

Charla “La Investigación Interna, debido a fraudes e irregularidades y La Gestión Integral de Riesgos Corporativos”

23 de agosto de 2017, en la sede del Colegio de Ingenieros de Chile A.G. de Santiago y organizada por la especialidad de Ingeniería Comercial y de Control de Gestión.

Expositores:

- Christian Nino-Moris, Auditor Forense, Contados Público y Auditor, primer latinoamericano en obtener el Master of Forensic Accounting en la U de Wollongong, Australia, miembro de la Association College of Forensic Examiners de EE.UU.
- Pedro Hernández, MGN, MBA(c), CGEIT, CRISC, CICA. Socio Fundador y CEO de GRC Latam, con más de 17 años de experiencia en Corporate Governance, Risk Management & Compliance.

Moderador:

- Christian Cancino, consejero de la Especialidad Ingeniería Comercial y Control de Gestión.

En la charla de Nino-Moris sobre Auditoría Forense, el expositor nos dice que esta especialidad de la Auditoría está recién dando sus primeros pasos en Chile. Existe mucha confusión al respecto. Aclaró que la Auditoría Externa no cumple en absoluto un rol forense; ella tiene el propósito de dar una opinión de los aspectos más significativos de los estados financieros, para un aseguramiento razonable de la información, en base a muestreos. Por otra parte, la Auditoría Interna es una actividad de monitoreo permanente, siendo parte del Control de Gestión, por tanto, tiene un objetivo disuasivo frente a posibles malas prácticas. La Auditoría Forense, en cambio, se trata de DETECCIÓN E INVESTIGACIÓN, y comienza en base a un hecho irregular gatillador, llamado “predicamento”, teniendo un enfoque criminalístico-investigativo.

Para mayor aclaración, el término “Criminalístico” implica “Investigación” y “Delito”. Y cuando lo “criminalístico” es base de información que va al Tribunal, estamos hablando de “Forense”. Por lo tanto, una Auditoría Forense tiene un resultado que será utilizado por tribunales y, por tanto, su estándar debe ser alto para ser prueba legal.

Las falencias más comunes por las que se producen los fraudes son la falta de control interno o su desactualización, escaso involucramiento de la gerencia en el control interno y escasa disciplina del Gobierno Corporativo. En definitiva, se trata de la conducta personal de los miembros de la organización.

¿Qué debemos entender por “fraude”?

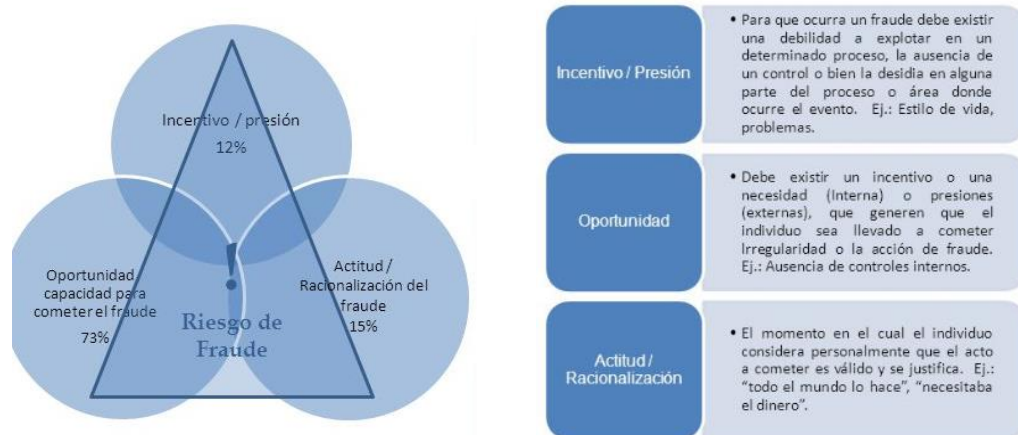
La utilización del cargo de una persona para su enriquecimiento personal a través del mal uso o mala aplicación, de manera deliberada de los recursos o activos de propiedad del empleador (ACFE)

Cualquier acto ilegal caracterizado por engaño, ocultación o violación de confianza. Estos actos no requieren la aplicación de amenaza de violencia o fuerza física. Los fraudes son perpetrados por individuos y por organizaciones para obtener dinero, bienes o servicios, para evitar pagos o pérdidas de servicios, o para asegurarse ventajas personales o de negocio. (IIA)

El uso de acciones que buscan presentar ante los inversionistas, analistas y/o mercado una situación no realista de la Compañía, con el fin de cumplir con las expectativas de alguno o algunos de los grupos de interés. (AICPA)

En resumen se considera fraude, cualquier acto ilegal caracterizado por engaño, ocultación o violación de confianza, sin violencia física. En general, se entiende como cualquier falta a la cultura y normas internas de la organización. Las razones que se esgrimen para que ocurran los fraudes son: Crecimiento explosivo, “no tuvimos tiempo de ordenar la casa”; Colusión (se concertan personas para relajar los controles); Conducto regular de denuncia muy burocrático y tedioso; y Desidia de la administración (no cree que le puede pasar a ellos y considera alarmistas algunas opiniones de denuncia).

Teoría del TRIANGULO DEL FRAUDE, de Donald R.Cressey.



La Auditoría Forense incluye indagación, es decir, el proceso reflexivo para determinar el predicamento, el cual debe documentarse adecuadamente, y luego la investigación, que es el proceso para obtener evidencia del delito y profundizar los hallazgos. Las irregularidades encontradas y probadas pueden terminar en desvinculación o querrela, y se hace para recuperar dinero, sentar precedente y/o para mantener la honra de la persona o institución violada.

Es necesario que las organizaciones chilenas progresen en estos aspectos y que sus ejecutivos den la debida importancia al Control Interno. Como complemento de esta excelente exposición del expositor Christian Nino-Moris, el profesor Pedro Hernández nos expone sobre la Gestión Integral de Riesgo Corporativo (GRC), cuyo objetivo es ayudar a preservar el valor de las organizaciones en

el largo plazo, dado que “nadie está ajeno al riesgo empresarial, sin importar tamaño, tipo y composición de las organizaciones.

¿Qué es el riesgo corporativo? Riesgo de imagen, incumplimiento de normativas (Ambientales, financieros, recursos humanos, regulatorios, operativos, Continuidad del Negocio, etc.).

Es una amenaza de que algo malo ocurra o de que algo bueno no ocurra. De acuerdo a la definición otorgada por el estándar australiano AS/NZS 4360:1999 riesgo es la posibilidad que suceda algo que tendrá un impacto sobre los objetivos. Se mide en términos de consecuencias y probabilidades. La incertidumbre siempre la tenemos, producto de la globalización, cambios tecnológicos, reestructuraciones, competencia, ciberataques, cambios de mercado, etc. Pero todos ellos, de ocurrir, no llevan a una destrucción de valor de la organización, ya sea cualitativo o cuantitativo.

Según el nivel de la organización, tenemos dos tipos de riesgos: estratégicos, a nivel de gerencia y operacionales. Los primeros son más fáciles de administrar y su control puede hacerse sin o con poco apoyo tecnológico, pues son menos en cantidad. Los operacionales deben controlarse en forma automática, con alto apoyo tecnológico, pues son muchos, por cada operación dentro de cada unidad de negocio de la organización. El apoyo tecnológico se hace a través de SAP u otros sistemas similares. La idea es llegar a confeccionar y administrar un Mapa de Procesos de Negocios, con riesgos estratégicos y operacionales y sus respectivas probabilidades de ocurrencia, y con los controles y actividades asociadas a cada uno. Los responsables de los procesos y actividades asociadas deben estar claramente identificados. Dado que este es un proceso dinámico, es necesaria una gestión apoyada en tecnología.

La administración de riesgos empresarial se puede definir como la disciplina que busca incrementar el nivel y la estabilidad del valor económico de la empresa, identificando, midiendo y monitoreando las incertidumbres a las que está expuesta; de tal manera que se optimicen las decisiones sobre riesgo y capital. *(Fuente: Rurik Magos. Revista Electrónica “Actuarios Trabajando”. CONAC, 2009).*

La gran pregunta es ¿cómo administramos la GRC de manera holística y compleja? Los grandes problemas que enfrentamos para una buena administración del riesgo corporativo son: Controles manuales con poco uso de tecnología, riesgos desconectados de los objetivos estratégicos, ejecutivos aislados, procesos y herramientas diferentes no coordinadas entre sí. Un modelo ERM (Enterprise Risk management), hace que todas las unidades de la organización actúen integrada y sistematizadamente, en forma permanente. Esto implica un enfoque corporativo, una gestión de riesgos integrada y basado en programas con fuerte ayuda tecnológica.

La gestión de riesgos es un proceso integral que debe estar alineado con los objetivos estratégicos corporativos. Una Gestión de Riesgos Integral adecuada nos dará una seguridad razonable, nunca absoluta. La gestión de riesgos persigue la disminución de las probabilidades de los impactos negativos en un proyecto o en determinada actividad de la empresa y, al contrario busca aumentar las probabilidades de que se produzcan impactos positivos en esas actividades.

Usualmente, uno de los pasos iniciales para una organización en el desarrollo de su gestión de riesgos es la estructuración de un mapa de riesgos estratégicos.

Ejemplo matriz de riesgo y controles.

MATRIZ DE RIESGO Y CONTROL																									
PROCESO		IDENTIFICACIÓN Y EVALUACIÓN DEL RIESGO						IDENTIFICACIÓN Y EVALUACIÓN DEL CONTROL								PLAN DE MEJORA									
Id. Proceso	Proceso	Id. Actividad	Id. Riesgo	Descripción del Riesgo (Evento/Causa/Efecto)	Impacto	Probabilidad	Riesgo Inherente	Id. Control	Descripción del Control (Medida/Cebs/Indicador/Cómo/Por qué?)	Responsable	Sugerencias de Parámetro	Evidencia del Control	Efecto del Control	Documentación del Control	Periodicidad	Opportunidad	Naturalidad	Evidencia Directa del Control del Evento	Clasificación del Evento	Riesgo Residual	Respecto al Riesgo	Id. Mejora	Oportunidad de Mejora Seguros		
4.42	Proceso de Mantenimiento	4.42.1	4.42.1.1	El equipo de mantenimiento no realiza a tiempo los trabajos de mantenimiento preventivo de los equipos generadores del sistema de generación de energía eléctrica, lo que puede ocasionar un paro de generación de energía eléctrica.	Alto	Alto	Alto	4.42.1.1.1	El equipo de mantenimiento realiza a tiempo los trabajos de mantenimiento preventivo de los equipos generadores del sistema de generación de energía eléctrica.	Equipo de Mantenimiento	Horario de trabajo	Reportes de mantenimiento	Reportes de mantenimiento	Reportes de mantenimiento	Reportes de mantenimiento	Reportes de mantenimiento	Reportes de mantenimiento	Reportes de mantenimiento	Reportes de mantenimiento	Reportes de mantenimiento	Reportes de mantenimiento	Reportes de mantenimiento	Reportes de mantenimiento	Reportes de mantenimiento	Reportes de mantenimiento

Hay una ecuación básica: OBJETIVO + RIESGO - CONTROL = EXPOSICIÓN

En el Riesgo tenemos probabilidad e impacto de ocurrencia. En el Control tenemos el diseño del sistema y su operación.

Otro tema importante son los “Frameworks”, que son buenas prácticas estándar a cualquier industria, que podemos aplicar a nuestras organizaciones. Destacando el más conocido, es decir el estándar australiano-neozelandés: AS/NZS 4360:2004, padres de este estándar, entre otros estándares y normas, se encuentran la guía ISO 31000, el estándar de continuidad de negocio ISO 22301, o lo referente a COSO ERM Integrated Framework, Basilea (Conjunto de principios y recomendaciones del Comité de Basilea sobre la Supervisión Bancaria) y COBIT (Objetivos de control para la información y tecnologías), entre otros.

¿Cómo controlo la gestión del negocio? A través de los KPI. ¿Cómo los preservo? A través de los KRI (indicadores de control de riesgo).

Retención y Transferencia del Riesgo

Retención del Riesgo: El auto-seguro es aquella situación en que una persona, ya sea física o jurídica, soporta con su propio patrimonio las consecuencias que se pueden derivar de los posibles siniestros en su giro comercial o industrial, es decir, sin recurrir a la intervención de ninguna aseguradora.

Transferencia del Riesgo: Cuando la empresa decide no auto-asegurarse, busca entonces transferir el riesgo. En este caso una persona pacta con otra a través del pago de una prestación, una contraprestación para resarcir el daño económico que un acontecimiento a futuro e incierto pueda causar un deterioro en su patrimonio.

En Resumen: Actualmente Chile está en un grado de madurez muy bajo en estas materias y debemos capacitar a las personas para que haya una Gerencia comprometida con estos temas, indexar bonos a los KRI y hacer una evaluación REAL del desempeño. No obstante cabe destacar

que hoy en día a nivel país la industria financiera es la más avanzada en materia de Gestión de Riesgos, dada la intervención de los entes reguladores (SVS, SBIF, etc). Le siguen la AFP's, compañías de seguros, Cajas de Compensación, Retail, Energía y Minería.

Como se observó, el riesgo siempre va a existir, es imposible vivir sin riesgo, pero sí se puede de algún modo administrarlo y disminuirlo en la medida de lo posible. Absorberlo o transferirlo es lo que queda a discreción del empresario y esta decisión se debe tomar de forma conjunta con el administrador de finanzas.

Decidir retenerlo o transferirlo depende de los costes de oportunidad de los riesgos, las dificultades externas a la empresa, la imposibilidad de encontrar en el mercado de seguros las coberturas adecuadas y otros factores, como el que no existan proveedores confiables o bien los costos de estos sean muy difíciles de cubrir; todo esto obliga a que los empresarios realicen un análisis de la retención de riesgos en la empresa.

Con frecuencia, en esta idea, algunos de los problemas planteados por la retención pueden solventarse a través de la experiencia adquirida y el tratamiento apropiado que posibilite una adecuada predicción de riesgos. Con esta base, los empresarios pueden decidirse por una retención financiera, ya sea total o bien parcial, de eventualidades que se presenten en la empresa.

Con todo, es importante que se ejecute un método de análisis para basar con criterios objetivos un proceso racional de decisión en este rubro

Finalmente, es importante definir e implementar una política de gestión de riesgos, sin embargo esta no tiene sentido si no se garantiza que ésta sea socializada, comunicada y divulgada a toda la organización.