La auditoría que se viene. Una realidad en nuestras empresas

Calvino, Gustavo A.

Abstract: En el artículo se analiza cómo los cambios en las modalidades de negocio y de la administración, impactan fuertemente en los aspectos de control interno y por carácter transitivo, en la labor de los auditores.

Si bien hay varias formas de "dividir" o "clasificar" la auditoría, en particular prefiero la que la segrega en dos grandes grupos:

- Auditoría tradicional: definimos así a aquella que surge de un plan de auditoría anual, aprobado por el Comité de Auditoría (en caso de corresponder), basada en planes de revisión generalmente estandarizados.

En esta auditoría realizamos una revisión de cierta cantidad de objetos, que pueden surgir de algún sistema de muestreo (contratos, facturas, remitos, inventario físico, pagos, arqueos, conciliaciones, etc.).

Finalizada la etapa de revisión, confeccionamos el informe, lo discutimos con los responsables del área auditada y lo emitimos.

Este proceso, dependiendo la magnitud de la empresa y de la revisión, desde que se inicia hasta la emisión suele demorarse en promedio 45 días. Seguramente hay numerosas entidades que están por debajo de este promedio y otras que lo superan ampliamente.

La base de muestreo, objeto de la auditoría, puede ser el año calendario anterior a nuestra revisión, el semestre anterior o un año móvil.

- Auditoría en tiempo real: definimos así a una auditoría basada en "Alertas" que surgen de un set de indicadores que monitorean constantemente los sistemas transaccionales de la empresa.

Estas alertas surgen de un análisis del total de los registros de la empresa en forma diaria, semanal o mensual (depende de la periodicidad de ejecución definida para cada indicador) y nos indican, en principio, que algún proceso o procedimiento habitual no se ha cumplido conforme a lo previsto, pero no implica que sea un ilícito o un hecho sujeto a informar.

Esta auditoría es puntual, no tiene un plan de revisión estandarizado, sino que se confecciona en cada caso "a medida" y conforme a las respuestas que se reciben y a la documentación de respaldo que aportan las áreas consultadas / auditadas.

Ambos tipos de auditoría son necesarias y presentan aspectos a favor y en contra.

La idea es que a lo largo de este artículo podamos "discutir" sobre lo que humildemente creo que es lo que se viene en materia de auditoría.

Si al menos logro que reflexionemos sobre los equipos de trabajo (enfoque de la auditoría, objetivo de auditoría, relación con la Alta Dirección, capacitación de recursos, desarrollo de habilidades, entre otros), mi tarea se ha cumplido.

I. Tiempos de cambio: en la legislación, en los negocios y en su administración

Los avances y cambios tecnológicos en los procesos productivos y administrativos, de vinculaciones entre los "actores" de un mercado, son conocidos por todos.

Solo por mencionar algunos de los que afecta directamente a nuestra labor de auditores:

- Cobranzas y pagos: podemos realizarlos a través de una aplicación en una "red social", utilizando cualquier medio (tarjeta de crédito, tarjeta de débito, transferencia bancaria, etc.).

Quedó atrás el cobro con un medio de pago específico (efectivo, tarjeta de crédito, tarjeta de débito) o con una tarjeta determinada, a la cual había que presentarle una liquidación periódica.

- E-commerce: el mercado electrónico es una herramienta de marketing cada vez más difundida y no solo en redes sociales, sino en empresas de envergadura que comercializan sus productos y servicios a través de sus sitios web.

- Cambios tecnológicos y mercados universales: afectan directamente o en forma indirecta al "objeto de negocio".

La tecnología y la universalidad de los negocios avanzan a un ritmo complejo de seguir y las empresas siempre quieren estar a la vanguardia.

Es un caso de estudio el hecho de una empresa de fotografía que se dedicó a mejorar la calidad del revelado y de los rollos de fotos, mientras le pasaba la ola de las cámaras digitales.

- La nube: Los sistemas informáticos migran del procesamiento de datos en un equipo instalado en nuestras dependencias, hacia otro ubicado en "la nube". La citada "nube" es un lugar al cual no tenemos acceso físico y quizás ni siquiera sepamos dónde se ubica físicamente.

- Hardware: los smartphones son computadoras complejas desde las que se pueden realizar prácticamente la totalidad de las operaciones de las empresas.

Sin embargo, su resguardo físico es tan endeble que se pueden olvidar en la mesa de un bar, restaurante o perderse en la playa.

- Firma digital: en diciembre de 2001 se sancionó la ley nacional 25.506 que le da a la firma digital el mismo valor que la firma holográfica.

En las empresas a partir del año 2013/2014 se ha intensificado el uso de esta herramienta, en la firma de contratos, convenios, etc.

El clásico "remito conformado" o "contrato firmado" ahora tiene una conformidad electrónica en lugar de la clásica firma holográfica.

- Ciberataques: nuevos riesgos de intrusión a los negocios de nuestras empresas.

Hoy quizás por diversión, quizás por "reto" entre hackers, quizás por malestar de empleados o exempleados, terceros intentan acceder al proceso productivo, a los sistemas administrativos y operativos, a la funcionalidad de nuestras plantas productoras, a las cámaras de monitoreo, etc.

El fin puede ser solo mostrar una debilidad y luego percibir un honorario por solucionarla, o bien tener una primicia ante un problema productivo o simplemente hacerle un daño a la empresa.

- Formas de trabajo: es tendencia mundial y no escapa a las empresas locales, la conciliación de la actividad laboral con la familiar y/o personal.

Esto genera que las empresas implementen modalidades de trabajo a distancia, bajo el concepto de home office. Incluso esta modalidad ha provocado que se encuentre en crecimiento un concepto de negocio, que en Argentina comenzó a desarrollarse allá en los albores de los años 2000, que es el de "estaciones de trabajo móviles".

- Ley de Responsabilidad Penal Empresaria (27.401): esta ley, sancionada a fines de 2017, que entró en vigor en marzo de 2018, pone el foco en las empresas como responsables de los actos de corrupción.

Impone sanciones que implican:

- Multa equivalente a 2 a 5 veces el beneficio indebido obtenido o que se hubiese podido obtener.

- Suspensión total o parcial de las actividades.

- Imposibilidad de participar en concurso y licitaciones públicas.

- Disolución y liquidación de personería cuando hubiese sido creada al solo efecto de cometer delito o esos actos constituyen la principal actividad.

- Pérdida o suspensión de beneficios estatales.

En su art. 9º, la ley 27.401 establece que, como condición de exención de pena entre otros aspectos, las empresas deben implementar un "Programa de Integridad" (arts. 22 y 23 de la ley).

El dec. 277/2018 del 5 de abril de 2018 estableció que la Oficina Anticorrupción del Ministerio de Justicia y Derechos Humanos establezca los lineamiento y guías para el cumplimiento de los arts. 22 y 23 de la ley 27.401.

Ahora bien, nosotros como auditores (en cualquier nivel de la organización) los conocemos, pero:

- A la Alta Dirección, ¿le preocupan estos aspectos? ¿Quiere que los auditemos?

- ¿La empresa tiene identificados estos riesgos / procesos?

- ¿El plan de auditoría tiene mapeado estos riesgos / procesos?

- ¿Los equipos tienen los conocimientos adecuados para auditar estos aspectos?

- ¿La empresa tiene un equipo de Auditoría de Sistemas desarrollado?

- Ese equipo de Auditoría de Sistemas, ¿cuenta con un laboratorio para realizar actividades de ethical hacking?

- Contempla el plan de auditoría, ¿algún proyecto para auditar la implementación y cumplimiento del "Programa de Integridad" de la empresa?

- El plan de auditoría, ¿contempla el plan la revisión de denuncias por parte de los auditores?

Como vemos, nos encontramos en un mercado cambiante, sumamente tecnológico, ampliamente conectado a través de las redes sociales, con posibilidades de desempeño laboral en diversos ámbitos (algunos más privados que otros, pero ambos fuera del concepto de "oficina").

A su vez, cada vez más se van difundiendo normas que eran solo aplicables a empresas que cotizaban en Nueva York u otras bolsas internacionales, a empresas del ámbito local.

Los planes de auditoría de las empresas y los programas de trabajo deben adecuarse a este escenario.

II. Nuevos desafíos para los paradigmas clásicos de auditoría

Hago un comentario personal. Cuando me inicié en auditoría interna, hace algunos años, recuerdo que había 2 paradigmas o aspectos, que me resaltaron en su momento:

- El plan de auditoría lo aprobó el Comité de Auditoría y debe ser cumplido sin modificaciones.

En relación con este aspecto, algunas empresas se reservan entre un 10 y un 15% de las horas totales, para tareas "no planificadas" (léanse: denuncias, pedidos especiales, participaciones en tareas específicas, etc.).

- La auditoría no se encarga del fraude. Es responsabilidad del negocio.

Incluso recuerdo que en la misión de alguna de las empresas que conocí, figuraba tácitamente: "La detección de hechos de origen fraudulentos no es objeto de esta auditoría".

En general, todos los auditores comenzamos el proceso de auditoría con la planificación anual.

Esta planificación la podemos realizar por diversos métodos (que no es intensión comentarlos en este artículo), por riesgos, por procesos, un mix de ambos, por línea de negocios, etc.

Así es que, en la planificación, tenemos un inventario de aquellos procesos/riesgos/negocios que consideramos que debemos auditar en "algún momento" y habitualmente, a efectos de optimizar los recursos, le asignemos una criticidad.

De esta forma, tenemos un "mapeo de procesos y riesgos" de la sociedad con su correspondiente criticidad asignada y según los recursos de nuestro "equipo de auditores" planificamos las revisiones a realizar en los próximos años, poniendo énfasis en el plan del año venidero.

A fin de validar el plan, lo exponemos ante el Comité de Auditoría, que es el órgano que "aprueba" la labor del auditor.

Ahora bien, en este complejo proceso, descripto muy sucintamente, se encuentran presentes varios paradigmas. Solo por mencionar algunos, debe entenderse que el plan anual:

- Comprende el universo auditable, sea que estemos hablando de procesos, de riesgos o líneas de negocio.

- Surge de un proceso de asignación de riesgos y a partir de la aplicación de una metodología de evaluación y asignación de criticidades.

- Se encuentra en línea con los recursos que disponemos.

- Aprobado por el Comité de Auditoría debe ser cumplido en el ejercicio o justificar debidamente las causas por las cuales no se ha realizado algún proyecto de los previstos.

En relación con este aspecto, no es habitual que las empresas revean a lo largo del año el plan y lo modifiquen.

Estos paradigmas, históricos y generalmente aceptados por todos los auditores, son válidos y deben estar presentes, pero les propongo que analicemos los siguientes hechos:

- ¿El plan contempla la visión de la Alta Dirección para la empresa?

- ¿Está representado en el "mapeo de procesos y riesgos" el rumbo previsto para la empresa?

- Los cambios del mercado y/o políticas del país, ¿se encuentran identificados?

- ¿El plan es "secreto" o es conocido por la Alta Dirección?

- ¿Los cambios de la legislación debieran ser contemplados por la empresa? ¿Qué impacto tienen en nuestra planificación?

- Las actualizaciones informáticas y/o de procesos están consideradas? ¿Alguien las está analizando? ¿La empresa las quiere adoptar?

Si no se están analizando, ¿son un riesgo para la continuidad de alguna de las líneas de negocio?

- Los recursos actuales, con sus conocimientos actuales, ¿son los adecuados para auditar en 2 o 3 años?

El plan de auditoría no debiera contemplar un horizonte menor a 4 o 5 años vista, así no solo tendríamos ese universo auditable, sino que estaríamos monitoreando las "habilidades" que se requerirán en los equipos.

- Si la empresa posee una línea de denuncias, ¿tenemos previsto un tiempo para analizar los hechos denunciados, que pudieran afectar los procesos de control establecidos?

- ¿Qué tipo de auditoría estamos planificando?

a) La auditoría tradicional, con:

- Tiempo de preparación - Pre auditoría

- Tarea de campo

- Tiempo de discusión de hechos relevados y emisión de informe

b) La auditoría en tiempo real, que:

- Surge a partir de "alertas" o "red flag" en los registros de la empresa.

- Su tarea de campo es variada. No se puede estandarizar. Son revisiones puntuales de hechos disímiles.

- No tiene tiempo de discusión, o es mínimo porque la revisión fue puntual.

c) Un mix de ambas, con tiempos asignados para ambos tipos de revisiones.

III. Nuevos riesgos. Nuevos procesos de auditoría

Como vimos, hay cambios en las modalidades de negocio y de administración que impactan fuertemente en los aspectos de control interno y por carácter transitivo, en nuestra labor como auditores.

Nos enfrentamos a nuevos riesgos o a riesgos conocidos, pero que "actualizaron" su impacto o forma de cometerse.

Así es que hoy podemos enfrentarnos, entre otros, a:

- Riesgo de imagen societaria: Hoy, con la difusión de las redes sociales y el alto impacto que estas tienen en los consumidores finales, una "filtración de una imagen no adecuada" rápidamente escala a niveles impensados.

Se viraliza una mala imagen de la compañía, que demandará años y altos costos cambiarla.

- Riesgo de filtración de información: hoy, aquellas empresas que se encuentran en un fuerte plan de reconciliación laboral y familiar prevén el acceso a información confidencial y secreta de la compañía desde distintos lugares, como dijimos algunos más "privados" que otros.

Este acceso, implica un alto riesgo de acceso a información privilegiada de personas no autorizadas.

- Riesgos de ciber-ataques: hay generaciones que podrían reírse horas respecto a este riesgo, sin embargo, está presente en Argentina y en el mundo, haciendo verdaderos desastres empresariales.

Las empresas en general, recién en los últimos 2 o 3 años comenzaron a tomar verdadera conciencia sobre este riesgo y su altísimo impacto, tanto en la sociedad (persona jurídica) como en sus empleados.

- Riesgos asociados a la información en la nube: el concepto de desarrollar los sistemas en la nube, cada vez toma mayor fuerza en las grandes empresas y es de esperar que en un tiempo prudencial todos estemos con nuestras aplicaciones en la nube.

Ahora bien, en estos momentos en los que se puede mezclar "tendencia" con "moda", ¿las empresas están evaluando todas aquellas soluciones que se les presentan asociadas a desarrollos en la nube?

Por otro lado, ¿estamos seguros de que los datos de nuestros clientes, proveedores y colaboradores están a

resguardo en la nube? La Ley de Protección de los Datos Personales (25.326), ¿que indica respecto a esta situación?

- Aplicación de la Ley de Responsabilidad Penal Empresaria (27.401): ¿estamos considerando los riesgos asociados a no poseer un adecuado "Programa de Integridad"? ¿O que este no se cumpla?

En relación con este aspecto, no olvidemos The Foreign Corrupt Practices Act (FCPA), de los Estados Unidos y las UK Bribery Act, que traspasan las fronteras de sus países y aplican a varias de nuestras empresas.

La demanda de transparencia del mundo se encuentra en constante movimiento y requiriendo cada vez más la aplicación de políticas y leyes de apertura de información tanto a los funcionarios públicos como a las empresas.

Esta mayor apertura de información trae aparejado un mayor proceso de control sobre las operaciones de la empresa, los socios, clientes, proveedores, etc.

- Nuevos riesgos laborales: estos riesgos son los originados en las nuevas metodologías de trabajo, en las que quizás no se den las condiciones físicas adecuadas (desde temas de salud laboral —como ser posturas óptimas o que generen enfermedades o afecciones físicas—, hasta aspectos de confidencialidad / seguridad de la información con la cual nos encontramos trabajando).

IV. Hacia una nueva auditoría

Como vemos, hay cada vez mayor demanda del concepto "auditar". En mi opinión es un momento ideal para subirse a esta, que llamo la "segunda ola de control" (la primera fue allá por los años 2006/2007, con la implementación de la Ley Sarbanes Oxley - SOX).

En esta segunda ola, considero que debiéramos darle un mayor protagonismo a:

- Auditoría de Sistemas: hoy, con los avances tecnológicos que vemos día a día, con la mayor automatización que buscan las empresas, no sería concebible un equipo de auditoría que no tenga un área especializada en este tipo de revisiones.

Dos preguntas para hacernos en este punto serían:

- ¿Cuántos auditores de sistemas tenemos en el equipo?

- ¿Qué porcentaje representan sobre el total de auditores?

En caso de que las respuestas sean similares a las que siguen a continuación, es un buen momento para el replanteo.

- Ninguno

- Menos del 10% de la dotación total de auditoría interna

Las revisiones de este tipo de auditoría debieran ir más allá del clásico análisis de funcionalidad de una aplicación, revisión de permisos y mantenimiento del soft/hard asociado.

Hoy, el riesgo de intrusión a nuestros procesos productivos automatizados, a las cámaras internas de monitoreo, sumados a los clásicos riesgos de acceso a los sistemas de administración (pedidos, compras, pagos, cobranzas, recursos humanos, etc.), podrían llevar a la extinción de la empresa.

Son riesgos que en un primer momento se minimizan, porque nos preguntamos la probabilidad o frecuencia de ocurrencia. En este aspecto, he tomado conocimiento que aquellas empresas en las que sucedieron estos hackeos no tuvieron la oportunidad de contestarlas.

Creo que, en este sentido, hoy debiéramos estar pensando en el desarrollo de un laboratorio de auditoría de sistemas que pueda, bajo ciertas condiciones, desarrollar los conceptos de ethical hacking que, aunque suene contradictorio (hackeo ¿ético?), es esencial para conocer a qué estamos expuestos en la organización.

En este tipo de revisiones, sugiero que evaluemos la opción de "trabajar" en forma conjunta con el área responsable de Seguridad de la Información.

Hay organizaciones que poseen un laboratorio en el área de Auditoría de Sistemas desde hace algunos años, pero la mayoría de las empresas aún ni tienen los ciber-riesgos en su "radar".

- Auditoría tradicional: debemos actualizar los programas de revisión, de selección de muestras, relacionar

cada día más estas revisiones con los indicadores de la auditoría en tiempo real. Los tiempos de informe y de discusión debieran tender a cero.

Todo ello, apuntando a tener una revisión "integral" pero ágil y que prácticamente al finalizarse el trabajo de campo, los resultados sean conocidos por la Alta Dirección.

Varias empresas trabajan arduamente en este sentido, porque suele ser la mayor crítica por parte de sus autoridades (suele ser poco efectivo decirle a la Alta Dirección el 15 de enero de 2019, que en marzo de 2018 se contrató por encima de los valores de mercado y que el servicio se finalizó el 31 de octubre).

Quizás debamos evaluar más auditorías de este tipo, en menores plazos de duración y con mayor periodicidad. Este análisis probablemente nos indique que se requieren más recursos, pero antes de solicitarlos (a la Alta Dirección y/o Comité de Auditoría), aconsejo que probemos el cambio en los planes, su alcance y evaluemos el verdadero impacto en la organización.

Dos aspectos no menores para tener en cuenta en estas revisiones son:

- Participar del proceso de elaboración del plan a la Alta Dirección, a efectos que pueda incorporar su visión macro, indicándonos aspectos a considerar o a descartar.

- Reevaluar el plan anual de auditoría, al menos una vez al año. El plan es una herramienta esencial para hacer una auditoría dinámica y no predecible, pero para ello debiera reconsiderarse si hay nuevos hechos que lo ameriten.

- Auditoría en tiempo real: es una herramienta muy mencionada en cursos, foros de discusión, programas de estudio, etc.

Ahora, ¿cuántas empresas han implementado un verdadero sistema de auditorías que consulten hechos que sucedieron en las últimas 48/72 horas, incluso en la última semana o en el último mes?

Estas alertas tempranas, solo nos van a permitir detectar hechos que se salen de algo reglado por las normas y procedimientos de la compañía.

La auditoría en tiempo real no reemplaza a la auditoría tradicional, sino que la complementa. En la auditoría tradicional, un auditor analiza una serie de hechos que van más allá de lo que posiblemente se pueda desarrollar como un indicador.

La auditoría en tiempo real nos permitirá "prevenir" en cierta forma el fraude en la empresa. Al darle mayor visión al auditor, sumado a que quien intenta cometer un ilícito no sabe en qué momento aparecerá un auditor consultando por un hecho particular, propician un mayor "ambiente de control".

En relación con este hecho, contar con un equipo de auditores especializado en este tipo revisiones, sería un objetivo a plantearse por los departamentos de auditoría de las empresas.

Este equipo de auditores es aconsejable que no sea el mismo que analiza las revisiones de auditoría tradicional, dado que tiene que estar más enfocado a analizar un solo aspecto y eventualmente, a partir de este hallazgo, expandir su revisión.

Podemos tener dos equipos de auditores e intercambiarlos con cierta frecuencia, para que ambos tengan habilidades similares, pero hay que darle un tiempo a cada auditor para que internalice los conceptos de ambos tipos de revisiones.

- Auditoría de denuncias o auditoría forense: ante todo, es imprescindible definir si la empresa requiere implementar un "Programa de Integridad". En caso de tener una respuesta afirmativa, este tipo de revisión pasa a ser uno de los focos del cumplimiento de la ley 27.401.

A mi entender, las denuncias que se reciben en la Línea Ética / Línea de Denuncias o como se denomine en cada empresa (implementada para dar cumplimiento de la ley 27.401 o por decisión empresarial), es esencial que sean analizadas por un equipo de auditoría.

Los auditores internos, por definición, son quienes tienen el mayor conocimiento de los aspectos de control, normativos y de procedimientos de la empresa. A su vez, son responsables, en cierta medida, de garantizar los procesos de control establecidos en la empresa (tema de discusión para otro momento).

Por su parte, una denuncia conlleva implícitamente una "falla" en los sistemas / procesos de control de la empresa.

Dependiendo de la antigüedad de los hechos denunciados, además de preguntarnos las causas por las que no pudo prevenirse el ilícito, debiéramos preguntarnos los motivos por los cuales no fue detectado por los sistemas de control de la empresa.

Como vemos, ambos aspectos "fallas en la prevención" y "fallas en la detección" debieran ser de incumbencia del auditor interno.

El equipo de auditoría de denuncias o auditoría forense, como prefiero llamarlo, debe tener habilidades especiales de revisión y conocimientos que van más allá de las normas y procedimientos de la empresa.

Este equipo, al formar parte directa o indirectamente del Programa de Integridad, debe estar al corriente de otros aspectos, como ser: nómina de personas expuestas políticamente, resolución de la UIF (11/2011, modificada por la 52/2012), conformación societaria de proveedores y clientes, leyes y normativa relacionada con el lavado de dinero, declaraciones de conflicto de Intereses presentadas por los empleados de la empresa, Registros de firma del Código de Ética, etc.

A su vez, el equipo de Auditoría Forense debiera contar con un laboratorio, dónde implemente sus herramientas de análisis, procesos de revisión y reuniones, que garantice la estricta confidencialidad de las identidades de las personas involucradas y los temas analizados.

Los hechos denunciados van a evolucionar, en la medida que la empresa tenga un programa "serio" de tratamiento de los hechos, reservando la identidad del denunciante, no afectando su desarrollo interno (en caso de ser un empleado) o su vinculación comercial (en caso de ser un proveedor y/o cliente).

Las denuncias en general nos muestran casos que no pueden ser detectados por las revisiones de auditoría tradicional, ni surgen de "alertas" en las auditorías en tiempo real.

Si implementamos un área de auditoría forense, con sus normas y procedimientos específicos, no solo daremos respuestas a los hechos denunciados, sino que se estará dando cumplimiento a una parte del "Programa de Integridad" y lo más importante, detectando debilidades en los procesos de la empresa, que de otra forma sería casi imposible de descubrir.

Un tema particular y que requiere un tratamiento por profesionales experimentados, son las denuncias por "acoso", "maltrato", "discriminación". En este sentido sugiero que, si estos temas van a ser analizados por auditoría interna, se incorpore personal con conocimientos acordes para evaluar estos aspectos.