Fernando Pons Ortega
Auditor Informático y Socio de Deloitte

Auditoría Informática, una aproximación a la mejora del Control Interno

INTRODUCCIÓN

Los escándalos contables de principios de la década han provocado un aumento en la sensibilización, tanto de los reguladores como de las organizaciones (públicas y privadas) por el control interno. La existencias de nueva normativa al respecto (como por ejemplo la Sarbannes-Oaxley), las buenas prácticas de gobiernos corporativo, las necesidades de transparencia en la gestión como un activo más de las organizaciones, o la búsqueda de la eficiencia en los procesos internos han actuado durante los últimos años como catalizadores para la mejora de los mecanismos de control interno en las organizaciones.

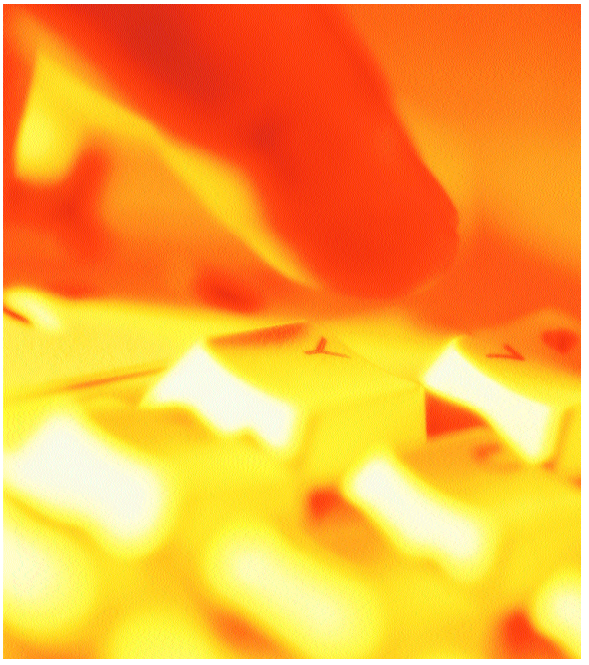
Entramos así, en una fase de madurez de las organizaciones, en las que la mejora de la eficiencia y el control de sus actividades comienzan a ser una de las necesidades básicas.

Dentro de las diferentes actividades que componen la estrategia de control interno de las organizaciones, el control sobre la gestión de los sistemas de información día a día adquiere una mayor relevancia. Para ello podemos encontrar, de manera inmediata, algunas razones:

- La creciente dependencia de las organizaciones y sus procesos (tanto internos como externos) respecto a sus sistemas de información.
- Derivado de lo anterior, el aumento de la complejidad de los mismos, con entornos heterogéneos y abiertos, a la vez que integrados.
- El éxito de las estrategias de externalización de la gestión de los sistemas de información, con los que la dependencia de los sistemas de información se refuerza con la dependencia de uno o varios proveedores de servicio.

Prueba de la mayor importancia que el control sobre la gestión de los sistemas de información gana día a día, son el hecho de que, por ejemplo, la normativa europea de autorización de organismos pagadores, define, como uno de sus cuatro grandes criterios de autorización, el del fomento del uso de los sistemas de información como soporte a todos sus procesos y el del establecimiento de un Sistema Integrado de Gestión de la Seguridad (SGSI), que no es más que el reflejo del aumento del nivel de control sobre los Sistemas de Información.

En este escenario, el papel de la auditoría informática se muestra como una nueva herramienta para la mejora del control interno en las organizaciones.



AUDITORÍA INFORMÁTICA COMO ELEMENTO DE CONTROL INTERNO

En el momento en el que las organizaciones adquieren conciencia sobre la necesidad de aumentar el nivel de control sobre la gestión de sus sistemas de información, surge la siguiente pregunta natural: ¿pero qué es realmente la auditoría informática y cómo puede ayudarme?

Es natural esta duda desde la perspectiva de que, tradicionalmente, los departamentos de control interno o auditoría interna, están compuestos por perfiles muy cercanos al negocio, principalmente financiero y, en algunos casos, operativo.

A continuación intentaremos desgranar algunos de los ámbitos en los que la función de la auditoría informática puede ayudar a la mejora de los sistemas de control interno de las organizaciones, a través de la propia evolución que la labor del auditor informático ha ido experimentando desde sus inicios.

En sus inicios, el auditor informático surge como un apoyo a los tradicionales equipos de auditoría. Su labor de apoyo consistía básicamente en la obtención de información financiera de los sistemas de información en los que residía y tratarla, con herramientas específicas de tratamiento masivo de datos, para facilitar la labor de los equipos de auditoría financiera. Entre las grandes ventajas que el apoyo del auditor informático ofrecía era el da la validación del total de la información disponible, en lugar de los habituales procedimientos de muestreo. Dicha labor continúa siendo hoy día una de las principales tareas del auditor informático. Así, es fácil encontrar auditores informáticos tratando información para validar información contable compleja de obtener como pueden ser, por ejemplo, en el ámbito financiero, la validación del cálculo de la periodificación de intereses, o en ámbitos productivos el de la amortización de inmovilizados o la valoración de existencias.

En paralelo, el hecho de que, cada vez más, la información contable de las organizaciones fuese tratada automáticamente y casi por completo en sistemas informáticos, condujo a una nueva preocupación. ¿Son íntegros los datos de que dispone el equipo de auditoría? Con esa preocupación, poco a poco, en esa labor de apoyo al auditor financiero, el auditor informático pasa, de meramente tratar los datos contables, a cuestionarse la fiabilidad de los mismos. Comienza entonces a plantearse nuevos objetivos de control, como son el control de acceso sobre la información, la gestión de autorizaciones, y los mecanismos de registro de actividad sobre dicha información.

En el momento en el que el auditor informático comienza a plantearse objetivos de control sobre quién debe acceder a qué información, qué puede hacer con ella, o a cuestionarse la integridad de la misma, comienza a necesitar y a obtener un conocimiento profundo sobre los procesos de negocio de la compañía. Por otra parte, la integración de dichos procesos en aplicaciones informáticas, provoca que gran parte de los controles que se aplican sobre los mismos se definan en dichas aplicaciones. A partir de este instante, la labor del auditor informático comienza a confluir con la del auditor financiero, adquiriendo una doble versión de especialista en la

definición de procesos de control interno en los procesos de negocio y en su aplicación o análisis sobre los sistemas de información que los soportan.

Finalmente, en paralelo a la función de apoyo de la auditoría financiera, comenzaron a plantearse nuevas funciones relacionadas con la auditoría informática. Entre los principales impulsores de esas nuevas funciones, podemos encontrar:

- Los reguladores, que empezaron a generar normativa específica aplicable sobre los sistemas de información de las organizaciones y sus procesos de gestión. Los ejemplos más conocidos son la Ley Orgánica de Protección de Datos (LOPD en adelante en este documento), desarrollada por el Reglamento de Medidas de Seguridad recogido en el Real Decreto 994/1999, o la Ley de Servicios de la Sociedad de la Información.
- Los sistemas de comercio electrónico, tanto entre organizaciones (B2B), como orientada a clientes finales (B2C), que han impulsado la mejora de los procesos de comercialización de productos pero a la vez han abierto la puerta a nuevos riesgos derivados de la necesidad de "abrir" los sistemas de información de las organizaciones a terceros.
- El aumento de la complejidad de los sistemas de información y la dependencia de las organizaciones respecto a los mismos, que en ocasiones se muestran opacos para la dirección de las organizaciones y para sus usuarios.

Con ellos, se generó una sensibilización hacia la seguridad de los sistemas de información, entendiendo la misma desde los tres puntos de vista tradicionales:

- Confidencialidad.
- Disponibilidad.
- Integridad.

Y con ella, los auditores informáticos comenzaron a analizar los riesgos asociados al uso de los sistemas de información y los controles destinados a garantizar sus tres pilares básicos. Así, se platean nuevas funciones como la de análisis de vulnerabilidades de los sistemas y aplicaciones, evaluación de planes de continuidad de negocio, y, en general, el análisis de los procesos de gestión de los sistemas de información.

En definitiva, el papel actual del auditor informático dentro de las organizaciones lo podemos resumir en dos grandes tareas principales:

- Apoyo del auditor interno, en la definición y aplicación de controles sobre los procesos de negocio de las organizaciones, en tanto que gran parte de los mismos se aplican desde sus sistemas de información.
- Auditoría de la gestión de los sistemas de información, que se plantea básicamente dos objetivos:

  - Que los sistemas de información soportan adecuada y eficientemente los procesos de negocio de las organizaciones.

  - Que la información tratada por los sistemas de información dispone de un nivel de seguridad adecuado a su valor y a los riesgos asociados a su uso.

OPCIONES DE IMPLANTACIÓN

Una vez que las organizaciones adquieren conciencia de la necesidad de disponer de una función de auditoría informática y de qué objetivos persigue con ella, surge la siguiente cuestión; ¿cómo lo llevo a la práctica de mi organización? No nos debe generar gran preocupación el encontrarnos con esta cuestión sin tener muy clara la respuesta. A día de hoy, no es atrevido decir que el 80% de las organizaciones en España se encuentran todavía en este punto, y que sólo un 20% (principalmente entidades financieras y aseguradoras), lo tienen resuelto.

A la hora de formalizar la función de auditoría informática dentro de una organización, existen varias alternativas y, a su vez, diferentes puntos a considerar:

- La complejidad de los sistemas de información de nuestra organización y la dependencia de nuestros procesos internos respecto a los mismos (no sólo en términos de disponibilidad, sino también de confidencialidad e integridad).

- El nivel de especialización necesario para llevar a cabo dicha función.

La complejidad de nuestros sistemas de información nos puede dar una medida del volumen de trabajo potencial que podría realizar la función de auditoría informática en nuestra organización. Para muchas organizaciones, la complejidad de sus entornos todavía puede no ser tal como para requerir una dedicación "full-time" de personal para el desarrollo de la función de auditoría informática.

Por otra parte, de acuerdo a las funciones típicas del auditor informático, descritas en el punto anterior, el perfil del auditor informático es un perfil muy específico. Si desgranamos un poco los principales "skills" del auditor informático, nos encontramos:

- Buen conocimiento de los procesos de negocio.
- Buenos conocimientos contables.
- Conocimientos informáticos desde varios puntos de vista:
  - Programación.
  - Administrador de sistemas.
  - Administrador de Bases de datos.
  - Herramientas de auditoría informática.
  - Soluciones de seguridad.
- Nociones de manejo normativo.

En ocasiones, las tendencias naturales a la hora de cubrir las necesidades de auditoría informática son básicamente dos:

- Reaprovechar a algún auditor interno con conocimientos avanzados de informática.
- Incluir un informático dentro del equipo de auditoría interna.

En ambos casos, desde nuestra experiencia podemos contar algunas excepciones dentro de un nutrido número de decepciones, tanto para la organización como para el empleado que se ve responsable de una función a la que no sabe muy bien cómo dotar de contenido.

Desde los dos puntos de vista antes mencionados, una opción razonable, al menos en el arranque de la función de auditoria informática, es la de contar con el soporte de expertos en la materia.

Así, como decíamos anteriormente, podemos encontrar diferentes aproximaciones a la hora de formalizar la función de auditoría informática dentro de las organizaciones:

- Externalizar totalmente la función, mediante acuerdo marcos, en los que, de manera mixta, la organización y expertos en la materia definen los objetivos de control y son los expertos los que desarrollan los trabajos de auditoría.
- Arrancar de manera inicial la función de auditoría informática, dotando a la organización de personal dedicado a ello, con el apoyo de expertos que asesoren a la hora de dotar de contenido a la función y formar al personal interno en el desarrollo de las habilidades necesarias.
- Dotar a la organización de recursos específicos dedicados en exclusiva a la función de auditoría informática.

Cualquiera de las anteriores será válida en función del análisis que cada organización haga de sus necesidades en este sentido. Así, podemos encontrar entidades financieras que han optado con éxito por externalizar totalmente su función de auditoría informática, contando siempre con expertos en cada materia concreta, mediante acuerdos marcos, mientras que otras han optado por dotar de personal interno dicha función y acometerlo totalmente de manera interna.

CONCLUSIÓN

A medida que las organizaciones adquieren mayor tamaño, y una mayor sensibilidad por el control interno, en la búsqueda de la eficiencia en sus procesos, la necesidad de formalizar la función de auditoría informática se hace más patente.

A la hora de formalizar dicha función, las organizaciones deben tener muy presentes los objetivos que se plantean con ella, sus necesidades en cuanto a recursos y las diferentes estrategias que se pueden adoptar para ello, sin olvidar la posibilidad de externalizar total o parcialmente la función.