CIRCULAR DE AUDITORÍA N° 34

2015

APROBACIÓN DE LA COMISIÓN DE AUDITORÍA

Esta Circular de Auditoría ha sido preparada por la Comisión de Auditoría del Colegio de Contadores de Chile A.G. y fue aprobada con el voto unánime de todos sus miembros.

Los miembros de la Comisión de Auditoría que participaron en la preparación de esta Circular de Auditoría, son los siguientes:

Jesús Riveros G.
Presidente

Víctor Aguayo H.
Alejandro Espinosa G.
Jaime Goñi G.
Edgardo Hernández G.
Hans Caro L.

Álvaro Leiva C.
Miguel Sapag P.
José Salas A.
Hernán Quililongo C.
Roberto Villanueva B.

Miller Templeton M.
Director Técnico

Sergio Mercado P.
Gerente Técnico

APROBACIÓN DEL HONORABLE CONSEJO NACIONAL

La presente Circular de Auditoría Nº 34 fue aprobada por el Honorable Consejo Nacional del Colegio de Contadores de Chile A.G., en su sesión ordinaria del día 24 de septiembre de 2015, de acuerdo a las atribuciones contenidas en el Artículo Nº 13.11 del Estatuto del Colegio (Art. 13°, letra (g) de la Ley Nº 13.011), y acordó hacer obligatoria la aplicación de esta Circular de Auditoría N° 34 para los informes de los profesionales a ser emitidos en organizaciones de servicios cuando se examine la afirmación de los controles de tales organizaciones de servicios, que sean distintos, de los establecidos por la Sección AT 801, *Informar sobre los Controles en una Organización de Servicios*. La aplicación anticipada del contenido de esta Circular de Auditoría N° 34 se encuentra permitida.

OSVALDO DE LA FUENTE INFANTA
Secretario General

RAÚL MUÑOZ VALLE
Presidente Nacional

SEPTIEMBRE 2015

CIRCULARES DE AUDITORÍA Nº 34

EMITIDAS POR:

COLEGIO DE CONTADORES DE CHILE A.G.

Materia

Esta trigésima cuarta Circular de Auditoría se refiere al Modelo de Informe del Profesional cuando se realice un trabajo de examen sobre la afirmación de la administración de una organización de servicios respecto de otros controles, distintos, de los establecidos por la Sección AT 801, *Informar sobre los Controles en una Organización de Servicios*.

Antecedentes

Muchas entidades recurren a la externalización de algunas de sus funciones por variadas razones, entre ellas, principalmente, por eficiencia y rentabilidad. Una organización que presta servicios a otras entidades se identifica como una "*organización de servicios*" y las entidades que hacen uso de los servicios de una organización de servicios se identifican como "*entidades usuarias*". Ejemplos de algunos de los servicios proporcionados por esas organizaciones de servicios, son los siguientes:

- Servicios computacionales del tipo "*cloud*", esto es, acceso en línea a recursos compartidos (redes, servidores, almacenamiento, aplicaciones y servicios específicos en línea).

- Administración y/o gestión de la seguridad, esto es, la administración y/o gestión del acceso a redes y sistemas computacionales.

- Servicio al cliente, por ejemplo: apoyo de post-venta y tramitación de reclamos de clientes en línea.

- Automatización de la fuerza de ventas, esto es, proporcionar y mantener aplicaciones que automaticen tareas en entidades que mantienen una fuerza de ventas. Algunas de estas aplicaciones son aquellas relacionadas con el procesamiento de pedidos, el compartir información y la evaluación del desempeño y/o actuación de los empleados.

- Servicios de externalización de tecnologías de la información (TI), por ejemplo todo lo relacionado con la operación de un centro de procesamiento y/o de cómputo.

Además de los riesgos normales que enfrenta la administración de una entidad usuaria, se expone también a riesgos adicionales relacionados con el sistema de la organización de servicios. Aunque la administración de una entidad usuaria puede delegar tareas o funciones en una organización de servicios, la administración de una entidad usuaria no puede delegar la responsabilidad por el producto o servicio proporcionado a los clientes de la entidad usuaria.

Para evaluar y tratar los riesgos asociados con un servicio externalizado, la administración de la entidad usuaria requiere información sobre los controles de la organización de servicios. Tales controles en la organización de servicios aseguran la prestación del o de los servicios. Al evaluar los controles que en una organización de servicios puedan ser pertinentes y afectar el o los servicios proporcionados a las entidades usuarias, la administración de una entidad usuaria puede solicitar el informe de un profesional respecto del diseño y efectividad de los controles relacionados con la prestación del o de los servicios por parte de la organización de servicios.

Algunos de los controles pertinentes a evaluar en una organización de servicios, específicamente, se refieren a alguna de las siguientes materias:

- Seguridad del o de los servicios que proporciona la organización de servicios.
- Continuidad y disponibilidad del o de los servicios de la organización de servicios.
- La integridad de la prestación del o de los servicios de una organización de servicio.
- La integridad de los procedimientos internos para lograr la prestación del o de los servicios de una organización de servicio.
- La confidencialidad de la información que con motivo de la prestación del o de los servicios, la organización de servicio procese o mantenga para entidades usuarias.
- Información privilegiada que con motivo de la prestación del o de los servicios, la organización de servicio: capte, retenga, revele o proporcione a entidades usuarias o a terceros.

Alcance

Esta Circular de Auditoría, se refiere, específicamente:

- A los criterios aplicables a utilizar por parte del profesional en su examen.

- A los antecedentes técnicos considerados como una base para la emisión de la presente Circular de Auditoría.

- Al modelo del informe del profesional que se emite cuando se examina la afirmación de la descripción del o de los servicios de una organización de servicio y lo adecuado del diseño y de la efectividad de los controles en funcionamiento para cumplir con los principios y criterios aplicables *[Por ejemplo, "Seguridad de la Información, Continuidad del Negocio y Riesgo" aprobados por las entidades usuarias].* Asimismo, se especifica, la diferencia en el informe del profesional, si la organización de servicios utiliza, a su vez, organizaciones de sub-servicios.

- Al modelo de la afirmación de la descripción del o de los servicios de la administración de una organización de servicio.

Los criterios aplicables a utilizar

Al evaluar la razonabilidad de la afirmación sobre la descripción efectuada por la administración de la organización de servicios, el profesional que realiza el examen de dicha afirmación debiera determinar si la descripción cumple con los criterios aplicables requeridos en el examen *[Por ejemplo, "Seguridad de la Información, Continuidad del Negocio y Riesgo" aprobados por las entidades usuarias].* Debido a que tales criterios pueden no estar fácilmente disponibles para todas las entidades usuarias, la administración de la organización de servicios debiera incluir en su afirmación todos los referidos criterios en su descripción. Aunque todos los criterios debieran ser incluidos en la afirmación sobre la descripción efectuada por la administración de la organización de servicios, algunos de los criterios pueden no ser relevantes a una organización de servicios o a la prestación del o de los servicios en particular. En este caso, los usuarios del informe encontrarían útil que la administración de la organización de servicios presente todos los criterios en la descripción e indique cuáles son los criterios que no son relevantes a la organización de servicios y/o a la prestación del o de los servicios y las razones de aquello. La administración puede hacerlo en su afirmación de la descripción o en una nota a los criterios de la descripción específicos.

Antecedentes técnicos

Las *Normas de Atestiguación* emitidas por el Colegio de Contadores de Chile A.G. (Secciones AT), le permiten a un profesional informar sobre una afirmación, distinta de la información financiera histórica. La mayoría de las Secciones AT tratan acerca de materias específicas, tal como el informar sobre el cumplimiento de la entidad con requerimientos específicos de leyes y/o regulaciones (Sección AT 601) o el informar sobre información financiera prospectiva (pronósticos y proyecciones financieras, Sección AT 301). Asimismo, la Sección AT 801, *Informar sobre los Controles en una Organización de Servicios* establece los requerimientos y guías para un profesional que examine e informe sobre la afirmación realizada por la administración de una organización de servicios

respecto de los controles que probablemente sean pertinentes al control interno de las entidades usuarias. Con frecuencia, las organizaciones de servicio requieren presentar estos tipos de informes a las entidades usuarias, a solicitud de los auditores externos de las entidades usuarias, a modo, de obtener información respecto de los controles en la organización de servicios que pueda afectar a los estados financieros de las entidades usuarias.

La Sección AT 101, *Trabajos de Atestiguación* proporciona un marco general para la realización del trabajo y la emisión de informes en todos los trabajos de atestiguación. Esta Circular de Auditoría proporciona un ejemplo ilustrativo del informe del profesional, a base de la Sección AT 101, cuando se realice el examen de la afirmación de la descripción del o de los servicios efectuados por la administración de una organización de servicios y de los controles que probablemente sean pertinentes para cumplir con la prestación del o de los servicios.

Esta Circular de Auditoría, para los ejemplos ilustrativos del modelo de informe del profesional y del modelo de la afirmación de la administración de la organización de servicio, ha considerado adicionalmente, las guías incluidas en: "*Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2^{SM})*" del American Institute of Certified Public Accountants (AICPA). También, se consideraron los ejemplos ilustrativos de los modelos de informe del profesional y de la afirmación de la administración de la organización de servicio, desarrollados posteriormente, para la mencionada guía de AICPA.

Anexos

En los siguientes Anexos, se presentan los modelos del informe del profesional para el examen de una afirmación de la administración de la organización de servicios y de esa afirmación. Dichos modelos, redactados en términos generales, especifican la diferencia cuando la organización de servicios utiliza, a su vez, a organizaciones de sub-servicios, y siendo este el caso, se excluya del alcance del examen del profesional.

En esta Circular de Auditoría, se incluyen:

Anexo A. Modelo del informe del profesional sobre el examen de la afirmación de la administración de la organización de servicios.

Anexo B. Modelo de la afirmación de la administración de la organización de servicio.

ANEXO A

Informe del Profesional Independiente

A: (*nombre de la organización de servicio*)

Alcance

Hemos examinado la afirmación de la descripción adjunta de **[*nombre del o los servicios*]** de **[*nombre de la organización de servicio*]** para el período **[*considerar un período comprendido desde (fecha) a (fecha)*]** y lo adecuado del diseño y de la efectividad de los controles en funcionamiento para cumplir con los principios y criterios de ***[Por ejemplo, "Seguridad de la Información, Continuidad del Negocio y Riesgo" aprobados por las entidades usuarias]***, según lo acordado con la entidad usuaria **[*Por ejemplo: nombre de la entidad usuaria*]**.

La descripción indica que ciertos servicios y criterios especificados en la descripción pueden lograrse sólo si las consideraciones de control de **[*las entidades usuarias*]** están razonablemente diseñadas y operando eficazmente, junto con controles relacionados de la organización de servicio. No hemos evaluado la conveniencia del diseño o la eficacia de funcionamiento de dichas consideraciones de control de **[*las entidades usuarias*]**.

[El siguiente párrafo es aplicable únicamente si la organización de servicios ha subcontratado, a su vez, parte de sus servicios en una sub organización de servicios]:
[La organización de servicio utiliza sub organizaciones de servicio como: "empresa 1". La descripción indica que ciertos criterios sólo pueden cumplirse si los controles en la organización subcontratada se encuentran razonablemente diseñados y operando eficazmente. La descripción presenta **[*nombre del o los servicios*]** y los controles correspondientes a los criterios de ***[Por ejemplo, "Seguridad de la Información, Continuidad del Negocio y Riesgo" aprobados por las entidades usuarias]*** y los tipos de controles que la organización espera que estén implementados, razonablemente diseñados y operando eficazmente en la sub organización para satisfacer ciertos criterios ***[Por ejemplo, "Seguridad de la Información, Continuidad del Negocio y Riesgo" aprobados por las entidades usuarias].*** La descripción no incluye ninguno de los controles implementados en la sub organización de servicios. Nuestro examen no se extendió a los servicios prestados por la sub organización de servicios.***]***

La información adjunta a la descripción "otra información proporcionada por **[*nombre de la organización de servicio*]** que no está cubierta por el informe del profesional de la organización de servicio" describe el servicio de la organización de servicio **[*mencionar contenido de la otra información proporcionada*]**. Esta información es presentada por la dirección de la organización de servicio de **[*nombre del o los servicios*]** para proporcionar información adicional y no es parte de la descripción de la organización de servicio a disposición de las entidades usuarias durante el período **[*comprendido desde (fecha) a (fecha)*]**. La información adjunta a la descripción sobre el **[*nombre del o los servicios*]** no ha sido sometida a los procedimientos aplicados en el examen de la afirmación de la

descripción adjunta de **[*nombre del o los servicios*]** y en consecuencia, no expresaremos ninguna opinión sobre tal información adjunta.

Responsabilidades de la Organización de Servicios

La organización de servicio ha proporcionado una afirmación basada en los principios y criterios identificados sobre ***[Por ejemplo, "Seguridad de la Información, Continuidad del Negocio y Riesgo" aprobados por las entidades usuarias]***. **[*Nombre de la organización de servicios*]** es responsable de preparar: *(1)* la descripción y la afirmación; *(2)* la integridad, exactitud y método de presentación de la descripción y la afirmación; *(3)* proporcionar los servicios cubiertos por la descripción; *(4)* especificar los controles que cumplen los criterios de servicios aplicables y que se indican en la descripción, y; *(5)* diseñar, implementar y documentar los controles para cumplir con los criterios de servicios aplicables ***[Por ejemplo, "Seguridad de la Información, Continuidad del Negocio y Riesgo" aprobados por las entidades usuarias]***.

Responsabilidad del Profesional que examina una Organización de Servicios

Nuestra responsabilidad consiste en expresar una opinión sobre la afirmación respecto de la razonabilidad de la descripción basada en los criterios de ***[Por ejemplo, "Seguridad de la Información, Continuidad del Negocio y Riesgo" aprobados por las entidades usuarias]*** de **[*nombre del o los servicios*]** y sobre la idoneidad del diseño y la operatividad eficaz de los controles para cumplir con los criterios de servicios aplicables, basados en nuestro examen. Efectuamos nuestro examen de acuerdo con las normas de atestiguación establecidas por el Colegio de Contadores de Chile. Tales normas requieren que planifiquemos y realicemos nuestras pruebas para obtener una seguridad razonable acerca de si, en todos los aspectos significativos: *(1)* la descripción se presenta basándose en la descripción de los criterios; *(2)* los controles fueron adecuadamente diseñados, y; *(3)* su funcionamiento fue efectivo para cumplir con los criterios de servicios aplicables ***[Por ejemplo, "Seguridad de la Información, Continuidad del Negocio y Riesgo" aprobados por las entidades usuarias]*** durante todo el período **[*mencionar el período de revisión comprendido desde (fecha) a (fecha)*]**.

Nuestro examen consistió en realizar procedimientos para obtener evidencia acerca de la razonabilidad de la presentación de la descripción basada en la descripción de los criterios y lo adecuado del diseño y el funcionamiento efectivo de los controles para cumplir con los criterios de servicios aplicables ***[Por ejemplo, "Seguridad de la Información, Continuidad del Negocio y Riesgo" aprobados por las entidades usuarias]***. Nuestros procedimientos incluyeron evaluar los riesgos que la descripción no esté presentada razonablemente y que los controles no estén diseñados adecuadamente ni operando con efectividad para cumplir con los criterios relacionados indicados en la descripción. Nuestros procedimientos también incluyen realizar pruebas de la efectividad operativa de los controles que consideramos necesarios para proporcionar una seguridad razonable de que se cumplieron los criterios de servicios aplicables. Nuestro examen incluyó también evaluar la presentación general de la descripción. Consideramos que la evidencia que hemos obtenido es suficiente y apropiada para proporcionar una base razonable para nuestra opinión.

Limitaciones Inherentes

Debido a su naturaleza y limitaciones inherentes, los controles de una organización de servicio no siempre funcionan eficazmente para cumplir con los criterios de servicios aplicables. Además, la proyección al futuro de cualquier evaluación de la razonabilidad de la presentación de la descripción o cualquier conclusión respecto de lo adecuado del diseño y de la efectividad de los controles en funcionamiento para cumplir con los criterios de servicios aplicables están sujetos a los riesgos de que puede cambiar el sistema o que los controles en una organización de servicio pueden convertirse en inadecuados o fallar.

Conclusión

En nuestra opinión, en todos sus aspectos significativos, a base de los criterios de ***[Por ejemplo, "Seguridad de la Información, Continuidad del Negocio y Riesgo" aprobados por las entidades usuarias]*** identificados en la afirmación de **[*Nombre de la organización de servicio*]** y los criterios de servicios aplicables:

a. La descripción presenta razonablemente **[*mencionar el o los servicios*]** que fueron diseñados e implementados durante todo el período **[*mencionar el período de revisión comprendido desde (fecha) a (fecha)*]**.

b. Los controles indicados en la descripción fueron diseñados para proporcionar una seguridad razonable de que los criterios aplicables se cumplirían si los controles funcionan eficazmente durante todo el período **[*mencionar el período de revisión comprendido desde (fecha) a (fecha)*]**.

c. Los controles probados e indicados en la descripción fueron los necesarios para proporcionar una seguridad razonable de que se cumplieron los criterios aplicables y operaron de manera efectiva durante todo el período **[*mencionar el período de revisión comprendido desde (fecha) a (fecha)*]**.

Descripción de las Pruebas de Controles

Los controles específicos que probamos y la naturaleza, oportunidad y resultados de las pruebas se presentan en la sección del informe titulada "Criterios, controles, procedimientos de prueba y resultados".

Uso Restringido

Este informe y la descripción de las pruebas de controles y sus resultados son destinados para la información y el uso de **[*nombre de la organización de servicio*]** o de entidades usuarias **[*nombre de las entidades usuarias*]** durante parte o todo el período **[*mencionar el período de revisión comprendido desde (fecha) a (fecha)*]** y profesionales que proporcionen servicios a dichas entidades usuarias, los que tienen suficiente conocimiento y comprensión de los siguientes asuntos:

- La naturaleza del servicio prestado por la organización de servicio.

- Cómo interactúa el servicio de la organización con las entidades usuarias del servicio, organizaciones de sub servicio y otras partes.

- El control interno y sus limitaciones.

- Los criterios de ***[Por ejemplo, "Seguridad de la Información, Continuidad del Negocio y Riesgo" aprobados por las entidades usuarias]*** aplicables al servicio.

- Los riesgos asociados al servicio que pueden amenazar el logro de los criterios aplicables y cómo se controlan esos riesgos.

Este informe no tiene por objetivo ser y no debiera ser utilizado por nadie que no sean estas partes especificadas.

(*Firma del profesional que examina la organización de servicios*).

(*Fecha del informe*).

(*Ciudad y región*).

ANEXO B

Afirmación de [*nombre de la organización de servicio*]

Hemos preparado la descripción de los servicios de **"[*nombre del o los servicios a revisar*]"** de **[*nombre de la organización de servicio*]** durante parte o todo el período comprendido **[*mencionar el período de revisión comprendido desde (fecha) a (fecha)*]**, basado en los criterios aplicables establecidos para este tipo de revisión ***[Por ejemplo, "Seguridad de la Información, Continuidad del Negocio y Riesgo" aprobados por las entidades usuarias]***. La descripción pretende proporcionar a los usuarios de los servicios mencionados, particularmente los controles de los servicios destinados a satisfacer los criterios aplicables de ***[Por ejemplo, "Seguridad de la Información, Continuidad del Negocio y Riesgo" aprobados por las entidades usuarias]***.

Confirmamos que, de acuerdo a nuestro mejor entender y saber que:

a. La descripción presenta razonablemente los servicios de **"[*nombre del o los servicios a revisar*]"** de **[*nombre de la organización de servicio*]** durante parte o todo el período comprendido **[*mencionar el período de revisión comprendido desde (fecha) a (fecha)*]**, basado en los siguientes criterios de Descripción:

i. La descripción contiene la siguiente información:

(1)Los servicios prestados.

(2)Los componentes del sistema utilizados para proporcionar los servicios, que son los siguientes:

- Infraestructura. Los componentes físicos y hardware de un sistema (instalaciones, equipos y redes).
- Software. Los programas y software operativo de un sistema (sistemas, aplicaciones y utilidades).
- Personas. El personal involucrado en la operación y el uso de un sistema (desarrolladores, operadores, usuarios y administradores).
- Procedimientos. Los procedimientos automatizados y manuales involucradas en la operación de un sistema.
- Datos. La información utilizada y soportada por un sistema (flujos de transacción, archivos, bases de datos y tablas).

(3)Los límites o los aspectos cubiertos por la descripción de los servicios.

(4) Cómo los servicios capturan y dirigen a las condiciones y acontecimientos significativos.

(5) El proceso usado para preparar y entregar informes y otra información para entidades usuarias y otras partes.

(6) Si la información es proporcionada o recibida desde organizaciones subcontratadas u otras partes, como se recibe o suministra tal información, el rol de la organización de sub-servicios y otras partes y los procedimientos realizados para determinar si dicha información y su procesamiento, mantenimiento, y almacenamiento de información están sujetos a controles apropiados.

ii. Para cada principio están descritos los criterios aplicables y los controles diseñados para cumplir con estos criterios, incluyendo, según corresponda, los controles de usuario-entidad complementarios que contemple en el diseño de los servicios de **"[*nombre del o los servicios a revisar*]"** de **[*nombre de la organización de servicio*]** durante parte o todo el período comprendido **[*mencionar el período de revisión comprendido desde (fecha) a (fecha)*]**, entre ellos considerando lo siguiente:

[El siguiente párrafo es aplicable únicamente si la organización de servicios ha subcontratado, a su vez, parte de sus servicios en una sub organización de servicios]:

(1) ***[***Para organizaciones subcontratadas utilizando el método de exclusión de acuerdo a la naturaleza de los servicios prestados por la organización subcontratada; cada uno de los criterios que están destinados a cumplirse por los controles de la organización subcontratada en combinación con los controles en la organización de servicio, y los tipos de controles que se esperan implementarse en las organizaciones subcontratadas, cumplan esos criterios.***]***

(2) Cualquier criterio aplicable que no tenga un control asociado de la organización de servicio o de una organización subcontratada y las razones de ello.

(3) Otros aspectos del entorno de control de la organización de servicio, del proceso de evaluación de riesgos, de los sistemas de información y comunicación y de la supervisión de los controles que son pertinentes para los servicios de **"[*nombre del o los servicios a revisar*]"** y aplicables a los criterios del servicio.

(4) Los detalles relevantes de los cambios al servicio de **[*nombre de la organización de servicio*]** durante el período **[*mencionar el período de revisión comprendido desde (fecha) a (fecha)*]**.

iii. La Descripción no omite ni distorsiona información pertinente al alcance de los servicios de **"[*nombre del o los servicios a revisar*]"** mientras reconoce que

la descripción es preparada para cumplir con las necesidades comunes de un amplio rango de entidades usuarias del servicio, de los auditores independientes de esas entidades usuarias y de la Asociación de Bancos e Instituciones Financieras y, por lo tanto, pueden no incluir cada aspecto de los servicios de **"[*nombre del o los servicios a revisar*]"** que cada entidad usuaria individual del servicio y su auditor puedan considerar importante dentro de su propio entorno en particular.

b. Los controles se encontraban diseñados e implementados durante **[*mencionar el período de revisión comprendido desde (fecha) a (fecha)*]** para cumplir los criterios aplicables en los servicios de **"[*nombre del o los servicios a revisar*]"**.

c. Los controles mencionados en la descripción de los servicios de **"[*nombre del o los servicios a revisar*]"**, operaron de manera efectiva durante el período **[*mencionar el período de revisión comprendido desde (fecha) a (fecha)*]**, para cumplir los criterios aplicables.

(*Identificación de la organización de servicios*)

(*Firma del representante de la organización de servicios*).

(*Fecha de la afirmación de la organización de servicios*).

(*Ciudad y región de la organización de servicios*).