ENTREVISTA

Fernando Pons Ortega
Auditor informático y socio de Deloitte

"No se puede hacer una auditoría sin analizar los sistemas de información"

Fernando Pons Ortega, socio de Deloitte, informático y responsable de auditoría de sistemas de la firma, ofreció una conferencia sobre "La auditoría de sistemas como apoyo al auditor financiero" en el marco del I Foro Tecnológico de los Órganos de Control Externo, celebrado en Valencia el pasado mes de septiembre. AUDITORÍA PÚBLICA aprovechó la ocasión para hablar con él.

Auditoría Pública. Comencemos acotando los conceptos. Cuando hablamos de auditoría de sistemas, ¿a qué nos estamos refiriendo?

Lo más importante cuando eres parte complementaria de un trabajo, y la auditoría informática lo es respecto a la auditoría financiera, es definir el alcance, es decir, qué resultado se espera de esa auditoría financiera para integrar tu trabajo dentro de los objetivos de dicha auditoría. Esto es una parte de la auditoría informática, limitada a cumplir determinadas pruebas utilizando tu capacidad técnica. Pero la auditoría informática va más allá, desde conocer el grado de control del entorno informático hasta ver cómo se adaptan las organizaciones al cumplimiento de la normativa en aspectos como, por ejemplo, la ley de protección de datos. En Deloitte definimos la Auditoría informática como la aportación de valor al control interno respecto a la tecnología y su entorno (más allá del hardware y del software), desde los procesos de negocio hasta el buen gobierno del área de Sistemas de Información, o su alineamiento con la estrategia corporativa.

A.P. ¿Hasta qué punto considera a la auditoría de sistemas como una exigencia a la hora de pronunciarse sobre el control interno de una determinada organización?

A mí me resulta difícil entender la auditoría sin un análisis de los sistemas de información. La auditoría tradicional alrededor del ordenador, entendido como una caja negra que te da la información sobre la que vas a trabajar, ya no

nos sirve porque nos perdemos parte de lo que exige el control interno: de dónde surge la información, cómo se ha manejado, cómo se calculan los datos, quién accede a la información y la manipula… Estaríamos perdiendo una parte muy importante de la fiabilidad de la información sobre la que nos pronunciamos. En la actualidad, salvo casos en los que la complejidad tecnológica sea mínima o inexistente, me parece impropio dar opinión del control interno de una organización sin conocer sus sistemas de información. Los propios auditores financieros hace quince años se dieron cuenta de que había que cambiar la forma de auditar. Y esto se está haciendo de forma paulatina en un proceso que yo considero imparable, alineado con el obligado "escepticismo saludable" que debe tener todo profesional de la auditoría.

A.P. ¿Y quién debe ser el responsable de ese análisis que usted considera necesario? ¿Debería dejarse en manos de expertos informáticos o podrían hacerlo los auditores?

Pienso que el auditor, consciente de que necesita unas competencias adicionales, puede acudir a la colaboración de auditores informáticos o desarrollar esas habilidades él mismo. Estamos hablando de realizar unos análisis, unas pruebas que antes no se hacían y que ahora son imprescindibles porque el entorno sobre el que se pronuncian ha cambiado. De hecho, la mitad de los profesionales que hacen auditoría informática no son informáticos. Por tanto, es factible que un auditor, con cierta colaboración, desarrolle esa habilidad lo mismo que ha desarrollado otras como consecuencia de normas nuevas, porque se les obliga a hacer determinadas pruebas, etc. En definitiva, se trata de que el auditor se vaya dotando de capas adicionales de conocimiento técnico, teniendo en cuenta que en esto hay mucho de lógica y poco de tecnología. Y siempre podrá acudir a profesionales de la Auditoría informática.

A.P. El futuro, por tanto, parece llevarnos a una auditoría que integrará ese análisis de sistemas.

Sí, al final acabaremos hablando de auditoría, no de auditoría informática, y los análisis y pruebas relacionadas con el componente tecnológico serán una parte más de la auditoría, como lo puede ser una circularización o la entrevista con un responsable de la organización. Utilizando términos informáticos para definir la auditoría, hemos de pasar de la auditoría "analógica" a la "digital".

A.P. Partiendo de la premisa de que la auditoría de sistemas mejora la calidad del producto, hablemos de costes.

Este tipo de auditoría, tanto en el control interno como externo, exige un coste inicial importante porque hay que definir muy bien los programas y pruebas que se van a realizar, aunque la curva va disminuyendo y, a largo plazo, la reducción de costes es evidente. En el mismo tiempo puedes hacer más pruebas, aumentar el campo de prueba (la muestra) y reducir tiempos que se pueden utilizar para incrementar el número de pruebas. Esto es importante porque estamos hablando de un tipo de auditoría que las organizaciones se plantean a medio y largo plazo. La ventaja es que se va creando una base de auditoría permanente, con pruebas que las repites en cualquier momento a costes cada vez menores. Sin olvidar que el esfuerzo es el mismo

"En definitiva, se trata de que el auditor se vaya dotando de capas adicionales de conocimiento técnico"

ejecutando esa prueba sobre una muestra que sobre la totalidad, lo que implica hablar del universo, del 100%, no de muestreos sobre cuya fiabilidad cuando se aplican a conclusiones de auditoría tampoco es fácil ponerse de acuerdo. En mi opinión, no es un tema de coste, sino decidir si queremos auditar de forma profesional y rigurosa o no.

"La manera de minimizar el impacto del auditor es una buena planificación, tener claro el objetivo de cada trabajo y establecer sinergias"

A.P. La Ley Orgánica de Protección de Datos obliga a auditar cada dos años los sistemas de información que contengan datos de carácter personal. ¿Esta auditoría está al margen de lo que debe ser una auditoría informática integral?

Metodológicamente es lo mismo, la diferencia es que existe un reglamento de medidas de seguridad que se debe cumplir, por lo que el programa de trabajo te viene dado por la propia ley. Por lo tanto, estamos hablando de auditoría informática con un alcance determinado: las medidas de seguridad que exige la ley. Considero que auditar conforme a la LOPD no puede considerarse una auditoría informática integral porque tiene un campo de acción limitado: los ficheros con datos personales y sus entornos, que han de cumplir unas determinadas condiciones, por lo que hay áreas y aspectos que quedan fuera del alcance.

A.P. ¿Cómo se pueden coordinar los diferentes tipos de auditoría (financiera, operativa, informática…) para reducir costes y, al mismo tiempo, entorpecer menos el día a día de las organizaciones auditadas?

Creo que la clave es encontrar sinergias entre los diferentes tipos de auditoría. Nosotros como auditores de cuentas, por ejemplo, analizamos la situación de nuestro cliente desde el punto de vista de la protección de datos pensando en que puede haber una sanción, es decir, una contingencia. Lo mismo se puede hacer respecto a otro tipo de auditoría. Cuando hacemos una auditoría financiera puedes estar mirando un proceso de negocio o el entorno informático. La manera de minimizar el impacto del auditor es una buena planificación, tener claro el objetivo de cada trabajo y establecer sinergias.

A.P. Por último, ¿qué mensaje mandaría a los órganos de control externo respecto a la auditoría informática?

Que no se puede entender la auditoría externa –y tampoco la interna– sin tener en cuenta la tecnología, es decir, sin analizar los sistemas que soportan la información. Obviar ese análisis es hacer una auditoría incompleta.