debe evaluar en la etapa de planificación de la auditoría (NIA 300, A. A2) la necesidad o conveniencia de contar con el asesoramiento oportuno de especialistas[8], con conocimientos adicionales o más profundos de los que él mismo posea en algún área de sistemas (González; 2004; NIA 620, A. 7; Presa, 2013). La norma internacional se refiere al *experto del auditor*, nombrando de este modo a "una persona u organización, especializada en un campo distinto al de la contabilidad y auditoría, cuyo trabajo en ese campo se utiliza por el auditor para facilitarle la obtención de evidencia de auditoría suficiente y adecuada" (NIA 620, A. 6(a)).

Diversos estudios analizaron la interacción entre ambos profesionales. 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. Singleton (2011) también considera que la Ley SOX (2002) y la adopción de una metodología de auditoría basada en riesgos incrementaron la importancia y necesidad de la participación de auditores de TI en la auditoría financiera. Algunos estudios citados por Brazel y Agoglia (2007) (Bagranoff & Vendrzyc, 2000; O'Donell, Arnold & Sutton, 2000) indican que los test realizados por los auditores de TI pueden representar más de la mitad del trabajo de una auditoría financiera, más aún cuando el profesional contable no cuenta con el nivel de conocimiento adecuado.

[8] Especialización: cualificaciones, conocimiento y experiencia en un campo concreto (NIA 620, A. 6(c)).

Vîlsanoiu y Şerban (2010) analizaron la relación entre la auditoría financiera y la de sistemas de información. Se destaca que a partir la implementación de la metodología de auditoría basada en riesgos del negocio en la década del ´90 (dejando de lado el enfoque tradicional orientado a los ciclos de transacciones) se incrementa la importancia de la auditoría de los sistemas. En ese contexto, se consideran dos hechos que justifican dicha situación: la implementación del modelo COSO –u otro modelo de CI– por parte de las organizaciones, haciendo que los auditores financieros deban considerar nuevas dimensiones de controles internos relevantes para los estados contables; y la aparición de la Ley Sarbanes Oxley en Estados Unidos, que en su Sección 404 requiere que la administración del ente emita una evaluación de sus controles internos y que el auditor financiero opine sobre dicha evaluación. En ambos casos el auditor financiero está obligado a formarse una opinión sobre controles que cada vez más están incorporados en las soluciones de TI utilizadas por el auditado, requiriéndose de la participación de auditores de sistemas para que brinden seguridad sobre su funcionamiento. Ambas situaciones propiciaron además la prestación de servicios de consultoría relacionados a los sistemas y procesos en los grandes estudios de auditoría a partir de la incorporación de los auditores de TI en su estructura.

Otros factores pueden propiciar dicha intervención: 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 (Astiz & Sole, 2008; Presa, 2013).

En la auditoría de estados contables, la participación de los especialistas puede ser útil en diversos aspectos. ISACA (2011) y Minguillón (2006), entre otros, destacan 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) y 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.

Singleton (2011) por su parte considera que el conjunto de contribuciones clave que los auditores de TI pueden hacer a una auditoría financiera se refieren a: a) efectuar las pruebas de los controles que se encuentren automatizados para verificar que operan en forma efectiva y que lo han hecho a lo largo del ejercicio, colaborando con la etapa de evaluación de riesgos de la auditoría financiera; b) utilizar las TAACs principalmente para la extracción y análisis de datos de los sistemas del auditado en el proceso de obtención de evidencias para ciertos objetivos de auditoría; c) colaborar en la planificación de procedimientos de auditoría, proponiendo la ejecución de algunos de ellos utilizando la tecnología, incrementando el nivel de eficiencia y obteniendo mejores evidencias de auditoría (por ejemplo, analizando universos de transacciones en forma electrónica en vez de muestras en forma manual, u obteniendo muestras para la aplicación de pruebas sustantivas con una importante reducción de tiempos); d) finalmente, los auditores de TI pueden

realizar valiosos aportes en la identificación de debilidades de CI que fuera necesario informar a la administración del ente –en la carta con recomendaciones– aun cuando estas no necesariamente estuvieran vinculadas a la información financiera (ejemplo, debilidades en la seguridad que no afecten a datos contables, pero que la administración podría querer solucionar).

La intervención de los expertos puede darse al menos de dos modos (NIA 620, A. 6(a)):

1) que sean miembros internos del estudio (socios o empleados, incluso temporales, de la firma de auditoría) incorporados al equipo de trabajo de auditoría externa; en general, además de prestar soporte a la auditoría, brindan otros servicios de aseguramiento y consultoría en sistemas (testeos de ataques a redes y de penetración, planes de continuidad de negocio, comercio electrónico (Vendrzyk & Bagranoff, 2003)). En estos casos el especialista requiere el mismo grado de supervisión y revisión que cualquier otro colaborador (Tucker, 2001). El supervisor –auditor financiero a cargo de la auditoría– deberá poseer el conocimiento suficiente de sistemas de información y TI tal que le permita comunicar los objetivos del trabajo a ser desarrollado por el auditor de TI, evaluar si los procedimientos planificados cumplirán los objetivos de auditoría y evaluar los resultados de los procedimientos aplicados, en la medida en que se relacionan a otros procedimientos de auditoría aplicados (Curtis et al., 2009).

2) si el estudio de auditoría no cuenta con personal que tenga dicho conjunto de habilidades, se debe considerar la complementación del equipo de trabajo con individuos que las posean, siendo éstos contratados por el auditor como personal externo, a efectos de que emitan un informe independiente sobre alguna materia específica, que luego será tenido en cuenta en el examen profesional como evidencia de auditoría.

La normativa argentina y la internacional (NIA 620, A. 9, 10, 12; RT 37) prevé que el auditor financiero debe evaluar si el experto tiene la competencia, la capacidad, la objetividad y la independencia necesarias para sus fines, dependiendo del riesgo involucrado. A su vez, deberá determinar la naturaleza, el alcance y los objetivos del trabajo del experto, y posteriormente evaluar la labor y los resultados alcanzados y obtener evidencia suficiente de que el trabajo es adecuado a los fines de una auditoría financiera.

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 financieros y por la opinión expresada no puede ser delegada (NIA 620, A. 3; Presa, 2013). Singleton (2011) se refiere al concepto de *auditoría integrada*, resaltando que se trata de una auditoría, no dos. El auditor de TI debe colaborar en la elaboración de un plan de auditoría óptimo, haciendo sus aportes e involucrándose desde la planificación del trabajo, integrándose a la labor de los auditores de estados contables.

De acuerdo a lo expresado por Brazel (2008), el mayor conocimiento de TI que adquiera el

auditor financiero, así como su mayor pericia en sistemas de información contable complejos, le permitirán lograr una mayor comprensión de cuáles son los controles del sistema que el auditor de TI ha testeado (o no), y 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. A su vez, la incorporación de expertos en TI con pericia suficiente beneficia a todo el equipo de auditoría, dado que sus miembros pueden confiar en los testeos que él realice y concentrarse más en los problemas asociados a la auditoría de estados financieros.

Ahora bien, aun cuando es reconocida la necesidad de intervención de especialistas en TI, más aún en entornos de tecnologías complejas como lo es el de la computación en la nube, diversos estudios han detectado deficiencias en la relación auditor financiero-auditor de sistemas. Si bien algunos de ellos datan de varios años atrás, las evidencias son válidas considerando que, en la Argentina, así como en otros países similares, la implementación de las tecnologías se ve demorada respecto de otros países en los que se desarrollan los estudios.

Trabajos como el de Janvrin et al. (2008) sobre 181 auditores de firmas de diverso tamaño de Estados Unidos muestran que los auditores de TI son utilizados con poca frecuencia en una auditoría típica, y que cuando se los usa, se lo hace con poca intensidad; a su vez, la frecuencia de uso de especialistas en TI es menor cuanto menos compleja es percibida la TI utilizada por el cliente auditado. Finalmente, los auditores de TI son utilizados con mayor frecuencia e intensidad por los auditores financieros de las BIG-4 respecto de los auditores del resto de las firmas más pequeñas; ello puede deberse a que los estudios grandes tienden a poseer clientes con TI más complejas.

Otra problemática encontrada por Vendrzyk y Bagranoff (2003) en su trabajo con auditores financieros y de sistemas de las BIG-4 se relaciona a las distintas percepciones entre auditores financieros y de sistemas sobre el valor de la auditoría de sistemas de información y el aporte que los segundos pueden hacer en la definición del enfoque de auditoría, lo cual puede demostrar problemas de comunicación e ideas erróneas entre los dos grupos de profesionales.

El trabajo de Brazel y Agoglia (2007) trata sobre la interacción entre auditores financieros y auditores de TI mediante un estudio experimental en la que participaron auditores *senior* de 6 firmas. Encontraron que dicha relación se ve influenciada por la pericia del auditor de TI tanto como por el nivel de pericia en sistemas de información complejos del auditor financiero. Destacan las ventajas de lograr un entrenamiento suficiente de ambos tipos de auditores, de modo que posean el nivel de habilidad requerida de acuerdo a la complejidad de la TI de sus clientes. El estudio sugiere que el conocimiento sobre sistemas de información del auditor financiero juega un rol importante en los ambientes de sistemas de información contable (SIC) complejos y en su habilidad para compensar las competencias deficientes de los auditores de TI. En particular determina, entre otras cuestiones:

a. la competencia del auditor de TI tiene un efecto sustancial en la evaluación de riesgo de control realizada por el auditor financiero; si la competencia del primero aumenta, los auditores tienden a confiar en los resultados positivos de sus test de control, y considerar el riesgo de control bajo –si bien los auditores con alta pericia SIC tienden a considerar el riesgo de control en un nivel mayor que los que tienen una pericia baja;

b. cuando el auditor financiero considera que el auditor de TI posee pericia adecuada, confía en su evaluación del sistema y se concentra en otros procedimientos; por el contrario, cuando la pericia del auditor de TI es considerada baja, un auditor con alta pericia en SIC expande el alcance de las pruebas sustantivas, incluyendo sus propios testeos sobre el sistema, todo lo cual no ocurre si posee baja pericia en SIC;

c. en un entorno ERP, la pericia en SIC parece triunfar sobre la experiencia en auditoría general; en la conformación de los equipos de auditoría para encargos en empresas con sistemas de información contable complejos debe tenerse en cuenta la pericia en SIC de los potenciales miembros contadores públicos, más que la experiencia general en auditoría –puede ser más efectivo asignar un *senior* con 4 años de experiencia y pericia en SIC y que un *senior* con 5 años de experiencia en auditoría y sin pericia en SIC.

En relación al entorno de TI estudiado, 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 contable, que trasciende lo técnico e incluye los aspectos legales.

En la medida en que los entornos cada vez más complejos de TI son aplicados en Argentina –y en otros países de Latinoamérica– con cierta demora respecto de los países desarrollados, se hacen necesarios más estudios que analicen estos aspectos de conocimientos requeridos al auditor y formas de interacción con especialistas en TI en este contexto en particular.

El Cuadro 14 resume los principales conceptos que complementan el esquema conceptual.

Cuadro 14 - Competencias profesionales del auditor externo e intervención de expertos en entornos de TI

TÓPICO	CATEGORÍAS	SUBCATEGORÌAS	
COMPETENCIAS PROFESIONALES DEL AUDITOR. INTERVENCION DE EXPERTOS EN TI	**CONOCIMIENTOS TÉCNICOS DEL AUDITOR**	**Aspectos**	Cuestiones y normativa contable Cuestiones y normativa de auditoría financiera Cuestiones y normativa tributaria *Tecnología de información* • *Sistemas de información* • *Características de ambientes de TI* • *Riesgos de TI* • *Seguridad de la información* • *Controles internos* • *Procedimientos* • *Evidencias digitales* • *Uso de TAACs y herramientas informáticas para la auditoría* • *Objetivos de la auditoría de sistemas*
		Importancia / Utilidad	Comprender el sistema de información del auditado y su influencia sobre EEFF Planificar, dirigir y ejecutar el encargo Poder evaluar riesgos y controles específicos Decidir la necesidad de intervención de expertos • Evaluar la idoneidad del experto • Comunicar objetivos • Evaluar procedimientos aplicados y resultados de la intervención • Interpretar sus informes
	USO DE EXPERTOS	**Factores que lo justifican**	Complejidad de los sistemas Tecnologías emergentes Significatividad de la evidencia digital Conexiones remotas Acceso simultáneo de usuarios Normativa que requiere opinión sobre controles internos afectados por TI
		Aportes	Comprensión del sistema de información Colaboración en planificación Evaluación de riesgos informáticos Pruebas de funcionamiento de controles Utilización de TAACs Recomendaciones a la gerencia
		Formas de intervención	• Miembros del estudio de auditoría • Experto externo

Fuente: Elaboración propia.

3. METODOLOGÍA

"El diseño metodológico de una investigación tiene como finalidad la planificación de la investigación científica, es decir, la concepción de una estrategia para averiguar algo"

Vázquez et al. (2006).

En el presente capítulo se describe la metodología aplicada en la tesis, justificando las elecciones realizadas y detallando aspectos operacionales. En primer lugar, se presenta la caracterización y diseño de la investigación y a continuación se describen cada una de las etapas de su ejecución.

3.1. CARACTERIZACIÓN Y DISEÑO DE LA INVESTIGACIÓN

La presente es una investigación exploratoria, de enfoque cualitativo, utilizándose el método de entrevistas en profundidad a expertos como técnica de recolección y análisis de datos en el campo.

Se considera de tipo exploratorio, debido a que no se han encontrado en la literatura antecedentes específicos sobre el tema en cuestión –la auditoría financiera en contextos de tercerización de TI, particularmente computación en la nube–, menos aún en el contexto del estudio, la República Argentina (Hernández Sampieri et al., 2010).

Se ha optado por implementar un enfoque de investigación cualitativa, siendo esta recomendada cuando existen deficiencias en el conocimiento del problema, sea porque son fenómenos para los que no existe una teoría o, si existe, ésta es insuficiente (Ragin, Nagel & White, 2004:11); el tema de estudio ha sido poco explorado; no se ha hecho investigación al respecto en algún grupo social específico; o el fenómeno de interés es muy difícil de medir o no se ha medido anteriormente (Hernández Sampieri et al., 2010), permitiendo entonces descubrir lo nuevo y desarrollar teorías empíricamente fundamentadas (Flick, 2009:15); situaciones todas que se consideran aplicables al tema de investigación aquí planteado.

Según López y Salas (2009), la investigación en administración posee particular interés por el uso de métodos cualitativos, por la cercanía de su teoría a las disciplinas sociales, las cuales hacen amplio uso de estos en el estudio de organizaciones, grupos o individuos.

Siendo una investigación cualitativa, se ha diseñado a pequeña escala, pero buscando profundizar en el análisis de las experiencias, perspectivas, opiniones y significados brindados por los participantes, considerando la novedad del problema de investigación (López & Salas, 2009:134), sin pretender realizar inferencias o predicciones a partir de patrones que surgen de la comparación de distintos casos.

El estudio se fundamenta entonces en la experiencia e intuición de los participantes (no en la revisión de la literatura como en el caso de los estudios cuantitativos), orientándose a generar

teorías fundamentadas en sus perspectivas (no así a probar teorías, hipótesis y/o explicaciones o evaluar efectos de unas variables sobre otras como lo hacen los estudios cuantitativos correlaciónales y explicativos) (Hernández Sampieri et al., 2010).

El enfoque cualitativo es considerado adecuado a los fines de este trabajo por lo siguiente: a) se ha detectado una escasez de estudios académicos sobre la auditoría financiera en relación a la TI en general, y a la computación en la nube en particular; b) existe interés por conocer la opinión y experiencia de expertos en el tema.

La investigación cualitativa puede ser llevada adelante por diversos métodos, los que incluyen: entrevistas, observación, estudios de caso, grupos de enfoque, cuestionarios, investigación documental, entre otras. Ninguna de las fuentes posee una ventaja indiscutible sobre las otras.

Siguiendo a Taylor y Bogdan (1987) y a Valles (1999), se ha elegido utilizar las entrevistas cualitativas en profundidad como técnica útil para conocer la opinión de expertos respecto del tema de investigación.

Las *entrevistas* son definidas en términos amplios como un reporte a varias personas para obtener información (Vázquez et al., 2006). La característica de ser entrevistas *en profundidad* las define como abiertas, no estructuradas, con miras a lograr un mayor conocimiento del tema estudiado, a la vez que se obtienen experiencias y puntos de vista de diferentes personas.

Este tipo de entrevistas se clasifican como *profesionales de investigación* (según Millar, Crute & Hargie, 1992, citados por Valles, 1999). Son definidas como técnicas de obtención de información relevante para los objetivos de un estudio, siendo su campo de aplicación el de las ciencias sociales.

Las entrevistas en profundidad se dirigen al *aprendizaje sobre acontecimientos o actividades que no se pueden observar directamente* (Taylor & Bogdan, 1987:103) –tal como lo es un proceso de auditoría de estados financieros en un entorno de tercerización, en particular de uso de CN. En este sentido, los interlocutores son verdaderos *informantes*, que no solo revelan su modo de ver las cosas, sino que describen lo que sucede y el modo en que otras personas de su entorno lo perciben[9].

Su aplicación se consideró especialmente adecuada por las siguientes situaciones: a) los intereses de la investigación son relativamente claros y bien definidos; b) las personas involucradas no podían ser abordadas de otro modo; c) permitió el acceso a información que resultaba difícil de observar; d) existieron limitaciones de tiempo para la recolección de datos, dado que las entrevistas

[9] El término *informante* es utilizado en el sentido otorgado por Taylor y Bogdan (1987), quienes se refieren a los participantes de las entrevistas en profundidad de este modo. Se decide no adoptar la posición de Gorden (1975) descripta por Valles (1999:212-213), quien se refiere con esta denominación únicamente a personas que tienen un papel en las investigaciones de campo, no aportando información directamente relacionada con los objetivos de la entrevista, sino más bien brindando datos sobre la situación local y colaborando en la obtención de cooperación, así como la localización y contacto con los potenciales entrevistados, entre otras cuestiones (estos han sido denominados en este trabajo como *intermediarios*, según se describe mas adelante).

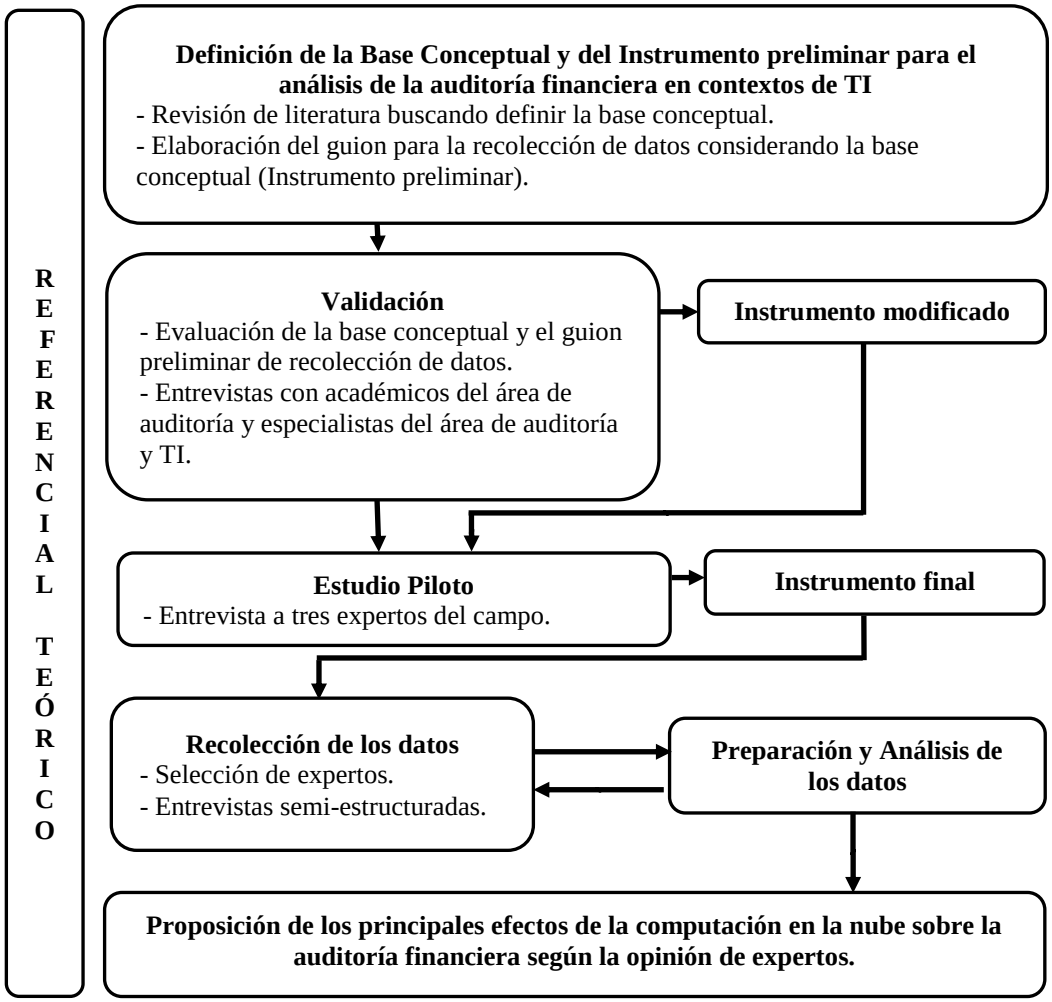
se pudieron concretar en un lapso de tiempo menor al requerido por otros métodos (como la observación participante) (Taylor & Bogdan, 1987; Valles, 1999: 196-198).

Según Flick (2009:165), en la *entrevista a expertos* los participantes resultan interesantes por sus capacidades en un ámbito de actividad, siendo incluidos en la investigación no como casos individuales, sino como representantes de un grupo.

Una cuestión que caracteriza a la investigación cualitativa es la flexibilidad en cuanto al modo de llevar adelante el estudio; aun cuando existen lineamientos orientadores, estos no devienen en reglas, sino que el investigador es quien debe crear su propio método (Taylor & Bogdan, 1987). En consecuencia, se describe en este capítulo el conjunto de decisiones que han llevado a diseñar la estructura de la investigación desarrollada en esta tesis.

Para ilustrar las elecciones metodológicas y visualizar las etapas y detalles del estudio se presenta el diseño de la investigación en la Figura 5. Cada una de las etapas será explicada en los apartados siguientes.

Figura 5 - Estructura y diseño metodológico



Fuente: Elaboración propia.

3.2. REVISIÓN BIBLIOGRÁFICA PARA LA ELABORACIÓN DEL ESQUEMA CONCEPTUAL Y DEL INSTRUMENTO DE RECOLECCIÓN DE DATOS

En los estudios cualitativos, la revisión bibliográfica sirve al planteamiento del problema cualitativo inicial. El fundamento no se limita a dicha revisión, sino que sirve como apoyo o consulta. Es así que este tipo de investigación se basa principalmente en el proceso mismo de recolección y análisis, siendo de carácter interpretativo, en la medida que el investigador hace su propia descripción y valoración de los datos (Hernández Sampieri et al., 2010).

Se realizó una revisión sistemática de antecedentes referidos a la auditoría financiera en general, la auditoría financiera en entornos de tecnología de información y en entornos de computación en la nube en particular. Se inició mediante el estudio de diversos autores tradicionales, nacionales y extranjeros, referidos a los temas en cuestión. La misma se complementó con la revisión de normas de auditoría (nacionales e internacionales) y estándares (relacionados a la auditoría financiera y a la implementación de la nube), así como recomendaciones de diversos organismos especializados en esta tecnología.

Los resultados de dicha revisión estuvieron presentes en el desarrollo de las diferentes etapas de la investigación. Los mismos fueron reveladores de la falta de estudios académicos relacionados al tema bajo análisis, en particular en el contexto argentino. Sin embargo, fueron útiles a los efectos del planteamiento del problema y la elaboración de un marco teórico o esquema conceptual de referencia para la investigación en su conjunto. Se pretendió reflejar conceptos de la literatura nacional e internacional en relación a la auditoría financiera en entornos de TI, en particular en contextos de tercerización, así como cuestiones relacionadas a la computación en la nube, de modo de construir una base amplia respaldada por autores y organismos con reputación en el área, buscando identificar los aspectos que debían ser indagados mediante el trabajo empírico para cumplir el objetivo de la tesis.

Siguiendo a Martens (2009), el esquema conceptual fue sometido a diversas revisiones a fin de verificar su adecuación y aplicabilidad.

En primer lugar, la revisión bibliográfica y el esquema conceptual preliminar fueron presentados parcialmente en congresos nacionales e internacionales y revistas científicas, y mejorados a partir de las devoluciones y comentarios recibidos (verificar López, 2012; López & Albanese, 2013; López, Albanese & Sánchez, 2011a; López, Albanese & Sánchez, 2011b; López, Albanese & Sánchez, 2014; López, Rumitti & Albanese, 2013; López, Sánchez & Albanese, 2010). Una versión preliminar del marco de referencia fue presentada para su publicación en una revista nacional del área en el año 2014 (verificar López, Albanese & Durán, 2013 – Revista Escritos Contables y de Administración). Las revisiones en cada una de estas instancias dieron cuenta de la relevancia del tema y de la adecuación de la revisión bibliográfica y la elaboración del marco teórico.

Además de ello, tanto el esquema de conceptos como el guion de recolección de datos fueron sometidos a revisión por profesionales y académicos vinculados al tema de investigación, según se describe en el apartado *3.3. Validación del instrumento de recolección de datos.*

En el esquema conceptual se buscó reflejar los conceptos principales relacionados al problema de investigación y sus interrelaciones. De este modo sirvió de soporte a la elaboración del guion para las entrevistas con los profesionales, permitió definir los criterios para la selección de los entrevistados (en función de su experiencia y conocimientos en relación al tema en cuestión) y la organización y análisis de los datos y resultados.

Aun cuando se utilizó una técnica de entrevistas en profundidad, por definición no estructurada, se consideró necesaria la preparación de un instrumento de recolección de datos. Este no resultó ser un protocolo estructurado, sino la descripción de un conjunto de temas y subtemas a cubrir con cada informante, de acuerdo con los objetivos de la investigación.

El instrumento permitió guiar las conversaciones sobre los tópicos definidos como relevantes y proponer una forma de preguntar, decidiéndose en cada caso cómo y cuándo formular las preguntas de acuerdo al modo en que se desarrollara la entrevista –clasificadas como entrevistas semi-estructuradas o estandarizadas no programadas, de respuestas abiertas (Flick, 2009; Taylor & Bogdan, 1987; Valles, 1999).

La versión preliminar del instrumento de recolección de datos fue elaborada sobre un conjunto de bloques, basados en cada uno de los tópicos relevantes según el esquema conceptual. Se tuvieron en cuenta los siguientes aspectos:

- Presentación del objetivo de la investigación.
- Preguntas para determinar el perfil del entrevistado (formación; estudio al que pertenece; cargo actual; tiempo de ejercicio de la profesión y en el cargo actual).
- Preguntas Específicas referidas a:
  - Potenciales efectos que el uso de la CN por parte del ente auditado podría tener sobre la auditoría financiera en general; planteo de los principales aspectos a ser relevados (pregunta amplia).
  - Conocimiento del cliente. Identificación de factores de riesgo de la nube y su potencial probabilidad de ocurrencia e impacto sobre la auditoría de estados financieros.
  - Evaluación del sistema de control interno en un ambiente de CN.
  - Evidencias digitales de auditoría en la nube.
  - Competencias profesionales y uso de expertos.
- Preguntas de cierre: aportes adicionales que el entrevistado quisiera realizar; solicitud de contactos con otros profesionales que pudieran ser entrevistados.

En la versión preliminar del guion para las entrevistas dichos tópicos fueron desglosados en preguntas o líneas de indagación. En el mismo se abordaron todas las áreas definidas en el esquema teórico, dado que se realizaría una única entrevista con cada informante (Valles, 1999: 205-206).

Se incluyó la descripción de muchos conceptos relativos a la auditoría financiera en general, así como otros referidos a la computación en la nube, en busca de clarificar ciertas cuestiones al momento del planteo de las preguntas.

3.3. VALIDACIÓN DEL INSTRUMENTO DE RECOLECCIÓN DE DATOS

Concluida la etapa de elaboración del esquema conceptual y de la versión preliminar del instrumento de recolección de datos, se procedió a validarlos con la finalidad obtener cierta seguridad razonable sobre su validez y utilidad (tomando como modelos las investigaciones de Martens (2009), Sobragi (2012) y Rech (2012)). Para ello se anticipó en el uso de entrevistas con un fin exploratorio preparatorio (Valles, 1999: 201-202) para la posterior realización de las entrevistas en profundidad en el campo.

3.3.1. Revisión por especialistas

En primer lugar, el esquema conceptual y el instrumento de recolección de datos fueron sujetos a la evaluación de académicos y especialistas de las áreas de incumbencia.

Este tipo de revisión en investigación cualitativa se encuentra, por ejemplo, en Rech (2012) –quien previo a la recolección de los datos evaluó el guion a ser utilizado mediante una revisión de investigadores y especialistas y un contacto preliminar con el campo de investigación– y Sobragi (2012) –quien sometió su protocolo de investigación a la revisión por tres especialistas heterogéneos en relación al tema de estudio para obtener un análisis amplio.

El objetivo de la revisión consistió en la mejora del instrumento a fin de garantizar su aplicabilidad a la investigación, considerando:

- la adecuación de las preguntas;
- la estructura y disposición equilibrada y armónica de los bloques temáticos;
- el orden de las preguntas dentro de cada bloque;
- la cantidad de preguntas planteadas;
- la ausencia de preguntas relevantes o la existencia de preguntas superfluas o reiterativas;
- la inexistencia de inconsistencias o problemas.

La evaluación fue realizada por especialistas del área de auditoría financiera y sistemas de información. Se optó por consultar a especialistas con formación en ciencias contables, pero de distintas áreas de actuación profesional y académica, a fin de obtener una visión amplia y variada. La selección de los revisores se basó en sus antecedentes, en su disponibilidad a participar de la investigación, así como la posibilidad de reiterar consultas en caso que fuera necesario.

Los especialistas son profesores universitarios (todos de grado; dos de ellos de postgrado), investigadores de las áreas de auditoría y/o TI, con experiencia profesional, según se detalla en el Cuadro 15.

Cuadro 15 - Perfil de los especialistas revisores del esquema conceptual y del instrumento de recolección de datos

CÓDIGO	FORMACIÓN	ANTECEDENTES	ÁREA DE ACTUACIÓN
Revisor 1	Contador Público	Profesor Universitario de Grado y Postgrado. Profesional: auditor, especialista en sistemas con actuación en organismos del estado, asesor externo de empresas en el área de sistemas de información.	Auditoría de estados financieros. Auditoría de sistemas. Tecnología de la información.
Revisor 2	Contador Público Magíster en Auditoría de Sistemas Magíster en Administración de Negocios	Profesor Universitario de Grado y Postgrado. Consultor del Consejo de Profesionales en Ciencias Económicas de la Provincia de Buenos Aires. Profesional: asesor de entidades gubernamentales en relación al uso de TI.	Auditoría de Sistemas. Tecnología de la información.
Revisor 3	Contador Público	Profesor Universitario de Grado. Profesional: contador público independiente.	Tecnología de la información.

Fuente: Elaboración propia.

En primer lugar, se realizó una entrevista personal con el **Revisor 1** (duración: 1 hora 40 minutos), en la que se dio lectura a los objetivos de la investigación, se expuso el esquema teórico y se conversó sobre cada una de las preguntas incluidas en la versión preliminar del guion. El especialista realizó comentarios acerca de las cuestiones planteadas y dio algunas respuestas preliminares. La entrevista fue grabada y transcripta en forma textual. A partir de su lectura y análisis se realizaron las modificaciones que se consideraron pertinentes, creándose una versión mejorada del instrumento. Luego, a pedido del revisor, se envió la nueva versión por e-mail para confirmar que los cambios fuesen adecuados.

En términos generales, el **Revisor 1** consideró adecuado el esquema conceptual planteado, así como las categorías de temas que se pretendía profundizar. Propuso modificaciones en cuanto a simplificación de las preguntas planteadas, disminución de conceptos teóricos, entre otras cuestiones, resultando en un cuestionario modificado de manera significativa.

Por lo expuesto en el párrafo anterior, se decidió someter la versión modificada del instrumento a evaluación por los **Revisores 2 y 3**.

Al **Revisor 2** se le envió por correo electrónico el detalle de los objetivos de la investigación y el instrumento de recolección de datos modificado. Sus recomendaciones fueron recibidas por el mismo medio. Entre sus principales propuestas se encontraban la incorporación a la investigación de auditores de sistemas, por los conocimientos técnicos requeridos para poder opinar sobre algunas cuestiones. A su vez, propuso incorporar preguntas iniciales que permitieran determinar el

nivel de conocimiento y familiaridad de los entrevistados en relación al ambiente de TI analizado, lo cual serviría para conducir la entrevista y analizar los resultados. Este tipo de preguntas descriptivas serían útiles además para iniciar las conversaciones y determinar los temas que el informante considerara más importantes.

Finalmente, el **Revisor 3** recibió una copia del instrumento por correo electrónico y se realizó una entrevista personal (duración: 1 hora 30 minutos). En ella se discutieron nuevamente todas las preguntas, recibiéndose recomendaciones para la mejora de la estructura del instrumento y la claridad de las preguntas. Volvió a indicar la conveniencia de entrevistar a personas con conocimientos técnicos del tema, no solo auditores financieros.

Un mayor detalle de las propuestas de mejora de los revisores y las acciones tomadas sobre la base de ellas se exponen en el Anexo 1.

La versión revisada del instrumento para la recolección de datos fue sometida a una evaluación final mediante los estudios piloto que se describen a continuación.

3.3.2. Estudios Piloto

Weiss (1994:52) destaca la importancia de realizar entrevistas piloto, que sirven para probar los borradores del guion de recolección de datos y dar experiencia al entrevistador. Ademas, permiten una primera inmersión en el campo (Hernández Sampieri et al., 2010). Los guiones que resultan de estas validaciones, aunque probados, continúan siendo provisionales y susceptibles de mejora.

En consecuencia, una vez elaborado el guion modificado de acuerdo a las sugerencias de los revisores, fue utilizado para realizar los estudios piloto mediante entrevistas con 3 profesionales extranjeros. El detalle de los entrevistados se encuentra en el Cuadro 16.

Cuadro 16 - Perfil de entrevistados para estudios piloto

CÓDIGO	PAÍS	FORMACION	ANTECEDENTES	ÁREA DE ACTUACIÓN
EP1	Colombia	Ingeniero de sistemas, especialista en auditoría de sistemas de información Magíster en Administración Magíster en Educación	Profesor universitario. Responsable de la formación en informática en la carrera de grado de contador público. Certificación Internacional COBIT 4.1, COBIT 5, ISO 27001. Auditor de sistemas en empresas privadas. Titular de empresa de servicios de consultoría en sistemas de información y seguridad informática.	Sistemas de información. Auditoría de sistemas. Seguridad informática.
EP2	Uruguay	Contador Público MBA	Profesor universitario en el área de auditoría y contabilidad. Socio Director de un estudio de auditoría (BIG4).	Contable. Auditoría de estados financieros.

			Experiencia en Auditoría y Asesoramiento Financiero, particularmente atención de clientes nacionales e internacionales del Sector Financiero.	
EP3	Uruguay	Ingeniero en Computación Magíster en Computación Diplomado en Sistemas de Información (Oxford) Certificado en Seguridad de la Información	Director de Consultoría en el área de Estrategia y Operaciones de un estudio de auditoría (BIG4).	Sistemas. Gestión de proyectos de incorporación de tecnología y seguridad de la información.

Fuente: Elaboración propia.

Las entrevistas fueron realizadas vía Skype, a fin de probar este medio de comunicación y determinar si sería viable su aplicación con el resto de los entrevistados. Las conversaciones fueron grabadas –previo aviso a los entrevistados– y desgrabadas en forma textual para su análisis. La realización de estos estudios permitió además experimentar el proceso de conducción de entrevistas.

Se obtuvieron evidencias empíricas preliminares para validar la estructura conceptual y el instrumento de recolección de datos. Aun cuando los entrevistados están sujetos a marcos normativos y contextos diferentes a los de Argentina, los resultados obtenidos fueron útiles a los fines de esta etapa de la investigación.

Respecto de las respuestas obtenidas, las mismas demostraron que el tema es de interés para los profesionales y que resulta relevante en el contexto actual, no solo en referencia a la computación en la nube en particular, sino respecto de la tercerización de TI en general. En todos los casos existe un estado incipiente de implementación, con algunas cuestiones a ser resueltas para su generalización, en particular en lo que se refiere a la información financiera (EP1 y EP2). Sin embargo, existen casos de éxito en sus países tanto de uso de CN como de otros servicios similares, considerando que es una opción de tercerización de TI que en definitiva será utilizada por las empresas –dedicándose estas a su verdadero objeto social y delegando el manejo de la tecnología en expertos como los proveedores en la nube. En consecuencia, se requiere de su análisis en diversos aspectos a fin de estar preparados para cuando ello ocurra (EP 1).

Los tres entrevistados mostraron poseer conocimientos de tercerización de TI en general y de la computación en la nube en particular, haciendo posible conversar sobre los diferentes temas propuestos.

La consulta a los especialistas en áreas de sistemas dio buenos resultados, en la medida en que complementan la experiencia y opinión de los del área de auditoría de estados financieros, confirmándose la decisión de su incorporación en la investigación.

Al ser consultados sobre la variedad de los puntos tratados y la necesidad de incorporar otros aspectos en la investigación, coincidieron en que el enfoque era adecuado y completo. En general pudieron dar respuesta a las diversas cuestiones, comprendiendo los puntos que se pretendían tratar.

De todos modos, se realizaron un conjunto de ajustes finales al guion de recolección de datos, descriptos en el Anexo 2.

La versión final del instrumento se incluye en el Anexo 3. Ésta fue utilizada para la conducción de las entrevistas abiertas realizadas a los profesionales argentinos. Cabe aclarar, tal como lo hacen Hernández Sampieri et al. (2010), Taylor y Bogdan (1987) y Valles (1999), que la planificación en la investigación cualitativa está en permanente revisión, implicando que el guion necesariamente debe ser adaptado durante cada entrevista y con posterioridad a su realización, capitalizando la experiencia adquirida en cada oportunidad. Esto resulta central en la entrevista cualitativa, a fin de adaptarse para alcanzar puntos de vista complementarios y contrastantes sobre el mismo tema o cuestión (Rapley, 2004:18).

3.4. MUESTRA DE EXPERTOS

3.4.1. Definición de características de los potenciales informantes

Un aspecto fundamental es la definición de las personas a las que se deberá entrevistar y los grupos de los que provienen (Flick, 2009:114). Deben tenerse en cuenta criterios diversos (Valles, 1999:213, citando a Gorden, 1975), considerando no solo a quien tiene la información relevante (sujetos informados), sino también aquellos que son accesibles física y socialmente (sujetos informados y accesibles), que están dispuestos a informar y que tienen mayor capacidad de comunicar la información con precisión.

Al momento de definir los posibles entrevistados, se consideró que un ambiente propicio para encontrar profesionales que pudieran conocer sobre el tema estudiado eran los grandes estudios de auditoría ubicados en Argentina, a saber: PwC Argentina, Deloitte, Ernst & Young, KPMG y BDO. El orden expuesto es el indicado en el ranking de auditores argentinos elaborado por MERCADO (2013), de acuerdo al nivel de facturación y cantidad de clientes en el país durante el año 2012. Esta decisión se justificó en las siguientes razones:

- en los grandes estudios se hace un mayor uso y se da más importancia a la TI, porque poseen mayores recursos que les permiten adquirir soluciones de TI costosas y contar con la colaboración de especialistas en TI; además asesoran a grandes clientes que normalmente hacen uso de alternativas de TI más complejas (Janvrin et al., 2008; Yigitbasioglu, 2015);

- concentrar el estudio en las grandes firmas de auditoría permite un mejor examen del estado del arte de las prácticas de auditoría y aseguramiento (Vendrzyc & Bagranoff, 2003; Yigitbasioglu, 2015). Es de esperar que los profesionales que se desempeñan en dichos estudios posean mayor experiencia en relación a la TI que quienes se desempeñan en estudios nacionales, regionales o locales, más aun considerando el caso de la computación en la nube, una alternativa de TI de reciente aplicación por parte de las organizaciones;
- muchas de las empresas usuarias de estos servicios son filiales nacionales de empresas extranjeras (USUARIA, 2012), siendo en general auditadas por alguno de estos estudios, no sólo las filiales sino también las matrices del exterior. Ello implica mayor probabilidad de que hubiesen tenido a su cargo una auditoría, ya sea en un entorno de computación en la nube, o al menos en entornos de sistemas de información complejos, que incluyeran la tercerización de servicios de TI;
- muchas publicaciones relacionadas a la computación en la nube y análisis de normas son realizadas por profesionales de estos estudios de auditoría;
- según fue comentado por los entrevistados de los estudios piloto y en la realización de las entrevistas en profundidad, en estos estudios el *know how* es compartido a nivel mundial; en consecuencia, aun cuando no se hubieran ejecutado auditorías financieras en entornos de CN en el país, las personas poseen acceso al conocimiento compartido en sus bases de datos así como capacitaciones permanentes sobre estos temas de vanguardia sobre la base de experiencias adquiridas en filiales de otros países, donde la implementación de estas soluciones de TI se encuentra más avanzada.

En la definición de los informantes, se analizaron los actores que componen la arquitectura de la nube (Liu et al., 2011) mencionados en el apartado *2.2.4*. (Figura 6). Inicialmente se consideró que a los efectos de esta investigación resultaría útil entrevistar a los auditores financieros del ente usuario del servicio, que son quienes se enfrentan con la problemática aquí planteada y deben resolver –según sus conocimientos, experiencia, procedimientos y técnicas disponibles– como actuar frente a esta tecnología. Luego de las revisiones y los estudios piloto comentados en el apartado anterior, se decidió incorporar a profesionales que se desempeñan en los departamentos de auditoría de sistemas de los grandes estudios, dado que en muchos casos integran los equipos de auditoría financiera.

A modo de resumen, las características que debían cumplir los potenciales entrevistados para formar parte de esta investigación son las siguientes:

a) pertenecer a alguno de los cinco principales estudios de auditoría del país (PwC Argentina, Deloitte, Ernst & Young, KPMG, BDO);

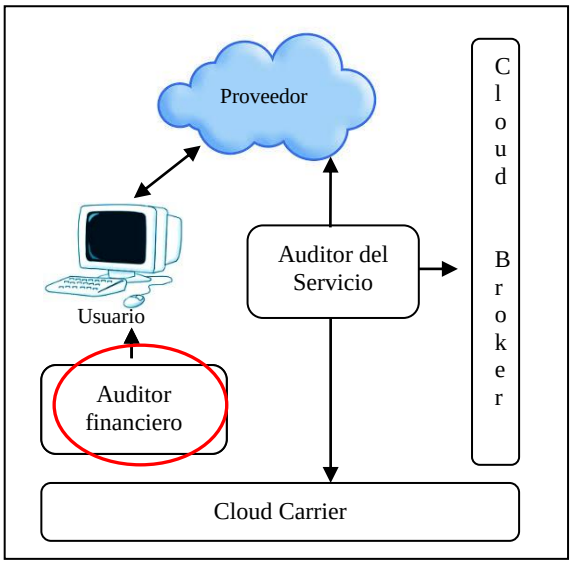
b) desempeñarse en los departamentos de auditoría financiera o auditoría de sistemas;

c) poseer experiencia en auditorías de estados financieros en contextos de sistemas de TI complejos;

d) conocer el concepto de computación en la nube;

e) haber alcanzado como mínimo el cargo de *senior* dentro del estudio.

Figura 6 - Selección de los informantes dentro de la arquitectura de la nube



Fuente: Elaboración propia.

3.4.2. Determinación de la muestra de informantes

Según Hernández Sampieri et al. (2010), en la investigación cualitativa el tamaño de la muestra no es importante desde una perspectiva probabilística, dado que no se pretende generalizar los resultados; se busca la profundidad, mediante participantes que ayuden a comprender el fenómeno de estudio y responder las preguntas de investigación. El estudio se realiza sobre un pequeño número de casos, menor que en los estudios cuantitativos. Este tipo de muestras dirigidas poseen valor dado que permiten obtener los casos que interesan al investigador y que ofrecen riqueza para la recolección y análisis de los datos.

Siendo difícil determinar a priori la cantidad de personas a entrevistar, la selección de la muestra se ha realizado en función a un criterio no probabilístico (o dirigido), es decir, la elección de los elementos dependió de las características de la investigación y decisiones del investigador que construye la muestra (Hernández Sampieri et al., 2010; Vázquez et al., 2006).

La estrategia del muestreo teórico (Flick, 2009; Hernández Sampieri et al., 2010; Taylor & Bogdan, 1987:108; Valles, 1999:214) resultó útil a dicho fin: el número de casos estudiados carecía relativamente de importancia y no fue definido a priori; lo que interesa es el potencial de cada informante a los fines de la investigación. Se iniciaron las entrevistas con algunos informantes, y se continuó con otros hasta encontrar toda la gama de perspectivas en las que se estaba interesado –

obteniendo representantes de los 5 grandes estudios de auditoría– y considerando que las unidades adicionales no aportaban información o datos novedosos (saturación de categorías).

Se utilizó la alternativa de muestra de expertos (Hernández Sampieri et al., 2010), dado que por los objetivos de la investigación se buscaba la opinión de individuos con amplios conocimientos y experiencia en el tema. La muestra fue definida en dos etapas:

a) Muestra inicial: basada en el criterio de muestreo intencionado (Flick, 2009:168; Weiss, 1994:24) o por conveniencia del investigador (Malhotra, 2011), pretendiendo la participación de expertos, pero considerando además la posibilidad de acceso, así como su interés, compromiso y disponibilidad para participar de la investigación. Esta fue una limitante importante, tal como se comenta en el apartado *3.4.3. Proceso de* r*eclutamiento de expertos*.

b) Adiciones a la muestra: para ampliar la muestra inicial se utilizó la alternativa de muestra en cadena o por redes (Hernández Sampieri et al., 2010; Weiss, 1994:25); en cada entrevista se les solicitó a los participantes clave si podían establecer el contacto con otros profesionales –de su estudio u otro– que pudieran proporcionar datos útiles para la investigación. Dichas personas fueron contactadas, y en los casos de respuestas favorables, se agregaron a la muestra.

Yigitbasioglu (2015) utiliza estos mismos métodos en su estudio con auditores de firmas de auditoría grandes y medianas de Australia.

En definitiva, la muestra quedo conformada por ocho representantes de los cinco grandes estudios de auditoría, integrada por auditores financieros y de sistemas, tal como era pretendido, según se expone en el Cuadro 17. El número de casos seleccionado se consideró adecuado en función de los siguientes factores (Hernández Sampieri et al.; 2010):

- es un número tal que ha sido posible manejar de manera realista y de acuerdo con los recursos disponibles;
- el entendimiento del fenómeno ha sido satisfactorio con este número de casos, logrando la saturación de categorías;
- se trabajó con todas las personas que tuvieron disponibilidad para participar de la investigación. En el caso de los contactos fallidos, se insistió en el pedido de participación, desistiéndose ante reiteradas faltas de respuesta.

Cuadro 17- Conformación de la muestra

ESTUDIO	AUDITORES FINANCIEROS	AUDITORES DE SISTEMAS
Deloitte	1	1
E&Y		1
PWC	1	1
KPMG	1	
BDO		2
TOTAL	**3**	**5**

Fuente: Elaboración propia.

3.4.3. Proceso de reclutamiento de expertos

En esta etapa se tuvieron en cuenta los criterios de selección de entrevistados en relación a accesibilidad, disposición y capacidad de comunicación, descriptos en el punto *3.4.1*.

Según indica Rapley (2004:17), si bien el proceso de encontrar a los informantes y realizar las entrevistas es central para la investigación, en la práctica pueden existir ciertas trabas para el reclutamiento, realizándose el mismo según las oportunidades que se presentan. Una descripción de las cuestiones de acceso y reclutamiento ayuda a comprender los resultados de la investigación.

Siguiendo la propuesta del autor mencionado y la de Weiss (1994:25), para acceder a los potenciales entrevistados se han seguido diferentes caminos, partiendo de colegas de la tesista y sus directoras, y luego accediendo a contactos brindados por los entrevistados, generándose una red a partir de la cual se obtuvo la información.

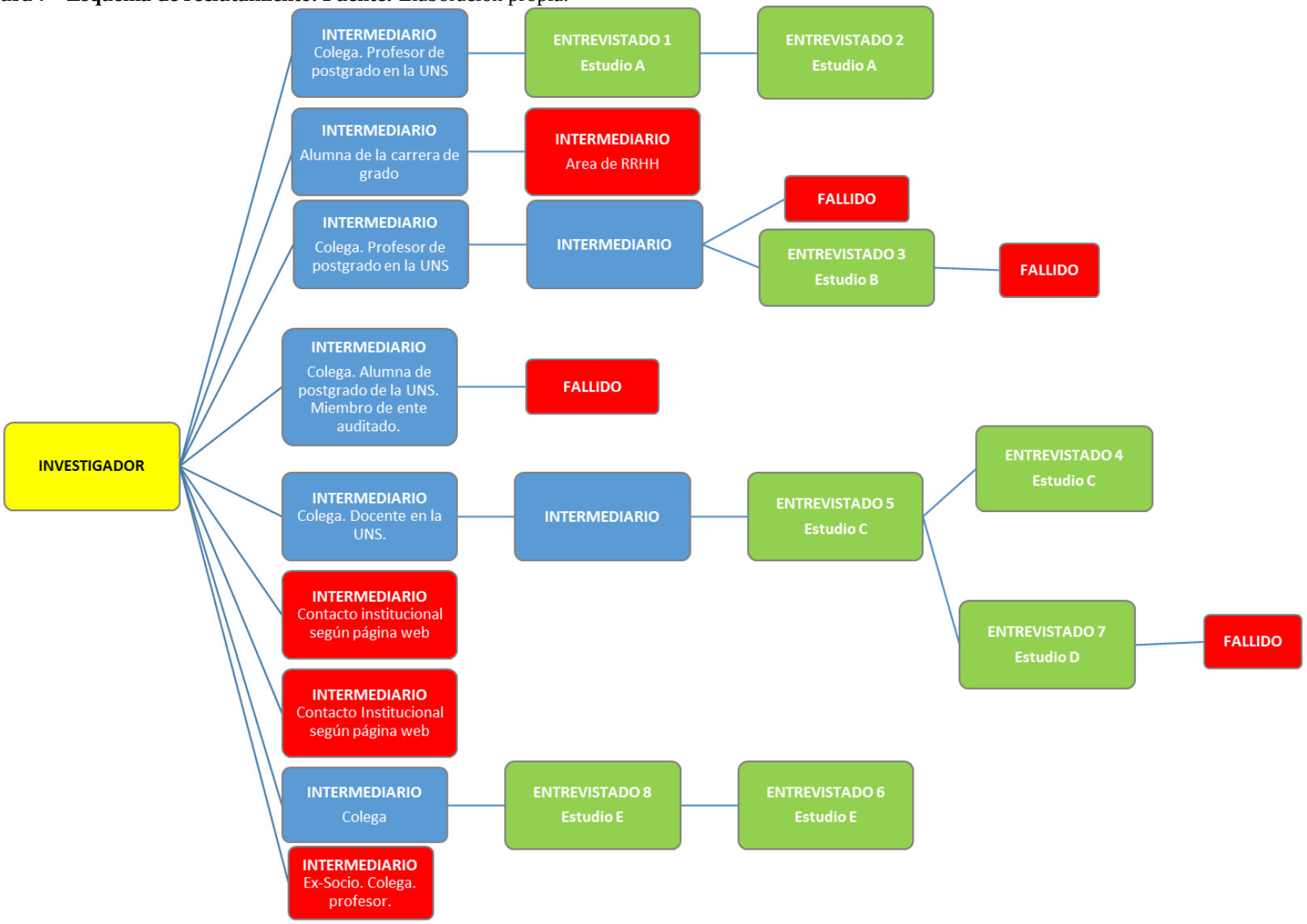
Para la selección de los informantes se tuvo en cuenta además la experiencia de Bandeira (2009), quien en su tesis doctoral realizó el contacto con los sujetos a ser entrevistados a través del sector de recursos humanos de las organizaciones que le interesaban, indicándoles el perfil necesario, para luego poder contactar a las personas propuestas.

Tomando dicho antecedente, en el presente trabajo se realizó una primera comunicación con quienes actuaron como *Intermediarios*: miembros de los estudios de auditoría con los cuales se había realizado un contacto inicial. Mediante una comunicación formal (Anexo 4) se les informaron los objetivos de la investigación y se les solicitó que indicaran los potenciales informantes de su estudio considerando el tema de investigación y las características pre definidas según se indica en la sección *3.4.1*.

Obtenidos los contactos de los potenciales entrevistados, se realizó una invitación formal vía correo electrónico (Weiss, 1994:35) (Anexo 5), y se acordó a través de sucesivas comunicaciones la fecha y modalidad para la realización de las entrevistas. En más de una ocasión las mismas debieron ser reprogramadas por cuestiones de disponibilidad de los entrevistados.

La Figura 7 resume la red de contactos realizada para el reclutamiento, indicando en color celeste los contactos intermediarios, en verde los contactos con los que finalmente se realizó una entrevista (informantes) y en rojo los que no respondieron o desistieron de participar de la investigación.

Figura 7 - Esquema de reclutamiento. Fuente: Elaboración propia.



3.5. PROCESO Y TÉCNICA DE RECOLECCIÓN DE LOS DATOS

Una entrevista de investigación consiste en una conversación destinada a obtener información y comprensión de cuestiones relevantes para un objetivo y responder a preguntas de un cierto proyecto (Guillham, 2000).

Rapley (2004:15) indica que las entrevistas consisten en un intercambio entre dos personas, en general desconocidas, que se sientan y conversan sobre un tema específico; agrega que las llamadas *en profundidad* se refieren a un tipo de entrevistas en las que se alienta al entrevistado a producir respuestas elaboradas y detalladas mediante preguntas y otros métodos verbales y no verbales. Se refiere en su trabajo a las *entrevistas cualitativas* para englobar las diferentes denominaciones que les asigna la bibliografía.

En este apartado se describen las decisiones adoptadas y la forma en que los datos fueron obtenidos en el campo.

Siendo que la cantidad de sujetos disponibles no era demasiado elevada, y no podía perderse ninguno de ellos, es que se realizaron entrevistas cara a cara (Gillham, 2000), evitándose las preguntas por correo electrónico o teléfono. De este modo se logró un mayor compromiso y calidad de respuestas. Aprovechando el potencial de Internet, que ofrece la comunicación e interacción con personas de todo el mundo en tiempos impensados (Salgado, 2007), se ofreció realizar las entrevistas mediante teleconferencias (a través de Skype), opción que fue aceptada por todos los informantes. Ello permitió un importante ahorro de recursos y tiempo, teniendo en cuenta que las personas entrevistadas se encuentran en la Ciudad Autónoma de Buenos Aires, y por la naturaleza de sus trabajos poseen agendas muy complicadas, de modo que la realización de las entrevistas por este medio permitió coordinar una y otra vez los encuentros cuando no era posible cumplir con las citas pactadas.

El lugar y momento en que se realizan las entrevistas son factores de producción que podrían afectar positiva o negativamente la obtención de información (Rapley, 2004:18; Valles, 1999: 217). En consecuencia, se requirió de los entrevistados cierta disponibilidad de tiempo y la permanencia en un lugar tranquilo y privado, atendiendo a sus preferencias para la definición de momentos y espacios en particular.

Según fue informado por los entrevistados, y visto a través de las comunicaciones con video, todos ellos se encontraban en sus lugares de trabajo o en sus hogares al momento de las comunicaciones, en general solos, no existiendo interrupciones de terceras personas o llamados telefónicos, pudiendo estar las personas atentas a las conversaciones. Únicamente en dos casos hubo interrupciones en las comunicaciones por fallas de la red, las que fueron solucionadas, pudiendo obtenerse las respuestas requeridas.

Un aspecto adicional para lograr resultados adecuados se refiere a la condición del entrevistador (Valles, 1999:215-216). En este caso, la coordinación de las reuniones fue realizada a posteriori de un profundo estudio del marco teórico y normativo de modo tal que se tuviera un

amplio conocimiento del tema al momento de preguntar. Cabe mencionar que no existía ningún tipo de vínculo personal ni relación con los entrevistados que pudieran entorpecer la investigación. Informantes y entrevistador no tenían diferencias significativas, por ejemplo, en cuanto a formación, no existiendo obstáculos que pudieran generar dificultades en la comunicación. Ello excepto la experiencia profesional en un campo específico, lo cual era pretendido para llevar a cabo el trabajo. El contexto de las entrevistas fue neutral, de modo que no se generaron circunstancias que pudieran afectar el objetivo de las mismas.

La recolección de los datos ocurrió en el período julio a diciembre de 2014. Las entrevistas fueron orientadas por el guion de recolección de datos. Las mismas tuvieron una duración de 1 hora en promedio, con un mínimo de 52 minutos y un máximo de 1 hora 40 minutos. Fueron grabadas, previo aviso a los entrevistados. Aun cuando esto pudiera tener ciertas desventajas, por inhibir a las personas (Taylor & Bogdan, 1987:130), se consideró necesario a fin de poder captar en forma adecuada la información para su posterior análisis.

Tal como se indica en el instrumento de recolección de datos, las entrevistas se iniciaron con *preguntas descriptivas* (Taylor & Bogdan, 1987: 115), solicitando a los informantes que manifiesten sus experiencias en relación al uso de la computación en la nube, ya sea personal o por parte de sus clientes. Esto sirvió como disparador para permitirles relatar lo que ellos consideraban importante, sin forzar ni estructurar las respuestas preliminares, evitando influenciar a los entrevistados.

Esto permitió además enfocar luego las entrevistas en los temas programados que no hubieran sido comentados. Se ha pretendido ser flexibles en la utilización del guion de preguntas, siguiendo el modelo de una conversación normal y no de un intercambio formal de preguntas y respuestas, a fin de reducir los efectos que el propio investigador causa sobre los informantes (Taylor & Bogdan, 1987).

El uso de entrevistas en profundidad permitió aprovechar ciertas ventajas de este método (Valles, 1999:196). Por ejemplo, la utilización de preguntas abiertas aportó una riqueza informativa en las palabras y enfoques de los informantes, a la vez que facilitó un marco de interacción en el que se pudieron solicitar aclaraciones y realizar un seguimiento de preguntas y respuestas más directo, personalizado, flexible y espontáneo.

Durante las entrevistas los participantes mostraron alto conocimiento e interés en relación al tema, facilitando la realización de la investigación. La totalidad de las cuestiones pudieron ser abordadas y se obtuvieron respuestas satisfactorias que permitieron realizar un análisis adecuado.

3.6. PREPARACIÓN Y ANÁLISIS DE LOS DATOS

En este apartado se describe de manera detallada la forma en que los datos fueron analizados con el propósito de demostrar que los resultados y conclusiones son producto de un trabajo

metódico, riguroso y objetivo, a fin de otorgar credibilidad a los mismos (López & Salas, 2009:140).

La investigación cualitativa se basa principalmente en el proceso mismo de recolección y análisis, siendo de carácter interpretativo, en la medida en que el investigador hace su propia descripción y valoración de los datos (Hernández Sampieri et al., 2010).

A decir de Taylor y Bogdan (1987), los investigadores desarrollan sus propios modos de analizar los datos cualitativos. Sin embargo, ha resultado útil en el diseño de la estrategia de organización y análisis de la información recolectada tomar en cuenta las recomendaciones de diversos autores ya citados previamente (Hernández Sampieri et al., 2010; Taylor & Bogdan, 1987; Valles, 1999).

Según Freitas y Moscarola (2000), el análisis de los textos puede ser de distintos tipos: a) el análisis de contenido en profundidad, que implica realizar una lectura y un análisis profundo de cada una de las respuestas obtenidas de las personas involucradas en el estudio, obteniéndose a partir de la codificación de cada una de ellas una idea sobre el todo; b) el análisis léxico, a partir del cual se hace un análisis de las palabras que componen las respuestas obtenidas, realizando distintos tipos de contabilización y navegación por las respuestas, permitiendo mediante el uso de *software* un proceso de lectura más rápido y automatizado.

En el trabajo se ha optado por el análisis de contenido en profundidad dado que –según los autores– a partir de la lectura reiterada se pueden enriquecer los temas que se están interpretando. La codificación resultante es expresiva, caracterizando la realidad inherente a la muestra y posibilita al analista el dominio pleno sobre los datos y las sutilezas de las entre-líneas del texto analizado.

Este proceso se ha desarrollado en tres etapas, que se describen a continuación:

3.6.1. Preparación y pre-análisis de los datos

En la primera fase, denominada de *descubrimiento* según la propuesta de Taylor y Bogdan (1987), se pretende identificar temas y desarrollar conceptos y proposiciones.

Hernández Sampieri et al. (2010) sostienen que para realizar un análisis adecuado de los datos éstos deben ser organizados. En primer lugar, se procedió a realizar la transcripción textual de las entrevistas grabadas. Posteriormente se compararon nuevamente los audios originales con el resultado de la transcripción para corroborar su fidelidad. A su vez, se comparó la información con anotaciones tomadas por el entrevistador en cada conversación, a fin de tener en cuenta cualquier aclaración útil para la interpretación de los resultados.

La investigación cualitativa requiere un análisis de los datos en progreso, como un proceso continuo, que se ejecuta de la mano de la recolección (Taylor & Bogdan, 1987). El pre-análisis de los datos mediante la lectura de las transcripciones y las anotaciones del entrevistador, permitió comenzar a identificar ideas generales, temas emergentes y puntos clave, verificar preguntas que

debían ser reforzadas en próximas entrevistas y definir los temas que se repetían con mayor frecuencia, comenzando a desarrollar proposiciones que daban sentido a los datos.

Se definió mediante la lectura de cada entrevista que el segmento de análisis adecuado serían los párrafos (Hernández Sampieri et al., 2010), en la medida en que cada uno de ellos podía referirse a un solo tópico y contener una idea completa que sirviera para su análisis. En consecuencia, estos fueron enumerados en forma correlativa en cada entrevista para su mejor identificación.

Este proceso requirió una lectura de los datos a partir de la cual se realizó una primera categorización basada en los tópicos relevantes definidos en el marco teórico, que fueron descriptos en la estructura del instrumento de recolección de datos. Dichos tópicos guiaron posteriormente el análisis de los resultados, permitiendo estructurar su comprensión y elaboración. Esta categorización se realizó asignando a cada párrafo el nombre de un tema en los que se dividiría el análisis de resultados, según se muestra en el Cuadro 18.

Cuadro 18 - Categorías para el análisis de los datos

NOMBRE DE LA CATEGORIA	TÓPICO
Perfil	Perfil del informante.
Utilización	Experiencia y grado de utilización de la CN en empresas argentinas clientes del entrevistado.
Conocimiento del cliente	Conocimiento del cliente de auditoría financiera y su entorno en ambientes de CN.
Riesgos	Identificación y valoración de riesgos de la CN relevantes para la auditoría financiera.
Controles internos	Evaluación del sistema de control interno en la nube.
Evidencias	Evidencias digitales de auditoría en la nube.
Conocimientos-Expertos	Conocimientos requeridos al contador público y colaboración de expertos en las auditorías financieras en la CN.

Fuente: Elaboración propia.

Con este primer análisis se pudo corroborar que en cada entrevista se habían tratado los diferentes temas definidos previamente como relevantes, y se comenzó a hacer una comparación tendiente a analizar la existencia de una saturación de categorías.

3.6.2. Análisis de los datos

En la segunda fase del trabajo con los datos se realizó una exploración más profunda del material, refinando la categorización y codificación de los mismos, así como la comprensión del tema de estudio. Esta etapa se ejecutó una vez finalizada la recolección de los datos.

Según Krause (1995:30-31) la codificación de la información consiste en fragmentar, conceptualizar y luego articular analíticamente los datos, generándose conceptos y categorías que tienen el carácter de hipótesis que son luego contrastadas.

Las categorías utilizadas han sido de dos tipos: en primer lugar se utilizaron las *categorías definidas a priori* según el esquema conceptual de la investigación (para cada una de las categorías de primer nivel asignadas en el punto anterior se otorgaron sub-categorías de acuerdo a los temas específicos tratados en cada párrafo). Luego surgieron las denominadas *categorías emergentes*, que resultaron a partir de la clasificación progresiva de los elementos sobre aspectos que no habían sido considerados a partir de la revisión bibliográfica. Estas últimas maximizan las posibilidades de descubrir algo nuevo sobre el objeto de estudio (Krause, 1995:30).

Habiendo finalizado el pre-análisis de la información, se procedió entonces a realizar el análisis de los datos, el cual se dio en forma progresiva, generando una fragmentación y organización de las fuentes según diferentes criterios, y un análisis mediante comparación permanente, según se describe a continuación[10]:

a) En primer lugar, se separaron los datos pertenecientes a los diferentes tópicos de acuerdo al pre-análisis. Es decir, el material de las entrevistas fue fragmentado por tópico o categoría, manualmente en archivos electrónicos y en papel, identificando en forma adecuada el informante que había dado cada una de las respuestas y sin perder la unidad original completa de cada entrevista.

b) Se inició el análisis profundo sobre cada uno de los temas, por separado a nivel de cada entrevistado. Para ello, se buscó comprender el contenido de las respuestas, tomando nota de los temas tratados, asignando las sub-categorías predefinidas e identificando categorías emergentes. Esto permitió refinar el esquema de categorías planteado inicialmente.

c) Posteriormente, sobre cada bloque de temas, se analizaron las respuestas de los informantes en forma comparativa, a fin de determinar puntos de convergencia y diferencias en relación a determinadas cuestiones. En este análisis se tuvo en cuenta el área del cual provenía cada informante (auditoría financiera o de sistemas), lo cual podría enriquecer la comprensión de los datos.

d) La estrategia de *comparación permanente* permitió generar los resultados que fueron registrados en forma de texto y resúmenes gráficos relacionados a cada tema en particular. El proceso continuó con la contrastación de los conceptos e hipótesis con los datos siguientes, corrigiéndolos sobre la base de la nueva evidencia, generando nuevos conceptos hasta lograr la saturación teórica de las categorías conceptuales que surgieron en el análisis, esto es, el momento en que los nuevos datos no agregan nueva información.

En este punto se tuvo especial cuidado en intervenir los documentos de manera tal de asegurar que ningún fragmento fuera utilizado en más de un punto de la investigación. Esta precaución sirvió también para poder identificar los *datos sobrantes*. Respecto de los mismos, se analizó si pertenecían a alguna de las categorías predeterminadas, si permitían la incorporación de

[10]La propuesta de Taylor y Bogdan (1987:167-170) en relación a la fase de *Codificación* fue la base para esta propuesta de análisis.

una categoría emergente, o si realmente eran datos que no debían ser utilizados a los fines del estudio.

A partir del proceso de codificación, siguiendo los pasos mencionados, se logró reunir y analizar en conjunto todos los datos referidos a un mismo tema o tópico. En los casos en los que en el análisis de un tópico se encontraran respuestas que pudieran aportar al análisis de otro, se tomaban notas respectivas para efectuar las relaciones correspondientes.

El Cuadro 19 esquematiza la organización de los datos y los niveles de análisis realizados.

Cuadro 19 - Esquema de análisis de los datos

ETAPA	NIVEL	ASPECTOS CONSIDERADOS
1er análisis	A nivel de entrevistado	Lectura del material perteneciente a cada entrevistado e identificación de tópicos y categorías.
2do análisis	A nivel de tema o categoría	Lectura del material de todos los entrevistados, vinculado a un tema o categoría en particular (posterior a la fragmentación) identificando sub-categorías aplicables.
3er análisis	A nivel de categoría y sub-categoría, en forma comparativa entre informantes.	Lectura del material de todos los entrevistados, vinculado a las subcategorías, realizando comparaciones entre los diversos informantes, considerando su área de desempeño profesional (auditoría financiera o de sistemas).

Fuente: Elaboración propia.

3.6.3. Interpretación y elaboración de resultados

En la última etapa, una vez clasificados y analizados en conjunto los datos obtenidos de los informantes, se procedió a su tratamiento e interpretación, a fin de dar validez y significatividad a la información. Se orienta a relativizar los descubrimientos, comprendiendo los datos en el contexto en que fueron recogidos (Rapley, 2004) a fin de evaluar su credibilidad (Taylor & Bogdan, 1987:171).

En la elaboración de los resultados se tienen en cuenta las interpretaciones realizadas a partir del análisis de los datos, pero se utilizan además ejemplos y citas, a fin de clarificar los conceptos, permitir al lector acceder a datos que respaldan las conclusiones y brindar confiabilidad a las mismas (Taylor & Bogdan, 1987).

3.7. VALIDEZ DE LOS DATOS

En la investigación cualitativa se pone énfasis en la validez de la investigación, procurando un ajuste entre los datos y lo que los informantes realmente dicen o hacen; distinto al caso de la investigación cuantitativa, en la que se busca la confiabilidad y reproducibilidad de la investigación. Con este fin se realizaron *controles cruzados* (Taylor & Bogdan, 1987:127).

Durante el desarrollo de las entrevistas esto se logró repreguntando a los informantes sobre una misma situación en diferentes momentos de la conversación, e intentando relacionar sus dichos

con cuestiones mencionadas previamente, a fin de garantizar la adecuada comprensión y coherencia en los discursos.

Por otro lado, en los casos en los que pudo entrevistarse más de un profesional del mismo estudio, siendo que estos habían compartido equipos de trabajo, se analizó la coherencia de experiencias y opiniones mencionadas por unos y otros. En muchos casos, los mismos informantes hacían referencia a información que podría ser provista con mayor detalle por el otro profesional de su estudio, en general por cuestiones de especificidad en los temas tratados y formación de los entrevistados.

En todos los casos, dichos controles cruzados sobre las afirmaciones de los informantes fueron satisfactorios.

4. CARACTERIZACIÓN DEL OBJETO DE ESTUDIO. PERFIL DE LOS PROFESIONALES ENTREVISTADOS

Tal como fue explicado en el capítulo *3. Metodología*, las entrevistas fueron realizadas a profesionales de los cinco principales estudios de auditoría de Argentina. Los participantes pertenecen tanto al área de auditoría de estados contables como al de consultoría y auditoría de sistemas. La incorporación de éstos últimos a la investigación se dio por dos razones: a) las recomendaciones realizadas por los Revisores 2 y 3, descriptas en el apartado *3.3.*; b) en todos los estudios, los contactos obtenidos propusieron que se entrevistara a los profesionales del área de TI.

Las políticas de las grandes firmas de auditoría para aquellos encargos en los cuales los auditores financieros deban confiar en información obtenida de sistemas informáticos y en los controles implementados en los procesos computadorizados, establecen que se debe realizar una revisión del área de TI o una auditoría de sistemas, que involucra a expertos en la materia (Entrevistado 3).

En consecuencia, personal del área de auditoría de TI o de consultoría de los grandes estudios generalmente participa del proceso de auditoría para la toma de conocimiento y evaluación de los sistemas. Existe una separación de funciones entre dos sectores, y al mismo tiempo una interacción y retroalimentación entre ellos. Por dicha razón los expertos de TI fueron referenciados por los contactos como personas competentes para participar de la investigación.

Al inicio de cada entrevista se solicitó a los participantes que describan su perfil profesional, brindando datos de su formación y experiencia laboral. Esto permitió evaluar las características de los informantes y la pertinencia de su participación a los fines de la investigación, y considerar a priori la calidad de sus respuestas.

A continuación, se describe el perfil de cada uno de ellos, elaborado a partir de la información obtenida de su parte y datos obtenidos de Internet. El orden en que se describen es aquel en que fueron contactados. El nombre que se les otorga ("Entrevistado X") será el que se utilice en el desarrollo de la tesis para referenciarlos.

- **ENTREVISTADO 1**[11]

Ingeniero Electromecánico, con orientación Electrónica, recibido en la Universidad de Buenos Aires en 1982.

Fue Gerente en Consultoría y Auditoría Informática en un estudio de auditoría (1989-1998) y Gerente de Seguridad Informática en una entidad financiera (1998-2002). Integró la Comisión Directiva del capítulo Buenos Aires de ADACSI ISACA (1996-2010), el Comité Académico de

[11] Por razones de anonimato y confidencialidad, se eliminaron los nombres de las empresas en las que se han desempeñado los entrevistados a lo largo de su carrera.

Usuaria Segurinfo (2001-2011) y desde 2011 a la actualidad forma parte del Comité Consultivo de Segurinfo.

Actualmente es Socio del estudio en el área Aseguramiento de Procesos Informáticos. Su área comprende auditoría informática, de tecnología y de la información; seguridad informática y de la información; computación forense; riesgos de IT; *compliance* (cumplimiento) de normas nacionales e internacionales.

Las auditorías informáticas ejecutadas por el área a su cargo se desarrollan en conjunto con equipos de profesionales no informáticos –entre ellos contadores públicos–, particularmente en relación a auditorías de estados financieros.

Además, se realizan auditorías de bases de datos, de interfaces, de sistemas operativos, de tecnologías particulares, de proyectos informáticos. El equipo de auditores posee distintas especializaciones, como por ejemplo aquellos dedicados a entidades financieras, cuya auditoría está altamente relacionada a las regulaciones que tiene en Argentina el Banco Central.

El entrevistado es representante de Latinoamérica en una comisión internacional de auditores de sistemas dentro del estudio en el que trabaja. Dentro de ella, existe una comisión en la que anualmente se realizan búsquedas de nuevos estándares y se adaptan o crean nuevos planes y programas de auditoría de sistemas adaptados específicamente para colaborar con la auditoría financiera.

- **ENTREVISTADO 2**

Analista de sistemas de nivel universitario, posee además certificación CISA (*Certified Information Systems Auditor*, por ISACA).

Se desempeñó como líder de proyecto de desarrollo en una consultora (1997-2000), en la cual trabajó con tecnología de avanzada sobre un ERP (*Enterprise Resource Planning*, por sus siglas en inglés) en la nube por requerimiento de una empresa ".com". Dicho proyecto se agotó en los años 2000-2001 por la crisis que sufrieron estas empresas.

En el período 2001-2004 se desempeñó en un estudio propio, dedicándose a la implementación de nuevas tecnologías. Se vinculó a un estudio de auditoría desde mediados de 2004, ingresando como *Senior*. En el año 2007 fue nombrado gerente, cargo desempeñado hasta diciembre de 2012.

Durante los ocho meses posteriores, trabajó en un proyecto para el desarrollo del área de TI en un estudio impositivo, y desde noviembre de 2013 se desempeña como auditor de sistemas en el estudio al que pertenece actualmente.

Como fortaleza destaca que en todos los proyectos en los que participó sus desarrollos se vincularon a sistemas ERP, lo cual le facilitó luego su trabajo en auditorías informáticas en apoyo a las de estados contables.

- **ENTREVISTADO 3**

Contador Público, recibido en 1995 en la Universidad Argentina de la Empresa (UADE).

Trabajó previamente en un estudio de auditoría muy pequeño en la Argentina, haciendo auditorías contables. Luego integró el estudio Arthur Andersen (1996-2002). Desde el año 2002 trabaja en el estudio actual, siempre en el área de sistemas. Desde 2013 es Director Ejecutivo del área de consultoría.

Mencionó como fortalezas para participar de la entrevista que el sector a su cargo se ocupa de la evaluación de los controles internos de los sistemas que alimentan la auditoría de estados contables, así como su vasta experiencia en presentaciones frente a la Inspección General de Justicia (IGJ) en Capital Federal de los Informes de Contador Público Independiente para obtener la autorización para llevar los registros contables en un medio mecánico –siendo estos para la IGJ cualquier medio que no sea un libro copiativo rubricado (Art. 61, Ley General de Sociedades, Nro. 19.550).

- **ENTREVISTADO 4**

Ingeniero en sistemas, recibido en la Universidad Nacional de la Matanza (2001). Ingresó al estudio como asistente en el año 1997, trabajando siempre en el área de Auditoría de Sistemas.

En su formación de grado se especializó en el área de sistemas de información –descartando el área de desarrollo–, a fin de perfeccionarse en el área de auditoría en la cual se estaba desempeñando en el estudio.

En sus 16 años de experiencia fue creciendo dentro del mismo estudio, hasta llegar a ser actualmente Gerente del Área de *Enterprise Risk Services* (ERS), en el área de Auditoría Externa de Sistemas. Dicho área se divide en dos partes: auditoría del sistema propiamente dicha –a nivel de equipamiento, bases de datos y desarrollo– y de procesos –contables, financieros, de compras, ventas, inventarios, focalizado en los controles automáticos o sistematizados. Trabaja con clientes de distinto tipo, incluyendo empresas financieras, de seguros, manufactureras, de medios, de publicidad.

A su vez, en el estudio es referente o responsable de capacitación en el área de interrogación de archivos mediante herramientas informatizadas, brindando cursos en forma anual.

- **ENTREVISTADO 5**

Contador público recibido en la UBA (1998-2005) y *Master of Business Administration* (MBA) en Administración y gestión de empresas de la Universidad Argentina de la Empresa (2008-2010)

Inició su carrera profesional en una editorial médica Pyme (2000-2005), donde trabajó como analista contable. Según mencionó, el conocimiento allí obtenido le fue de mucha utilidad al

momento de desempeñarse como auditor, porque conoció en profundidad cómo funciona la administración de una PyME.

Posteriormente, luego de un breve paso por otra empresa, ingresó en Enero de 2006 en el estudio en el área de auditoría de estados contables. Allí ascendió a *Senior* (2007-2011), llegando a ser Gerente (2012), cargo en el cual permanece.

En su trayectoria como auditor financiero ha tenido clientes muy variados, incluyendo rubros como textil, publicidad, cines, petróleo, entre otros, habiendo trabajado principalmente con clientes del sector agropecuario. Ello le ha brindado experiencias muy variadas.

- **ENTREVISTADO 6**

Contador Público recibido en la Universidad de Buenos Aires (1988-1997), posee una Maestría en Sindicatura Concursal-Administración de empresas en crisis (2004-2005).

Fue Auditor en la Sindicatura General de la Nación (1994-1999). En 1999 ingresó al estudio donde se desempeñó como *Senior Manager*, accediendo en 2012 al cargo actual de Director del área de Auditoría de Sistemas y Procesos. Se ha especializado en consultoría y auditoría en compañías de distintas industrias, incluyendo agronegocios, minería, automotriz y *retail* (venta al por menor). Ha trabajado en proyectos en diferentes países, incluyendo Argentina, Brasil, México, España, Puerto Rico y Chile.

El área del cual es director es la que, básicamente, da soporte al área de auditoría contable en lo que hace a sistemas y procesos, razón por la cual consideró ser una persona indicada para entrevistar dentro del estudio.

- **ENTREVISTADO 7**

Contador Público, recibido en la Universidad Argentina de la Empresa (2012).

Fue administrativo *Senior* en una empresa, a cargo de tareas generales de administración y finanzas (2007-2008).

En el año 2008 ingresó al estudio actual. Allí posee el cargo de *Senior* A –o *Senior* Experimentado–- en el área de auditoría contable. Ha trabajado con diversos tipos de clientes, incluyendo laboratorios y petroleras. Actualmente se desempeña en forma permanente en el sector de *Oil and Gas*, habiendo sido asignado a una empresa en particular en la cual permanecerá hasta su ascenso a gerente. Habiendo estado designado en encargos de grandes empresas, ha trabajado no sólo con normas nacionales, sino también con USGAAP y Normas Internacionales de Contabilidad.

A pesar de desempeñarse como *Senior*, consideró adecuada su participación en la investigación dado que, debido a los años de experiencia en el cargo, se ve involucrado en todas las etapas del proceso de auditoría. Participa en la planificación, incluyendo evaluación de riesgo y selección de procedimientos (sujeto a revisión de gerentes y socios); en la ejecución, aplicando

procedimientos globales y dirigiendo al equipo de auditoría a su cargo; y en el cierre, mediante la revisión final de los estados contables.

Destacó que en la etapa de planificación participa de la coordinación con personal de las áreas de *Tax* (Impuestos) y TI. Justifica además su participación en la investigación debido a que, en relación a estos últimos, participa de reuniones con los especialistas para la definición del alcance de las pruebas de funcionamiento de los controles sobre los sistemas de las empresas auditadas.

- **ENTREVISTADO 8**

Contador público egresado de la Universidad Nacional de Córdoba (1998-2003). Posee una Maestría en Contabilidad Internacional de la Universidad de Buenos Aires (UBA) (2007-2010), un Posgrado en Docencia Universitaria también de la UBA (2011-2012) y ha realizado diversos cursos de postgrado vinculados a normas contables nacionales e internacionales.

Es docente universitario en la Universidad Austral (desde 2009) y la Universidad de Belgrano (desde 2008). Ha tenido a su cargo el dictado del Curso Especialización en Normas Contables y de Auditoría Nacionales e Internacionales en el Consejo Profesional de Ciencias Económicas de la Ciudad Autónoma de Buenos Aires.

Se desempeña en el estudio desde el año 2003. Fue *Senior* desde 2003 al 2009, y desde dicha fecha es gerente de auditoría de estados contables. Siempre ha trabajado en el área de auditoría contable, con empresas comerciales (excluyen a las entidades financieras y de seguros). Además participa en la división capacitación como coordinador y como instructor en cursos internos de la firma.

Ha trabajado en clientes de diversos tamaños[12]; desde que ascendió a gerente tomó a su cargo diversos clientes chicos. Según mencionó, esto le ha brindado distintas experiencias, ya que los trabajos son muy diferentes unos de otros: el proceso en los clientes chicos es un poco más manual y en los grandes mucho más tecnológico. Ello se debe a que los grandes hacen un uso mucho más amplio de las aplicaciones de los sistemas que implementan, como por ejemplo SAP – no sólo bajada básica de mayores contables como en el caso de los pequeños, sino cuestiones más complejas como consolidaciones automáticas– y poseen mayor cantidad de personal abocado al área de sistemas.

4.1. RESUMEN

La caracterización de los entrevistados resulta útil para la interpretación de las respuestas obtenidas en las entrevistas.

[12] El tamaño de los clientes se mide por la cantidad de horas dedicadas a la auditoría.

Cinco (5) de los ocho (8) entrevistados se desempeñan en el área de TI dentro de los estudios de auditoría, ya sea como auditores o consultores. Habiendo sido propuestos por sus colegas como las personas competentes para participar de la investigación, se enfatiza la importancia de haber incorporado a los auditores de sistemas en la muestra. Debe tenerse en cuenta que, al momento de evaluar las respuestas, puede existir una orientación hacia aspectos técnicos, debido a la propia formación de los entrevistados.

Al efectuar el análisis de los datos siempre se intentará confrontar las opiniones de quienes poseen un perfil de sistemas respecto de quienes poseen un perfil contable (o de auditoría financiera), a fin de identificar los puntos de similitud o divergencia respecto de los potenciales efectos de la computación en la nube sobre la auditoría de estados contables.

El Cuadro 20 resume el perfil de todos los profesionales que han participado de la investigación.

Cuadro 20 - Perfil de los entrevistados

ENTREVISTADO	FORMACIÓN	CARGO ACTUAL	AÑOS DE EXPERIENCIA	PERFIL
Entrevistado 1	Ingeniero Electromecánico, con orientación Electrónica.	Socio - Aseguramiento de Procesos Informáticos.	26 años	Sistemas
Entrevistado 2	Analista de Sistemas. CISA.	Auditor de Sistemas.	16 años	Sistemas
Entrevistado 3	Contador Público.	Director Ejecutivo del área de Consultoría.	19 años	Sistemas
Entrevistado 4	Ingeniero de Sistemas.	Gerente de ERS – Auditoría de Sistemas.	16 años	Sistemas
Entrevistado 5	MBA Administración y gestión de empresas. Contador Público.	Gerente de Auditoría.	9 años	Contable
Entrevistado 6	Magíster en Sindicatura Concursal y Administración de Empresas en Crisis. Contador Público	Director de Auditoría de Sistemas y Procesos.	16 años	Sistemas
Entrevistado 7	Contador Público	*Senior* A de Auditoría.	6 años	Contable
Entrevistado 8	Magíster en Contabilidad Internacional Contador Público.	Gerente de Auditoría. Docente.	11 años	Contable

Fuente: Elaboración propia con base en los datos de la investigación.

5. RESULTADOS

5.1. ESTADO DE UTILIZACIÓN DE LA CN EN EL CONTEXTO ARGENTINO[13]

"Confiamos en que en nuestro país la implementación en la nube tendrá una aceptación exitosa, al igual que en el resto de América latina".

Marina Hasson
Gerente de Canales de Microsoft para Argentina y Uruguay
(Iprofesional, 2014)

El presente apartado tiene el propósito de dar cumplimiento al primer objetivo específico planteado para esta tesis:

Indagar respecto de la utilización de la CN por las empresas argentinas.

A partir de ello es posible:

- Describir el contexto argentino respecto de la utilización de la computación en la nube de acuerdo a la experiencia de los entrevistados, confrontando con los resultados otros estudios que lo han analizado (ORACLE-MERCADO, 2013; USUARIA 2013, 2014).
- Conocer las características del entorno en el que se desempeñan los informantes y su nivel de conocimiento y familiaridad con la nueva tecnología y con alternativas de tercerización de TI similares, lo cual permitiría valorar la calidad de las respuestas recibidas.

Una vez realizada la introducción de la investigación, y habiendo obtenido los datos referidos al perfil de los entrevistados, se les propuso que comentaran sobre dos aspectos: a) su experiencia en el uso de servicios de CN; b) su práctica en relación a clientes del estudio de auditoría que utilizaran o estuvieran evaluando aplicar soluciones de tercerización de TI, en particular en la nube, describiendo las alternativas implementadas.

Del análisis de las respuestas surgieron dos categorías emergentes: factores que demoran la implementación de la CN en la Argentina y aspectos que la favorecerían. Si bien estos aspectos no se vinculan específicamente con el objetivo general de la investigación, se ha decidido incluir estas respuestas en la medida en que ayudan a contextualizarla y demuestran el conocimiento que los profesionales poseen de la tecnología y de la realidad actual en el país sobre el tema analizado.

5.1.1. ALTERNATIVAS DE CN UTILIZADAS EN LA REPÚBLICA ARGENTINA

La utilización de la computación en la nube por parte de las empresas es una realidad innegable, siendo necesario que los estudios de auditoría adapten sus procedimientos a esta nueva situación (Entrevistado 6). Sin embargo, la mayoría de los entrevistados concuerdan en que los

[13] Una adaptación de este capítulo fue incluida en el trabajo denominado "Computación en la Nube: Una alternativa de TI para las PyMEs", elaborado en co-autoría con la Mg. Diana Albanese y la Mg. Regina Duran. Veáse López, Albanese & Durán (2015).

servicios implementados hasta el momento por empresas argentinas no incluyen los procesos principales (*core*) de negocio, sino que se refieren más bien a procesos de apoyo.

Los servicios más utilizados se refieren en general a alternativas de tipo SAAS (*Software* como un Servicio). Esto es, no se orientan al desarrollo de aplicaciones propias en la nube, las cuales requieren del conocimiento de expertos dentro de la empresa, sino a aquellas disponibles para su utilización dentro de los procesos del ente.

Se exponen a continuación las experiencias descriptas por los entrevistados en relación a la CN y otros casos de tercerización, divididas por el área de pertenencia de los profesionales (de sistemas y financieros). La descripción se realiza identificando a cada profesional, a efectos de determinar el nivel de conocimiento de cada uno de ellos.

A) Auditores de sistemas

Los auditores de sistemas demostraron tener un mayor dominio del tema en cuestión, principalmente por razones de su formación y experiencia profesional.

El Entrevistado 4 ha prestado servicios a clientes que hacen uso de servicios en la nube, quienes lo han implementado como una obligación, siendo que sus casas matrices en Estados Unidos han optado por esta tecnología. El mismo ha tenido oportunidad de auditar estos entornos de TI. Uno de los casos se refiere a una empresa de publicidad, que posee su información financiera en la nube para poder consolidarla con la de su casa matriz en el exterior. Su trabajo en el año 2013 consistió en efectuar una auditoría de sistemas, cuyos resultados fueron utilizados por los auditores financieros en la etapa de evaluación del sistema de control interno. Un año después, el trabajo consistiría en realizar la planificación de la revisión sobre dicho sistema.

Según indica, en su experiencia esta situación representó todo un cambio de paradigma para el desarrollo de la labor de auditoría. Según sus palabras:

> Cuando pude hablar con esta empresa (…) para mi resultó ser una especie de cambio de paradigma. Porque yo iba y le preguntaba: "¿Cuál es la plataforma donde está tu sistema contable?" Yo me refería a la parte de Windows, UNIX… "No, está montado en Google…"… Y la verdad quedé totalmente descolocado, y tuve que empezar a investigar acá en el estudio para ver de qué se trataba. (Entrevistado 4)

Esta apreciación revela que las primeras experiencias de auditorías en la nube son novedosas, no esperadas e implican que los auditores muchas veces no se encuentran preparados para el desarrollo de estos encargos, en la medida en que –para los auditores de sistemas en particular– el uso de la CN por parte de los clientes representa un cambio significativo en su trabajo.

A su vez, el profesional mencionó conocer el caso de utilización de soluciones en la nube para el procesamiento de información interna del ente, por ejemplo para la elaboración de reportes e informes gerenciales, aun cuando no se refiera a información contable. Esto es, por ejemplo,

sistemas corporativos de casas matrices ubicadas en el exterior, que exigen a las filiales cargar cierta información a la herramienta para lograr su consolidación, sin que necesariamente ello alimente al sistema de información contable utilizado para la preparación de los estados financieros, sino más bien a los sistemas de gestión. Por otra parte, las soluciones provistas en la nube permiten procesar una gran cantidad de información, que puede ser recuperada de los sistemas internos, y realizar diversos tipos de análisis y presentaciones de reportes mediante aplicaciones que muchas veces no están disponibles en las soluciones adquiridas bajo el formato *on-premisse*, principalmente en el caso de empresas de tipo PyMEs.

Como elemento adicional que respalda la experiencia del entrevistado, mencionó casos de tercerización aplicada por clientes argentinos del estudio, que si bien no responden exactamente a la concepción de la nube, poseen características similares:

a) casos de una entidad financiera y una empresa productora y comercializadora de agroquímicos, cuyas casas matrices se encuentran en el exterior –España y Estados Unidos respectivamente– que a nivel corporativo hacen uso del sistema SAP.

En estos casos, por tratarse de un sistema *core* financiero, se encuentra alojados en la casa matriz. Las operaciones ejecutadas en Argentina –como la carga de una venta– quedan registradas, son procesadas y almacenadas en los equipos que se encuentran ubicados en el exterior.

Aquí el entrevistado mencionó que podría no considerarse una nube, dado que el ente es propietario de la licencia para el uso del sistema, el cual se encuentra ubicado en equipos propios, que son administrados por su personal; es decir, no existe tercerización. Las similitudes se refieren al traslado de la información a través de Internet y su alojamiento en jurisdicciones distintas a la República Argentina, con imposibilidad de acceso por parte de los auditores locales;

b) empresas que tercerizan la guarda de equipos y servidores y la gestión de las medidas de seguridad inherentes en organizaciones de servicios que poseen centros de cómputos o de procesamiento hiper-protegidos, y que prestan el mismo servicio a diversos clientes.

El Entrevistado 6 se refirió al nivel de utilización en general, respaldando la experiencia del Entrevistado 4. Si bien reconoce que la CN es *la novedad del momento*, la mayoría de las grandes compañías aún no han migrado su sistema de gestión contable a la nube, sino que han comenzado con soluciones más sencillas, como respaldo de archivos (*file server*), correo electrónico u otro tipo de soluciones no vinculadas directamente a la gestión de información financiera. Sin embargo, en muchos casos estos procesos que parecen no esenciales suelen tener relación con la auditoría de estados financieros, por ejemplo en el caso del *e-mail*.

> Si bien el correo, hasta no hace mucho tiempo, no era una aplicación crítica, hoy muchos procesos de autorización o declaraciones de por sí o de por no, quedan evidenciados a través de transacciones plasmadas en e-mails; incluso hay confirmaciones de evidencias que quedan documentadas en correos electrónicos. En definitiva, el auditor lo que busca es el sustento sobre determinada información contable o sobre determinada característica de la información, que a veces queda en otros sistemas. (Entrevistado 6)

En su respuesta se ha referido expresamente a empresas grandes, que son con las que trabajan habitualmente dentro del estudio en el cual se desempeña. Lo mismo ocurre en general con el resto de los entrevistados. Sin embargo, muchos autores han documentado la importancia y el nivel creciente de uso de la CN en el caso de empresas PyMEs, como ser Budniks y Didenko (2014), Marino (2014), Sultan (2011) y Tarmidi et. al. (2014).

En su opinión, también confirmando lo dicho por el Entrevistado 4, para la auditoría de sistemas –íntimamente vinculada a la auditoría financiera– estos entornos plantean un nuevo paradigma, que requiere la búsqueda de soluciones y respuestas que hoy todavía no están preparados para darlas, representando un nuevo desafío para los profesionales. Entre los principales obstáculos se refirió a la dificultad para identificar la ubicación física de los equipos, quiénes son los que los administran, los propietarios de las aplicaciones, quiénes pueden acceder a la información almacenada, todas cuestiones que entorpecen el normal desarrollo de la auditoría de sistemas tal como está planteada hoy en día.

Sin embargo reconoció que el proceso de adaptación obligatoriamente deberá ocurrir, porque de lo contrario se estaría desconociendo la realidad, en la medida en que las empresas apuntan a utilizar la nube en el futuro por los beneficios que ella otorga.

Por su parte, el Entrevistado 3 reitera que en la Argentina el uso de la CN aún no es una práctica corriente a pesar de su popularidad, al menos para la elaboración de la información contable, si bien reconoce su aplicación a otros procesos.

En este sentido, mencionó conocer casos concretos de clientes de auditoría y consultoría que implementan o están evaluando alternativas de CN para correo electrónico (de hecho su estudio lo tiene *hosteado* en la nube) y aplicaciones para la gestión de recursos humanos, referidas principalmente la gestión de novedades de nómina, consulta de recibos de sueldos y planes de capacitación.

Al igual que los demás auditores, mencionó poseer clientes que son sucursales de una casa matriz que se encuentra en el exterior, cuyos sistemas están alojados donde ella se localiza –esto es, que los servidores están físicamente fuera de Argentina. En algunos casos, incluso la casa matriz tiene alojados los servidores en un tercero, como ser IBM o HP. La justificación de esta práctica es que las compañías a nivel mundial pretenden tener un único ERP y que todas las empresas de las distintas regiones trabajen con el mismo modelo de negocios y los mismos procesos.

La falta de casos concretos de clientes de auditoría financiera que hagan uso de la nube justifica que dentro del estudio en el que se desempeña, en Argentina, aún no se haya previsto un programa de trabajo concreto para la realización de auditorías de sistemas en este contexto. Cabe mencionar que, desde su perspectiva, la CN no es algo totalmente inesperado para los auditores, sino que desde hace algunos de años que se está hablando de este tema.

En relación con el nivel de preparación que pueden tener los auditores para afrontar este tipo de encargos realiza una diferenciación entre los BIG4 y los estudios de auditoría más pequeños. En su opinión, en los estudios internacionales, que poseen el *know how* por las experiencias en otros países, el camino parece ser más sencillo. Esto es, ante una nueva situación, poseen en sus bases de datos bibliotecas, capacitaciones y la información que necesitan para formarse y trabajar en el nuevo entorno. Esta situación refuerza la decisión adoptada en el desarrollo de esta tesis de, por un lado, trabajar con profesionales de los grandes estudios que podrían tener mayor conocimiento del tema en cuestión, y por el otro, incorporar a los auditores de sistemas.

> Yo creo que las compañías como pueden ser las "BIG4", al tener casas matrices en Estados Unidos o en Europa, donde ya se están preparando, están más adelantados. Entonces para las locaciones como puede ser Argentina o Sudamérica, que a lo mejor venimos más atrasados en cuanto a temas de tecnología y estas novedades informáticas, yo creo que en una "BIG4" estamos preparados, pero porque tenemos la experiencia a nivel metodológico y a nivel de mejor práctica de afuera. (…) Muy probablemente en Estados Unidos haya clientes que quizás estén en la nube, y como todo son bases compartidas de conocimiento, nos adaptaremos, preguntaremos y nos van a explicar cómo tenemos que hacer una auditoría así. (…) Seguramente a un estudio más pequeño o estudios locales, sí les cueste un poco más este tema, adaptarse, entender y ver cómo pueden auditar una compañía que tiene la información en la nube. (Entrevistado 3)

El Entrevistado 2 también manifestó tener clientes de la República Argentina que *han dado el salto a la nube*. En particular se refirió a dos entidades financieras que corporativamente han implementado soluciones de *e-mail* en la nube y relacionado a ello lo referido a *file server*, no así los sistemas *core* ni transaccionales. Según explicó, la información sensible de los clientes sigue obrando en los sistemas transaccionales, que están implementados localmente (esto es, en servidores propiedad del ente). Los correos o la información que se encuentra en la nube no deberían contener este tipo de información, dada la confidencialidad y las limitaciones que impone la propia normativa del Banco Central de la República Argentina.

Siendo un sector en el que se hace un uso intensivo de la información, la CN puede ser ventajosa para otros procesos. Estos otros usos también están sujetos a la aplicación de la normativa indicada y a la evaluación de los riesgos estratégicos, reputacionales, legales y operacionales a los que se expone la entidad (López et al., 2014).

La respuesta concuerda con Noceti y Freijo (2015) quienes coinciden en que no existe aún una implementación masiva de la CN por parte de las entidades bancarias y su uso se limita a aplicaciones no vinculadas al negocio principal, sino más bien a mail corporativo, soluciones de productividad y colaboración, aplicaciones de oficina. Justifican que esto se debe principalmente a que el cambio es importante, requiriéndose previamente una maduración del mercado y los proveedores, además del riesgo de incumplimiento de normativa aplicable a esta industria. Los autores proponen algunas alternativas de usos que serían posibles para las entidades financieras, como servicios SAAS para aplicaciones no críticas del negocio, o nubes privadas que permitan

aprovechar sus beneficios, pero manteniendo el control sobre los datos y sistemas sensibles, entre otros.

Al menos hasta el momento, los usos que están haciendo las entidades financieras argentinas de la nube no estarían afectando en forma significativa la elaboración de la información contable que luego se utiliza para la preparación de los estados financieros. De todos modos, esto demuestra un comienzo en su aplicación. Aun cuando no fuera posible generalizar el uso de esta TI para sus operaciones transaccionales, son un antecedente para su implementación por otros entes, según se describe en el punto *5.1.2. Motivadores del uso de la CN.*

El Entrevistado 1 es el único que resta un poco de importancia a la novedad que representa la CN para la auditoría, asimilándolo a otros casos de tercerización. L*a nube es un mecanismo más de outsourcing que está muy de moda comercialmente*, mencionó. En este sentido considera que en todas las auditorías en entornos de tercerización de TI se requiere hacer un mayor énfasis en lo que ello implica. Según expresó:

> Esto es una tercerización, y es una delegación de algo, pero quien delega no deja de ser dueño de aquello que terceriza. (…) Yo puedo delegar operación, donde va a estar el repositorio de datos, quien va a hacer el *back up* o donde lo va a alojar; puedo delegar parte de las comunicaciones; pero quien tiene que definir la seguridad, las normas y los reportes hacia esos terceros soy yo. Ahí yo creo que se está fallando bastante, en la poca exigencia que hay de parte de las empresas usuarias sobre los proveedores de los servicios. (Entrevistado 1)

Es así que, para la generalidad de las auditorías en entornos de tercerización, considera que se debe agregar en los planes y programas de auditoría una mayor revisión de estas cuestiones. Opina que, si bien estaban incluidos, *no se hace suficientemente bien en todos lados.*

Menciona que, desde su experiencia y punto de vista, en relación a las auditorías en entornos de CN recién están saliendo algunas publicaciones más interesantes, como la *IT control objectives for Cloud Computing, de ISACA (2011), orientada a ayudar al auditor informático, y algunas otras emanadas de asociaciones internacionales de auditores internos y de contadores públicos.* Si bien considera que existe bastante bibliografía que puede apoyar una auditoría en un entorno de la nube, él lo ve como un caso más de tercerización.

B) Auditores financieros

A continuación se describen las experiencias de los auditores financieros. Éstos demostraron tener un menor nivel de conocimiento respecto de la CN y las consecuencias de su uso por parte de los entes auditados, lo que se justifica en parte en la separación de funciones y especialización que existe en los grandes estudios de auditoría: auditores de sistemas y auditores contables, con campos de actuación fuertemente diferenciados (esta cuestión fue mencionada por todos los auditores contables). Esta situación refuerza una vez más la decisión de haber incorporado a los auditores de sistemas en la investigación.

En primer lugar, el Entrevistado 8 menciona que el uso de la CN por parte del ente auditado genera cambios en el proceso de auditoría financiera y en la de sistemas, considerando que su mayor impacto se da en esta última. A su vez, describe dos experiencias que consideró relevantes a los efectos de la entrevista:

a) En primer lugar, la utilización en el estudio en el cual se desempeña de una herramienta de trabajo colaborativo para el intercambio de documentación entre auditores y clientes a través de Internet. En un ambiente compartido por ambos actores, los profesionales cargan los requerimientos de información y las fechas en que se necesitan, y el personal del ente auditado las respuestas (sumas y saldos, mayores contables, documentación de respaldo de dicha información, etc.).

Originariamente se utilizaba para el intercambio de información ente diferentes oficinas del estudio de auditoría en el mundo. Según indicó, comenzó a aplicarse con los clientes para agilizar los pedidos de información y las respuestas respectivas, de modo de poder preparar los estados contables en forma oportuna. A la vez se obtiene un registro de la ruta de la documentación –momentos de solicitud y respuesta– para determinar las responsabilidades de las demoras en la ejecución del encargo.

Allí el gerente de la auditoría y el gerente financiero del ente son los administradores y poseen acceso a toda la información compartida, mientras que el resto de los miembros del equipo de auditoría y del auditado poseen un acceso restringido, administrado por los primeros.

Una vez cerrada la auditoría, la información permanece allí por un plazo breve para que pueda obtenerse lo necesario para la adecuada documentación de la labor realizada en los papeles de trabajo del auditor. Finalizado el mismo, es destruida por razones de confidencialidad. Solo se retiene la información documentada por los plazos que establezca la normativa a los fines probatorios en instancias judiciales o situaciones similares.

En Argentina, esta solución comenzó a implementarse recientemente para el intercambio de información con los clientes, teniendo el Entrevistado 8 experiencia en su aplicación. Según indicó, ha encontrado cierta resistencia para su utilización por parte de los auditados, por desconocimiento y desconfianza en el sistema respecto de la confidencialidad y seguridad de la información. Éstos prefieren enviarla por *e-mail* o *pendrives*, que según él entiende, pueden resultar mucho más riesgosos.

Considera que en este aspecto es fundamental que se involucre al personal de sistemas de los clientes y de la firma de auditoría para la elaboración de acuerdos en los que se creen compromisos respecto de la confidencialidad de los datos compartidos.

La información obtenida de acuerdo al conocimiento del Entrevistado 8 sobre la herramienta no ha permitido determinar exactamente si se trata de un servicio en la nube o no; sin embargo, algunas de sus características están presentes: el acceso a las aplicaciones se realiza a través de la

red; uso compartido de recursos; escalabilidad; posibilidad de realizar un trabajo colaborativo sobre la información (Mell & Grance, 2011).

b) Respecto del uso de opciones de tercerización de TI por parte de sus clientes, reconoce el caso de servicios de mantenimiento de TI, de almacenamiento de grandes volúmenes de información, de sistemas contables; incluso subcontratan en empresas que prestan el servicio de consultoría el asesoramiento para la implementación de sistemas como SAP. No obstante, no podría asegurar que estos correspondieran a alternativas en la nube.

Considerando la participación del entrevistado en las negociaciones con los clientes para la utilización de la herramienta de colaboración y su rol de administrador, así como en encargos de auditoría en entidades que efectúan diferentes tipos de tercerización, se entiende que su opinión es útil para los resultados de esta tesis dados los conocimientos que posee.

Por su parte, el Entrevistado 5 menciona que los clientes de auditorías financieras al momento de la entrevista no utilizaban este modelo de TI. No obstante, se refirió al caso de un cliente[14] que posee todos sus datos en la nube pero hasta el momento él no habría tenido que realizar una auditoría sobre el mismo (existían posibilidades de un cambio en el alcance del servicio prestado a partir del año 2014). Con lo cual, aun no habiendo trabajado en el caso, hay evidencia de utilización de la nube en Argentina.

También mencionó casos similares de tercerización:

a) empresas cuyos datos son almacenados en servidores en el exterior, bajo la guarda de su casa matriz. La actualización de la información almacenada en el exterior se produce en forma automática a partir de las operaciones procesadas dentro del ente en Argentina. Los usuarios locales acceden a dichos servidores para recuperarla.

En uno de estos casos el ente posee además autorización de la Inspección General de Justicia (IGJ) para poder llevar los libros en forma electrónica, debido al importante volumen de información procesada. El entrevistado se ha visto involucrado –junto con personal del área de sistemas (ERS)– en el proceso de solicitud de la autorización y de las revisiones anuales respecto de las actualizaciones del sistema, el soporte que se debe brindar al servidor y el *back up* de la información que se debe realizar en forma local para garantizar que existe un resguardo adecuado;

b) clientes que realizan reportes a casas matrices del exterior con una tecnología similar a la nube, los cuales hasta el momento no eran auditados por el entrevistado, porque el alcance del trabajo solo requería revisar que su información no difiriese significativamente del balance estatutario;

c) caso de *Due Dilligence*, en el cual comprador y vendedor intercambiaban información en un ambiente compartido (*e-room*) al que se le dio acceso al profesional para su intervención en el proceso;

[14] El cliente mencionado pertenece al grupo económico del cliente del Entrevistado 4 que está haciendo uso de servicios CN (ambos entrevistados trabajan en el mismo estudio de auditoría).

d) caso de un cliente que tercerizaba la liquidación de nóminas. Éste recibía no sólo las liquidaciones sino también los asientos contables correspondientes a los sueldos y las cargas sociales que eran incorporados automáticamente al sistema contable. Este tipo de tercerización, sin intervención por parte del auditado en la elaboración de la información, implica ciertas dificultades para la auditoría financiera, en la medida en que si de la aplicación de pruebas globales surgen diferencias significativas, no se posee información adecuada para determinar el origen del problema, dado que los detalles de las liquidaciones los posee el tercero. Si bien no existe seguridad de que este último fuera el caso de uso de un servicio en la nube de *payroll*, este tipo de servicios existe, y las dificultades que puede generar su uso es similar al de este caso de tercerización.

Finalmente, en el caso del Entrevistado 7, la mayoría de los clientes del estudio en el cual se desempeña hacen uso del ERP de SAP mediante licencias adquiridas (modelo *on-premisse)*. Mencionó que todos sus clientes poseen servidores propios en el país donde realizan el almacenamiento de toda la información. En los casos en que deben realizar consolidaciones con casas matrices del exterior, las sucursales locales efectúan transferencias de la información solicitada; las casas matrices no realizan el almacenamiento ni poseen amplio acceso a la información.

En cuanto a la experiencia en el estudio en el cual trabaja, tampoco hacen uso de este tipo de alternativas de TI para el desarrollo de las auditorías. Poseen un *software* para la planificación y ejecución de los encargos, y luego de cada auditoría deben efectuar el almacenamiento de la información y los papeles de trabajo digitales en un servidor propio.

Aun cuando este entrevistado no ha tenido posibilidad de trabajar en entornos de tercerización similares o correspondientes a la CN, se han tenido en cuenta sus comentarios porque ha brindado información interesante en relación al proceso de auditoría ejecutado en los grandes estudios y a la relación entre los auditores contables y de TI.

5.1.2. MOTIVADORES DEL USO DE LA CN

Aun cuando la implementación de soluciones en la nube por parte de las empresas argentinas es incipiente, tal como lo plantean los estudios descriptos en la introducción de esta tesis y según fue confirmado por los entrevistados, es de esperar que su utilización se profundice en el futuro. Los informantes se refirieron espontáneamente a un conjunto de factores que según ellos motivan el uso de esta alternativa de tercerización por parte de las empresas.

A) Disminución y flexibilización de costos

En primer lugar, cuatro de los entrevistados estuvieron de acuerdo en que en muchos casos las organizaciones utilizan esta alternativa como una forma de reducir costos (Entrevistados 1, 3, 6,

7), a la vez que se obtienen beneficios como agilidad en la contratación y disponibilidad de recursos.

El ahorro se lograría en principio debido al sistema de pago en función del uso. Esto es, no se posee la propiedad de la infraestructura física ni de los sistemas, sino que se utilizan recursos alquilados a un proveedor, pudiendo invertirse los recursos disponibles en otras áreas del negocio. La reducción se logra por diversas razones: a) se evitan las grandes inversiones en recursos de *hardware* y *software* al momento de emprender un nuevo negocio o proyecto (*up-front capital expense*), eliminándose una barrera de entrada a algunos negocios (Armbrust et al, 2010; Grossman, 2009); b) se disminuyen costos de funcionamiento, actualización y mantenimiento de TI; c) se reemplazan las inversiones de capital por gastos operativos, evitando pérdidas generadas por recursos inmovilizados y por capacidad ociosa y reemplazando erogaciones de licencias de pago único por pagos periódicos en función del uso mensual o anual.

La variable económica podría ser, según fue manifestado, una de las principales razones para la implementación por parte de las PyMEs, pudiendo tener ésta mayor peso que la variable seguridad, sin hacer una evaluación profunda de los riesgos que este tipo de tecnologías puede implicar para el ente. Algunos trabajos han demostrado que en el caso particular de las PyMEs las reducciones de costos son reales e importantes al movilizar las instalaciones de TI a la nube (McAfee, 2012; Rao, 2012).

El Entrevistado 1 manifestó que dicha reducción de costos podría darse *en teoría*. Se debe tener presente que el análisis de costos no debe contemplar únicamente los incluidos en el contrato y el acuerdo de prestación de servicio (SLA, por sus siglas en inglés), sino que se deben contemplar las inversiones a realizar para la adecuación de las estructuras de gobierno del ente, procesos y procedimientos, arquitecturas de la empresa y cultura, aplicaciones, capacitación del personal, obtención de certificaciones profesionales que demuestren sus competencias, entre otras. Así, el costo total de la computación en nube debe ser comparado con la inversión total y los costos vigentes por la prestación de servicios similares mediante el uso de recursos internos (ISACA, 2012:12).

B) Ventajas competitivas para el área de sistemas: agilidad, flexibilidad y escalabilidad

Asociado al beneficio de reducción de costos, se mencionó también como factor motivador la ventaja competitiva que obtienen las áreas de tecnología o de sistemas a partir del uso de la CN, por la agilidad en la implementación de soluciones de TI (Entrevistados 2, 6).

> Representa una ventaja competitiva para las áreas de tecnología. La velocidad de implementación y el costo asociado al crecimiento que van teniendo los distintos requerimientos, hace que sea mucho más flexible y le da mucho más aire a los presupuestos del área de sistemas. (Entrevistado 2)

Es decir, la contratación de los servicios en la nube resulta ágil y brinda rapidez al desarrollo de los negocios, en la medida en que los servicios pueden ser utilizados en el momento en que se

los necesita, evitando las demoras originadas por el desarrollo, configuración y operación de los proyectos de TI tradicionales (ISACA, 2009). A su vez, permite que el presupuesto financiero del área de sistemas no se agote, como sucedería con las grandes inversiones asociadas a otras alternativas de adquisición de recursos de TI.

Al mismo tiempo, los servicios brindados por los proveedores son escalables, garantizando la disponibilidad de recursos mediante la capacidad de almacenamiento y uso ilimitado. De esta forma, los servicios en la nube ofrecen mayor flexibilidad, permitiendo la cobertura de los picos de demanda, evitando los recursos ociosos el resto del tiempo (servicios *on demand)*.

C) Disponibilidad permanente de la información

La disponibilidad de la información ha sido mencionada también como un factor motivador (Entrevistado 6). Los datos y aplicaciones se encuentran disponibles en forma permanente y en todo lugar, en la medida en que los proveedores poseen un ancho de banda e infraestructura que aseguran la satisfacción de las necesidades de los consumidores, permitiendo un acceso universal a los documentos que siempre se encuentran disponibles en la *web*. Al mismo tiempo, el acceso puede darse a través de diferentes dispositivos con acceso a Internet (PC, *laptop*, celulares, *tablets*, etc.), generando una conexión tal entre las organizaciones y sus trabajadores que permite el trabajo colaborativo y fuera de las oficinas.

D) Simplificación de la estructura organizacional

Otra razón que puede motivar el uso de la CN a nivel organizacional es que no es necesario contar con personal propio experto en sistemas, delegando la especialización en los profesionales que integran el plantel del proveedor del servicio. Tal como se mencionó en el marco teórico, son beneficios del uso de esta tecnología el mantenimiento y actualización constante, así como la disponibilidad permanente de expertos que logran un alto nivel de experiencia y conocimientos por la prestación del servicio en gran escala.

> Algunos la adoptan para vivir más tranquilos sin tener personal propio de sistemas. (…) Muchos de los que se van a la nube –no solamente para ERP o sistemas contables, sino para otros sistemas– lo hacen porque quieren tercerizar y delegar todo este conocimiento técnico que no pueden mantener en su personal. (Entrevistado 1)

E) Tendencia (*Benchmarking*): grandes usuarios y grandes proveedores

El Entrevistado 2 considera que puede existir un factor de imitación en el futuro, en la medida en que se conozcan casos de éxito de utilización de la nube; este factor motivador también ha sido mencionado por ORACLE-MERCADO (2013) y por Yigitbasioglu (2015).

Siendo que grandes corporaciones de nivel internacional, entre ellas entidades financieras, lo utilizan, cree que esto puede brindar cierta seguridad a potenciales usuarios, generando una tendencia y motivando a la aplicación por parte de otras empresas. El razonamiento presupone que

si empresas que suelen basar sus decisiones en la seguridad de la información más que en el factor económico, han migrado a la nube, ello puede brindar cierto respaldo y seguridad a otras organizaciones para adoptar ellas también esta alternativa siguiendo la tendencia marcada por los grandes.

> (…) creo que a empresas PyMe, medianas y grandes les da una visión mucho más atractiva de la tecnología. (…) Sabemos que en el *benchmarking* es parte de la toma de decisiones en la cual se basan las empresas; si indica que corporaciones como estas que estoy nombrando, a nivel internacional, migraron a la nube, da un respaldo y seguridad que lleva a lograr un poco más de aceptación que si lo adoptan corporaciones que se guían únicamente por el tema económico. (Entrevistado 2)

Además, el Entrevistado 2 se refiere a la tendencia que marcan los grandes proveedores (que poseen una reputación reconocida y brindan servicios de calidad), quiénes comienzan a subir a la nube las aplicaciones que habitualmente ofrecían mediante la venta de licencias. Por ejemplo, en relación a los sistemas ERP, el hecho de que grandes proveedores como son Oracle y SAP, además de pequeños proveedores locales, comiencen a dar servicios en la nube, da cierta confianza para su utilización. A su vez, se debe considerar que lo hacen a un costo mucho menor de lo que representa la adquisición de las licencias de las alternativas *on-premisse* por parte de los usuarios. Según mencionó:

> Ya tenemos grandes *players* en ERP como son Oracle o SAP que empiezan a dar servicios en la nube. (…) Eso también da una garantía o una sensación de seguridad distinta. Hasta hace muy poco tiempo eran pequeñas empresas proveedoras con sistemas ERP muy chicos en la nube. ¿Qué estaban haciendo ahí? Querían ganar una posición en el mercado en forma competitiva. Hoy empresas consolidadas entienden que la tendencia está yendo para la nube, por lo cual tienen que tener ese servicio para seguir siendo primeras marcas. (Entrevistado 2)

El Entrevistado 1 también se refirió a la importancia de los grandes proveedores como prestadores de servicios en la nube y la reducción de costos para la adquisición de sus productos. Sin embargo, indicó que aun considerando la relevancia de los prestadores, según conoce, las empresas en Latinoamérica, y en particular Argentina, no están migrando a la nube fácilmente (ello puede deberse a que el servicio de ERP en la nube aún no está disponible en la Argentina[15], según se pudo conocer mediante comunicaciones personales con oferentes de dichos servicios a través de sus respectivas páginas *web*).

> El tema es que en los ERP, los proveedores hoy te están ofreciendo que en lugar de comprar las licencias y mantenerlos vos, que es muy caro, vayas a la nube con procesamiento, base de datos e ERP completo. Pero lo hace gente de ese tamaño, nivel y conocimiento. (…) Hay empresas, como por ejemplo Oracle, que en Estado Unidos está dando la operación de su ERP en la nube, con todos los recaudos necesarios. Estamos hablando de "EL" fabricante del producto ERP,

[15] Las soluciones de ERP en la nube ofrecidas por ORACLE y SAP aún no se encontraban disponibles para su uso en Argentina (ORACLE, comunicación personal, 11/06/2015; ORACLE, 2015; SAP, 2012; SAP, comunicación personal, 06/05/2015). Se pudo indagar que la aplicación ERP de SAP –denominada *All in one*– disponible es *on-premise*, esto es, deben ser instaladas en los servidores del ente.

> "EL" creador de la base de datos Oracle, donde obviamente más conocimiento que ellos sobre su plataforma y sus bases de datos nadie pueden tener. Y aun con eso, por lo menos hasta donde se de Latinoamérica, no muy fácilmente la gente está migrando hacia allá. (Entrevistado 1)

F) Transparencia para el usuario

Finalmente, se mencionó la transparencia que este tipo de servicios representa para los usuarios finales, que podrían ser quienes participan de los procesos de generación de información financiera en los entes. Esto implica que el usuario cuando utiliza los sistemas no puede dimensionar o determinar la diferencia entre un servicio o aplicación en la nube y uno tradicional (Entrevistado 2). Esto hace sencillo su uso y podría fomentar su adopción por las empresas.

El Entrevistado 4, quien tuvo oportunidad de trabajar con un cliente que utilizaba servicios ERP en la nube, mencionó que para los usuarios resultaba sumamente transparente y sencillo, en la medida en que el acceso al sistema para ellos se daba a través de un icono en el escritorio, del mismo modo que lo harían con cualquier otro sistema, sin tener en cuenta que la información sobre la cual estaban trabajando finalmente sería almacenada y procesada en un servidor del exterior, perteneciente al tercero proveedor del servicio.

5.1.3. BARRERAS PARA LA IMPLEMENTACIÓN DE CN POR LAS EMPRESAS ARGENTINAS

Al momento de describir sus experiencias, espontáneamente algunos entrevistados se refirieron a factores que, según ellos, demoran la utilización de la computación en la nube en empresas argentinas, al menos en lo que a sus clientes se refiere. El conjunto de factores identificados por los profesionales coincide en su mayoría con aquellos mencionados en los estudios no académicos realizados en el país (ORACLE-MERCADO, 2013; USUARIA 2013,2014) y los antecedentes de estudios desarrollados en otros países que han sido mencionados previamente. Ello es indicativo de que los entrevistados conocen la tecnología y respalda la pertinencia de su participación en el estudio.

Las barreras de uso que fueron mencionadas incluyen:

A) Desconfianza sobre la confidencialidad y seguridad de la información

El principal factor inhibidor nombrado por los entrevistados se refiere a la desconfianza que poseen los potenciales usuarios argentinos sobre la seguridad y confidencialidad de la información subida a la nube (Entrevistados 1, 3, 4, 6, 7, 8); según el Entrevistado 3 se debe a las dudas de los usuarios respecto de las medidas aplicadas por los proveedores. Este inhibidor también fue detectado por Yigitbasioglu (2015) en su estudio sobre adopción de CN por empresas australianas.

La percepción de los entrevistados es que los empresarios –dueños de los datos– pretenden tener el control sobre su información, ubicándola en servidores propios, que conocen dónde están

ubicados y a las personas que los administran, antes de dejarlo en manos de terceros, en una ubicación desconocida.

> A las compañías, como a cualquier persona, no les gusta mucho que su información este en una nube, que no sabe que es. Hay determinada información que las empresas no quieren que las vea cualquier persona. Por eso lo veo medio difícil de aplicar. (Entrevistado 7)

El mayor temor que tienen los usuarios es respecto de las garantías sobre la confidencialidad de la información almacenada en la nube (Entrevistados 3, 4); esto no necesariamente porque la nube sea más riesgosa en este sentido –eso depende del servicio en particular– sino porque representa un cambio de paradigma al que los empresarios deben adaptarse. Según el Entrevistado 7, los entes en muchos casos no están preparados internamente para adoptar este tipo de soluciones, requiriéndose un cambio en la cultura organizacional al respecto.

La experiencia del Entrevistado 8 en relación a la implementación de una solución de trabajo colaborativo con clientes de auditoría es un ejemplo de esta barrera en cuanto a la reticencia de los mismos para utilizar la aplicación. El desconocimiento de la localización exacta de la información y del tratamiento que se dará a la misma son factores que generan dudas sobre la seguridad. Esta sensación de incomodidad se profundiza cuando se refiere a información confidencial para la compañía (Entrevistado 6).

En consecuencia, como medida previa a la utilización de la nube resulta necesario realizar una clasificación de los datos para definir las medidas de protección que deben ser aplicadas sobre éstos (sea por su sensibilidad o por la aplicación de normativa que establezca ciertos requisitos). A partir de ello se podrá determinar si es posible hacer la transferencia de dicha información a la nube y qué modelo de servicio y distribución puede ser aplicado en cada caso en particular (Jericho Forum, 2009:2).

Las apreciaciones demuestran que en algunos casos la barrera de implementación es la *inseguridad percibida*. Esto es, lo que los empresarios *creen* acerca de la seguridad de la nube, más allá de lo que *conocen*. La sensación de exposición de sus datos les impide utilizar la solución, en vez de tratar de garantizar que las medidas de seguridad adecuadas sean implementadas a fin de lograr un nivel de seguridad y confidencialidad requerido.

Como una forma de superar este inhibidor, el Entrevistado 3, en forma similar a lo que indicaba el Entrevistado 1 cuando se refería a los casos de tercerización en general, mencionó la necesidad de mayores exigencias por parte de los usuarios en relación a las medidas de seguridad a ser aplicadas por los proveedores para la protección de su información. Deben garantizarse, previo a la contratación del servicio, que el proveedor cumpla con todas las medidas de seguridad y confidencialidad de los datos que consideren adecuadas.

Para ello deberán incorporar dentro de las cláusulas de los contratos las medidas que consideren pertinentes y las formas en que ellos mismos podrían monitorear su cumplimiento. Ello depende además del tipo de acuerdo de servicio en la nube según el nivel de negociación de sus

cláusulas (CSA, 2011a:16; Jansen & Grance, 2011): los predefinidos o no negociables (simples contratos de adhesión), que resultan ser los más utilizados principalmente en las nubes públicas, y los negociables (en los podrían realizarse acuerdos en relación a los puntos aquí mencionados). De todas formas, si bien estos últimos se asemejan a los contratos tradicionales de tercerización de servicios de TI, el ente necesitaría asesoramiento técnico y legal de modo de asegurarse que los requerimientos de seguridad de la organización se ven satisfechos. Al mismo tiempo implican un mayor costo para la organización, en la medida en que recibe un servicio a medida y se eliminan los beneficios de la economía de escala. Todo lo cual comienza a hacer más compleja la contratación del servicio en la nube.

B) Regulación normativa y de los organismos de contralor

La regulación normativa y de los organismos de contralor también fue mencionado como un obstáculo para la implementación de la CN y otras nuevas tecnologías (Entrevistados 3, 6). Estas restricciones pueden relacionarse principalmente a la protección de datos personales de empleados, clientes y proveedores, pero también a los requisitos establecidos en la normativa respecto de la forma de procesamiento y conservación de la información contable que respalda los estados financieros.

Según los profesionales, la plena y rápida aplicación de este tipo de alternativas se dificulta en parte por el atraso que los organismos de contralor argentinos presentan en relación a las nuevas tecnologías.

> Los reguladores, que a lo mejor son los que menos agilidad tienen, los menos dinámicos en nuestro país, lo primero que hacen es negar la realidad. Es decir: "Bueno, pueden existir entornos en la nube, pero yo lo que necesito es que el respaldo este físicamente, primero dentro de mi jurisdicción –que es el país– y después necesito tenerlo mapeado con un servidor en un lugar determinado". Es decir, lo quieren tangible, y básicamente lo que genera la nube es la intangibilidad de los datos, es decir, uno no sabe dónde están. (Entrevistado 6)

Ello podría implicar un conflicto en el caso de uso de una solución en la nube *transfronteriza* (Svantesson & Clarke, 2010). La característica de la localización independiente de los datos del usuario, que en muchos casos se encuentran en jurisdicciones extranjeras, dificulta la utilización de esta tecnología por el desconocimiento de la ubicación exacta de la información.

Una solución a esta situación consiste en que quienes opten por aplicar de todos modos estas alternativas pueden efectuar copias locales de la información almacenada en la nube y ubicada en otro país, trayéndola a la Argentina para cumplir una disposición legal (Entrevistado 6). Sin embargo, según el Entrevistado 3, esto resulta antieconómico para el ente: por un lado, contrataría un servicio en la nube para reducir costos de almacenamiento –entre otros beneficios–, pero simultáneamente se le estaría exigiendo el almacenamiento local, duplicando la información. Al mismo tiempo, genera la dificultad de que se debe contar con la tecnología necesaria para el acceso a los datos resguardados en forma local.

En consecuencia, resulta que la utilización de servicios en la nube no siempre es compatible con los requerimientos de los entes reguladores en cuanto a que el respaldo esté físicamente dentro de su jurisdicción. Por lo tanto, frente al riesgo de que la tecnología no pueda ser explotada en su máximo potencial y aprovechados los beneficios que ella otorga, las empresas se resisten o demoran su utilización.

Este aspecto será tratado con mayor profundidad en el apartado *5.3.2.d)* al tratarse los riesgos legales de la CN y sus consecuencias sobre la auditoría de estados financieros.

C) Atraso tecnológico por parte de los usuarios

Otro factor mencionado se refiere al nivel de atraso tecnológico por parte de las organizaciones argentinas. Este tema está vinculado al factor de la cultura organizacional mencionado previamente, y tiene que ver con que los empresarios aún prefieren mantener soluciones que ya utilizan y consideran más seguras. Las empresas recién están comenzando a aplicar la virtualización de servidores, lo cual puede ser un paso previo en la evolución hacia un mayor nivel de uso de la CN (Entrevistado 4) (USUARIA, 2014).

D) Deficiente infraestructura de las telecomunicaciones en la República Argentina

La infraestructura de telecomunicaciones del país es vista por algunos usuarios como un obstáculo para el uso de soluciones en la nube (Entrevistados 4, 7). Considerando la característica esencial de acceso a los servicios en la nube a través de una red, como puede ser Internet, creyeron que el sistema de telecomunicaciones del país podría no ser adecuado para dar soporte a los requerimientos del uso de la nube.

Esto, según indicaron, podría depender de la localización de la empresa usuaria –en las grandes ciudades los servicios pueden ser mejores que en algunas ubicaciones alejadas en el interior del país.

Una falla en las comunicaciones podría resultar un problema sumamente grave en el caso de que la empresa estuviera actualizando grandes volúmenes de información, de modo que la posibilidad de que esto ocurra podría estar impidiendo la aplicación por parte de los potenciales usuarios.

Otros profesionales mencionaron los problemas de infraestructura al referirse a los riesgos técnicos de aplicación de la CN, según será descripto en el apartado *5.32.c)* de esta tesis.

E) Oferta aun inexistente en Argentina de los grandes prestadores de servicios en la nube

Finalmente, derivado de los comentarios de los entrevistados, se encontró que mencionaron a los grandes prestadores de servicios (como Oracle y SAP en el caso de servicios de ERP) (Entrevistados 1, 2).

Si bien ellos indicaron que la prestación por parte de estas importantes empresas brindaría seguridad a los usuarios y fomentaría la utilización de la nube, según se pudo conocer en relación a los sistemas ERP, ninguno de los prestadores posee soluciones de este tipo disponibles en la República Argentina, no obstante contar con ellas en otros países como ser Estados Unidos o México.

En consecuencia, cabe agregar como factor inhibidor del uso de la CN por parte de empresas argentinas –al menos en cuanto a servicios ERP– la falta de disponibilidad de servicios en el mercado prestados por grandes proveedores. Si bien existen servicios de proveedores locales o pequeños, estos podrían no ser lo suficientemente confiables como para promover el uso por parte de los empresarios. Lo mismo podría ocurrir con otros usos de la CN respecto de los cuales aún no exista oferta en el país.

5.1.4. RESUMEN

En el presente apartado se pretendió describir el estado de utilización de la computación en la nube en la República Argentina y conocer la experiencia de los profesionales entrevistados en relación a esta tecnología.

De acuerdo a los resultados obtenidos, y respaldando los estudios previos, la implementación de la CN se encuentra en un estado de implementación incipiente. Si bien es un tema en las agendas de los empresarios, su utilización no está muy difundida. Su aplicación a los negocios no está en auge y en la práctica la utilización se está dando principalmente sobre servicios de apoyo, no sobre los sistemas principales ni los transaccionales.

Los clientes de los estudios en los que se desempeñan los entrevistados no han implementado hasta el momento la CN para procesos que tengan influencia significativa sobre la elaboración de los estados financieros. Los entes no transfieren tan fácilmente sus procesos críticos o la información sensible que les dan una ventaja competitiva y/o contribuyen a su imagen pública, del mismo modo que no lo hacían con otras soluciones de tercerización (Yigitbasioglu et al., 2013:103).

Aun cuando el nivel de uso es incipiente en Argentina, y para procesos no claves, hay perspectivas de una mayor utilización en el futuro. En consecuencia, los auditores deben adaptarse al nuevo escenario o incluso mejorar sus conocimientos en aquellos casos en los que ya participen en procesos de tercerización.

El caso de aplicación descripto para elaborar información de carácter financiero se debe a un requerimiento de la casa matriz del ente auditado, que se encuentra en el exterior. La experiencia de auditoría en entornos de CN fue novedosa, dado que no se habían dado casos previos y no estaban preparados para realizar auditorías de sistemas en estos entornos.

Los profesionales pudieron describir experiencias de clientes que están aplicando la CN o considerándolo para procesos o servicios de apoyo, como correo electrónico, gestión de recursos

humanos, almacenamiento de información. En todos los casos tienen experiencia respecto de auditorías en otros ambientes de tercerización de TI. Incluso se conoció el caso de utilización de la CN por parte de los estudios de auditoría (si bien este no es el foco de esta tesis, sino más bien el efecto que el uso por parte de los clientes auditados tiene sobre el proceso de auditoría financiera).

También los informantes expusieron sus conocimientos y experiencias en relación a otras alternativas de tercerización que consideraron presentan características y dificultades similares a la nube. Estas respuestas se incluyen en este apartado, porque se entiende respaldan la experiencia de los profesionales en entornos similares y que sus opiniones pueden ser consideradas como válidas.

Los auditores entrevistados pertenecen a filiales de estudios de auditoría internacionales y poseen una base de conocimiento compartida con casas matrices del exterior que están más avanzadas en estas cuestiones.

En relación a su nivel de experiencia, los auditores de sistemas demostraron tener mayor familiaridad con el concepto de CN que los auditores financieros; ello puede deberse a su formación y a su función dentro de los grandes estudios, en los cuales existe un importante grado de especialización y separación de funciones.

Según se pudo evidenciar, los auditores de sistemas son los que se muestran mayormente afectados por la implementación de la CN por parte de los clientes; los auditores contables parecieran estar más ajenos a esta realidad, principalmente por el nivel de separación de funciones mencionado previamente. En consecuencia, las respuestas obtenidas no se deben tanto a la experiencia de realización de auditorías en el entorno de TI analizado, sino más bien a los análisis previos que se están efectuando y a la formación que han obtenido hasta el momento en relación al tema en cuestión.

Los profesionales se refirieron espontáneamente a factores que potencian el uso de la CN así como a barreras que demoran su implementación en la Argentina.

El capítulo demuestra entonces que existen expectativas de una mayor utilización de la CN por las empresas argentinas en el futuro, incluso en procesos con influencia en la elaboración de la información contable que luego se ve reflejada en los estados financieros. En consecuencia, la auditoría contable y la de sistemas deberán adaptarse a estos nuevos entornos. El análisis de los aspectos de la auditoría que se verán influenciados resulta pertinente en este contexto, justificando la importancia de los próximos capítulos de esta tesis.

El Cuadro 21 resume los resultados obtenidos en relación a las categorías de respuestas identificadas (preliminares y emergentes) en relación al tópico de análisis aquí descripto.

Cuadro 21 - Estado de Aplicación de la CN en Argentina

TÓPICO	CATEGORÍAS	SUBCATEGORÍAS	
USO DE CN POR EMPRESAS ARGENTINAS	**ALTERNATIVAS DE USO**	**COMPUTACIÓN EN LA NUBE**	Correo Electrónico Gestión de Recursos Humanos Elaboración de información financiera – Estados Contables Procesamiento de información interna – Reportes gerenciales al Exterior Almacenamiento de información
		TERCERIZACIÓN SIMILAR	Sistema *Core* Financiero en servidores de casa matriz en el exterior Almacenamiento de información en servidores de terceros Almacenamiento de servidores propios en locales de terceros Trabajo colaborativo Mantenimiento de TI *Payroll*
	FACTORES MOTIVADORES	Disminución y flexibilización de costos Ventajas competitivas para el área de sistemas: Agilidad/Flexibilidad/Escalabilidad Disponibilidad permanente de la información Simplificación de la estructura organizacional (evitar poseer personal de sistemas propio) Tendencia/Benchmarking: grandes usuarios y grandes proveedores Transparencia para el usuario	
	FACTORES INHIBIDORES	Desconfianza sobre la confidencialidad y seguridad de la información Cultura organizacional Regulación normativa y de los organismos de contralor Atraso tecnológico por parte de los entes usuarios (estadio previo a la nube) Infraestructura de las telecomunicaciones Falta de oferta del servicio en el país respecto de algunas aplicaciones	

***LECTURA**: Letra azul: elemento nuevo. Letra en negro: elemento original.*

Fuente: Elaboración propia.

5.2. CONOCIMIENTO DEL CLIENTE Y SU ENTORNO

En el presente apartado se pretende dar cumplimiento al siguiente objetivo específico:

Identificar los principales aspectos del uso de la CN que el auditor deberá considerar para obtener un acabado conocimiento del cliente y su entorno.

Para la elaboración de los resultados se utilizaron las categorías definidas en el marco teórico, basadas principalmente en lo establecido por la NIA 315 (Revisada) y la NIA 402. Allí se indican los principales aspectos a tener en cuenta por el auditor en esta etapa a fin de lograr una comprensión adecuada del cliente que le permita efectuar un correcto análisis de riesgos y planificación de su trabajo, así como definir el conjunto de procedimientos a aplicar.

A su vez, el análisis de los datos permitió evaluar dos aspectos adicionales: la relevancia que el conocimiento del cliente tiene en un encargo de auditoría en la nube y las particularidades de este proceso según se trate de una primera auditoría o una auditoría recurrente.

Para ello se describe la experiencia y opinión de los ocho entrevistados, poniendo especial énfasis en las características específicas que presenta el uso de la CN por parte de su cliente, así como las similitudes con otros entornos de TI.

Las cuestiones vinculadas a la comprensión del control interno, si bien algunos autores las incluyen en esta etapa y fueron en parte mencionadas por los profesionales en relación a este tópico, serán tratadas en el apartado *5.4. Evaluación del sistema de control interno en CN*, dada la importancia que esta tarea representa en una auditoría financiera en un entorno de TI.

5.2.1. IMPORTANCIA DE ESTE ASPECTO EN LA AUDITORÍA EN AMBIENTES DE CN

El conocimiento del cliente y su entorno incluye el análisis del *nivel de informatización del ente a auditar*. En consecuencia, la utilización de un entorno de CN por parte del cliente debe ser tenida en cuenta desde el inicio de la auditoría financiera.

Desde un principio el desarrollo del trabajo se ve afectado significativamente por el uso de la nube por parte del potencial ente auditado. Antes de iniciar el encargo, debe decidirse acerca de la aceptación o continuación de un cliente. A fin de tomar dicha decisión, entre otros factores, resulta fundamental la consideración de los sistemas utilizados y la seguridad informática, principalmente en los entes en los cuales los procesos dependen fuertemente de la TI. A partir de la evaluación realizada por el área de sistemas en esta etapa inicial, debería surgir que el sistema cumple ciertos requisitos para que los auditores pueden confiar en la información que brinda y su almacenamiento a fin de que el encargo de auditoría pueda ser aceptado (Entrevistado 8).

Es decir, aun cuando el conocimiento del cliente y su entorno –incluyendo el CI– es fundamental al momento de planificar el trabajo de auditoría, el auditor deberá cumplir con este requisito como una actividad previa a la decisión de aceptar, o no, el encargo de auditoría propuesto (Fowler Newton, 2004).

Desde la perspectiva de los entrevistados del área de sistemas, el proceso de conocimiento del cliente que utiliza la CN se asimila al aplicado en otros casos de tercerización de TI, con ciertas particularidades (Entrevistados 1, 3). En consecuencia, mucha de la experiencia adquirida por los profesionales resulta aplicable al nuevo entorno.

Aun así, resulta interesante identificar aquí aspectos diferenciales y mejoras que se puedan implementar en los procesos de auditoría en entes que hacen uso de organizaciones de servicios en relación a este tópico. Ello considerando las fallas en estos tipos de encargos mencionados por los profesionales, en particular: deficiente planificación del encargo; inadecuada evaluación de riesgos; falta de consideración de la importancia de la tercerización y la responsabilidad que cabe al usuario; interacción deficiente entre auditores financieros y de TI (Entrevistado 1).

5.2.2. OPORTUNIDADES DE CONOCIMIENTO DEL CLIENTE QUE UTILIZA LA NUBE

La necesidad de profundizar en el conocimiento del sistema de información del ente que utiliza la CN puede darse en dos supuestos: a) auditorías recurrentes: que sea un cliente del estudio de auditoría que realiza un cambio en sus sistemas y comienza a aplicar CN; resulta una modificación importante, que requiere un conocimiento similar al necesario en otros supuesto de cambio de sistema informático; b) primeras auditorías: que sea un cliente nuevo, que se encuentra haciendo uso de la CN, debiendo tomarse los recaudos de revisar toda la información pertinente y lograr una adecuada comprensión del sistema antes de comenzar a trabajar (Entrevistado 8).

Cuando se trata de una *primera auditoría*, y como actividad previa a la contratación, el profesional podría tomar contacto con el auditor anterior del potencial cliente, si es que lo considera necesario y si esto fuera posible (Fowler Newton, 2004). El contacto, así como la revisión de sus papeles de trabajo, requeriría además la autorización expresa del cliente. En este caso, los entrevistados destacaron que un factor a tener en cuenta es la reputación e idoneidad del auditor anterior, que tendrá relación directa con la profundidad y extensión del trabajo del nuevo profesional en esta etapa de conocimiento y aceptación del cliente.

> Si recibimos un cliente que previamente era auditado por otro de los BIG4, los servicios de inicio no serán tan relevantes, dado que podemos estar tranquilos por la labor realizada por el otro profesional. Realizamos una revisión, consultamos los papeles de trabajo del auditor anterior. En cambio, si lo hubiera auditado un profesional que no sea conocido, que tal vez no tenga papeles de trabajo para presentar, deberíamos hacer un trabajo adicional que con los BIG4 no lo tendría que hacer, lo que seguramente implicará una mayor cotización de honorarios con respecto al caso anterior. (Entrevistado 5).

En estos casos se buscaría conocer la experiencia del auditor anterior en el entorno *cloud computing* en particular: incidencias sobre su trabajo; evidencias obtenidas sobre la utilización de la CN para el procesamiento de información contable; resultados de la evaluación del entorno de TI y posibles deficiencias del sistema de control interno detectadas; problemas que hubiera generado

para su trabajo, derivadas por ejemplo de la obtención de evidencias virtuales y el acceso a resguardos de datos.

La situación será igualmente compleja en el caso de una *auditoría recurrente*. Sin embargo, es de esperar que los profesionales acompañen y asesoren en el proceso de implementación de la nueva tecnología, antes de tener que auditarla, lo cual representa una ventaja. Ello podría darse realizando evaluaciones de diversas alternativas de servicios y proveedores, informando sobre los riesgos y ventajas involucrados en cada uno de ellos, evaluando las condiciones de contratación, aconsejando y participando de este modo del proceso de toma de decisiones, lo cual permite anticipar el proceso de conocimiento por parte del personal de auditoría y facilitar la comprensión del sistema de TI (Entrevistado 3).

5.2.3. ASPECTOS RELEVANTES A CONOCER DEL CLIENTE Y SU ENTORNO

A continuación se describen los principales aspectos que deberían ser conocidos y comprendidos sobre el uso de la CN en esta etapa inicial de la auditoría, de acuerdo a la opinión y experiencia de los entrevistados.

A) Sistemas contables y de control interno afectados por la CN

Según los profesionales, en primer lugar, se debe conocer qué información o procesos están siendo delegados en el proveedor del servicio de la nube, tal como ocurre en otros casos de tercerización. Ello a fin de determinar de qué manera la información que respalda los estados contables se ve influenciada por el ambiente de control del tercero (Entrevistado 2). Resulta necesaria una amplia comprensión de las transacciones y actividades ejecutadas electrónicamente, y los controles relacionados, para verificar la validez y confiabilidad de la información generada en dicho entorno (Pastor, 2011).

El conocimiento de este aspecto del entorno de TI se divide en dos etapas, muy bien descriptas por el Entrevistado 8, destacándose la importancia de la participación de los auditores de sistemas en cada una de ellas[16]:

a) En primer lugar, el ENTENDIMIENTO EN GENERAL por parte de los auditores financieros del conjunto de sistemas utilizados por el ente, independientemente de que posean o no efecto sobre la contabilidad. Aquí se conocería que el ente se encuentra haciendo uso de la computación en la nube y se indagaría e intentaría comprender el entorno de TI y los tipos de servicios utilizados, independientemente del objetivo para el cual la organización lo hubiera implementado.

> Al momento de iniciar la auditoría hacemos un mapeo de todos los sistemas y de cómo van afectando los procesos de la empresa, y después vemos cómo afecta a

[16] Las denominaciones de "Entendimiento en General "y "Entendimiento en Particular" fueron otorgadas por la autora de esta tesis. El auditor se refirió a la primera como entendimiento, pero no otorgó una denominación específica a la segunda etapa.

> la contabilidad; puede ocurrir que el uso de dichos sistemas no la termine afectando. Ese sería un entendimiento inicial. (Entrevistado 8)

En este punto, y tal como fue mencionado en el marco teórico, se buscará evaluar el nivel de importancia que la nube tiene para el ente. Si su utilización afecta gran cantidad de información o información significativa para los estados contables, la consideración y el conocimiento que se debe obtener es mayor, pasando a la etapa de *entendimiento en particular* que se describe a continuación. Incluso, a partir de la evaluación del nivel de importancia y complejidad, los auditores pueden considerar la necesidad de la intervención de los profesionales de sistemas en el proceso de auditoría (Entrevistado 5).

b) Luego debe realizarse un ENTENDIMIENTO EN PARTICULAR solo de aquellos sistemas que posean un efecto sobre la contabilidad y sobre la información que formará parte de los estados financieros sujetos a auditoría. Ello puede ser porque se almacena en la nube la información que respalda las registraciones contables, porque se gestionan allí procesos que afectan a saldos contables (por ejemplo, liquidación de haberes, gestión de deudores y cobranzas, etc.) o porque toda la contabilidad es llevada en sistemas en la nube.

Se profundiza la evaluación del sistema y su seguridad, generalmente con la colaboración del personal del área de sistemas.

El Entrevistado 8 ejemplifica que la utilización de un sistema ERP en la nube implicaría un nivel de integración tal que necesariamente impactará en el sistema de información contable, requiriendo su evaluación en profundidad. El Entrevistado 4, basado en su experiencia, mencionó que en general los entes utilizan este tipo de aplicaciones integradas en la nube, aprovechando todos los módulos que las componen, dejando por fuera en algunos casos los sistemas de gestión de recursos humanos instalados en servidores propios de la empresa. En estos casos se deberá obtener un entendimiento en particular sin lugar a dudas.

El Entrevistado 1 puso énfasis en que el análisis se deberá realizar no solo sobre los sistemas de contabilidad propiamente dichos, sino también sobre cualquier otro que pudiera estar siendo gestionado en la nube y que genere transacciones o información que luego impacte directa o indirectamente en la contabilidad financiera (por ejemplo, un sistema de facturación en la nube a partir del cual se importa la información de ventas al sistema contable local). Según él, la determinación de los sistemas y subsistemas informáticos relevantes a ser comprendidos se realiza a partir de la identificación de las cuentas o saldos que resultan significativas para el auditor financiero, y que se pueden ver influenciadas por la TI.

> Se debe realizar además un análisis, que obviamente lo hacen en general los que trabajan en auditoría contable, que es la ponderación de la importancia de las distintas cuentas. El análisis de riesgos tiene que partir de estas cuentas más significativas, que van a determinar los sistemas, los procesos y las transacciones relevantes, que definirán cuáles son los subsistemas que se van a analizar. Después de saber qué subsistemas voy a analizar, tengo que ir a ver qué sistemas me alimentan esa contabilidad, los cuales pueden ser propios del ente o de terceros –como es el caso de la nube. Los mismos pueden haber sido generados a

> partir de desarrollos internos, o se pueden haber adquirido sistemas desarrollados por un tercero. (Entrevistado 1)

Respecto de aquellos sistemas que son utilizados en la nube, pero que no impactan en la contabilidad, en principio no necesariamente deben ser revisados por los equipos de auditoría financiera. Un ejemplo de ello son los reportes internos –aplicación que se estaría utilizando en Argentina–, que muchas veces no respetan las normas contables y que además no generan asientos contables. En consecuencia, aun cuando contengan errores no representan un riesgo para el profesional porque no emite una opinión sobre su razonabilidad (Entrevistado 8).

Sin embargo, el análisis de la importancia e impacto de información procesada en la nube para usos internos debe ser cuidadoso. Pueden darse dos supuestos que el auditor financiero deba considerar como relevantes:

a) que el ente auditado utilice la CN para elaborar reportes internos, que en principio no afecten los saldos contables, pero que contengan información que sea utilizada para elaborar la información por segmentos que requieren algunas normas. En este supuesto, la CN debe ser analizada, porque puede afectar indirectamente la información sujeta a auditoría (Entrevistado 8);

b) Que el ente auditado esté alcanzado por normativa de la *Security Exchange Comission* (SEC) de Estados Unidos, de modo que el auditor no solo deba emitir una opinión en relación a los estados contables, sino también sobre los controles internos del auditado (Entrevistados 5, 8). El uso de la CN estaría afectando esta última opinión del auditor.

En resumen, esta distinción entre entendimiento en general y en particular se considera importante en una auditoría en un entorno de CN, dado que:

- en la etapa preliminar de conocimiento del cliente, se deberá lograr un entendimiento en general de la CN, independientemente que afecte o no a la contabilidad financiera. Esto es, en cualquiera de los supuestos de uso mencionados en el apartado *5.1.*;
- luego, es posible que se deba profundizar sobre aquellos sistemas en la nube con efecto sobre la información contable con la que se elaboran los estados financieros, de modo que la aplicación de la CN requerirá especial atención por parte del auditor financiero. Esto es, por ejemplo, en el caso de utilización de sistemas ERP en la nube;
- en los casos de empresas que hagan uso de la nube y que estén sujetas a la normativa de la Comisión Nacional de Valores (CNV), de la SEC, que apliquen normas internacionales de contabilidad o que estén sujetas a normas de otro organismo de contralor, el entendimiento general necesariamente deberá ser ejecutado, debido a los requerimientos de información que imponen dichas normas y a la eventual necesidad de opinar sobre el sistema de control interno del auditado. En cuanto al entendimiento particular, será necesario cuando en los estados contables se incluya información de uso interno, pero que sea incorporada indirectamente en los reportes financieros por los requerimientos de la normativa. Los clientes de los grandes estudios a los que pertenecen los entrevistados pueden estar sujetos a dichas normas.

Un aspecto adicional a considerar al momento de identificar y evaluar los sistemas de contabilidad y control interno afectados por la TI se refiere a la *complejidad que adquiere el sistema de información*.

La CN en particular posee varias de las características que de acuerdo a la bibliografía relevada harían al sistema más complejo: posibilidad de que existan servicios a medida o customizados; modificaciones y actualizaciones a sistemas que, de acuerdo al servicio contratado, pueden ser implementadas por el proveedor y no informadas al usuario; interfaces entre sistemas; uso de alternativas de ERP en la nube; infraestructura tecnológica compleja; entornos multinacionales para el procesamiento y almacenamiento de las aplicaciones y la información; intercambio de información a través de Internet (Minguillón, 2006).

Sin embargo, los entrevistados mencionaron que el uso de la CN no necesariamente va a implicar mayor complejidad para el encargo, aunque va a requerir un cambio en la metodología tanto en el proceso de la auditoría financiera como de la auditoría de sistemas que la alimenta (Entrevistados 5, 8).

B) Características de la información y los procesos del ente. Normativa aplicable

Un aspecto mencionado como fundamental en esta etapa se refiere al conocimiento de las características de la información que el ente estaría almacenando y/o procesando en la nube, incluso aquella que excede la información del sistema contable.

En este sentido, cabe analizar tanto la *sensibilidad* de la información que será cargada a la nube, como la *incidencia de la regulación* (leyes, reglamentaciones, disposiciones) que rige el tratamiento de la información administrada por la organización (Entrevistado 2), a fin de determinar si existen restricciones para el uso de la nube.

Este último aspecto es mencionado por la NIA 250 (A. 12), la cual establece que en la etapa del conocimiento del ente y su entorno el auditor deberá identificar el marco normativo aplicable y la forma en que el ente da cumplimiento al mismo.

En particular la preocupación mencionada se refiere a que las normas argentinas rigen *dentro del territorio* (por ejemplo, la Ley 25.326 de protección de datos personales). Sin embargo, una de las características de la CN es la independencia de localización entre el usuario y el proveedor del servicio, encontrándose muchas veces los servidores en ubicaciones definidas por el proveedor de acuerdo a su conveniencia y desconocidas para el ente, incluso en otros países. De esta forma, al mantener bases de datos en la nube, la información puede quedar alojada fuera del ámbito de aplicación de la norma, sin la protección que ésta requiere (Entrevistado 2).

Ello conlleva al análisis de los riesgos legales relacionados –descriptos en el próximo apartado de los resultados–, para lo cual resulta fundamental obtener una adecuada comprensión de la normativa aplicable en este primer acercamiento al cliente.

C) Naturaleza del servicio contratado

La comprensión del servicio y el tipo de producto contratado en la nube es un elemento al que se han referido varios de los profesionales.

Puede ocurrir que el servicio corresponda a una alternativa de las conocidas como *enlatados*, o sea, alguno de los servicios ampliamente conocidos (como SAP u Oracle), entregado en la nube en vez de la alternativa *on-premisse*, pero que en definitiva tienen gran parte de sus características en común con los servicios de licencia adquirida utilizados habitualmente por los clientes. En estos casos, los auditores pueden tener conocimiento del sistema por haber auditado otras empresas que lo utilicen, de modo que la comprensión del sistema parecería ser más sencilla.

Distinta es la situación cuando el servicio contratado ha sido *diseñado a medida* del usuario o su *uso no es tan difundido*, de modo que es posible que los auditores no tengan un conocimiento previo del producto (Entrevistado 5).

Por otro lado, respecto de la computación en la nube, la comprensión del servicio contratado implica determinar el modelo de servicio y de distribución implementados por el auditado. La distinción del modelo adoptado por el cliente es importante, dado que cada uno de ellos comprende distintos tipos de actividades, riesgos y responsabilidades que deberán ser comprendidos por el auditor.

> (…) los diferentes mecanismos de *infraestructure as a service*, *software as a service*, etc., o sea, los modos de conectarse, de utilizar servicios de la nube, son distintos; cada vez vas delegando más cosas o tercerizando más cosas, pero también vas teniendo menos control directo sobre la seguridad. (Entrevistado 1)

En particular, los usos mencionados por los auditores en las empresas argentinas se orientaban al modelo SAAS, aquel en el que se produce el mayor nivel de delegación y menor nivel de control por parte del usuario.

En lo que respecta a los modelos de despliegue, los entrevistados se refirieron en particular al conocimiento de la nube privada o pública, dejando de lado las alternativas de nube híbrida y comunitaria. Según los datos obtenidos, en el caso de una nube privada, el auditor puede a priori estar un poco más tranquilo en relación a la seguridad que si se tratara de una nube pública (Entrevistado 4), dado que, en principio, el acceso a los recursos en esta alternativa podría ser más restringido. Ello respalda los antecedentes encontrados que asignan a la nube privada un menor nivel de riesgo inherente (COSO, 2012).

> El mayor nivel de riesgo lo encontramos en una nube totalmente pública. Pero al menos hoy, las empresas que hayan realizado algún análisis de riesgo, no creo que la hayan adoptado. Es posible hacer uso de la tecnología a través de la nube privada, si bien con proyectos un poco más caros, logrando un cierto nivel de tercerización. Yo hoy todavía no recomendaría una tercerización abierta, total, en una nube pública. (Entrevistado 1)

A su vez, se analizaron las dos interpretaciones de la nube privada: que esté administrada por el ente usuario o por un tercero. El primer caso es considerado similar a un entorno de TI interno.

Esto se debe a que la administración y uso del servicio está a cargo únicamente del personal del auditado; presenta el menor nivel de delegación y el ente posee el mayor nivel de control sobre los recursos y los sistemas. En consecuencia, la auditoría en este caso no sería muy distinta a la realizada en un entorno de TI tradicional. Las nubes privadas administradas por un proveedor implican un cierto grado de tercerización, pero menor al de las nubes públicas; aquí la intervención del tercero aumenta la complejidad del servicio y requiere la aplicación de procedimientos de auditoría para un escenario de utilización de una organización de servicios (Entrevistado 2).

D) Infraestructura tecnológica

Los auditores de sistemas entrevistados indicaron que resulta necesario conocer cuál es la infraestructura tecnológica que subyace a los sistemas implementados por el ente, en particular en el servicio de la nube.

Ello implica el conocimiento de diversos aspectos de la CN que hacen en cierto modo a la complejidad del sistema: existencia de servidores virtualizados; uso de recursos compartidos; localización local o en el exterior de los servidores físicos que alojan la información; conectividad; medidas de control de acceso a los servidores; prácticas, normas, procedimientos y estándares de seguridad que definen al *data center* (Entrevistado 1).

> En definitiva, en la nube no es en el cielo, es en algún *data center* que no me pertenece a mí y que está conectado vía Internet en un proveedor externo en algún lugar. (Entrevistado 1)

Se menciona en la evaluación de la infraestructura la consideración de la forma de comunicación con la nube para comprender cuál es el esquema tecnológico (Entrevistado 4). Esto es, la revisión del responsable de la conexión y transporte de los servicios entre el usuario y la nube, a cargo de la transferencia de los datos.

La existencia de recursos compartidos con otros usuarios, según Mell y Grance (2011), es una de las características que definen a la CN. La diferencia puede darse entre nubes públicas y privadas, según se explicó previamente, ya que en estas últimas pueden no existir usuarios ajenos al ente auditado (los usuarios que comparten pertenecen únicamente a la organización). La comprensión de la infraestructura implica que el auditor necesita conocer la existencia o no de esos usuarios externos (Entrevistado 3).

E) Capacidad y solidez financiera del prestador del servicio

Este aspecto ha sido mencionado por los profesionales, quienes consideraron que el conocimiento de la capacidad del proveedor para garantizar un servicio de calidad al cliente es importante en esta etapa.

> Lo importante en este tema es la reputación de quien está prestando el servicio. (…) Si AAA[17] , que ya es un prestador de servicios de TI reconocido, presta servicio de CN a mi cliente, alguna seguridad me da. Con otros clientes nosotros vemos que utilizan ZZZ[18], que también prestan ese servicio, y nos quedamos tranquilos dado que conocemos sus procedimientos porque los auditamos. Si uno no lo auditara, te guías por lo que es dice el mercado. Ahora si lo tiene PPP -un proveedor pequeño y desconocido-, hoy no sé quién es y la verdad que no podría confiar mucho. Me haría un poco de ruido y vería que puedo hacer para mitigar ese riesgo y quedarme tranquilo respecto de que esa información está resguardada. (Entrevistado 5)

Los antecedentes y reputación del proveedor del servicio son una variable relevante al momento de evaluar riesgos de implementación de la CN por parte de los auditados. En este sentido, mencionaron que el hecho de que grandes proveedores como Accenture, SAP y Oracle estén comenzando a brindar servicios de CN es una seguridad sobre la orientación del mercado y una garantía para el usuario y el auditor de que todo el conocimiento generado por estos grandes proveedores estará puesto a disposición para garantizar la seguridad en la prestación del servicio.

Los auditores se sienten más confiados realizando auditorías sobre servicios prestados por un proveedor reconocido en el mercado, con trayectoria y una buena reputación, en particular considerando que el caso de la CN se trata de una nueva tecnología, cuyo uso aún no está muy difundido y no existen muchos antecedentes de prestación de este servicio en la República Argentina.

Distinta es la evaluación de los riesgos involucrados cuando el proveedor es un ente pequeño, muchas veces local, que no tiene la experiencia de los grandes. El hecho de que estos posean pocos clientes implica que es posible que estuvieran experimentando con el servicio que le están prestando al cliente de auditoría, incrementando los riesgos.

A partir del conocimiento de la reputación del prestador del servicio, podrá lograrse además el conocimiento de la capacidad y solvencia, que servirá para realizar la evaluación de riesgos vinculados a la permanencia del proveedor en la prestación del servicio.

F) Condiciones de la contratación y relación con la empresa de servicios

La evaluación del contrato firmado con el prestador del servicio ha sido uno de los aspectos fundamentales mencionados por la mayoría de los entrevistados, convirtiéndose en uno de los puntos más importantes en esta etapa. En parte, ello se debe a que mediante la lectura y comprensión de este documento se conocen diversos aspectos del servicio y de la relación usuario-proveedor.

A partir de la lectura del contrato, además de definir el servicio que el cliente está obteniendo del proveedor, se puede conocer las *actividades y responsabilidades a cargo de cada una de las*

[17] Por cuestiones de confidencialidad acordadas con los entrevistados se eliminaron los nombres de los prestadores del servicio en la nube mencionados.
[18] Idem nota anterior.

partes, lo cual ayuda planificar la auditoría, en particular en lo que respecta a la estrategia de auditoría del sistema (Entrevistado 3).

La distinción de responsabilidades es fundamental, considerando la importancia que adquiere el proveedor del servicio en la nube –garantizando la seguridad y confidencialidad de la información del usuario– y el rol de evaluador que debe asumir el usuario.

Considerando que el usuario sigue siendo el responsable por los procesos y la información gestionados en la nube, en el contrato podrá imponer ciertas *exigencias al proveedor* en relación a la forma en que el servicio debería ser prestado y a buenas prácticas de seguridad y tratamiento de información a ser implementadas –considerando la posibilidad de un contrato sujeto a negociación (Entrevistados 1, 2).

Desde el punto de vista de la auditoría, es importante que se incluya en los acuerdos la posibilidad de *monitoreo y evaluación de parte del usuario sobre el servicio del proveedor* y el cumplimiento que este haga de los requerimientos del usuario. El monitoreo debe referirse no solo a la calidad y disponibilidad del servicio en sí mismo, sino también a las buenas prácticas y controles internos que debe tener implementados el prestador para garantizar la seguridad de la información del usuario, considerando en particular la sensibilidad de la información financiera (Entrevistado 2).

> Yo incluiría, pero con mayúscula y con resaltador, en todo lo que son los planes de auditoría para este tipo especial de tercerización (…) un mayor énfasis en verificar el armado del contrato y el monitoreo de los cumplimientos. (Entrevistado 1)

La importancia de esta tarea se debe a que, como se ha dicho previamente, la tercerización no implica la delegación de la responsabilidad sobre el proveedor, debiendo el usuario verificar el cumplimiento de las normas y buenas prácticas que a él mismo le corresponden y en relación a su propia información y procesos delegados.

Se debe considerar además que, en la tercerización, el éxito de la externalización de TI depende de los términos del contrato, pero también de la forma como se gestiona la relación con el proveedor, lo cual es crítico considerando la noción de contratos incompletos (Hart & Moore, 1988, citado por Yigitbasioglu et al., 2013:103), en la medida en que es difícil cubrir la totalidad de las alternativas que podrían darse en la nube dentro del acuerdo. Ambas situaciones deben ser tenidas en cuenta en la auditoría.

5.2.4. PROCEDIMIENTOS A APLICAR PARA EL CONOCIMIENTO DEL ENTE Y SU ENTORNO EN RELACIÓN A LA COMPUTACIÓN EN LA NUBE

En esta etapa el acceso a la información resulta fundamental. Es usual incluir en el acuerdo o contrato de auditoría financiera la obligación del ente auditado de facilitar el acceso del profesional a los registros, información y documentos que sean necesarios de acuerdo a las circunstancias (Fowler Newton, 2004).

En la bibliografía se suelen mencionar las entrevistas con personas clave como uno de los primeros procedimientos para lograr un adecuado conocimiento del cliente. Sin embargo, en lo que respecta a la comprensión del uso de la CN por el auditado, todos los profesionales se refirieron como primer y principal procedimiento a la lectura de documentación relevante.

Ello se debe a que mucha de la información del sistema está en poder del prestador del servicio y según fue informado, es improbable que se pueda acceder al mismo para realizar indagaciones, debiendo aplicarse procedimientos como la lectura de documentación relevante relacionada al servicio para una adecuada comprensión.

También se mencionan las entrevistas con el personal del auditado para el conocimiento de otros aspectos además del ambiente de TI, los sistemas y el uso de la nube.

A) Observación e inspección de documentación

Tal como surge de la descripción de aspectos a ser indagados en la etapa de conocimiento del cliente, en general los entrevistados están de acuerdo en que la lectura de los contratos con el proveedor del servicio de la nube suele ser una fuente de información importante (Entrevistados 1, 2, 4).

La relación entre el proveedor y el usuario del servicio *cloud* se regula a través de los *acuerdos o contratos de servicios*, que definen los términos y condiciones de acceso y uso del mismo, el período de prestación, las condiciones de culminación de la relación, la disposición de los datos (por ejemplo, el plazo de conservación al que están sujetos), entre otras cuestiones. Para la organización, es un medio para reforzar el control y mantener la responsabilidad (*accountability*) sobre el ambiente de *cloud computing* (Jansen & Grance, 2011). En general dichos acuerdos constan de múltiples documentos que deberán ser considerados por el auditor e incluyen:

- acuerdo de nivel de servicio (*Service Level Agreement* – SLA): comprende el acuerdo entre el proveedor y el usuario acerca del nivel de servicio a prestar y las eventuales compensaciones que debe brindar el proveedor en caso de que no se cumpla;
- política de privacidad: en ella se establecen las prácticas para el procesamiento (*handling)* de los datos, esto es la forma en que la información del usuario es recolectada, utilizada y administrada por el proveedor;
- política de uso aceptable (*acceptable use policy)*: identifica los comportamientos prohibidos por el usuario de la nube;
- términos de uso: comprende aspectos adicionales, tales como autorización de servicios, limitaciones de responsabilidad y las modificaciones de los términos de los acuerdos.

Dichos contratos podrán variar según el nivel de negociación de las clausulas (CSA, 2011a:16; Jansen & Grance, 2011:7), diferenciándose entre los predefinidos o no negociables (que resultan ser los más utilizados principalmente en las nubes públicas) y los negociables.

Los no negociables adoptan la forma de contratos de adhesión, en los cuales los términos del servicio son fijados en su totalidad por el proveedor y en muchos casos pueden ser modificados de manera unilateral sin previo aviso.

En los acuerdos negociables las condiciones son establecidas de común acuerdo por el proveedor y el usuario, buscando la mayor satisfacción de sus necesidades. Los aspectos a ser acordados se refieren a niveles de servicio, seguridad, gobernanza, privacidad, antecedentes requeridos a los empleados del proveedor, propiedad de los datos, culminación del contrato, cumplimiento de normas, etc. Se asemejan a los contratos tradicionales de tercerización de servicios de TI. Para su utilización el usuario debiera contar con asesoramiento técnico y legal de modo de asegurarse que los requerimientos y necesidades de la organización se vean satisfechos.

El auditor deberá considerar que los contratos adaptados a la necesidad del usuario en general implican un mayor costo para la organización, ya que recibe un servicio a medida y se eliminan los beneficios de la economía de escala. Una alternativa sería la utilización de un servicio estándar y la posibilidad de mayores controles complementarios sobre el mismo por parte del usuario. Otra posibilidad sería el uso de nubes internas privadas que brindan a la organización mayor autoridad y control sobre la seguridad y privacidad, limitando el número de usuarios que comparten una plataforma de servicios.

Resulta relevante además la lectura de los *contratos con el proveedor del canal de transmisión de los datos*, que le será útil para conocer la infraestructura relacionada a la transmisión de la información (este puede y suele ser diferente de quien administra la nube) (Entrevistado 4).

Otros documentos que el auditor debe obtener y conocer en esta etapa –en caso que existan– incluyen manuales de procedimientos, organigramas, cursogramas, mapas de procesos y manuales técnicos de los sistemas utilizados (Entrevistado 8). Éstos permiten evaluar principalmente el sistema de control interno asociado al uso de la nube. Muchos de ellos deberían ser generados tanto en el proceso de implementación de la nube como durante su utilización. Según Cansler et al. (2007), en relación a la TI se incluyen:

- plan de sistemas a corto y largo plazo, debidamente formalizado, aprobado y comunicado a todos los involucrados. Cuando se considera la posibilidad de aplicación de una arquitectura de *cloud computing* se debe llevar a cabo a nivel organizacional un proceso de planificación preliminar, previo al contacto con el proveedor del servicio (Jansen & Grance, 2011:42); el resultado del mismo debiera verse plasmado en un conjunto de documentos que respalden: la definición de requisitos, la evaluación de seguridad y riesgos, la evaluación de competencia del proveedor;
- planificación de los recursos tecnológicos a ser utilizados (*hardware*, dispositivos de comunicaciones, sistemas operativos, etc), los cuales habrán sido adaptados al aplicar el nuevo entorno de CN;

- organigrama del área de sistemas y la descripción de roles, funciones y responsabilidades de cada puesto, los cuales pueden verse modificados a partir de la utilización de la CN, considerando que parte de las actividades son tercerizadas en el proveedor del servicio, y que se incorporan nuevos actores en la prestación del mismo (proveedor/*broker/carrier*/auditor de la nube) (Liu et al., 2011);
- manual de políticas y procedimientos relacionados con el ambiente de sistemas de información computadorizado. Las prácticas de gobernanza de la TI deberían haberse adaptado teniendo en cuenta las particularidades de la computación en la nube (éstas comprenden las políticas, procedimientos y estándares para el desarrollo de aplicaciones y el aprovisionamiento de servicios, así como para el diseño, implementación, testeo, uso y monitoreo de servicios desplegados (*deployed*) o contratados);
- políticas y procedimientos para adquisición/desarrollo de *software*, evaluación de calidad y pedidos e instrumentación de cambios;
- políticas de seguridad física y lógica. La planificación de estos aspectos en relación a la nube garantiza que el ambiente virtual es tan seguro como es posible y que se cumplen las políticas organizacionales y de seguridad;
- plan de cobertura de contingencias y continuidad de las actividades. La organización debe considerar el nivel de disponibilidad del servicio y su capacidad de *back up* y recupero de desastres –para asegurarse la restauración de los servicios *cloud* interrumpidos– y la utilización de servicios, equipos y localizaciones alternativas, en caso de que fueran requeridas para continuar con la operatoria habitual (Jansen & Grance, 2011:32). Para su elaboración se necesita la coordinación entre usuario y proveedor;
- documentación técnica de los sistemas. Permite al auditor obtener conocimiento de las aplicaciones que deberá evaluar e identificar los puntos de riesgo. Si ésta no existe o es parcial, debería solicitar los papeles de trabajo o anotaciones de quien desarrolló el sistema utilizado por el auditado.

Además de la documentación ya mencionada, los auditores coinciden en que resulta fundamental contar con informes sobre el control interno de la organización de servicios emitidos por auditores independientes. Estos informes serán analizados en el apartado *5.4. Evaluación del Control Interno,* por ser relevantes para dicha tarea del auditor.

B) Indagaciones a personas relevantes

La obtención de información mediante indagaciones a personas clave puede ser realizada mediante entrevistas tanto a personal del ente auditado como del proveedor del servicio.

En primer lugar, las entrevistas se realizan con el *personal de la empresa auditada*, tanto a los responsables del área de contabilidad o financiera, que son los usuarios de los sistemas, como al

personal del área de TI. Según mencionaron los Entrevistados 5 y 8, aquí participan los auditores contables.

El Entrevistado 8, quien propuso la diferenciación del entendimiento de los sistemas en general y en particular, propone una distinción de la ejecución del procedimiento en cada una de esas dos etapas:

a) en el ENTENDIMIENTO EN GENERAL los auditores contables realizan reuniones preliminares con el personal del auditado del área financiera (contadores, economistas), sin participación del personal de sistemas. En estas entrevistas se pretende conocer el mapa de los sistemas utilizados para comprender la visión del proceso del auditado;

b) en el ENTENDIMIENTO EN PARTICULAR, las entrevistas se realizan al personal del área de sistemas del auditado, con fuerte participación de los auditores de sistemas del estudio de auditoría. El objetivo consiste en profundizar la comprensión de los sistemas utilizados en cada uno de los procesos desarrollados por el auditado, que pueden ser diferentes para cada uno de ellos (que una parte de los procesos utilice SAP y otra parte algún sistema complejo no conocido por los auditores). En esta etapa los auditores financieros pueden participar de una primera reunión, en la que se discute el mapa de procesos, y continúan los auditores de sistemas más activamente para efectuar las revisiones correspondientes.

La posibilidad de mantener conversaciones con representantes del *proveedor del servicio* fue analizada por los auditores de sistemas entrevistados, dado que son quienes deben profundizar en aspectos más técnicos. Las opiniones fueron divergentes.

En algunos casos se considera posible tener acceso al proveedor para realizar consultas e incluso para ejecutar procedimientos de auditoría (el Entrevistado 6 lo ha tenido). Los Entrevistados 3 y 5 también lo consideran posible, si bien lo ven como un procedimiento alternativo para la obtención de información en el caso de que no existieran informes de control interno del proveedor, dado que se requerirá de información que seguramente excede a la que podría brindar el usuario. El contacto con el proveedor seguramente requerirá la participación de quien sea el jefe de tecnología del auditado como intermediario.

Por el contrario, los Entrevistado 4 y 2 consideran que en principio hay imposibilidad de acceder al proveedor; una de las particularidades que encuentran en el servicio de la nube, y que la distinguen de una tercerización común, es justamente la imposibilidad de acceder al proveedor del servicio, por ejemplo, porque en general no se encuentran en Argentina, o porque suelen poner restricciones para los contactos. Por eso es necesario contar con cualquier otro tipo de documentación que pudiera ser provista por el cliente.

La posibilidad de acceso a los proveedores sería improbable en el caso de los grandes proveedores de servicios (Google, Amazon, etc.) dado que poseen miles de usuarios de diferentes partes del mundo y les resultaría muy costoso atenderlos a todos. Por el contrario, en el caso de

proveedores pequeños, incluso locales, el acceso puede ser más sencillo, estando más dispuestos a dar respuesta a los auditores.

Cabe analizar aquí también el tamaño del ente auditado: grandes empresas –que en general son las asesoradas y auditadas por los profesionales entrevistados– tal vez no arriesgarían su información en proveedores pequeños sin una reputación que los respalde; en cambio los entes pequeños y medianos, por razones de costo o de facilidad, tal vez contratarían este tipo de proveedores, de modo que para sus auditores el acceso sería posible.

C) Observación de procesos y prueba de sistemas por el auditor

La *observación de procesos* es un procedimiento usual cuando se trabaja en ambientes influenciados por la TI. Incluso los auditores contables mencionaron participar de este procedimiento. Implica revisar en forma conjunta con el usuario o propietario de un proceso la eficacia y eficiencia de los controles diseñados y flujo de la información dentro de los sistemas, las interfaces, etc.; es decir, cómo se va agregando valor a la información que se utilizará para la elaboración de los estados contables. Permite verificar que las operaciones y controles que son comentadas durante la indagación se aplican tal cual lo expresan verbalmente (Entrevistados 2, 5, 7).

También dentro del ámbito del cliente auditado, además de la observación de las actividades ejecutadas por las personas a cargo del proceso, es importante la información que pueden recabar los auditores a partir de la *prueba de los sistemas*. Esto les permite obtener datos vinculados a la auditoría y probar las aplicaciones y controles internos implementados en los sistemas (Entrevistado 7). Para ello las empresas les asignan una terminal (PC) con usuarios específicos con alcance de auditoría, es decir con permiso para realizar ciertas actividades, pero sin generar cambios en las bases de datos del cliente. Esto sería particularmente útil en un entorno de CN, en el que tanto la información como las aplicaciones se encuentran protegidas mediante claves o controles de acceso para su seguridad.

Sería importante tener acceso a los proveedores no solo para solicitar información mediante entrevistas, sino también para realizar estas observaciones o pruebas de procesos, que facilitan el conocimiento y comprensión de los sistemas en la nube (Entrevistados 3, 6). Dicha apreciación se relaciona principalmente con la evaluación del sistema de control interno que será tratada en el apartado *5.4.*, pero resulta pertinente su mención en este apartado.

> (…) generalmente cuando hacemos una auditoría de sistemas lo que evaluamos es la seguridad de la base de datos o el servidor. Por ejemplo, ¿qué políticas de contraseña tiene? ¿Cuáles son los usuarios que están accediendo? Para eso les pedimos que nos corran determinados *scripts* que nos brindan parámetros de los servidores. Siendo que la información está fuera del ente auditado, deberíamos hacer algo parecido, solicitando la información al proveedor. (Entrevistado 3)

Sin embargo, y al igual que ocurre con las *indagaciones a personas relevantes*, existen opiniones encontradas en relación a la factibilidad de acceso al proveedor. El Entrevistado 6 considera que sería posible, pero el Entrevistado 1 sostiene que en ambientes de uso de CN se debe dar un proceso gradual hasta superar las dificultades para la obtención de información directamente del proveedor del servicio.

Según manifiesta, los proveedores han comenzado por obtener certificaciones o reportes de control interno, mediante auditorías independientes, brindando ese tipo de información a los usuarios y sus auditores de manera estandarizada y mediante la emisión de informes. Pero el entrevistado resalta que la dificultad está en obtener las *propias* evidencias sobre los sistemas vinculados a una auditoría en particular, el nivel de cumplimiento de los requerimientos de usuarios y el funcionamiento de los controles internos necesarios.

Las posibilidades de que los prestadores de servicios se sometan a auditorías de control interno por parte de los usuarios son más tangibles y se cumplen en sectores en particular, como es el caso de las entidades financieras, en las que la normativa está más madura. Lo ejemplifica de este modo:

> Por ejemplo, para darte una idea, una de las principales normas del Banco Central de la República Argentina es la comunicación A4609; dentro de esa norma, se exige que para los servicios tercerizados, quien presta el servicio está obligado a aceptar una auditoría del cliente. En el contrato no puede negarse a incluir una cláusula mediante la cual eventualmente el cliente puede mandar a sus auditores a revisar los servicios. De todos modos, todo lo que es legislación bancaria está un poco más avanzada y es más exigente. Pero esto no va a tardar en expandirse a otros sectores. (Entrevistado 1)

Se recomienda a usuarios y auditores intentar obtener datos teniendo como fuente de información primaria al proveedor, más aun si se han podido incluir en los contratos cláusulas que permitan a los auditores del ente usuario realizar evaluaciones sobre los sistemas del proveedor de la nube. Si no es posible, realizar evaluaciones detalladas sobre los contratos, certificaciones y cualquier otra documentación disponible vinculada al servicio.

Por su parte, el Entrevistado 2 considera que intentar este tipo de procedimientos no resulta pertinente en un ambiente de CN, y lo justifica indicando que una primera etapa de una auditoría de sistemas requiere una evaluación de los cimientos, de la infraestructura de base al sistema de información. Para ello, la aplicación de un procedimiento de observación requeriría acceder a las instalaciones del proveedor, lo cual es considerado improbable por la particularidad que presenta la nube en cuanto a restricciones de acceso, más aún cuando se trata de grandes proveedores que atienden a una cantidad importante de usuarios en todo el mundo, según ya se ha mencionado.

> Hacer una revisión sobre la infraestructura de la nube es ir en contra de la corriente de la nube. (…) Cuando hablo de un esquema de nube tengo una restricción, a priori, de que no podría acceder al proveedor, sino estoy en una tercerización común (…). Insisto en esto, ir a revisar las instalaciones del proveedor es posible en un esquema de tercerización, no en un esquema de nube, porque justamente la nube es intangible, y no podría acceder. (Entrevistado 2)

Incluso la independencia de localización entre usuario y proveedor, y en muchos casos el desconocimiento de la ubicación exacta de los servidores en los que se encuentra la información del ente (Buyya et al., 2009) es una particularidad de la nube que limita la posibilidad de aplicar este tipo de procedimientos para lograr un adecuado conocimiento y comprensión de los sistemas.

Una vez comprendidos los cimientos, el profesional indicó que el proceso continúa con la evaluación de los departamentos o procesos que están sobre ellos, respecto de lo cual considera que la nube no genera ninguna diferencia respecto de otros ambientes de TI, pudiéndose hacer la observación de procesos al lado de los usuarios en instalaciones del cliente auditado, como se mencionó al principio de este apartado.

D) Información obtenida a partir de otros servicios prestados al ente auditado

El punto expuesto ha surgido como una sub-categoría emergente en el análisis de este tópico. Es posible que el ente cuyos estados financieros deberán ser auditados sean clientes del estudio por auditorías u otros servicios de consultoría. También existe la posibilidad de que personal del estudio haya participado y brindado asesoramiento al cliente en el proceso de implementación de la CN durante el ejercicio cerrado sujeto a auditoría.

En estos casos, una fuente de información importante es el conocimiento que el equipo de auditoría o consultoría pueda haber obtenido durante el asesoramiento brindado al cliente auditado. La propia NIA 315 (Revisada) (A. 8) establece que cuando el profesional hubiera realizado otros encargos para el ente auditado, debería considerar si la información obtenida es relevante o no para la identificación de riesgos de distorsiones significativas en los estados financieros.

De hecho, los profesionales entrevistados consideraron importante que los clientes acudan a ellos antes de la implementación de la CN, para acompañar dicho proceso y asesorar en la toma de decisiones. Esto permite evitar problemas posteriores y obtener elementos de juicio que les facilite conocer y analizar los riesgos inherentes a la contratación del servicio de la nube en general, y de un proveedor en particular.

> Nosotros cuando vemos que los clientes -ya sean de auditoría, o del área de consultoría- están yendo a una solución en la nube, uno de los servicios que les ofrecemos es ayudarles en el proceso de evaluación. Nuestra idea es tratar de anticiparnos para que los proveedores no firmen un contrato y que después esa información esté expuesta. La idea es que antes de contratar un servicio hagan una evaluación de las medidas de seguridad que este proveedor les brinda. (Entrevistado 3)

Si bien en este trabajo se entrevistó a representantes de grandes estudios de auditoría, donde el área de consultoría de TI es un departamento independiente, los autores Tarmidi et al. (2014) reconocieron que en el caso de las PyMEs los contadores públicos, que actúan como auditores, son los principales asesores externos para la implementación y soporte de TI para la gestión contable, pudiendo verse involucrados en un proceso de aplicación de la CN. En consecuencia, es probable que sean consultados en la etapa de implementación, pudiendo opinar, aconsejar y obtener

información relevante que les sirva para el conocimiento del servicio, del proveedor y la evaluación de riesgos inherentes desde el inicio de la relación usuario-proveedor.

5.2.5. RESUMEN

La etapa del conocimiento del cliente es relevante en la realización de cualquier auditoría, y según surge del análisis, éste ha resultado ser un aspecto especialmente importante en la ejecución de encargos en entornos de CN.

Se destaca que su conocimiento será necesario al momento de decidir la aceptación del cliente o la continuidad de la relación con clientes que hubieran adoptado la nube. En este sentido, el entendimiento de los sistemas de información del auditado puede darse en dos oportunidades, a saber: a) en una primera auditoría, en la que sería útil el contacto con el auditor anterior, si fuera posible; b) en una auditoría recurrente, cuando el cliente hubiera adoptado la CN durante el ejercicio cuyos estados financieros deberán auditarse, debiendo tener en cuenta si el contador hubiese brindado asesoramiento al cliente para la implementación de la nube.

En particular se pretende conocer cuáles son los *aspectos* relevantes para el auditor en relación al cliente y su entorno en un ambiente de CN. Éstos han sido de lo más variados.

La identificación de las particularidades del *sistema de información y control interno afectados por la CN* se realiza a partir de la determinación de la información y procesos delegados al tercero. Para ello habría que lograr un entendimiento en general de los sistemas del ente auditado, identificar aquellos procesos ejecutados en la nube que pudieran tener efecto sobre los estados financieros, para luego profundizar su conocimiento y evaluación. Respecto de los procesos en la nube que no impactan directamente en la contabilidad, debería analizarse en cada caso si su evaluación es necesaria, por ejemplo, porque alimentan de algún modo la elaboración de los reportes financieros o porque se deba emitir opinión sobre el sistema de control interno del auditado.

Un aspecto que agregaron los entrevistados, incorporado como una sub-categoría dentro del esquema teórico, se refiere a las *características de la información y los procesos del ente delegados en la nube*. Interesa en particular la evaluación de la sensibilidad de la información y la existencia de normativa referida a su tratamiento, teniendo en cuenta la territorialidad de la aplicación de las normas y la particularidad de la nube respecto a la localización de la información, que muchas veces es desconocida por el usuario.

La comprensión de las *especificidades del servicio contratado en la nube* permitiría evaluar la complejidad del sistema de información del ente. Así resultaría posible comprender las actividades y responsabilidades del usuario derivadas del modelo de nube implementado, sus riesgos y controles internos relacionados. Estos aspectos son necesarios para la planificación de la auditoría. Los auditores de sistemas agregaron además, la importancia de comprender la

infraestructura tecnológica que sostiene al servicio en la nube, incluyendo la vinculada a las telecomunicaciones que permiten el uso del servicio.

La nube es reconocida como un modelo de tercerización; en consecuencia, mencionaron que también se debe tener en cuenta la *capacidad y solidez financiera del prestador del servicio*. Ello se justifica por los posibles riesgos vinculados al proveedor en lo que respecta a la disponibilidad de la información y en consecuencia la elaboración de los estados financieros, la cual debe trascender el ejercicio económico auditado.

El conocimiento de las *condiciones de la contratación y las pautas para la relación entre usuario y proveedor* ha sido resaltado por los entrevistados. Muchos de los aspectos indicados pueden conocerse a partir de estos documentos. En particular, se enfocaron en las cláusulas incluidas en los contratos de CN que permitan efectuar un seguimiento y monitoreo por parte del usuario, no solo de la calidad del servicio prestado, sino de los controles y las medidas de seguridad y confidencialidad adoptadas por el proveedor.

Finalmente, respecto de los procedimientos a aplicar por ambos tipos de auditores, se menciona como principal la *observación e inspección de documentación* tales como: contrato y accesorios, documentación elaborada por el ente auditado durante la implementación y utilización del servicio en la nube, informes de control interno de organizaciones de servicios, entre otros.

Las *entrevistas a personas clave* del personal del auditado y del proveedor fueron consideradas una fuente importante de información. Sin embargo, la obs*ervación de procesos y realización de pruebas de controles* en el proveedor se indicaron como poco probables.

Como fuente de información adicional a la mencionada por la bibliografía, se agrega aquella que los auditores hubieran obtenido en la *prestación de otros servicios al ente auditado*, como ser el asesoramiento para la aplicación de la nube.

En el Cuadro 22 se resumen los aspectos y procedimientos aplicables para el conocimiento del ente y su entorno cuando el auditado hace uso de servicios de computación en la nube.

Cuadro 22 - Conocimiento del cliente y su entorno en ambientes de CN

TÒPICO	CATEGORIAS	SUBCATEGORÌAS	
CONOCIMIENTO DEL ENTE Y SU ENTORNO Uso de una organización de servicios para la prestación de servicios de TI	**ASPECTOS**	**CLIENTE Y SU ENTORNO**	Sistemas de Contabilidad y CI afectados por la TI (importancia y complejidad) • Entendimiento general de los sistemas, incluyendo la CN • Entendimiento particular de procesos en la CN que afectan la información de los EEFF
			Naturaleza y significatividad del servicio contratado a la OS • A medida o estandarizado • Modelo de servicio de CN • Modelo de distribución de CN
			Naturaleza e importancia de transacciones/cuentas/procesos afectados por la OS • Características de la información y los procesos del ente • Sensibilidad • Normativa aplicable
			Grado de interacción entre actividades de la OS y entidad auditada (controles complementarios)
			Naturaleza de la relación y condiciones de la contratación con la OS • Confidencialidad • Monitoreo por el usuario • Auditorías
			Infraestructura tecnológica • Servidores virtualizados • Recursos compartidos • Telecomunicaciones
			Capacidad del prestador del servicio y solidez financiera
		CONTROL INTERNO	*Tratado en el apartado 5.4.*
	PROCEDIMIENTOS	Indagaciones a personas relevantes • Personal del ente auditado (contabilidad; sistemas)	
		Observación e inspección de procesos • Del ente auditado • De la OS	
		Observación e inspección de documentación • Contrato y documentación complementaria • Documentación generada en el proceso de implementación de la nube • Informes de Control Interno de la empresa de servicios	
		Procedimientos analíticos	
		Contacto y eventual visita a la OS	
		Información obtenida de otros servicios prestados al ente auditado.	

***LECTURA**: Letra azul: elemento nuevo. Letra en otro color: elemento original nombrado con mayor (verde) o menor (rojo) énfasis en las entrevistas.*

Fuente: Elaboración propia.

5.3. IDENTIFICACIÓN Y VALORACIÓN DE RIESGOS DE LA CN RELEVANTES PARA LA AUDITORÍA DE ESTADOS FINANCIEROS

El presente apartado pretende dar satisfacción al siguiente objetivo específico:

Identificar y describir los riesgos derivados del uso de la computación en la nube para la elaboración de información contable, relevantes para la auditoría de estados financieros.

El análisis realizado contempla que si bien distintos autores plantean múltiples factores de riesgos que afectan a las organizaciones por el uso de la computación en la nube, no todos ellos serán considerados en la evaluación de riesgos realizada en el marco de una auditoría financiera, o al menos no serán valorizados del mismo modo.

Se utiliza la clasificación de los diferentes factores de riesgo presentada en el marco teórico de esta tesis, los cuales fueron incluidos en el instrumento para la realización de las entrevistas a los profesionales.

5.3.1. ANÁLISIS GLOBAL DE RIESGOS DERIVADOS DEL USO DE LA COMPUTACIÓN EN LA NUBE

Los entrevistados concuerdan en que muchos de los riesgos de la CN identificados en la bibliografía son eventos que tienen probabilidad de ocurrencia, con un potencial efecto negativo en las organizaciones usuarias. Pero su análisis debe ser realizado como una medida estratégica por parte de los administradores, con colaboración de personal interno del área de TI o de un asesor externo, decidiendo si se asumen los riesgos o se toman las medidas necesarias para mitigar el impacto de su ocurrencia. Sin embargo, no todos esos eventos se relacionan o podrían incidir en la auditoría de estados financieros.

Por otro lado, se mencionó que todos los riesgos aquí descriptos deben ser considerados por los entes auditados en sus evaluaciones de riesgos y serán analizados por los auditores financieros, aun cuando pareciera imposible su ocurrencia o nulo su potencial impacto. En su caso, corresponderá asignar probabilidades de ocurrencia o impacto cercano a cero cuando se considere que no son relevantes para el encargo de auditoría en particular (Entrevistados 5, 8).

Algunos de los riesgos analizados, en caso de ocurrencia, podrían tener un fuerte impacto sobre la auditoría financiera, e incluso podrían generar la imposibilidad de ejecutar el encargo, por ejemplo cuando la consecuencia fuera la pérdida total de la información sujeta a auditoría.

Existen opiniones dispares acerca de si auditoría en un entorno en la nube debe ser considerada como más riesgosa que una realizada en otro entorno de TI. A priori, podría pensarse que esto es así, porque se posee un menor control sobre los sistemas y la información, y no es posible tener seguridad absoluta acerca del modo en el que el tercero los administra. Pero los entrevistados recomiendan analizar cada caso, teniendo en cuenta factores como la reputación y experiencia del proveedor del servicio, los recaudos adoptados por el cliente al momento de la

contratación, los controles internos aplicados por el usuario y las medidas de seguridad implementadas, entre otras cuestiones (Entrevistados 3, 4, 6).

5.3.2. CATEGORÍAS DE RIESGOS DERIVADOS DEL USO DE LA CN Y SU RELEVANCIA PARA LA AUDITORÍA DE ESTADOS FINANCIEROS

A continuación, se resumen los resultados de la evaluación de factores de riesgos realizada por los entrevistados. Los comentarios fueron obtenidos a partir de la consulta realizada sobre cada fuente de riesgos definida en el marco teórico, identificándose aquellos factores relevantes para la auditoría. En algunos casos los entrevistados propusieron una valoración en cuanto a probabilidad de ocurrencia e impacto esperado, si bien es claro que estas cuestiones deben ser analizadas en cada encargo.

El análisis se divide, tal como fue expuesto en la RBS presentada en el marco teórico, en los siguientes grupos de riesgos:

a) Riesgos derivados del proceso de implementación de la nube por el ente;

b) Riesgos propios de la tercerización;

c) Riesgos técnicos;

d) Riegos legales;

e) Riesgos contra la seguridad física.

a) Riesgos derivados del proceso de implementación de la nube por el ente

En un proceso de auditoría, es probable que este tipo de riesgos sean evaluados principalmente por los auditores del área de sistemas, en caso de que sean convocados. Caso contrario, según opinión de un auditor financiero, es posible que no sean detectados o evaluados (Entrevistado 5).

La *falta de planificación del proceso de implementación de la nube*, si bien es un riesgo a tener en cuenta por su potencial impacto, es valorado con una probabilidad de ocurrencia baja en el caso de que el usuario sea una gran empresa (Entrevistado 4). Esto es porque los administradores comprenden su importancia y tratan de implementar controles para mitigar los factores de riesgos identificados. En el caso de la nube, es de esperar que las organizaciones solo migren sus sistemas una vez que estén convencidas en cuanto a la seguridad de la alternativa. Tal como se ha mencionado en otras oportunidades, es posible que si la auditoría se estuviera realizando sobre empresas de menor tamaño, con sistemas de evaluación de riesgos y de control interno deficientes, la probabilidad de este riesgo sea valorizada como alta.

> Dudo que una empresa ponga en riesgo toda su información en subirse a la nube sin antes hacer una buena planificación y una buena evaluación del riesgo. (Entrevistado 5)

Los riesgos derivados de un mal proceso de aplicación de la nube por parte del ente auditado pueden tener un alto impacto en la auditoría financiera. Su evaluación se asimila a los casos en los que los auditados efectúan cambios o actualizaciones en los sistemas de procesamiento de la información contable (Entrevistado 8). La evaluación que se realice de dicho proceso define si es posible depositar mayor o menor confianza en la información que surge de su posterior utilización. Este tipo de decisiones del cliente afectan el proceso de auditoría financiera, y en particular la planificación, dado que la misma utiliza información contable originada en dichos sistemas.

Seguramente la falta de planificación y un proceso de implementación del sistema no adecuado serán evaluados como una deficiencia de controles relevantes y afectará el enfoque de auditoría a aplicar: no será posible confiar en controles y aplicar un enfoque de cumplimiento, ya sea para la auditoría en general o para la auditoría del componente específico respecto del cual se hubiera implementado la CN (Entrevistados 5, 8). En el análisis de las respuestas de los auditores financieros se distinguen las siguientes situaciones:

- Frente a un cambio de sistemas es posible que se decida la aplicación de enfoque sustantivo en el ejercicio económico en el que el mismo se produce, no confiando en los controles, aunque en encargos previos se hubiera aplicado un enfoque de cumplimiento. De todos modos, se debería realizar la evaluación de controles y específicamente los riesgos relacionados a la implementación del nuevo sistema, dado que serviría para las auditorías sucesivas. Si el sistema es adecuado y funciona correctamente, puede confiarse en el mismo en adelante y aplicarse un enfoque de control.
- Si a priori se decide aplicar un enfoque sustantivo, considerando el conocimiento que se tiene del ente auditado y concluyendo que su sistema de control interno no es digno de confianza, este tipo de riesgos no modificaría el enfoque de auditoría; la detección de un error en el proceso de implementación simplemente implicará deficiencias de control a ser informadas a la gerencia en la carta con recomendaciones.

Una de las dificultades que se detectan en relación a la aplicación de un enfoque de cumplimiento en este tipo de situaciones es que aun cuando los controles para la implementación del nuevo sistema estuvieran diseñados, muchas veces los mismos no son ejecutados, o son realizados informalmente, sin que queden evidencias escritas de su cumplimiento. Esto lleva a que los auditores no puedan validar la correcta ejecución de los mismos a fin de decidir si depositan confianza en ellos o no (Entrevistado 5).

Respecto del *riesgo de uso no autorizado de la nube* dentro de un ente, el Entrevistado 6 mencionó que –según su experiencia en auditorías informáticas– es conveniente analizar el efecto de las operaciones ejecutadas en el sistema no autorizado sobre el circuito contable. Es así que distinguió las siguientes situaciones:

- Pensando en un sistema de gestión contable completo, se estarían analizando operaciones con efecto transaccional, hechos económicos que deben ser incorporados en el sistema contable. Es

improbable que esto sea escondido en la nube o utilizado sin autorización dentro del ente, dado que está integrado por diferentes módulos, y no podría desglosarse una parte para gestionarlo en la nube. Al momento de efectuar el entendimiento del sistema de gestión, y la forma en que la información financiera se genera dentro de la compañía, es posible detectar si existen desvíos de información no autorizados a la nube. Según su evaluación, este no sería un riesgo probable con efecto en la auditoría financiera.

- Si se considera la posibilidad de uso de la nube como un *file server* para resguardo de información por parte de los empleados sin que los niveles superiores o el área de sistemas conozca estas prácticas –sea con una intención maliciosa o no– no se estaría afectando a las transacciones en sí mismas. Dicha información podría llegar a ser confidencial pero no transaccional (ej. un listado de ventas mensuales). Este no sería un riesgo de alto impacto en la auditoría financiera, dado que la información transaccional debería estar incluida en el sistema de gestión del cual se obtiene la información a auditar.

En caso de empresas más pequeñas, los módulos de registración pueden ser más independientes, de modo que se consideró la posibilidad de que alguno de ellos estuviera cargado en la nube (por ejemplo, un Excel almacenado en la nube con el inventario de bienes de uso); aun en este caso considera que no sería un sistema de soporte transaccional, sino que se estaría utilizando la nube como un medio de almacenamiento.

En definitiva, el riesgo de uso no autorizado pareciera no tener alta probabilidad o alto impacto a los fines de la auditoría financiera, según se interpreta de sus comentarios.

Respecto de la *forma de prevenir este tipo de riesgos*, es importante la intervención del auditor –de sistemas o financiero– en todo el proceso de selección e implementación de la computación en la nube: en la identificación de los distintos oferentes, en la definición de los requerimientos de control interno y pistas de auditoría, en la evaluación del sistema en la etapa de pre-producción. Cabe aclarar que, si bien esta es una situación deseable, no siempre ocurre en la realidad (Entrevistados 2, 3).

> (…) La intervención del auditor en la implementación va a hacer que se tengan presentes muchas más cuestiones que simplemente el funcionamiento del negocio, como la definición de controles internos que después es mucho más difícil de aplicar. Me parece que ahí es el paso fundamental. Pero la idea de que el auditor debe estar presente es más de libro que de la realidad, lamentablemente. (Entrevistado 2)

b) Riesgos propios de la tercerización

Este riesgo no ha sido necesariamente considerado como propio de la nube, sino que se presenta en otros tipos de tercerización. Si bien se reconoce su existencia, en parte puede ser gestionado mediante una correcta selección del proveedor del servicio en la nube (Entrevistado 6). Ello requiere la comparación de las prestaciones y reputación de los potenciales prestadores d como parte de un adecuado proceso de implementación de la nube.

El primer factor mencionado como un aspecto negativo de la CN es el *riesgo de pérdida de gobernabilidad*.

> Es como tener tu valor o activo fuera de tu control (…) lo hace más inseguro que tenerlo adentro de la empresa. Lo que pasa ahí es el equilibrio entre el riesgo asumido y la alta disponibilidad y elasticidad del servicio. Cada empresa evaluará desde su perspectiva esa ecuación beneficio versus riesgo asumido. (Entrevistado 2)

Tanto la *falta de gobernabilidad de los datos* como *la falta de transparencia* afectan significativamente a la auditoría financiera en lo que hace a la etapa de evaluación de riesgos (Entrevistado 8). Esto es así porque al momento de decidir aceptar el cliente (o continuar) y planificar la auditoría, es necesario evaluar los riesgos del cliente. Si existe externalización de sistemas y/o procesos, la evaluación se extiende al prestador del servicio, requiriéndose información del tercero involucrado; ésta podría ser obtenida, por ejemplo, de los informes tipo SSAE 16[19] (si estuvieran disponibles), que serán analizados en el próximo capítulo.

Solo el Entrevistado 5 se refirió al riesgo de eventual *incumplimiento de requisitos de certificaciones*, pero relacionándolo a las autorizaciones que el ente auditado pudiera haber obtenido de parte del órgano regulador –en su caso la IGJ, o el que corresponda– en relación a llevar sus libros en forma electrónica, de acuerdo a lo que establece el artículo 61 de la Ley General de Sociedades, que será analizado más adelante junto con los riesgos legales. Cuando el ente hubiera obtenido la autorización mencionada y posteriormente comenzara a utilizar servicios en la nube, puede requerirse la obtención de una nueva autorización, en la medida en que los cambios en los sistemas informáticos pueden ser sustanciales.

Podría ocurrir que el usuario perdiera otras certificaciones obtenidas a partir del uso de la CN, porque dejara de cumplir con sus requisitos (por ejemplo, certificaciones sobre gestión de la calidad). Sin embargo ninguno de los entrevistados se refirió a este riesgo como relevante para el auditor financiero.

Respecto del riesgo de *lock-in*, pareciera que afecta más al ente auditado que a la auditoría financiera. En particular podría quedar cautivo del *software* de gestión utilizado, el cual puede ser específico del proveedor en la nube, dificultando la migración a uno nuevo o el retorno a los sistemas propios del ente. La apropiada comprensión de las características del servicio antes de la contratación es útil para prevenir este riesgo. En estos casos es fundamental el asesoramiento de personas con conocimientos jurídicos, de modo de poder interpretar adecuadamente los acuerdos de prestación de servicios y conocer que se puede esperar y/o requerir al proveedor en caso de culminar el contrato y necesitar cambiar de ambiente para continuar con el procesamiento de la información (Entrevistado 6).

[19] Al momento de realizar las entrevistas el SSAE 18 todavía no se encontraba vigente.

Desde el punto de vista del auditor de estados financieros, este riesgo no pareciera afectarlo, en la medida en que independientemente de que el auditado sea cautivo del sistema contratado, su preocupación es que la información se encuentre disponible para poder auditarla.

El resto de los factores de riesgo incluidos en esta categoría no fueron mencionados por los entrevistados.

c) Riesgos técnicos

En las conversaciones sobre esta fuente de riesgos, los entrevistados se refirieron a las subcategorías mencionadas inicialmente en el marco teórico, de modo que se decidió incluirlas en el Nivel 2 de la RBS propuesta, a saber:

a) riesgos de continuidad, o sea, problemas en la disponibilidad del servicio y la información, sea por fallas en el proveedor o de los prestadores de servicios relacionados (como Internet);

b) riesgos de seguridad, referidos a fallas que permiten el acceso de terceros no autorizados.

El *riesgo de continuidad*, o potencial falta de disponibilidad de la información, es considerado un riesgo importante para la auditoría financiera, en la medida en que es imposible ejecutar el encargo si la información sujeta a revisión no puede ser consultada (Entrevistado 5). En este caso, son importantes las medidas que adopte el proveedor para asegurar de alguna manera la disponibilidad de la información, debiéndosele exigir, por ejemplo, políticas de *back up* seguras (Entrevistado 6).

> Yo puedo entender que se me caiga el servicio por dos, tres horas o por dos días, pero acabada la interrupción la información tiene que estar de vuelta disponible y eso es lo más difícil. (Entrevistado 6)

Respecto de la *falta de disponibilidad del servicio por fallas en la conexión*, existe acuerdo en que no es un riesgo específico de la nube, pero que posee probabilidad e impacto alto considerando los problemas de infraestructura de las telecomunicaciones en la Argentina que fueron mencionados también como una barrera para la implementación de esta alternativa en el apartado *5.1.3*. de esta tesis. En general, inclusive cuando no se hace uso de la nube, este tipo de problemas en las comunicaciones genera complicaciones importantes en las empresas (Entrevistados 3, 5, 6, 7, 8).

> Imagínate una empresa que está mandando megas y megas de información por la red. Si se llega a producir una caída de la red de comunicaciones, es gravísimo. A cualquier empresa, que a fin de mes se le caiga la comunicación, es un problema, porque todos los procesos de facturación, de pago de clientes, etc., se cancelan. Entonces, ¿cómo haces para decirle a un proveedor que en realidad no le pagaste porque se pinchó la nube? La verdad es algo complicado. (Entrevistado 5)

> Antes de entrar en alguna compañía que use la nube o no, creo que los problemas de Internet los tenemos todos. Por eso en las compañías, cuando se corta Internet, es como que la empresa se paraliza. De todos modos me parece que no sería nada adicional a los problemas que ya tenemos. (Entrevistado 8)

Este es un riesgo que debe ser gestionado por el ente usuario, porque el proveedor del servicio en la nube se hace cargo desde que la información le llega y entra a la puerta de su data center. El traslado de la información desde la compañía hasta el proveedor es responsabilidad del usuario, debiendo éste contratar los proveedores de servicios intermedios, como Internet.

En consecuencia, es el ente usuario quien debe analizar los contratos y evaluar costos ocultos en el uso de la nube, además de garantizar las medidas de seguridad adecuadas sobre este tramo, así como la redundancia sobre las conexiones de comunicaciones (de modo de tener siempre una vía alternativa funcionando en caso de desperfectos), así como el encriptado de los datos para evitar su interceptación por parte de terceros cuando están en tránsito (Entrevistados 3, 6).

El riesgo relacionado a las comunicaciones depende del país y de su disponibilidad tecnológica (Entrevistados 3, 6). En la Argentina pareciera que existen ciertas restricciones que deberá enfrentar el ente usuario para gestionarlo, ya que –al menos por el momento– los servicios de telecomunicaciones parecieran no estar preparados en todo el territorio para soportar este tipo de servicios: no existen muchos proveedores de transmisión de datos, e incluso en algunas zonas del interior del país puede existir una única oferta u ofertas con servicios deficientes. El ente que desee utilizar CN u otra opción de tercerización similar, podría analizar otras soluciones de infraestructura de comunicaciones (como el uso de satélites o microondas). Puede ocurrir que esta inversión en infraestructura haga que la solución de la nube comience a ser más onerosa que tener un *data center* y administrarlo internamente, debido a estos costos operativos que inicialmente no estaban previstos (Entrevistado 6).

El Entrevistado 2 considera otros riesgos técnicos más específicos y ciertas medidas que deberían tomarse el respecto:

a) el funcionamiento de interfaces entre los servicios locales y los montados en la nube es más complejo. Propone evitar la utilización de sistemas muy específicos de nicho (por ejemplo, sistemas para una parte de un proceso de una industria en la nube, que se deba integrar con un sistema local), sino más bien integrar todo en una misma solución para evitar las conexiones, dado que es mucho más complejo darles un contexto de seguridad;

b) ante la posibilidad de cortes inesperados en el proceso de actualización de información en la nube, la integridad de la información puede verse amenazada. En consecuencia, plantea la necesidad de tener controles de totales permanentes entre información de detalle almacenada en la nube y saldos almacenados localmente (por ejemplo, totales de inventario con el saldo contable);

c) el control sobre la continuidad de la información es más complejo. Teniendo el proceso en los sistemas propios, se conoce con exactitud cuál es la ventana de tiempo de falencia de recuperación que se tiene (es decir, si se hace un *back up* todas las noches, dependiendo del momento en que se tenga la interrupción o se genere la vulnerabilidad, se va a poder determinar cuanta información se perdió ante un incidente). En cambio, la nube no permite determinar con

exactitud cuál es la ventana de tiempo, justamente porque el ente usuario no está administrando el proceso de *back up*. En todo caso, se deberían adoptar medidas de resguardo adecuadas para poder superar este problema.

Las limitaciones mencionadas, referidas a la disponibilidad de la información, son importantes desde el punto de vista de la auditoría financiera dado que podrían restringir el acceso a la información sujeta a revisión. Ahora bien, es un riesgo inherente a la utilización de la nube, respecto del cual es poco lo que el auditor puede hacer. En todo caso sería 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.

Respecto del segundo grupo de factores de riesgo, relacionados con la *seguridad de la información y el resguardo frente al acceso por parte de terceros*, el Entrevistado 3 consideró que es uno de los principales riesgos a tener en cuenta, en particular por la auditoría financiera, dada la eventual pérdida de datos y modificaciones no autorizadas, que hacen que la información a auditar en los estados contables no sea confiable.

Por su parte, el Entrevistado 5 considera que son riesgos que de algún modo se encuentran más controlados desde el punto de vista de la infraestructura, al menos en lo que respecta al acceso por parte de sujetos ajenos al ente auditado. Por ejemplo, en relación a las *fallas de los mecanismos de aislamiento en los equipos virtualizados compartidos*, considera que es improbable que un usuario pudiera acceder a los datos de otro, dado que se han desarrollado a la fecha medidas de separación lógica adecuadas que permiten mitigar este riesgo.

Los demás factores de riesgos se refieren a los *accesos intencionales de terceros*. En estos casos, lo que importa para el auditor financiero es la eventual modificación de la información por alguien no autorizado; es decir, no preocupa que la información sólo sea vista por el tercero. Este último caso se trata de un problema relacionado a la confidencialidad, que preocupa al ente propietario de los datos quien seguramente pretenderá incorporar cláusulas de protección en los acuerdos de servicio, aunque es imposible tener certeza de que éstas se respeten de manera absoluta (Entrevistado 5).

En general, estos problemas no se deben tanto a fallas del sistema en sí mismo, sino que requieren de una participación intencional de un humano, que intente robar la información o que deje *abierta una puerta del sistema para que entre otra persona*. Según la experiencia del Entrevistado 5, en la mayoría de los casos los robos de información a empresas no son efectuados por parte de los proveedores de estos servicios tercerizados, sino por personas internas al ente auditado.

Existen diferentes medidas de seguridad que se pueden aplicar para evitar esta clase de riesgos. A fin de prevenir la modificación no autorizada, en un sistema de información contable en la nube sería necesario abolir cualquier tipo de asiento manual o tener muy claro quiénes son

aquellos sujetos autorizados a hacerlo, gestionando la seguridad de perfiles, roles y funcionalidad (Entrevistado 2).

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. Desde el rol de usuario, resulta importante la evaluación inicial y periódica de las medidas de seguridad del proveedor (Entrevistado 3). Por ejemplo, mediante la contratación de especialistas para efectuar la selección del proveedor, así como para la realización posterior de lo que se conoce como *tests de intrusión*; esto es, un *hackeo ético* a fin de probar con anticipación cuan vulnerables son las medidas de seguridad implementadas por los proveedores del servicio tercerizado.

Estos servicios son prestados por los equipos de TI en los grandes estudios de auditoría. Los entrevistados –integrantes de esos estudios– manifestaron que según su experiencia, en muchas compañías –incluso en las grandes– suelen dejarse de lado estas precauciones, denotando una deficiente gestión de riesgos por parte de los usuarios de servicios tercerizados. En empresas pequeñas esto podría verse acentuado, tanto por desconocimiento como por el costo que representa su contratación (Entrevistado 3).

d) Riesgos legales

Nuevamente el análisis de los profesionales fue realizado distinguiendo dos grupos de factores de riesgos, incluyéndose también las subcategorías emergentes en la RBS final propuesta en este capítulo, a saber:

a) riesgos derivados del marco jurídico del país donde está alojada la información;

b) riesgos de incumplimiento de la normativa que rige al ente auditado.

El primer grupo, vinculado a la *ubicación en la que se encuentra la información* –muchas veces desconocida para el ente usuario– pareciera ser más relevante para el auditado que para el auditor financiero.

Implica conocer la jurisdicción que corresponde en caso de reclamos o juicios, y la normativa aplicable cuando la información se encuentre alojada en jurisdicciones diferentes al país del ente usuario (nubes transfronterizas). 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 de los contratos es fundamental para mitigar el riesgo (Entrevistado 6).

Sin embargo, el principal factor de riesgo considerado por los entrevistados fue el referido al *incumplimiento de normas*.

Este es un riesgo difícil de gestionar por el usuario. El negocio del ente define la normativa que le es aplicable. Si esta impidiera o restringiera el uso de la computación en la nube, el ente en principio no podría hacer nada al respecto, salvo evitar el uso de esta alternativa.

> [Los riesgos legales] son los menos administrables por la organización, son los que vienen fácticos, por decirlo de alguna manera, por la definición del negocio del usuario. Todos los otros que se mencionan son más o menos atribuibles al cliente, en cambio, el legal no. Por lo cual, es el primero que se debe tener claro porque el cliente no lo puede administrar. (Entrevistado 2)

En este grupo los entrevistados se focalizaron principalmente en las normas referidas a los *sistemas de información contable.* El Entrevistado 7 mencionó que en general la obligación de los entes es llevar los libros de acuerdo a las exigencias legales y mantener la información en la sede de la compañía que corresponda. El Cuadro 23 resume la normativa relacionada.

Cuadro 23 - Normas legales analizadas

Código Civil y Comercial de la Nación – Ley 26.994	ARTICULO 322.- Registros indispensables. Son registros indispensables, los siguientes: a) diario; b) inventario y balances; c) aquellos que corresponden a una adecuada integración de un sistema de contabilidad y que exige la importancia y la naturaleza de las actividades a desarrollar; d) los que en forma especial impone este Código u otras leyes. ARTICULO 323.- Libros. El interesado debe llevar su contabilidad mediante la utilización de libros y debe presentarlos, debidamente encuadernados, para su individualización en el Registro Público correspondiente. (…)(el resaltado es propio) ARTICULO 325.- Forma de llevar los registros. Los libros y registros contables deben ser llevados en forma cronológica, actualizada, sin alteración alguna que no haya sido debidamente salvada. También deben llevarse en idioma y moneda nacional. Deben permitir determinar al cierre de cada ejercicio económico anual la situación patrimonial, su evolución y sus resultados. Los libros y registros del artículo 322 deben permanecer en el **domicilio de su titular**. (el resaltado es propio) ARTICULO 329.- Actos sujetos a autorización. El titular puede, previa autorización del Registro Público de su domicilio: a) sustituir uno o más libros, excepto el de Inventarios y Balances, o alguna de sus formalidades, por la utilización de ordenadores u otros medios mecánicos, magnéticos o electrónicos que permitan la individualización de las operaciones y de las correspondientes cuentas deudoras y acreedoras y su posterior verificación; b) conservar la documentación en microfilm, discos ópticos u otros medios aptos para ese fin. La petición que se formule al Registro Público debe contener una adecuada descripción del sistema, con dictamen técnico de Contador Público e indicación de los antecedentes de su utilización. Una vez aprobado, el pedido de autorización y la respectiva resolución del organismo de contralor, deben transcribirse en el libro de Inventarios y Balances. La autorización sólo se debe otorgar si los medios alternativos son equivalentes, en cuanto a inviolabilidad, verosimilitud y completitud, a los sistemas cuyo reemplazo se solicita. (el resaltado es propio)
Ley General de Sociedades Comerciales – Ley 19.550	**Medios mecánicos y otros.** **ARTICULO 61.** — Podrá prescindirse del cumplimiento de las formalidades impuestas por el artículo 53 del Código de Comercio para llevar los libros en la medida que la autoridad de control o el Registro Público de

	Comercio autoricen la sustitución de los mismos por ordenadores, medios mecánicos o magnéticos u otros, salvo el de Inventarios y Balances. La petición deberá incluir una adecuada descripción del sistema, con dictamen técnico o antecedentes de su utilización, lo que, una vez autorizada, deberá transcribirse en el libro de Inventarios y Balances. Los pedidos de autorización se considerarán automáticamente aprobados dentro de los treinta (30) días de efectuados, si no mediare observación previa o rechazo fundado. El libro Diario podrá ser llevado con asientos globales que no comprendan períodos mayores de un (1) mes. El sistema de contabilización debe permitir la individualización de las operaciones, las correspondientes cuentas deudoras y acreedoras y su posterior verificación, con arreglo al artículo 43 del Código de Comercio. (el resaltado es propio)

Fuente: Ley 26.994 y Ley 19.950[20].

Los informantes se refirieron ampliamente a la aplicación de estas normas. Uno de los primeros temas destacados fue la *obtención de autorización para llevar libros en medios mecánicos* en entornos de tercerización similares a la CN (de acuerdo a lo establecido por el art. 61 de la Ley 19.550, regulado en los artículos 328 y 335 de la Resolución 07/2015 de la IGJ).

En particular se basaron en los requerimientos de la Inspección General de Justicia (IGJ), ente regulador de entidades con domicilio en la Ciudad Autónoma de Buenos Aires, que se corresponden en muchos casos con los clientes de los estudios a los que pertenecen los entrevistados (Entrevistados 3, 5, 8). Sus opiniones se refieren no solo a lo que establece la normativa, sino también a las dificultades prácticas que han encontrado en su aplicación.

Uno de los principales problemas se refiere a la *ubicación de la información contable fuera de la jurisdicción de la Argentina* (Entrevistado 3). Si bien la normativa de la IGJ no indica que la información contable *no pueda* estar ubicada en el exterior, se establecen ciertos requisitos que lo limitan en el proceso de otorgamiento de la autorización para el empleo de medios mecánicos u otros similares para llevar libros de comercio.

La incorporación de este tipo de requisitos se debe a las dificultades que encuentra el ente de contralor para cumplir sus funciones cuando la información se transnacionaliza. El Entrevistado 8 mencionó conocer la existencia de casos de tercerización aplicada por compañías argentinas cuyos servidores se encontraban en el exterior. Esto en más de una ocasión representaba un obstáculo para la IGJ, por la falta de disponibilidad de la información financiera de las compañías requeridas para control. Según manifestó, en algunos casos se utilizaría la tercerización como excusa para no brindar la información al regulador.

En consecuencia, el organismo emitió normativa que obliga a indicar donde se encuentran los servidores y la información, a fin de cumplir con sus tareas de revisión. La norma establece que

[20] En la Ley 19.950 actualizada, la cita hace referencia a artículos del anterior Código de Comercio (no al Código Civil y Comercial de la Nación), en la medida en que no han sido modificados en el texto publicado de la norma.

toda la información se debe encontrar en la sede legal de la firma a disposición del regulador; y en caso contrario, que se indique su ubicación física para poder acceder (ubicación de los servidores). Si el servidor está localizado en *extraña jurisdicción*, se debe garantizar el acceso a la información. Este tipo de jurisdicciones son, por ejemplo, países de alto riesgo donde los gobiernos pueden aprobar legislación que les permita acceder a todos los datos dentro de sus fronteras (Brender & Markov, 2013) o calificados como países con legislación permisiva.

Según el Entrevistado 3, en una oportunidad le fue solicitado que certifique la existencia de una réplica de la base de datos en la sede social de la compañía. Si bien estos requerimientos no han surgido como consecuencia del uso de la CN, sino de otras alternativas de TI, las disposiciones resultarían igualmente aplicables.

> Tiene lógica, porque de alguna manera lo que está pidiendo el regulador no es que los servidores estén en Argentina; es que toda la información necesaria para el regulador este en Argentina, más allá que el servidor pueda estar en otro lado. (…) Te están obligando a que digas donde tenés la información. (…) Me imagino que en algún momento lo que se va a tratar de llegar es que si la información está tercerizada en algún lugar fuera de la Argentina, que cierto *back up* se encuentre en Argentina. (Entrevistado 8)

La norma que resulta aplicable al respecto se refiere al artículo 328 Inciso 1.f de la Resolución General 7/2015.

> **Registros por ordenadores, medios mecánicos, magnéticos u otros (artículo 61, Ley Nº 19.550).**
> **Artículo 328**.– Para la autorización del empleo de ordenadores, medios mecánicos, magnéticos u otros prevista por el artículo 61 de la Ley Nº 19.550, se debe presentar:
> **1.** Primer testimonio de escritura pública o instrumento privado original con los recaudos del artículo 37, incisos 1 y 2, conteniendo la transcripción de la resolución del órgano de administración de la sociedad, de solicitar la autorización reglamentada en este artículo. La resolución del órgano de administración deberá contener:
> (…) **f.** En caso de tercerización de archivo de documentación física y/o informática, deberá contener la denominación del tercero proveedor del servicio, radicación de los archivos y/o medio de procesamiento, vigencia del contrato y las políticas de seguridad en la información implementadas.

Los Entrevistados 3 y 5 se refirieron en particular a la ubicación de la información en *extrañas jurisdicciones* (por ejemplo, Islas Caimán). Estos son países con regulación muy flexible, en los cuales las restricciones impuestas por el regulador son mayores y con alta posibilidad de no otorgar la autorización. Por el contrario, en caso que se tercerizara a un centro de cómputos de un país considerado seguro (por ejemplo, Estados Unidos) la IGJ lo autorizaría, sujeto al cumplimiento de los requisitos descriptos previamente y al otorgamiento de información respecto a la seguridad lógica que tienen sus equipos.

Otro tema controvertido en entornos de CN se refiere a la *ubicación de los registros contables y la información que le da soporte*. Según el artículo 325 del Código Civil y Comercial de la Nación, los libros indicados en el artículo 322 deben permanecer en el domicilio del titular.

La Resolución General 7/2015 de la IGJ especifica que los registros y libros contables deben permanecer en la sede social inscripta. Sin embargo, 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, el cual no necesariamente se encuentra en el país. Incluso la ubicación de los datos podría modificarse sin conocimiento del usuario de acuerdo a las necesidades y conveniencia del proveedor (Entrevistados 3, 5, 6).

> Hoy por hoy tenemos organismos regulatorios que nos están diciendo que por más que vos tengas la información en la nube, la tenés que tener disponible en un equipo dentro de tu compañía, porque desde el punto de vista legal, la información contable tiene que estar en el país. (Entrevistado 6)

En consecuencia, a la fecha los entes que utilizan este tipo de servicios realizan copias locales de información alojada en la nube, trayéndola al país para cumplir las disposiciones, según fue comentado en el apartado *5.1.3* de esta tesis, como alternativa para superar una barrera para la utilización planteada por la normativa (Entrevistados 3, 6).

De todas formas, el Entrevistado 5 consideró que este tipo de incumplimientos por parte del ente auditado no representa un riesgo de alto impacto. Esto se debe a que frente a una migración de la información a la nube, el problema podría ser la pérdida de la autorización otorgada por el órgano de contralor para llevar los libros en forma electrónica. En el peor de los casos, dicha situación requeriría la ejecución de un conjunto de trámites complejos para recuperarla, solucionándose el problema.

Del análisis previo surge que aun cuando la normativa (Código Civil y Comercial de la Nación y Ley General de Sociedades) no se ha actualizado en relación a este tipo de servicios tercerizados –incluso no solo los basados en computación en la nube– la forma de regular estas situaciones es a través de los requisitos impuestos por los organismos de contralor. Esto en consonancia con lo que expresa Suárez Kimura (2007) respecto del desfasaje temporal entre lo exigido por la normativa y lo que ofrece la tecnología. Según el Entrevistado 3, un aspecto importante a nivel local es que los organismos reguladores hagan un cambio de mentalidad en relación a estas tecnologías y que lo reflejen en la normativa y sus requerimientos.

> Para mí van siempre atrás y la verdad que complican a las empresas a ir para adelante. Todas las compañías, por el volumen de información que generan, quieren llevar sus registros en CD, (…) que es mucho más práctico y ágil. Pero la verdad que la IGJ hoy por hoy está complicando algo que antes era más simple, de ir a pedir una autorización para llevar en CD. O esto que no entienden que las empresas tengan un servidor afuera. Hoy la mayoría de las compañías que tienen su casa matriz en el exterior tienden a que haya un único sistema para todas las compañías del grupo, para que trabajen iguales, y la verdad que no lo entienden. Pero, bueno, yo creo que se van a ir modernizando. (Entrevistado 3)

Existen otros casos particulares de entes que podrían verse restringidos en su posibilidad de uso de la CN, como las empresas públicas, sujetas a control de la CNV con requerimientos

similares a los de la IGJ (Entrevistado 8) y las entidades financieras, sujetas a la normativa del Banco Central de la República Argentina (BCRA) (Entrevistados 4, 5, 6).

Sin pretender profundizar el análisis en este tipo de normas, cabe mencionar que el BCRA ha regulado aspectos vinculados al uso de tecnología por parte de las entidades financieras, si bien no específicamente en relación al uso de la computación en la nube. Los entrevistados mencionaron como relevante la Comunicación A 4609 del BCRA (2006), que establece en su *Sección* 7 - *Delegación de actividades propias de la entidad en terceros* un conjunto de pautas referidas a la tercerización. Indica en su punto 7.1. que "las entidades financieras podrán delegar en terceros actividades vinculadas a la administración y/o procesamiento de datos, sistemas o tecnologías relacionadas" y establece en los puntos sucesivos responsabilidades a cargo de la entidad y del tercero, requisitos para el contrato mediante el cual se formalice la delegación y cuestiones asociadas a la implementación del procesamiento de datos en el proveedor del servicio y el control que debe realizar la entidad financiera.

A través de la Comunicación A4609 y sus actualizaciones, el BCRA determina las medidas a aplicar para poder operar en equipos que no están en la Argentina y en el dominio del banco, siendo estas muy estrictas. Según interpretan los Entrevistados 4 y 6, la norma en principio restringe el uso de servicios en la nube, no permitiéndolo ni para el almacenamiento de información.

> Lo que vos podes tener son empresas o bancos que contratan un tipo *data center*. Pero eso yo no lo tomo como la nube, porque en realidad es un cable que sale del banco y que va hasta el servidor en el centro de cómputos de la empresa proveedora. No es información que anda dando vueltas por Internet. (…) El centro de cómputos es de un tercero, en donde se encuentra un servidor que puede ser propiedad de dicho tercero o del propio banco, pero es el banco el que mantiene el control sobre los datos. (Entrevistado 4)

> Estoy casi seguro que los bancos están obligados a tener todos sus *data centers* en la Argentina, y la nube no sería una solución para ellos. El Banco Central no se los permite; es decir, los *data centers* tienen que estar en la Argentina y tienen que tener determinadas características, que ninguna de esas características es estar en la nube. (Entrevistado 6)

Al respecto, Noceti y Freijo (2015) destacan también la ubicación de los centros de datos de los proveedores fuera de la Argentina como una limitante para la utilización de la CN, debido al riesgo de incumplimiento de la normativa vigente. Estos podrían estar en jurisdicciones que no son consideradas adecuadas desde el punto de vista de protección de los datos para las autoridades argentinas, cuestiones sumamente relevantes en dicha industria por la sensibilidad de la información.

En relación a los demás tipos de normas que podrían ser infringidas, referidas a la *confidencialidad de los datos* (por ejemplo, datos de clientes cargados en la nube) o la *protección de la propiedad intelectual*, el Entrevistado 5 mencionó que como auditor financiero los considera

riesgos cuya evaluación es muy compleja. En principio, son cuestiones posibles, pero cuya probabilidad de ocurrencia es muy difícil de estimar a priori.

> Son eventos para los que es muy difícil de estimar una probabilidad de ocurrencia, buscarle un impacto contable y cuantificarlos hasta que no suceden y se descubren. Riesgos de que sucedan muchas cosas siempre hay, pero hasta que no suceden, a veces no se puede hacer nada más que una advertencia a la gerencia. (Entrevistado 5)

El impacto del riesgo analizado pareciera depender de la sensibilidad de la información afectada. En particular las cuestiones relacionadas a la eventual divulgación de datos personales, sea por negligencia o dolo del proveedor, generan el riesgo de situaciones litigiosas contingentes que deberían afrontar las entidades.

Si se tratara de datos personales, por ejemplo, de clientes o proveedores, el impacto podría ser mínimo, dado que la información en poder del ente auditado en general está disponible en otros sitios (número de CUIT/CUIL, domicilio, CBU, transacciones realizadas con el cliente/proveedor). Sería un riesgo más alto si se tratara por ejemplo de contratos confidenciales firmados con otras empresas.

En caso que sucedan dichos eventos negativos, el profesional indica que corresponde analizar el grado de responsabilidad atribuible al ente auditado frente al incumplimiento de las leyes, revisando por ejemplo el contrato firmado con el proveedor del servicio en la nube. Considera que los riesgos de intromisión por parte de terceros malintencionados suceden tanto en un servidor propio como en uno en la nube, no siendo diferencial de estos servicios. En todo caso se podría discutir si estos servicios son más o menos seguros que los servidores *in-house*, existiendo posiciones encontradas al respecto.

En principio, 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, podría salvar su responsabilidad (Entrevistado 5). De todos modos, se reconoce que en este tipo de conflictos de divulgación de información protegida por normas de confidencialidad, el ente contratante de la nube –en este caso el auditado– seguramente también será responsabilizado.

En consecuencia, indica que los auditores financieros evalúan dichos eventos cuando la infracción ya ha ocurrido, a fin de determinar su potencial efecto contable:

> (…) Si tenemos conocimiento de que se violó alguna de esas normas, lo que vamos a tratar de analizar es cuál es el impacto contable que va a tener esto, solicitado una explicación del abogado o analizando la jurisprudencia. (…) Si vos descubriste algo que se infringió, obviamente vas a tener una precisión sobre esto, verás si realmente la podes cuantificar o si a lo mejor merezca simplemente una nota a los estados financieros. (Entrevistado 5)

La NIA 250 (A. 18) plantea justamente que ante el conocimiento de un incumplimiento (o de indicios sobre el mismo) el auditor deberá procurar comprender la naturaleza del hecho y las circunstancias en las que se produjo, así como cualquier otra información necesaria para poder evaluar el posible efecto sobre los estados financieros.

e) Riesgos contra la seguridad física

Aun cuando estos riesgos pueden ser considerados como no específicos de la nube, deben ser incluidos en el proceso de evaluación tanto por el ente usuario como por el equipo de auditoría, razón por la cual se exponen en la estructura de riesgos propuesta, debiendo analizarse el impacto y probabilidad de cada uno de los factores (Entrevistado 5). Según fue expresado, los auditores cuando solicitan a sus clientes los documentos en los que reflejan las evaluaciones de riesgos realizadas respecto de los servicios tercerizados, corroboran la inclusión de todos los factores de riesgos, para luego verificar el proceso de análisis efectuado por el ente y las valoraciones otorgados a cada uno de ellos.

Por ejemplo, para un riesgo de terremoto como desastre natural en Ciudad Autónoma de Buenos Aires podría considerarse con una probabilidad de ocurrencia baja; sin embargo, el factor ha de ser considerado. En todo caso, aquí debería analizarse según la ubicación geográfica de los servidores del proveedor del servicio –en caso que esta fuera conocida– y las medidas de seguridad que éste hubiera adoptado al respecto.

5.3.3. RESUMEN

En el presente capítulo se presenta un análisis genérico de riesgos de la computación en la nube, a fin de evaluar su potencial impacto en una auditoría financiera. Se completa la RBS presentada en el marco teórico, agregando sub-categorías que surgieron del análisis de las entrevistas, ya que se considera una herramienta útil para la evaluación de riesgos de una auditoría en contexto de CN.

A priori, estos encargos realizados en contextos de CN no necesariamente son calificados como más riesgosos por los auditores entrevistados, sino que ello depende en principio del proveedor contratado, de los recaudos del cliente al momento de la contratación y de los controles adoptados.

En primer lugar, se analizan los *riesgos derivados del proceso de implementación de la nube.* Pareciera que una deficiente planificación del uso de la nube es un riesgo de baja probabilidad de ocurrencia, al menos en lo que respecta a grandes empresas, que son cautas al momento de implementar nuevas tecnologías. Sin embargo, su ocurrencia puede tener un alto impacto en la auditoría financiera, pudiendo afectar el enfoque a aplicar, dada la escasa confianza que podrían depositar los auditores sobre los nuevos sistemas y los controles internos implementados en ellos. Respecto del uso no autorizado de la nube, es un riesgo de baja probabilidad. Para la prevención de este tipo de riesgos se recomienda la participación real de los auditores (de sistemas o financieros) en el proceso de evaluación e implementación del nuevo sistema, 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.

Los *riesgos propios de la tercerización* no representan situaciones específicas de la nube. La pérdida de gobernabilidad y la falta de transparencia son los factores de riesgo indicados como relevantes para la auditoría financiera, en la medida en que el proveedor es quien proporciona la información sobre el funcionamiento y diseño del control interno.

Los *riesgos técnicos* fueron clasificados en dos subcategorías: *a) los riesgos de disponibilidad de la información*, que poseen alta probabilidad de ocurrencia y alto impacto, y que deben ser gestionados tanto por el proveedor de la nube como por el ente usuario, considerando las limitaciones de infraestructura de telecomunicaciones existentes en el país; *b) los riesgos de seguridad y accesos no autorizados* a los sistemas y la información, que dependen más de las malas intenciones de los sujetos involucrados que de fallas en la tecnología implementada, y requieren una permanente evaluación de las medidas de seguridad adoptadas. Ambos poseen alto impacto en la auditoría financiera, dado que su ocurrencia puede implicar la falta de disponibilidad de la información, así como la disminución del nivel de confianza que el auditor puede depositar en ella.

Los *riesgos legales* fueron considerados relevantes para la auditoría de estados financieros; sin embargo, no son totalmente controlables por el ente auditado (son riesgos inherentes), dado que la normativa está vigente en el contexto en el cual se desempeña y la industria a la que pertenece. Nuevamente, se propuso una separación en dos sub-categorías: *a) riesgos del marco jurídico según la ubicación de la información*, y *b) riesgos de cumplimiento.*

Los primeros estarán determinados por la ubicación del proveedor del servicio, pero parecieran afectar más al usuario que al auditor. Los segundos son importantes para la auditoría de estados financieros; en particular respecto del cumplimiento de leyes y normas referidas a los sistemas de información. También se deben considerar las obligaciones impuestas por los órganos de contralor de cada jurisdicción. Esto es así, dado que en las regulaciones suelen establecerse requisitos más específicos respecto de la forma de llevar los registros comerciales y las autorizaciones para el uso de medios electrónicos, que determinan la posibilidad de utilizar alternativas como la de la CN. Los auditores deben verificar el cumplimiento de todas las leyes y normas para poder afirmar que la información sujeta a auditoría surge de libros llevados en legal forma. Asimismo se creen relevantes ciertos riesgos de incumplimiento de normas vinculadas a la divulgación de información protegida; en estos casos, la probabilidad e impacto serían de difícil evaluación a priori, de modo que sólo podrían ser analizados luego de la ocurrencia de los hechos con eventuales consecuencias patrimoniales negativas para el ente que debieran ser reflejadas en los estados financieros.

Los *riesgos de seguridad física* no fueron considerados distintos en el caso de la CN. De todas formas es necesario incluirlos en la evaluación de riesgos, teniendo en cuenta la ubicación, infraestructura y medidas de seguridad del proveedor del servicio y del auditado.

Finalmente, se elaboró la RBS presentada en el Cuadro 24, herramienta propuesta como disparador para la evaluación de riesgos en la planificación de una auditoría de estados financieros

en contextos de computación en la nube. En particular, se considera que podría resultar de utilidad para los auditores dado que presenta un resumen de factores a considerar, elaborada con el aporte de la experiencia de los profesionales de grandes estudios, con mayores conocimientos de diferentes entornos de TI, y el apoyo de la opinión de especialistas del área de sistemas. Posteriormente, cada profesional debería ampliar esta estructura determinando la probabilidad e impacto de cada factor en el ente auditado para luego elaborar una matriz de riesgos. La misma, junto con la evaluación del funcionamiento de los controles, será de utilidad para en forma conjunta definir el enfoque de auditoría.

Cuadro 24 - RBS para la auditoría financiera en entornos de CN

NIVEL 0	NIVEL 1 - FUENTES DE RIESGOS	NIVEL 2 - SUBCATEGORÍAS	NIVEL 3 - FACTORES DE RIESGO
RIESGOS DE UNA AUDITORÍA EN CONTEXTOS DE CN	**RIESGOS DERIVADOS DEL PROCESO DE IMPLEMENTACIÓN**	Falta de planificación en el proceso de implementación (*Due Dilligence* insuficiente)	
		Actividad no autorizada en la nube	
		Falla en la adecuación de la estructura organizacional	
	RIESGOS DERIVADOS DE LA TERCERIZACIÓN	Pérdida de gobernabilidad por parte del usuario	
		Viabilidad del proveedor	
		Vinculación al proveedor (*Lock in*)	
		Falta de transparencia	
		Incumplimiento de requisitos de certificaciones	
		Reputación compartida	
	RIESGOS TÉCNICOS	RIESGOS DE CONTINUIDAD	Insuficiencia de recursos (sub-aprovisionamiento)
			Fallas de la conexión a Internet
		RIESGOS DE SEGURIDAD	Fallas de los mecanismos de aislamiento de la información en equipos virtualizados compartidos
			Empleado malicioso
			Fuga/Interceptación de datos en tránsito
			Eliminación de datos insegura o no efectiva
			Acceso a través de navegadores de Internet conocidos
			Problemas de gestión de la identidad y claves de encriptado
	RIESGOS LEGALES	RIESGOS DEL MARCO JURIDICO SEGÚN LA UBICACIÓN	Cambio de jurisdicción
			Determinación de la autoridad competente en caso de conflicto
			Confiscación judicial
		RIESGOS DE INCUMPLIMIENTO	Requisitos de los sistemas de información
			Revelación de cuestiones sobre controles internos
			Protección de datos y confidencialidad
			Protección de la propiedad intelectual
	RIESGOS CONTRA LA SEGURIDAD FÍSICA	Acceso físico no autorizado a instalaciones y edificios	
		Desastres naturales	

LECTURA: *Rojo: riesgos altos o relevantes para la auditoría financiera. Verde: riesgos bajos o de menor importancia para la auditoría financiera. Azul: categorías emergentes.*

Fuente: Elaboración propia.

5.4. EVALUACIÓN DEL SISTEMA DE CONTROL INTERNO EN CN

El presente apartado pretende dar cumplimiento al siguiente objetivo específico planteado para esta tesis:

Determinar las particularidades de la evaluación del sistema de control interno en entornos de CN para la planificación de la auditoría financiera.

Del análisis de los datos obtenidos en las entrevistas surge que los profesionales se refirieron principalmente a tres cuestiones:

a) la vinculación que el profesional de la auditoría contable debe tener con los auditores de sistemas en esta etapa en particular;

b) los controles internos que les interesa conocer y evaluar, los cuales en algunos casos fueron descriptos inicialmente al ser consultados respecto de las incidencias de la CN sobre el conocimiento del cliente y su entorno, pero que por la importancia del tema se decidió exponerlos por separado en este apartado específico;

c) los procedimientos que podrán ser aplicados o no en un entorno de computación en la nube para lograr una adecuada comprensión y evaluación de los CI, teniendo en cuenta sus particularidades.

Es así que se ha decidido exponer los resultados respetando estas tres categorías de temas que han surgido de las entrevistas y que se relacionan a los aspectos mencionados en el referencial teórico.

5.4.1. USO DEL TRABAJO DE LOS AUDITORES DE TI

En primer lugar, resulta fundamental distinguir la participación que los auditores financieros y los de sistemas tienen en esta etapa, vinculado a lo que se describió en el apartado de conocimiento del cliente.

En principio, los auditores financieros (Entrevistados 5, 7, 8) al conocer la existencia de contextos de TI con influencia significativa en la elaboración de la información contable del ente, convocan dentro del equipo de auditoría a los especialistas en sistemas del estudio. El objetivo principal es contar con su colaboración para efectuar la evaluación de riesgos y de controles internos vinculados, en todo lo relacionado a los sistemas informáticos.

Los requerimientos para la revisión de los controles sobre los sistemas de TI que afectan la contabilidad, y en definitiva los estados auditados, deben ser establecidos por los auditores financieros, quienes son los responsables del encargo (Entrevistado 8).

Los auditores informáticos efectúan un reporte a los auditores financieros sobre su propia evaluación del sistema de control interno del auditado, para que estos últimos definan el enfoque de auditoría a aplicar (Entrevistado 5). Los reportes de los auditores de TI pueden comprender las siguientes situaciones:

a) que todo el sistema de control interno esté funcionando correctamente;

b) que existan debilidades de CI que debieran ser mejoradas, pero funcionen otras actividades de control que las compensan;

c) que existan debilidades que no están siendo mitigadas por otros controles, puestas a consideración de los auditores contables.

En la evaluación de las debilidades de los controles los auditores financieros deben identificar aquellos que resultan relevantes para su trabajo, en la medida en que afectan a información que impactará en los estados contables (NIA 315 (Revisada)), principalmente considerando que los reportes de las auditorías de sistemas en muchos casos son demasiado amplios, abarcando muchos controles no significativos en este sentido (Minguillon, 2010).

Por ejemplo, en el caso c), si bien los auditores de sistemas informan las debilidades detectadas como una fuente de riesgo, los auditores contables analizarán si la información contable afectada por las mismas es significativa y si puede ser evaluada mediante otros procedimientos de modo de satisfacerse de su validez (Entrevistado 5).

Si los auditores financieros consideran que pueden depositar confianza en los controles, es posible que decidan aplicar un enfoque de cumplimiento. De lo contrario, en la medida en que ellos puedan validar la información mediante otros procedimientos, aplicarán un enfoque sustantivo, y las debilidades de control detectadas por los auditores de TI serán informadas a la gerencia en la carta con recomendaciones para su eventual solución (Entrevistado 5).

Esta situación denota, tal como se discutirá más adelante, que el auditor financiero, aun cuando delega parte de la evaluación de riesgos y controles en el auditor de sistemas, deberá tener ciertos conocimientos de la TI aplicada por los usuarios a fin de poder interpretar los resultados en los reportes de sus colaboradores y tomar las decisiones sobre su trabajo.

5.4.2. CONTROLES INTERNOS RELEVANTES PARA EL AUDITOR FINANCIERO EN UN AMBIENTE DE CN

La evaluación de CI en la nube incluye –según se indicó en el marco teórico y fue mencionado por los entrevistados– los dos tipos de controles que deberán ser comprendidos y evaluados en cualquier ambiente de TI: los controles generales y los de las aplicaciones.

> El requerimiento de evaluación que hacen los auditores financieros a los de sistemas generalmente es una revisión del entorno de IT, que es lo que llamamos controles generales, y después según los sistemas que tengan para cada uno de los procesos, una mayor revisión de los controles de aplicaciones. (Entrevistado 8)

La evaluación de los *controles generales* es fundamental para los auditores contables, en la medida en que les brindan seguridad acerca de si el ambiente de control es adecuado y si pueden confiar a priori en las salidas del sistema informático (Entrevistados 7, 5, 8). Esta evaluación en los grandes estudios la encargan a los auditores de TI y comprende: los sistemas utilizados; el soporte

técnico; la ubicación de los servidores; las normas de seguridad implementadas; los usuarios, uso de contraseñas y niveles de acceso establecidos; la segregación de funciones; entre otros.

La evaluación de los *controles de las aplicaciones* se realiza sobre ciertos procesos y componentes relevantes para la auditoría financiera, determinados de acuerdo a la evaluación de la significatividad de las afirmaciones contenidas en los estados financieros. En general se refiere a aserciones respecto de las cuales resultaría muy costoso tener una certeza de auditoría utilizando únicamente pruebas sustantivas o globales (Entrevistados 5, 7, 8).

Esta distinción entre controles generales y de las aplicaciones fue mencionada por varios entrevistados al referirse a la etapa de evaluación del control interno. Sin embargo, del análisis de los controles relevantes en la nube resulta que el interés se refiere principalmente a controles generales, en la medida en que la nube modifica el entorno y la infraestructura de la TI.

Las aplicaciones utilizadas por el cliente pueden ser similares, independientemente de que se encuentren en servidores locales o en la nube. Su revisión dependerá del servicio que se estuviera utilizando; si el mismo es conocido y enlatado, como SAP en la nube, la evaluación es similar a la que se haría con un SAP *on-premisse*; si fuera un sistema a medida, se haría una revisión más exhaustiva por el desconocimiento que los auditores tuvieran del sistema. De todos modos, pareciera que los requerimientos serían los mismos si las aplicaciones están en la nube o en un sistema propio; la diferencia, como se verá más adelante, será la posibilidad de que los auditores de sistemas realicen la evaluación de dichos controles en las aplicaciones cuando se encuentran alojadas en la nube, administrada por el tercero (Entrevistado 8).

La exposición de los controles relevantes se realizara en dos categorías: A - Controles internos del proveedor del servicio de CN; B - Controles implementados en relación a la CN por parte del usuario auditado; esta distinción fue propuesta por los propios informantes.

A. Controles internos del proveedor del servicio de CN

En el supuesto de la CN, como en el resto de los modelos de externalización de TI, existe una delegación de actividades de control en el proveedor del servicio. El nivel de tercerización varía de acuerdo al modelo de nube adoptado, según se expuso anteriormente.

En consecuencia, los 8 entrevistados se vieron ampliamente interesados en conocer desde el inicio de la auditoría *aspectos del sistema de control interno del proveedor del servicio* con incidencia en el resguardo de la información y las aplicaciones del ente usuario, y que afectan en definitiva la información que luego se verá reflejada en los estados financieros auditados.

Los controles relevantes del proveedor comprenden principalmente *controles generales***,** evaluados en la etapa preliminar de conocimiento, que permiten conocer la seguridad del sistema para definir el nivel de confianza que merece, y en función de eso decidir la aceptación o no del encargo de auditoría contable. En caso de aceptarlo, definir posteriormente –en la etapa de planificación– el enfoque de auditoría a aplicar (Entrevistado 8). Estos controles dan el marco de

seguridad del sistema de TI utilizado por el ente, por eso su evaluación se realiza con anterioridad a la de los controles de las aplicaciones. Desde un principio, si este conjunto de controles no funciona correctamente, el auditor financiero desistirá en la aplicación de un enfoque de confianza en controles del entorno en la nube en el que se encuentra alojada la información sujeta a auditoría. De ahí la importancia de su análisis y comprensión por parte de estos profesionales, aun cuando la evaluación en la práctica la realicen los auditores de sistemas.

El Entrevistado 6 detalló cuatro actividades de controles generales ("torres de servicios") que analizan cuando inician una revisión de sistemas, independientemente de donde se encuentren *hosteadas* las aplicaciones (en la nube, en una casa matriz del exterior, en un *datacenter* de un tercero o en el mismo *datacenter* de la compañía) y de la aplicación a evaluar (correo, aplicación financiera, *file server*, etc). Éstas comprenden la revisión de la seguridad física de las aplicaciones, los procedimientos para su modificación, el ABM[21] de usuarios y el ambiente de control. Todas ellas serán descriptas a continuación.

Las principales preocupaciones en relación a los controles implementados por el proveedor se refirieron a la *seguridad de la información contable*, que comprende la confidencialidad, la integridad y la disponibilidad de la información.

- La *confidencialidad* de la información se refiere a que ésta solo sea accedida por las personas que están autorizadas a hacerlo. La principal dificultad para la auditoría y para el proveedor está en probar que la información está protegida contra el acceso por terceros no autorizados porque –independientemente de la actividad del usuario y de la sensibilidad de los datos– su información le pertenece (Entrevistado 1).

Los requisitos y medidas para lograr la confidencialidad de la información deben ser establecidos en el contrato de prestación del servicio. Sin embargo, al entregar la información propia a un tercero para que la almacene y/o administre, no existe certeza de los requerimientos se cumplan y que la confidencialidad sea garantizada o no se haga un mal uso de la información; ello depende en gran medida de la ética y reputación del proveedor del servicio en la nube, siendo que él mismo estará interesado en evitar este tipo de incidentes para garantizar su futuro en el negocio. Desafortunadamente, es posible que el incumplimiento en este aspecto sea conocido recién cuando ocurra un incidente en el que la confidencialidad sea vulnerada (Entrevistado 5).

A pesar de estas apreciaciones, existe un conjunto de medidas de control a aplicar a fin de procurar preservar la confidencialidad de la información, que aportan además a otros objetivos.

- La *integridad* se refiere a la protección de la información contra la modificación no autorizada, siendo este un aspecto sumamente relevante para la auditoría (Entrevistados 1, 7). Incluso el Entrevistado 7 considera que desde el punto de vista de la auditoría de estados financieros es más importante el riesgo de que la información sea modificada, y no tanto que sea

[21] Alta, baja y modificación de usuarios.

vista por terceros. En consecuencia, deben preverse y auditarse las medidas de control implementadas para minimizar este riesgo, si bien nuevamente puede ser complejo para el proveedor demostrar y para el auditor evaluar la imposibilidad de edición de los datos (Entrevistado 1).

- Finalmente, se menciona la importancia de la *disponibilidad de la información*, esto es, que se encuentre a disposición de quien la necesite en el momento en que se la requiera; deberá ser garantizada también a través de diversas medidas de control.

Como se puede apreciar, estos controles de seguridad que han sido marcados como importantes por los entrevistados comprenden medidas preventivas en relación a muchos de los riesgos que fueron identificados y valorados como relevantes en el apartado anterior (riesgos técnicos de continuidad o disponibilidad y vinculados al acceso de terceros no autorizados; riesgos de incumplimiento de normas vinculadas a la divulgación de información protegida con eventuales consecuencias patrimoniales negativas para el ente).

Cabe mencionar que este aspecto ha sido tratado con mayor profundidad por los auditores de sistemas, quienes realizan la evaluación de estas cuestiones e informan sus conclusiones a los auditores contables, tal como se indicó previamente. En todo caso se incluyen las apreciaciones de estos últimos en relación a la importancia que pudieran tener las fallas en los controles sobre la auditoría financiera.

A continuación, se describen las categorías de controles de la CN indicadas como importantes por los auditores.

a) Ambiente de control

En relación al ambiente de control, se destaca la necesidad de conocer si el proveedor hubiera utilizado un estándar en particular para la aplicación de las mejores prácticas de control interno. Conociéndolo es posible entender como han construido su ambiente de control y auditarlo, considerando las limitaciones que serán expuestas más adelante para la evaluación del sistema de control en su conjunto.

> (…) interesa entender cuál es el ambiente de control que ellos definieron sobre ese entorno [de TI]. Ver si ellos siguieron un estándar determinado, si sus políticas y procedimientos están alineados con mejores prácticas de control interno, establecida en marcos de referencia reconocido como ITIL, COSO o COBIT, para que conociendo ese *framework*, poder recorrerlo, es decir, hacer una especie de *walk through* de este esquema de control que ellos implementaron, y asegurarme que es lo que ellos me están ofreciendo como un servicio de seguridad en un entorno de control. (Entrevistado 6)

b) Control de Acceso. Gestión de usuarios y contraseñas

Este conjunto de controles es importante para la gestión del riesgo de modificación no autorizada de los sistemas y la información, relevante para la auditoría financiera. Incluyen las

medidas de control de acceso, por ejemplo, a través de contraseñas, así como las de gestión de usuarios.

> Porque si esto está afuera [tercerizado] (…) evaluamos la seguridad de la base de datos o el servidor. Por ejemplo, ¿qué políticas de contraseña tiene? ¿Cuáles son los usuarios que están accediendo? Después todo lo que sea referido a gestión de usuarios. Es algo muy importante. Porque no es un sistema que yo tengo en mi equipo. Sino es un sistema que yo tengo en la nube y tengo que ver como es el proceso ABM de usuarios y todos los requerimientos que tengo, como hago para asignar o des-asignar accesos a los distintos módulos. (Entrevistado 4)

Las actividades de control sobre usuarios y contraseñas habitualmente son consideradas por los auditores de sistemas y reportadas, en caso de fallas, a los auditores contables. Comprenden, en primer lugar, la *autenticación de la identidad* de quien pretende tener acceso a la nube (asegurarse que los usuarios son quienes dicen ser) (Hunton et al., 2004). Los niveles de autenticación varían de acuerdo a la confidencialidad y sensibilidad de la información protegida. Ello debe ser considerado previamente por la organización a efectos de determinar cuáles serán sus requerimientos al proveedor en relación a esta medida de seguridad (en los casos de contratos no negociables o de adhesión, deberá evaluarse en qué medida el proveedor del servicio cumple con las expectativas y en caso contrario, o si no pudiera acordarse un nivel de seguridad mayor, desistir de la contratación).

Estos controles, al prevenir el acceso de terceros no autorizados, pueden brindar tranquilidad al auditor –en caso de poder corroborar que funcionen correctamente – acerca de la inexistencia de ingresos no autorizados que tuvieran como consecuencia posibles fraudes cometidos sobre la información

A su vez se incluye la *gestión de usuarios* del personal del ente auditado (Entrevistado 8), que incluye sus altas, bajas y modificaciones y los permisos que se les otorgan para la ejecución de tareas, según las autorizaciones dadas a cada uno, controlando el ingreso y utilización de los recursos informáticos, las aplicaciones y la información. Su análisis permite controlar las actividades desarrolladas respecto de los datos e información, entre ellas: acceso (visualizar los datos, crearlos, copiarlos, transferir archivos, diseminarlos y otras formas de intercambio), procesamiento (realización de operaciones sobre los datos, sea actualizándolos, usándolos en el procesamiento de transacciones) y almacenamiento (retención de los datos en un archivo, base de datos, etc.) (CSA, 2011a:54).

La evaluación de este aspecto es importante para los auditores a fin de obtener evidencia de que nadie sin los permisos adecuados haya intervenido en los datos (Entrevistado 8). A través de informes de accesos y actividades realizadas por los usuarios el auditor puede verificar si cada persona involucrada realiza únicamente las actividades y accede solo a los recursos que le son autorizados, evidenciándose que no se hubieran generado modificaciones no autorizadas en los registros de información contable, cumpliéndose además el principio de separación de funciones.

Ello requiere que el sistema mantenga pistas de auditoría almacenadas en la nube, lo cual resulta una complicación para el proveedor dado el volumen de información a mantener. Algunas evidencias de los cambios podrían ser analizadas a partir de los datos almacenados en la PC del usuario que hubiera generado las modificaciones, pero ello implicaría tener acceso a todos los dispositivos utilizados por los miembros de la organización para la modificación de la información almacenada (computadoras del trabajo y de los hogares, celulares, *tablets*, etc.) (Taylor et al., 2011).

En la nube esto tiene especial importancia, dado que la gestión de usuarios muchas veces no estará a cargo de los responsables de TI del ente, sino que será realizada por el proveedor del servicio, que será quien habilite usuarios, gestione contraseñas, les otorgue los permisos, etc. Es por ello que evaluar las medidas de control adoptadas por el proveedor resulta fundamental, desde las perspectivas de los auditores de TI.

En consecuencia, sería relevante identificar aquellos empleados del proveedor que administran los permisos a usuarios sobre las aplicaciones y los que tienen permisos especiales como administradores de seguridad o administradores de bases de datos dentro de la prestación del servicio, dado que dichas funciones les otorgan un amplio acceso a la información del auditado (Entrevistado 6). La revisión de estos controles podría relacionarse al riesgo de empleado malicioso en el proveedor (que intencionalmente modificara, dañara o extrajera la información del ente usuario, o que sin malicia produjera algunas de estas irregularidades).

De acuerdo a la experiencia de los auditores, suelen existir debilidades en este tipo de controles, como por ejemplo: existencia de usuarios genéricos (una persona con habilitación para ejecutar actividades diversas), usuarios vigentes de personas que ya no pertenecen al ente, contraseñas compartidas o que no son lo suficientemente seguras (Entrevistado 5). Todas ellas son de especial interés para los auditores de sistemas, y seguramente su existencia será reportada a los auditores financieros. Luego, ellos deben analizar la gravedad de estas debilidades y el verdadero impacto que tiene sobre la información financiera. Seguramente ante estas situaciones no se pueda confiar en los controles; por ejemplo, la existencia de un usuario general hace que los riesgos se expandan a todas las cuentas.

Según el Entrevistado 5, en la medida en que dichas situaciones puedan ser compensadas mediante otros procedimientos de auditoría para la validación de saldos y transacciones potencialmente afectados, pueden salvarse a los efectos de la auditoría de estados contables.

> Algo que pasa muy seguido es que no estén bien definidos quienes son los usuarios que pueden hacer asientos contables, o que haya usuarios generales. Ellos [los auditores de sistemas] lo informan. Son riesgos sinceramente, porque que cualquiera pueda meter un asiento contable no está bueno, pero son cosas que pasan. (…) Después nosotros [los auditores financieros] hacemos un análisis de los asientos manuales y nos fijamos que determinada persona no haya hecho un asiento. Esos son unos de los primeros controles que hacemos, siempre y cuando se pueda. (…) En definitiva lo que se audita es el saldo al final, con lo cual si en el medio hubo alguien que metió cualquier cosa y está dentro del

> alcance del trabajo de auditoría, en algún momento va a surgir si es que genera un error significativo. (Entrevistado 5)

c) Seguridad en la transferencia de la información

En la nube existe una transferencia de la información entre partes, a través de una red que en general es Internet. Esta situación genera una exposición a los ya descriptos riesgos técnicos, vinculados tanto a la disponibilidad de las telecomunicaciones (como las fallas en la conexión de Internet) como a la seguridad en la transmisión de los datos (fuga/interceptación de datos en tránsito). Estos tienen consecuencias sobre la confidencialidad, integridad y disponibilidad de la información.

> La nube está basada en Internet. Internet es algo maravilloso, es como nos conectamos ahora para todo, pero no es una red que nació siendo segura. Es una red que nació con fines didácticos, universitarios. Poco a poco se le están poniendo cada vez más formas de asegurar, pero lo que es TCP/IP no es de por sí un protocolo hiperseguro, pero es un protocolo de comunicación muy económico. (Entrevistado 1)

Por lo dicho, es importante la protección de la información que se traslada desde el cliente hacia el proveedor del servicio en la nube a través de la red –y viceversa– mediante la aplicación de mecanismos tecnológicos y políticas de seguridad lógica (Entrevistados 1, 6). Las medidas a ser adoptadas en general están a cargo del usuario y del proveedor de transmisión de la información que hubiera contratado.

Entre ellas se menciona el *encriptado* de los datos sensibles, previo al movimiento a la red. Consiste en un conjunto de algoritmos utilizados para convertir un texto en un código o un formato de texto ilegible, proveyendo privacidad durante la transmisión. Para descifrar el texto, el destinatario debe utilizar las claves correspondientes (Lakhtaria, 2011), las cuales deben ser cuidadosamente administradas (CSA, 2011a). Será necesario indagar acerca de las medidas utilizadas y verificar su correcto funcionamiento.

d) Redundancia de almacenamiento y fraccionamiento de la información

Estas medidas de control aportan a las restricciones de acceso por parte de terceros a la información del ente auditado.

Permiten que los datos estén fraccionados para su correcta conservación, y evitar la pérdida de la información íntegra –los datos no están todos en una misma base de datos, en un mismo servidor y no viajan todos juntos. Si ocurre un incidente, éste afecta solo a una parte de los datos, y quien los recupera no accede a información legible o entendible (Entrevistado 1).

La dispersión de los datos, basada en la fragmentación de un archivo en una determinada cantidad de componentes, los cuales son firmados y distribuidos en diversos servidores, implica que, para poder reconstruir el archivo, se debe acceder a una cantidad arbitraria de fragmentos. Si se lo combina con el encriptado, quien desee acceder a los datos sin autorización no solo debería

reconstruir el archivo, sino que una vez que lo hubiera logrado debería decodificar el mecanismo de encriptado utilizado (CSA, 2011a: 52).

e) Aislamiento de la información

Los terceros prestadores del servicio deben proveer un nivel de seguridad de acceso y medidas de custodia de la información al menos similar al que la compañía genera internamente. En particular, estas medidas de seguridad colaboran con las garantías de confidencialidad de la información (Entrevistado 6).

Los métodos de aislamiento de los datos de los diferentes usuarios son una medida de seguridad necesaria para la preservación de la información en la nube, de modo cada uno pueda acceder solamente a sus datos y aplicaciones. Ello se debe a la particularidad de los recursos computacionales de la nube, que son compartidos por varios usuarios que alojan la información en un único servidor físico.

Estas medidas debieran asegurar que cuando el proveedor del servicio acceda a información de un usuario, no comprometa la privacidad y seguridad de los datos y aplicaciones de la organización auditada y viceversa, previniéndose el riesgo de modificación, pérdida o daño en los archivos que contienen la información contable auditada.

Tal como se expresó en la evaluación de riesgos, la probabilidad de que un usuario pudiera acceder a información de otro en forma accidental es considerada casi nula. A la fecha, existen medidas de seguridad desarrolladas por los proveedores y sometidas a mejoras continuas, de manera tal de evitar estos riesgos para la preservación del negocio.

Aun teniendo en cuenta lo indicado en los párrafos anteriores, se reconoce que el riesgo de acceso por un *hacker* (tercero que estuviera intentando vulnerar intencionalmente las medidas de seguridad, aprovechándose de la existencia de recursos compartidos) existe, pero no es mayor al riesgo que existe en el caso de uso de servidores locales (Entrevistado 6).

De igual manera, cuando se lleva adelante el proceso de auditoría, deben tomarse los recaudos necesarios para realizar las evaluaciones de controles y la obtención de datos vinculados únicamente al cliente auditado, procurando no comprometer los intereses de otros clientes del proveedor de la nube.

f) Procedimientos para la modificación de las aplicaciones

Dentro del conjunto de controles generales se deben considerar los procedimientos definidos para la modificación de las aplicaciones (Entrevistado 3), esto es, la definición de quienes son las personas autorizadas para introducir cambios, los pasos a seguir y la conservación de evidencias de los cambios realizados (Entrevistado 6).

Estos controles cobran fundamental importancia cuando el ente auditado hubiera contratado servicios de ERP o similares –con incidencia en la elaboración de la información contable– de tipo

SAAS, en los que las modificaciones o actualizaciones de los programas están a cargo del proveedor del servicio, quien podría realizarlas incluso unilateralmente sin aviso previo al cliente. En cambio, si el usuario hubiera contratado un servicio del tipo IAAS e implantado sus propias aplicaciones, muchos de estos controles estarán a su cargo.

g) Interfaces entre sistemas

En muchos casos los reportes entregados por los auditores de sistemas mencionan debilidades del sistema de control interno vinculadas a las interfaces entre sistemas, las cuales pueden ser relevantes en un ambiente de CN para la auditoría financiera (Entrevistados 5, 7, 8).

Este tipo de controles resultan fundamentales si el ente auditado no utiliza sistemas integrados de ERP en la nube, sino que los aplica solo para determinados procesos que generan información (contenida en reportes emitidos por el sistema) que luego debe ser cargada en la contabilidad.

Por un lado, la configuración de interfaces automáticas entre sistemas locales y los montados en la nube es compleja (Entrevistado 2).

Por el otro, puede ocurrir que las interfaces no sean automáticas (por no estar integrados los sistemas, por ejemplo, de ventas o liquidación de sueldos y el de contabilidad), sino que la información deba ser ingresada en forma manual. Esto conlleva un alto riesgo de error humano, así como de modificación intencional de la información. En consecuencia, si las interfaces no existen o no funcionan correctamente, se requiere una revisión manual por parte de los auditores financieros respecto de la congruencia de la información entre uno y otro sistema (Entrevistado 5).

Al mismo tiempo, si las aplicaciones de la nube se encuentran integradas, se deberá verificar que las interfaces funcionen de manera adecuada, para garantizar exactitud e integridad de la información contable.

h) Seguridad física

La seguridad física surgió en las entrevistas como un aspecto que necesita ser evaluado por los auditores, aun cuando no representa un riesgo especifico de la CN. Se refiere no solo a las medidas que limitan el acceso físico de personas no autorizadas a los equipos (acceso restringido, entradas de teclado numérico, sistemas de entradas con credenciales, cámaras y personal de seguridad, huellas digitales, escaneo de retinas), sino también a las condiciones medioambientales para la preservación de su correcto funcionamiento (niveles de frío, humedad, ventilación, protección contra accidentes naturales de los equipos).

Este es un control evaluado y reportado en forma habitual por los auditores de sistemas a los financieros (Entrevistado 5); su evaluación requiere revisar dónde están los servidores, quiénes los tienen, quiénes los resguardan (Entrevistado 6). En la nube, dicho control esta fundamentalmente a cargo del prestador del servicio (o del proveedor contratado por él, quien en definitiva tiene

posesión del servidor físico sobre el cual está montada la nube). Su revisión resulta compleja, en la medida en que el acceso a las instalaciones del proveedor para verificar las condiciones de seguridad adoptadas suele estar restringido, según fue expresado:

> (…) Cuando tenés el *data center* en un perímetro controlado, sabes quienes son las personas que pueden acceder de manera física y que de alguna manera pueden tomar el control de esos equipos. Entones, la seguridad física es importante. Al no saber dónde están físicamente estos equipos en la nube, tenemos un primer interrogante de tratar de entender cómo asegurar ese acceso, independientemente de la aplicación que este *hosteada* allí. (Entrevistado 6)

La imposibilidad de acceso a las instalaciones del prestador del servicio en la nube puede darse ya sea por el desconocimiento de la localización exacta de la información del cliente en los servidores del proveedor, o por la restricción que el propio proveedor pueda imponer al acceso. Ello representa una limitación en el alcance de la tarea de los auditores que deberá ser considerada en este entorno de la nube.

i) Planes de contingencias y recupero de desastres

Los *planes de contingencias* implementados por los prestadores del servicio en la nube –en los que se prevé un método organizado para enfrentar las consecuencias de potenciales incidentes y ataques a la seguridad– es un control relevante para los auditores de sistemas. Estos están vinculados a la disponibilidad de la información.

En principio, este riesgo suele ser gestionado y minimizado a través de la implementación de los planes de contingencias por parte de los proveedores de servicios en la nube (es decir, si bien el riesgo inherente al uso de la CN existe, mediante los controles adecuados el riesgo de control es bajo, y se reduce el nivel de riesgo combinado). Ello resulta de interés para el proveedor, dado que parte de su negocio es brindar la mayor seguridad de disponibilidad al usuario (Entrevistado 1).

Estos planes deben incluir no solo las políticas de *back up* y resguardo de la información del ente, sino también aquellas referidas a la restauración del servicio y la posibilidad de acceso a la información en caso de incidentes, de modo que ésta realmente se encuentre disponible para el usuario luego de una eventualidad (Entrevistado 6).

> Ellos te pueden decir "yo la información la tengo en cintas o la tengo en discos", pero yo lo que necesito es la disponibilidad de esas cintas en un tiempo determinado. Ahí es dónde empieza a funcionar el concepto de *bussiness continuity plan*: ¿de qué manera yo puedo convivir con una falta de servicio de mi proveedor en la nube, cuánto tiempo puedo estar sin servicio? (Entrevistado 6)

Dentro del conjunto de controles generales relevantes, fue mencionado el conocimiento de las políticas de *back up* implementadas (Entrevistado 4). Si bien el proveedor de la CN ofrece el servicio de almacenamiento, frente a la contingencia de una pérdida del servicio o de la información, se debe prever un procedimiento para garantizar la continuidad del negocio y la disponibilidad de los datos allí almacenados, en particular considerando que son el respaldo de la

información contenida en los estados financieros y que existen ciertas obligaciones en relación con su conservación.

Estas políticas deben considerar, siempre que fuera posible, las necesidades del usuario del servicio. Las recomendaciones sobre implementación de la nube indican que es fundamental la coordinación para la elaboración de los planes en conjunto por usuario y proveedor, para reducir daños, costos y tiempo de recuperación de desastres.

Cuando no fuera posible contemplar las necesidades del cliente, se espera que el potencial usuario haya considerado las situaciones vinculadas a las políticas de *back up* al momento de evaluar la contratación de un prestador, teniendo en cuenta si están en condiciones o no de satisfacer sus requerimientos. El ente usuario debiera evaluar el plan de contingencia del proveedor, las medidas de seguridad adoptadas, sus capacidades de *back up* y recuperación de desastres, y sus previsiones frente a potenciales cortes de servicio, y determinar las medidas adicionales que él mismo debiera adoptar en consecuencia.

El rol del proveedor es fundamental en la recuperación de desastres, dado que es quien efectúa el monitoreo de eventos que facilita la detección oportuna de incidentes. A partir de ello es su responsabilidad analizar los ataques sufridos, recolectar y preservar los datos, remediar los problemas y facilitar la restitución del servicio.

Sin embargo, debe tenerse en consideración que frente a un incidente –sea falla del sistema o ataque de terceros– el proveedor resolverá el conflicto respecto de la nube en general; no es común que ante este tipo de eventos se ocupe de atender los requerimientos de cada cliente en particular. En consecuencia, el plan de contingencias no debe descansar sólo en las acciones del proveedor del servicio, sino que el propio usuario debe prever sus acciones frente a dichos escenarios (COSO, 2012:15).

El plan de contingencias debería contener políticas para la recuperación luego de un incidente –como la utilización de servicios, equipos y localizaciones alternativas– así como la definición de medidas para asegurar la continuidad de las operaciones que afectan funciones esenciales. También se recomienda que en su plan el ente usuario prevea una estrategia de salida para evitar el riesgo de *lock in*, anticipando los pasos para hacer un traspaso a otro proveedor o directamente volver al entorno de TI interno –por ejemplo, contar con el servicio de un segundo proveedor de *cloud* para asegurar que durante un desastre serio o una interrupción prolongada en el servicio primario los datos se mantengan disponibles para continuar inmediatamente las operaciones críticas (López & Albanese, 2013).

Una adecuada implementación del plan de contingencia debiera contemplar la capacitación de todos los miembros involucrados –tanto de la organización usuaria como del proveedor del servicio– de modo que conozcan cómo actuar en caso de un incidente y la importancia de su accionar oportuno para facilitar la solución. Además debieran realizarse comprobaciones periódicas

–por ejemplo, a través de simulacros– para experimentar y demostrar prácticamente la efectiva capacidad de recupero y la vigencia de los planes, o determinar su necesidad de actualización.

Los resultados de dichos simulacros, así como los registros de incidentes que documenten las causas, efectos y soluciones de los eventos ocurridos en un determinado período, pueden brindar evidencias al auditor acerca de la efectividad de los controles. La existencia y funcionamiento de adecuados planes de recuperación y manejo de contingencias es relevante en la medida en que reducen el riesgo de pérdida de información y de interrupción de operaciones que afectan su integridad.

Si hubieran existido a lo largo del período auditado eventos críticos, y el auditor no confiara en el correcto diseño y funcionamiento de los planes, debiera realizar evaluaciones adicionales para asegurarse que no se hubiera dañado o perdido parte de la información sujeta a auditoría.

j) Soporte

Si la utilización de la computación en la nube fuese exigencia impuesta por parte de las casas matrices del exterior, el Entrevistado 4 considera que en esta etapa es importante conocer el soporte que brindan a la filial local para la aplicación y gestión de la CN.

B. Controles del usuario del servicio

Un aspecto interesante a destacar es el interés de los auditores (tanto de sistemas como contables) por conocer y evaluar los controles que los usuarios hubieran implementados sobre el servicio en la nube, más allá de los que hubieran sido aplicados por el prestador (Entrevistados 4, 6).

> (…) ¿Cuáles son los controles que vos como empresa realizas sobre la seguridad y la confidencialidad de la nube? O sea, como la empresa no tiene acceso a la nube, vos tenés que evaluar todos los niveles de control que la empresa tiene sobre ese proceso. (…) Descansamos mucho en controles propios que hacen ellos sobre la empresa de servicios. (Entrevistado 4)

Como en todo modelo de tercerización, los usuarios continúan siendo responsables de la información allí almacenada y/o procesada, debiendo cerciorarse de la protección que otorga el proveedor del servicio. Este es uno de los grandes defectos de la gestión de sistemas de muchas compañías, que por externalizar un proceso creen que dejan de ser responsables (Entrevistados 1, 6). De ahí la importancia de auditar estos aspectos.

Lo dicho complementa las opiniones expuestas en el párrafo *5.2.3.e) Condiciones de la contratación y relación con la empresa de servicios*, donde los auditores resaltan la importancia del monitoreo que el usuario puede hacer sobre el servicio prestado por el proveedor de la nube, no solo en cuanto a la calidad del servicio, sino además respecto de las medidas de seguridad adoptadas.

Entre los controles del usuario que se esperaría encontrar en un caso de utilización de la CN, se incluye la determinación de los parámetros de seguridad a ser implementados por el proveedor y la revisión periódica (por ejemplo, semestral) de los reportes que emita sobre la configuración vigente (Entrevistados 4, 6). Dichos parámetros de seguridad incluyen:

- Gestión de usuarios: aprobación previa a cargo de un responsable en el ente de las altas, bajas y modificación de usuarios y sus permisos sobre las aplicaciones (Entrevistado 6). Reportes periódicos de usuarios y sus accesos, para asegurar que todos pertenezcan a la empresa y tengan los permisos correctos (Entrevistado 4).
- Gestión de claves: definición de la cantidad de intentos fallidos antes del bloqueo de una cuenta; longitudes máximas y mínimas de claves; análisis del historial de claves repetidas (Entrevistado 4).
- Procedimientos de modificación de programas: supervisados, aprobados y autorizados por el cliente usuario (Entrevistado 6).
- Ejecución de procesos y mantenimiento de registros de auditoría: revisión por parte del usuario de *logs* de auditoría para asegurarse que los procesos ejecutados son los que se piden (Entrevistado 4). Revisión de reportes de eventos para verificar el modo en que el proveedor de la nube se encuentra operando el servidor o el ambiente de TI, referidos a caídas del sistema, utilización de súper-usuarios, eventos de modificación de datos en producción o restauración de información en producción, o cualquier otro tipo de operaciones sensibles ejecutadas por el proveedor respecto de las cuales sea importante que brinde trazabilidad (las operaciones de mantenimiento normales y habituales no debieran ser de mucho interés para el usuario y su auditor) (Entrevistado 6).
- *Back up*s: reporte de la herramienta de *back up* para verificar que se estén ejecutando todas las copias de seguridad que se definieron previamente (Entrevistado 4).

En particular la protección de los datos en la nube requiere medidas de control de acceso a la información, que además debieran ser conocidas, evaluadas y monitoreadas por el usuario, principalmente cuando se almacena y/o procesa información sensible o sujeta a regulación especial.

La evaluación que efectúe el ente usuario deberá referirse no solo a la *implementación* de los controles por parte del proveedor, sino que será necesario que verifiquen su correcto *funcionamiento o eficacia operativa* periódicamente (Entrevistado 4). Nuevamente, esto es no solo de utilidad para el auditor, sino para la propia empresa usuaria.

En la contratación del servicio se deberán definir tanto los controles que deben ser aplicados por el proveedor como los reportes que entregará al usuario para hacer el monitoreo, junto con las penalizaciones a ser aplicadas en caso de incumplimiento (Entrevistado 4).

Ahora bien, además de efectuar el monitoreo de controles del proveedor, y participar en la definición de parámetros de seguridad, el ente usuario es responsable de aplicar sus propios recaudos, como por ejemplo implementar prácticas de *back up* de la información almacenada en la

nube (Entrevistados 4, 5). Los resguardos de información periódicos, por ejemplo, mensuales, aseguran que si se produjera un incidente en el proveedor, la información perdida solo correspondería a un período corto de tiempo. De esta forma, el ente logra definir su propio umbral de recupero independientemente del definido por el proveedor, pudiendo determinar la información perdida desde el último resguardo hasta la fecha del incidente.

Este control es evaluado por los auditores de sistemas y reportado en forma recurrente a los financieros. Según se expresó, es usual que usuarios con servidores locales no cumplan en la práctica con las normas de resguardo que han establecido (Entrevistado 5), de modo que es de esperar que esta falla ocurra también en la nube.

Estas previsiones también son implementadas por los auditores cuando las empresas elaboran y almacenan su información financiera en servidores de casas matrices del exterior. Sirven no solo a los auditores, sino también a la IGJ –según se expresó en la descripción de riesgos legales– en la medida en que si se produjera un incidente, existe un resguardo de la información relevante (Entrevistado 5).

5.4.3. PROCEDIMIENTOS APLICABLES PARA LA EVALUACIÓN DE CONTROLES INTERNOS

Los procedimientos a ser aplicados para la evaluación de controles fueron analizados en profundidad por los profesionales. Las propias características de la CN, dependiendo del modelo utilizado, referidas a la independencia de localización entre el usuario y el proveedor, así como la intangibilidad del servicio, pueden imponer ciertas restricciones respecto de la forma en que se realizará la evaluación del sistema de control interno. Cabe recordar que es difícil, pero no imposible, conocer la ubicación de los servidores y la identificación de los responsables de la administración de las aplicaciones (Entrevistado 6).

A los auditores, en particular a los de sistemas, se les plantea un nuevo paradigma, requiriéndose en algunos casos el diseño de nuevas soluciones para la evaluación de los controles (Entrevistado 6). La principal diferencia en un entorno de CN es la forma en que se van a poder obtener las evidencias para ganar confianza –o no– sobre el sistema de control interno del ente.

Así como la evaluación de controles distingue entre los implementados por el proveedor y el usuario, los procedimientos a ser aplicados también deben ser diferenciados.

A. Procedimientos sobre el proveedor del servicio

a) Informes de Control Interno de la Organización de Servicios

En principio, sería deseable para el auditor del usuario realizar auditorías sobre el proveedor del servicio en la nube (Entrevistado 1). Sin embargo, en casos de tercerización como el de la CN, resulta complejo –y hasta imposible– acceder a los proveedores para realizar la evaluación del sistema de control interno (Joint et al., 2009; Nicolaou et al., 2012), ya sea para llevar a cabo

entrevistas con el personal como para la ejecución de procedimientos para validar la efectividad de los controles internos en los centros de cómputo (Entrevistados 2, 4, 8). Estas limitaciones de acceso también fueron mencionadas para el proceso de conocimiento del cliente.

Frente a estas dificultades encontradas en los entornos de CN, los profesionales mencionaron que la solución utilizada por los proveedores para informar a los usuarios y sus auditores respecto de su sistema de control interno consiste en brindar informes en los que describen todas las características de sus sistemas y centros de cómputos, así como los detalles de las medidas de seguridad y otros controles adoptados (Entrevistado 4).

Esas descripciones son acompañadas por una de las principales fuentes de información descriptas por los profesionales para estos casos: los *informes de control interno de las organizaciones de servicio emitidos por auditores independientes* (Entrevistados 1, 2, 3, 5, 6, 8), confirmando lo que había sido mencionado en la bibliografía como la solución para la evaluación de controles internos en entornos de tercerización de TI.

En estos casos, los auditores utilizarían los informes para conocer y comprender el sistema de control interno del proveedor del servicio en la nube. Les brindan información sobre los controles implementados por los proveedores y la seguridad razonable de su diseño, implementación y/o funcionamiento, de acuerdo al reporte emitido por el auditor del servicio (Entrevistado 8).

Es de esperar que la mayoría de los proveedores de la CN opten por obtener estos informes emitidos por auditores independientes. Según la opinión de los profesionales, esto les implicaría dos beneficios: a) satisfacer la demanda de información de todos sus clientes con un único informe, evitando dar respuesta a auditorías redundantes y los costos que ello les representaría; b) brindar seguridad a sus clientes respecto del cumplimiento de buenas prácticas de control interno.

La emisión de estos informes, si bien en muchos casos es decidida por el proveedor del servicio, también puede ser exigida –en el caso de los contratos negociables– por el propio usuario. En caso contrario, cuando por ejemplo se trata de proveedores más chicos que no hubieran contratado estas auditorías del servicio, se recomienda que el cliente exija la inclusión de cláusulas que le garanticen el derecho a efectuar sus propias auditorías sobre el sistema de CI del proveedor (Entrevistado 3).

- **Tipos de Informes de Control Interno**

Todos los entrevistados del área de sistemas estuvieron de acuerdo en que el tipo de informe que se debe solicitar al proveedor es el más general, referido a diversos dominios: seguridad, continuidad, integridad de procesamiento de un sistema y confidencialidad o privacidad de la información procesada por dicho sistema (denominado SOC2 por la normativa estadounidense), debido a que es de mayor utilidad para las revisiones que ellos deben realizar.

Cabe mencionar que la opinión es dada principalmente por los auditores de sistemas, para quienes toda la información de un ente que pudiera estar almacenada en la nube (sea contable o no) posee el mismo nivel de importancia. Esto es, ellos analizan los controles en general, y no necesariamente aquellos vinculados a la información que impactará en los estados contables. Por eso es que prefieren disponer de este tipo de informes (Entrevistados 2, 3). Y es por eso que los auditores financieros atribuyen el carácter de general a los reportes que emiten los auditores de sistemas.

En relación a la efectividad del funcionamiento de los controles, existió consenso unánime en cuanto a que el informe requerido debe ser de los denominados Tipo II, referido no solo al diseño e implementación de los controles internos, sino también a su efectividad operativa en el período de tiempo establecido (Entrevistados 2, 3, 4, 6), debido principalmente a la limitación en el alcance de la tarea del auditor que no podría probar por sí mismo el funcionamiento de los controles. El requerimiento de un informe Tipo II atiende no solo a los intereses de los auditores sino también a los de los propios usuarios.

> Todo tiene que ser evaluado a nivel de eficacia operativa. (…) No solo para mí como auditor, sino también para la empresa; la empresa no se puede quedar tranquila cuando el proveedor solo le diga que tiene los controles implementados. (Entrevistado 4)

- **Inclusión de las organizaciones de servicio subcontratadas por el proveedor de la nube**

La subcontratación de parte de las actividades del proveedor en otros proveedores de la nube ha sido vista por los entrevistados como un factor que incrementa significativamente la complejidad de la nube y de la evaluación del sistema de control interno. La principal dificultad radica en que para el usuario es muy difícil darse cuenta que parte de los servicios que le son prestados se encuentran a su vez tercerizados. El único modo de saberlo sería si el proveedor se lo declara al momento de la negociación, o si ocurre un evento o accidente durante la utilización del servicio por el cual se le revela al usuario el tercero subcontratado por el proveedor (Entrevistado 2).

Incluso el Entrevistado 2 menciona que en ciertos países de Europa la discusión sobre la tercerización se volvió sumamente compleja, al punto que existía la intención de abolirla, ya sea impidiendo la tercerización, o en caso que sucediera, exigiendo que los proveedores lo informaran explícitamente a sus clientes. Las siguientes situaciones sirven para ejemplificar las razones por las que la subcontratación es tan importante:

- aun cuando el usuario se asegure que el proveedor del servicio está ubicado en su mismo país y que aplica las mismas leyes, podría darse la localización transfronteriza del proveedor subcontratado, fuera de la jurisdicción del ente usuario, con el riesgo de violación de leyes que le son aplicables, incluso sin su conocimiento;

- pueden existir problemas de ineficiencia de las medidas de control interno adoptadas en relación a planes de contingencia, por una referencia circular a través de las subcontrataciones, de modo que el primer proveedor que subcontrata el proceso de *back up* termina siendo el depositario de las copias de *back up* realizadas por su subcontratado.

> Caso dónde el servicio de contingencia de una empresa que estaba en la nube terminaba siendo en el mismo servidor nativo: yo te doy servicios en la nube, utilizando los servicios de Amazon. A su vez contrato a un tercero para que me dé el servicio de contingencia del servicio que estoy brindando originalmente. Este tercero, para dar el servicio de contingencia, termina contratando el servicio de Amazon, por lo cual tenía el mismo problema. O sea, en realidad, no tenía solución a mi problema. (Entrevistado 2)

El método que se debe requerir para la emisión del informe de control interno en relación a las organizaciones de servicio subcontratadas debe ser el inclusivo (Entrevistados 2, 3). Esto es, el proveedor debe incluir en su descripción los servicios que subcontrata, y el trabajo del auditor del servicio debe alcanzar al tercero involucrado.

- **Estándares de CI específicos para la CN**

La elaboración de los informes de control interno de las organizaciones de servicio está basada en estándares específicos, marcos de referencia que sirven como punto de comparación, aplicable por cualquier profesional que efectúe la auditoría (Entrevistados 4, 5).

Existen estándares de control interno específicos para la CN, elaborados principalmente por organizaciones europeas o norteamericanas que nuclean a representantes de usuarios y proveedores de servicios en la nube. Éstos además de servir para guiar a proveedores y usuarios en el diseño e implementación de los controles internos en estos entornos, según las pretensiones de sus emisores, pueden ser útiles para realizar auditorías de control interno de los servicios en la nube y la emisión de los informes de CI de las organizaciones de servicios.

Su uso es útil para homogeneizar el lenguaje y que todos –auditores y usuarios– se refieran del mismo modo a los controles, facilitando la interpretación de los informes de control interno de las organizaciones de servicios en la nube (Entrevistados 2, 3). Si bien se haría más dinámica la comunicación, su utilización no necesariamente hará mejor o más seguro el servicio.

Aun cuando estos estándares estuvieran disponibles para la realización de auditorías de sistemas en la nube, el Entrevistado 6 considera que las entidades certificantes o auditoras de estos servicios necesitan aplicar procedimientos que les permitan obtener satisfacción respecto del funcionamiento de los controles allí mencionados. Ello puede deberse a que éstos son muy recientes.

> Teniendo a COSO como la ley, ahora lo que tenemos que hacer es aterrizar los principios de totalidad, exactitud, validez, acceso restringido que nos plantea COSO, y ver como elaboramos procedimientos para poder auditar entornos en la nube (…) Ahí es donde todos tenemos nuestros pequeños grises. (Entrevistado 6)

b) Solicitud al auditor del servicio

Un procedimiento adicional que está previsto en la NIA 402 (A.12, A9) para la obtención de evidencias respecto del control interno del proveedor consiste en recurrir al auditor del servicio para que aplique procedimientos específicos que proporcionen cierta información necesaria sobre controles, por ejemplo, porque la información obtenida del ente auditado no fuera suficiente y no estuviera disponible en el informe de controles internos de la organización de servicios.

Esta alternativa fue considerada por el Entrevistado 8, quien mencionó que los informes de CI son utilizados para la evaluación del sistema en general. En los casos en que se necesite confiar en un ciclo de operaciones determinado, la opción de enviar *instrucciones* al auditor del proveedor para indicarle determinados controles internos específicos que resulta necesario evaluar es al menos deseable.

Sin embargo, considerando que los auditores del sistema emiten informes genéricos para todos los usuarios, y que son contratados por el proveedor del servicio a su costo, existen dudas acerca de si esta alternativa sería aplicable.

c) Pruebas de eficiencia de los controles sobre el proveedor en la nube

A efectos de verificar la implementación y funcionamiento de las medidas de seguridad lógica del sistema, sería interesante realizar pruebas de los controles sobre el proveedor de la nube. En estos casos, suelen intervenir los laboratorios de sistemas de los grandes estudios de auditoría (Entrevistado 4).

> Nosotros tenemos lo que es la parte de laboratorio, que depende del área de sistemas. Este se ocupa de hacer ataques a las redes, *test* de penetración, evaluación de debilidades, todo a nivel lógico. En caso de tener sistemas montados en la nube, si o si aplica su participación en la auditoría. (Entrevistado 4)

Esta posibilidad depende de la disponibilidad que el estudio de auditoría tenga de este tipo de laboratorios y de personal capacitado para la ejecución de las pruebas. Además, su aplicación demanda una mayor cantidad de horas destinadas a la auditoría del sistema, que implica un presupuesto superior dentro del costo total del encargo, que debe ser aceptado por el cliente auditado. Se podría requerir además la aceptación por parte del proveedor del servicio de ser sometido a este tipo de pruebas, existiendo dudas acerca de que lo permita.

Esta solución parece estar restringida en estudios más pequeños –salvo que contraten especialistas externos– requiriéndose la aplicación de otros procedimientos para la evaluación del control interno.

B. Procedimientos sobre el usuario del servicio

En este caso el acceso es más sencillo. En consecuencia, pueden realizarse entrevistas con el personal del ente auditado para realizar un relevamiento de los controles internos aplicados sobre

las actividades tercerizadas, y en su caso, si fuera necesario, podría observarse documentación que respalde la ejecución de los controles, e incluso de los controles en operación (Entrevistado 4).

5.4.4. CARTA CON RECOMENDACIONES

Durante la labor de auditoría es posible detectar debilidades de control interno que muchas veces no afectan directamente a la auditoría financiera –por ejemplo, por referirse a controles que no son *relevantes* para ésta. Sin embargo, las mismas pueden ser incluidas en la carta con recomendaciones a fin de asesorar a la dirección del ente sobre el diseño y/o funcionamiento de ciertos controles, principalmente en un caso de servicio tercerizado como el de la nube, en el cual –como se ha descripto– la evaluación del sistema de control interno es compleja (Entrevistado 5).

En otros apartados de esta tesis se han mencionado aspectos que podrán ser informados a la dirección del ente por este medio, no expresadas nuevamente aquí para evitar repeticiones.

5.4.5. RESUMEN

Conocer el diseño y funcionamiento del control interno es fundamental al momento de planificar una auditoría de estados financieros. Del mismo modo fue considerado por todos los entrevistados en una auditoría en entorno de CN.

En primer lugar se planteó la importancia de la participación de los auditores de sistemas en esta etapa del encargo. Dada su especialización, son capaces de colaborar significativamente en el conocimiento y evaluación de controles de TI, más aun en entornos con cierta complejidad y características diferenciales como es el de la nube.

En segundo lugar se analizaron en detalle los controles internos relevantes para los auditores en este punto. Por tratarse de un servicio tercerizado, la evaluación alcanza no solo a los controles del ente usuario, sino también los implementados por el proveedor del servicio, razón por la cual los entrevistados plantearon su análisis por separado.

Se refirieron en primer lugar a los controles relevantes del proveedor, que incluyen principalmente aquellos de carácter *general* y políticas tendientes a lograr la seguridad de la información del ente usuario, en particular en lo que se refiere a su confidencialidad e integridad, y en menor medida a su disponibilidad.

Se expone una descripción detallada de las diferentes subcategorías de controles relevantes, enfatizando aquellos con incidencia en la auditoría de estados financieros: adecuado ambiente de control en el proveedor; controles de acceso y gestión de usuarios con otorgamiento de permisos según los requerimientos del ente; medidas de seguridad implementadas para la transferencia de datos; redundancia en el almacenamiento y aislamiento de información de diferentes usuarios, considerando la existencia de recursos compartidos; control sobre modificaciones a los sistemas; medidas de seguridad física y adecuados planes de contingencia y recuperación de desastres.

A su vez, son relevantes para el auditor los llamados *controles complementarios de la entidad usuaria,* según los denomina la normativa. Es responsabilidad del ente efectuar el monitoreo de las actividades de control implementadas por el prestador del servicio, dado que la responsabilidad sobre la seguridad de la información sigue siendo del usuario. Estos incluyen el análisis de distintos tipos de reportes emitidos por el proveedor sobre el funcionamiento de sus controles e incidentes ocurridos, así como la realización de copias de resguardo de la información almacenada en la nube, más allá de los planes de contingencia implementados por el prestador.

Por último, se efectúa un análisis de los procedimientos usuales aplicados para la evaluación del sistema de control interno y la factibilidad de su utilización en entornos de la CN.

La comunicación con los proveedores y la realización de pruebas sobre sus sistemas, previstas por la normativa, no fueron mencionadas como procedimientos de ejecución probable por los entrevistados. Esto se debe a la imposibilidad de acceso, así como la reticencia que ellos demuestran –en general– a abrir sus sistemas a terceros que no sean sus propios auditores del servicio.

Del mismo modo, la solicitud de información al auditor del servicio, o la aplicación de procedimientos determinados sobre controles puntuales de interés para el auditor financiero, resulta poco probable. Esto principalmente cuando el auditado hubiera contratado grandes proveedores de CN, quizás ubicados en el exterior, situación que tal vez podría ser diferente si se contratan pequeños proveedores locales.

En consecuencia, la utilización de informes sobre los controles internos de la organización prestadora del servicio sería la alternativa más viable para comprender el sistema de control interno del proveedor.

En este sentido, según los auditores es preferible la obtención de informes de alcance amplio, del tipo SOC2, referidos a varios dominios de control interno (seguridad, continuidad, integridad de procesamiento de un sistema o la confidencialidad o privacidad de la información por él procesada), y no solo a controles relacionados con la información financiera (SOC1). Esto puede deberse a que el uso de estos informes se da por parte de los auditores de sistemas de acuerdo a la estructura de los grandes estudios, quienes pretenden un conocimiento más amplio de los controles del proveedor.

A su vez, en esta etapa el auditor necesita conocer si los controles han funcionado correctamente durante un período de tiempo determinado, requiriéndose entonces un informe Tipo II. Un informe Tipo I, que solo indique si los controles se han diseñado e implementado de acuerdo a los objetivos de control planteados, no brinda evidencia adecuada y suficiente en esta instancia.

Si bien resulta prácticamente inviable, tal como lo manifestaron los entrevistados, sería interesante realizar pruebas de funcionamiento sobre los controles del proveedor, contratadas por el usuario del servicio. Estas pueden incluir *hackeos* éticos o *tests* de penetración, que a la vez que

brindan garantías a los usuarios sobre el buen o mal funcionamiento de los controles del proveedor, otorgan evidencias para el auditor financiero.

Por último, se destaca que las debilidades de control vinculadas al uso de CN que fueran detectadas durante el proceso de la auditoría financiera, podrían ser informadas a la dirección del ente junto con las recomendaciones que se consideren adecuadas, de modo de permitirle gestionarlas y mejorar los procesos vinculados.

El Cuadro 25 resume los principales aspectos de este apartado.

Cuadro 25 - Evaluación del sistema de control interno relevante para la auditoría

<table>
<tr><th>TÓPICO</th><th>CATEGORÍAS</th><th colspan="2">SUBCATEGORIAS</th></tr>
<tr><td rowspan="6">EVALUACIÓN DEL SISTEMA DE CONTROL INTERNO</td><td rowspan="3">CONTROLES INTERNOS DE TI RELEVANTES PARA EL AUDITOR</td><td rowspan="2">Controles Generales

Relevancia para auditor financiero para depositar confianza en los controles de las aplicaciones.</td><td>De los sistemas de información del proveedor
• Ambiente de control
• Control de acceso y gestión de usuarios
• Seguridad en la transferencia de información
• Redundancia de almacenamiento y fraccionamiento de la información
• Aislamiento de la información
• Procedimientos para la modificación de aplicaciones
• Interfaces entre sistemas
• Seguridad física
• Modificación de aplicaciones
• Planes de contingencias y recuperación de desastres
• Soporte</td></tr>
<tr><td>Del cliente sobre las actividades del proveedor del servicio
• Monitoreo de controles del proveedor
• Copias de resguardo de la información</td></tr>
<tr><td colspan="2">Controles de las Aplicaciones</td></tr>
<tr><td rowspan="4">PROCEDIMIENTOS APLICABLES</td><td>Informes de CI de la organización prestadora del servicio</td><td>• Alcance: SOC2
• Tipo: II - Efectividad operativa del CI
• Método Inclusivo respecto de empresas subcontratadas por la OS</td></tr>
<tr><td>Contacto con prestador de servicio</td><td>• Consultas
• Visitas para aplicar procedimientos sobre controles relevantes</td></tr>
<tr><td>Solicitud al auditor del servicio</td><td>Indicaciones para evaluación de controles o solicitud de información específica.</td></tr>
<tr><td>Pruebas de eficiencia de los controles sobre el proveedor en la nube</td><td>• Laboratorios
• Test de penetración</td></tr>
</table>

***LECTURA**: Letra azul: elemento nuevo. Letra en otro color: elemento original nombrado con mayor (verde) o menor (rojo) relevancia en las entrevistas.*

Fuente: Elaboración propia.

5.5. EVIDENCIAS DE AUDITORÍA DIGITALES EN ENTORNOS DE CN

El presente apartado pretende dar cumplimiento al siguiente objetivo específico:

Indagar las posibles consecuencias sobre el proceso de obtención, procesamiento y conservación de las evidencias de auditoría que surjan en el contexto de la nube.

Basados en las apreciaciones de los expertos que realizaron la revisión del cuestionario, se esperaba que éste resultara un aspecto especialmente afectado por el uso de la CN por parte del auditado. No obstante, los resultados de las entrevistas no cumplieron con las expectativas. Es probable que muchos de los aspectos vinculados al tema ya hubieran sido conversados durante las instancias previas, razón por la cual los especialistas evitaron las repeticiones de conceptos.

En primer lugar, se hace referencia a aspectos vinculados a la obtención de las evidencias –tema que fuera desarrollado con mayor amplitud– y posteriormente a las tareas referidas al procesamiento y conservación, las cuales no son afectadas de manera significativa por la CN, según surge del análisis de los datos recopilados.

5.5.1. OBTENCIÓN DE LAS EVIDENCIAS DE AUDITORÍA

Según se expresó en el marco teórico, las evidencias digitales –al igual que las tradicionales– pueden ser tanto de cumplimento como sustantivas. Del análisis de las respuestas de los profesionales resulta que la problemática es distinta para uno u otro tipo, razón por la cual se analizan por separado.

En cuanto a las *evidencias de funcionamiento de controles*, los entrevistados hicieron referencia a lo mencionado en la parte de la entrevista sobre la evaluación del sistema de control interno en entornos de tercerización de TI en general, y la nube en particular, cuestión analizada en el apartado anterior.

La obtención de este tipo de evidencias parecer ser más bien un problema para los auditores de sistemas, encargados de la evaluación del sistema de control interno. Las dificultades de acceso a los proveedores del servicio para la obtención de información y la evaluación de controles vuelven a ser mencionadas, estableciéndose como solución la utilización de los informes de control interno de la organización de servicio como alternativa.

Como aspecto diferencial, el Entrevistado 2 hizo mención en este punto a lo que se conoce como *auditoría continua*, resaltando la importancia de las alertas permanentes que informen al usuario sobre cambios significativos en la información del ente almacenada en la nube (como actualización o eliminación masiva de datos). Esto sirve como medida de control sobre la disponibilidad y confiabilidad de la información almacenada en el tercero, generándose evidencias de auditoría en forma permanente. Podría requerirse un mayor análisis sobre la forma de implementación de *auditorías continuas* (Pastor, 2011) en un entorno en la nube, el tipo de alertas a

generar y la utilidad para los auditores, no solo de sistemas sino también financieros, a efectos de mejorar y facilitar el proceso de auditoría en estos entornos.

> (…) se podría implementar más fácilmente, a mi entender, auditorías continuas sobre la información de la nube. O sea, yo diría que la información en la nube debería tener más alertas que cuando esté en forma local. (…) sería ya empezar a trabajar la auditoría por detrás de los sistemas y no con la interpretación que hacen los sistemas de información sobre la información que administro. Me parece que es el paso de evolución de auditoría de una vez por todas. (Entrevistado 2)

Respecto de las *evidencias sustantivas*, que son mayormente obtenidas y procesadas por los auditores financieros, existe acuerdo en que el uso de la computación en la nube por el cliente no representa una diferencia importante para el profesional; la obtención de los datos, en principio, no varía respecto de un entorno de TI local, ni siquiera haciendo más compleja su obtención (Entrevistados 2, 3,4, 5, 6).

En relación a este tipo de evidencias se analizaron tres aspectos, a saber:

a) La forma de acceso a la información

La obtención de los datos por parte del auditor puede darse de dos maneras: a) solicitando información específica a personal del cliente auditado; o b) extrayendo el contador los datos del sistema en forma independiente. Esta última opción es posible principalmente cuando los sistemas del ente permiten generar usuarios exclusivamente de consulta y en caso que se les facilitara una terminal (computadora) en el cliente. Ambas alternativas pueden ser aplicadas en una auditoría en entorno de CN. El acceso a los datos en vez de darse sobre los servidores locales, se hará sobre los del proveedor del servicio en la nube, ubicados externamente; sin embargo, esto no estaría cambiando el desarrollo de la auditoría (Entrevistados 3, 5).

La utilización de TAACs puede ser un elemento que brinde transparencia y facilite la extracción de los datos del sistema, en la medida en que las herramientas tecnológicas y los *software* específicos de auditoría existan o sean adaptados para ser aplicados a la nube; sin embargo, esto no es considerado como un elemento diferenciador de la nube, dado que la forma de aplicación y la utilidad para el auditor financiero sería la misma que en el caso de un sistema local (Entrevistado 2).

b) La disponibilidad de la información contable sujeta a auditoría

Esta cuestión fue analizada como un riesgo técnico (en el apartado *5.3.2.c)*), respecto del cual corresponde aplicar medidas de control adecuadas, como precauciones al momento de contratar los proveedores de servicios de telecomunicaciones o los planes de contingencia (planteados en el apartado *5.4.2.*). En la medida en que tanto el ente usuario como el proveedor adopten los recaudos correspondientes, la disponibilidad de la información no debería verse afectada (Entrevistado 6).

Cabe aclarar que los riesgos de continuidad no son importantes en situaciones de interrupciones temporales del servicio, que no produjeran la pérdida de información en forma permanente. Pueden impedir el acceso del auditor a la información en determinado momento, pero en principio seria solucionable con posterioridad. En caso de pérdida total de la información que respalda los saldos de los estados financieros sujetos a auditoría, el encargo no podría ser ejecutado.

> O sea, no es como una venta, que si o si la tenés que hacer ahora porque si no se te va el cliente y la perdiste. El auditor puede decir: "bueno, hoy no hay sistema, mañana saco el reporte". (Entrevistado 4)

Un aspecto interesante resaltado por el Entrevistado 8, vinculado con la disponibilidad de los datos, es la falta de comunicación con *personas* que puedan facilitar información adecuada a los fines de la auditoría financiera. Según su experiencia, en los entornos locales de TI, si bien la auditoría se ve afectada por la tecnología, siempre es posible para el contador encontrar alguien a quien solicitar un cambio en un reporte o manifestar que cierta información no le resulta útil de la forma en la que le fue proporcionada. Sin embargo, cuando existen procesos o sistemas tercerizados, dicha comunicación es más compleja, dado que en general no existen personas disponibles para atender estos requerimientos en los proveedores de servicios. En definitiva, esto podría terminar afectando la disponibilidad de información adecuada para la auditoría.

> Hoy en día hay mucha interacción entre el auditor y la empresa auditada, a pesar de que las computadoras cada vez nos afectan más la relación entre las personas. Hay una parte muy importante de la auditoría que es personal y cuando hay mucha información o muchos procesos tercerizados, eso se pierde. Y esa es la parte a la que yo como auditor financiero más miedo le tengo al momento de hacer una auditoría (…) Acá es como que el problema del sistema va a quedar tercerizado en algún lugar en una nube, entonces va a ser difícil darle una respuesta inmediata… pero creo que es algo que va a ser un proceso, en el cual vamos a tener que estandarizar muchos procesos para que incluso cuando surjan esos problemas, podamos darles una respuesta. (Entrevistado 8)

Estas dificultades de los entornos de tercerización de la TI aún requieren la propuesta de soluciones.

c) La fiabilidad de la información obtenida de los sistemas en la nube

Tal como en una auditoría en un entorno de TI local, la confianza que los auditores puedan depositar en la información obtenida de los sistemas en la nube dependerá especialmente de la evaluación del sistema de control interno realizada por los auditores de sistemas.

Ello tiene importancia no solo por la falta de disponibilidad, sino por la fiabilidad de la información. En la medida que los controles internos en la nube funcionen correctamente, es de esperar que la información resultante sea confiable (Entrevistados 3, 4, 5, 6, 8).

El Entrevistado 6 se refirió a las garantías que debe obtener el auditor respecto de la información brindada por los sistemas del ente para poder confiar en ella. Según indicó:

> Una vez obtenida la información del ente, trabajamos en nuestros propios equipos. Básicamente, siempre que se saca información de cualquier sistema, el auditor se tiene que asegurar la totalidad, exactitud y validez de los datos que está obteniendo. Es decir, eso significa que los bajé todos, que son los correctos y que bajé los datos productivos, no los bajé de otro ambiente; es decir, bajé los datos que tengo que auditar. Una vez que yo me hice de esa información, la reproceso en mi equipo o saco mis listados o hago mis análisis, y la verdad que debiera ser transparente si está en la nube o dónde este. Digamos, a partir de ahora, es todo exactamente lo mismo para la auditoría. (Entrevistado 6)

Entre los controles relevantes para contribuir a la fiabilidad de la información se resaltaron aquellos referidos a la imposibilidad de adulteración de los datos en el momento de la extracción de la información proporcionada al auditor.

> Incluso en el caso de auditorías bajo normativa de la SEC se le está dando mucha importancia a esa información que proporciona la entidad, previendo que la gente de TI analice como es el trasfondo del sistema, para garantizar que esos listados salen bien y no pueden ser adulterados. (Entrevistado 5)

Esto se debe a que dichas modificaciones pueden ser muy difíciles de detectar por parte del auditor financiero durante la revisión de muestras de la documentación respaldatoria de las operaciones. Por pequeña que sea la cantidad de registros adulterados, dicha situación hace que todo el conjunto de datos deje de ser confiable.

5.5.2. PROCESAMIENTO Y CONSERVACIÓN DE LAS EVIDENCIAS

En cuanto al procesamiento y conservación de las evidencias, los resultados coinciden con lo anticipado en el marco teórico. Una vez obtenida la información, en la medida en que los datos obran en poder del auditor financiero, siendo analizados en sus propios sistemas, no deberían existir diferencias, independientemente del entorno de TI utilizado por el ente auditado (Entrevistados 3, 5, 6, 8).

> Las técnicas de auditoría para el análisis de la información son las mismas. Ya estamos hablando de la auditoría financiera, salimos del ambiente de control de TI, y estamos sobre el procesamiento de la información. Son exactamente las mismas, no debiera haber ninguna diferencia. (Entrevistado 6)

El Entrevistado 5 enfatizó algunas precauciones interesantes para el resguardo evidencias referidas a la información que estuvo sujeta a auditoría. Habitualmente, en su caso solicita al ente auditado la siguiente información:

1. Balance de comprobación de sumas y saldos al inicio del ejercicio.
2. Balance de comprobación de sumas y saldos posterior a la realización de los ajustes de auditoría, para asegurarse mediante un reporte emitido y entregado por el ente auditado, que a determinada fecha –luego de los ajustes propuestos y aceptados por el ente– su información coincide con la del equipo de auditoría.
3. La base de asientos de todo el ejercicio, con lo que ERS toma los saldos al inicio, agrega todos los asientos del libro diario, y los saldos de cierre deberían coincidir, a fin de garantizar la integridad.

> Ya con eso, si después desaparece la información o no, yo tengo un mail de la compañía, que me dijo que esta es la base de datos y yo la crucé, y me confirmó que está ok; ese es mi resguardo. Después si desaparece, o si mete un ajuste después de que sacamos el balance, es un tema de ellos; nosotros hasta ese día estuvimos cubiertos. (Entrevistado 5)

Si bien esta precaución es aplicable a cualquier sistema de información en contextos de TI, resulta especialmente interesante cuando se utilizan sistemas tercerizados, y en el caso de la CN en particular, considerando los diversos riesgos analizados previamente.

En la nube, existe una fuerte dependencia de las medidas de conservación adoptadas por el proveedor del servicio. La disponibilidad de la información financiera con posterioridad a la emisión del informe de auditoría queda sujeta a su voluntad y a la continuidad de la relación del auditado con su proveedor. Con esta solución, dichos problemas podrían verse superados, al menos parcialmente, teniendo el auditor resguardo de toda la información relevante.

Cabe mencionar al respecto la obligación impuesta por la RT 37 en su punto *II.B.2. Documentación del encargo*, que establece que el profesional está obligado a documentar apropiadamente su trabajo en papeles de trabajo. De acuerdo a lo establecido por la normativa, y en relación a la conservación de los mismos:

> El contador debe conservar, **en un soporte adecuado** a las circunstancias y **por el plazo que fijen las normas legales o por diez años, el que fuera mayor**, los papeles de trabajo, una copia de los informes emitidos y, en su caso, una copia de los estados contables u otra información objeto del encargo, firmada por el representante legal del ente al que tales estados contables o información correspondan. (RT 37, Segunda parte, Sección II.B.2.4) (el resaltado es propio)

Tratándose de evidencias digitales, es fundamental prever los medios adecuados que garanticen el acceso en el futuro a los papeles de trabajo y a las evidencias. El plazo de conservación previsto por la norma podría ser considerado excesivo, teniendo en cuenta la dependencia de un tercero con el cual el cliente auditado podría cesar su relación comercial, o incluso un plazo en el cual podría darse una superación de la tecnología que haga que la información pueda no estar disponible si no se han previsto las medidas adecuadas al efecto, tal como se detalla en el referencial teórico.

Todo ello limitaría la posibilidad de acceder a la información en el futuro, cualquiera sea la causa de dicha necesidad. En consecuencia, las precauciones adoptadas por el auditor para la conservación de sus propias evidencias como respaldo del trabajo realizado en entornos de CN resultan fundamentales.

5.5.3. RESUMEN

Los resultados obtenidos evidencian que este aspecto de la auditoría no se considera alterado en forma importante por el uso que el ente auditado haga de un servicio de tercerización de TI, sea éste computación en la nube u otro.

Respecto de las evidencias, se distingue entre las de control y las sustantivas. Si bien en los grandes estudios unas y otras son obtenidas por diferentes profesionales, en el caso de contadores que se desempeñen en estudios más pequeños, en los que usualmente no existe tanta especialización, resultaría relevante tener en cuenta las apreciaciones referidas a ambos tipos.

Las evidencias de control fueron tratadas en el apartado anterior de esta tesis. Se introdujo aquí el concepto de auditoría continua, como una forma de facilitar significativamente la labor del auditor y que puede ser importante en un entorno en la nube. No habiéndose obtenido más precisiones al respecto, resulta un concepto que es posible ampliar mediante futuras investigaciones, más aun considerando que no parece tener implementación generalizada en la Argentina.

En general existe acuerdo en que una vez evaluado el sistema de control interno en la nube –tanto del proveedor como del usuario– la obtención de evidencias sustantivas no presenta diferencias significativas respecto a lo que ocurre en un ambiente de TI tradicional. Respecto del acceso a la información, el auditor aplicara técnicas similares al resto de los ambientes de TI.

En cuanto a la disponibilidad de los datos, en la medida en que los controles internos funcionen correctamente, no debería haber problemas significativos. Se debe considerar que las interrupciones temporales del servicio no representan dificultades para los auditores de estados contables; no así el caso de interrupciones permanentes o de pérdida de datos, lo cual podría incluso impedir la ejecución del encargo de auditoría por falta de disponibilidad y oportunidad de la información. A su vez, el contador debe tener en cuenta la restricción que supone la falta de comunicación con personas que puedan dar respuesta a sus demandas de mejora de la información necesaria a los fines de la auditoría. Dicha limitación existe en principio en la mayoría de los ambientes de tercerización de TI.

Respecto a la fiabilidad de la información que generan los sistemas, la misma es determinada por la evaluación que se hubiera realizado del ambiente de control interno y de los controles generales de TI. En este punto resulta fundamental la consideración de la posibilidad de adulteración de la información en el momento de la obtención, a fin de garantizar la exactitud, totalidad y validez de los datos, como también desechar la posibilidad de fraudes o errores.

En cuanto al procesamiento y almacenamiento de la información, no existen diferencias causadas por el entorno en el cual se genera, dado que esta etapa del proceso de auditoría se realiza en los sistemas del auditor.

Es importante destacar las precauciones vinculadas a la conservación de los papeles de trabajo y los datos obtenidos de los sistemas del ente como evidencia, a fin de garantizar no solo el cumplimiento de la normativa respecto a la forma de conservación y plazos, sino también contar con los medios de justificación del trabajo realizado y de defensa en caso de cuestionamiento de la responsabilidad del auditor.

El Cuadro 26 resume los resultados de este apartado.

Cuadro 26 - Evidencias de auditoría digitales en la nube

TÓPICO	CATEGORÍAS	SUBCATEGORÍAS	
EVIDENCIAS DIGITALES DE AUDITORÍA EN CN	**OBTENCIÓN**	**Procedimientos para la obtención**	**Evidencias de controles** • Auditoría continua **Evidencias sustantivas** • Solicitud a personal del ente • Autenticación de usuarios de auditoría • Uso de TAACs Inalterabilidad de información de origen
		Disponibilidad de la información	Ubicación de la información Temporalidad de los datos Interrupción del servicio • Temporal • Permanente - Pérdida de la información o modificación no autorizada Falta de interacción personal
		Confiabilidad de la información	Autenticidad de registros Evaluación de controles internos
	PROCESAMIENTO	Procesamiento y evaluación de las evidencias de auditoría obtenidas No alteración de datos originales. Uso de copias de archivos digitales	
	CONSERVACIÓN	**De evidencias y papeles de trabajo**	Disponibilidad futura • Obsolescencia • Destrucción • Dependencia de un tercero Plazos de conservación según la normativa

***LECTURA**: Letra azul: elemento nuevo. Letra en otro color: elemento original nombrado con mayor (verde) o menor (rojo) énfasis en las entrevistas.*

Fuente: Elaboración propia.

5.6. CONOCIMIENTOS DEL PROFESIONAL CONTABLE. USO DE EXPERTOS EN TI

El presente apartado pretende dar cumplimiento al último objetivo específico planteado para esta tesis:

Analizar la formación y las habilidades requeridas al contador público y la eventual colaboración de especialistas en TI para el desarrollo de encargos de auditoría financiera en entornos de TI complejos, en particular los basados en la computación en la nube.

En primer lugar se describe la estructura de los grandes estudios de auditoría, en la medida en que su conocimiento puede resultar útil a los efectos de comprender las respuestas obtenidas de los entrevistados, quienes pertenecen a este tipo de organizaciones.

Luego se exponen los resultados respecto de los conocimientos que se espera posean los contadores públicos para poder desarrollar encargos de auditoría en contextos tecnológicos similares a los de CN. Se enfatiza en la importancia de la formación de los profesionales en esta área, brindando lineamientos sobre los temas a ser profundizados.

Por último, se presentan las opiniones respecto de la relevancia del trabajo interdisciplinario, mediante la participación de auditores de sistemas en las auditorías financieras en aquellos casos en los que el entorno tecnológico utilizado por el auditado requiera de conocimientos que excedan los que posea el profesional contable.

5.6.1. ESTRUCTURA DE LOS GRANDES ESTUDIOS DE AUDITORÍA ARGENTINOS

Una de las cuestiones que resulta interesante considerar, y que hace a los resultados obtenidos en esta tesis, se relaciona a la forma en que están estructurados los grandes estudios de auditoría a los que pertenecen los entrevistados y el modo en que los diferentes profesionales participan de los encargos de auditoría financiera.

En los cinco estudios existen al menos dos áreas fuertemente diferenciadas que prestan servicios distintos: auditoría financiera (o *assurance*) y de sistemas (con diferentes denominaciones).

Las áreas de sistemas brindan servicios específicos[22] referidos a procesos informáticos de los clientes, a la vez que prestan colaboración a los auditores financieros. Éstos solicitan su participación para la conformación de los equipos de auditoría, siempre que lo consideren necesario y de acuerdo al entorno de TI del auditado. De esta forma, el *trabajo interdisciplinario* es permanente y se encuentra facilitado por la disponibilidad inmediata de los expertos.

[22] Los servicios incluyen asesoramiento en procesos informáticos; auditorías de proyectos informáticos; auditorías de bases de datos, de interfaces, de sistemas operativos; servicios de laboratorios de computación forense; *hacking* ético y *tests* de penetración; auditorías informáticas especializadas en determinadas industrias (por ejemplo, auditorías especializadas en entidades financieras según la normativa del BCRA) (Entrevistados 1, 3, 7).

Es posible que en otros estudios, estructurados de manera diferente a la descripta, los contadores públicos al momento de realizar una auditoría financiera en entornos de TI complejos deban requerir el acuerdo del cliente para la contratación de especialistas de TI externos que intervengan en el encargo en particular (Entrevistado 5).

5.6.2. IMPORTANCIA DE LA FORMACIÓN DEL CONTADOR PÚBLICO EN TEMAS VINCULADOS A LA TI

Dado el nivel de utilización de la tecnología que presentan las organizaciones en la actualidad, resulta importante que el contador público posea habilidades relacionadas a diversos aspectos vinculados a la TI para poder desarrollar las auditorías de estados financieros. Aun cuando los entrevistados coinciden en que la principal formación que debe tener el auditor financiero, y sobre la que debe profundizar a lo largo de su carrera, es fundamentalmente sobre aspectos contables y de auditoría.

> Sin duda el contador público va a tener que tener conocimiento de sistemas. Si bien es cierto que en definitiva el proceso [de evaluación de la TI] lo termina haciendo la gente de sistemas, al liderar nosotros el proceso de auditoría, somos los que les pedimos que hagan ciertas cuestiones: revisamos y les decimos que cosas tienen que hacer; por lo cual si no entendemos esta nueva herramienta, no vamos a saber que pedirles a ellos o de qué manera pedírselo, porque no vamos a saber leer sus conclusiones. (Entrevistado 8)

Los contadores son los responsables y líderes del proceso de la auditoría financiera, independientemente del entorno tecnológico utilizado para el procesamiento de la información contable. Resulta relevante que comprendan aspectos de la TI dado que *son los dueños del proceso de auditoría externa.* El fin último es emitir una opinión sobre la razonabilidad de la información contenida en los estados contables, y dicha opinión será emitida por el contador público a cargo de la auditoría. Diversos autores respaldan esta postura, como por ejemplo González (2004), Presa (2013) y Rumitti y Falvella (2013); inclusive esta opinión fue anticipada por el Revisor 1.

El auditor evalúa si posee los conocimientos de TI necesarios para ejecutar el trabajo en forma responsable y eficiente o si debe requerir la participación de expertos, desde el inicio del encargo –luego del conocimiento del cliente, para realizar la planificación. Debería ser capaz de comprender en términos generales el entorno tecnológico utilizado por el ente, de modo de identificar los sistemas relevantes para la auditoría financiera, considerando aquellos componentes de los estados financieros y riesgos contables sobre los que se focaliza el trabajo. Si se decide contar con la participación de expertos, además debería indicar cuáles son los requerimientos para la evaluación de los sistemas a fin de obtener información útil, y entender el reporte preparado por los especialistas para determinar el enfoque de auditoría a aplicar (Entrevistados 5, 7, 8).

Los conocimientos requeridos al profesional contable deben *limitarse* a determinadas cuestiones que le permitan cumplir con los objetivos antes mencionados, sin necesidad ni posibilidad de llegar a ser un especialista en estos temas, considerando principalmente los cambios

constantes que se producen en la TI (Entrevistado 5). La carrera contable y la de sistemas son sustancialmente diferentes, y ambas requieren alto nivel de especialización y actualización constante (Entrevistado 1). En consecuencia, el menor nivel de conocimiento del contador para realizar auditorías en estos entornos de TI se verá compensado con una mayor dependencia de los resultados de las auditorías de sistemas (Entrevistado 3).

> Me parece que cada cual debe tener su propio conocimiento y *expertice*. Tratar que un contador tenga los conocimientos para poder evaluar la seguridad de la información, es como que nosotros [auditores de sistemas] nos queramos poner a hacer la evaluación de los estados contables de una compañía. Me parece que no es posible. Hay que trabajar en forma más colaborativa. (Entrevistado 2)

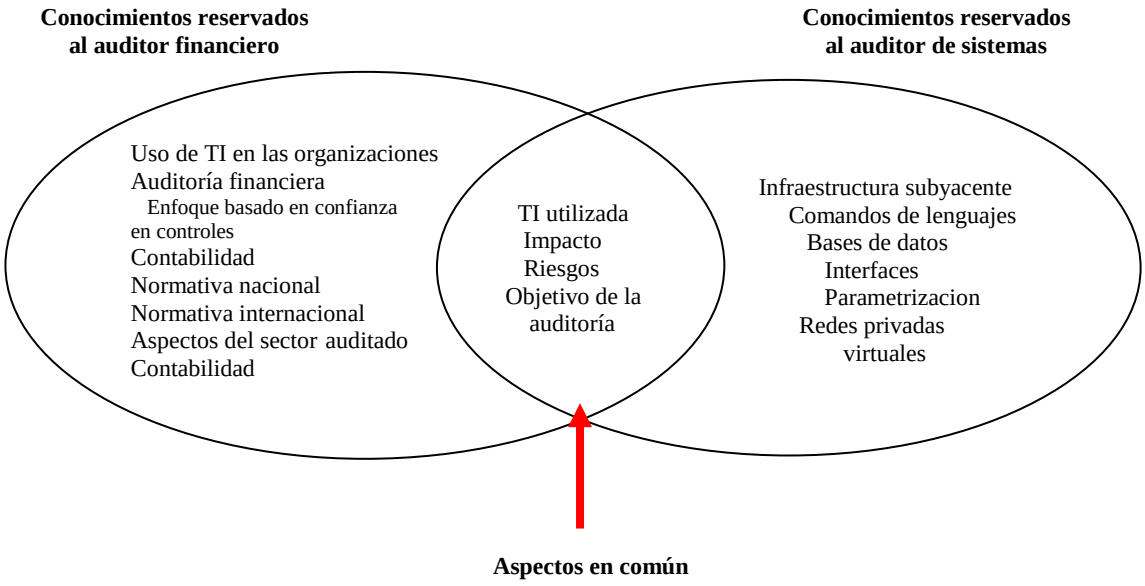
Los entrevistados entienden que los *temas* que deben comprender los auditores financieros son en sí bastante genéricos (Entrevistados 1, 3, 6):

- que es la tecnología (y no como funciona, cuestión relevante para el auditor de sistemas);
- cómo las organizaciones hacen uso de la TI en sus procesos de manera integral (dejando de lado en muchos casos la contabilidad manual);
- los riesgos asociados a la información contable;
- los procesos administrativos involucrados para la elaboración de la información contable mediante los sistemas informáticos, cuestión fundamental para poder desarrollar auditorías en entornos de TI y garantizar una buena comunicación con los auditores de sistemas que los asistan, según se verá en el apartado siguiente;
- y principalmente, cómo todo ello puede definir la aplicación de un enfoque de auditoría basado en la confianza en los controles más que en pruebas sustantivas, principalmente cuando existe un intenso uso de la TI por parte el auditado.

Existen a su vez aspectos que deberán ser comprendidos por ambos profesionales al momento de desarrollar un encargo en un ambiente de TI determinado, como son los riegos, los objetivos del uso de la tecnología por la organización y su posible impacto sobre los procesos. Una vez acordados estos conceptos, cada uno de ellos debería participar del proceso de acuerdo a su especialidad (Entrevistado 1).

En la Figura 8 se grafican las opiniones de los entrevistados, destacando las áreas de incumbencia específica para cada tipo de profesional, así como las áreas en común para garantizar una buena comunicación y comprensión para el adecuado desarrollo de la auditoría.

Figura 8 - Conocimientos requeridos a auditores financieros y de sistemas



Fuente: Elaboración propia.

5.6.3. NECESIDAD DE INTERVENCIÓN DE ESPECIALISTAS EN TI

a) Importancia del trabajo interdisciplinario

Dada la amplia utilización de la tecnología por parte de las empresas auditadas, la imposibilidad de que los auditores contables sean expertos en temas de informática, y la disponibilidad de los auditores de sistemas que existe en los grandes estudios de auditoría, es que, según los entrevistados, siempre que exista un ambiente de TI *resulta fundamental la composición interdisciplinaria de los equipos de auditoría.* El trabajo colaborativo entre profesionales contables y de sistemas debería darse en todo encargo de auditoría en estos entornos, particularmente cuando se complejizan como consecuencia de la tercerización.

> Toda la tercerización tiene más riesgos y ahí es donde veo que una ayuda y un trabajo conjunto es más que aplicable. La nube le sube un grado de riesgo, siendo más necesaria la colaboración entre los profesionales. (Entrevistado 1)

> (…) lo que va a tener que hacer el profesional es descansar más en nuestro trabajo y confiar más. Cuando encuentre que hay una empresa que tiene sus sistemas en la nube va a tener que pedir nuestro trabajo y con base en nuestras conclusiones, él va a tener que realizar su planificación de auditoría. (…) no le va a quedar otra que descansar en nuestro trabajo. (Entrevistado 4)

> En realidad, estos entornos [de TI] los encuentran todos los días, porque hoy no hay compañías que no tenga un sistema. Entonces siempre tienen que involucrar a alguien de sistemas para que de alguna manera les hagan un diagnóstico. (Entrevistado 6)

Según los entrevistados del área contable, la intervención de expertos es una solución natural, no solo para auditorías en entornos de CN, sino para cualquier entorno de TI medianamente complejo. Desde el momento de la planificación de la auditoría se inicia la

interacción con el personal de TI y las conclusiones obtenidas por los especialistas de sistemas son valoradas de manera tal que permiten al auditor financiero definir el enfoque de su auditoría (Entrevistado 7). De hecho, se asimila la situación a otros casos de intervención de expertos en la auditoría financiera, como agrónomos (para la valuación de un silo de cereales), ingenieros (para la valuación de un pozo de petróleo), asesores financieros o abogados. Los entrevistados con formación y experiencia en el área de sistemas refuerzan dicha idea (Entrevistados 1, 4, 5, 6).

Aun cuando se resalta la importancia del trabajo interdisciplinario, parecieran existir dificultades en el proceso de integración de los profesionales, algunas de las cuales ya habían sido mencionadas en el marco teórico. Estas surgieron espontáneamente en las conversaciones mantenidas con los entrevistados; dada la relevancia que otorgaron algunos de ellos a la cuestión, se decide su incorporación en los resultados.

Según el Entrevistado 1, tanto en Argentina como en Latinoamérica (ámbito en el cual posee experiencia), ocurre que en muchos casos no se logra un verdadero trabajo en conjunto con el auditor de sistemas. El Entrevistado 2 –del mismo estudio que el anterior– también considera que si bien en su estudio el trabajo se realiza en conjunto, en muchos casos no existe una verdadera integración. Incluso el Entrevistado 8 menciona que en su firma se realiza un importante trabajo de capacitación para mejorar el trabajo colaborativo.

> Yo creo que todavía falta la interface entre las dos auditorías. Me parece que en algunos casos todavía se hace más por una tendencia que por una verdadera retroalimentación, un verdadero apoyo al proceso... Te digo sinceramente, encuentro muchos casos dónde la auditoría de los sistemas se hace después que se hicieron los estados contables. (Entrevistado 2)

> Hoy una de las cosas que más está costando relacionar es la persona de sistemas con el auditor puro. Esa interrelación cuesta muchísimo; nosotros llevamos mucho tiempo, con mucho entrenamiento para poder lograrlo, pero es un camino para seguir educándonos. Y esto es un paso anterior a la nube, es para los sistemas en general. (Entrevistado 8)

Una descripción de estos obstáculos permite realizar un diagnóstico de la situación actual, destacando diversos puntos que es necesario mejorar por ambos profesionales para alcanzar una mayor eficiencia y eficacia en el desarrollo de las auditorías:

- En algunos encargos, *los auditores financieros no requieren la intervención de los auditores informáticos*, tal vez por desconocimiento o por el intento de desarrollar el encargo en forma independiente. Se esperaría que se les otorgue a estos profesionales una verdadera participación, aprovechando sus conocimientos y habilidades, siendo necesario que los contadores sean capaces de definir sus necesidades e identificar los riesgos del negocio –lo cual resulta complejo para el auditor de sistemas– de modo que puedan brindarles respuestas útiles (Entrevistados 1, 4). Janvrin et al. (2008) habían descripto esta problemática previamente.

> He visto auditores contables que entrevistan y piden directamente la información al personal de sistemas [del auditado] para ver cómo es la tercerización, cómo son las bases de datos, cómo son las normas de programación, los controles de cambios, las puestas en producción, la segregación entre ambientes… hacen el

> relevamiento únicamente, o pretenden hacer la auditoría del marco de control interno informático ellos mismos, pero la realidad es que un buen técnico informático en el cliente los puede engañar. Entonces, la realidad es que la mejor forma es trabajar en equipo. (Entrevistado 1)

Es fundamental la concientización sobre los beneficios de la utilización de los servicios de los profesionales del área tecnológica, con una definición conjunta de las necesidades y objetivos que les permitan obtener una seguridad razonable sobre las características y los riesgos involucrados en la tecnología utilizada por el auditado con impacto en los estados financieros.

- *Los auditores de sistemas deben adaptarse a las necesidades de los auditores contables*, realizando su labor y esforzándose por definir su foco y sus programas en pos del cumplimiento del objetivo del encargo.

Los expertos en TI, además de actualizarse sobre los avances de la tecnología y sus vulnerabilidades, deben comprender el objetivo y el proceso de la auditoría financiera para poder satisfacer las necesidades de los contadores. Deben dejar de pensar en la auditoría de TI específicamente y basarse en la búsqueda de riesgos con impacto contable (Entrevistado 1).

> Yo he visto casos donde auditores informáticos se regocijaron encontrando debilidades tecnológicas, pero que no tenían impacto ni peso material para los estados contables. (Entrevistado 1)

> Muchas veces el auditor informático corre el riesgo de no focalizar y de auditar la tecnología o los sistemas *per se*, para encontrar vulnerabilidades tecnológicas, pero que a veces no tienen impacto grande en los riesgos y en el negocio de la empresa. Se debe tener en cuenta el distinto *scope*: como auditor interno nos interesa los riesgos de la empresa; como auditor contable nos interesa la validez, integridad y credibilidad de lo que está en la información contable, como llegó la información y si es fiable e íntegra al momento en que él va a revisar un estado financiero. Los objetivos de la auditoría de sistemas y de la financiera son distintos. (Entrevistado 1)

Si bien esta crítica no debe generalizarse a todas las auditorías de información contable basadas en tercerización, cabe llamar la atención en este punto. En un entorno como el de la computación en la nube, con sus características y los múltiples riesgos que representa, el verdadero trabajo interdisciplinario y la comprensión del objetivo de la auditoría financiera por parte de los auditores de sistemas es fundamental para el logro del objetivo.

- *Existen dificultades en la comunicación entre los profesionales contables y los de la parte "dura de sistemas",* justificándose en posibles deficiencias en la comprensión de cada uno de ellos sobre el objetivo y el alcance de las tareas del otro (Entrevistados 6, 8). Una dificultad similar fue descripta según Vendrzyc y Bagranoff (2003).

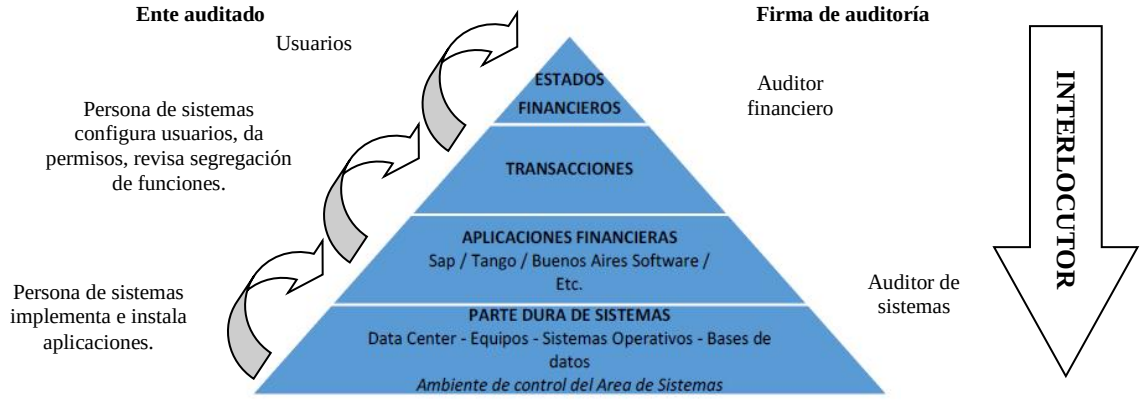
Una solución planteada por los entrevistados es la intervención de un interlocutor; esto es, incluir en el equipo de auditoría un colaborador con una formación tal que le permita actuar como nexo entre ambos.

> Tiene que haber alguien con la suficiente amplitud para moverse sin ser un especialista en sistemas ni en análisis de estados financieros, que pueda ir interpretando las necesidades del equipo de auditores contables y ser su

> interlocutor con el área de sistemas y procesos. Por ejemplo, en el estudio hay un área que es a la que yo pertenezco que se llama "Sistemas y procesos", que lo que hacemos es empezar a dialogar con la gente de sistemas, con la gente de procesos, para poder darle *input* al área más dura de la auditoría que es la de estados financieros. Yo en mis equipos de trabajo tengo ingenieros en sistemas, que los pongo a hablar con un contador y no saben de qué hablar. Entonces es dónde ahí en el medio yo les hago un poco de traductor. (Entrevistado 6)

La Figura 9 expone la situación descripta, imaginando el sistema como una pirámide, donde la información es mantenida en un área de sistemas y procesada por una aplicación; se cargan transacciones y se genera la salida de datos para preparar los estados financieros. Se requiere entonces ese interlocutor que a partir de los estados financieros a auditar sepa definir los requerimientos a quienes están analizando en la base la parte dura de sistemas.

Figura 9 - Intervención de especialistas y necesidades de comunicación



Fuente: Elaboración propia con base en los datos brindados por el Entrevistado 6.

Otra alternativa de solución implementada en el estudio al que pertenecen estos profesionales –que fue mencionada por Borthick et al. (2006)– son los programas de capacitación continua que se dan a nivel corporativo, en los que se fomenta la capacitación de ambos tipos de profesionales en los temas que desconocen y la interacción en los procesos de auditoría.

Siendo este un estudio de carácter exploratorio, quedan expuestas el conjunto de limitaciones planteadas por los entrevistados y que se presentan en el desarrollo de auditorías en los grandes estudios argentinos. Dichas situaciones podrían requerir de un mayor análisis para el planteo de alternativas de solución concretas.

b) Aspectos a destacar respecto de la intervención de auditores de sistemas

Los profesionales resaltaron diversos aspectos en los que el conocimiento específico sobre tecnología que poseen los auditores de sistemas puede potenciar a la auditoría financiera, algunos de los cuales ya han sido referenciados en los capítulos anteriores de esta tesis por tener incidencia en las distintas etapas del proceso de auditoría.

A modo de resumen: el análisis de la necesidad de intervención de expertos en tecnología de la información se realiza desde el inicio del encargo, etapa en que el auditor financiero define el enfoque de auditoría a aplicar (sustantivo o de cumplimiento de controles). Ante la decisión y/o necesidad de depositar confianza en los controles, se requiere la participación de los especialistas del área de sistemas, que son quienes dan seguridad sobre el ambiente tecnológico, debiendo aplicar un enfoque sustantivo cuando según sus evaluaciones aconsejen no depositar confianza en los controles. Finalmente, si no pudieran hacerse las pruebas sustantivas, el auditor financiero debería abstenerse de dar una opinión (Entrevistado 5).

Es decir que, según los profesionales, la intervención es fundamental al momento de realizar la *evaluación del sistema de información, de riesgos y de los controles internos* del ente auditado y de la nube utilizada. En esta etapa, hay dos situaciones que seguramente motivaran su participación:

a) que según el conocimiento obtenido del cliente, sus transacciones se vean fuertemente afectadas por los sistemas informáticos o estos son muy complejos (Entrevistados 5, 6);

b) que el ente auditado este sujeto a normativa de algún organismo de contralor que exija la evaluación del sistema de control interno y la emisión de informes sobre su funcionamiento (como es el caso de la SEC de Estados Unidos) referidos a los controles en los sistemas (Entrevistados 5, 8).

Los conocimientos específicos de los auditores de sistemas facilitan la evaluación de diversos aspectos, incluyendo:

- evaluación del *ambiente de control de TI* (Entrevistado 3);
- evaluación del proceso de *cambios en los programas* (Entrevistado 3);
- verificación del *diseño y funcionamiento de los controles automatizados* (Entrevistado 3);
- determinación de las *vulnerabilidades del sistema informático y de la infraestructura tecnológica* que pudieran afectar la integridad de la información contable (Entrevistado 2);
- análisis de *interfaces entre distintos software* que alimentan al sistema de información contable (Entrevistado 7);
- evaluación de las medidas tendientes a garantizar la *seguridad y confidencialidad de la información contable* (Entrevistado 2);

Otra etapa relevante en este sentido se refiere a la *obtención de evidencias en entornos de TI.* Según mencionó el Entrevistado 1, los conocimientos de los especialistas en sistemas les permitirán obtener evidencias por sí mismos, evitando la intervención de los auditados, lo cual permite superar la falla mencionada en el apartado anterior cuando los contadores públicos buscan hacerlo solos. De esta forma es posible otorgar mayor confiabilidad a la evidencia obtenida (Gramling, Johnstone & Rittenberg, 2012:244; Slosse et al., 2007).

> En la auditoría informática, en lo posible, apuntamos a tomar evidencias reales nosotros mismos, que no sea sólo un cuestionario, y que las pruebas no nos las dé el auditado, sino a sacarlas nosotros del sistema. Y no tiene sentido que un auditor contable aprenda comandos de lenguajes, de bases de datos, de interfaces, de firewall, de redes privadas virtuales, parametrización y todo ese tipo de cosas para poder hacerlo. (Entrevistado 1)

5.6.4. RESUMEN

En la actualidad, prácticamente todas las organizaciones hacen uso de sistemas informáticos para la elaboración de información financiera, con soluciones de mayor o menor complejidad. Es importante que los contadores públicos posean formación en tecnología y procesos administrativos para poder desempeñarse y liderar auditorías financieras en ambientes de TI variados y en permanente cambio.

Se describen diversos aspectos de la TI que deben comprender los contadores públicos, sin perder de vista que su principal formación debe centrarse en cuestiones contables y de auditoría. Entre ellos, deben entender las opciones tecnológicas que podrían utilizar los clientes, la forma en que las empresas las aplican de manera integral en sus procesos administrativos y de qué modo estos se ven afectados por la TI, así como los riesgos derivados de su uso, para poder decidir la conveniencia o no de aplicar un enfoque basado en controles.

Siendo los líderes de los encargos de auditoría, deberán evaluar sus habilidades y decidir la eventual participación de especialistas en sistemas que aporten sus conocimientos y experiencia, principalmente en temas o áreas que superen las posibilidades de formación del profesional contable. En ambientes de TI complejos el trabajo interdisciplinario es considerado fundamental.

Los principales aportes de los auditores de sistemas se refieren a la evaluación del sistema de control interno del ente auditado, necesaria para la definición del enfoque de auditoría. Adicionalmente, colaboran en la obtención de evidencias en forma independiente por parte del equipo de auditoría –sin intervención del auditado–, aumentando la confiabilidad de los elementos de juicio.

Un aporte de este apartado del trabajo es la identificación y descripción de diversas circunstancias que dificultan la verdadera integración de los auditores financieros y los de sistemas, que fueron mencionadas espontáneamente por los entrevistados. Los obstáculos vinculados al trabajo interdisciplinario incluyen la pretensión de los auditores financieros de realizar las auditorías en forma independiente; la falta de adaptación de los auditores de TI a los requerimientos de los auditores financieros; y fallas en la comunicación entre ambos profesionales. Se considera que cada uno de ellos puede ser objeto de un análisis más profundo mediante trabajos de campo que permitan plantear soluciones, considerando que la evolución de alternativas de TI utilizadas por los entes auditados podría requerir en el futuro que se profundice dicha integración.

Si bien en este aspecto la investigación estuvo orientada a la CN en particular, los resultados obtenidos en este apartado parecen ser generalizables a otros entornos de TI.

En el Cuadro 27 se resumen los resultados sobre el tema recientemente desarrollado.

Cuadro 27- Competencias profesionales del auditor externo e intervención de expertos en entornos de TI

TÓPICO	CATEGORÍAS	SUBCATEGORÍAS	
COMPETENCIAS PROFESIONALES DEL AUDITOR. INTERVENCION DE EXPERTOS EN TI	**CONOCIMIENTOS TÉCNICOS DEL AUDITOR**	**Aspectos**	Cuestiones y normativa contable Cuestiones y normativa de auditoría financiera Cuestiones y normativa tributaria Tecnología de información • Sistemas de información • Características de diferentes ambientes de TI • Aplicación de soluciones de TI a los procesos organizacionales • Riesgos de TI asociados a la información contable • Seguridad de la información • Controles internos • Efecto del ambiente de TI sobre el enfoque de auditoría • Procedimientos aplicables en ambientes de TI • Evidencias digitales • Uso de TAACs y herramientas informáticas para la auditoría • Objetivos de la auditoría de sistemas
		Importancia / Utilidad	Comprender el sistema de información del auditado y su influencia sobre EEFF Planificar, dirigir y ejecutar el encargo Poder evaluar riesgos y controles específicos Decidir la necesidad de intervención de expertos • Evaluar la idoneidad del experto • Comunicar objetivos • Evaluar procedimientos aplicados y resultados de la intervención • Interpretar sus informes
	USO DE EXPERTOS	**Factores que lo justifican**	Complejidad de los sistemas Tecnologías emergentes Significatividad de la evidencia digital Conexiones remotas Acceso simultáneo de usuarios Normativa que requiere opinión sobre controles internos afectados por TI
		Aportes	Comprensión del sistema de información Colaboración en la planificación Evaluación de riesgos informáticos Pruebas de funcionamiento de controles Obtención de evidencias digitales en forma independiente Utilización de TAACs Recomendaciones a la gerencia
		Formas de intervención	• Miembros del estudio de auditoría • Experto externo

		Dificultades en la integración	• Poca frecuencia e intensidad en el uso de expertos en TI en la auditoría financiera • Necesidad de adaptación de los expertos en TI a las necesidades del auditor financiero • Problemas de comunicación entre los profesionales

***LECTURA**: Letra azul: elemento nuevo. Letra en otro color: elemento original nombrado con mayor (verde) énfasis en las entrevistas.*

Fuente: Elaboración propia.

6. CONSIDERACIONES FINALES

La computación en la nube es una solución de TI compleja que se está adoptando paulatinamente en diversos aspectos de la actividad empresarial. Académicamente, es incipiente la investigación desde la perspectiva organizacional y escasa desde la auditoría financiera. Ello ha representado una oportunidad para el desarrollo de esta tesis, pretendiendo fortalecer los conocimientos en el área y colaborar en la elaboración de recomendaciones que sirvan de guía para los profesionales al momento de ejecutar encargos de auditoría en la nube.

El objetivo general propuesto para la tesis fue *analizar las particularidades de la auditoría financiera cuando el ente auditado utiliza la computación en la nube en procesos que afectan a la información financiera*. Se plantearon una serie de objetivos específicos a fin de dar cumplimiento al mismo.

El primero consistió en indagar el grado de utilización de la CN por las empresas argentinas. De esta forma fue posible contextualizar la investigación empírica, encontrándose que las organizaciones están optando por utilizar la herramienta para procesos de apoyo –como servicios de correo electrónico, gestión de recursos humanos, almacenamiento de información–, no así para procesos clave del negocio. Pudieron identificarse factores que motivan e inhiben el uso de la CN en el país, según la opinión de los entrevistados. Entre los motivadores se encuentran la disminución de costos relacionados a la TI; ventajas competitivas provistas al área de sistemas; disponibilidad permanente de la información, entre otros. En relación a los obstáculos, se destacaron la desconfianza sobre la confidencialidad y seguridad de la información; las restricciones impuestas por la normativa respecto del tratamiento a dar a la información; el atraso tecnológico tanto de parte de los entes usuarios como de la infraestructura de las telecomunicaciones del país. Ambos grupos podrían ser tenidos en cuenta por los proveedores de servicios y los hacedores de política, para fomentar unos y solucionar los otros, de modo de acelerar el proceso de generalización de uso de la nube.

De acuerdo a las expectativas de los profesionales, aun cuando las organizaciones argentinas se encuentran en un estado preliminar de evaluación e implementación –coincidiendo con estudios previos–, es esperable que su nivel de uso se incremente significativamente, incluso en procesos con influencia en la elaboración de la información con impacto en los estados financieros. De modo que la auditoría contable y la de sistemas deberán adaptarse a estos nuevos entornos, justificando la pertinencia del tema de investigación.

En el planteo del segundo objetivo específico se abordó una etapa relevante de la auditoría, cual es el conocimiento del cliente y su contexto. Ésta fue destacada por los entrevistados como especialmente importante en el ambiente de TI bajo estudio para definir la aceptación o continuidad del encargo de auditoría y la planificación del trabajo. En particular, fue destacada la comprensión

de los sistemas de contabilidad y control interno afectados por la TI en la nube –a través de dos etapas que se denominaron entendimiento en general y en particular– a fin de establecer en qué medida los estados financieros se ven afectados por su uso; la identificación de la información y procesos delegados en la nube, para evaluar su sensibilidad; y la normativa aplicable, restringiendo o regulando el uso de este tipo de servicio. También fue resaltada la importancia de las condiciones de la contratación y relación con la empresa de servicios, a fin de conocer la factibilidad del seguimiento y monitoreo por parte del usuario de los controles internos y las medidas de seguridad y confidencialidad que se aplican sobre su información.

A su vez, pudieron identificarse procedimientos de auditoría necesarios para obtener una adecuada comprensión del auditado y sus sistemas. En este sentido, se evaluó no sólo la conveniencia sino también la factibilidad de ejecución de los mismos, concluyendo que la lectura de documentación relevante vinculada al servicio, las entrevistas al personal del auditado y la obtención de información proveniente del asesoramiento previo brindado al cliente al momento de implementación de la nube, son relevantes y posibles para esta etapa.

El tercer objetivo específico se orientó a la identificación y descripción de factores de riesgo derivados del uso de la computación en la nube. En principio, estos encargos de auditoría no fueron considerados en forma general como más riesgosos que los desarrollados en otros contextos de TI, sino que debe evaluarse cada caso en particular.

Si bien en la literatura se describen una amplia variedad de riesgos de la nube en general, a través de este trabajo se pudieron identificar aquellos considerados por los entrevistados como significativos a los efectos de una auditoría financiera. Fueron destacados: los riesgos técnicos –que pudieran comprometer tanto la disponibilidad como la seguridad y confidencialidad de la información financiera–, requiriéndose la aplicación de adecuadas medidas por parte del usuario y proveedor para gestionarlos; y los riesgos legales –por el eventual marco jurídico desfavorable aplicable según la ubicación de la información y el incumplimiento de normativa aplicable al ente–, que en apariencia no son totalmente controlables por el usuario. Otros factores como los riesgos derivados del proceso de implementación de la CN, los propios de la tercerización y los de seguridad física también fueron discutidos, pero considerados como de menor impacto y/o probabilidad de ocurrencia.

Se propuso una herramienta denominada estructura de desglose de riesgos, un método de identificación de riesgos estructurado que permite el reconocimiento de patrones de exposición a eventos contingentes. En ella se exponen los diversos factores de riesgo de la CN, categorizados de acuerdo a sus fuentes. La exposición jerárquica podría ser útil a los profesionales, facilitando la identificación, comprensión y evaluación de riesgos específicos de contextos de CN.

Posteriormente, dando respuesta al cuarto objetivo específico, se indagó sobre las particularidades de la evaluación del sistema de control interno en entornos de CN para la planificación de la auditoría financiera. En este punto ha sido fundamental el aporte de los

auditores de sistemas. Como peculiaridad de un entorno de tercerización, se destacó que los controles internos a evaluar comprenden tanto los del ente auditado como los del proveedor del servicio en la nube y se identificaron controles clave para los auditores. Desde el punto de vista del proveedor, se incluye al conjunto de controles generales y políticas aplicadas para lograr la seguridad y confidencialidad de la información, gestionando principalmente los riesgos técnicos mencionados anteriormente tales como: ambiente de control; controles de acceso y gestión de usuarios; redundancia y aislamiento de la información; planes de contingencia y recuperación de desastres. Desde la perspectiva del usuario, se deberían analizar las políticas implementadas para el monitoreo de los controles del proveedor del servicio así como la aplicación de una estrategia de resguardo de copias de la información.

Se destacó la limitación que enfrenta el auditor como consecuencia de las restricciones de acceso al proveedor del servicio, concluyendo que incluso cuando la normativa prevé diversos procedimientos para el conocimiento y evaluación del control interno en casos de tercerización, en un entorno de CN la principal alternativa aplicable sería la obtención de informes sobre los controles internos de organizaciones de servicios. Según las preferencias de la mayoría de los informantes, para obtener un nivel adecuado de satisfacción para la planificación de la auditoría, dichos informes deberían ser amplios en cuanto al alcance de los controles evaluados (informes SOC2) y referirse tanto al diseño e implementación como al funcionamiento de los mismos (informes Tipo II).

El quinto objetivo específico estuvo orientado a conocer las particularidades derivadas del proceso de obtención, procesamiento y conservación de las evidencias de auditoría en un entorno de CN. Este no parece ser un aspecto diferencial de la nube respecto a otras alternativas de TI utilizadas por los auditados. En cuanto a la obtención de las evidencias digitales, las técnicas habituales resultarían aplicables, pudiendo solicitarse la información al personal del cliente u obteniendo los datos el propio auditor. En relación a la disponibilidad de la información, una restricción para la auditoría financiera estaría dada por las interrupciones permanentes del servicio o de pérdidas de los datos, pudiendo impedir la ejecución del encargo.

En cuanto al procesamiento y conservación de las evidencias, no se detectaron características específicas relevantes en este entorno de TI, ya que ambos son ejecutados en los sistemas del auditor. Resultan de importancia las medidas preventivas que debe aplicar el profesional para la conservación de copias de las evidencias obtenidas de los sistemas en la nube del usuario en sus papeles de trabajo, teniendo en cuenta el cumplimiento de los plazos previstos por la normativa vigente. Ello en virtud de la necesidad de contar en el futuro con los elementos de juicio y las posibles limitaciones de acceso a los sistemas del proveedor luego de períodos de tiempo prolongados, posteriores a la ejecución del encargo.

Finalmente, se analizaron los conocimientos y habilidades requeridos al contador público para realizar auditorías en entornos de TI, considerando la evolución permanente de opciones

tecnológicas para la elaboración de información con impacto en los estados financieros. Este punto ha sido indicado como importante, en la medida en que los contadores deben ser capaces de liderar los encargos de auditoría financiera. Más aún, teniendo en cuenta "que la formación deficiente de los contadores públicos compromete el interés público poniendo en riesgo de modo directo derechos patrimoniales de los actores sociales", siendo una de las actividades reservadas la de "dictaminar sobre la razonabilidad de la información contable destinada a ser presentada a terceros y efectuar procedimientos de auditoría contable" (Ley 24.521).

La formación del auditor debe orientarse a los diferentes tipos de tecnologías disponibles, el modo en que las empresas las incorporan a sus procesos, los riesgos derivados de ello, y cómo impactan en la decisión sobre la conveniencia de aplicar un enfoque basado en controles en cada caso en particular. En estos entornos se ha comentado además la necesidad de fomentar el trabajo colaborativo con especialistas del área de sistemas, mediante su incorporación en los equipos de auditoría o la contratación como expertos externos, cuando los encargos se realizan en entornos de TI complejos.

Es posible concluir que, aun cuando la investigación estuvo orientada a un tipo de tecnología en particular, cual es la computación en la nube, muchos de los hallazgos de este último objetivo son aplicables a otros contextos de TI.

En conclusión, a través de cada uno de los objetivos específicos se ha podido dar cumplimiento al objetivo general propuesto. Se ha detectado que, en la opinión de los informantes, la CN representa un entorno de tercerización específico para la realización de auditorías de estados financieros con ciertas particularidades que fueron descriptas a lo largo del trabajo. La etapa de planificación –incluyendo el conocimiento del cliente y su entorno, la valoración de riesgos y la evaluación de controles internos– es la que se ve principalmente afectada. En este sentido, los resultados obtenidos coincidieron en general con la bibliografía de referencia. Se han podido ampliar y profundizar aspectos y dificultades para el desarrollo de los encargos que no habían sido tratados específicamente para el entorno de TI analizado.

Este estudio, de carácter exploratorio, no pretende alcanzar una generalización de los resultados obtenidos, sino más bien realizar una contribución al desarrollo de la disciplina de la auditoría de estados financieros, en particular en relación a las tecnologías de la información. En consecuencia, se espera que resulte ser un antecedente útil para profesionales que en el futuro se enfrenten a encargos en entornos de CN.

A su vez, pretende ser un aporte que sirva como disparador de futuras investigaciones científicas y académicas, llevadas a cabo tanto por investigadores como por profesionales con una visión amplia, capaz de contribuir a esta área de conocimiento. A partir del presente trabajo surgen varios interrogantes que se considera pueden motivar futuras líneas de investigación para dar respuestas a los mismos.

En su mayoría, los trabajos sobre auditoría financiera en entornos de TI poseen un enfoque técnico o conceptual. La realización de estudios empíricos, basados por ejemplo en el estudio de casos, podría ayudar a profundizar aspectos que requieran ser investigados y a capitalizar el conocimiento adquirido en el ejercicio profesional de encargos ejecutados en entornos de CN.

Dada la velocidad de avance de la tecnología, se podrían replicar las entrevistas en un lapso de tiempo, por ejemplo cinco años, para detectar la existencia de eventuales cambios, e indagar si se han generado modificaciones en las experiencias adquiridas por los profesionales, que pudieran complementar los resultados de este trabajo. Asimismo sería un aporte a los resultados obtenidos conocer la opinión de otros actores como usuarios y proveedores del servicio de CN.

El hecho de que las entrevistas hayan sido realizadas a auditores pertenecientes a los grandes estudios de Argentina, determina dos cuestiones relevantes: poseen un método de trabajo sistematizado, con una fuerte independencia entre quienes se dedican a la auditoría de los estados financieros y a la de sistemas; y los clientes que auditan en general son empresas medianas o grandes, con ciertas particularidades respecto al uso de tecnologías como la computación en la nube. La realización de estudios de campo con entrevistas a contadores públicos de pequeños estudios de auditoría, donde los clientes son empresas más pequeñas con otro comportamiento de uso de la CN, podría brindar una visión distinta de las consecuencias de su uso sobre el proceso de auditoría.

Según se expuso previamente, es de esperar que en el futuro se produzca una expansión en el uso de la CN por parte de las empresas y que se generalice el desarrollo de auditorías financieras en estos entornos. En la medida en que ello ocurra, sería interesante la generación de un panel de datos que resuma la experiencia de un mayor número de auditores argentinos –incluso de diferentes ciudades y pertenecientes a estudios de distinto tamaño– a partir de cuyo análisis fuera posible la validación de distintas hipótesis. La realización de un estudio cuantitativo de este tipo permitiría complementar y profundizar los resultados aquí presentados.

Finalmente, puede ser necesario profundizar el estudio de las dificultades detectadas en la integración de auditores financieros y de sistemas, de manera tal de desarrollar estrategias para un mejor trabajo colaborativo que permita la realización de auditorías más eficientes y responsables.

REFERENCIAS BIBLIOGRÁFICAS

Abdulelah, A. A.R. (2014). E-Government Based on Cloud Computing and Service-Oriented Architecture. *International Journal of Computer and Electrical Engineering, 6*(3), 201-206.

Agrawal, N. (28/02/2017). Amazon cloud service outage breaks parts of the Internet. *Los Angeles Times.* Consultado el 15/06/2017. Disponible en http://www.latimes.com/business/technology/la-fi-tn-amazon-service-outage-20170228-story.html

Alali, F. A., & Yeh, C. L. (2012). Cloud Computing: Overview and Risk analysis. *Journal of Information Systems, 26*(2), 13-33.

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

American Institute of Certified Public Accountants (2016). Statements on Standards for Attestation Engagements (SSAE) Nro. 18 - Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting.

American Institute of Certified Public Accountants (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., & Beasley, M.S. (2007). *Auditoría. Un enfoque Integral.* (11a ed.). A. G. Valladares Franyuti (Trad.). Mexico: Pearson Education.

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., et al. (2009, febrero). Above the clouds: a Berkeley view of Cloud computing. UC Berkeley Technical Report. Consultado el 06/09/2010. Disponible en http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., et al. (2010). A view of Cloud Computing. *Communication of the ACM, 53*(4), 50-58.

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

Banco Central de la República Argentina (2006). Comunicación A 4609 – Requisitos mínimos de gestión, implementación y control de los riesgos relacionados con tecnología informática y sistemas de información. Consultado el 23/03/2017. Disponible en http://www.bcra.gov.ar/pdfs/comytexord/A4609.pdf

Banco Central de la República Argentina (2008). Comunicación A 4793 - Lineamientos para la gestión del riesgo operacional en las entidades financieras. Texto ordenado. Consultado el 23/03/2017. Disponible en http://www.bcra.gov.ar/pdfs/comytexord/A4793.pdf

Bandeira, R.A. de M. (2009). *Fatores de decisão de terceirização logística : análise baseada na percepção dos executivos* (Tesis doctoral). Universidade Federal do Rio Grande do Sul, Porto Alegre, Brasil. Recuperado de http://hdl.handle.net/10183/17636

Bayramustra N., & Nasir, V.A. (2016). A fad or future of IT?: A comprehensive literature review on the cloud computing research. *International Journal of Information Management, 36*(2016), 635–644.

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

Benítez Palma, E. (2017, septiembre). Blockchain, auditoría pública y confianza. En *XII Encuentros técnicos y VII Foro Tecnológico de los OCEX*, Barcelona, España.

Bierstaker, J.; Chen, L.; Christ, M.; Ege, M. & 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*, *32*(1), 209-250.

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

Böhm, M., Leimeister, S., Riedl, C., & Krcmar, H. (2011). Cloud Computing – Outsourcing 2.0 or a new Business Model for IT Provisioning? En F. Keuper, C. Oecking, & A. Degenhardt (eds.). *Application Management*. *Challenges - Service Creation – Strategies* (pp. 31-56). Alemania: Gabler.

Borthick, A.F., Curtis, M.B., & Sriram, R.S. (2006). Accelerating the acquisition of knowledge structure to improve performance in internal control reviews. *Accounting, Organizations and Society*, 31, 323–342.

Brandas, C., Stirbu, D., & Didraga, O. (2013). Integrated Approach Model of Risk, Control and Auditing of Accounting Information Systems. *Informatica Economică, 17*(4/2013), 87-95.

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

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

Brender, N., & 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.

BSA (2016). 2016 BSA Global Cloud Computing Scorecard. Consultado el 07/05/2017. Disponible en http://www.bsa.org

Budniks, L., & Didenko, K. (2014). Factors determining application of Cloud Computing services in Latvian SMEs. *Procedia - Social and Behavioral Sciences*, 156, 74 -77.

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

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

Cansler, L., Elissondo, L., Godoy, L.A., & Rivas, R. (2007). *Informe 15. Área Auditoría. Auditoría en ambientes computarizados.* Buenos Aires: Federación Argentina de Consejos Profesionales en Ciencias Económicas.

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

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

Casal, A. M. (2011). La identificación y valoración de los riesgos en la auditoría de estados financieros. *Revista Desarrollo y Gestión, XII*(140), 539-550.

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.

Cerullo, M. J. & Cerullo, M. V. (1997). Conducting a financial audit in an automated environment. *Computer Audit Update, 1997*(9), 8-16.

Chow, R., Golle, P., Jakobsson, M., Shi, E., Staddon, J., Masuoka, R., et al. (2009, noviembre). Controlling data in the cloud: outsourcing computation without outsourcing control. En *Actas del 2009 ACM workshop on Cloud computing security,* Nueva York, USA. (pp. 85-90).

Cloud Security Alliance – CSA (2010). Top Threats to Cloud Computing - Version 1.0. Consultado el 17/09/2010. Disponible en http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

Cloud Security Alliance (2011a). Security Guidance for Critical Areas of Focus in Cloud Computing - Version 3.0. Consultado el 28/08/2012. Disponible en https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf

Cloud Security Alliance (2011b). 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 04/12/2012. Disponible en http://www.coso.org/documents/Cloud%20Computing%20Thought%20Paper.pdf

Curtis, M.B., Jenkins, J.G., Bedard, J.C., & Deis, D.R. (2009). Auditors´ training and proficiency in information systems: a research synthesis. *Journal of Information Systems, 21*(1), 79-96.

Deloitte (2016). Blockchain Technology. A game-changer in accounting? Consultado el 27/10/2017. Disponible en https://www2.deloitte.com/content/dam/Deloitte/de/Documents/Innovation/Blockchain_A%20game-changer%20in%20accounting.pdf

Eilifsen, A., Knechel, W.R., & Wallage, P. (2001). Application of the Business Risk Audit Model: A field study. *Accounting Horizons, 15*(3), 193-207.

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.

Español, G., & Subelet, C. (2013). *R.T. Nº37. Normas de Auditoría. Revisión, Otros Encargos de Aseguramiento, Certificación y Servicios Relacionados*. Buenos Aires: Osmar D. Buyatti.

Federación Argentina de Consejos Profesionales de Ciencias Económicas (2001). Código de Ética Unificado.

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

Flick, U. (2009). *An introduction to qualitative research*. (4ta. Ed.). London: Sage

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

Fraser, S. (22/12/2011). The risk-based audit approach. Institute of Chartered Accountants – Australia. Consultado el 24/04/2013. Disponible en http://www.charteredaccountants.com.au/News-Media/Charter/Charter-articles/Audit-and-assurance/2011-07-The-Risk-Based-Audit-Approach.aspx

Freitas, H., & Moscarola, J. (2000). *Análise de dados quantitativos & qualitativos: casos aplicados usando o Sphinx®.* Porto Alegre: Editora Sagra Luzzato.

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

Gomes da Silva, P.A., & Pimenta Alves, P. A. (2001). As novas tecnologías como veículo de transmissao da informaçao financeira. *Contabilidade & Finanzas, 16*(27), 24-32.

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

González A., J.C., & 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,

Gramling, A. A., Johnstone, K. M., & Rittenberg, L. E. (2012). *Auditoría.* (7ma. ed). A. Zoratto Sanvicente (Trad.). San Pablo: Cengage Learning.

Grossman, R.L. (2009). The case for cloud computing. *IT Professional, 11*(2), 23-27.

Guillham, B. (2000). *The researck interview.* Londres:Continuum.

Hayes, B. (2008). Cloud Computing. *Communications of the ACM, 51*(7), 9-11.

Hernández Bravo, Á. (2009). El SAAS y el Cloud-Computing: una opción innovadora para tiempos de crisis. *Revista Española de Innovación, Calidad e Ingeniería del Software, 5*(1), 38-41.

Hernández Sampieri, R., Fernández C., C., Baptista L., P. (2010). *Metodología de la Investigación.* (5ta ed.). México: McGraw-Hill.

Hillson, D. (2002a, octubre). Use a Risk Breakdown Structure (RBS) to Understand Your Risks. En *Actas del Project Management Institute Annual Seminars & Symposium,* San Antonio, Texas, USA.

Hillson, D. (2002b, junio). The Risk Breakdown Structure (RBS) as an aid to effective risk management. En *Fifth European Project Management Conference,* Cannes, Francia. (pp. 1-11)

Holzmann, V., & Spiegler, I. (2011). Developing risk breakdown structure for information technology organizations. *International Journal of Project Management, 29*(5), 537-546.

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

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.

Information Systems Audit and Control Association (2009). Cloud computing – Business Benefits with security, governance and assurance perspectives. White paper. 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 (2011). ITcontrol 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 (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

Inspección General de Justicia (2015). Resolución General 7/2015 – Normas de la Inspección General de Justicia. Consultado el 13/03/2017. Disponible en: http://www.jus.gob.ar/media/2951604/resolucion_general_07-15_actualizada.pdf

International Federation of Accountants (2015). Framework for International Education Standards for professional accountants and aspiring professional accountants. En IFAC (2017), *Handbook of International Education pronouncements,* (pp.5-18). Nueva York: Autor.

International Federation of Accountants (2015). International Education Standard 2 – Initial Professional Development – Technical Competence. En IFAC (2017), *Handbook of International Education pronouncements,* (pp.32-42). Nueva York: Autor.

International Federation of Accountants (2014). International Education Standard 7 – Continuing Professional Development. En IFAC (2017), *Handbook of International Education pronouncements,* (pp.87-97). Nueva York: Autor.

International Federation of Accountants (2016). International Education Standard 8 – Professional Competence for Engagement Partners Responsible for Audits of Financial Statements. En IFAC (2017), *Handbook of International Education pronouncements,* (pp.98-111). Nueva York: Autor.

International Federation of Accountants (2013). Norma Internacional de Auditoría 220 – Control de calidad de la auditoría de estados financieros. En IFAC (2016), *Manual de Pronunciamientos Internacionales de Control de Calidad, Auditoría, Revisión, Otros Encargos de Aseguramiento, y Servicios Relacionados, Edición 2013, Parte I,* (pp.109-124). Nueva York: Autor.

International Federation of Accountants (2013). Norma Internacional de Auditoría 250 – Consideración de las disposiciones legales y reglamentarias en la auditoría de estados financieros. En IFAC (2016), *Manual de Pronunciamientos Internacionales de Control de Calidad, Auditoría, Revisión, Otros Encargos de Aseguramiento, y Servicios Relacionados, Edición 2013, Parte I,* (pp.174-184). Nueva York: Autor.

International Federation of Accountants (2013). Norma Internacional de Auditoría 265 – Comunicación de las deficiencias en el control interno a los responsables del gobierno y a la dirección de la entidad. En IFAC (2016), *Manual de Pronunciamientos Internacionales de Control de Calidad, Auditoría, Revisión, Otros Encargos de Aseguramiento, y Servicios Relacionados, Edición 2013, Parte I,* (pp.205-213). Nueva York: Autor.

International Federation of Accountants (2013). Norma Internacional de Auditoría 300 – Planificación de la auditoría de estados financieros. En IFAC (2016), *Manual de Pronunciamientos Internacionales de Control de Calidad, Auditoría, Revisión, Otros Encargos de Aseguramiento, y Servicios Relacionados, Edición 2013, Parte I,* (pp.214-224). Nueva York: Autor.

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 (2016), *Manual de Pronunciamientos Internacionales de Control de Calidad, Auditoría, Revisión, Otros Encargos de Aseguramiento, y Servicios Relacionados, Edición 2013, Parte I,* (pp.225-266). Nueva York: Autor.

International Federation of Accountants (2013). Norma Internacional de Auditoría 330 – Respuestas del auditor a los riesgos valorados. En IFAC (2016), *Manual de Pronunciamientos Internacionales de Control de Calidad, Auditoría, Revisión, Otros Encargos de Aseguramiento, y Servicios Relacionados, Edición 2013, Parte I,* (pp.275-293). Nueva York: Autor.

International Federation of Accountants (2013). Norma Internacional de Auditoría 402 – Consideraciones de auditoría relativas a una entidad que utiliza una organización de servicios. En IFAC (2016), *Manual de Pronunciamientos Internacionales de Control de Calidad, Auditoría, Revisión, Otros Encargos de Aseguramiento, y Servicios Relacionados, Edición 2013, Parte I,* (pp.294-312). Nueva York: Autor.

International Federation of Accountants (2013). Norma Internacional de Auditoría 500 – Evidencia de auditoría. En IFAC (2016), *Manual de Pronunciamientos Internacionales de Control de Calidad, Auditoría, Revisión, Otros Encargos de Aseguramiento, y Servicios Relacionados, Edición 2013, Parte I,* (pp.322-334). Nueva York: Autor.

International Federation of Accountants (2013). Norma Internacional de Auditoría 620 – Utilización del trabajo de un experto del auditor. En IFAC (2016), *Manual de Pronunciamientos Internacionales de Control de Calidad, Auditoría, Revisión, Otros Encargos de Aseguramiento, y Servicios Relacionados, Edición 2013, Parte I,* (pp. 524-539). Nueva York: Autor.

International Federation of Accountants (2013). Norma Internacional de Encargos de Aseguramiento 3402 – Informes de aseguramiento sobre los controles en las organizaciones de servicio. En IFAC (2016), *Manual de Pronunciamientos Internacionales de Control de Calidad, Auditoría, Revisión, Otros Encargos de Aseguramiento, y Servicios Relacionados, Edición 2013, Parte II,* (pp.90-129). Nueva York: Autor.

International Federation of Accountants (2013). Norma Internacional de Encargos de Aseguramiento 3000 – Encargos de aseguramiento distintos de la auditoría o de la revisión de información financiera histórica. En IFAC (2016), *Manual de Pronunciamientos*

Internacionales de Control de Calidad, Auditoría, Revisión, Otros Encargos de Aseguramiento, y Servicios Relacionados, Edición 2013, Parte II, (pp.67-81). Nueva York: Autor.

IPROFESIONAL (22/08/2014). El tradicional Tango se potencia gracias a la nube de Microsoft en la Argentina. *Iprofesional.com.* Disponible en http://m.iprofesional.com/notas/194435-El-tradicional-Tango-se-potencia-gracias-a-la-nube-de-Microsoft-en-la-Argentina

Islam, S., Fenz, S., Weippl, E., & Mouratidis, H. (2017). A Risk Management Framework for Cloud Migration Decision Support. *Journal of Risk and Financial Management, 10*(2), 10.

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

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

Janvrin, D., Bierstaker, J., & Lowe, J.D. (2008). An examination of audit information technology use and perceived importance. *Accounting horizons, 22*(1), 1-22.

Jericho Forum (2009). Cloud Cube Model. V. 1.0. Consultado el 20/01/2010. Disponible en http://www.opengroup.org/jericho/cloud_cube_model_v1.0.pdf

Joint, A., Baker, E., & Eccles, E. (2009). Hey, you, get off of that cloud? *Computer and security review, 25*(3), 270-274.

Kaufman, L. (2009). Data security in the world of cloud computing. *IEEE Security and Privacy, 7*(4), 61-64.

KPMG (5/4/2012). Effectively using SOC1, SOC 2, and SOC 3 reports for increased assurance over outsourced operations. White paper. Consultado el 08/08/2013. Disponible en http://www.kpmg.com/US/en/IssuesAndInsights/ArticlesPublications/Documents/SOCWhitepaper.pdf.

Krause, M. (1995). La investigación cualitativa - Un campo de posibilidades y desafíos. *Revista Temas de Educación, 7*, 19-39.

Kumar, S., & Goudar, R. (2012). Cloud Computing – Research Issues, Challenges, Architecture, Platforms and Applicatios: A Survey. *International Journal of Future Computer and Communications, 1*(4), 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.

Lakhtaria, K. I. (2011). Protecting computer network with encryption techniques: A study. *International Journal of u- and e- Service, Science and Technology, 4*(2), 43-52.

Ley Nro. 19550. Ley General de Sociedades. Boletín Oficial, Buenos Aires, 25/04/1972. Disponible en http://servicios.infoleg.gob.ar/infolegInternet/anexos/25000-29999/25553/texact.htm

Ley Nro. 24.521. Ley de Educación Superior. Boletín Oficial, Buenos Aires, 10/08/1995. Texto actualizado de la norma disponible en http://servicios.infoleg.gob.ar/infolegInternet/anexos/25000-29999/25394/texact.htm

Ley Nro. 25.326. Habeas data. República Argentina. Boletín Oficial, Buenos Aires, 02/11/2000. Texto actualizado de la norma disponible en http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/texact.htm

Ley Nro. 26.994. Código Civil y Comercial de la Nación. Boletín Oficial, Buenos Aires, 08/10/2014. Texto actualizado de la norma disponible en http://servicios.infoleg.gob.ar/infolegInternet/anexos/235000-239999/235975/texact.htm

Liu, F., Tong, J., Mao, J., Bohn, R., Messina, J., Barger, L., et al. (2011). NIST Special Publication 500-292. NIST Cloud Computing Reference Architecture. Recommendations of the National Institute Standards and Technology. Consultado el 06/08/2013. Disponible en http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909505.

López, M.A. (2012, octubre). Planificación de la Auditoría en un ambiente de Cloud Computing. Evaluación del control interno. *Reunión de Cátedras de Auditoría 2012, La Plata, Argentina.*

López, M.A., & Albanese, D. (2013, agosto). Incidencias de Cloud Computing en la Auditoría Financiera. Particularidades de la evaluación del sistema de control interno. En *Actas de 2das Jornadas Internacionales de Investigación en Organización y Desarrollo Económico y 3eras Jornadas Nacionales de Investigación en Organización y Desarrollo Económico*, San Juan, Argentina.

López, M.A., Albanese, D., & Durán, R. (2013). Auditoría Financiera en Entornos de Computación en la Nube: Revisión del Estado del Arte. *Escritos Contables y de Administración, 4*(1), 109-147.

López, M.A., Albanese, D., & Sánchez, M.A. (2011, septiembre). Identificación de Riesgos vinculados con el uso de Cloud Computing en la Gestión Organizacional.Aplicación de La Risk Breakdown Structure a Entidades Financieras de la República Argentina. En Actas XXXV Encontro da Associação Nacional de Pós-Graduação e Pesquisa em Administração (XXXV EnAnpad), Rio de Janeiro, Brasil.

López, M.A., Albanese, D., & Sánchez, M.A. (2011, diciembre). Identificación de Riesgos en Proyectos de Implementación de Tecnología Cloud Computing en el Contexto de Entidades Financieras. En Actas de 7° Simposio Regional de Investigación Contable, La Plata, Argentina.

López, M.A., Albanese, D., & Sánchez, M.A. (2014). Gestión de riesgos para la adopción de la computación en la nube en entidades financieras de la República Argentina. *Contaduría y Administración, 59*(3), 61-88.

López, M.A., Rummitti, C.A., & Albanese, D. (2013, diciembre). Auditoría financiera en contexto de TI. Análisis de las evidencias digitales. *En Actas de XXX Conferencia Interamericana de Contabilidad*, Punta del Este, Uruguay.

López, M.A., Sánchez, M.A., & Albanese, D. (2010, diciembre). Impacto del uso de Soluciones Informáticas basadas en Cloud Computing para el procesamiento de la Información Contable en la Auditoría Financiera. En *Actas de 16° Encuentro Nacional de Investigadores Universitarios del Área Contable - 6° Simposio Regional de Investigación Contable*, La Plata, Argentina.

López, M.A., Albanese, D., & Durán R. (2015, octubre). Computación en la Nube: Una alternativa de TI para las PyMEs. En Actas XX Reunión Anual de la Red PyMEs Mercosur, Bahía Blanca, Argentina (pp. 203-233).

López H., F., & Salas H., H. (2009). Investigación Cualitativa en Administración. *Cinta de Moebío 35*, 128-145.

Malhotra, N. K. (2011). *Pesquisa de Marketing*. Pearson: São Paulo.

Mansfield, D. S. (2008). Danger in the clouds. *Network security*, *2008*(12), 9-11.

Mantilla Blanco, S.A., & Casal, A.M. (2012 noviembre). Estándares internacionales de Auditoría. Cambios sustanciales y desarrollos recientes. *Revista Desarrollo y Gestión*, *XIII*(158), 1159-1182.

Marino, J.P. (16/06/2014). Subirse a la nube para evitar la tormenta. *Ambito.com.* Consultado el 17/06/2014. Disponible en http://www.ambito.com/diario/noticia.asp?id=745409

Martens, C.D.P. (2009). *Proposição de um conjunto consolidado de elementos para guiar ações visando a orientação empreendedora em organizações de software.* (Tesis doctoral). Universidade Federal do Rio Grande do Sul, Porto Alegre, Brasil. Recuperado de http://hdl.handle.net/10183/15608

McAfee, A. (24/10/2012). Modeling the Costs of Cloud vs. On-Premise Computing. Blog. Consultado el 02/07/2013. Disponible en http://policybythenumbers.blogspot.com.ar/2012/10/modeling-costs-of-cloud-vs-on-premise.html -

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

Mercado (2013 julio). El ranking de los auditores. (pp. 102-104). Consultado el 11/12/2013, Disponible en http://www.mercado.com.ar/notas/carta-del-director/public/documentos/0000041377.pdf

Miller, M. (2008). *CLOUD COMPUTING: Web based applications that change the way you work and collaborate on-line.* USA: Que Publishing.

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

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

Mora, C.A.V., Mauro, J.C., & Villacorta C., A. (2001, noviembre). La auditoría ante operaciones con evidencias virtuales. En *Anales de la XXIV Conferencia Interamericana de Contabilidad*, Punta del Este, Uruguay.

Motahari-Nezhad, H., Stephenson, B., & Singhal, S. (2009). Outsourcing Business to Cloud Computing Services: Opportunities and Challenges. *IEEE Internet Computing*, *10*(4), 1-17.

Mohamed, A. (2009). A history of cloud computing. *Computerweekly.com.* 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*, *6*(1), 132-146.

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

Nearon, B. H. (2005). Foundations in auditing and digital evidence. *The CPA Journal*, *75*(1), 32.

Nicolaou, C. A., Nicolaou, A. I., & Nicolaou, G. D. (2012). Auditing in the cloud: Challenges and opportunities. *The CPA Journal, 82*(1), 66-70.

Noceti, H., & Freijo, A. (2015, agosto). *Cloud Computing. Su aplicación en la banca privada argentina*. En Anales de las *44° JAIIO – Jornadas Argentinas de Informática y STS 2015 - 2º Simposio Argentino sobre Tecnología y Sociedad*, Rosario, Argentina.

Oggero, P. B. (2006, octubre). Riesgos de auditoría y su relación con el trabajo del auditor externo de estados contables en un ambiente de tecnología informática. En *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.

ORACLE (2015). Productos. Enterprise Resource Planning. Consultado el 11/6/2015. Disponible en https://www.oracle.com/applications/enterprise-resource-planning/index.html

ORACLE-MERCADO (2013, agosto). El potencial revolucionario de la "nube" y sus consecuencias. *Revista Mercado*, 176-191.

Pan, G., & Seow, P.S. (2016) Preparing accounting graduates for digital revolution: A critical review of information technology competencies and skills development. *Journal of Education for Business, 91*(3), 166-175.

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

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

Proyect Management Institute (2008). Guía de los Fundamentos para la Dirección de Proyectos (Guía del PMBOK®) (4ta ed). Pennsylvania: Project Management Institute, Inc.

Ragin, C. C, Nagel, J., & White, P. (2004). *The Workshop on Scientific Foundations of Qualitative Research. Reporte.* Virginia: National Science Foundation.

Rao, R. (26/10/2012). Helping SMBs save money with the cloud. Blog. Consultado el 02/07/2013. Disponible en http://googleenterprise.blogspot.com.ar/2012/10/helping-smbs-save-money-with-cloud.html?utm_source=entblog&utm_medium=blog&utm_campaign=Feed:+OfficialGoogleEnterpriseBlog+%28Official+Google+Enterprise+Blog%29

Rapley, R. (2004). Interviews. En: C. Seale et al. (Eds.), *Qualitative research practice* (pp. 15-33). Londres: Sage.

Rech, I. (2012). *O valor da tecnologia da informação nos processos e projetos de co-creação de valor em relacionamentos interorganizacionais*. (Tesis doctoral). Universidade Federal do Rio Grande do Sul, Porto Alegre, Brasil. Recuperado de https://www.lume.ufrgs.br/bitstream/handle/10183/55126/000855101.pdf?sequence=1

Rîndasu, S.M. (2016). Information security – a new challenge for the young and future financial auditors. *Audit Financiar, XIV*(6), (138)/2016,670-679.

RSA (2009, mayo). La función de la seguridad en cloud computing de confianza. Whitepaper. Consultado el 20/11/2012. Disponible en http://www.rsa.com/solutions/business/wp/11021_CLOUD_WP_0209_SP.pdf

Rumitti, C., & Falvella, M. (2013). La Nube – Mitos y Realidades. En C. Slosse (Compilador), *Contabilidad IV. Auditoría*, La Plata: Edulp. Consultado el 8/01/2014. Disponible en http://sedici.unlp.edu.ar/bitstream/handle/10915/30203/Documento_completo__.pdf?sequence=3

Salgado L., A.C. (2007). Investigación cualitativa: diseños, evaluación del rigor metodológico y retos. *Liberabit, 13*, 71-78.

Sánchez H., J., Sálas A., J., & Rodríguez B., C. (2006). Competencias profesionales en la auditoría externa. *Contabilidad y Auditoría*, año 12, nro. 24, 46-63.

SAP (2012). Resumen de la Solución SAP. Soluciones SAP para pequeñas y medianas empresas. Soluciones SAP Business All in One. Consultado el 06/05/2015. Disponible en http://www.sap.com/latinamerica/solution/sme.html.

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

Schultz, J.J. Jr., Bierstaker, J. L., & O´Donell, E. (2010). Integrating business risk into auditor judgement about the risk of material misstatement. The influence of a strategic-systems-audit approach. *Accounting, Organization and Society,* 35, 238-251.

Scutella, J., & Barg, V. (2010, junio). Riesgos de uso de ambientes computarizados. En *Anales del 18° Congreso Nacional del Profesionales en Ciencias Económicas*, Ciudad Autónoma de Buenos Aires, Argentina. Buenos Aires: Buyatti.

Sepúlveda, O. E., Salcedo, O. J., & Gómez Vargas, E. (2010). Manejo del riesgo y seguridad en el consumo de servicios de TI en cloud computing. *Redes de Ingeniería, 1*(2), 10-21.

Singleton, T.W. (2011). Cómo el auditor de TI puede hacer contribuciones sustanciales a una auditoría financiera. *ISACA Journal*, 1, 1-3.

Slosse, C. A., Gordicz, J. C., & Gamondés, S. F. (2007). *Auditoría* (1era ed.). Buenos Aires: La Ley.

Sobragi, C.G. (2012). *Cloud computing adoption: a multiple case study*. (Tesis de maestría). Universidade Federal do Rio Grande do Sul, Porto Alegre, Brasil. Recuperado de http://hdl.handle.net/10183/99410

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

Sultan, N. A. (2011). Reaching for the "cloud": How SMEs can manage. *International Journal of Information management*, 31, 272-278.

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

Tarmidi, M., Rasid, S.Z.A.R., Alrazi, B., & Roni, R. A. (2014). Cloud Computing awareness and adoption among accountings practitioners in Malaysia. *Procedia- Social and Behavioral Sciences*, 164, 569-574.

Taylor, S.J., & Bogdan, R. (1987). *Introducción a los métodos cualitativos de investigación.* J. Piatigorsky (Trad.). Buenos Aires: Paidós.

Taylor, M., Haggerty, J., Gresty, D., & Hegarty, R. (Mayo 2010). Digital evidence in cloud computing systems. *Computer law & security review, 26*(3), 304-308.

Taylor, M., Haggerty, J., Gresty, D., & Lamb, D. (2011). Forensic investigation of cloud computing systems. *Network Security, 2011*(3), 4-10.

Tsidulko J. (27/07/2016). The 10 Biggest Cloud Outages Of 2016 (So Far). *CRN*. Consultado el 14/06/2017. Disponible en http://www.crn.com/slide-shows/cloud/300081477/the-10-biggest-cloud-outages-of-2016-so-far.htm

Tucker, G.H. (2001). IT and the Audit. *Journal of Accountancy, 192*(3), 41-43.

USUARIA – Asociación Argentina de Usuarios de la Informática y las Comunicaciones (Enero 2014). Crece la adopción de Cloud Computing. Informe anual elaborado por la división Usuaria Research.

USUARIA – Asociación Argentina de Usuarios de la Informática y las Comunicaciones (Enero 2013). Cloud Computing en empresas argentinas. Informe anual elaborado por la división Usuaria Research.

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

Valles, M.S. (1999). *Técnicas cualitativas de investigación social*. Madrid: Editorial Síntesis.

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

Vázquez, R., Bongianino de S., C., Sosisky, L., & Albano, H.R. (2006). Modelización del esquema de investigación en contabilidad. En E. Scarano et al. (2006). *Metodología de la Investigación Contable*, Buenos Aires: Universidad de Buenos Aires.

Vendrzyk, V. P., & Bagranoff, N. A. (2003). The evolving role of IS audit: A field study comparing the perceptions of IS and financial auditors. *Advances in Accounting,* 20, 141-163.

Vîlsanoiu, D., & Şerban, M. (2010). Changing methodologies in financial audit and their impact on information systems audit. *Informatica Economică, 14*(1), 57-65.

Weiss, R.S. (1994). *Learning from strangers: the art and method of qualitative interview studies.* Nueva York: The Free Press.

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

Yigitbasioglu, O., Mackenzie, K., & 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.

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

ANEXOS

ANEXO 1 – Revisiones por especialistas al instrumento de recolección de datos.

REVISOR	RECOMENDACIONES Y CORRECCIONES
Revisor 1	**1.** Se redujo la cantidad de conceptos teóricos introductorios a cada una de las preguntas, considerando que se estaba tratando con profesionales que conocen en detalle el proceso de auditoría financiera. **2.** Se simplificó y resumió la redacción de algunas preguntas que no eran comprendidas de inmediato por el revisor, por ejemplo por su extensión. **3.** Se simplifico la pregunta general en la que se consulta sobre los potenciales efectos de la CN sobre la auditoría financiera, a fin de focalizar la entrevista sobre los aspectos específicos que se plantean en la investigación. Se agregó al final de la entrevista una pregunta de cierre en la que se consulta si el profesional cree que es necesario indagar algún aspecto que no hubiera sido tratado durante el transcurso de la conversación. **4.** En relación a la evaluación de riesgos, se decidió no solicitar una calificación en cuanto a impacto y probabilidad para cada factor de riesgo (alto/medio/bajo), dado que según el Revisor 1 esto requeriría ser aplicado a una nube en particular, y en una situación de uso por parte de una organización, siendo muy complejo evaluarlo en abstracto. En reemplazo, se definió una pregunta en la que se solicita que dentro de las fuentes de riesgos definidas a partir de la bibliografía, se identifiquen aquellos factores de riesgo relevantes que necesariamente deberían ser evaluados en una auditoría de estados financieros, con la justificación de la respuesta. Asimismo, la evaluación del nivel en que la "auditabilidad" de un ente usuario de la CN podría verse comprometida se consideró de difícil evaluación en el contexto de una entrevista de este tipo. **5.** Respecto del bloque de preguntas referido a la evaluación del sistema de control interno, fue necesario reducir la cantidad de preguntas y la cantidad de información y conceptos incluidos. Considerando la opinión del Revisor 1, se decidió consultar cuáles son los principales efectos del uso de la CN sobre esta etapa; qué controles internos relevantes para la auditoría financiera deberían ser evaluados y se esperaría encontrar en este entorno; procedimientos a ser aplicados para el relevamiento y evaluación de controles internos. Se agregaron preguntas específicas referidas a los tipos de informes de control interno emitidos por auditores independientes (tipo de informe pretendido, características del SOC2 relevantes para el auditor financiero, estándares para la elaboración del informe, caso de subcontratación por parte del proveedor). Se evitaron las opciones que podrían inducir las respuestas de los entrevistados. **6.** En relación a las preguntas sobre evidencias digitales de auditoría en un entorno de CN, se incorporó una pregunta general y se mantuvieron preguntas referidas a la obtención, procesamiento y conservación de las evidencias, tal como se plantea en el marco teórico. **7.** Finalmente, respecto de las competencias profesionales y el uso de expertos, se consideró adecuado consultar no solo cuales son los conocimientos requeridos a los profesionales de ciencias económicas, y la forma en que los expertos en sistemas pueden colaborar, sino también cual es el estado actual del conocimiento y si los profesionales están en condiciones de realizar auditorías en estos entornos. **8.** Las preguntas de cierre fueron consideradas adecuadas.
Revisor 2	**1.** Debido al carácter técnico del tema, propuso que deberían ser incorporados en la investigación auditores especializados en sistemas, dado que resulta necesario entrevistar personas con conocimientos amplios sobre la TI (R2) y a fin de evitar respuestas que lleven a confusión en los resultados. En consecuencia se decidió incorporar estos profesionales entre los entrevistados. **2.** Consideró adecuado estructurar la entrevista de modo de medir, desde un inicio, el conocimiento y la experiencia que posee el auditor de la modalidad de la Computación en la Nube y el conocimiento de la normativa involucrada. Esto permitiría medir el nivel de

	conocimiento y la relevancia de la opinión del entrevistado. Se incorporaron preguntas iniciales sobre la experiencia de los entrevistados en relación al uso y a la ejecución de auditorías en entornos de tercerización de TI, en particular computación en la nube (atención de clientes que fueran usuarios), que permitieron determinar su familiaridad con la tecnología y el nivel de utilización de estas alternativas por sus clientes. **3.** Propuso utilizar preguntas cerradas a fin de facilitar la tabulación y análisis de los resultados, debido a que la dispersión de opiniones o el desconocimiento del tema podría llevar a conclusiones no del todo válidas. A su vez consideró la posibilidad de realizar una encuesta utilizando una herramienta en la nube, como formularios on-line, para realizar preguntas cerradas, y una entrevista posterior para preguntas abiertas. Considerando la definición de la investigación como exploratoria y cualitativa, y pretendiendo utilizar entrevistas en profundidad, se entendió que sería mejor mantener la opción de preguntas abiertas para obtener la opinión y experiencia de los entrevistados. Además dada la dificultad de obtener la participación de profesionales en la investigación, se prefirió reducir el nivel de intervención de los mismos a una sola entrevista. **4.** En relación al instrumento, fue considerado adecuado en cuanto a extensión, temas tratados, estructura de los temas. Se realizaron algunas modificaciones en cuanto al orden de algunas preguntas, así como la eliminación de otras que resultaban demasiado técnicas y que no podrían ser respondidas por profesionales sin conocimientos específicos o que no aportaban al objetivo de la investigación.
Revisor 3	**1.** En general consideró adecuada la variedad de aspectos a ser tratados (elaborados a partir del esquema teórico planteado) y la disposición general de los temas en el instrumento de recolección de datos, salvo alguna excepción comentada a continuación. **2.** En algún caso se propuso la modificación de la redacción para lograr una mejor comprensión por parte de los entrevistados. **3.** Se eliminaron las opciones o ejemplos, dado que se entendió que podrían sesgar las respuestas de los entrevistados o que estos se limitarían a responder respecto de los aspectos allí planteados, lo cual iría en contra del diseño exploratorio de esta tesis. Las preguntas se plantearon como abiertas, a fin de obtener la información directamente de los entrevistados, según su conocimiento y experiencia, sin motivarlos a responder en un sentido en particular. Los ejemplos solo serían utilizados en caso de ser necesaria alguna aclaración en particular. **4.** En cuanto a la estructura del guion, se decidió separar las preguntas referidas a "conocimiento del cliente y su entorno" e "identificación y valoración de riesgos" en bloques distintos. **5.** Para la evaluación de los riesgos de la nube con impacto en la auditoría financiera, considerando que los factores son muchos y puede hacerse difícil la evaluación en medio de una conversación, el revisor propuso que se mencionen por fuente de riesgo (considerando las definidas en la RBS planteada en el marco teórico) y que la evaluación se haga para cada conjunto de factores, ejemplificando en todo caso los que incluye cada fuente. Esto ayudó a simplificar el planteo de esta cuestión a los entrevistados, orientarlos sobre diferentes aspectos a ser tenidos en cuenta y obtener respuestas más concretas. **6.** Respecto de la evaluación de controles internos en entornos de TI, se debió simplificar más aun la cantidad y profundidad de las preguntas planteadas luego de las consideraciones del Revisor 1, porque el bloque era demasiado extenso, restando importancia y tiempo a los demás. Se modificaron las preguntas a fin de que fuera más equilibrado con el resto del guion. **7.** Propuso la utilización de herramientas (como matrices de riesgos, el cuestionario escrito para entregar a los entrevistados, entre otras) para facilitar el desarrollo de la entrevista. Las mismas fueron diseñadas para uso del entrevistador a fin de guiar la conversación, pero no fueron utilizadas en el desarrollo de las mismas, dado que fueron realizadas vía Skype o telefónicamente, evitándose la anticipación del contenido del cuestionario a los entrevistados. **8.** Comentó que podría ser útil enviar previamente el instrumento de recolección de datos a los entrevistados, a fin de optimizar el resultado de las entrevistas, considerando la complejidad del tema tratado, si bien algunos profesionales podrían arrepentirse de

	participar al recibirlo previamente. Al momento de efectuar la recolección de datos en el campo, en principio se evitó enviar el guion a los profesionales. Cuando fue solicitado por los entrevistados para evaluar si estaban en condiciones de participar de la investigación o si era preferible recomendar otro profesional, se envió únicamente un listado de temas a tratar. **9.** Mencionó que a fin de poder dar respuesta a algunas preguntas, el entrevistado debería tener conocimientos muy específicos sobre tecnología de la información. Esto hizo plantear la posibilidad de entrevistar no solo a auditores de estados financieros, sino también a auditores de sistemas, en forma similar a lo planteado por el Revisor 2.

ANEXO 2 – Modificaciones al instrumento de recolección de datos derivadas de los estudios piloto.

1. Estructura general del instrumento

- Se redujo la cantidad de definiciones utilizadas en el planteo de las preguntas para su simplificación, dado que siendo expertos en los temas tratados, no necesitaban mayores aclaraciones.

2. Experiencia de los entrevistados

- Se confirmó la importancia de esta pregunta a fin de poder analizar los resultados a la luz de la experiencia y los conocimientos demostrados. A su vez, permitía basar el resto de la entrevista en la respuesta obtenida en esta instancia.
- Siendo que se abordaban en este punto los usos que las empresas hacen de la CN, se decidió preguntar cuales consideraban que tienen potencial impacto en la auditoría de estados financieros, para no retomar el tema en el apartado de conocimiento del cliente.

3. Conocimiento del cliente

- Se excluye una pregunta específica referida a los modelos de prestación de servicios en la nube, dado que si bien es considerada relevante por los profesionales, forma parte de la pregunta general de aspectos a ser conocidos por el auditor en esta etapa.
- Se incluye una pregunta para evaluar en qué medida el sistema de información del ente auditado se vuelve más complejo (o no) por el hecho de que se utilice un servicio de tercerización basado en la nube. La complejidad del sistema de información es un aspecto a ser abordado en esta etapa de la auditoría.

4. Identificación y Valoración de riegos de la CN para la auditoría financiera

- Se decidió separar el bloque de preguntas referido a este aspecto de la planificación de la auditoría, dado que es sumamente relevante en un entorno de TI como el estudiado, y podría obtenerse información valiosa en relación al mismo.
- Se utilizó la opción definida con el Revisor 2, haciendo las preguntas basadas en las fuentes de riesgos identificadas, concluyendo que es una alternativa viable.

5. Evaluación del sistema de control interno en la nube

- Se decidió disminuir la cantidad y profundidad de las preguntas, dado que por el nivel de conocimiento de los entrevistados ellos mismos cubrían en sus respuestas los diferentes temas.
- Se redujeron a cuatro aspectos en relación con la auditoría financiera: efectos generales de la CN sobre la evaluación del control interno; controles internos relevantes en estos ambientes; procedimientos para conocer y evaluar el sistema de control interno del ente; particularidades de los informes de control interno del proveedor del servicio emitidos por auditores independientes.

6. Evidencias digitales de auditoría en un entorno de CN

- Se confirmó que las preguntas resultaban adecuadas a los fines de la investigación.

7. Competencias profesionales y participación de expertos

- Se corroboró la pertinencia de las preguntas para los fines del estudio. Los entrevistados mostraron interés en expresarse al respecto.

ANEXO 3 - Instrumento de recolección de datos.

AUDITORÍA FINANCIERA EN ENTORNOS DE COMPUTACIÓN EN LA NUBE

INSTRUMENTO DE RECOLECCIÓN DE DATOS

Entrevista Nro.: _____

Entrevistado:_____ Estudio: _____

Fecha: _____ Hora de inicio: _____ Medio: _____

Introducción: Descripción general de la investigación: objetivo, participantes elegidos, razón por la cual fueron seleccionados, utilización de los datos.

Características de la entrevista: Confidencialidad, necesidad de grabarla, duración aproximada.

Perfil del entrevistado: A fin de definir un perfil de los entrevistados, ¿podría comentar brevemente su trayectoria en cuanto a su formación y profesión? (Formación / Cargo actual / Tiempo de actuación en su cargo)

Experiencia en relación a la Computación en la Nube

- **Uso personal:** En el desarrollo de su labor, ¿ha tenido la posibilidad de utilizar algún servicio basado en la nube? ¿Cuál ha sido su experiencia?
- **Uso por clientes:** ¿Conoce si las empresas con las que trabaja su estudio utilizan o están evaluando utilizar servicios de tercerización de TI, en particular a través de soluciones de computación en la nube? ¿Qué alternativas han implementado? ¿Cuáles de ellas serían relevantes para la auditoría financiera, requiriendo especial atención del auditor? ¿Por qué?

A) PREGUNTAS

A. CONOCIMIENTO DEL CLIENTE AUDITADO Y SU ENTORNO: Un primer paso en la etapa de planificación de la auditoría consiste en lograr un conocimiento integral del negocio del ente auditado y su entorno. En este momento el profesional toma conocimiento del uso de la CN que realiza el cliente. Considerando los diversos usos que el ente auditado puede hacer de los servicios de CN relevantes para la auditoría financiera:

1. ¿Qué **aspectos** del uso del servicio en la nube buscaría conocer Ud. para lograr una adecuada comprensión del sistema de información del ente auditado en esta etapa inicial?

2. ¿Qué **procedimientos** de auditoría considera, según su experiencia, pueden ser utilizados para profundizar en el conocimiento de los aspectos mencionados en el punto anterior y cuáles no? ¿Por qué?

3. En la etapa de conocimiento del cliente el auditor evalúa la **complejidad del sistema de información del ente**. ¿El uso de la CN supone un factor que incrementa dicha complejidad? ¿Por qué?

B. IDENTIFICACIÓN Y VALORACIÓN DE RIESGOS: Una vez logrado el adecuado conocimiento del ente, el auditor debe realizar la identificación y valoración de riesgos significativos para la auditoría, esto es, aquellos que requieren especial consideración porque podrían generar distorsiones significativas en los estados financieros.

4. Considerando las siguientes categorías de **factores de riesgo** que representa el uso de la CN, ¿cuáles de ellos identificaría como significativos para la auditoría financiera, considerando su probabilidad de ocurrencia e impacto? ¿Por qué?

FUENTES DE RIESGOS	FACTORES DE RIESGO
RIESGOS DEL PROCESO DE IMPLEMENTACIÓN	Falta de planificación en el proceso de implementación
	Actividad no autorizada en la nube
	Falla en la adecuación de la estructura organizacional
RIESGOS DERIVADOS DE LA TERCERIZACIÓN	Pérdida de gobernabilidad por parte del usuario
	Viabilidad del proveedor
	Vinculación al proveedor (*Lock in*)
	Falta de transparencia
	Incumplimiento de requisitos de certificaciones
	Reputación compartida
RIESGOS TÉCNICOS	Insuficiencia de recursos (sub-aprovisionamiento)
	Fallas de la conexión a Internet: vulnerabilidades de la red
	Fallas de los mecanismos de aislamiento de la información
	Empleado malicioso
	Fuga/Interceptación de datos en tránsito
	Eliminación de datos insegura o no efectiva
	Acceso a través de navegadores de Internet conocidos
	Problemas de gestión de la identidad y claves de encriptado
RIESGOS LEGALES	Cambio de jurisdicción
	Determinación de la autoridad competente en caso de conflicto
	Confiscación judicial
	Requisitos de los sistemas de información
	Revelación de cuestiones sobre controles internos
	Protección de datos y confidencialidad
	Protección de la propiedad intelectual
RIESGOS CONTRA LA SEGURIDAD FÍSICA	Acceso físico no autorizado a instalaciones y edificios
	Desastres naturales

5. Teniendo en cuenta sus respuestas sobre la evaluación del riesgo de auditoría, ¿considera Ud. que el uso de la CN representa o no un **escenario de mayor riesgo** que otros casos de tercerización del servicio de TI? ¿Por qué?

C. EVALUACIÓN DEL SISTEMA DE CONTROL INTERNO: Una vez identificados los riesgos significativos, el auditor debe evaluar los controles internos de la entidad para mitigarlos. En entornos de la nube, dichos controles dependen no solo del ente auditado, sino también del sistema de control interno propio del proveedor del servicio.

6. ¿Qué efectos podría tener el uso de un servicio tercerizado como la CN sobre la evaluación del sistema de control interno (SCI) en la auditoría financiera?

7. ¿Qué **controles internos relevantes** para la auditoría financiera esperaría encontrar en un entorno de este tipo de acuerdo a los factores de riesgo identificados?

8. Según su experiencia en entornos en donde existiera tercerización de las actividades de TI, ¿Qué **procedimientos** es posibles aplicar para conocer y evaluar el sistema de control interno? ¿Qué dificultades han encontrado en casos similares?

8.1. Informes sobre el control interno del proveedor del servicio emitido por auditor independiente

- ¿Qué alternativas de las disponibles podría satisfacer las necesidades del auditor financiero? ¿Por qué?
- ¿Sería adecuado que el auditor del servicio utilizara un estándar de control interno específico referido a la CN para la elaboración de un informe a ser provisto al usuario y su auditor financiero? ¿Por qué?

- ¿El informe debería basarse preferentemente en el método *inclusive* o *carved-out* en caso de subcontratación por parte del proveedor del servicio en la nube?

D. EVIDENCIAS DE AUDITORÍA: Las evidencias de auditoría obtenidas en un entorno de CN son un caso particular de evidencias digitales de auditoría.

9. ¿Qué efectos puede tener el uso de la CN sobre las evidencias de auditoría digitales obtenidas de dicho entorno?

10.¿Cómo considera que se ve afectada la **obtención** de evidencias en un ambiente de CN?

- ¿Es posible aplicar las **Técnicas de Auditoría Asistidas por Computadora** utilizadas en los entornos de TI tradicionales? ¿Que técnicas deberá aplicar el auditor para su obtención?
- ¿El uso de la CN puede afectar la **disponibilidad** de la información financiera para la obtención de evidencias?
- ¿El uso dela CN puede afectar la **fiabilidad** de las evidencias?

11.¿Considera que la CN introduce modificaciones en el **procesamiento** de los datos relacionados a las afirmaciones contenidas en los estados contables una vez que estos han sido obtenidos? ¿Cuáles?

12.¿Qué particularidades podría introducir el uso de la CN en relación con la **conservación** de las evidencias y los papeles de trabajo?

E. COMPETENCIAS PROFESIONALES Y PARTICIPACIÓN DE EXPERTOS: En principio, el auditor que ejecuta un encargo en cualquier ambiente de TI debe poseer un conjunto de habilidades especiales que le permitan desarrollar su trabajo, o en su caso evaluar la necesidad o conveniencia de contar con el asesoramiento de un experto en la materia y utilizar su trabajo en forma responsable y diligente.

13.¿Cuáles considera Ud., según su experiencia, que deberían ser los **conocimientos y habilidades específicas que debiera poseer un contador público** para realizar un encargo de auditoría en un entorno de CN?

14. PARTICIPACIÓN DE EXPERTOS: Dadas las particularidades que representa un entorno de tercerización de TI para la auditoría financiera:

- ¿Considera Ud. que es conveniente contar con la colaboración de un experto en el área de sistemas para realizar una auditoría de este tipo? ¿Por qué?
- ¿De qué manera son incorporados los expertos en el trabajo de auditoría financiera?
- De acuerdo a los encargos en los que ha participado, ¿en qué aspectos de la auditoría financiera colabora un auditor de sistemas en entornos de este tipo?

F. APORTES ADICIONALES

15.¿Le gustaría realizar algún aporte adicional?

16.¿Cree que existe alguna cuestión sobre la que no hemos conversado que debería ser tenida en consideración?

17.¿Podría indicar algún profesional (de su estudio u otro) que estuviera en condiciones de realizar aportes a la investigación mediante una entrevista?

CIERRE

Hora de finalización:

ANEXO 4 – Modelo de carta de contacto con intermediarios de los estudios de auditoría.

Bahía Blanca, … de …. de 20…..

UNIVERSIDAD NACIONAL DEL SUR

TESIS - DOCTORADO EN CIENCIAS DE LA ADMINISTRACIÓN

Estimado ……,

Mi nombre es María de los Ángeles López. Soy docente de la Universidad del Sur (UNS, Bahía Blanca, Argentina) y becaria del CONICET.

Me dirijo a Ud. a fin de invitarlo a participar de una investigación que me encuentro realizando para completar mi trabajo de tesis para acceder al título de Doctora en Ciencias de la Administración en la UNS.

La misma tiene por objetivo analizar las particularidades de la auditoría financiera cuando el ente auditado utiliza la computación en la nube en procesos que afectan a la información contable, a partir de la opinión y experiencia de profesionales pertenecientes a los principales estudios de auditoría de la República Argentina.

Es así que quisiera proponerle a Ud. y otros miembros del estudio …… participar de una entrevista, en la que podamos conversar sobre algunas cuestiones relacionadas al tema de investigación, a fin de garantizar la representación del estudio en la muestra del trabajo.

En caso que considere posible colaborar, ya sea participando de una entrevista o contactándome con otros miembros de ……, le solicito me lo haga saber a fin de brindarle mayores detalles.

Su colaboración será fundamental para poder concretar mi investigación.

Desde ya agradezco su atención y quedo a la espera de sus noticias.

Cra. María de los Ángeles López
Universidad Nacional del Sur - Departamento de Cs. De la Administración
Campus Palihue - San Andrés 800 Tel. 0054-291/4595132/33/34 (int. 2509)
E-mail: angeles.lopez@uns.edu.ar
(8000) Bahía Blanca
Buenos Aires
República Argentina

ANEXO 5 – Modelo de carta de invitación a los profesionales.

Bahía Blanca, … de …. de …..

UNIVERSIDAD NACIONAL DEL SUR

TESIS - DOCTORADO EN CIENCIAS DE LA ADMINISTRACIÓN

Estimado/a ……..,

Por medio de la presente, y en relación al contacto iniciado por el Dr. ……..…., pretendo brindarle mayores detalles sobre la investigación que me encuentro realizando para la elaboración de una tesis de Doctorado en Ciencias de la Administración de la Universidad Nacional del Sur (UNS, Bahía Blanca, Argentina).

El objetivo general de la tesis consiste en *analizar las particularidades de la auditoría financiera cuando el ente auditado utiliza la computación en la nube en procesos que afectan a la información contable.*

El estudio comprende la realización de entrevistas a profesionales que pertenezcan a los grandes estudios de auditoría de nuestro país, considerando que pueden realizar aportes interesantes a la investigación debido a la vasta experiencia que hubieran obtenido desarrollando su labor en estos estudios y considerando la variedad e importancia de las empresas con que se encuentran vinculados.

Las entrevistas serán guiadas mediante preguntas abiertas a través de las cuales se pretende orientarlo a fin de conocer su opinión y experiencia respecto de los temas que nos interesa analizar.

Se pretende conocer la opinión de los entrevistados, de modo que no habrá respuestas correctas o incorrectas. La información obtenida será utilizada únicamente para fines académicos y será analizada en conjunto con los datos obtenidos de otros profesionales. Es política de las investigaciones académicas la estricta confidencialidad de la información obtenida.

Me interesaría poder contactarme con Ud. a fin de conocer si es posible que participe de la investigación en representación del estudio al cual pertenece, siendo fundamental la colaboración de los profesionales para la realización de este trabajo.

Esperando contar con su participación, saludo a Ud. atentamente,

Cra. María de los Ángeles López
Universidad Nacional del Sur - Departamento de Cs. De la Administración
Campus Palihue - San Andrés 800 Tel. 0054-291/4595132/33/34 (int. 2509)
E-mail: angeles.lopez@uns.edu.ar
(8000) Bahía Blanca
Buenos Aires
República Argentina