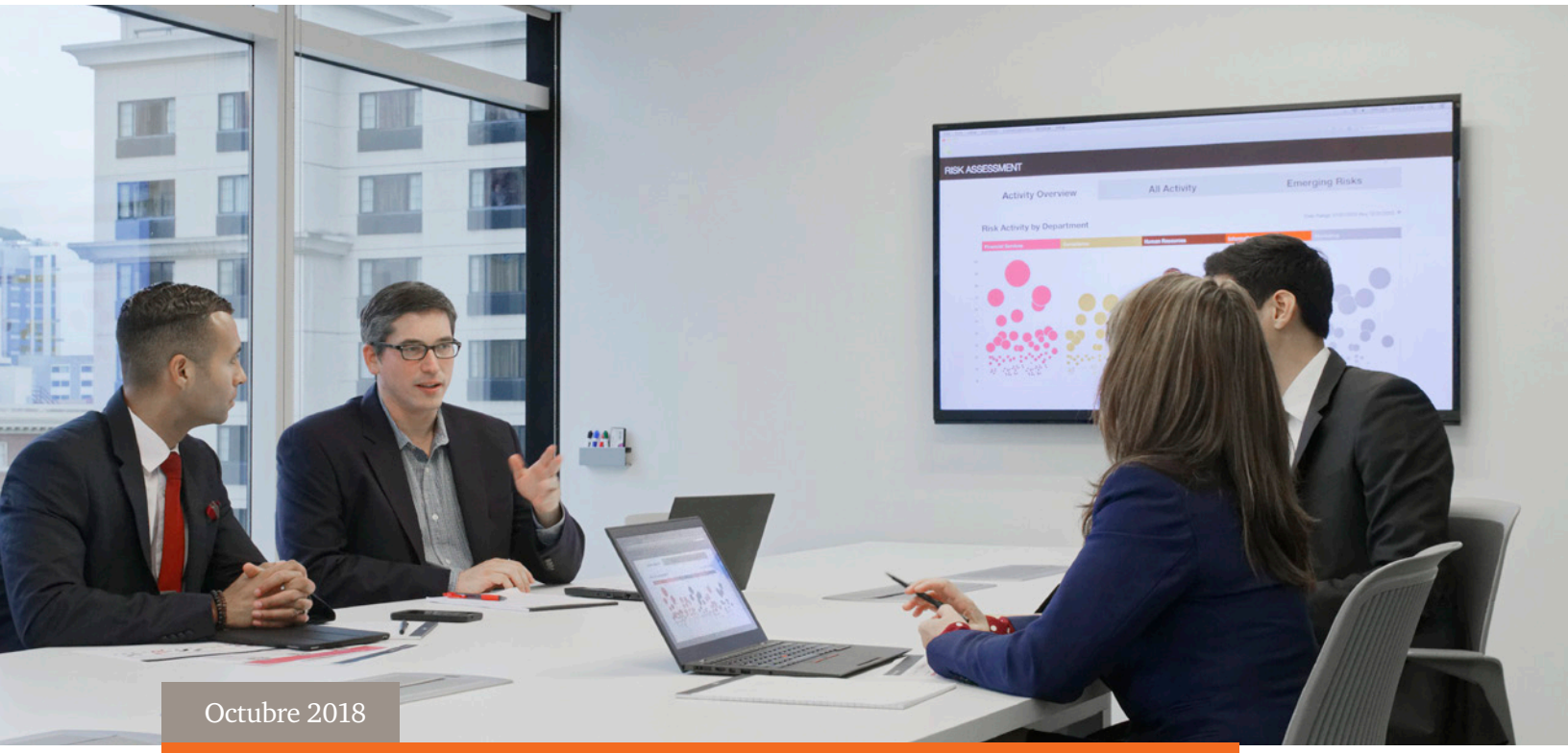
Governance Insights Center
ACES (Audit Committee Excellence Series)

www.pwc.cl



Octubre 2018

Supervisión de riesgos introducidos por terceros

La serie de comités de auditoría de excelencia de PwC (ACES) propociona conocimientos, perspectivas e ideas prácticas y procesos para ayudar a los comités de auditoría a maximizar el desempeño del comité.

pwc

Este módulo de ACES analiza aspectos importantes de la supervisión de procesos de mitigación de riesgos de terceros y el papel crítico que juegan los comités de auditoría:

1. Por qué entender los riesgos de terceros es crítico para los comités de auditoría
2. Qué tienen de especial los riesgos de terceros
3. Comprender plenamente los riesgos de terceros
4. Evaluar los estándares existentes de la compañía para la realización de negocios y la contratación con personas ajenas a la misma.
5. Las relaciones de larga duración pueden plantear desafíos particulares
6. Los riesgos de seguridad de terceros merecen especial atención
7. Es un proceso interminable

Anexo – Herramienta de gestión de riesgos de terceros

1. Por qué entender los riesgos de terceros es crítico para los comités de auditoría

Las empresas de hoy en día están cada vez más integradas con sus proveedores, distribuidores y otros terceros. Considere que las organizaciones externas, terceros, tienen tanta influencia en las compañías de hoy que, como grupo, 89 de los Fortune 500 tienen un promedio de más de 100.000 proveedores cada uno, es decir, más de 9 millones de relaciones directas con los proveedores. Con este gran número, viene el riesgo, ya que las empresas están expuestas a riesgos relacionados con las acciones de sus proveedores externos. Y debido a este mundo altamente integrado, muchas entidades no diferencian a un proveedor crítico, parte de la "cadena de valor", de cualquier otro. Esto, aumenta el riesgo de que terceros proveedores puedan dañar la reputación y la marca de su organización y crear obligaciones legales y comerciales.

Además del riesgo de reputación, existen otros riesgos de cumplimiento y regulatorios. En otras palabras, un problema creado por un proveedor estratégico en la "cadena de valor" puede poner a una empresa de rodillas. Entre las áreas más críticas, se incluyen las violaciones de la protección de datos personales, la legislación laboral, el mal uso de información financiera y la propiedad intelectual (PI). Además, muchos terceros tienen acceso a la red de la empresa, lo que fomenta el potencial para infracciones cibernéticas y de privacidad.

Nuestra leyes en Chile sobre cohecho, financiamiento de actividades terroristas y lavado de dinero son ejemplos de regulaciones que pueden ser de particular interés para las empresas que utilizan proveedores externos críticos. En Estados Unidos la SEC y el Departamento de Justicia han hecho responsables a las compañías por los actos de este tipo cometidos por terceros. Los reguladores a menudo analizan la responsabilidad de una empresa basándose en el conocimiento real o en la ceguera intencional, lo que significa que consideran si la empresa se ha mantenido intencionalmente inconsciente de las acciones del tercero, para evitar su responsabilidad. Desafortunadamente, para muchas compañías, argumentar que un tercero tiene la culpa no ha tenido éxito, porque no pudieron demostrar suficientes controles internos diseñados para monitorearlos.

La SBIF en Chile y la OCC en Estados Unidos han brindado orientación a los bancos para evaluar y gestionar los riesgos asociados con estas relaciones. Las directrices dejan claro que el uso de terceros no disminuye la responsabilidad de la administración y del personal directivo del banco de asegurar que la actividad se realiza de acuerdo con las normas aplicables.

En estructuras complejas como la de instituciones financieras, hay un rol preponderante del comité de riesgos y de la función de riesgo operacional. Sin embargo muchos directorios asignan la coordinación de la supervisión de riesgos al comité de auditoría, ya que normalmente es responsable del cumplimiento de la presentación de informes financieros y de las estructuras de control interno relacionadas. Además, el comité de auditoría supervisa la función de auditoría interna de la compañía, quien a su vez aborda la supervisión de los riesgos de terceros, como una tercera línea de defensa.

Esta edición de ACES se centra en el papel de los comités de auditoría en la supervisión de los riesgos que son inevitablemente introducidos al tratar con proveedores externos y críticos.

2. Qué tienen de especial estos riesgos

Los riesgos de terceros se relacionan con áreas como continuidad operacional, el soborno, protección de datos, la piratería de software, la salud, la seguridad, y las leyes laborales, y es posible que no se aborden en su totalidad mediante controles internos convencionales o procesos de evaluación de riesgos desde los propios terceros.

Otro atributo de los riesgos de terceros es que los riesgos de reputación y otros tienen un denominador común: están regidos y controlados por un contrato legal celebrado con el tercero que establece las obligaciones, derechos y recursos de la empresa y sus terceros proveedores.

Dado que estos riesgos de terceros no suelen estar cubiertos por los procesos de evaluación de riesgos existentes en las empresas, los controles diseñados para mitigar estos riesgos deben considerarse como parte de un subcomponente específico de la estructura general de control interno de la empresa. En términos generales, los controles necesarios para monitorear a terceros deben aplicar, independientemente del tipo de riesgo que se esté mitigando o de si el tercero es un proveedor, un suministrador de infraestructura o un distribuidor.

Las empresas deben diseñar un sistema de control interno completo que cubra todas las relaciones significativas críticas con terceros. Debido a que estas relaciones se rigen por un contrato, es particularmente importante incluir la visión jurídica como parte integral de ese proceso.

Consideraciones sobre el papel del comité de auditoría

- *Entender cuántas relaciones significativas con terceros tiene la empresa y la naturaleza de aquellas relaciones.*

- *Evaluar cómo la organización monitorea estos riesgos, cuales son los controles y quien los ejecuta, para asegurar un proceso integral*

- *Evaluar si los asesores legales de la empresa están suficientemente involucrados en el entorno de control de riesgos de terceros, y si comprenden la importancia de su papel, en la definición de las atribuciones de la organización sobre los terceros y de los límites del riesgo legal asumido.*

El asesor jurídico de la empresa necesita ser parte integral del proceso, junto con operaciones y tecnología

3. Comprender plenamente los riesgos introducidos por terceros

Sería difícil nombrar a una compañía que no estuviera sujeta a riesgos en relación con terceros, ya sea que esa parte sea un socio comercial, un proveedor, un distribuidor, un contratista, o que tenga alguna otra relación con la compañía.

Esencialmente, cualquier organización que tenga acceso a la PI o a la red corporativa de su empresa, que proporcione infraestructura de TI o que participe en la "cadena de valor" de la empresa, crea un riesgo de terceros que debe ser gestionado de alguna manera. Es importante integrar la gestión de riesgos de terceros en el programa general de gestión de riesgos de una empresa.

Existen retos especiales que diferencian la supervisión de los riesgos de terceros de otros riesgos. Considere que muchas compañías no tienen un inventario de sus relaciones con terceros. Las relaciones pueden haberse desarrollado a nivel de la unidad operativa o de un proceso y pasar por alto cualquier control de la empresa que pueda existir. O la empresa puede carecer de políticas y procedimientos para crear y supervisar relaciones con terceros. Los controles no pueden ser efectivos si la lista de las terceras partes externas con las cuales está interactúa no es completa y precisa.

Para complicar aún más el asunto, muchos terceros tienen sus propias relaciones externas que les proporcionan servicios, lo que convierte a estos en terceros de segundo nivel de la empresa. Puede ser importante para la empresa entender cómo sus terceros de primer nivel gestionan los riesgos que para la empresa representan los terceros de segundo nivel.

Cuando esto sucede, es fundamental entender la interdependencia entre los proveedores de primer nivel y los de segundo nivel. Ocurre que las organizaciones creen haber diversificado el riesgo de continuidad operacional entre varios proveedores de primer nivel, cuando estos en verdad dependen de uno o más proveedores de segundo nivel que le son comunes, por ejemplo proveedores de comunicación o enlace.

Además, los terceros pueden estar ubicados en el extranjero con diferentes leyes, prácticas y ética de negocios. Otras relaciones pueden ser a largo plazo y/o de fuente única, lo que aumenta la complejidad de definir y mitigar los riesgos de la relación.

En el anexo presente al documento se ofrece un ejemplo de un instrumento eficaz de gestión de riesgos de terceros:

- Inventariar las relaciones con terceros
- Priorizar las más significativas
- Asignar una calificación de riesgo a cada tipo de riesgo y una calificación de riesgo global para cada tercero
- Identificar a la gerencia responsable de la gestión del riesgo
- Mapear la supervisión de riesgos para cada relación con el directorio o su comité
- Requerir certificaciones de proceso sobre ellos
- Abordar la frecuencia de las actualizaciones de informes sobre cada relación con el directorio o comité

4. Evaluar los estándares existentes de la compañía para la realización de negocios y la contratación con personas ajenas a la misma

Una práctica estándar e integral para la gestión de riesgos de terceros podría ayudar a la empresa a mitigarlos y facilitar su supervisión.

Procedimientos iniciales

Due diligence sobre la reputación y las capacidades - Un proceso formal de due diligence es importante para las empresas que trabajan rutinariamente con terceros. En su forma más simple, el due diligence podría incluir la búsqueda en bases de datos y la revisión de los medios de comunicación y sitios de Internet para obtener información sobre la reputación y las capacidades de una empresa. Un due diligence más sólido podría incluir el uso de cuestionarios para conocer las prácticas de cumplimiento y el uso de terceros de segundo nivel, la obtención de información sobre las relaciones con funcionarios y organizaciones gubernamentales, la realización de visitas a terreno, la obtención de certificaciones sobre controles, e incluso podría incluir la solicitud de pruebas de licencias para cualquier PI que el tercero utilice en sus procesos, como el software. La cantidad de due diligence realizada sobre una posible relación con terceros debe basarse en el nivel de riesgo que la parte crea para la empresa.

Líneas de reporte apropiadas para el programa de cumplimiento de terceros desde el punto de vista de la gobernanza - Es importante identificar a la persona en la empresa que gestiona la relación con los terceros.

Contratos y políticas adecuadas, incluida la protección de la PI, la capacitación de sus empleados y el derecho a la auditoría - Las relaciones con terceros se rigen generalmente por un contrato. Éste debe definir términos específicos de cumplimiento y calidad, la forma en que la parte protegerá la PI de la empresa, la forma en que se capacitará a los empleados en la protección de la PI, y también las medidas anticorrupción para los empleados. La empresa debe tener el derecho de auditar el cumplimiento de estos criterios y su director jurídico debe entender la importancia de este tipo de disposiciones contractuales. Esto se hace mediante el requerimiento de certificaciones externas del uso habitual y/o la realización de auditorías internas.

Derecho a terminar la relación por violaciones del acuerdo - Por lo general, una empresa tendrá el derecho de terminar un contrato por incumplimiento de los términos del contrato. Con un contrato bien redactado, la compañía tendrá el derecho de terminarlo en caso de incumplimiento. Estos podrían incluir no sólo métricas de cumplimiento y calidad, sino también métricas de alerta temprana sobre asuntos que podrían llevar a un daño a la reputación o a la marca. Por ejemplo: violaciones de los derechos laborales; problemas de calidad; filtrar o facilitar el acceso a datos a una parte externa que podría perjudicar el mercado de la empresa.

Ampliar las líneas directas de los empleados - Crear un mecanismo que permita a los empleados de terceros clave acceder a las líneas directas de denuncia de irregularidades y la empresa acceder a estas denuncias. Esto podría dar a la empresa una alerta temprana sobre una debilidad cultural en un tercero que debe ser abordada. También podría ser un factor para decidir cuándo es necesaria una visita a terreno, o podría afectar el calendario de su próxima auditoría de cumplimiento.

Procedimientos en curso

Auditoría y seguimiento de las relaciones con terceros, clave para la compañía - Las "partes de alto riesgo" pueden definirse de diferentes maneras dependiendo de la empresa. Podría basarse en el valor económico de la relación, en la importancia de la relación para la empresa, en la posición de la parte (si se trata de una posición de alto riesgo de fraude), en la naturaleza de la PI de la empresa a la que el tercero tiene acceso, o en otras medidas. Las partes definidas como de alto riesgo deben ser sometidas a seguimiento continuo.

Obtener representaciones de cumplimiento periódicas - Dependiendo de la evaluación de la compañía sobre el riesgo asociado a terceros, se podría requerir que los terceros presenten representaciones de cumplimiento periódicamente.

La certificación normalmente se basa en una auditoría que el tercero contrata a un auditor para efectuarla, o podría ser simplemente una representación interna por parte del tercero de que no se han producido violaciones. La decisión de la compañía sobre qué enfoque funciona para un determinado tercero debe basarse en el nivel de riesgo que el tercero presenta a la empresa.

Ejercer el derecho a la auditoría con un proceso documentado – En la medida en que la empresa puede tener un derecho contractual para auditar a un tercero, también es importante aprovechar ese derecho. El departamento de auditoría interna puede llevar a cabo la auditoría, o bien externalizarla en una empresa de auditoría. El ejercicio del derecho de auditoría envía un mensaje claro al tercero sobre la seriedad con la que la empresa se toma el cumplimiento de los términos contractuales.

La realización de auditorías podría ayudar a la empresa en caso de que el tercero sea acusado de conducta indebida, al demostrar que la corrupción se produjo a pesar de los esfuerzos razonables de la empresa para hacer seguimiento al comportamiento de un tercero.

Monitoreo de métricas y reportes - Para cada acuerdo con terceros, se deben identificar métricas significativas y notificarlas a la empresa en forma regular. Las métricas específicas a supervisar dependerán de la naturaleza de la relación entre la empresa y cada tercero, ya que no existe una fórmula única para todos los casos.

Para tener un entorno de control eficaz, las empresas necesitan hacer un seguimiento de los informes no presentados a tiempo, revisar las métricas de anomalías reportadas, ejercer su derecho a la auditoría y mantener una comunicación continua con el tercero.

Consideraciones sobre el rol del comité de auditoría

- *Evaluar si el responsable del programa de supervisión de riesgos de terceros tiene la capacidad y visibilidad adecuada en la empresa para asegurar su efectividad. Evaluar el tono y la actitud de la gerencia respecto al cumplimiento*

- *Evaluar si el proceso de due diligence de la empresa es apropiado para identificar los riesgos potenciales que las relaciones con terceros podrían representar para la empresa, y la forma en que la empresa planea mitigar y monitorear esos riesgos*

- *Comprender las actividades de la empresa que son dependientes de terceros y el criterio de las mismas. Discutir si la empresa está utilizando terceros en puntos críticos de fraude ó corrupción y por qué*

- *Averiguar si la empresa ejerce los derechos de auditoría, verificación y de terminación, y si hace un seguimiento adecuado del cumplimiento de forma continua*

- *Comprender cómo la gerencia identifica las métricas y los protocolos de reporte para las relaciones con terceros. Discutir el proceso de revisión y seguimiento de los informes por parte de la gerencia*

- *Entender el papel de riesgo operacional y de la auditoría interna (o de la empresa de auditoría contratada) que realizará auditorías de terceros importantes con respecto a los riesgos de terceros, así como a la prevención y detección de fraudes. Considerar el uso de herramientas de detección y seguimiento de fraudes en entidades ajenas a la empresa*

5. Las relaciones de larga duración pueden suponer desafíos particulares

Para muchas empresas, las relaciones con algunos proveedores tienen una larga historia. Es probable que estas relaciones no vengan con la formalidad que pueden tener las relaciones más recientes. Hace veinte años, puede que haya habido un menor foco en el seguimiento de los comportamientos de terceros, por lo que las empresas deberían plantearse si los contratos existentes con estos terceros cumplen con los estándares necesarios en el entorno actual. Dicho esto, la transición de un socio de negocios o proveedor de larga data, a una nueva estructura debe ser manejada cuidadosamente.

Un enfoque que se ha considerado eficaz es la puesta en marcha de un programa integral de gestión de relaciones con terceros, para todas las relaciones con terceros nuevas y existentes. La mejor manera de hacerlo es desde una perspectiva de "amenazas y salvaguardas", centrándose en primer lugar en los terceros situados en un proceso, actividad o juridicción con un riesgo significativo de error, fraude o corrupción u otros problemas. La clasificación de cada tercero en base a factores de riesgo, incluyendo su ubicación, la interacción con funcionarios del gobierno y el volumen de ingresos/gastos o la sensibilidad de los procesos/datos que estos manejan, ayuda a establecer prioridades sobre en dónde debe la empresa enfocar sus esfuerzos. Los terceros que representen el mayor riesgo deben estar sujetos al due diligence más exhaustivo. Los terceros de menor riesgo pueden justificar una revisión menos rigurosa.

6. Los riesgos de seguridad de terceros merecen especial atención

Muchos terceros proveedores tienen acceso a información confidencial dentro ó fuera de la red de la empresa. Estos terceros pueden ser proveedores y responsables del procesamiento de tarjetas de crédito, carteras, nóminas de pago o de hosting de datos. Y las responsabilidades legales, reputacionales, y comerciales por infracciones de cyberseguridad de terceros siguen aumentando. Las mismas consideraciones mencionadas para otros riesgos de terceros aplican para estos cyberisk, con un enfoque particular en los terceros de alto riesgo y un énfasis en la necesidad de hacer un seguimiento efectivo y continuo.

Por supuesto, los terceros necesitan cumplir con ciertos requisitos de seguridad antes de permitir el acceso, pero la tecnología cambia todos los días y la sofisticación de los cyberataques, también. Una evaluación única de la cybersecurity de un tercero podría no ser relevante durante mucho tiempo. Ciertamente, una evaluación inicial es importante, pero comunicar las expectativas de seguridad continuas de la empresa es fundamental en este entorno en evolución. Y las métricas se deben establecer, monitorear y revisar según sea necesario para determinar si el programa de cybersecurity del tercero mantiene el cumplimiento con los controles requeridos. No es inusual que las empresas, incluidos los terceros, contengan el gasto en las últimas correcciones de errores, actualizaciones y mejoras de sus programas de software, lo que aumenta la posibilidad de que se produzca una posible filtración.

Es relevante limitar la cantidad de datos a la cual los proveedores externos pueden acceder, básicamente a sólo lo que es necesario. Adicionalmente los terceros deben estar obligados contractualmente a alertar a la empresa sobre una filtración y a realizar auditorías de seguridad.

Consideraciones sobre el papel del comité de auditoría

- *Averiguar si la empresa sabe a qué datos críticos tienen acceso los terceros y si el acceso a los datos se limita a la información necesaria*

- *Averiguar sobre los terceros que dan soporte a la infraestructura de TI, comunicaciones y operaciones de la empresa y cómo son monitoreados*

- *Averiguar si los contratos proporcionan derechos a las auditorías de seguridad y notificación de infracciones*

- *Evaluar si la empresa tiene un proceso en curso para supervisar el cumplimiento de los mandatos contractuales de cybersecurity*

- *Conocer los proveedores y terceros que tengan una incidencia relevante sobre la información financiera y la operación de la empresa*

7. Es un proceso sin fin

Es importante que las relaciones con terceros se revisen periódicamente. A medida que se establecen nuevas relaciones y cambian las existentes, será necesario hacer actualizaciones en el programa de gestión de riesgos de terceros para reflejar estos cambios. A medida que la PI de la empresa se amplíe con nuevos productos o se vayan adoptando nuevas tecnologías, inevitablemente se crearán las relaciones con terceros. Además, si la empresa pasa por una fusión o adquisición, podría ser necesario hacer cambios significativos en el programa.

Consideraciones sobre el papel del comité de auditoría

- *Comprender los planes de la gerencia para actualizar continuamente y renovar periódicamente los controles de terceros para asegurar su integridad e idoneidad*
- *Considerar el impacto de cualquier cambio en el entorno operativo de la empresa y la forma en que estos cambios pueden afectar sus relaciones con terceros*

Una evaluación puntual de la ciberseguridad de un tercero podría no ser relevante durante mucho tiempo.

Anexo

Muestra de una matriz de evaluación de riesgos para catalogar y evaluar las relaciones con terceros

Tercero proveedor	**Calificación de riesgo** (evaluar una puntuación de riesgo de 1 a 5)						Calificación general	Responsabilidad de la Administración	Supervisión del Directorio	Frecuencia de revisión
	Cohecho	Ingresos	Seguridad de la infomación	Ambiental	Piratería	Lavado				
Proveedor	x	x	x	x	x		x	Gerente de Adquisiciones	Todo el Directorio	Anual
Distribuidor	x	x	x	x	x		x	Gerente Financiero	Comité De Auditoría	Trimestral
Proveedor de servicios de nube	x	x	x	x	x		x	Gerente de Teconología	Comité De Auditoría	Trimestral
Revendedor	x	x	x	x	x		x	Gerente de Seguridad de la Información	Comité De Auditoría	Anual
Agente	x	x	x	x	x		x	Administración	Todo el Directorio	Anual
(continuar con todos los terceros proveedores)										

Cómo PwC puede ayudar

Para profundizar más sobre cómo este tema podría afectar a su negocio, póngase en contacto con su socio de compromiso o con un miembro del Centro de Conocimientos sobre la Gobernanza de PwC.

Renzo Corona
Socio Líder de PwC Chile
(56) 2 2940 0064
renzo.corona@cl.pwc.com

Fernando Orihuela
Socio Líder de Auditoría
(56) 2 2940 0064
fernando.orihuela@cl.pwc.com

Raúl Arteaga
Socio de Seguridad de la Información
(56) 2 2940 0182
raul.o.arteaga@cl.pwc.com

Boris Gajardo
Senior Manager
Riesgo Operacional
(56) 2 2940 0921
boris.gajardo@cl.pwc.com

Enzo Delorso
Senior Manager
Seguridad SAP
(56) 2 2940 0182
enzo.daniel.delorso@cl.pwc.com

Otros temas de la “Serie de Excelencia de Comité de Auditoría” incluyen:

- Supervisando a los auditores externos (Agosto 2018)
- Moviendose a la velocidad de la innovación (Septiembre 2018)