Índice

Introducción y objetivos

En primer lugar, queremos transmitir nuestro agradecimiento a todas las organizaciones que han cumplimentado los cuestionarios que han servido de base para elaborar este informe. Sin su participación no hubiera sido posible la realización de este **Primer Estudio sobre la Función de Auditoría Interna de Sistemas de Información en España**.

Este estudio es una iniciativa llevada a cabo por la firma de servicios profesionales **KPMG**, la Asociación de Auditores de Sistemas, **ASIA** (Capítulo de Madrid de **ISACA**), el Instituto de Auditores Internos de España, **IAI** y representantes de algunas de las principales empresas españolas: **MAPFRE, Seat, Liberty Seguros, BBVA y Endesa**.

El objetivo del estudio es conocer el papel y la actividad que desempeña la auditoría interna de sistemas de información en las empresas que desarrollan su actividad en España.

En los últimos años hemos asistido, tanto en España como en los países de nuestro entorno, a una gran proliferación de leyes y recomendaciones que subrayan la importancia del buen gobierno y que hacen un especial hincapié en la necesidad de crear / rediseñar la función de auditoría interna en general, así como la auditoría de sistemas de información en particular, y de establecer procesos formales de gestión de riesgos.

Creemos, y las respuestas recibidas confirman, que la auditoría interna de sistemas debe estar integrada en un plan director global de auditoría interna, estratégico. Otro aspecto clave y destacado en este estudio, es la importancia de una adecuada selección de recursos, que permitirá obtener eficiencias de los trabajos de auditoría interna en las organizaciones.

Una función de auditoría interna de sistemas **integrada**, con los recursos apropiados, permitirá automatizar las pruebas de forma que se cubran mayores riesgos, se asegure el cumplimiento de controles y se reduzcan los costes, a través de la centralización y racionalización de recursos y tiempos.

De las conclusiones de este primer estudio podemos afirmar que la implantación de la función de auditoría interna de sistemas está en sus inicios en las empresas españolas, principalmente en grandes empresas, existiendo por delante un largo camino por recorrer. Un camino marcado y ya iniciado por las grandes empresas.

Creemos que este **Primer Estudio de la Función de Auditoría Interna de Sistemas de Información** aportará un mayor conocimiento de cómo las empresas españolas aúnan en sus procesos de revisión el asesoramiento de expertos, las metodologías y formas de trabajo de auditoría de sistemas de información.

Por otro lado, nos gustaría adelantarles que esta iniciativa, pionera en España, ha sido adoptada por KPMG a nivel internacional, lo que, estamos seguros, contribuirá a enriquecer el conocimiento y la comparativa de la profesión en nuestro país con otras entidades y organizaciones de todos los continentes.

Finalmente, confiamos en tener la oportunidad de poder compartir diferentes comparativas, tanto sectoriales como de estructura y metodología, adaptadas a su caso concreto. Y, por supuesto, esperamos poder contar de nuevo con su colaboración en la edición de 2007 de este estudio.

Metodología del estudio

El estudio se ha realizado mediante un cuestionario dirigido a **332 empresas** de todos los sectores, en las que, por su tamaño, sector o tipo de organización, entendemos que pueden contar con la función de auditoría interna. Los cuestionarios fueron enviados durante el mes de septiembre de 2005 de forma individualizada, por parte de IAI y de KPMG. Igualmente, se facilitó una dirección en Internet para cumplimentar la encuesta de forma interactiva.

En total, se recibieron **80 respuestas**, lo que supone casi el **24%** de los cuestionarios enviados. El alto grado de respuesta conseguido, muy por encima del 10% ó 15% que suele ser habitual en este tipo de estudios, pone de manifiesto la buena acogida de esta investigación y el interés que la iniciativa ha despertado entre el colectivo empresarial.

El 84% de los cuestionarios han sido cumplimentados por los **responsables de los departamentos de auditoría interna** de las organizaciones encuestadas, mientras en un 5% de los casos, ha sido respondido por los responsables/directores de finanzas.

El cuestionario utilizado para este estudio se estructuró en once secciones:

Sección A. Perfil de la organización e información general

Sección B. Organización de la auditoría de sistemas de información

Sección C. Funciones de la auditoría de sistemas de información

Sección D. Tipología de trabajos y metodología

Sección E. Planificación de los trabajos

Sección F. Comunicación y seguimiento de los resultados de los trabajos

Sección G. Valoración y control de calidad

Sección H. Utilización de herramientas

Sección I: Habilidades de los profesionales

Sección J: Formación y evaluación

Sección K: Desarrollo profesional

Resumen ejecutivo

El Primer Estudio sobre la Función de Auditoría Interna de Sistemas de Información en España, llevado a cabo por la firma de servicios profesionales **KPMG**, la Asociación de Auditores de Sistemas, **ASIA** (Capítulo de Madrid de **ISACA**), el Instituto de Auditores Internos de España, **IAI** y representantes de algunas de las principales empresas españolas: **MAPFRE, Seat, Liberty Seguros, BBVA y Endesa**, analiza las principales características de la función de auditoría de sistemas de información y cómo están avanzando las empresas españolas en su implantación y desarrollo.

El estudio se ha realizado mediante un cuestionario dirigido a **332 empresas** de todos los sectores, en las que, por su tamaño, sector o tipo de organización, entendemos que pueden contar con la función de auditoría interna. En total, se recibieron **80 respuestas**, lo que supone casi el **24%** de los cuestionarios enviados.

- **Siete de cada diez** empresas consultadas consideran importante la función de auditoría de sistemas de información.

  Casi la mitad de las empresas participantes de banca y seguros, cuentan con esta función, (43%).

- El 33% de las empresas que han respondido confirman contar con una función de auditoría de sistemas de información. Aún así, más de la mitad de los encuestados, un 67%, reconocen **no contar con la función de auditoría de sistemas de información**.

- Por otro lado, en un 18% de las empresas, los departamentos de auditoría interna están realizando esfuerzos considerables en la **mejora del funcionamiento de los departamentos**, aplicando en sus prácticas habituales, metodologías de auditoría tecnológicamente avanzadas, utilizando: metodologías estándar (CobiT), herramientas de interrogación de ficheros y análisis de riesgo, entre otras.

- Dentro de la organización de auditoría interna de las empresas encuestadas, la función está cubierta por recursos internos (50%) con conocimientos de sistemas de información (78%), orientados fundamentalmente a la ejecución de trabajos relativos a la verificación de la eficacia y eficiencia de los controles internos informáticos (82%), auditorías de seguridad (86%) y de cumplimiento normativo (80%).

- La dedicación global de esta función en las empresas consultadas se sitúa entorno al 10% del total de las horas del plan de auditoría, en el 61% de las respuestas, mientras que, en un 27%, llega hasta el 20% de las horas.

- Con el objetivo de poder planificar adecuadamente los trabajos de auditoría de sistemas de información, en **siete de cada diez empresas** que han respondido a la encuesta, 74%, **se realizan análisis de riesgos previos**, siendo informado formalmente tanto el Comité de Auditoría (31%) como el responsable de sistemas (75%) y de la unidad afectada por la auditoría (73%).

- El 66% de las empresas consultadas coincide en destacar la importancia de exigir conocimientos específicos a los auditores internos de sistemas de información, señalando la certificación internacional, CISA, como la más relevante para el desempeño de la profesión (82%).

- Resulta sorprendente que la titulación académica de los profesionales que integran los departamentos de auditoría de sistemas de información es, en prácticamente, la misma proporción, técnica, ingenieros informáticos, y economistas.

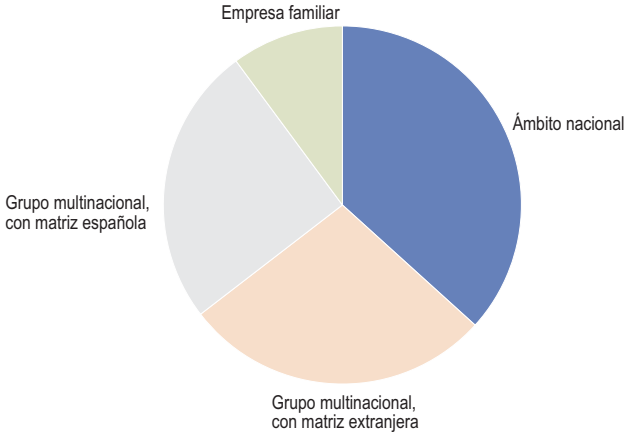
- En la mitad de las empresas consultadas, 51%, los recursos especializados y dedicados a la auditoría de sistemas de información desarrollan sus carreras profesionales dentro del departamento de sistemas de información. La rotación de estos profesionales es baja, en el 63% de los casos.

Perfil de la organización e información general

El perfil de las 80 empresas que contestaron al cuestionario, en función del sector al que pertenecen, se resume en la siguiente tabla:

Sector	% Participantes
Banca y servicios financieros	33%
Industria	13 %
Consumo y distribución	15 %
Seguros	10 %
Energía	8%
Telecomunicaciones	5 %
Ocio	1 %
Administración pública	1 %
Otros sectores	14 %
Total	100%

Por otro lado, al ámbito de actuación de las empresas que han cumplimentado el cuestionario se resume en el siguiente gráfico:



49 de las empresas consultadas son **nacionales**, de las que **20** son empresas **españolas multinacionales con matriz en España**.
Mientras, **22 empresas multinacionales con matriz extranjera** han cumplimentado el cuestionario y **nueve empresas familiares** han aportado sus comentarios sobre la situación actual de la función de auditoría de sistemas de información.

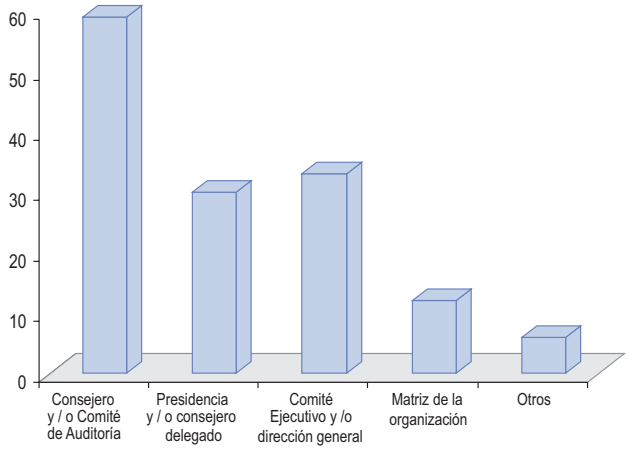
Entre otros datos cuantitativos relevantes para la muestra del estudio, desglosamos en la siguiente tabla promedio de auditores internos de los departamentos de auditoría interna de las empresas, destacamos los siguientes:

Tamaño medio del volumen de facturación de las empresas

	Nº empresas	% empresas
Hasta 500 millones euros	17	21%
Entre 501 y 2.500 millones euros	28	35%
Más de 2.500 millones euros	35	44%

Organización de la auditoría de sistemas de información

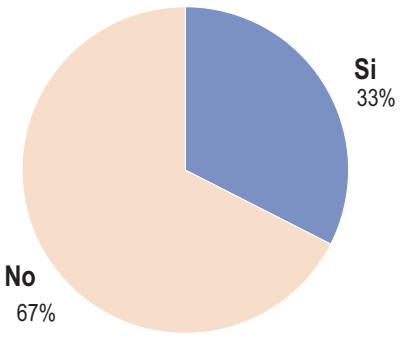
¿A quién reporta el departamento de auditoría interna?



En un **42%** de las empresas consultadas, los departamentos de auditoría interna **reportan al Consejo y / o Comité de Auditoría**, mientras que el porcentaje de empresas en las que se reporta a presidencia y / o al consejero delegado, o al Comité Ejecutivo y / o dirección general desciende hasta el 22% y el 24%, respectivamente

Existencia del área de auditoría interna en las organizaciones

Con respecto a la existencia de un área de auditoría de sistemas de información dentro de las organizaciones encuestadas, observamos que únicamente un 33% cuenta con un departamento específico para esta función.

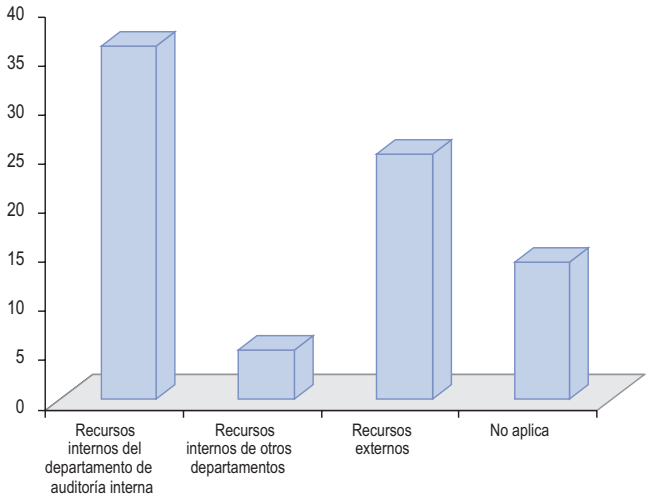


Una de las principales conclusiones que se desprenden de este estudio es la identificación de la **generalizada carencia de la función de auditoría de sistemas de información** en las empresas españolas.

Los informes enviados desde el área de auditoría de sistemas están dirigidos en su mayor parte al responsable de auditoría interna en un 64%, mientras que al Consejo y / o Comité de Auditoría pasa a ser de un 33%.

Cobertura de necesidades de recursos especializados para la auditoría de sistemas de información

En el siguiente gráfico se recoge la distribución de la cobertura de las necesidades de recursos en auditoría de sistemas de información:



La función de auditoría de sistemas de información queda cubierta principalmente por **recursos internos del departamento de auditoría interna** en el **45%** de las empresas consultadas. Mientras, un 31% opta por la opción de contratar recursos ajenos y externos a la organización.

Independientemente de lo anterior, estos recursos son gestionados y dirigidos por el equipo de auditoría interna en un 49% de los casos.

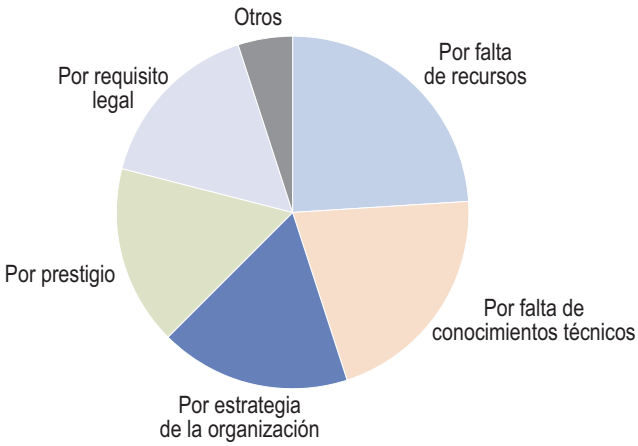
El equipo dedicado a dar **soporte a auditoría interna** en el área de sistemas de información está formado principalmente por **auditores externos**, en un **29%**, y por auditores internos con experiencia en sistemas de información, en un 30%. En el 16 % de los casos, está integrado por profesionales de auditoría interna de la organización a nivel internacional.

Por otro lado, en los casos de **subcontratación del servicio**, las horas repercutidas al área de sistemas de información con respecto al total de horas de auditoría interna, suelen representar:

- **Hasta el 10% de las horas: 61%**
- **Entre 11% y 20% de las horas: 27%**
- **Entre 21% y 40% de las horas: 9.7%**
- **Más del 40% de las horas: 2.44%**

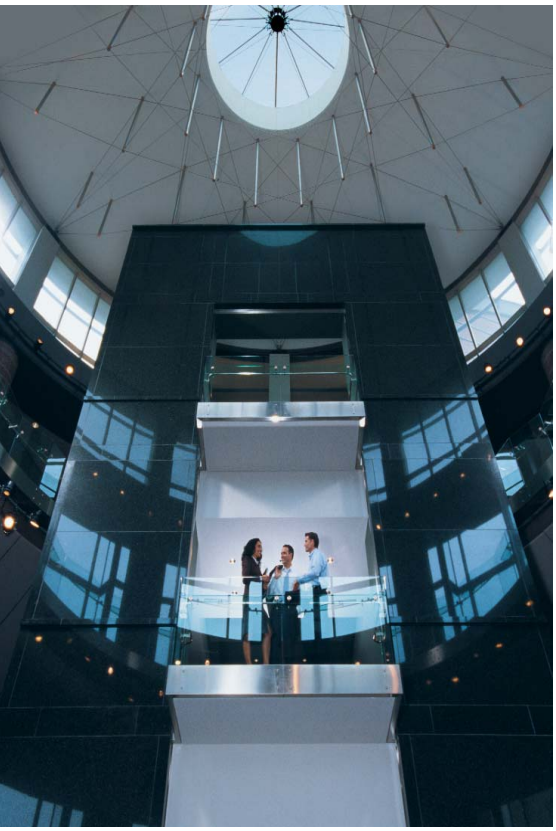
Necesidad de contratar especialistas externos

Algunas de las principales razones para la contratación externa de especialistas en auditoria de sistemas de información, se recoge en términos porcentuales en el siguiente gráfico:



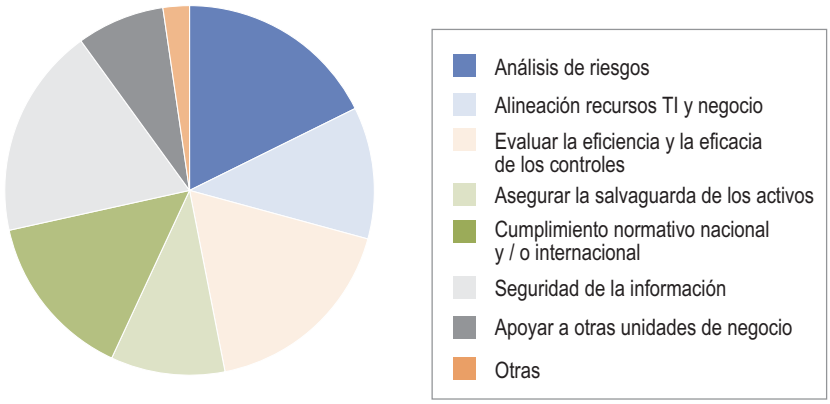
Podemos observar que uno de los factores más importantes que se destacan en este estudio es la **carencia de recursos y de especialización** de los mismos. Esto se traduce, a nuestro juicio, en una **oportunidad de desarrollo profesional para los especialistas** en este área, a medio y largo plazo.

Funciones de la auditoría de sistemas de información



Principales funciones del auditor de sistemas de Información

Las funciones a desempeñar en auditoría de sistemas de información están definidas en casi la mitad de las organizaciones participantes en este estudio, un 49%.

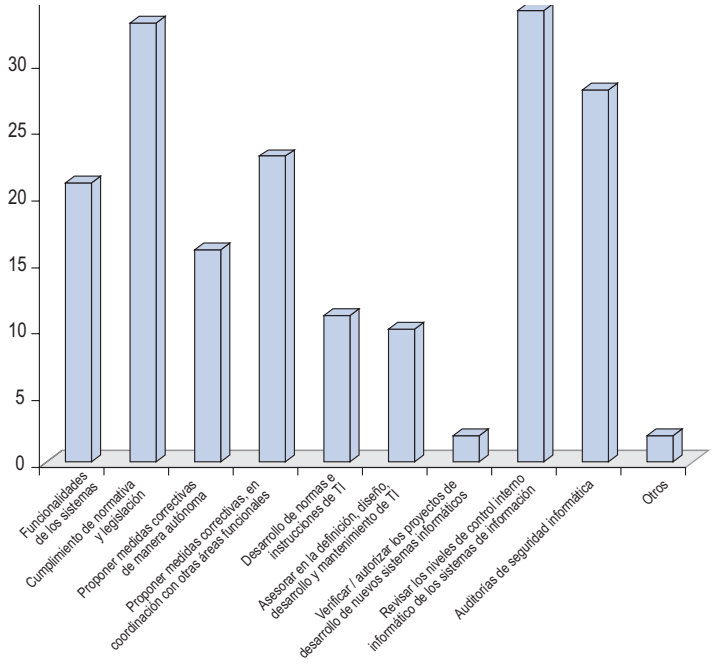


	Nº de operaciones
Si	29
No	30

Así las funciones más habituales son las de **seguridad de la información**, en un **19%** de los casos, seguidas de **evaluación de eficiencia y eficacia de controles** y **análisis de riesgos**, ambas con un **18%**, y cumplimiento normativo nacional y / o internacional, 68%.

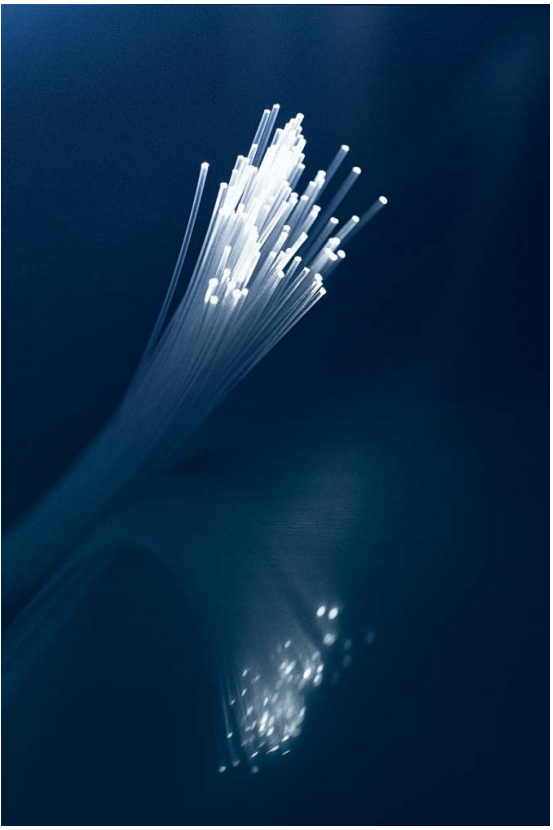
Objetivos de las revisiones

Los objetivos básicos definidos para la función de auditoría de sistemas de Información son principalmente:



Destacan, sobre todos los objetivos comentados, las **revisiones de los modelos de control interno informático**, en ocasiones en marcos de aplicaciones informáticas integradas complejas, la **revisión de la seguridad informática** y verificar el **cumplimiento de la normativa vigente**, tanto nacional como internacional.

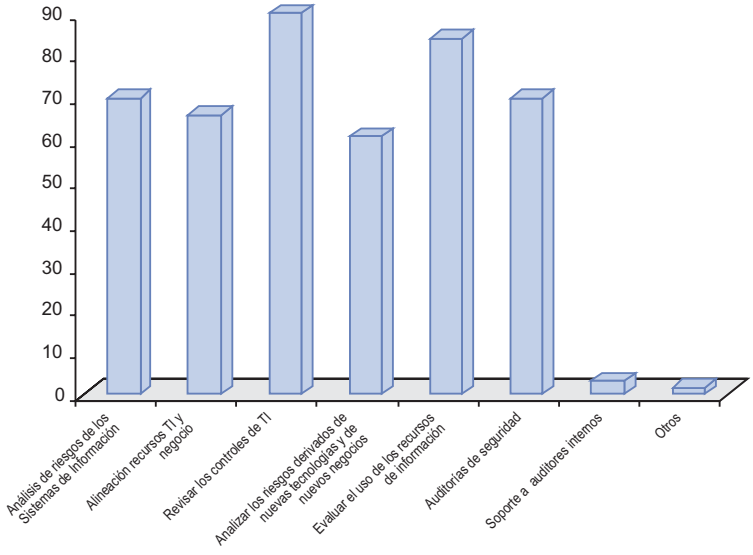
Tipología de trabajos y metodología



En esta sección se ha solicitado información sobre la tipología de trabajos encomendados a los especialistas y auditores de sistemas de información así como la metodología utilizada en la ejecución de sus trabajos:

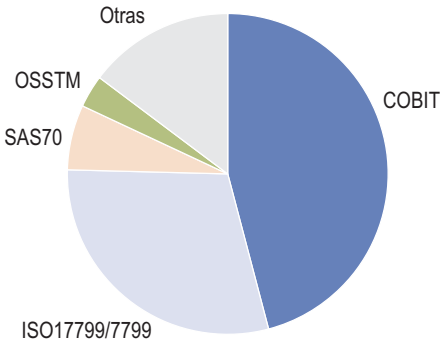
Tipología de trabajos de los auditores

Resulta llamativa la diversidad de los trabajos realizados por los auditores de sistemas de información, a tenor de las respuestas obtenidas.



Destaca el hecho de que el trabajo menos realizado es la prestación de soporte a otras áreas de auditoría, sólo en un 5% de los casos.

Para la realización de estos trabajos, según se extrae del estudio, la mayoría de las organizaciones suele utilizar alguna metodología o marco de referencia estándar para determinar la revisión de actividades relacionadas con los sistemas de información (64%).



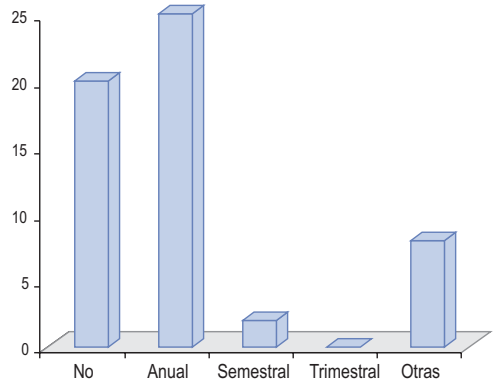
De los resultados del estudio se desprende que, para la realización de estos trabajos, el **46%** de las empresas que han respondido al cuestionario, **utilizan la metodología COBIT**, si bien, **ISO17799/7799** con un **29**% está siendo cada vez mejor valorada, teniendo en cuenta su relativamente reciente implantación. En algunos casos, y especialmente para em**presas españolas cotizadas en Estados Unidos, SAS-70** empieza a ser el marco de referencia.

Planificación de los trabajos

Los encuestados fueros preguntados por aspectos relativos a la planificación, entreo otros: integración en la planificación de auditoría interna, aspectos clave para la planificación, análisis de riesgos y comunicación de la ejecución de los trabajos.

Fase de planificación de los trabajos

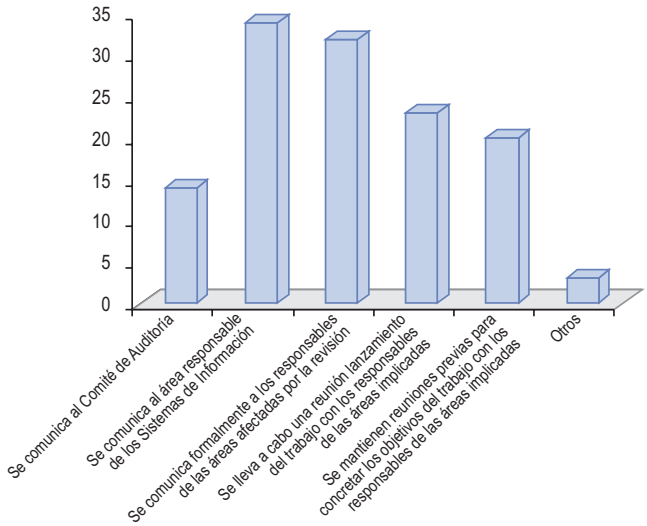
Una amplia mayoría de los encuestados, el **63%**, ha respondido positivamente en relación a la **planificación efectiva de los trabajos de auditoria de sistemas de información**.



En el 43% de las empresas consultadas, la planificación de los trabajos de auditoría interna de sistemas es realizada, en la mayoría de casos, con un horizonte temporal anual; solo es realizada de forma semestral en un 3% de los casos.

Formalización de la planificación

Más de la mitad de los encuestados, 56%, señala que realmente existe una comunicación formal de la planificación de los trabajos, que se dirige a:



Para definir el alcance de cada auditoría, en la mayoría de los casos, se realiza y formaliza una evaluación de riesgos. Este análisis se comunica a las áreas responsables de los sistemas de información en un 27% de los casos y a las áreas afectadas por la revisión, en un 25%. Estas comunicaciones se producen, en la mitad de las empresas, con una antelación de entre una y dos semanas.

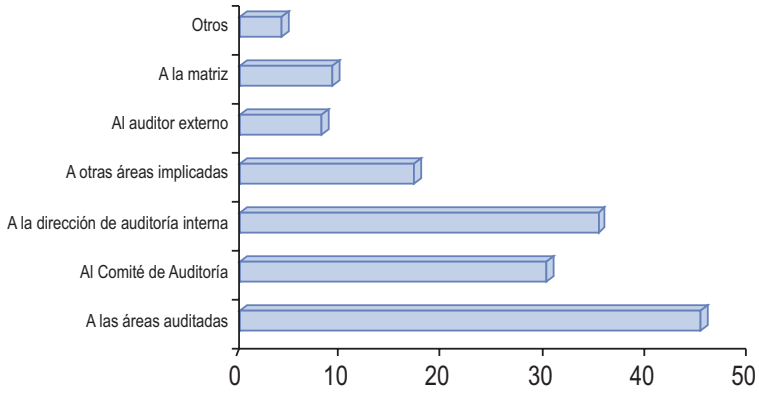
Comunicación y seguimiento de los resultados de los trabajos

La totalidad de las respuestas han coincidido en señalar la **necesidad de formalizar un procedimiento de comunicación** de los trabajos de auditoría de sistemas de información.

De las respuestas recibidas, el 60% de las empresas indican que los resultados se recogen en un informe detallado con conclusiones y recomendaciones, y el 12% incluyen un resumen ejecutivo. Los objetivos y alcance de los trabajos realizados junto a las conclusiones y recomendaciones son los contenidos más comunes en las comunicaciones a las diferentes áreas de la organización.

Receptores de los trabajos realizados

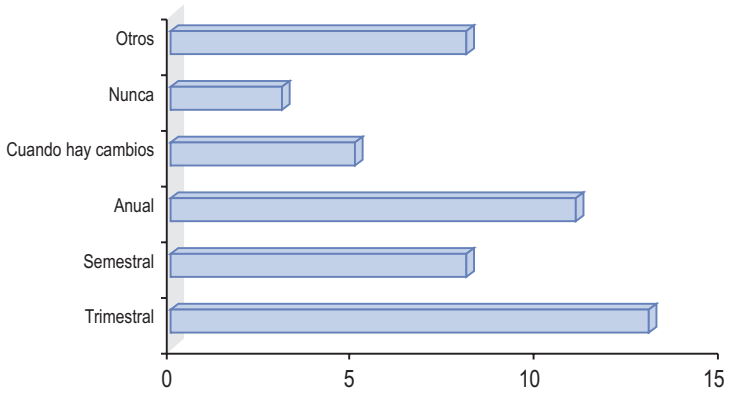
Los receptores de estas comunicaciones formales son principalmente las áreas auditadas, el **Comité de Auditoría** y la **dirección de auditoría interna**, como se desprende del siguiente gráfico



Cabe destacar, que el Comité de Auditoría y la dirección de auditoría interna son **informados periódicamente** sobre el estado de las recomendaciones, en el 65% de los casos.

Seguimiento de las recomendaciones

El seguimiento de las recomendaciones, incluidas en los resultados de las auditorías, se realiza mayoritariamente por el departamento de auditoría interna con diferentes periodicidades:

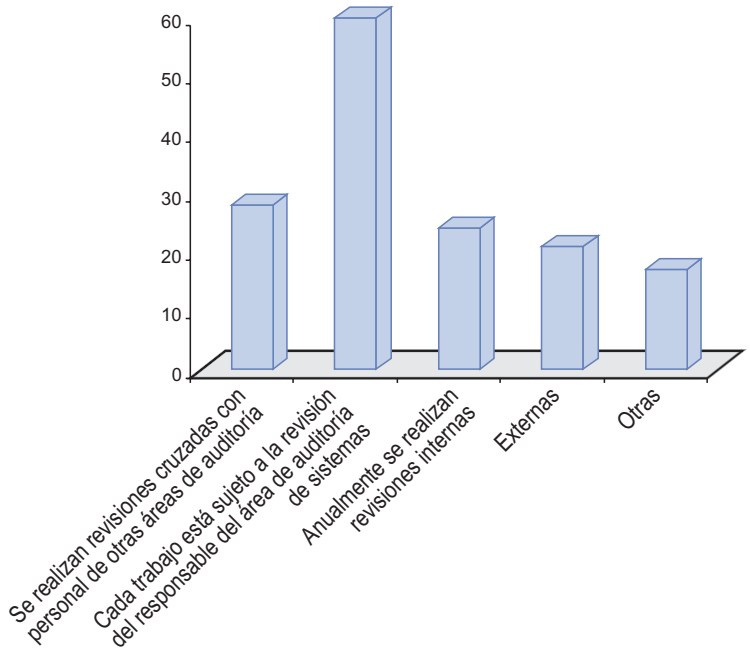


Valoración y control de calidad

En esta sección se ha solicitado confirmación sobre la existencia de pruebas de calidad de los trabajos y la forma en la que se realizan, entre otros.

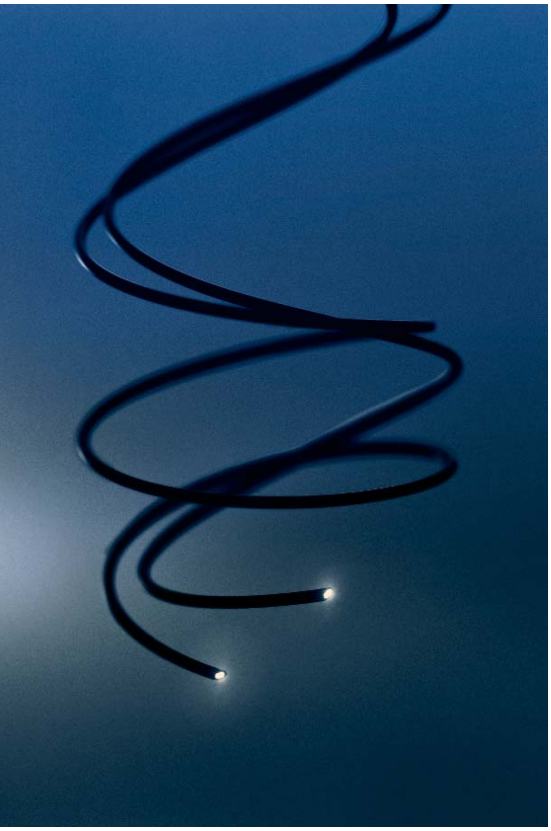
Resulta sorprendente que, del 70% de las empresas que responden a esta pregunta, más de la mitad, un **53%, reconoce no efectuar ningún tipo de revisión de calidad**. Mientras el resto, un 47%, realizan el siguiente tipo de revisiones:

Tipologías de revisiones de calidad



Cabe destacar que una vez finalizado el trabajo de auditoría, la valoración de la opinión de las áreas auditadas no es una práctica que esté extendida, ya que el 56% de encuestados no la realizan o la realizan de manera informal.

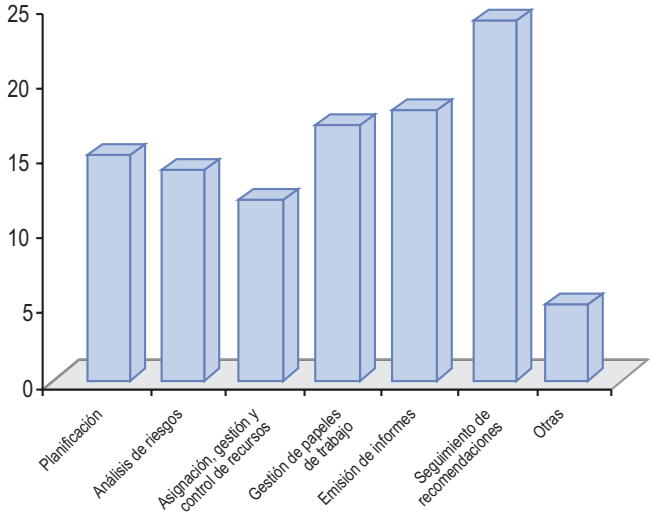
Utilización de herramientas



De las respuestas recibidas, se desprende que el uso de diversas herramientas informáticas está cada vez más extendido.

El siguiente cuadro resume el grado de utilización de los distintos tipos de herramientas automatizadas:

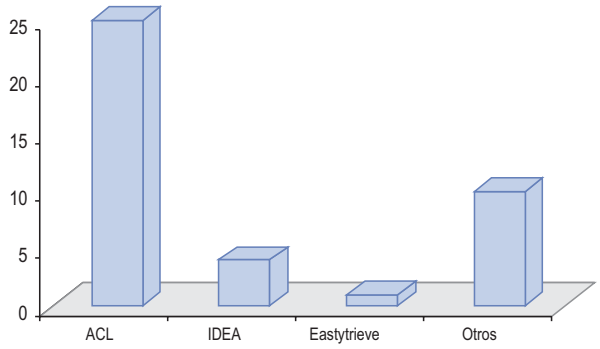
Uso de las herramientas automatizadas

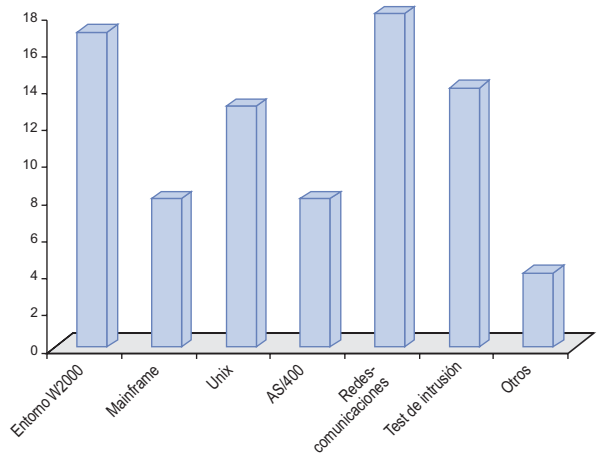


El **seguimiento de recomendaciones** es la fase en la que más herramientas automatizadas son utilizadas, según indica el **22%** de las empresas consultadas, seguidas por la gestión de papeles de trabajo, emisión de informes y análisis de riesgos.

Para la ejecución de pruebas de auditoría se recurre asimismo a la utilización de herramientas específicas, siendo estas principalmente, los tratamientos masivos de datos, con ACL como principal herramienta y, por otro lado, los análisis de seguridad lógica con redes y entorno W2000 como principales herramientas.

Ejecución de la auditoría versus herramientas



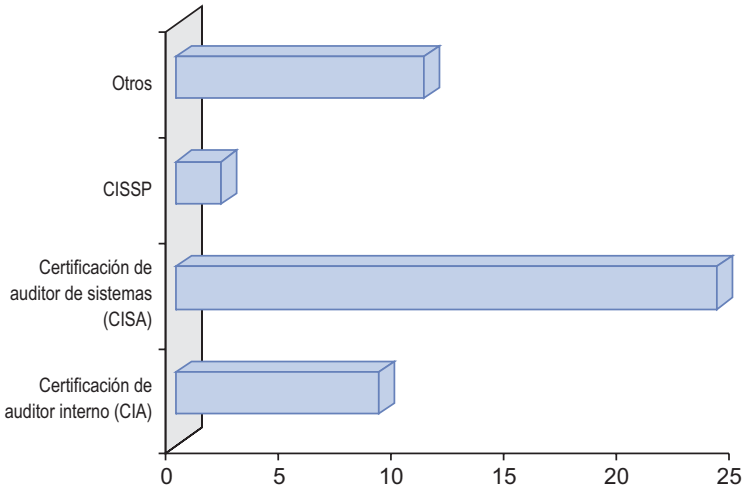


Habilidades de los profesionales

En **siete de cada diez empresas consultadas**, los profesionales que componen los departamentos de auditoría interna tienen un nivel de **titulación superior**, que, en algunos casos, están complementados con un master o titulación de postgrado. Resulta significativo que los perfiles más habituales en los departamentos de auditoría de sistemas de información, son, en prácticamente igual proporción, **ingenieros informáticos, 34%,** y **economistas, 33%.**

Podemos observar en el siguiente gráfico que en muchos casos se exige otro tipo de conocimiento o titulación específica, siendo la más habitual la certificación de auditor de sistemas, CISA.

Titulaciones especializadas

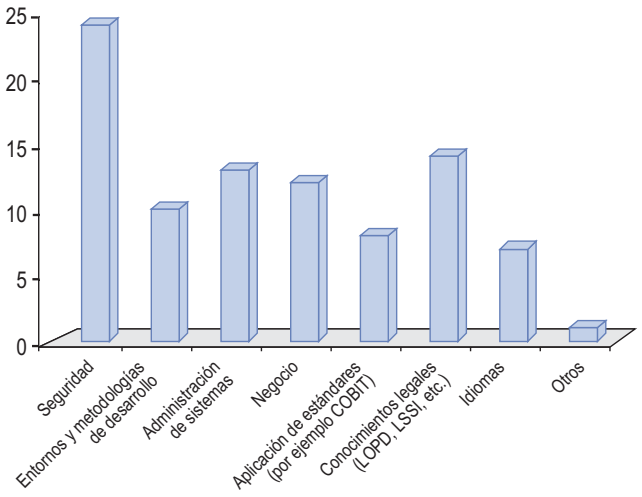


Es importante destacar que para la mayor parte de los encuestados, más del 52%, la titulación CISA es una de las mejor valoradas para complementar sus calificaciones profesionales.

Más de la mitad de las empresas que respondieron a nuestros cuestionarios, un **54%**, **incorporan nuevos profesionales** en el departamento de auditoría de sistemas de información, **procedentes de la propia organización**, mientras que en el 46% de los casos, selecciona nuevos **recursos externos a la organización**.

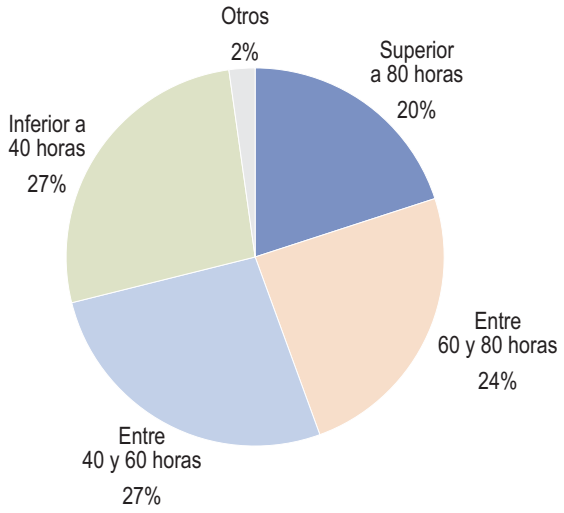
Para la incorporación externa, la fuente más utilizada es Internet (44%), tanto a través de la página Web propia como a través de terceros utilizando este canal.

Igualmente los conocimientos más demandados son: seguridad, seguidos de administración de sistemas y conocimientos relativos a la LOPD, como se recoge en el siguiente grafico:



Formación y evaluación

Los datos obtenidos con respecto a la formación de los auditores por año no resultan muy positivos, teniendo en cuenta que más de un **57% de las organizaciones no superan las 60 horas/año**. Sólo dos de cada diez empresas que han respondido el cuestionario dedica más de 80 horas/año.



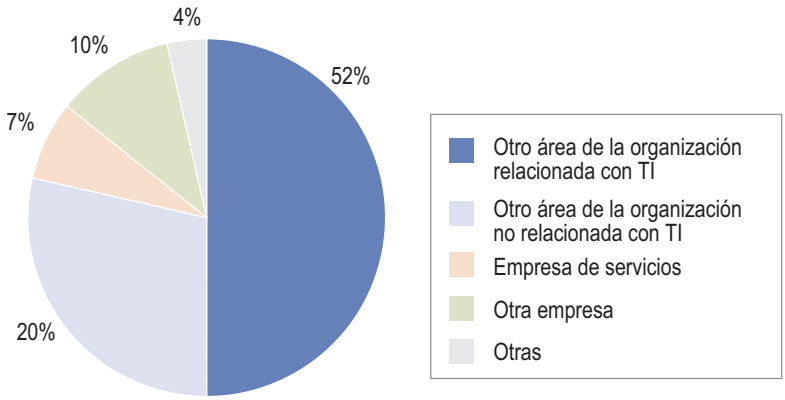
La formación recibida por los auditores se centra principalmente en **especialización informática en un 27%,** y en la obtención de **certificaciones internacionales** (CIA, CISA, CISM, CISSP) **en un 23%**.

Por otro lado, las evaluaciones de personal son anuales, en la práctica totalidad de las empresas, 70%.

Desarrollo profesional

En un 37% de las empresas consultadas, los **auditores de sistemas de información no tienen un plan de carrera establecido por la compañía**, y en aquellos casos en que cuentan con uno, se incluye dentro del plan de carrera del área de auditoría. De este modo, la promoción de categoría se decide, principalmente, por criterios de conocimientos adquiridos.

La gran mayoría de las organizaciones, un **65%**, consideran que la **rotación del departamento de auditoría de sistemas de información es baja**.
En caso de abandonar la función, la salida de los profesionales se dirige principalmente a áreas de la organización relacionadas con sistemas de información.



Contactos

Ramón Poch
rpoch@kpmg.es

Pablo Montoliu
pmontoliu@kpmg.es

Francisco Gibert
fgibert@kpmg.es