Manuel Mendiola
Director del área de Riesgos Tecnológicos
PKF Attest

Supervisión y auditoría continua... ¿Es el momento?

Las herramientas de supervisión y auditoría continua suponen un cambio radical en la forma de prevenir y detectar fraudes, actividades irregulares u otros posibles riesgos. Un uso apropiado de estas tecnologías proporciona un grado de control muy superior al de los enfoques tradicionales. Se basan en evaluar -de forma recurrente y automática- una serie de indicadores y alertas relacionados con un conjunto de operativas y riesgos específicos que preocupan a la compañía.

Estos indicadores pueden encontrar desviaciones respecto a una situación de "normalidad" casi en el momento en que estas se producen, obteniéndose un determinado volumen de ocurrencias que han de analizarse después para confirmar si realmente son producto de una situación irregular o no deseada. Además, un buen uso de estos sistemas incrementa la sensación de "vigilancia" dentro de la organización, haciendo que los empleados sean mucho más cuidadosos.

Algunas posibles aplicaciones de un enfoque de supervisión y auditoría continua son por ejemplo, el fraude: Predicción de la probabilidad de fraude en la operativa de clientes según el análisis de sus variables económicas, sociales, laborales y las operaciones que realiza. Morosidad: Detección de patrones de incremento de la morosidad antes de que esta se produzca. Delitos informáticos: Prevención y detección de patrones anómalos. Tecnología: Evaluación automática del diseño y eficacia operativa de los controles automáticos. Gobierno del dato: Análisis global de la calidad de la información utilizada por la compañía. Pago a proveedores: Identificación de pagos duplicados, así como errores en el registro de facturas. Servicios Cloud: Seguimiento de la disponibilidad y calidad del servicio.

Además de control interno: Supervisión del funcionamiento de los controles implantados. Blanqueo de capitales: Identificación de posibles casos y tendencias geográficas. RGPD / LOPDGDD: Validación de determinadas medidas técnicas, políticas y controles automáticos establecidos para garantizar un nivel de seguridad adecuado en función de las evaluaciones de impacto (EIPDs). Compliance penal: Supervisión de los registros asociados a los controles que com-

ponen el sistema de Compliance Penal para comprobar que se cumplimentan correctamente y que los controles operan con normalidad.

Realmente, cualquier aspecto del que sea necesario o recomendable una evaluación recurrente, podría abordarse con este enfoque. Sin embargo, aunque en ámbitos como la ciberseguridad el uso de herramientas de supervisión continua o monitorización está muy extendido, (*Sistemas de Prevención de Intrusos -IPS-, Sistemas de Detección de Intrusos -IDS-, etc.*), en otras áreas su presencia es muy escasa o se reduce a analíticas e indicadores aislados que ha desarrollado un departamento por su cuenta.

¿Y cuál es la causa? ¿Por qué no hay una mayor presencia de este tipo de soluciones? La respuesta se podría resumir en lo complejo que resulta ponerlos en marcha. Recuerdo un cliente que argumentaba que un enfoque de supervisión continua es algo muy sencillo de desplegar: "*…estableces que aspecto quieres evaluar, desarrollas la consulta correspondiente a tus bases de datos y la parametrizas para que se repita automáticamente cada cierto tiempo*". Fácil, ¿verdad? Me temo que no...

Las pistas para evitar impactos económicos por actividades irregulares se encuentran en nuestros sistemas de información

Imaginemos que un departamento desarrolla un conjunto de indicadores que se ejecutan periódicamente de forma automática. ¿Y luego que? ¿Cómo hace para no verse desbordados por el volumen de ocurrencias? ¿para priorizarlas? ¿para que no le aparezcan todos los días los mismos resultados? ¿para llevar el seguimiento y registro del análisis realizado a cada una? ¿para modificar o actualizar los parámetros de los indicadores? ¿para obtener una clasificación de las unidades más problemáticas según el volumen de ocurrencias de cada una -y su importancia-?, etc.

Por tanto, aunque un modelo de supervisión y auditoría continua puede reducirse a un conjunto de consultas automáticas recurrentes, un buen modelo supone mucho más. Se ha de enfocar como un sistema de información o plataforma independiente desde el que se gestionen los diferentes indicadores y se agrupen, distribuyan y analicen las ocurrencias.

Es conveniente que esta plataforma disponga de una serie de módulos que permitan la administración y parametrización de los indicadores, la consulta de resultados, la asignación de estos a diferentes auditores, comunicación con las unidades evaluadas, etc.

En cuanto a la implantación de estas soluciones, es un proceso arduo y complejo que requiere -normalmente- la involucración de la alta dirección, la colaboración de otras áreas como Tecnología y un enfoque adecuado a medio/largo plazo para evitar que se conviertan en herramientas limitadas y difícilmente adaptables a la evolución continua del negocio.

Tampoco debemos olvidar aspectos como la disponibilidad de información suficiente para evaluar los indicadores, el grado de integridad y exactitud de dicha información, los costes de mantenimiento o la necesidad de medir la rentabilidad del sistema.

Sin embargo, aun con todos estos condicionantes, se puede afirmar que -actualmente- es necesario potenciar el uso de estos modelos, al no ser razonable ni conveniente seguir evaluando volúmenes ingentes de información mediante herramientas ofimáticas, muestras o consultas puntuales.

Las pistas para evitar impactos económicos por fraude o actividades irregulares se encuentran dentro de nuestros sistemas de información. Solo hay que ser capaces de analizar los datos de forma continua y adecuada.