Auditoría: ¿adelantarnos o adaptarnos a los tiempos actuales?

Calviño, Gustavo

Abstract: Desde hace un tiempo que la labor de los auditores requiere iniciar y finalizar revisiones en muy corto tiempo. Cada vez más se requiere mayor celeridad en los tiempos de revisión y de emisión de informes producto del avance tecnológico en estas acciones.

I. Introducción

Desde hace poco más de un año, nos cambió la vida: la vida familiar y la vida laboral. Nos cambió las reuniones con amigos, los festejos de cumpleaños, aniversarios, casamientos, nacimientos, bautismos, todo... todo ha cambiado.

Muchos de estos cambios, vinieron abruptamente y se van a quedar, ya será muy difícil volver el reloj atrás, acá en Argentina y en el mundo entero.

Esto no es un capricho de unos pocos y durante un tiempo acotado, es una realidad mundial que vino para cambiarnos la vida, la forma de relacionarnos, la forma de trabajo, etc.

Solo tengamos a mano un ejemplo, hasta ahora uno de los mayores logros en materia de combate de virus propagados a nivel mundial: La Viruela (1) (pandemia mundial con una tasa de mortalidad del 30%) demandó casi 200 años desde que se descubrió la vacuna (1796) hasta que se comenzó a erradicar en distintas partes del mundo la enfermedad. En 1967 se comenzó una lucha fuerte con planes de vacunación a nivel mundial y recién en 1980, podríamos decir que se erradicó la enfermedad. Es la única enfermedad que se ha eliminado por completo a nivel mundial gracias a una vacuna.

Dicho esto, ahora con un nuevo panorama mundial y frente a la realidad de nuestras empresas, surgen algunos interrogantes:

— ¿Hubo cambios en nuestras empresas? En las formas de producción, en la comercialización, en el manejo de stock, en la administración, en los sistemas, entre otras áreas.

— ¿Esperamos que esta realidad cambie, que la vacuna tenga efecto y que todo vuelva a ser como el 19 de marzo de 2020 (2)?

— Sabemos ¿cómo nos afectan los cambios en la Auditoría Interna?

— ¿Hay nuevos riesgos? ¿Los relevamos o los intuimos?

— ¿Adaptamos nuestros procedimientos?

— ¿Cambiamos nuestras técnicas de revisión?

— ¿El fraude es el mismo que antes?

—¿Qué rol juegan los sistemas hoy en día?

— ¿Tenemos un equipo de auditores de sistemas?

— ¿Estamos a la altura de los cambios que exige esta nueva realidad?

En fin, creo que estas son algunas de las preguntas que posiblemente nos estemos haciendo a diario desde nuestra labor cotidiana y que trataré de comentar y si es posible, aportar un pequeño granito de arena en este artículo.

II. Oportunidades de desarrollo

En los últimos años se han acentuado una serie de hechos que debieran impulsarnos a generar cambios en nuestra profesión.

Esos cambios debieran incluir desde lo estructural de la organización de un departamento de Auditoría Interna hasta la forma de resguardo de documentación soporte; pasando por los procedimientos de revisión, modalidades de trabajo, enfoque, etc.

Entre estos aspectos, destacamos:

1. Anticipación: Anticipar un posible problema futuro es en términos futbolísticos "hacer un gol de media cancha", es lo que esperan nuestros clientes principales: el Comité de Auditoría, el CEO, el Directorio.

Anticipar problemas de control interno, que afecten lo económico y/o lo reputacional a nuestra empresa, es lo que se espera de cada auditor.

La detección oportuna es buena, pero la anticipación es la gloria del auditor.

2. Presencia: Si bien históricamente se nos requirió mayor presencia en la compañía para generar un mejor "Ambiente de control", hoy es una necesidad de las organizaciones.

A mancera de ejemplo, esta noche (en un noticiero, en un diario, etc.) se hace una denuncia pública sobre un hecho "de fraude", que involucra a empresas y personas y al día siguiente a primera hora, suele suceder:

— Se analizan con Compras los contratos pendientes de ejecución a efectos de constatar si surgen algunos con las empresas involucradas.

— Se comunican con Auditoría a efectos de conocer, si se detectó algún inconveniente en los procesos de contratación y/o certificación de servicios/provisión de materiales, con las empresas involucradas.

— En caso de haberlo observado, las consultas se extienden al análisis de lo detectado, lo recomendado y el estado de cumplimiento de las sugerencias realizadas.

— Respecto de las personas involucradas, surge la inquietud: ¿Sabemos si están en otras empresas que nos brindan servicios o nos proveen materiales?

La mayor presencia del Auditor, a nivel compañía, dejó de ser una sugerencia para ser una exigencia de la Alta Dirección, del CEO, del Comité de Auditoría, de los Accionistas y Directores de la empresa.

Podemos no haber visto el problema puesto de manifiesto (al menos, como en los juegos electrónicos: tenemos un par de vidas), pero en 24 horas se requiere un reporte ad hoc de la situación, un primer relevamiento y un plan de trabajo urgente, con afectación de recursos. Esto es "presencia" en tiempo y en forma.

3. Celeridad: Las gestiones de auditoría requieren resultados a corto plazo. Presentar hechos u observaciones de hechos, con una antigüedad promedio de 6 a 8 meses, no es una opción.

Nuestra labor de auditores requiere iniciar y finalizar revisiones en muy corto tiempo. Cada vez más, se nos requiere mayor celeridad en los tiempos de revisión, de emisión de informes, de consenso de hechos con los auditados, etc.

No podemos tardar un mes y medio desde el inicio de una revisión hasta la emisión del respectivo informe.

Presentar una auditoría que iniciamos en a principio de marzo de 2021 y que, por disponibilidad de los auditados, complicaciones por la pandemia, dificultades para hacernos de las pruebas documentales, etc., etc., la estamos presentando el 22 de junio de 2021, es una realidad, pero no es lo que se espera de nosotros.

Ni hablar, si esta auditoría que estamos presentando, contiene un hecho que sucedió el 14 de agosto de 2020 (porque hicimos una muestra de un año, como alcance de nuestro trabajo y el problema detectado estuvo en un pago realizado en esa fecha). En este caso, casi inevitablemente se generan tres consultas:

— Ahora, casi un año después ¿me lo dicen?

— ¿Podemos hacer algo?

— ¿Por qué no lo vimos antes?

4. Sistemas de información y de operación: Los sistemas probablemente no sean el "Core Business" de nuestras empresas, pero son los que colaboran en gran medida con la "gestión" de la misma.

Los procesos, definidos como "Core Business Processes" de la empresa, son administrados, ejecutados y controlados por Tecnologías de la Información (IT) y por Tecnologías de la Operación (OT).

Hace unos años, en nuestros equipos de auditoría, teníamos eventualmente una persona, que en el mejor de los casos era un "Especialista en sistemas" que, entre otras revisiones, miraba algunas aplicaciones informáticas.

Hoy, la vida nueva, pasa por los sistemas: nos comunicamos, trabajamos en home office, vendemos, cobramos, producimos, etc. a través de los sistemas. No se concibe un negocio sin un sistema soporte.

Ante este avance tecnológico, en Auditoría Interna:

— ¿Tenemos desarrollado un equipo profesionalizado en Auditoría de Sistemas?

— Auditoría de Sistemas: ¿Tiene los recursos (personas, equipamiento, skills profesionales) actualizados y suficientes?

5. Recursos humanos y tecnológicos: Hoy los auditores, no solo deben tener los conocimientos técnicos suficientes, se requiere de una serie de habilidades que son tan imprescindibles como los anteriores:

— Empatía: Un auditor sin esta cualidad, difícilmente pueda lograr concretar una revisión adecuada, máxime en estos tiempos de pandemia, dónde se requiere de la mayor cooperación para organizar entrevistas desde el home office.

— Trabajo en equipo: Sin una adecuada conciencia de trabajo en equipo, no se puede traccionar para el logro de resultados. Hoy estamos en nuestros domicilios, trabajando con un objetivo en común y dependemos de nuestro propio compromiso y control.

— Adaptabilidad a los cambios: Si no cambiamos nuestra forma de revisión, documentación, análisis y emisión de conclusiones, no podremos aggiornarnos a los tiempos actuales. Hoy la "conciliación laboral y familiar" no es un título, un beneficio, una opción. Hoy es una necesidad.

La empresa cambió, se transformó el negocio y el mundo se modificó. Si no nos adaptamos, estamos afuera.

— Tecnología: Hoy estamos cada vez más dependientes de la tecnología. No se puede concebir el concepto home office sin el desarrollo tecnológico. Hoy en un mismo momento podemos tener 3, 4 o 5 puertas de acceso a nuestra información, al mismo momento y no ser consientes.

Los hackers del mundo detectaron que América del Sur tiene importantes empresas, fábricas, industrias y que no cuentan con el concepto de "Ciberseguridad" embebido en sus aspectos de control y desarrollo de personal.

— Capacitación de los recursos: Una falencia que tenemos en general es la falta de recursos orientados a la detección y prevención del cibercrimen. Hasta hace unos años, creíamos que eso era un problema de países desarrollados.

Hoy es una falencia que requiere una inmediata resolución. Incluso los planes de estudio de las facultades están en revisión, tendientes a incorporar materias e incluso orientaciones profesionales para cubrir estos aspectos.

III. Ayer, hoy y mañana

Cuando hablamos de la auditoría que dejamos atrás y hacia dónde vamos, sucintamente estamos diciendo, como evolucionamos como unidad, con: cambios de estructuras, incorporación de nuevos métodos de revisión, ampliación de los requisitos de expertise de los recursos que incorporamos, realización de capacitaciones actualizadas, etc.

Así, vemos como dejamos atrás a la Auditorías por Proceso y Riesgos, para ir a un enfoque más orientado a resultados en el corto plazo:

— Atención de denuncias.

— Revisión de alertas de posible incumplimiento o red flags.

— Desarrollo de nuevas técnicas de revisión de auditorías de sistemas, orientadas a prevenir ciber-ataques.

— Incorporación de técnicas de OSINT (3) en el ámbito de Auditorías orientadas a:

— Revisiones de sistemas.

— Manejo de denuncias.

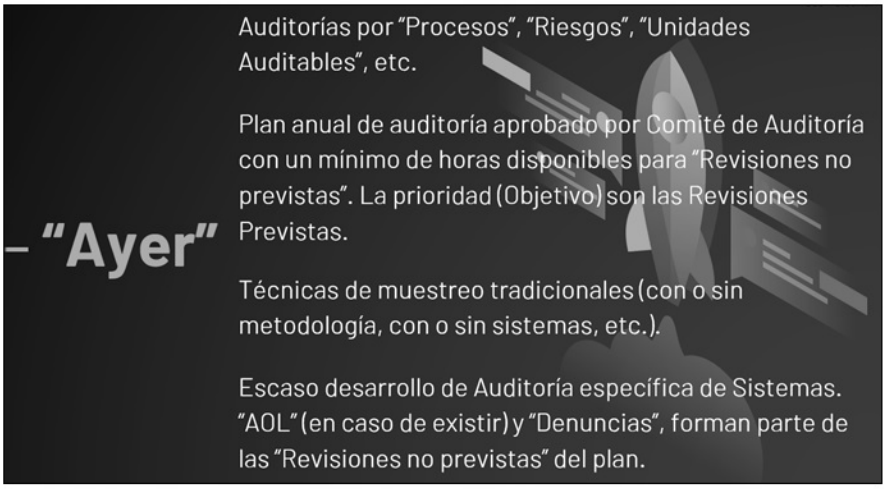
— Prevención del fraude.

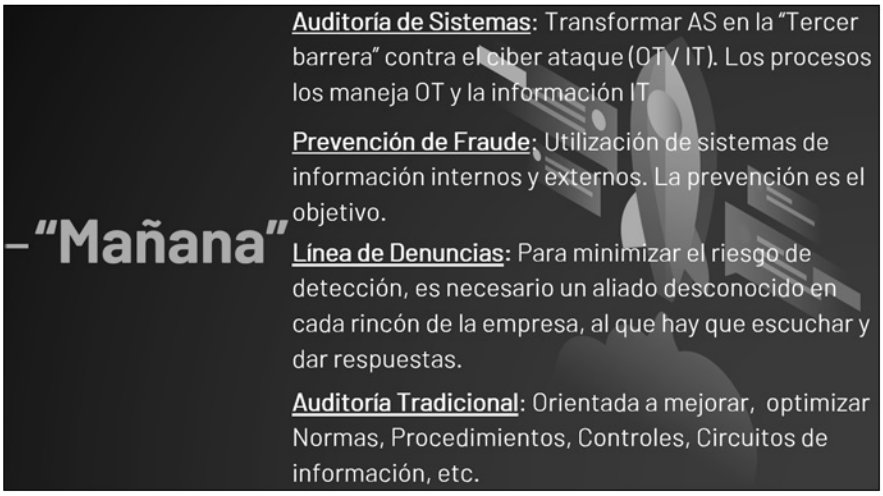
Por otro lado, dejamos de ver "muestras" para ir analizando "universos", con el fin de evaluar comportamientos y determinar posibles tendencias (ambos, orientados a la detección temprana y prevención del fraude).

Incorporamos nuevas prácticas, como lo son los Laboratorios de:

— Ethical hacking en el ámbito de la auditoría de sistemas.

— Revisión forense en análisis de denuncias y prevención del fraude.



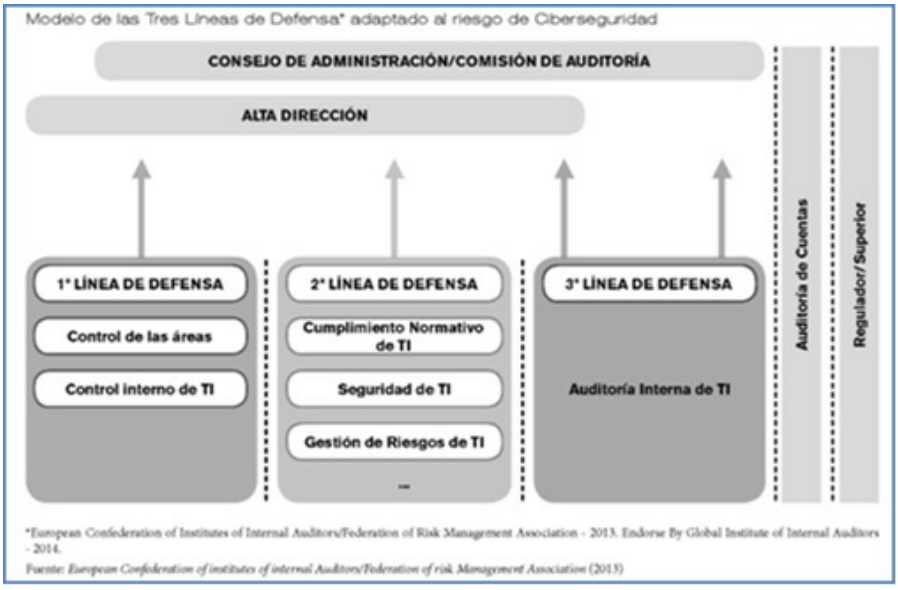


IV. Laboratorio de ethical hacking y laboratorio forense

Estas metodologías de trabajo tienen sus particularidades en la implementación y forman parte de ese futuro que necesitamos desarrollar en Auditoría.

IV.1. Laboratorio de ethical hacking

En materia de ciberseguridad, cada vez más se extiende el concepto de "3 Líneas de Defensa" en las que debiera accionar la empresa:



— Primera línea de defensa: Seguridad en las funciones "propietarias de riesgos". Está a cargo de las Áreas Operativas, Áreas de Negocio y Sistemas de Información.

— Segunda línea de defensa: Seguridad en las funciones que supervisan los riesgos. Está a cargo del Área de Seguridad de la Información.

— Tercera línea de defensa: Seguridad en las funciones que dan un aseguramiento en forma independiente. Está a cargo de Auditoría Interna.

En este marco de acción, implementar un laboratorio de ethical hacking, es un aporte para realizar las tareas que, como auditores, nos tocan en este esquema de "3 Líneas de Defensa".

El laboratorio de ethical hacking desarrolla una actividad de revisión que recurre a diversos métodos, herramientas y técnicas para identificar vulnerabilidades en la configuración física y lógica de un sistema informático de la empresa.

Las revisiones están orientadas a "atacar (en forma controlada) los sistemas de la empresa", para establecer las fallas de seguridad que pueden ser utilizadas para vulnerar el sistema y eliminar, modificar o robar información, realizar cambios en configuraciones o detener o alterar operaciones, etc.

Para lograr un caso de éxito en la implementación de un laboratorio de ethical hacking, es recomendable tener en cuenta, entre otros aspectos:

— Procedimientos internos: Se deben elaborar procedimientos claros y precisos de la actividad que se desarrollará.

Estos procedimientos, si bien sería recomendable que se establezcan en común acuerdo con el CISO de la empresa, cabe señalar que deben mantener la independencia entre Auditoría y Seguridad de la Información.

— Documentar la actividad: Ante un hecho, cualquier integrante de Auditoría y/o Seguridad de la Información deberá poder verificar las acciones realizadas y reproducir las pruebas realizadas en el Laboratorio.

— Monitoreo de los procesos de revisión: Las tareas deben ser realizadas por personal de extrema confianza, en especial sería aconsejable que fuera personal de plantilla. Los procesos de revisión debieran ser monitoreados y cotejados con los "Logs de Auditoría" que muestren la actividad realizada por el auditor en su función de "hacker interno".

IV.2. Laboratorio forense

Este laboratorio es el corazón de la prevención del fraude, de las revisiones de denuncias y de hechos delicados y de extrema confidencialidad.

Dada la complejidad que tiene esta área fuertemente vinculada con el fraude (prevención y detección oportuna), se requiere considerar algunos aspectos, como:

— Implementar procedimientos de acción: claros, específicos y avalados por el Comité de Auditoría.

— Dotar de herramientas de análisis y revisión, que permitan la trazabilidad de las pruebas y su "re-ejecución".

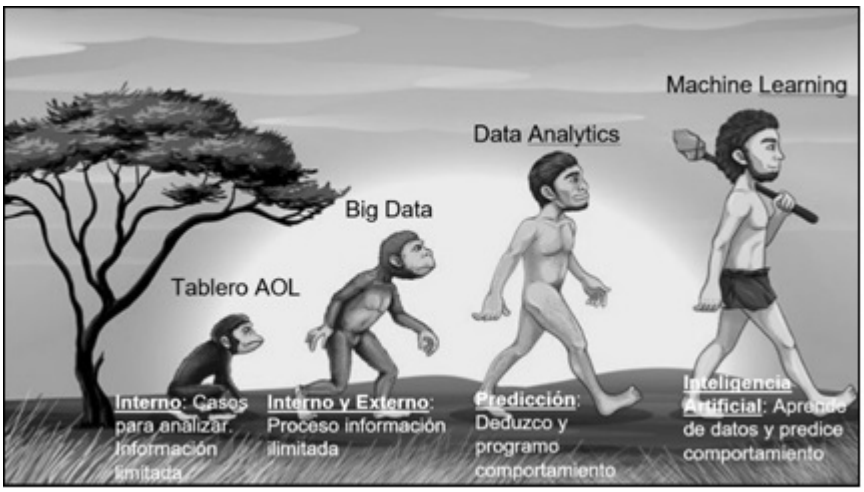
— Utilizar herramientas e información "pública" que permitan realizar un análisis acorde a los requerimientos de la FCPA (Foreign Corrupt Practices Act), la ley 27.401 (Responsabilidad Penal de Personas Jurídicas) y la res. 52/2012 de la UIF (PEP).

— Normas, políticas éticas y código de conducta, fuertes en la compañía, para complementarlos con esta actividad.

— Herramientas de big data / data analytics / machine learning: Estas herramientas muestran la evolución en materia de fraude que tienen los equipos de auditoría.

Desarrollo de herramientas en laboratorio forense: A efectos de orientar recursos económicos, es aconsejable comenzar el desarrollo de un tablero de indicadores de red flag, también conocido como Auditoría On Line (AOL).

Posteriormente, evolucionar al desarrollo de una herramienta de big data, que cruce/analice grandes bases de datos. Cuando estemos maduros en el uso de estas herramientas, podremos incorporar aspectos de predicción manual a partir del comportamiento que observamos (data analytics) y luego llegar al desarrollo de inteligencia artificial, dónde la herramienta nos indicará riesgos a prevenir, con base en los comportamientos que analice.

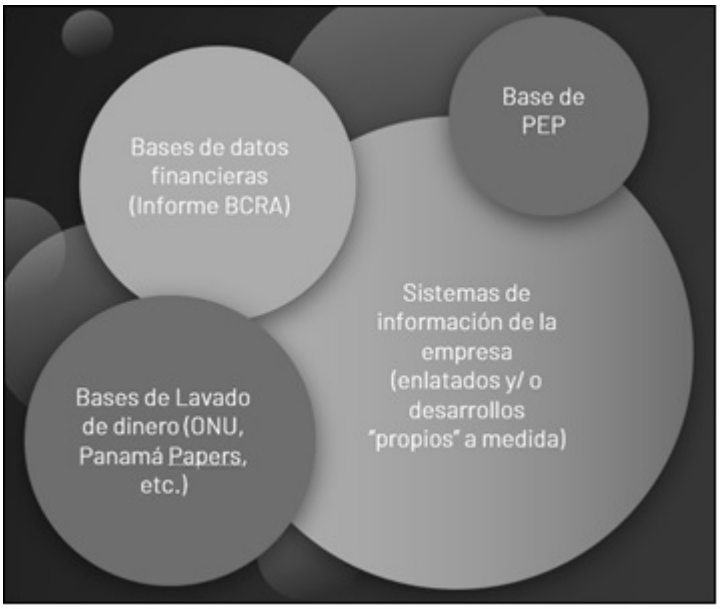


Una herramienta de big data clásica, que podemos desarrollar a bajo costo, debiese incluir información vinculada a: Datos propios de los sistemas de la empresa y algunas bases de datos públicas, como ser:

— Banco Central de la República Argentina (4).

— Nómina de Personas Expuestas Políticamente (5).

— Base de Lavado de Dinero (6).



(1) Fuente: https://fundacionio.com/algo-de-historia-cuanto-tiempo-llevo-desarrollar-estas-12-vacunas/.

(2) Fecha de sanción del DNU "Aislamiento Social Preventivo y Obligatorio", publicado en el BORA el 20 de marzo de 2020.

(3) "OSINT son las siglas de Open Source Intelligence (Inteligencia de Fuentes Abiertas). Se define como el conocimiento y explotación de fuentes abiertas de información para generar inteligencia. Se trata de un conjunto de técnicas y herramientas utilizadas para recopilar información pública, correlacionar los datos y procesarlos. Es decir, aplicarle análisis e inteligencia a la gran cantidad de información públicamente accesible en Internet con el objetivo de extraer conclusiones útiles para una investigación, un monitoreo, una campaña de marketing, etc.". Fuente: https://www.defensa.com/cyberseguridad.

(4) http://www.bcra.gov.ar/.

(5) https://mapadelestado.jefatura.gob.ar/ y https://datos.gob.ar/.

(6) https://offshoreleaks.icij.org/ y https://www.un.org/.