SINDICATURA DE COMPTES
DE LA
COMUNITAT VALENCIANA

La auditoría de sistemas de información integrada en la auditoría financiera. La perspectiva del sector público

Antonio Minguillón Roy

VIII premi
d'investigació
Mestre Racional

La auditoría de sistemas de información integrada en la auditoría financiera. La perspectiva del sector público

Antonio Minguillón Roy

SINDICATURA DE COMPTES
DE LA
COMUNITAT VALENCIANA

Edita: Sindicatura de Comptes de la Comunitat Valenciana

1ª edición: junio, 2010

ÍNDICE

Índice de anexos

Presentación

El acto de entrega del VIII Premio de investigación Mestre Racional, al que estas notas sirven de presentación, se ha celebrado conjuntamente con el XXV aniversario de la creación de la Sindicatura de Comptes de la Comunitat Valenciana.

Esta coincidencia nos permite reflexionar, aunque sea someramente, sobre la evolución del sector público valenciano en este periodo reciente de nuestra historia y la correlativa del control externo, representado por la Sindicatura de Comptes.

Si tuviéramos que señalar algunas de las principales características descriptivas de dicha evolución, sin duda deberíamos destacar dos: en primer lugar el extraordinario crecimiento del sector autonómico, que partiendo prácticamente de cero y como consecuencia de las transferencias de competencias del Estado, alcanza actualmente un presupuesto anual consolidado superior a los 16.000 millones de euros y consta de más de un centenar de entidades; en segundo lugar, el incremento de servicios que se ofrecen al ciudadano, tanto en el sector autonómico como en el sector local, que ha ido acompañado de una evolución tecnológica sin precedentes de las herramientas informáticas y las telecomunicaciones que dan soporte a la gestión de dichos servicios y que ha desembocado en la denominada administración electrónica.

La primera de las tendencias señaladas ha provocado que la Sindicatura, a lo largo de sus veinticinco años de existencia, haya incrementado sus efectivos personales y materiales y perfeccionado sus técnicas de auditoría para mantener su capacidad fiscalizadora en unos niveles razonables de eficacia y eficiencia, adaptándose a los cambios y evolución continua del sector público de nuestra comunidad.

La segunda de las tendencias ha introducido, especialmente en los últimos diez años con la consolidación del concepto de administración electrónica, una serie de cambios cualitativos (no sólo en la Comunitat Valenciana, puesto que la evolución ha sido universal) que afectan de forma sustancial a la forma en que se pueden llevar a buen término las auditorías públicas y que ha provocado el crecimiento exponencial de lo que en la terminología auditora se denomina el componente tecnológico del riesgo de auditoría.

Para hacer frente a este reto y abordar con profesionalidad el nuevo entorno de trabajo, los auditores públicos deben introducir

profundos cambios en sus métodos de trabajo de forma que se pueda hacer frente y conseguir reducir dichos riesgos tecnológicos. En este sentido la Sindicatura de Comptes de la Comunitat Valenciana ha planteado en sus dos planes trienales, e implementado posteriormente, medidas tendentes a adaptar su organización al nuevo entorno de la administración electrónica.

Pero aunque puedo afirmar con satisfacción que la Sindicatura está dando pasos firmes en esa dirección y pronto estará en condiciones de homologarse con cualquier organización puntera en esta materia a nivel europeo, el proceso no está resultando sencillo, debido tanto a la complejidad intrínseca de los factores tecnológicos que sustentan la administración electrónica, como a la dificultad de cambiar y adaptar una organización (sus personas y sus métodos de trabajo) nacida y con una muy asentada trayectoria de trabajo en el tradicional mundo administrativo «analógico», basado en el documento físico.

Ante las dificultades existentes para comprender el cambio que es necesario realizar hacia el nuevo entorno fiscalizador de la administración electrónica, resulta de gran utilidad la lectura del trabajo *La auditoría de sistemas de información integrada en la auditoría financiera. La perspectiva del sector público*, que, entre otras, responde a dos preguntas esenciales relacionadas con el reto que acabo de mencionar.

Este trabajo tiene la virtud de facilitar, a los no iniciados, la comprensión del *porqué* es necesario integrar las auditorías de sistemas de información entre las técnicas utilizadas por los auditores públicos. De porqué, en las fiscalizaciones de entidades que operan en entornos informatizados complejos (que son la mayoría de los entes públicos hoy en día) es necesario introducir en el conjunto de procedimientos y herramientas que utilizan nuestros auditores las relacionadas con la auditoría informática, ya que con los métodos tradicionales resulta muy difícil, y en algunos casos imposible, reducir el riesgo de auditoría a unos niveles aceptables.

Además del porqué, facilita la comprensión del *cómo*. De cómo puede introducirse y encajarse sin disonancias el trabajo de un auditor informático en los procedimientos de una auditoría o fiscalización tradicional. Es precisamente este factor (trabajar integrados) un aspecto fundamental para que el trabajo de fiscalización en su conjunto, el de los auditores «tradicionales» y los auditores informáticos, alcance su máxima eficacia y eficiencia; aspecto este último que siempre ha sido una de las principales preocupaciones en la Sindicatura de Comptes.

En este sentido me ha parecido un acierto el enfoque general del trabajo, al tratar la auditoría informática, no como una materia autónoma, sino como una materia que alcanza su máxima utilidad sólo en la medida en que está debidamente integrada en una auditoría financiera y de legalidad.

En el trabajo, además de plantearse, de una forma general, cómo deben integrarse las auditorías informáticas en las fiscalizaciones, también se desciende a un nivel de detalle tal que da pistas suficientes para que puedan darse pasos, desde muy modestos a muy audaces, en dicha integración.

Son interesantes las pinceladas de información que se dan sobre los distintos tipos y componentes de los actuales sistemas informáticos integrados o ERP, que facilitan su comprensión por los no especialistas a la hora de abordar su revisión de forma adecuada.

No cabe duda de que el estudio, además de ser útil para que los auditores «tradicionales» puedan comprender cómo se debe integrar el trabajo de auditoría informática en las fiscalizaciones, también resulta de especial interés para que los auditores informáticos comprendan cuáles son las necesidades de los auditores públicos y cómo deben enfocar su trabajo para que sea de la máxima utilidad de acuerdo con los objetivos de las auditorías financieras.

Debo destacar el esfuerzo de síntesis realizado sobre una materia en la que, a pesar de su importancia, existe un déficit de información y documentación indudable. No me estoy refiriendo a información técnica sobre auditoría informática pensada por y para informáticos, sino a metodología de auditoría informática o de sistemas de información pensada para los auditores financieros. En esta materia la carencia es casi total si pensamos en literatura en nuestro idioma. La completa bibliografía que acompaña al trabajo, la mayoría de procedencia anglosajona, también ayudará a aquellos interesados en profundizar en esta materia.

Para finalizar y en relación con el autor del trabajo premiado he de destacar, primero mi satisfacción porque un funcionario de la Sindicatura haya obtenido el Premio Mestre Racional y después su colaboración institucional y técnica en el desempeño de la Dirección del Gabinete Técnico de la Sindicatura con una especial dedicación a diversos aspectos relacionados con la utilización de las tecnologías de la información y la comunicaciones (TIC) en las tareas de fiscalización. En coherencia con los planteamientos basados en las TIC, el autor ha solicitado al Consell de la Sindicatura que el texto

del trabajo premiado no se edite en papel, sino tan solo en formato electrónico a través de nuestra sede electrónica.

Como es tradicional, he de terminar agradeciendo tanto a la Caja de Ahorros del Mediterráneo el patrocinio del premio como el rigor y dedicación del jurado que un año más y, puedo dar fe de ello, ha analizado con enorme profundidad y profesionalidad e independencia los trabajos presentados para llevar a cabo la concesión en los más estrictos términos de ecuanimidad y justicia, ante una muy alta cualificación y contenido científico de las candidaturas presentadas.

Valencia, 1 de junio de 2010
Rafael Vicente Queralt
Síndic major

Prólogo

La principal razón que motivó la elaboración de *La auditoría de sistemas de información integrada en la auditoría financiera. La perspectiva del sector público*, y que es su principal objetivo, fue analizar el impacto que la implantación plena de la administración electrónica (e-administración) va a tener en la forma de trabajar del auditor público.

En los capítulos 1 y 2 del trabajo, se hace una muy breve descripción de cuál es la situación que un auditor público se encuentra, con cada vez más frecuencia, al auditar un ente público, especialmente en aquellos de tamaño medio o grande. De cómo el entorno de trabajo (*los fiscalizados*) y los elementos materiales de nuestras pesquisas (*las evidencias o elementos probatorios de las auditorías*) se han ido transformando en los últimos años hacia una naturaleza digital cada vez más compleja, menos evidente y menos abordable con la metodología tradicional de auditoría.

En el periodo transcurrido desde la finalización y presentación del trabajo (20 de octubre de 2009) y el momento de escribir estas líneas, tan solo seis meses después, se han publicado las siguientes disposiciones que afectan a todo el sector público de la Comunitat Valenciana, que profundizan inexorablemente en el desarrollo de la administración electrónica y que van a impactar de forma muy relevante en la manera en que se deberán realizar las auditorías del sector público en el futuro inmediato:

- Ley 3/2010, de 5 de mayo, de la Generalitat de Administración Electrónica de la Comunitat Valenciana.
- Decreto 87/2010, de 21 de mayo, del Consell por el que se establecen las condiciones técnicas y normativas para el uso de la Plataforma de Facturación Electrónica de la Generalitat, Ge-factura.
- Real Decreto 3/2010, de 8 de enero, del Ministerio de la Presidencia, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Real Decreto 4/2010, de 8 de enero, del Ministerio de la Presidencia, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

– Real Decreto 1.671/2009, de 6 de noviembre, del Ministerio de la Presidencia, por el que se desarrolla parcialmente la Ley 11/2007, de acceso electrónico de los ciudadanos a los servicios públicos.

La aplicación de todo el conjunto de disposiciones amparadas en el concepto de administración electrónica y el desarrollo acelerado de las tecnologías de la información y las comunicaciones (TIC), supone que la fiscalización de los sistemas de información y de control interno, actualmente, presente una serie de características y de riesgos nuevos, que requieren un enfoque de auditoría, evaluación de riesgos y planificación de la auditoría con una perspectiva renovada, tal como se señala en los capítulos 3 y 4 del trabajo.

En el capítulo 4 se ha enfatizado en cuál ha sido la aproximación general a la materia del trabajo de investigación. Así, el estudio de las implicaciones que las TIC tienen sobre el trabajo del auditor público se ha realizado bajo la perspectiva de las necesidades de nuevos conocimientos y de los métodos especializados que se requieren para ejecutar las auditorías de regularidad basadas en el análisis de los riesgos.

El estudio de la metodología de auditoría de sistemas de información integrada en una auditoría financiera que se realiza en los capítulos 5 a 7, ha tenido como dificultad principal la ausencia casi total (con honrosas excepciones) de textos en castellano que aborden la cuestión, a pesar de la importancia que tiene tanto para el sector público como privado de la profesión auditora. En el capítulo 5 se analiza la metodología general y en el 7 se estudian las peculiaridades de los principales entornos TIC que pueden encontrarse en las administraciones públicas.

Finalmente en el capítulo 8 se hace un somero repaso de las técnicas y herramientas de auditoría asistida por ordenador, que son de ayuda indispensable tanto en la auditoría financiera como en la auditoría de sistemas de información.

La conclusión que debe extraerse del trabajo está implícita a lo largo del mismo, pero puede sintetizarse en unas pocas líneas: en un entorno digital propio de la e-administración, no es posible reducir los riesgos de auditoría a un nivel aceptable, si los auditores no utilizan de forma consistente técnicas y metodología adecuada de auditoría de sistemas de información; esto implica un importante esfuerzo de adaptación tanto a nivel personal de los auditores como a nivel organizativo de los órganos de control.

No quiero finalizar sin agradecer al Jurado la concesión del VIII Premio Mestre Racional y también al Patrocinador del mismo la Caja de Ahorros del Mediterráneo.

Por último, dedico este modesto trabajo a María Jesús, que durante meses ha soportado que le hurtara muchas horas y días de la vida familiar.

Valencia, 1 de junio de 2010
Antonio Minguillón Roy

1
Introducción

1.1. Los órganos de control externo y la auditoría informática

En los últimos años, desde los órganos de control externo autonómicos españoles (OCEX), se está dando una gran importancia al impacto que la utilización de las tecnologías de la información y las comunicaciones (TIC) tiene en los trabajos de fiscalización.

El pronunciamiento más importante al respecto proviene de los Presidentes de los OCEX, que el 19 de octubre de 2006 suscribieron la conocida como Declaración de Pamplona.[1]

La indudable y creciente importancia de la materia quedó explícitamente reconocida y reflejada en la citada Declaración de la siguiente forma:

> «…. las instituciones autonómicas de control deberán afrontar otros retos si quieren responder a las demandas de la sociedad y convertirse en puntas de lanza en la modernización de las administraciones. En este sentido, parece obligado realizar un mayor esfuerzo en la *fiscalización de los sistemas informáticos de las administraciones públicas*. Aún siendo conscientes de la complejidad del objetivo, cuya consecución exigiría la colaboración de expertos externos, la auditoría pública deberá pronunciarse sobre esos sistemas informáticos que actualmente son elemento fundamental en la gestión de las administraciones públicas.»

Los OCEX organizan, desde 2006, unos «Foros tecnológicos», en los que se pretende, según puede constatarse en la página de presentación[2] del primero celebrado en Valencia, hacer frente a los retos planteados por las tecnologías de la información y las comunicaciones:

> «Los auditores públicos en general, y los órganos de control externo de las comunidades autónomas (OCEX) en particular, se enfrentan desde hace años a una serie de importantes retos a los que hacer frente, siendo el desarrollo tecnológico y la evolución permanente y acelerada de los sistemas de información de gestión de la administración uno de los más importantes.

1. www.cfnavarra.es/camara.comptos/cas/DeclaracionPamplona.asp

2. www.sindicom.gva.es/web/wdweb.nsf/documento/ft. En esta misma página pueden encontrarse los enlaces a las páginas web dedicadas a los tres Foros tecnológicos celebrados hasta la fecha y puede accederse a las presentaciones realizadas.

El impacto que tienen los actuales sistemas informáticos en la forma en que se realiza y documenta toda la gestión pública, la paulatina transformación de la evidencia documental (el objeto material e inmediato de nuestras pesquisas) tal como la hemos conocido hasta ahora hacia una evidencia de carácter digital, afecta de forma radical a nuestros métodos de trabajo. Y debemos prepararnos para el nuevo escenario que ya tenemos aquí.

…

La puesta en común e intercambio de conocimientos de todas estas materias entre personal técnico de los OCEX ha de contribuir, no me cabe la menor duda de ello, a mejorar nuestra metodología fiscalizadora, a optimizar el uso de las distintas herramientas que las nuevas tecnologías ponen a nuestra disposición, y a mejorar en definitiva la eficiencia de nuestras entidades.

Valencia, 6 de julio de 2006

Rafael Vicente Queralt
Síndico Mayor»

El II Foro tecnológico se celebró en Pamplona en 2008 y el III Foro en Vitoria en mayo de 2009, con un creciente número de participantes, lo que muestra el interés tanto a nivel de los profesionales de los OCEX como a nivel institucional.

Pero no solo los OCEX de carácter autonómico están preocupados por el impacto de las tecnologías de la información y las comunicaciones en los trabajos de fiscalización. Las entidades fiscalizadoras superiores (EFS) europeas, incluido el Tribunal de Cuentas de España, organizadas en EUROSAI, y las de todo el mundo agrupadas en INTOSAI, también son conscientes de la necesidad de abordar la problemática que plantean las tecnologías de la información y las comunicaciones y han creado grupos de trabajo[3] especiales para desarrollar la metodología apropiada a las fiscalizaciones en entornos informatizados.

A nivel individual, los OCEX y las EFS, tienen un grado de evolución diferente en esta materia. En España, según consulta realizada en las páginas web de los OCEX, durante los últimos cinco años se han realizado o se están ultimando los siguientes informes relacionados con las tecnologías de la información y las comunicaciones:

Audiencia de Cuentas de Canarias

– Informe general sobre el grado de implantación de los objetivos de la Ley 11/2007, de 22 de junio, de Acceso Elec-

3. Pueden consultarse las páginas web de dichos grupos de trabajo en:
INTOSAI Working Group on IT Audit: www.intosaiitaudit.org
EUROSAI Information Technology Working Group: www.eurosai-it.org

trónico de los Ciudadanos a los Servicios Públicos (e-Administración).[4]

Cámara de Comptos de Navarra

– Informe de fiscalización sobre el contrato de suministro de un nuevo gestor informático de SOS Navarra (2006).

Cámara de Cuentas de Andalucía

– Fiscalización de la Oficina Virtual Tributaria y de Recaudación de la Consejería de Economía y Hacienda (2006).
– La presencia de la Administración de la Junta de Andalucía en la WEB (2005).

Sindicatura de Cuentas de la Comunidad Valenciana

– Fiscalización Cuentas anuales 2006 CIEGSA (Auditoría informática integrada en la auditoría financiera).
– Fiscalización Cuentas anuales 2006 VAERSA (Auditoría informática integrada en la auditoría financiera).
– Seguimiento de las recomendaciones de las dos auditorías anteriores en 2007.
– Auditoría de sistemas de información de la gestión de las subvenciones en IMPIVA en 2007.
– Auditoría de sistemas de información de la gestión de los ingresos en la Fundación Palau de les Arts en 2007.
– En el momento de finalizar este trabajo la Sindicatura no había emitido los informes del ejercicio 2008, pero de acuerdo con su Programa anual de actuación de 2009[5] la actividad relacionada con la auditoría de sistemas de información sería: en la fiscalización de la Cuenta de la administración de la Generalitat, de CACSA y de la Fundación Palau de les Arts.

4. A la fecha de elaboración de este trabajo, el informe todavía no se había publicado en la página web de la Audiencia de Cuentas de Canarias. Según señalaba en el artículo «Iniciativas para la gobernanza. Hacia un nuevo modelo de control de las finanzas públicas» publicado en *Auditoría Pública*, n.º 47 abril 2009, el Presidente de la Audiencia de Cuentas de Canarias, Rafael Medina Jáber, el Programa de Actuaciones del órgano de control externo canario para el ejercicio 2008, aprobado por el Pleno de la Audiencia de Cuentas en diciembre de 2007, incluyó dicha fiscalización, que se encontraba en un avanzado estado de ejecución al publicarse el artículo.

5. Programa anual de actuación de 2009: www.sindicom.gva.es/web/wdweb.nsf/documento/programaanual

Tribunal de Cuentas

– Informe de Fiscalización sobre la contratación celebrada para el desarrollo, implantación y mantenimiento, en el ámbito de la Seguridad Social, de la Administración electrónica como nueva modalidad de prestación de servicios y de relación con los ciudadanos tanto a través de Internet como de otras plataformas de comunicaciones (27 de octubre de 2005).

A la vista de los informes emitidos, la Sindicatura de Cuentas de la Comunidad Valenciana, posiblemente se encuentra entre los OCEX que más han avanzado en el desarrollo de metodología de auditoría de sistemas de información; en su vigente plan estratégico[6] contempla un objetivo detallado específico, que incluye una adaptación organizativa para el desarrollo de las auditorías de sistemas de información:

> «**3.15 Desarrollar la auditoría de sistemas de información**
> En los últimos años se ha producido una tendencia imparablemente creciente en la informatización de las administraciones públicas, en particular de la Generalitat y de sus distintas empresas y organismos.
>
> El volumen de transacciones que tienen lugar actualmente en el conjunto de la Generalitat puede cifrarse en varios millones. Se han implantado, o están en curso de implantación, los denominados ERP en las principales empresas y entidades, incluyendo la Administración general y la sanitaria. Estas aplicaciones informáticas están provocando que las pistas de auditoría (firmas, documentos contables, autorizaciones) en soporte tradicional en papel estén desapareciendo, siendo sustituidas por evidencias electrónicas. La Administración electrónica es un concepto y una realidad cada vez más extendida.
>
> La Sindicatura, en el ámbito del Plan Trienal precedente ha introducido, paulatina pero firmemente medidas tendentes a hacer frente eficazmente a las fiscalizaciones en este contexto, lo que técnicamente se denomina entornos informatizados. Se han efectuado acciones formativas especializadas, se ha contado con la colaboración de expertos externos en auditoría informática y se han realizado en 2007 dos trabajos «piloto» en esta área con resultado satisfactorio.
>
> La realización de revisiones/auditorías de los sistemas de información como parte de las fiscalizaciones, especialmente de aquellas entidades de mayor tamaño, constituye un aspecto absolutamente ineludible para emitir informes de calidad y con las máximas garantías técnicas.

6. PlanTrienal 2008-2010: www.sindicom.gva.es/web/wdweb.nsf/documento/plantrienal2008

El nuevo Plan Trienal considera ésta área como prioritaria por lo que **en 2008 se pondrá en marcha la Unidad de auditoría de sistemas de información**, que prestará asistencia a los distintos equipos de fiscalización. Estará integrado en el Gabinete Técnico de la Sindicatura y trabajará en estrecha coordinación con el Servicio de Informática de la Sindicatura».

1.2. La e-administración

1.2.1. Utilización de las TIC por la Administración

El motivo de esta creciente preocupación de los OCEX por el impacto de las tecnologías de la información y las comunicaciones en las fiscalizaciones que realizan, viene dado por el incremento del uso de las tecnologías de la información y las comunicaciones en la gestión pública.

El incremento en el uso de las tecnologías de la información y las comunicaciones por todas las Administraciones públicas es tanto cuantitativo como cualitativo.

Cuantitativamente puede medirse por las crecientes inversiones realizadas por las Administraciones públicas. Según el *Informe IRIA 2008* (páginas 27 y 102) la evolución de los gastos informáticos en la Administración del Estado y en las Administraciones locales ha sido la siguiente:

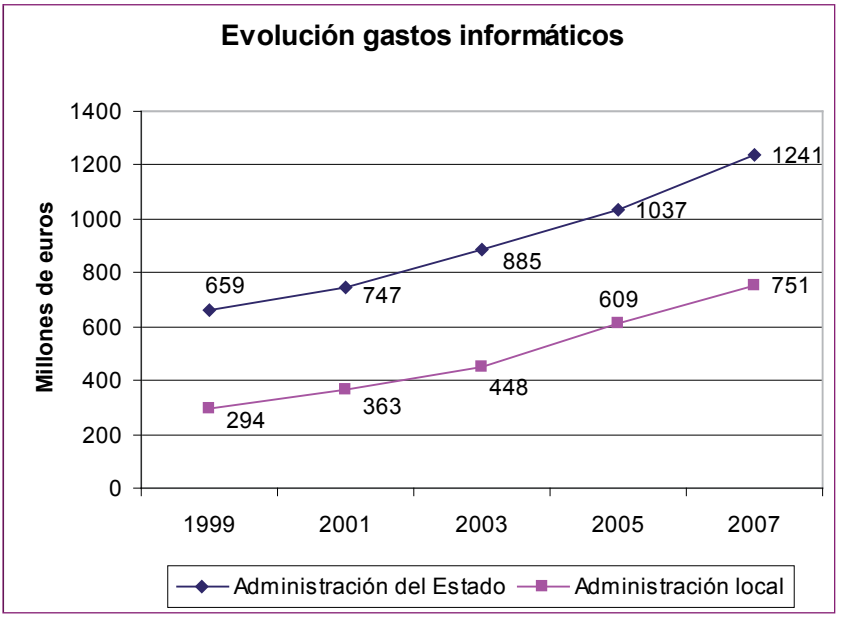


Figura 1.1

En los gastos informáticos se han incluido los conceptos relacionados de los capítulos 1 (gastos de personal), capítulo 2 (mantenimiento de hardware y software, alquileres y servicios), y del capítulo 6 (inversiones).

La proporción entre el gasto en TIC (gastos informáticos más los de comunicaciones) respecto del presupuesto total en España también ha sido creciente, según se refleja en el informe «*eEspaña 2009*» de la Fundación Orange:

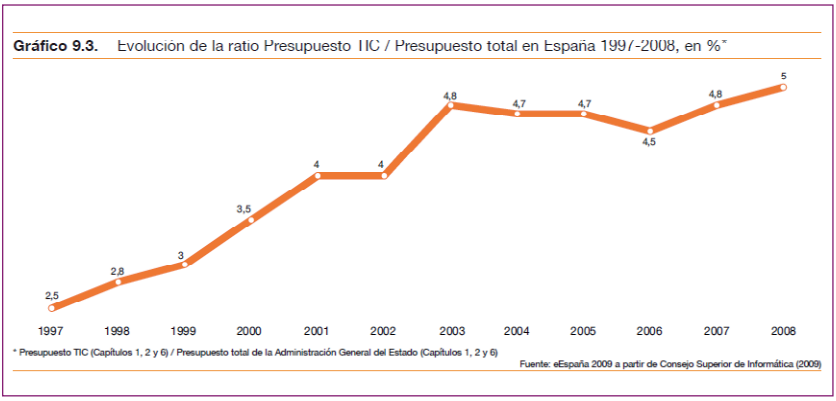


Figura 1.2

Además de este aumento de las inversiones y del gasto informático, en los últimos años también se ha producido un salto cualitativo en la utilización de las tecnologías de la información y las comunicaciones por parte de las Administraciones públicas, que ha ocasionado el nacimiento del concepto conocido como la «administración electrónica», «gobierno electrónico» o «e-administración» (e-government en inglés).

1.2.2. Definición de la e-administración

INTOSAI define[7] la e-administración como el intercambio online de información gubernamental con, y el suministro de servicios a, ciudadanos, empresas y otros entes públicos.

De forma más completa, EUROSAI define[8] la e-administración como el uso de las tecnologías de la información y las comunicaciones por las administraciones con el objetivo de:

7. *Auditing e-Government*, The INTOSAI Standing Committee on IT Audit, 2003, página 5.

8. *E-Government in an Auditing perspective*, EUROSAI, IT Working Group, marzo 2004, página 5.

a) proporcionar más y/o mejor información y otros servicios, externamente, a los ciudadanos y empresas e, internamente, a otras organizaciones públicas;

b) mejorar las operaciones de la administración en términos de mayor eficacia y/o eficiencia; y

c) mejorar la participación política.

1.2.3. Niveles de madurez en la e-administración

El Standing Committee on IT Audit de INTOSAI define cuatro niveles de madurez en la e-administración, que básicamente son los que se han utilizado (añadiendo el nivel 0) en el *Estudio Comparativo 2009 de los Servicios Públicos on-line en las Comunidades Autónomas Españolas*;[9] éstos consisten en:

– *Nivel 0*

  Ausencia total de cualquier sitio web accesible públicamente gestionado por el proveedor del servicio, o el proveedor del servicio tiene un sitio web, pero éste no ofrece ninguna posibilidad de información relevante, interacción, interacción bidireccional o transacción en relación con el servicio analizado.

– *Nivel 1* - Información.

  La información necesaria que describe el procedimiento para la obtención del servicio público está disponible *on-line*.

– *Nivel 2* - Interacción unidireccional.

  El sitio web ofrece la posibilidad de descargar el formulario de la *website* para su impresión y posterior cumplimentación manual. También se considera nivel 2 la posibilidad de obtener un formulario electrónico para su cumplimentación *on-line*, su posterior impresión y presentación física en la oficina correspondiente.

– *Nivel 3* - Interacción bidireccional.

  El sitio web ofrece la posibilidad de la introducción electrónica de datos mediante un formulario electrónico para iniciar *on-line* el procedimiento de obtención del servicio. Esta etapa requiere de una autentificación de la persona (física o jurídica) que solicita el servicio.

9. *Estudio Comparativo 2009 de los Servicios Públicos on-line en las Comunidades Autónomas Españolas*, Cap Gemini y Fundación Orange, abril 2009 (página 65).

– *Nivel 4* - Tramitación totalmente electrónica.

El sitio web ofrece la posibilidad de tramitar el servicio público de forma totalmente electrónica. No se requiere del solicitante ningún otro procedimiento formal mediante «documentos en papel» o presencia física en oficinas públicas.

1.2.4. Ley de la administración electrónica

La aprobación de la denominada Ley de la administración electrónica (Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos) ha conferido unos derechos concretos y explícitos a los ciudadanos en el uso de las tecnologías de la información y las comunicaciones en sus relaciones con la Administración.

Estos derechos hacia los ciudadanos obligan a las distintas administraciones (central, autonómica y local) a desarrollar, implantar y habilitar un conjunto de servicios para atender a una amplia diversidad de requerimientos, como son los de disponibilidad (servicio continuado, las 24 horas los 7 días de la semana), de universalidad (para todos los ciudadanos, allí donde se encuentren), de calidad (posibilidad de conocer en todo momento el estado de tramitación de sus procedimientos), o de eficiencia (simplificación de los procedimientos y de sus trámites, no aportar documentos que ya obran en poder de la Administración).

Las disposiciones que establece la ley determinan acciones que afectan tanto a la organización interna como a la forma de interactuar con los usuarios y ambos entornos deben desarrollarse alineadamente.

La administración electrónica no es únicamente comunicación electrónica entre ciudadano y Administración. Consiste, una vez alcanzado el nivel de madurez 4 (según los criterios antes citados), en disponer de un servicio completo, de principio a fin, en el que los procedimientos administrativos tengan una tramitación electrónica, desde la identificación del ciudadano y del empleado público que intervienen en el procedimiento hasta la elaboración del expediente enteramente electrónico, sin importar por qué administraciones haya transitado el expediente.

1.2.5. Grado de desarrollo de la e-administración en las Comunidades Autónomas

Hasta la aprobación de la Ley 11/2007 eran las propias Comunidades Autónomas las que definían sus estrategias de modernización

y decidían en qué situaciones, momentos y a través de qué canales se concedía el acceso de los ciudadanos y las empresas a los servicios públicos on-line.

La Ley obliga a desarrollar, implantar y habilitar un conjunto de servicios para atender a una amplia diversidad de requerimientos como son la disponibilidad, universalidad, calidad o eficiencia.

Debido a sus diferentes estrategias y calendarios de implantación de los servicios electrónicos, el grado de madurez de la e-administración en cada comunidad es diferente. Según un estudio[10] realizado sobre la disponibilidad de 26 servicios online en todas la CCAA, los resultados globales, son:

CC AA	Disponibilidad Media Total (26 Servicios)	Disponibilidad Media de Ciudadanos (16 Servicios)	Disponibilidad Media de Empresas (10 Servicios)	Diferencial Media Ciudadanos Vs Media Empresas
Andalucía	88	88	90	- 2
Aragón	63	69	55	+ 14
Asturias	97	97	98	- 1
Baleares	60	59	60	- 1
Canarias	64	66	63	+ 3
Cantabria	59	64	50	+ 14
Castilla-La Mancha	66	69	63	+ 6
Castilla y León	73	77	68	+ 9
Cataluña	74	77	70	+ 7
Comunidad Valenciana	71	72	70	+ 2
Extremadura	67	66	70	- 4
Galicia	77	81	70	+ 11
La Rioja	69	72	65	+ 7
Madrid	86	88	83	+ 5
Murcia	72	75	68	+ 7
Navarra	88	86	93	- 7
País Vasco	78	78	78	0
Ceuta	62	67	55	+ 12
Melilla	49	60	35	+ 25
Media Total	**72**	**74**	**68**	**+ 6**

Figura 1.3

10. *Estudio Comparativo 2009 de los Servicios Públicos on-line en las Comunidades Autónomas Españolas*, Cap Gemini y Fundación Orange, abril 2009.

Los mismos resultados mostrados en un gráfico bidimensional por la misma fuente:

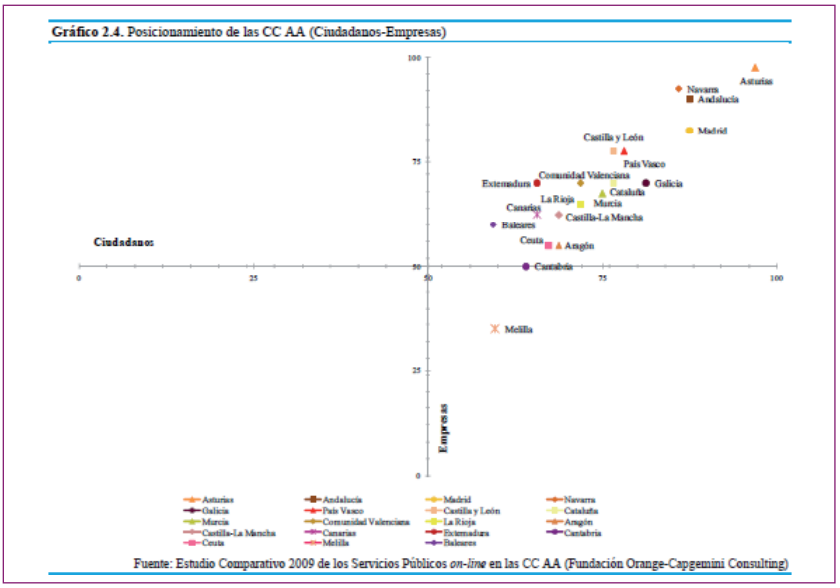


Figura 1.4

En el siguiente gráfico elaborado por la Comisión Europea[11] puede verse, comparativamente, en qué situación se encuentra nuestro país entre los países europeos:

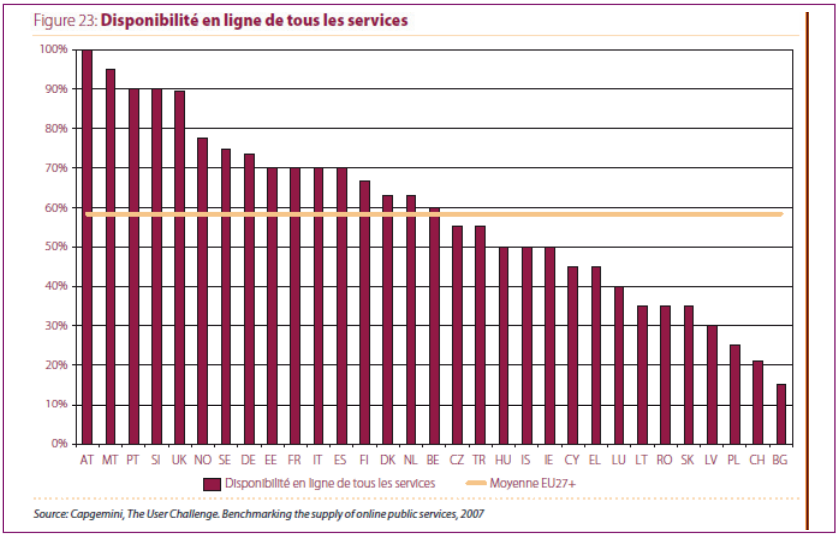


Figura 1.5

11. *Préparer l'avenir numérique de l'Europe. Examen à mi-parcours de l'initiative i2010*, Comunicación de la Comisión de la Unión Europea, abril de 2008 (página 54).

1.3. La e-gestión económica

Paralelamente al desarrollo de la interacción digital con los ciudadanos y empresas, fundamentalmente mediante el uso de Internet, las distintas administraciones públicas y entes dependientes, han desarrollado herramientas, aplicaciones y sistemas informáticos cada vez más complejos para automatizar y soportar las distintas áreas de gestión.

La relación de áreas o funciones soportadas por sistemas informáticos sería extensísima, hoy en día prácticamente todas las actividades se ejecutan en mayor o menor medida con el auxilio de dichos sistemas.

Por señalar solo algunos de los de mayor interés para los auditores públicos:

- Contabilidad
- Gestión presupuestaria
- Recursos humanos
- Gestión de las subvenciones
- Gestión tributaria y recaudación
- Gestión de la contratación
- Mantenimiento de inventarios. etc.

La utilización de ordenadores para la gestión de todas estas y otras muchas áreas no es nueva en la administración, pero especialmente en los últimos 10 o 15 años se ha producido una significativa evolución en la utilización de las tecnologías de la información y las comunicaciones aplicadas a la gestión de las administraciones públicas.

La utilización de complejas aplicaciones ERP (Enterprise Resource Planning) se ha extendido a buena parte de las administraciones españolas. Estas aplicaciones informáticas están diseñadas para cubrir varias o incluso todas las áreas funcionales de una organización de tal manera que se crea un flujo de trabajo entre los distintos usuarios (sin flujo físico de papel), con acceso instantáneo a toda la información; las operaciones que suponen movimientos monetarios se recogen automáticamente (sin intervención humana y sin papel) en el módulo contable. Las personas que deben autorizar las distintas operaciones lo hacen también firmando electrónicamente a través del sistema y muchas autorizaciones están automatizadas.

Esta intensa informatización plantea a los auditores públicos (y también a los privados) una serie de problemas de auditoría a los que se debe hacer frente aplicando una metodología de auditoría adaptada a las nuevas circunstancias.

Más adelante se comentan con mayor profundidad los nuevos problemas y situaciones, pero entre los más evidentes se pueden señalar:[12]

- Ausencia de transacciones y autorizaciones documentadas en soporte papel, como pedidos, albaranes, facturas, cheques, órdenes de transferencia de fondos, etc.
- Sustitución de procedimientos de control interno manuales (realizados por empleados-funcionarios) por otros que se realizan automáticamente por los sistemas informáticos, (p.e. segregación de funciones, conciliaciones de cuentas, etc.).
- Riesgo de manipulación de la información.
- Pérdida generalizada de las pistas visibles de auditoría.

Un ejemplo de este proceso de informatización de las administraciones públicas podemos apreciarlo en la *«Instrucción del modelo normal de contabilidad local»* (aprobada por la Orden EHA/4041/2004, de 23 de noviembre; BOE de 9.12.2004), que representa una decidida apuesta por la incorporación de las técnicas electrónicas, informáticas y telemáticas a la actividad administrativa local.

De acuerdo con esta Instrucción, una de las consecuencias más destacadas de la utilización de las tecnologías de la información y las comunicaciones en la función contable, es la desaparición de la obligación de obtener y conservar los libros de contabilidad tradicionales en papel, estableciéndose que las bases de datos del sistema informático donde residan los registros contables constituirán soporte suficiente para la llevanza de la contabilidad de la entidad. Desaparece, por tanto, la concepción tradicional de libro de contabilidad, y se sustituye por la de base de datos contable.

Además, como se señala en la exposición de motivos de la Instrucción, en la línea de «fomentar una nueva cultura administrativa en la que el papel, en la medida de lo posible, vaya siendo sustituido por los documentos automatizados, con los ahorros tanto económicos como de espacio físico que ello implicará, se ha establecido que los justificantes de los hechos que se registren en el SICAL-Normal po-

12. *La fiscalización en entornos informatizados*, Antonio Minguillón, Auditoría Pública n.º 40, diciembre de 2006.

drán conservarse por medios o en soportes electrónicos, informáticos o telemáticos, con independencia del tipo de soporte en que originalmente se hubieran plasmado, siempre que quede garantizada su autenticidad, integridad, calidad, protección y conservación. En estos casos las copias obtenidas de dichos soportes informáticos gozarán de la validez y eficacia de la justificación original.»

El efecto de todo este proceso es que se ha llegado a una situación en la que las pistas de auditoría (firmas, documentos contables, autorizaciones, libros de contabilidad) en soporte tradicional en papel, ya no existen. El reto al que se enfrentan los auditores públicos es que la actual situación implica un cambio profundo en la metodología de auditoría y en las herramientas que se deben utilizar y afecta también a aspectos relacionados con los perfiles formativos y profesionales requeridos por los auditores públicos.

2
Auditoría e informática

2.1. Tipos de auditoría informática

Las tecnologías de la información y las comunicaciones introducen una serie de nuevas áreas de actividad para los auditores públicos, cada una de ellas con retos, planteamientos y objetivos diferentes.

El término de auditoría informática o auditoría de sistemas de información, tiene un significado muy amplio, dependiendo de los objetivos fijados específicamente para cada auditoría.

Algunos tipos posibles de auditorías informáticas son:

– Auditoría de la administración electrónica.

  Esta es un área nueva de trabajo que en el futuro próximo puede suponer una importante fuente de trabajo para los auditores públicos.

  En el capítulo 1.1 de este trabajo se han citado sendos informes de la Audiencia de Cuentas de Canarias y de la Cámara de Cuentas de Andalucía, que son ejemplos de esta categoría.

  La capacidad de los órganos fiscalizadores para auditar la administración electrónica es generalmente proporcional al nivel de la madurez de la administración electrónica del país y la región de su ámbito de actuación y de las capacidades profesionales de aquellos órganos.

– Auditoría de gestión de datos personales.

  El artículo 96 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, estableció la obligatoriedad de realizar determinadas auditorías:

> Artículo 96. Auditoría.
> 1. A partir del nivel medio, *los sistemas de información e instalaciones de tratamiento y almacenamiento de datos* se someterán, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento del presente título.

Con carácter extraordinario deberá realizarse dicha auditoría siempre que se realicen modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas con el objeto de verificar la adaptación, adecuación y eficacia de las mismas. Esta auditoría inicia el cómputo de dos años señalado en el párrafo anterior.
2. El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles a la Ley y su desarrollo reglamentario, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias. Deberá, igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y las recomendaciones propuestas.
3. Los informes de auditoría serán analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del fichero o tratamiento para que adopte las medidas correctoras adecuadas y quedarán a disposición de la Agencia Española de Protección de Datos o, en su caso, de las autoridades de control de las comunidades autónomas.

La ley prevé en su artículo 1 que «tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal». Comprende por tanto el tratamiento automatizado y el no automatizado de los datos de carácter personal.

No obstante en los entornos actuales altamente informatizados, la mayor parte de los datos de carácter personal (como los no personales) son procesados y almacenados en sistemas informatizados. En consecuencia, las auditorías a las que hace referencia el artículo 96 del reglamento arriba trascrito se ha convertido en una «especialidad» de la auditoría informática y en una importante fuente de trabajos e ingresos de los auditores privados.

Los auditores públicos también podrían incluir en sus planes de trabajo la realización de este tipo de auditoría, como una parte de sus prerrogativas generales de revisión del cumplimiento de la legalidad prevista en la normativa reguladora de los OCEX. Siempre sin perjuicio de las competencias de inspección que tienen los entes públicos expresamente previstos en la Ley para velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos. Estos entes actualmente son:

- Agencia Española de Protección de Datos
- Agencia Catalana de Protección de Datos
- Agencia de Protección de Datos de la Comunidad de Madrid
- Agencia Vasca de Protección de Datos

– Auditoría forense

  En aquellos casos que existan sospechas de fraude o actuaciones ilegales, pueden realizarse investigaciones para obtener evidencia (pruebas) utilizando herramientas informáticas para recuperar datos de forma legal de equipos informáticos utilizados por los sospechosos y posteriormente analizarlos.

  Este tipo de actuaciones se realiza, generalmente, por la policía, fiscalía o a instancia judicial.

– Auditoría de gestión

  Examen de un sistema informático para evaluar si los objetivos previstos al implementar el sistema han sido alcanzados efectivamente, con criterios de economía y eficiencia.

  Entraría dentro del concepto más amplio de auditoría operativa o auditoría de performance.

– Auditorías específicas sobre adquisición de equipos y sistemas.

  Dada la complejidad, su efecto en la organización y el elevado coste de los actuales sistemas informáticos, este tipo de auditorías son de realización frecuente en los auditores públicos más avanzados a nivel internacional.[13]

  En España puede verse un ejemplo de informe: el realizado por la Cámara de Comptos de Navarra, citado en el capítulo 1.1 de este trabajo.

  Existe una relativamente abundante metodología a nivel internacional sobre este tipo de trabajos[14] y, curiosamente, es también muy abundante la literatura relacionada con el análisis de proyectos fallidos.

– Auditoría de seguridad informática.

  Auditoría de controles de seguridad en sistemas informáticos para evaluar la extensión en la que se mantiene la confidencialidad, integridad y disponibilidad de los datos y los sistemas, teniendo en consideración el perfil de riesgo de la entidad y de sus sistemas TI.

  Es una de las auditorías de mayor interés para las entidades y empresas, ya que en los complejos sistemas informatizados

13. Puede verse como ejemplo el informe de la UK Nacional Audit Office, *Improving the disposal of public sector Information, Communication and Technology Equipment*, de Julio 2007.

14. Por ejemplo la *GTAG 12: Auditing IT Projects*, del Institute of Internal Auditors.

actuales se multiplican las potenciales vulnerabilidades de seguridad que deben ser adecuadamente cubiertas.[15]

– Auditoría de aplicaciones informáticas/sistemas de información y auditorías limitadas sobre controles generales y de aplicación.

  Revisiones sobre los controles manuales y automatizados en un sistema informatizado, con el objetivo de evaluar el grado de confianza que puede depositarse en las transacciones procesadas y en los informes generados por el sistema.

– **Auditoría de sistemas de información realizada en el marco de una auditoría financiera.**

  Este va a ser el tema que vamos a desarrollar en el presente trabajo.

  No vamos a analizar la auditoría informática como una disciplina autónoma, con muchas áreas importantes para desarrollar, sino que vamos a centrarnos en el estudio de la auditoría de sistemas de información ejecutada como parte, importante, de una auditoría financiera de las cuentas anuales de una entidad pública.[16]

Como puede apreciarse (y la relación anterior no es exhaustiva) hay muchos tipos de auditorías informáticas, dependiendo de cuál sea el objetivo de la misma. En unos casos se tratará de trabajos autónomos, centrados exclusivamente en algún aspecto de la función informática, y en otros casos la auditoría informática será un elemento importante pero subordinado respecto del objetivo principal. Este último es el tipo de auditoría en el que se centra este trabajo.

En el presente trabajo se pretende exponer desde un punto de vista lo más práctico posible, un planteamiento para la realización de auditorías financieras integrando metodología de auditoría informá-

15. Pueden verse numerosos ejemplos de informes o testimonios sobre seguridad informática en el sitio web del U.S. Government Accountability Office (GAO). Entre los más recientes:

– *Information Security: Agencies Make Progress in Implementation of Requirements, but Significant Weaknesses Persist*, GAO-09-701T (Washington, May 19, 2009).
– *Cybersecurity: Continued Federal Efforts Are Needed to Protect Critical Systems and Information,* GAO-09-835T (Washington, June 25, 2009).

16. Cuando hablemos de una «entidad pública» genéricamente nos referimos a cualquier ente del sector público, independientemente de su forma jurídica, que formule cuentas anuales. Es decir puede tratarse de cualquier administración pública, organismos autónomos, entes de derechos público, sociedades mercantiles, fundaciones públicas, etc.

tica o auditoría de sistemas de información. Para ello nos basaremos en el análisis de las mejores prácticas a nivel internacional.

2.2. Evolución desde el enfoque de auditoría «tradicional» o «auditoría alrededor del ordenador» hacia el enfoque actual o «auditoría a través del ordenador»

Según se señala en la revista Auditoría Pública,[17] en nuestro país hasta la entrada en vigor de la *Norma Técnica de Auditoría del ICAC sobre la auditoría de cuentas en entornos informatizados (NTAEI)*, aprobada por Resolución del ICAC de 23 de junio de 2003, y su posterior aplicación, los auditores financieros han tenido muchas veces la tentación (ante situaciones para ellos desconocidas en mayor o menor grado y que por tanto no controlan) de asignar un riesgo alto a los sistemas de control interno informatizados y así confiar únicamente en las pruebas sustantivas para obtener evidencia suficiente y adecuada.[18]

En el enfoque denominado coloquialmente «auditoría alrededor del ordenador» se utilizan técnicas para comprobar la fiabilidad de la información que genera el sistema informático revisando los inputs al sistema y verificando que los outputs coinciden con los cálculos o estimaciones que realiza el auditor. Está basado casi exclusivamente en pruebas sustantivas y puede no ser viable cuando se audita una entidad con un entorno informatizado complejo, donde predomina la evidencia informática y la capacidad del auditor para obtener evidencia sólo a partir de pruebas sustantivas está muy limitada.

Este enfoque de «auditoría alrededor del ordenador» no debe ser considerado como totalmente obsoleto, pero debe limitarse estrictamente a aquellas situaciones en las que se verifique simultáneamente el cumplimiento de estas tres condiciones:[19]

1. La pista auditora es completa y visible. Esto implica que se utilizan documentos fuente en todo tipo de transacciones, se imprimen los libros diarios detallados, y se mantienen referencias de las transacciones tanto en el libro diario como en el mayor.

17. *La fiscalización en entornos informatizados*, Antonio Minguillón, Auditoría Pública n.º 40, diciembre 2006.

18. En el artículo de Virginia y Michael Cerillo *Impact of SAS n.º 94 on Computer Audit Techniques*, en *Information Systems Control Journal*, volume 1, 2003, se destaca que según una encuesta realizada antes de la entrada en vigor del SAS 94 la mayoría de los auditores en EEUU seguía la práctica mencionada. No obstante, en EEUU la promulgación de la Ley Sarbanes-Oxley en 2002 endureció mucho y multiplicó las exigencias respecto la evaluación de riesgos.

19. Ver Pablo Lanza en *Iniciación a la auditoría de sistemas de información* (página 27).

2. Las operaciones de proceso de la información son relativamente sencillas y directas.
3. El auditor tiene a su disposición la documentación completa del sistema, incluyendo diagramas de flujo, descripción de registros, etc.

Al auditar actualmente una entidad pública con un sistema de información avanzado e informatizado, no se cumplen dichas condiciones y en esos casos se debe aplicar el enfoque denominado «auditoría a través del ordenador» o más correctamente «enfoque de auditoría basado en el análisis de los riesgos», que se describe con mayor detalle en los siguientes capítulos.

La Norma Internacional de Auditoría 330, también estipula que el auditor debe planificar y ejecutar pruebas sobre controles clave (incluyendo los informáticos) si los procedimientos sustantivos no pueden por sí solos proporcionar evidencia apropiada de auditoría (párrafo 8b). Además, (párrafo A24) **en determinados casos, al auditor le puede ser imposible diseñar pruebas sustantivas eficaces que por sí solas proporcionen suficiente evidencia de auditoría apropiada**. Esto probablemente sucederá cuando la entidad desarrolle su actividad en un entorno informatizado complejo, en el que no se produce o conserva documentación de las transacciones si no a través de los sistemas informáticos. En estos casos se requiere al auditor que ejecute pruebas de los controles clave existentes en el sistema.

2.3. La evidencia informática de auditoría

2.3.1. Aspectos generales de la evidencia de auditoría

a) Concepto y naturaleza

La evidencia de auditoría es toda la información usada por el auditor para alcanzar las conclusiones sobre las que basa su opinión de auditoría, sus conclusiones y recomendaciones.

Los Principios y Normas de Auditoría del Sector Público (PNASP),[20] apartado 3.2.4 establecen que «para fundamentar sus opiniones y conclusiones, el auditor deberá obtener evidencia suficiente, pertinente y válida, mediante la realización y evaluación de las pruebas de auditoría que se consideren necesarias».

20. Principios y Normas de Auditoría del Sector Público, elaborados por la Comisión de Coordinación de los Órganos de Control Externo (OCEX) de España, 1991.

La naturaleza de la evidencia está constituida por todos aquellos hechos y aspectos susceptibles de ser verificados por el auditor, y que tienen relación con las cuentas anuales que se examinan.

La evidencia se obtiene por el auditor mediante la realización de las pruebas de auditoría, aplicadas según las circunstancias que concurran en cada caso, y de acuerdo con el juicio profesional del auditor.

Según cual sea su fuente, la evidencia puede obtenerse de pruebas materiales, documentales, testimoniales y analíticas.

b) Características de la evidencia

Dado que en pocas ocasiones se puede tener certeza absoluta sobre la validez de la información, el auditor, para tener una base razonable en que apoyar su informe, precisa que la evidencia tenga unas características esenciales; la evidencia debe ser: suficiente y apropiada (pertinente y fiable).

1. Suficiente

Evidencia suficiente es la evidencia que el auditor necesita en términos cuantitativos para obtener una seguridad razonable que le permita expresar una opinión en el informe de auditoría sobre las cuentas anuales auditadas.

Es decir, es la medida de la cantidad de evidencia. La valoración del número de elementos de prueba que se considera suficiente depende del juicio del auditor, que se ve afectado por factores tales como:

- El riesgo de que existan errores en las cuentas anuales auditadas.
- La importancia relativa de la partida analizada en relación con el conjunto de la información financiera.
- La experiencia adquirida en auditorías previas de la entidad.
- Los resultados obtenidos de los procedimientos de auditoría incluyendo errores o irregularidades que hayan podido ser descubiertos.
- La calidad de la información económico-financiera disponible.
- La confianza que le merezcan la Dirección de la entidad y sus empleados.
- El tipo de procedimiento utilizado para obtener la evidencia.
- La clase de evidencia obtenida (material, documental, testimonial o analítica).

En este contexto el auditor no pretende obtener toda la evidencia existente sino aquélla que cumpla, a su juicio profesional, con los objetivos de su examen. Por lo tanto, puede llegar a una conclusión sobre un saldo, transacción o control, realizando pruebas de auditoría, mediante muestreo (estadístico o de selección en base subjetiva), mediante pruebas analíticas o a través de una combinación de ellas.

El nivel de evidencia a obtener por el auditor, referido a los hechos económicos y otras circunstancias, debe estar relacionado con la razonabilidad de los mismos y proporcionarle información sobre las circunstancias en que se produjeron, con el fin de que pueda formarse el juicio profesional que le permita emitir una opinión.

Para decidir el nivel necesario de evidencia, el auditor debe en cada caso, considerar la importancia relativa de las partidas que componen los diversos epígrafes de las cuentas anuales y el riesgo de error en el que incurre al decidir no revisar determinados hechos económicos.

Debe considerarse el coste que supone la obtención de un mayor nivel de evidencia que el que está obteniendo o espera obtener, y la utilidad final probable de los resultados que obtendría. Ello no obstante, independientemente de las circunstancias específicas de cada trabajo, el auditor debe obtener siempre el nivel de evidencia necesario que le permita formar su juicio profesional sobre las cuentas anuales.

La falta del suficiente nivel de evidencia sobre un hecho significativo en el contexto de los datos que se examinan, obliga al auditor a expresar las salvedades que correspondan o, en su caso, a denegar su opinión.

2. Apropiada (o adecuada)

Apropiada es la medida de la calidad de la evidencia de auditoría, calidad que está condicionada por la relevancia (o pertinencia) y fiabilidad (validez) de la misma.

Es la característica cualitativa, en tanto que el concepto «suficiente» tiene carácter cuantitativo. La confluencia de ambos elementos, debe proporcionar al auditor el conocimiento necesario para alcanzar una base objetiva de juicio sobre los hechos sometidos a examen.

El concepto de evidencia **relevante** o pertinente se refiere a su razonabilidad y consiste en la apreciación de la relación entre la evidencia y su uso. En este sentido, las informaciones utilizadas para probar o desaprobar un dato son pertinentes si tienen una relación lógica y

sensible con ese dato, mientras que las informaciones que no posean tal característica, no deberán utilizarse como elementos de prueba.

La **fiabilidad** de la evidencia de auditoría está influenciada por sus fuentes, por su naturaleza y por las circunstancias individuales de su obtención. Una evidencia no confiable no constituye evidencia de auditoría.

2.3.2. La evidencia informática de auditoría

a) Concepto

Además de los cuatro tipos de evidencia antes señalados (material o física, documental, testimonial y analítica) en los últimos lustros ha ido aumentando la importancia de un nuevo tipo de evidencia, con características completamente diferentes, que condiciona buena parte del trabajo del auditor. Este tipo de evidencia, que se denomina evidencia informática, tiene una característica que a priori destaca sobre las demás:[21] la ininteligibilidad y la imposibilidad de su tratamiento o análisis por los medios tradicionales de auditoría.

Las Normas de Auditoría del Sector Público (NASP) de la Intervención General de la Administración del Estado, regulan con un cierto detalle aspectos relacionados con la obtención por el auditor de evidencia adecuada en un entorno informatizado.

De acuerdo con el apartado 5.3.2 de las Normas de Auditoría del Sector Público, la evidencia informática queda definida así:

«Evidencia informática. Información y datos contenidos en soportes electrónicos, informáticos y telemáticos, así como los elementos lógicos, programas y aplicaciones utilizados en los procedimientos de gestión del auditado. Esta evidencia informática incluirá los elementos identificados y estructurados que contienen texto, gráficos, sonidos, imágenes o cualquier otra clase de información que pueda ser almacenada, editada, extraída e intercambiada entre sistemas de tratamiento de la información, o usuarios de tales sistemas, como unidades diferenciadas.»

b) Tipos de evidencia informática

Esta definición de evidencia informática distingue entre dos tipos de evidencia informática de características muy distintas que requerirán de los auditores conocimientos, técnicas y procedimientos adaptados a cada tipo. Puede distinguirse entre:

21. Véase: *Técnicas de auditoría asistida por ordenador*, Pablo Lanza, 2000, Instituto de Estudio Fiscales (pág 25).

1. Información y datos

Al fiscalizar en entornos informatizados complejos, la pista visible de muchas transacciones revisadas por los auditores han desaparecido físicamente, transformándose en algo intangible. No se dispone en muchos casos de los documentos físicos para visualizarlos, comprobar firmas, fotocopiar, poner tildes, etc.

En muchos casos las facturas de proveedores, albaranes, etc, se reciben en formato digital[22] o se escanean,[23] se archivan en el ordenador y el original en papel desaparece, pudiéndose visualizar únicamente a través del sistema informático.

En este sentido es interesante revisar la Instrucción Modelo Normal de Contabilidad Local (IMNCL), que regula el soporte informático de los registros contables:

> Regla 14. Soporte de los registros contables
> 1. Los registros de las operaciones y del resto de la información capturada en el SICAL-Normal, estarán soportados informáticamente según la configuración que se establece en la regla anterior, constituyendo el soporte único y suficiente que garantice su conservación de acuerdo con la regla 93.

22. La factura electrónica es un equivalente funcional de la factura en papel y consiste en la transmisión de las facturas o documentos análogos entre emisor y receptor por medios electrónicos (ficheros informáticos) y telemáticos (de un ordenador a otro), firmados digitalmente con certificados reconocidos.

La factura electrónica es un documento electrónico que cumple con los requisitos legal y reglamentariamente exigibles a las facturas y que, además, garantiza la autenticidad de su origen y la integridad de su contenido, lo que permite atribuir la factura a su emisor.

De está definición extendida en todo el mercado, se transmite tres condicionantes para la realización de factura electrónica:

– Se necesita un formato electrónico de factura de mayor o menor complejidad (EDIFACT, XML, PDF, html, doc, xls, gif, jpeg o txt, entre otros).

– Es necesario una transmisión telemática (tiene que partir de un ordenador, y ser recogida por otro ordenador).

– Este formato electrónico y transmisión telemática, deben garantizar su integridad y autenticidad a través de una firma electrónica reconocida.

Las facturas electrónicas deben incorporar medios que garanticen la autenticidad e integridad de acuerdo con lo establecido en el Real Decreto 1496/2003, de 28 de noviembre, que aprueba el Reglamento que regula las obligaciones de facturación, así como en la Orden EHA/962/2007, de 10 de abril, por la que se desarrollan determinadas disposiciones sobre facturación telemática y conservación electrónica.

23. El escaneo o conversión de un documento en formato papel a formato digital, con todas las garantías jurídicas, también está regulado por la Orden EHA/962/2007.

2. **Las bases de datos del sistema informático** donde residan los registros **contables constituirán soporte suficiente** para la llevanza de la contabilidad de la entidad contable, sin que sea obligatoria la obtención y conservación de libros de contabilidad…

Regla 88. Medios de justificación

1. **La justificación** de los distintos hechos susceptibles de incorporación al SICAL-Normal **podrá estar soportada en documentos en papel o a través de medios electrónicos, informáticos o telemáticos**...

La evidencia informática es información creada, transmitida, procesada, grabada, y/o guardada en soporte informático que respalda el contenido del informe de fiscalización.

Únicamente se puede acceder a la información mediante la utilización de unos equipos y tecnología adecuados, tales como ordenador, software, impresora, escáner, lector o medios magnéticos. Los documentos electrónicos pueden ser textos, imágenes, archivos de audio o video.

La evidencia informática incluye asientos contables, documentos de referencia y justificantes como contratos electrónicos, documentos electrónicos relacionados con facturación, adquisiciones y pagos, confirmaciones electrónicas y cualquier otra información electrónica relacionada con la auditoría.

Los datos pueden variar en su formato (desde ficheros electrónicos a tablas en informes impresos). Algunos ejemplos son:

- Datos extraídos de bases de datos, data warehouses o repositorios de información.
- Datos mantenidos en Microsoft Excel o Access o productos similares.
- Datos extraídos de ERP mantenidos interna o externamente.
- Datos públicamente accesibles o datos replicados accesibles a través de una aplicación distinta del sistema fuente original.
- Datos obtenidos de formularios o encuestas en portales web.
- Datos resumidos en un informe o copiados en un documento, procedentes de una tabla.

Este tipo de evidencia afecta al grado de fiabilidad, así como a la competencia del auditor para trabajar con ella y al enfoque de la fiscalización. Igualmente afecta a los métodos y procedimientos utilizados para obtenerla, planteándose el problema de cómo recuperar, analizar y evaluar la evidencia informática (en el capítulo

8 se comentan las técnicas de auditoría asistida por ordenador). También se plantean problemas a la hora de documentar la evidencia informática.

Otro problema importante que afrontar, se deriva del hecho de que en muchos casos los datos en soporte magnético pueden no estar disponibles transcurrido un cierto tiempo por distintas razones (archivos temporales, cambio de formatos, incompatibilidades, deterioro o degradación de la información).

Resumiendo, la generalización de sistemas de información automatizados en el ámbito de la gestión pública ha llevado en paralelo la desaparición de las pistas visibles de auditoría en múltiples operaciones y procesos. De aquí surge la necesidad de desarrollar metodología adaptada a las circunstancia y utilizar herramientas informáticas, que permitan ejecutar el trabajo de fiscalización en el nuevo entorno tecnológico.

2. Programas y aplicaciones

Entre los procedimientos de una fiscalización está la revisión de los procedimientos administrativos y contables de la entidad auditada, del flujo de documentos, la comprobación de las autorizaciones, la evaluación y la prueba de los controles internos existentes (segregación de funciones, etc.).

La ejecución de estos procedimientos se complica cuando dejan de realizarse manualmente, y se transforman en procedimientos y controles realizados automáticamente por el sistema informático. Como en el apartado anterior, vamos a ver cómo la Instrucción Modelo Normal de Contabilidad Local, regula el tratamiento informatizado de determinados procedimientos y controles:

Regla 90.2:

2. Cuando las operaciones se incorporan al sistema mediante la utilización de soportes electrónicos, informáticos o telemáticos, los procedimientos de autorización y control mediante diligencias, firmas manuscritas, sellos u otros medios manuales podrán ser **sustituidos por autorizaciones y controles establecidos en las propias aplicaciones informáticas** que garanticen el ejercicio de la competencia por quien la tenga atribuida.

Regla 91.2 Toma de razón:

2. En el caso de que las operaciones sean registradas a partir de los datos contenidos en soportes electrónicos, informáticos o telemáticos, la diligencia de toma de razón se sustituirá por los oportunos procesos de validación en el sistema**, mediante los cuales dichas operaciones queden referenciadas en relación con las anotaciones contables que hayan producido.**

En un entorno automatizado, solo la revisión de los sistemas lógicos informáticos de gestión, de los programas informáticos, proporcionará evidencia de auditoría suficiente que permita al auditor conocer cuál es el flujo de documentos electrónicos, las autorizaciones explícitas e implícitas, si existe segregación de funciones, los controles de seguridad existentes y otros procedimientos de control interno.

La fiscalización de sistemas complejos que interrelacionan e integran distintas áreas funcionales de las organizaciones y la desaparición progresiva del soporte papel, implica que la obtención de evidencia mediante el análisis y evaluación de tales sistemas excederá normalmente las competencias de un auditor financiero requiriéndose la intervención de un especialista en auditoría informática.

2.3.3. Fiabilidad de la evidencia informática

a) Aspectos generales

En el apartado 5.3.16 de las NASP se dice que: «Los auditores deberán tener evidencia suficiente y adecuada (relevante y fiable) de que los datos provenientes de sistemas informáticos sean válidos y fiables cuando tales informaciones sean significativas para los resultados de la auditoría.»

El auditor podrá utilizar estas informaciones si otros auditores han verificado la validez y fiabilidad de los datos o la eficacia de los controles sobre el sistema que los genera. En caso contrario, deberán realizar la validación ellos mismos mediante una combinación de pruebas sustantivas y pruebas sobre el adecuado funcionamiento de los sistemas informatizados.

A fin de poder valorar si la evidencia informática obtenida para respaldar el informe de auditoría es suficiente y adecuada, el auditor debe considerar los riesgos específicos asociados al uso de este tipo de evidencia. Estos riesgos no pueden ser evaluados únicamente revisando la evidencia documental, como suele hacerse con los documentos en papel. La copia impresa de la información en soporte informático o la lectura de la información directamente de la pantalla del ordenador es solamente un formato. Y éste no proporciona ninguna indicación del origen y autorización, ni tampoco garantiza la integridad de la información.

Los auditores deben asegurarse que los controles y las distintas tecnologías utilizadas para crear, procesar, transmitir y guardar información en soporte informático son suficientes para garantizar su fiabilidad.

Cuando el equipo auditor emplee datos provenientes de sistemas informáticos y los incluya en el informe con fines tan sólo ilustrativos y no significativos para los resultados, bastará, para satisfacer las normas técnicas, con citar la fuente de tales datos indicando que no han sido verificados.

El apartado 5.3.10 de las NASP dice que «Cuando se emplee evidencia informática, o datos procedentes de sistemas informáticos del auditado, los auditores deberán evaluar la fiabilidad de esta evidencia, y no darla nunca por supuesta a priori.»

Es decir, cualquier documento o dato generado por un ordenador que utilicemos como evidencia en una auditoría debe ser específicamente validado para asegurarnos razonablemente de su fiabilidad en la misma medida que cualquier otro tipo de evidencia no informática.

Existen dos enfoques a la hora de evaluar la fiabilidad de los datos procedentes de sistemas informáticos: la revisión de sistemas y las revisiones limitadas o documentales.

Una revisión de sistemas evalúa y comprueba todos los controles en un sistema informático, abarcando todo el rango de sus aplicaciones, funciones y productos. Estas revisiones:

1. examinan los controles generales y de aplicación de una instalación informática,
2. verifican el cumplimiento de tales controles, y
3. efectúan pruebas sobre los datos generados o tratados por el sistema.

Mientras este enfoque proporciona un mejor entendimiento del diseño y operaciones de un sistema, también tiende a ser una actividad que consume una considerable cantidad de tiempo.

La revisión limitada (documental) está dirigida hacia unos datos en particular. De esta forma normalmente se requiere un conocimiento menos extensivo de los controles generales y de aplicación. Los controles pertinentes se examinan en la medida necesaria para juzgar el nivel de pruebas de datos a efectuar para determinar la fiabilidad de éstos.

b) Riesgos asociados y criterios para valorar la fiabilidad de la evidencia informática

Cuanto más integrado sea un sistema de información, más transacciones podrán ser procesadas y documentadas únicamente mediante medios informáticos. Los auditores tienen más probabilidades de utilizar la evidencia informática en entornos informatizados complejos.

Entre los riesgos inherentes a estos tipos de entornos figura la dependencia por parte de la entidad de su propio sistema informático, y de los de sus proveedores de servicios, junto con el riesgo de que ocurra algún fallo en cada uno de estos niveles.

Otros riesgos a considerar son la pérdida de integridad, la no autenticación, el no reconocimiento y la violación de la confidencialidad de la información, así como la pérdida de pistas de auditoría y las posibles dudas de carácter legal que puedan surgir.

A fin de poder valorar la fiabilidad de la evidencia informática recopilada para respaldar el informe de auditoría, el auditor debe considerar los riesgos específicos asociados al uso de este tipo de evidencia. Estos riesgos no pueden ser evaluados únicamente revisando la evidencia documental, como suele hacerse con los documentos en papel. La copia impresa de una información en soporte informático o la lectura de la información directamente de la pantalla del ordenador es solamente un formato. Y éste no proporciona ninguna indicación del origen y autorización, ni tampoco garantiza la integridad ni la integridad de la información. Los auditores deben asegurar que los controles y las distintas tecnologías utilizadas para crear, procesar, transmitir y guardar información en soporte informático son suficientes para garantizar su fiabilidad.

La siguiente figura 2.1 muestra los criterios para valorar la fiabilidad[24] de la información en soporte informático como evidencia de auditoría.

Autenticación	Se puede confirmar la identidad de la persona o entidad de quien procede la información.
Integridad	La completitud, exactitud, naturaleza actual y validez de la información. La integridad es la garantía de que la información ha sido validada y no ha sido alterada de forma involuntaria ni intencionada, ni ha sido destruida, al ser creada, procesada, transmitida, conservada y/o archivada.
Autorización	La información ha sido elaborada, procesada, modificada, corregida, enviada, recibida y se ha tenido acceso a ella por parte de las personas con autorización o responsabilidad para ello.
Reconocimiento (No repudio)	Una persona o entidad que haya recibido o enviado una información no puede negar haber intervenido en el intercambio y rechazar el contenido de la información. Dependiendo de si existen pruebas irrefutables del origen, recepción o contenido de la información en soporte electrónico, no se puede repudiar el origen de ésta, su recepción ni su contenido.

Figura 2.1

24. Según *Going electronic* de Andrée Lavigne and Caroline Émond, intoIT n.º 19, febrero 2004.

Estos criterios podrían utilizarse para valorar la fiabilidad de cualquier documento conteniendo información, bien en papel o en soporte informático.

La importancia de cada criterio depende de la naturaleza y del origen de la información electrónica y de su utilización para los propósitos de la auditoría. Además de valorar la fiabilidad de la evidencia de auditoría, el auditor debe investigar acerca de la disponibilidad de la evidencia electrónica para los propósitos de la auditoría. La confidencialidad de los datos también es de interés para el auditor ya que la violación de la confidencialidad podría representar un riesgo que podría afectar la situación financiera de la entidad.

La fiabilidad de la información en soporte informático depende de la fiabilidad de los sistemas de información y de las tecnologías utilizadas.

Cuando se recopila, procesa graba o guarda en soporte informático información significativa sobre una o más manifestaciones sobre los estados financieros de una entidad, puede resultar imposible reducir el riesgo de detección a un nivel aceptable confiando únicamente en la aplicación de procedimientos sustantivos. En tales casos, existe un riesgo elevado de que no puedan ser detectadas manifestaciones falsas contenidas en la información electrónica obtenida como evidencia de auditoría. El auditor puede tener que adoptar un enfoque combinado y examinar los controles para obtener unas evidencias de auditoría adecuadas.[25]

2.3.4. Propiedades diferenciadoras de la evidencia de auditoría informática respecto de la auditoría tradicional

La evidencia informática se distingue de la evidencia de auditoría tradicional en varios aspectos. En primer lugar, consiste en información en formato digital cuya estructura lógica es independiente de la información en sí. En segundo lugar, el origen de la información, el destino de ésta, así como las fechas de envío y recepción no son parte integrante del documento electrónico, mensaje u otro formato de información.

25. La US Government Accountability Office ha publicado en julio de 2009 una guía denominada *Assessing the Reliability of Computer-Processed Data* que proporciona un marco para evaluar la fiabilidad de los datos obtenidos por procedimientos informatizados para sus utilización en trabajos o auditorías no financieras (en las auditorías financieras se debe seguir una metodología como la descrita en el capítulo 5 de este trabajo, que es más completa que la descrita en la guía citada). La guía de la GAO ayuda a diseñar procedimientos para evaluar la fiabilidad de los datos utilizados para respaldar hallazgos, conclusiones o recomendaciones de los informes, y evaluar los resultados obtenidos.

De forma más detallada, en el siguiente cuadro se señalan las principales diferencias entre la evidencia de auditoría tradicional y la informática:[26]

Evidencia de auditoría tradicional	Evidencia informática de auditoría
Origen	
Se puede establecer con facilidad el origen/procedencia.	Es difícil determinar el origen si únicamente se examina información en soporte informático. Se requiere la utilización de controles y de técnicas de seguridad que permitan la autenticación y reconocimiento.
Alteración	
La evidencia en papel es difícil de alterar sin que se detecte.	Es difícil, si no imposible, detectar cualquier alteración únicamente mediante el examen de la información en soporte informático. La integridad de la información depende de los controles fiables y de las técnicas de seguridad empleadas.
Aprobación	
Los documentos en papel muestran la prueba de su aprobación en su superficie.	Es difícil de establecer la aprobación si únicamente se examina la información en soporte informático. Se requiere la utilización de controles y de técnicas de seguridad.
Integridad	
Todos los términos relevantes de una operación/transacción se incluyen por lo general en un mismo documento.	Los términos más significativos aparecen a menudo en distintos archivos de datos.
Lectura	
No se requiere ningún tipo de herramienta o equipo.	Es necesaria la utilización de distintas tecnologías y herramientas.
Formato	
Parte integral del documento.	El formato viene separado de los datos y puede modificarse.
Disponibilidad y accesibilidad	
Normalmente no es una restricción durante la fiscalización.	Las pistas de auditoría para la información en soporte informático puede que no estén disponibles en el momento de la auditoría y el acceso a los datos puede resultar más difícil.
Firma	
Es sencillo firmar un documento en papel y comprobar la firma.	Se necesitan las tecnologías adecuadas para realizar una firma electrónica fiable y revisarla.

Figura 2.2

26. Caroline Émond, *Electronic Audit Evidence*, The Canadian Institute of Chartered Accountants, 2003.

Las operaciones de obtención y análisis de evidencia informática, serán diferentes según el tipo de evidencia con la que se vaya a trabajar. La utilización de técnicas y herramientas de auditoría asistida por ordenador (como ACL, IDEA, etc.), será necesaria en buena parte de los casos, siendo una tarea abordable por cualquier auditor que reúna unos requisitos de formación mínima.

Para la revisión de los programas y aplicaciones será necesario el concurso de expertos en la revisión de sistemas informatizados, según se resume en el siguiente cuadro:

Clase de evidencia informática	Tipo de procedimiento de auditoría	Quien la obtiene y evalúa
Información y datos	Recolección y análisis con CAAT	Auditor financiero
Programas y aplicaciones	Revisión de procedimientos y controles	Auditor informático

Figura 2.3

2.4. Entornos informatizados

Según la *Norma técnica de auditoría sobre la auditoría de cuentas en entornos informatizados* del ICAC, una auditoría se lleva a cabo en un entorno informatizado, cuando la entidad, al procesar la información financiera significativa para la auditoría, emplea un ordenador, de cualquier tipo o tamaño, ya sea operado por la propia entidad o por un tercero.

De acuerdo con esta definición, hoy en día, prácticamente cualquier entidad pública opera en un entorno informatizado.

Cuando se efectúa una auditoría en una entidad que opera en un entorno informatizado, el auditor debe evaluar la manera en que el entorno informatizado afecta a la auditoría. Obviamente, afectará de forma diferente según el grado de complejidad de ese entorno.

El objetivo global y el alcance de la auditoría no cambian en un entorno informatizado. Sin embargo, el uso de un ordenador incide en el procesamiento, almacenamiento y comunicación de la información financiera y afecta a los sistemas contable y de control interno empleados por la entidad. En consecuencia, desde el punto de vista del auditor, un entorno informatizado afectará de forma importante a:

- Los procedimientos seguidos por el auditor en el conocimiento y evaluación de los sistemas de control interno de la entidad auditada.
- El análisis del riesgo inherente y de control.
- El diseño y aplicación por el auditor de las pruebas de cumplimiento y de los procedimientos sustantivos adecuados para alcanzar los objetivos de la auditoría.

El auditor puede utilizar tanto procedimientos manuales como técnicas de auditoría asistidas por ordenador o bien una combinación de ambos métodos, al objeto de obtener dicha evidencia. Sin embargo, en algunos sistemas contables que utilizan un ordenador para llevar a cabo aplicaciones significativas, puede ser difícil o imposible que el auditor obtenga ciertos datos sin apoyo informático.

De acuerdo con la citada norma técnica del ICAC el auditor debe tener en cuenta el entorno informatizado en el diseño de los procedimientos de auditoría necesarios para reducir el riesgo de auditoría a un nivel aceptable.

Los auditores deberán tener evidencia suficiente y adecuada de que los datos provenientes de sistemas informáticos sean válidos y fiables cuando tales informaciones sean significativas para los resultados de la auditoría.

Aunque deben efectuarse en todo caso pruebas sustantivas para verificar transacciones y saldos de importe significativo, en determinadas situaciones (básicamente, cuando una significativa cantidad de información es iniciada, registrada, procesada y reportado informáticamente), no será posible reducir el riesgo de detección a un nivel aceptable, realizando únicamente pruebas sustantivas.[27] En estas circunstancias el auditor probará los controles informatizados para obtener evidencia de auditoría sobre la eficacia del diseño y del funcionamiento de los controles para reducir el riesgo de auditoría a un nivel aceptablemente bajo.

La decisión para adoptar un determinado enfoque de auditoría no dependerá tanto del tamaño de la entidad auditada como del grado de complejidad del entorno informatizado.

27. Véase página 509 del *Federal Information System Controls Audit Manual* (FISCAM), que se manifiesta en el mismo sentido que la ISA ·330.

2.5. Normas técnicas de auditoría en entornos informatizados

2.5.1. Principios y Normas de Auditoría del Sector Público de los OCEX

Los Principios y Normas de Auditoría del Sector Público (PNASP) de los OCEX, aparte de los principios generales, no contemplan aspectos específicos relacionados con la problemática de auditoría derivada de la evidencia digital o de los sistemas informatizados.

No obstante, tal como se señala en la exposición de motivos de los PNASP «en todo lo no regulado en las presentes normas y en sus desarrollos posteriores, se aplicarán los principios y normas de auditoría generalmente aceptados a nivel nacional e internacional, y especialmente las normas técnicas del Instituto de Contabilidad y Auditoría de Cuentas». De acuerdo con ello, la Norma Técnica de Auditoría del ICAC tienen carácter supletorio.

2.5.2. Normas técnicas de auditoría del ICAC

La Norma técnica de auditoría sobre la auditoría de cuentas en entornos informatizados, publicada en el BOICAC n.º 54 de junio de 2003, introdujo en las normas españolas el concepto de entorno informatizado y regula diversos aspectos relacionados con la auditoría realizada en ese tipo de entornos.

La norma del ICAC es muy similar a la, ya derogada, Norma Internacional de Auditoría (ISA) 401, que ha sido sustituida por las ISA 315 y 330, en las que se refuerzan los principios básicos de aquélla (evaluación de riesgos y diseño de procedimientos efectivos para contrarrestarlos).

2.5.3. Normas de Auditoría del Sector Público de la Intervención General de la Administración del Estado

Tal como se ha comentado en el capítulo 2.3 las Normas de Auditoria del Sector Público de la IGAE aprobadas en 1997 tratan con cierto detalle el efecto en el trabajo del auditor de las consideraciones relativas a la evidencia informática y otros aspectos relacionados.

Además la Circular 2/2009, de 16 de septiembre, de la Intervención General de la Admnistración del Estado, sobre auditoría pública, en su instrucción 12ª.2.e) establece que en la aplicación de los procedimientos de auditoría se podrá «verificar la seguridad de los sistemas informáticos que soportan la información económico-financiera y contable».

2.5.4. Normas Internacionales de Auditoría y Normas INTOSAI

Las Normas Internacionales de Auditoría 315 y 330 han sido adoptadas por INTOSAI, al ser incluidas en las INTOSAI Financial Audit Guidlines y aprobadas como International Standards of Supreme Audit Institutions (ISSAI)[28] 1315 y 1330 en el XIX INCOSAI celebrado en noviembre 2007:

- ISSAI 1315 Directriz de auditoría financiera: Identificación y evaluación de los riesgos de irregularidades importantes a través de una comprensión de la entidad y su entorno.
- ISSAI 1330 Directriz de auditoría financiera: Las respuestas del auditor a los riesgos evaluados.

2.5.5. The Institute of Internal Auditors: Global Technology Audit Guides (GTAG)

Las guías GTAG han sido elaboradas por The Institute of Internal Auditors; esta serie de guías ha sido creada para proporcionar información de alto nivel sobre aspectos tecnológicos desde un punto de vista no demasiado técnico, de forma que puedan ayudar a los auditores internos (principales destinatarios de las guías) y externos a comprender mejor los diferentes riesgos, los controles y los temas del buen gobierno relacionados con aspectos tecnológicos.

Cada guía sirve como fuente de recursos para auditores e informáticos en distintos aspectos relacionados con los riesgos de las tecnologías de la información y las mejores prácticas aplicables. Las guías emitidas hasta el momento son:

GTAG 12: Auditing IT Projects
GTAG 11: Developing the IT Audit Plan
GTAG 10: Business Continuity Management
GTAG 9: Identity and Access Management
GTAG 8: Auditing Application Controls
GTAG 7: IT Outsourcing
GTAG 6: Managing and Auditing IT Vulnerabilities
GTAG 5: Managing and Auditing Privacy Risks
GTAG 4: Management of IT Auditing
GTAG 3: Continuous Auditing
GTAG 2: Change and Patch Management Controls
GTAG 1: Information Technology Controls

28. Pueden consultarse las ISSAI en la página web: www.issai.org

2.5.6. The Institute of Internal Auditors: los principios y la metodología GAIT

The Institute of Internal Auditors ha desarrollado y publicado un conjunto de principios y metodología, conocidos como *Guide to the Assessment of IT General Controls Scope Based on Risk* (GAIT), que pueden utilizarse para facilitar la tarea de revisión y evaluación de los controles generales TI.

Aunque es una metodología diseñada en principio para el auditor interno, es de utilidad para cualquier auditor financiero y de sistemas de información.

Esta metodología se focaliza en definir un alcance para la revisión y evaluación de los controles TI que sea eficiente, ayudando a identificar controles generales TI clave, dentro de un enfoque de arriba hacia abajo basado en el análisis de los riesgos como el descrito en el capítulo 4.1 y desarrollado en todo el apartado 5.

Los principios y la metodología GAIT son compatibles con CobiT facilitando su aplicación.

Principios GAIT

Los cuatro principios GAIT son:[29]

– *Principio 1*

La identificación de riesgos y controles generales TI será la continuación del enfoque de arriba hacia abajo basado en el análisis de riesgos utilizado para identificar cuentas significativas, los riesgos de estas cuentas y los controles clave en los procesos de negocio.

– *Principio 2*

Los riesgos y controles generales TI que deben ser identificados son los que afectan a la funcionalidad TI que sea crítica en las aplicaciones financieras significativas y los datos relacionados.

– *Principio 3*

Los riesgos y controles generales TI que deben identificarse existen en los procesos y en varios niveles TI: aplicaciones, bases de datos, sistemas operativos y redes.

– *Principio 4*

Los riesgos en los procesos TI de control son mitigados mediante el cumplimiento de los objetivos de control TI.

29. *The GAIT Principles*, The IIA, enero 2007.

La metodología GAIT[30]

Además de los cuatro principios se creó la metodología que permitiera implementarlos. Esta metodología da a los gestores y a los auditores una guía sobre el alcance de la revisión de los controles generales TI.

La metodología ayuda a examinar cada aplicación significativa para la información financiera y a determinar si fallos en los controles generales TI en cada nivel de la infraestructura TI representa una amenaza probable para las funcionalidades críticas de la aplicación. Si un fallo es probable, GAIT identifica los riesgos en detalle y los objetivos de los controles generales TI que si se alcanzan, mitigan esos riesgos.

2.5.7. Normas de Auditoría de Sistemas de Información de ISACA

Information Systems Audit and Control Association (ISACA) es una asociación reconocida mundialmente, dedicada al desarrollo de los conocimientos relacionados con la seguridad y auditoría de los sistemas de información, el gobierno TI de la empresa, los riesgos relacionados con las TI y el cumplimiento. Fundada en 1969, ISACA desarrolla estándares internacionales de auditoría y normas de control.

ISACA aprobó las Normas de Auditoría de Sistemas de Información, de aplicación obligatoria para los auditores de sistemas de información con la certificación CISA (Certified Information Sistems Auditor) que gestiona y concede la propia asociación ISACA. Estas normas son:

S1 Estatuto de auditoría

S2 Independencia

S3 Etica y normas profesionales

S4 Competencia profesional

S5 Planeación

S6 Realización labores de auditoría

S7 Reporte

S8 Actividades de seguimiento

S9 Irregularidades y acciones ilegales

S10 Gobernabilidad de TI

S11 Evaluación de riesgos en la planeación

30. *The GAIT Methodology*, The IIA, enero 2007.

S12 Materialidad

S13 Uso de otros expertos

S14 Evidencia de auditoría

2.5.8. COBIT

CobiT (Control Objectives for Information and Related Technology) es un marco conceptual para el buen gobierno de las tecnologías de la información, que fue desarrollado originalmente en 1994 por ISACA. La versión 4.1 de CobiT fue publicada en 2005 por el IT Governance Institute (ITGI).

CobiT es una referencia de control interno sobre procesos informáticos internacionalmente aceptada. Se utiliza como metodología para definir y monitorizar el control interno relacionado con los sistemas de información de las entidades y también como metodología de auditoría.

Define procesos relacionados con la función informática así como los elementos de control, buenas prácticas, gestión y auditores.

Desde un punto de vista práctico, tiene que ser «adaptado» en función del tamaño y la misión de la organización. El Tribunal de Cuentas Europeo ha desarrollado para aplicar esta metodología la herramienta **ECACOBIT**, que se comentará más adelante.

El marco de trabajo general CobiT se muestra gráficamente en la figura siguiente, con el modelo de procesos de CobiT compuesto de cuatro dominios que contienen 34 procesos genéricos, administrando los recursos de TI para proporcionar información al negocio de acuerdo con los requerimientos del negocio y de gobierno.

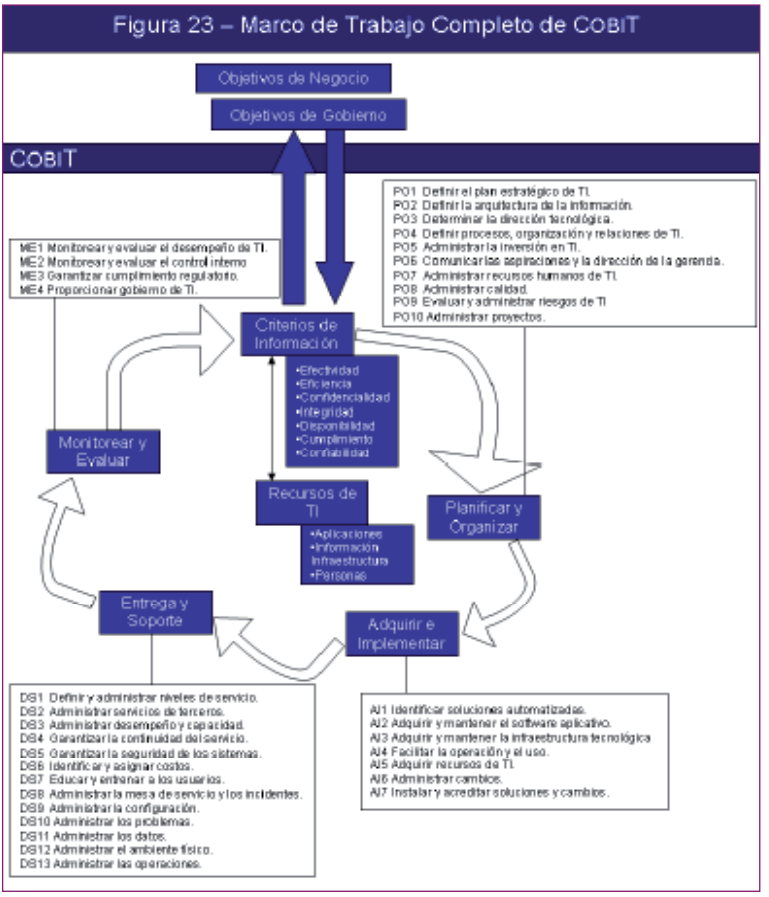


Figura 2.4. Marco de trabajo de CobiT

2.6. Perfil formativo del auditor

2.6.1. Conocimientos técnicos exigibles al auditor

El apartado 3 de la Norma técnica del ICAC de auditoría en entornos informatizados, establece que el auditor debe tener el conocimiento suficiente de los sistemas informáticos que le permita planificar, dirigir, supervisar y revisar el trabajo realizado.

Dada la complejidad creciente de los sistemas informáticos, en cada trabajo, el auditor debe evaluar si son necesarios para la auditoría conocimientos especializados sobre esta materia, que permitan:

– Obtener un conocimiento suficiente de los sistemas contable y de control interno afectados por el entorno informatizado.

– Determinar el efecto del entorno informatizado en la evaluación del riesgo global y del riesgo a nivel de saldos y de tipos de transacciones.
– Diseñar y aplicar las adecuadas pruebas de cumplimiento y procedimientos sustantivos.

Si el auditor considera que sí se requieren conocimientos especializados, deberá obtener el apoyo de un profesional que los posea, bien de su organización, bien ajeno a la misma.

En el caso de utilizar la ayuda de profesionales externos especializados, se deberá tener en cuenta el contenido de la Norma Técnica de Auditoría sobre la utilización de expertos independientes.

Además de la colaboración de expertos que se considere necesaria, el auditor responsable de la auditoría financiera debe tener los conocimientos suficientes que le permitan comunicar los objetivos del trabajo a los auditores informáticos, evaluar si los procedimientos específicos de revisión de controles están alineados con los objetivos generales de la auditoría, y evaluar los resultados obtenidos.[31]

2.6.2. Formación mínima del auditor financiero

a) IFCA

Según la International Education Guideline n.º 11 de la IFAC *Information Technology for professional accountants*, un auditor debe tener un conocimiento razonable de las principales técnicas de auditoría asistida por ordenador, sus ventajas, requisitos y limitaciones y debe ser capaz de usar al menos un programa de análisis y extracción de datos (como ACL o IDEA) y un programa de gestión de papeles de trabajo electrónicos (como TeamMate, Autoaudit, Pantana o Caseware Working Papers). Además de manejar internet, el correo electrónico, agenda electrónica y, por supuesto, hoja electrónica y tratamiento de textos.

b) Perfiles establecidos por el *The Institute of Internal Auditors (The IIA)*

En la Global Technology Audit Guide n.º 1: *Information Technology Controls* se incluye un anexo sobre «Las tres categorías de conocimientos TI para los auditores internos» identificadas por el Comité Internacional de Tecnología Avanzada del IIA, donde se dan

31. FISCAM, página 502.

las orientaciones que se comentan a continuación. Estas orientaciones son igualmente válidas para los auditores externos sean públicos o privados.

En dicha guía se señala que se necesitan diversos niveles de conocimientos sobre las tecnologías de la información y las comunicaciones a través de toda la organización auditora para proporcionar un enfoque sistemático, para evaluar y mejorar la efectividad de los procesos sobre la gestión de riesgos, los controles y del gobierno. El conocimiento de cómo se utilizan las tecnologías de la información y las comunicaciones, los riesgos relacionados, y la capacidad de utilizar las tecnologías de la información y las comunicaciones como un recurso en el desarrollo del trabajo de auditoría es esencial para la eficacia del auditor en todos los niveles.

Categoría 1 - Todos los auditores

La Categoría 1 es el conocimiento de tecnologías de la información necesario para todos los auditores profesionales, desde las nuevas incorporaciones hasta el Director de Auditoría.

El conocimiento de tecnologías de la información abarca el entender conceptos, tales como las diferencias en el software usado en aplicaciones, sistemas operativos y software de sistemas y redes. Esto implica entender los componentes básicos de seguridad de tecnologías de la información y de control, tales como seguridad perimetral, detección de intrusismo, autenticación, y controles de los sistemas de aplicación.

El conocimiento básico incluye entender cómo los controles de negocio y los objetivos de auditoría pueden verse afectados por vulnerabilidades en las operaciones de negocio y lo relacionado con los sistemas de soporte, y los componentes de redes y datos.

Es fundamental asegurar que los auditores tengan suficiente conocimiento para centrarse en la comprensión de los riesgos de tecnologías de la información, sin necesariamente tener conocimientos técnicos significativos.

Categoría 2 – Supervisores de auditoría

La categoría 2 se aplica al nivel de supervisión de auditoría (responsables técnicos de las auditorías). Además del conocimiento básico en tecnologías de la información, los supervisores deben entender los aspectos y elementos de tecnologías de la información, de forma suficiente para considerarlos en las tares de planificación, pruebas, análisis, informe y seguimiento, y en la asignación de tareas a los miembros del equipo.

Esencialmente, el supervisor de auditoría debe:

- Entender las amenazas y vulnerabilidades asociadas a procesos automatizados de negocio.
- Entender los controles de negocio y la mitigación del riesgo que deben de proporcionar las tecnologías de la información.
- Planificar y supervisar las tareas de auditoría para considerar las vulnerabilidades y los controles relacionados con las tecnologías de la información, así como la eficacia de las tecnologías de la información en la provisión de controles para las aplicaciones y entornos de negocio.
- Asegurar que el equipo de auditoría tiene competencia suficiente –incluyendo las habilidades en tecnologías de la información- para las tareas de auditoría.
- Asegurar el uso eficaz de CAAT en los trabajos de auditoría.
- Aprobar los planes y las técnicas para probar controles y realizar pruebas sustantivas.
- Evaluar los resultados de las pruebas de auditoría para evidenciar las vulnerabilidades o debilidades de control de tecnologías de la información.
- Analizar los síntomas detectados y relacionarlos con causas que pueden tener sus orígenes en el negocio o en tecnologías de la información: planificación, ejecución, operaciones, gestión de cambios, autenticación, u otras áreas del riesgo.
- Proporcionar recomendaciones de auditoría basadas en los objetivos del aseguramiento del negocio, centrándose en los orígenes de los problemas observados, más que divulgar simplemente los problemas o los errores detectados.

Categoría 3 - Especialista en auditoría informática

La categoría 3 se aplica al especialista en auditoría informática. Los auditores informáticos deben entender las tecnologías subyacentes que soportan componentes del negocio y estar familiarizados con las amenazas y las vulnerabilidades asociadas con las TI.

c) Conocimientos recomendados

Así, de acuerdo con lo establecido en las normas técnicas citadas, los órganos públicos de auditoría deben considerar la necesidad de formación para todos los niveles sobre los conceptos relacionados

con la auditoría en entornos informatizados, que debe incluir los siguientes aspectos:

- Normas técnicas de auditoría relacionadas.
- Características de los entornos informatizados.
- Profundización en la evaluación de los controles internos en entornos informatizados, distinción entre controles generales y controles de aplicación, su efecto en el riesgo de auditoría y en los procedimientos de auditoría aplicables.
- La evidencia informática.
- Introducción a los sistemas ERP y análisis de su impacto en los procedimientos de auditoría.
- Introducción y aplicaciones prácticas de herramientas de análisis y extracción de datos (CAAT).
- Utilización de papeles de trabajo electrónicos.
- Conceptos básicos sobre la auditoría de los sistemas de información.

3

Sistemas de información y control interno

3.1. Sistemas de información avanzados

3.1.1. Concepto de sistema de información

Un sistema de información está integrado por la infraestructura (componente físico y de hardware), personal, procedimientos (incluido el software en entornos informatizados) y datos.

Un sistema de información significativo para los objetivos de la información financiera, consiste en los procedimientos, documentos y registros establecidos para iniciar, registrar, procesar y reportar las transacciones de la entidad (así como los hechos y condiciones) y mantener un control responsable de los activos, pasivos y fondos propios, según se detalla a continuación:

- Las transacciones pueden ser introducidas o iniciadas en el sistema bien manualmente o de forma automática mediante procedimientos programados.
- El registro incluye la identificación y captura de la información relevante de las transacciones, hechos o condiciones.
- El procesamiento incluye funciones tales como anotar, validar, calcular, medir, valorar, resumir y conciliar, realizadas tanto mediante procedimientos manuales como automatizados.
- El reporte se relaciona con la preparación de la información financiera o presupuestaria, así como otra información, en formato impreso o electrónico, que la entidad usa para medir y revisar su actuación financiera, presupuestaria y otras funciones, y para la elaboración de las cuentas anuales.
- La calidad de la información generada por el sistema afecta a la capacidad, la dirección para tomar las decisiones apropiadas y la gestión y control de las actividades de la entidad y la preparación de las cuentas anuales.

En consecuencia, un sistema de información financiera y presupuestaria conlleva métodos y registros que:

- Identifican todas las transacciones válidas.

- Describe las transacciones con suficiente detalle para permitir la apropiada clasificación de las mismas a efectos de información financiera y presupuestaria.
- Valoran las transacciones de manera que permite registrar el importe monetario apropiado en los estados financieros y presupuestarios.
- Determina cuando las transacciones han tenido lugar para permitir su registro en el periodo contable apropiado.
- Procesa la información.
- Presenta apropiadamente las transacciones y revelaciones adecuadas en las cuentas anuales.

Un sistema de información debe estar convenientemente descrito; la descripción deberá incluir:

- Los tipos o clases de transacciones significativos para los estados financieros y presupuestarios de la entidad.
- Para cada tipo significativo de transacción, los procedimientos, tanto manuales como informatizados, de inicio, registro, proceso y reporte en los estados financieros y presupuestarios.
- La forma en la que los sistemas de información recogen tanto las transacciones como los hechos y condiciones que no son puramente las transacciones.
- Los registros contables correspondientes, tanto electrónicos como manuales, que soportan la información y las cuentas específicas de los estados financieros y presupuestarios en las que se inician, registran, procesan y reportan.
- El proceso utilizado de formulación de las cuentas anuales, incluida la correspondiente información en la memoria.

Si bien lo ideal es que todo sistema de información financiera y presupuestaria esté formalizado mediante políticas y procedimientos escritos y mediante un apropiado sistema de comunicación que identifique las funciones y responsabilidades individuales relativas al control interno de la información financiera y presupuestaria, en las pequeñas empresas o entidades, no se requiere necesariamente una descripción detallada de los procedimientos contables, registros o políticas escritas, especialmente cuando existe una involucración activa de la dirección. En estos casos la comunicación puede ser más informal y fácil de realizar, debido al pequeño tamaño de la entidad, la reducción del personal y mayor acceso y disponibilidad de la dirección.

3.1.2. Sistemas de información complejos

Un componente, importante de los sistemas de información, son los sistemas informáticos (hardware y software) relacionados con el procesamiento, almacenamiento, transmisión y emisión de la información financiera, que condicionan en buena medida el diseño y configuración de aquéllos.

Cuando se vayan a auditar entidades que tengan instalado un sistema de información complejo, como un ERP, es básico que el auditor financiero, sin perjuicio de la intervención de un auditor de sistemas de información, conozca los fundamentos de la arquitectura de dichos sistemas.

Aunque más adelante, en el capítulo 7, se analizan en profundidad estos sistemas, a modo de introducción consideraremos, en un modelo simplificado, que el sistema de información de una entidad consta de cinco niveles superpuestos (en la realidad las interacciones serán más complejas).

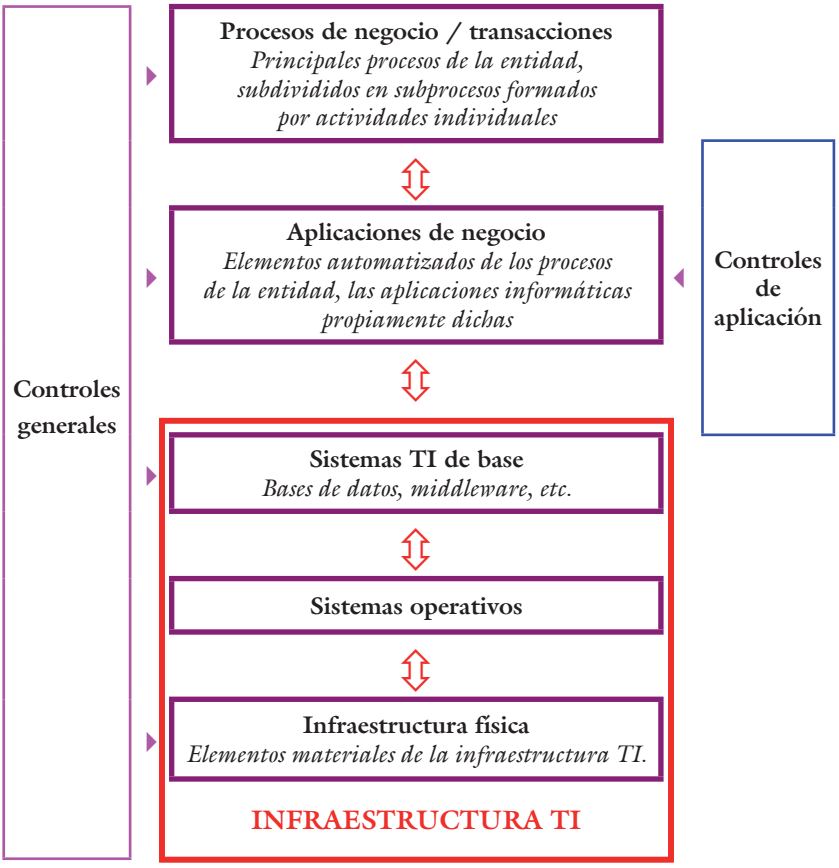


Figura 3.1

El enfoque de auditoría basado en el análisis de los riesgos, incluye la revisión del sistema de control interno embebido en los sistemas de información. Para ello se deberá partir de la consideración de esta estructura esquemática, que con configuraciones distintas según la empresa, fundación, ayuntamiento o entidad de cualquier tipo, su tamaño, actividad, estructura de hardware, software adoptado, complejidad, etc., se mantiene en lo esencial invariable.

Nos encontraremos con un sistema compuesto de varias capas o niveles que se superponen y en todas ellas se pueden producir determinados riesgos que deben ser considerados en nuestro análisis, tal como veremos más adelante. Estas capas son:

1. La primera capa está formada por la infraestructura física

   Contiene básicamente los elementos materiales, el hardware: mainframe, sistemas periféricos, servidores, sistemas de comunicaciones, pc, etc.

2. Sobre la capa anterior, para hacer que funcionen los elementos físicos y el resto del software, se ubican los sistemas operativos (SO)

   Los principales SO utilizados en entidades medianas y grandes son: UNIX-Linux (en sus distintas versiones), MS Windows Server (también con varias versiones) y Windows XP-Vista en las estaciones de trabajo.

3. La siguiente capa, que funciona sobre los SO, la llamaremos sistemas TI de base

   Este término recoge una gran diversidad de plataformas posibles soportando las aplicaciones del siguiente nivel.

   Se incluyen en este nivel los sistemas de gestión de bases de datos – SGBD (los más utilizados son Oracle Database, DB2, MS-SQL Server), componentes de base de aplicaciones integradas y sistemas más técnicos como el middleware (SAP Basis, NetWeaver, Oracle Fusion, IBM WebSphere), que permite integrar muy diversas aplicaciones y sistemas.

4. Aplicaciones de negocio o aplicaciones de gestión

   Este nivel contiene los elementos automatizados de los procesos de la entidad, las aplicaciones informáticas propiamente dichas que soportan los procesos de negocio y las principales líneas de actividad de la entidad

   Aquí pueden encontrase muchas aplicaciones disponibles en el mercado, las más habituales están basadas en Oracle E-Business Suite, SAP R/3, SAP ERP 6.0 o Microsoft Dynamics.

Todas ellas tanto en una configuración estándar, como muy adaptada o como desarrollo propio, funcionan sobre los SGBD y componentes de base incluidos en la capa precedente.

5. Procesos de negocio o procesos de gestión

   Principales procesos de la entidad, presentados por áreas de actividad y subdivididos en subprocesos y en actividades individuales. Están soportados por las aplicaciones informáticas del nivel anterior.

Como se desprende de la esquemática y breve explicación de la estructura de un sistema de información, las distintas capas o niveles están interrelacionados, y los riesgos y debilidades en una de ellas pueden afectar al conjunto del sistema y consecuentemente tener impacto en las cuentas anuales, que son el reflejo de la actividad económico y financiera de una entidad durante un ejercicio económico.

Para minimizar esos riesgos el auditor debe analizar a fondo el conjunto del sistema de información con una metodología adecuada, como la que se propone en el presente trabajo

De una forma más gráfica, aunque sustancialmente similar, al esquema representado en la figura 3.1, en la publicación *Guidelines on how to integrate IT AUDIT within the audit process-ECACIT* del Tribunal de Cuentas Europeo[32] se representa así un sistema de información:

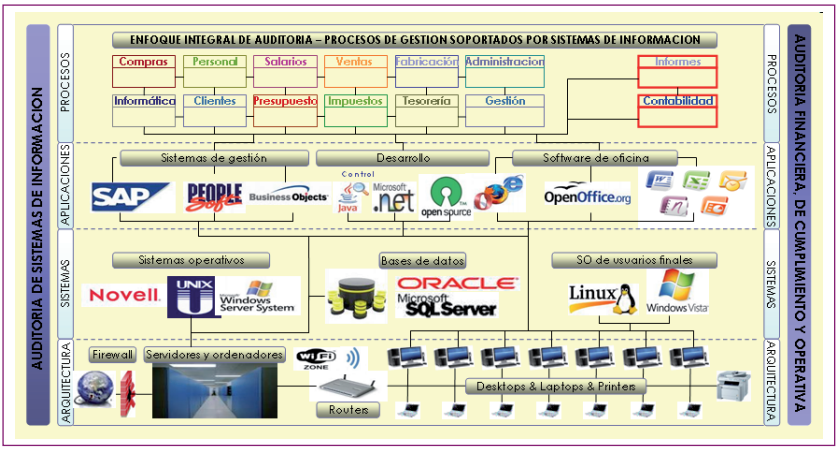


Figura 3.2

32. *Guidelines on how to integrate IT AUDIT within the audit process-ECACIT*, Tribunal de Cuentas Europeo. Versión en español de Ignacio Calleja Ruiz, Auditor informático del Tribunal de Cuentas Europeo presentada en el Seminario de Maspalomas, julio de 2007, en *Fiscalización en un entorno de @-Administración.*

3.2. El control interno

Definiciones y conceptos básicos.

Según las *Directrices de la INTOSAI para la Buena Governanza*:[33]

«El control interno es un proceso integral efectuado por la gerencia y el personal, y está diseñado para enfrentarse a los riesgos y para dar una seguridad razonable de que en la consecución de la misión de la entidad, se alcanzarán los siguientes objetivos gerenciales:

- Ejecución ordenada, ética, económica, eficiente y efectiva de las operaciones
- Cumplimiento de las obligaciones de responsabilidad
- Cumplimiento de las leyes y regulaciones aplicables
- Salvaguarda de los recursos para evitar pérdidas, mal uso y daño.»

El control interno no es un hecho o circunstancia, sino una serie de acciones que están relacionadas con las actividades de la entidad, y que se dan en todas las operaciones de la entidad continuamente. Estas acciones son inherentes a la manera en la que la gerencia administra la organización. El control interno por lo tanto es diferente a la perspectiva que tienen algunos de él, quienes lo ven como un hecho adicionado a las actividades de la entidad, o como una obligación.

El control interno comprende el plan de organización y el conjunto de métodos y procedimientos que aseguren que

- los activos están debidamente protegidos,
- los registros contables son fidedignos,
- la actividad de la entidad se desarrolla eficazmente,
- los procedimientos se cumplen según las directrices marcadas por la Dirección.

El control interno debe ser incorporado a las actividades de la entidad y es más efectivo cuando se lo construye dentro de la estructura organizativa de la entidad y es parte integral de la esencia de la organización.

La implantación y mantenimiento de un sistema de control interno es responsabilidad de la Dirección (y en última instancia de los administradores o de los máximos responsables políticos de una entidad), que debe someterlo a una continua supervisión para de-

33. *Guía para las normas de control interno del sector público (INTOSAI GOV 9100)*, aprobada por el XVIII INCOSAI en 2004.

terminar que funciona según está prescrito, modificándolo si fuera preciso, de acuerdo con las circunstancias.

El ambiente de control y el compromiso con comportamientos éticos es una filosofía de trabajo que debe emanar de arriba hacia abajo, desde los altos puestos directivos hacia el resto de la organización. Es esencial que el tono adecuado de control sea marcado por los máximos responsables de la entidad (*Tone at the top*),[34] que se envíe un mensaje a toda la organización de que los controles deben ser tomados en serio.[35]

Por definición, el control interno confiere una seguridad razonable, pero no absoluta de que los objetivos del mismo se cumplirán.

Todo sistema de control interno tiene unas limitaciones.

Siempre existe la posibilidad de que al aplicar procedimientos de control surjan errores por una mala comprensión de las instrucciones, errores de juicio, falta de atención personal, fallo humano, etc.

Además, aquellos procedimientos cuya eficacia se basa en la segregación de funciones podrían eludirse como consecuencia de existir colusión de los empleados implicados en el control interno.

Igualmente, los procedimientos basados en el objetivo de asegurar que las transacciones se ejecutan según los términos autorizados por la Dirección, resultarían ineficaces si las decisiones de ésta se tomaran de una forma errónea o irregular.

34. El *Tone at the top* es una expresión anglosajona que no tiene su equivalente en español, pero expresa una filosofía y puede ser considerado (*Tone at the Top and Audit Quality*, IFAC, 2007, página 8) como el estándar establecido por los líderes de una organización según el cual se mide su rendimiento, la cultura con la cual los miembros de la organización operan, el tono establecido por la alta dirección, con independencia de la documentación de la gestión estratégica y políticas, es la fuerza que impulsa a los profesionales individuales, la mano invisible que dirige las actividades sin importar la proximidad de la dirección a la acción, y un compromiso con la calidad en la atención que reciben los clientes y usuarios. Aunque el compromiso de calidad sea descrito en la estrategia de la organización, comunicaciones, descripciones de puestos, proceso de evaluación de desempeño, etc., a menos que el mensaje se transforme en una forma de vida en la organización, donde la dirección realmente predique con el ejemplo, la probabilidad de logro de los objetivos organizacionales podría ser sustancialmente disminuida.

Toda organización necesita un sentido de dirección y la dirección es determinada por el liderazgo. Estar en el tono correcto requiere una visión clara de los valores básicos bajo los cuales operar. *Tone at the top* es en última instancia la responsabilidad de los líderes de la organización, liderar desde lo más alto dando un mensaje consistente acerca de la importancia de la calidad. Esta responsabilidad es compartida por todos los niveles de gerencia de la organización, dado que las personas esperan que sus superiores inmediatos les den orientación respecto a ello.

35. KPMG: *Internal Control: A Practical Guide*. Londres, 1999 (página 19).

Los objetivos del sistema de control interno de tipo contable se deben relacionar con cada una de las etapas por las que discurre una transacción.[36]

Las etapas más importantes relativas a una transacción comprenden su autorización, ejecución, registro y la responsabilidad respecto a la custodia y salvaguarda de los activos que, en su caso, resulten de dicha transacción, con el fin de que las mismas hayan sido ejecutadas y que se encuentren clasificadas en las cuentas apropiadas.

En particular, la autorización de las transacciones es una función de la Dirección asociada directamente con su responsabilidad para alcanzar los objetivos.

3.3. Conocimiento del sistema de información y de control interno en una auditoría financiera

El control interno es el proceso diseñado y efectuado por los responsables de la dirección y el personal de la entidad para suministrar una seguridad razonable sobre el cumplimiento de los objetivos de la entidad con relación a la fiabilidad de la información financiera, la efectividad y eficiencia de las operaciones y el cumplimiento con las leyes y normativa aplicables. En consecuencia dicho control interno está diseñado e implantado para responder a los riesgos identificados del negocio que amenazan el cumplimiento de cualquiera de dichos objetivos.[37]

El auditor usa el conocimiento del control interno para identificar los tipos de manifestaciones erróneas potenciales que puedan contener las cuentas anuales, considerar los factores que afectan al riesgo de aquellas que sean significativas y diseñar la naturaleza, fechas de realización y extensión de los correspondientes procedimientos de auditoría.

El auditor tiene que alcanzar una comprensión del sistema de información y de los procesos de negocio relevantes para la información financiera en las siguientes áreas.[38]

- Las clases de transacciones en las operaciones de la entidad que son significativas para las cuentas anuales.
- Los procedimientos, tanto manuales como automatizados, mediante los que las transacciones son iniciadas, registradas, procesadas e integradas en las cuentas anuales.

36. Resolución de 19 de enero de 1991, del ICAC, por la que se aprueba las Normas Técnicas de Auditoría, (párrafo 2.4.9).
37. *Guía de auditoría* del REA, página 11.
38. *Guía de auditoría* del REA, páginas 12 y 13

- Los registros contables relacionados, electrónicos o manuales, que soportan la información, y las cuentas específicas de las cuentas anuales, respecto al inicio, registro, proceso e información de las transacciones.
- Cómo captura el sistema de información acontecimientos y condiciones (hechos contables), además de las transacciones, que son significativos para las cuentas anuales.
- El proceso de información financiera usado para preparar las cuentas anuales, incluidas las estimaciones contables significativas y las revelaciones en la memoria.

En la obtención del conocimiento del proceso de la información financiera, el auditor tendrá que obtener un conocimiento del entorno informatizado y demás procedimientos que una entidad usa para preparar las cuentas anuales y las revelaciones correspondientes y de qué manifestaciones erróneas pueden ocurrir.

Dichos procedimientos, informatizados y manuales, incluyen aquellos usados para:

- La valoración y obtención de la información relativa a las transacciones y hechos económicos para su registro contable.
- Iniciar, registrar y procesar los asientos de diario en el mayor general.
- Mantenimiento del control responsable de los activos, pasivos y fondos propios.
- Integración de la información financiera en las cuentas anuales.

El auditor necesitará entender cómo la entidad comunica las tareas y responsabilidades de la información financiera y asuntos significativos relacionados con la misma. Ello implica el conocimiento por el personal de sus funciones y responsabilidades individuales relativas al sistema de información financiera, de hasta qué medida sus funciones se relacionan con el trabajo de otros y de cómo reportar al nivel apropiado de la dirección las excepciones observadas.

El uso de TI afecta a la forma de implantación de las actividades de control. Por tanto, el auditor debe obtener un conocimiento de cómo la entidad responde a los riesgos de TI y debe considerar si la entidad ha reaccionado adecuadamente a los riesgos derivados de TI estableciendo controles efectivos de TI, generales y de aplicación.

Desde la perspectiva del auditor financiero, los controles sobre los sistemas TI son efectivos cuando mantienen la integridad de la información y la seguridad de los datos que dichos sistemas procesan.

Evaluación del sistema de control interno.

De acuerdo con la segunda norma sobre Ejecución del Trabajo de las Normas Técnicas de Auditoría del ICAC «deberá efectuarse un estudio y evaluación adecuada del control interno como base fiable para la determinación del alcance, naturaleza y momento de realización de las pruebas a las que deberán concretarse los procedimientos de auditoría».

El apartado 2.4.10 de la misma norma dice: «El estudio y evaluación del control interno incluye dos fases:

a) La revisión preliminar del sistema con objeto de conocer y comprender los procedimientos y métodos establecidos por la entidad. En particular, el conocimiento y evaluación preliminar de los sistemas de control interno de la entidad, incluyendo los sistemas informáticos, constituye un requisito mínimo de trabajo que sirve de base a la planificación de la auditoría.

b) La realización de pruebas de cumplimiento para obtener una seguridad razonable de que los controles se encuentran en uso y que están operando tal como se diseñaron.»

Una función de control interno, desde el punto de vista del auditor externo, es la de suministrar seguridad de que los errores e irregularidades se pueden descubrir con prontitud razonable, asegurando así la fiabilidad e integridad de los registros contables.

La revisión del control interno por parte del auditor independiente le ayuda a determinar otros procedimientos de auditoría apropiados para formular una opinión sobre la razonabilidad de las cuentas anuales.

La evaluación de los controles internos contables hecha por el auditor para cada tipo significativo de transacciones, debe dar lugar a una conclusión respecto a si los procedimientos establecidos y su cumplimiento son satisfactorios para su objetivo.

Los procedimientos y su cumplimiento deben considerarse satisfactorios si la revisión del auditor y sus pruebas no revelan ninguna situación que se considere como una deficiencia importante para su objetivo.

3.4. El riesgo de auditoría

3.4.1. Concepto

El riesgo de auditoría es la evaluación hecha por el auditor del riesgo de que las cuentas anuales contengan un error o irregularidad

significativa no detectada una vez que la auditoría ha sido completada. Es inevitable que exista algún grado de riesgo de auditoría.

Puede controlarse en gran medida el riesgo de auditoría variando la naturaleza y alcance de los procedimientos de auditoría. Al hacerlo, debe tenerse en cuenta que no es apropiado realizar trabajo adicional para obtener mayor satisfacción de auditoría de la que sea:

a) posible, debido a la subjetividad inherente de las cuentas anuales o

b) justificada, si el costo de una mayor satisfacción de auditoría excede el valor para los usuarios de las cuentas anuales.

Debe reconocerse también que un mayor trabajo de auditoría no siempre reduce el riesgo de un error o irregularidad significativa a un nivel adecuadamente bajo; por ejemplo, cuando surgen dudas acerca de la integridad de la gerencia o cuando hay insuficiente evidencia disponible sobre un hecho que implica un muy alto grado de subjetividad. En estos casos, sería conveniente considerar una salvedad en el informe de auditoría.

El tamaño o naturaleza de lo que es considerado importante debe ser evaluado en base a la percepción de las necesidades o del probable efecto para una persona razonable que utiliza las cuentas anuales. El riesgo se define en términos de errores o irregularidades significativas. Por consiguiente, una evaluación del riesgo sólo puede hacerse después y dentro del contexto de la evaluación de la materialidad para las cuentas anuales en su conjunto.

3.4.2. Componentes del riesgo de auditoría

El riesgo final del auditor es una combinación de tres riesgos diferentes:

a) Riesgo inherente

El riesgo inherente es la posibilidad inherente a la actividad de la entidad de que existan errores o irregularidades significativas en el proceso contable, del cual se obtienen las cuentas anuales, antes de considerar la efectividad de los sistemas de control.

Este riesgo varía entre los componentes. Por ejemplo, áreas como la de existencias/costes, que incluyen cálculos complicados, tienen más posibilidades de ser mal expresadas que las que contienen cálculos sencillos; el efectivo y los títulos al portador son más susceptibles de pérdida o manipulación que las acciones nominativas; las áreas que resultan de criterios gerenciales subjetivos tales como el deterioro de

las existencias o de las cuentas a cobrar generalmente son de mayor riesgo que las que resultan de determinaciones más objetivas.

Cuando el riesgo inherente es bajo o insignificante, el riesgo de control y el riesgo de detección asumen menor importancia en la planificación y ejecución de la auditoría.

Algunos de los factores importantes para la evaluación del riesgo inherente son:

- Naturaleza del negocio o actividad de la entidad auditada

  Naturaleza de los productos y servicios, incluyendo su facilidad de comercialización, volatilidad y susceptibilidad a desfalcos; naturaleza de la industria, circunstancias económicas y tendencias de negocios; políticas y prácticas financieras; estructura operativa y departamentos administrativos. Situación de equilibrio o desequilibrio presupuestario.

- Naturaleza de los componentes de las cuentas anuales

  La naturaleza de las transacciones y actividades de la entidad; subjetividad o complejidad de su contabilización; significatividad de los importes o saldos para las cuentas anuales en su conjunto; homogeneidad de los importes de las transacciones; transacciones entre empresas vinculadas; susceptibilidad a problemas de realización de transacciones no registradas o errores de corte y a la manipulación u otras irregularidades.

- Naturaleza de los sistemas contables y de información

  Diseño y efectividad de los sistemas; desarrollados por el cliente o por terceros; capacidad de manejar diferentes niveles de actividad; dependencia de los sistemas para el manejo diario del negocio; naturaleza, alcance y complejidad de los sistemas informáticos, de las aplicaciones significativas; efecto de la configuración del software, hardware y de la transmisión de datos sobre el riesgo relacionado con:

  — accesos de los usuarios (tanto de la entidad como terceros) a las funciones de procesamiento y archivo de datos
  — precisión e integridad de los datos registrados para su procesamiento
  — manejo adecuado de las transacciones rechazadas
  — precisión e integridad del procesamiento de las transacciones y de la información directamente relacionada, incluyendo las transacciones generadas por el sistema
  — operaciones del departamento informático

— cambios en los programas de aplicaciones
— acceso general a las funciones de procesamiento, archivos de datos y programas.

Una evaluación del riesgo inherente para un componente podría implicar la consideración por separado de los riesgos de diferentes manifestaciones que probablemente no tengan los mismos riesgos inherentes. Cada manifestación puede ser influida por diferentes aplicaciones informáticas, ser dependiente en varios grados del criterio de la gerencia o estar afectada por otros factores.

Es posible que en la práctica, las diferencias de riesgo entre las manifestaciones no afecten significativamente al enfoque de auditoría y, consecuentemente, sería suficiente realizar una evaluación global del riesgo inherente para el componente. No obstante, no debe ignorarse el hecho de que los riesgos inherentes pueden diferir en naturaleza y grado para cada componente, como, por ejemplo, entre recuentos o registros erróneos de existencias físicas, valoración incorrecta por deterioro o corte de operaciones erróneo.

b) Riesgo de control

El riesgo de control es el riesgo de que los sistemas de control no puedan evitar o detectar y corregir errores o irregularidades significativas en forma oportuna. Para ser efectivo, un sistema de control debe ocuparse de los riesgos inherentes percibidos, incorporar una segregación apropiada de tareas incompatibles y poseer un alto grado de cumplimiento.

Igual que el riesgo inherente, el riesgo de control existe, independientemente de la auditoría y está en gran medida fuera del control del auditor. No obstante, con el tiempo, las recomendaciones incluidas en los informes de fiscalización para mejorar los controles colaboran a reducir el riesgo de control.

Las evaluaciones del riesgo de control están basadas en la comprensión de los sistemas de control, sus puntos fuertes y débiles y los tipos de errores o irregularidades que podrían no ser detectadas. El interés principal del auditor recae en los controles destinados a reducir los riesgos inherentes y que, por consiguiente, respaldan directamente las manifestaciones referidas a los componentes individuales. La evaluación de estos controles y la confianza en los mismos también depende de la evaluación del medio de control y de los controles generales.

Durante la etapa de ejecución se obtiene evidencia adicional de la confiabilidad de los sistemas de control. La evidencia confirma o niega la evaluación preliminar del riesgo de control y en este último caso se requiere alguna modificación del plan de auditoría.

La reducción del riesgo inherente mediante controles puede ser ilustrada de la siguiente manera. El riesgo inherente asociado con la manifestación de que las cuentas a cobrar están adecuadamente valoradas, puede ser considerado más alto si el auditado continúa abasteciendo a clientes en dificultades financieras a fin de mantener una posición competitiva y su volumen de ventas. El riesgo de control, por el otro lado, puede ser más bajo si el cliente tiene un sistema de control de créditos efectivo, con una estricta aplicación de los límites de crédito, estricta supervisión de los cobros en efectivo y oportuna información de cuentas vencidas a los niveles gerenciales apropiados y rápida acción de cobro cuando sea necesario. Suponiendo que podemos obtener la satisfacción necesaria con respecto a la efectividad y confiabilidad del sistema de control de créditos, los otros procedimientos de auditoría (como identificación de incobrables, evaluación de cobrabilidad por análisis de cuentas y revisión de expedientes de crédito, revisión de cobros posteriores, etc.) podrían ser reducidos independientemente de la naturaleza del riesgo inherente.

c) Riesgo de detección

El riesgo de detección es el riesgo de que los procedimientos de auditoría no lleguen a descubrir errores o irregularidades significativas, en el caso de que existieran.

Este riesgo es una función de la efectividad de los procedimientos de auditoría, su alcance, oportunidad y procedencia y la interpretación de los hallazgos de auditoría.

El riesgo se puede originar por los siguientes factores:

- No examinar toda la evidencia disponible.
- La posible ineficacia del procedimiento de auditoría en sí mismo. Independientemente de lo bien que haya sido aplicado, un procedimiento particular podría no ser adecuado para detectar un cierto tipo de error.
- Posibles deficiencias en la aplicación de los procedimientos de auditoría o en la evaluación de los hallazgos de auditoría, incluyendo el riesgo de presunciones erróneas, errores y conclusiones equivocadas.

3.4.3. Consideraciones sobre los riesgos

Las causas de riesgo de auditoría nunca pueden ser eliminadas. Con el debido cuidado y el ejercicio de destreza profesional, pueden ser reducidas a un nivel aceptable mediante una buena planificación, ejecución y supervisión.

Los riesgos inherentes y de control están fuera del control del auditor pero no así el riesgo de detección. En la práctica, la diferenciación entre el riesgo inherente y el riesgo de control es menos importante que identificar los factores de riesgo que influyen en la naturaleza o alcance de los procedimientos de auditoría planificados.

Variando la naturaleza, oportunidad y alcance de los procedimientos de auditoría se puede alterar el riesgo de detección y, en última instancia, el riesgo final de auditoría. El riesgo de detección disminuye a medida que se obtiene satisfacción de auditoría mediante la aplicación de los adecuados procedimientos de auditoría.

El riesgo de que los procedimientos de auditoría no detecten un error o irregularidad es generalmente una combinación de los riesgos relacionados con cada procedimiento de auditoría. Por ejemplo, hay tres procedimientos de auditoría específicos, (confirmación de cuentas a cobrar, pruebas detalladas de corte y análisis del margen bruto) que tienen la posibilidad de detectar un error de corte en las ventas, en el caso de que existiera; pero además, cada uno está sujeto al riesgo de no poder detectar el error. El riesgo que implica que los tres procedimientos no hayan podido detectar el error es menor que el riesgo que implicaría la aplicación de un solo procedimiento. Sin embargo, existen límites prácticos para la reducción posible del riesgo de detección. Durante la planificación se deberá considerar cuidadosamente la satisfacción global de auditoría que se espera obtener al realizar todos los procedimientos contemplados.

Cuanto más alto sea el riesgo inherente y de control evaluado por el auditor, mayor será la satisfacción de auditoría requerida para reducir el riesgo de detección a un nivel aceptable.

3.4.4. Factores de riesgo de carácter general

Durante la planificación, deben identificarse las condiciones que en una organización podrían permitir la ocurrencia de irregularidades.

Algunas señales que indican la presencia de riesgo son:

- Insuficiente conciencia de control en la organización

  Cuando el entorno de control y el *tone at de top* de la organización son deficientes o inexistentes.

– Gerencia

  Ejecutivos dominantes con pocos límites reales de autoridad; interés excesivo en el efecto que sobre los resultados pueden tener las alternativas contables, excesiva presión política.

– Situación financiera o principio de empresa en funcionamiento

  Problemas financieros tales como, déficit presupuestarios o pérdidas recurrentes, beneficios en disminución, fondo de maniobra inadecuado, escasa flexibilidad en cláusulas de los contratos de préstamos, problemas de financiación, remanentes de tesorería negativos.

– Sistemas de control

  Fallos en los sistemas contables y de control; segregación inadecuada de actividades incompatibles a través de medios manuales o programados; debilidades significativas detectadas que aún no han sido corregidas.

– Personal

  Cantidad insuficiente de personal que requiere que los empleados trabajen horas extra o durante las vacaciones; alto rendimiento de los puestos financieros clave, formación insuficiente en puestos clave.

– Asesores

  Cambios frecuentes de asesores legales; pagos inusualmente grandes.

– Empresas vinculadas

  Transacciones significativas con empresas vinculadas; empresas vinculadas auditadas bajo circunstancias que no son efectivas.

– Estructura societaria

  La complejidad no parece ser necesaria considerando las operaciones o el tamaño de la compañía.

– Otras consideraciones

  Anuncio prematuro de los resultados del período o expectativas externas; los procedimientos analíticos señalan fluctuaciones significativas que no pueden ser explicadas en forma razonable; respuestas evasivas o no razonables de parte de la gerencia a las indagaciones de auditoría; retención de evidencia de auditoría; asientos inusuales o sin, explicación,

documentación o autorización incompleta; alteraciones en documentos o cuentas; transacciones significativas o inusuales (particularmente al cierre del ejercicio); transacciones que pueden involucrar conflictos de intereses; presiones ejercidas para que la auditoría sea completada en un tiempo inusualmente reducido o bajo condiciones difíciles.

Este listado no es completo. Tampoco indica que exista una irregularidad por la presencia de una o más de estas circunstancias. No obstante, si se detecta alguna de ellas se debe estar alerta a la posibilidad de que surjan irregularidades. De la misma manera, la ausencia de estas señales no significa que deba descartarse la posibilidad de que exista alguna irregularidad. En todo caso deben ser analizados con el debido escepticismo profesional.

3.4.5. Factores de riesgo y de control en un entorno informatizado

La utilización de un sistema informatizado, contribuye a aumentar la preocupación cuando se presentan otros indicios. En estos sistemas, las debilidades de control, particularmente la falta de segregación de tareas incompatibles, puede adquirir mayor importancia. Además, las consideraciones de seguridad relativas a los sistemas de información pueden cobrar mayor importancia en un entorno informatizado. El personal de la entidad y terceros no autorizados podrían acceder al sistema con el propósito de cambiar o destruir datos. El riesgo aumenta cuando se utilizan medios telemáticos.

Cuando los sistemas informáticos sean significativos, el auditor debe obtener el necesario entendimiento de su entorno, y si pueden influir en la evaluación del riesgo inherente y de control.

Un entorno informatizado implica entre otros los siguientes tipos de riesgos y características de control interno:[39]

– Ausencia de rastro de las transacciones.

  Algunos sistemas informáticos están diseñados de manera que el rastro completo de una transacción, útil para la auditoría, puede existir sólo durante un periodo corto de tiempo, o de manera que su lectura sólo sea posible a través de medios informáticos.

  Cuando una aplicación informática compleja lleva a cabo un amplio número de etapas de procesamiento, puede no

39. Ver párrafo 4.3 de la *Norma técnica de auditoría en entornos informatizados del ICAC.*

existir un rastro completo. Consecuentemente, los errores que pudiera tener un programa serían difíciles de detectar de manera oportuna por procedimientos manuales.

– Proceso uniforme de transacciones.

  El ordenador procesa uniformemente transacciones similares. De esta forma se eliminan en su totalidad los errores administrativos asociados a procesos manuales.

  Pero, por el contrario, los errores de programación, u otros errores sistemáticos en el hardware o en el software, darán lugar a que todas las transacciones similares procesadas bajo las mismas condiciones, lo sean incorrectamente.

– Falta de segregación de funciones.

  Muchos de los procedimientos de control que normalmente serían ejecutados por personas diferentes en sistemas manuales pueden encontrarse concentrados en sistemas informáticos. Así, una persona que tenga acceso a los programas, a los procesos o a los datos podría realizar funciones incompatibles.

– Posibilidad de errores e irregularidades.

  La posibilidad de errores humanos en el desarrollo, mantenimiento y ejecución de sistemas informatizados de control pueden ser mayores que en los sistemas manuales, en parte a causa del nivel de minuciosidad requerido.

  Además, la posibilidad de que algunas personas no autorizadas accedan a datos o los alteren sin que haya pruebas visibles de ello puede ser mayor con un sistema informático que con un sistema manual.

  Al disminuir la participación humana en las transacciones procesadas por sistemas informáticos se puede reducir la posibilidad de detectar errores e irregularidades.

  Igualmente, los errores e irregularidades ocurridos durante el diseño o modificación de los programas o aplicaciones pueden permanecer ocultos durante largos períodos de tiempo.

– Inicio o ejecución automático de transacciones.

  El sistema informático puede incluir la posibilidad de iniciar o ejecutar automáticamente determinados tipos de transacciones, cuya autorización puede no estar documentada de la misma forma que lo estaría en los sistemas manuales, e incluso dicha autorización puede estar implícita en la aceptación

por parte de la dirección del diseño del sistema informático y sus posteriores modificaciones.

- El ordenador genera de forma automática transacciones significativas o anotaciones directas en otras aplicaciones.
- Controles basados en procesos informáticos.

  El proceso informático puede producir informes y otros datos utilizados en la realización de controles manuales. La efectividad de estos controles manuales puede depender de la efectividad de los controles sobre la integridad y la exactitud del proceso informático.

  A su vez, la efectividad y el funcionamiento uniforme de los controles de las aplicaciones que procesan transacciones depende a menudo de la efectividad de los controles generales de los sistemas informáticos.
- Posibilidad de mayor supervisión de la dirección.

  Los sistemas informáticos pueden ofrecer a la dirección una variedad de herramientas analíticas para revisar y supervisar las operaciones de la entidad. La disponibilidad de estos controles adicionales, si se utilizan, puede servir para mejorar la estructura global de control interno.
- Posibilidad de utilización de técnicas y herramientas de auditoría asistidas por ordenador.

  La facilidad que los sistemas informáticos ofrecen para procesar y analizar grandes cantidades de datos brinda al auditor la oportunidad de aplicar herramientas y técnicas generales o CAAT especializados, como instrumentos para la ejecución de pruebas de auditoría.
- El volumen de transacciones es tal que los usuarios de la aplicación podrían tener dificultades para identificar y corregir errores de proceso.
- El ordenador realiza cálculos complicados de información financiera y/o genera de forma automática transacciones significativas que no pueden ser, o no son, validadas independientemente.

Con carácter general el riesgo de auditoría es creciente conforme se incrementa la complejidad de un sistema de información.

Los riesgos y los controles derivados de estas características de los sistemas informáticos tienen un impacto potencial en la evaluación del riesgo por parte del auditor, así como en la natu-

raleza, momento de realización y alcance de los procedimientos de auditoría.

Ante cada uno de los riesgos de auditoría que se identifiquen debe existir una respuesta clara y directa del auditor (un procedimiento de auditoría) que contrarreste y minimice ese riesgo.

3.4.6. Evaluación y documentación del riesgo

En todas las auditorías, independientemente del tamaño, el riesgo debe ser evaluado y documentado en forma apropiada.

La evaluación del riesgo significa realizar un análisis de los factores de riesgo significativos a través de una perspectiva de arriba hacia debajo de la siguiente manera:

– En la planificación estratégica, se debe considerar el riesgo de auditoría y los riesgos inherentes relacionados, identificando los factores de riesgo que son inherentes al negocio o actividad de la entidad, sus circunstancias económicas y de su sector. Luego, se realiza una evaluación preliminar de los riesgos por unidad operativa y por componente de las cuentas anuales para determinar el enfoque de auditoría para las unidades y componentes y las áreas globales de énfasis.

  Por ejemplo, en la auditoría de una comunidad autónoma, debe analizarse de forma independiente los riesgos relacionados con la actividad sanitaria, que son diferentes a los relacionados con la actividad docente o la puramente administrativa. También, dentro de las áreas anteriores, son diferentes los riesgos relacionados con la gestión de los gastos de personal, los gastos de funcionamiento o las subvenciones.

  Para abordar adecuadamente la auditoría recurrente de una gran entidad, es necesario efectuar la planificación a varios años, realizando un mapa de riesgos por funciones, clasificación económica, ubicaciones geográficas, etc, en el que se indicará el impacto en la entidad y la probabilidad de ocurrencia. De esta forma se dispondrá de una herramienta para priorizar las actividades, empezando por aquellas que abordan riesgos con mayor impacto y probabilidad de que ocurran.

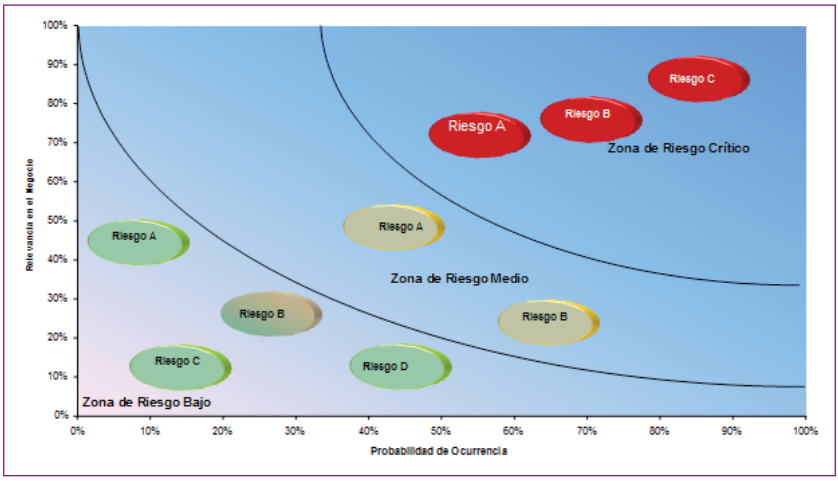


Figura 3.3 Ejemplo de mapa de riesgos

– En la planificación detallada, debe considerarse más detalladamente los factores de riesgo inherentes y de control importantes para cada componente y su impacto sobre las manifestaciones individuales, y luego reconsiderar si las evaluaciones preliminares son apropiadas.

Las evaluaciones del riesgo inherente se realizan en base al conocimiento de auditoría acumulado, indagaciones, actualizaciones de sistemas y procedimientos de diagnóstico. Cuando se posee menos conocimiento sobre la actividad de la entidad, sus sistemas y otras características, como en un trabajo de auditoría por primera vez, las evaluaciones sobre el riesgo en la planificación deben ser más cuidadosas.

Para cada componente se debe documentar los factores de riesgos inherentes y de control que, a criterio del auditor, influyen significativamente en la determinación de la estrategia y la selección de los procedimientos de auditoría.

Los miembros del equipo de auditoría deben comprender la razón por la cual se realizan mayores esfuerzos en algunas áreas de auditoría que en otras, de forma tal que puedan reaccionar adecuadamente cuando sus hallazgos se contraponen con la evaluación del riesgo en el plan de auditoría.

El plan de auditoría debe registrar las razones por las cuales es necesario el énfasis de auditoría en determinadas áreas, mediante la identificación de los riesgos particulares, o en caso contrario las circunstancias que justifican el menor énfasis de auditoría. Sin embargo, no es esencial que todos los aspectos del riesgo sean docu-

mentados, sino que los riesgos en sí mismos sean considerados y comprendidos.

La evaluación del grado de riesgo es una evaluación subjetiva basada en el criterio profesional. Por consiguiente, una vez que la naturaleza de los riesgos ha sido identificada, resulta apropiado evaluar globalmente, con la denominación **A**lto, **M**oderado o **B**ajo el nivel[40] de los riesgos inherentes y de control.

3.4.7. Efecto del riesgo en el enfoque de auditoría

El propósito de la evaluación del riesgo es poder determinar la naturaleza, oportunidad y alcance de los procedimientos de auditoría.

El nivel relativo de riesgo influye sobre el alcance requerido de evidencia de auditoría. No se debe intentar obtener grados significativamente más altos de evidencia de los que se requieren, teniendo en cuenta los objetivos de auditoría. Para aumentar la eficiencia de auditoría, también se debe estar atento a los factores que reducen el riesgo.

Después de obtener una comprensión general de los sistemas de control, se debe decidir confiar o no confiar en los controles. Cuando el riesgo inherente es bajo, la importancia del riesgo de control y el alcance de la satisfacción de auditoría requerido es menor.

A modo de ilustración, los riesgos inherentes y de control podrían afectar nuestro enfoque de auditoría de la siguiente manera:

- El riesgo inherente bajo, cualquiera sea el riesgo de control, pueden implicar que se puede obtener suficiente satisfacción de auditoría mediante procedimientos analíticos o pruebas sustantivas limitadas de transacciones y saldos o ambas cosas. La confianza en los controles clave generalmente no sería considerada eficiente.
- El riesgo inherente de medio a alto con un riesgo de control de medio a bajo puede requerir un enfoque que combine procedimientos sustantivos con pruebas de los controles clave, incluyendo los sistemas informatizados.
- El riesgo inherente de medio a alto con un riesgo de control alto sugerirá un enfoque que incluya extensos procedimientos sustantivos.

40. Esta evaluación en tres niveles será mínima, pudiendo utilizarse una escala tan detallada como se considere conveniente.

3.5. Controles internos en entornos informatizados

3.5.1. Concepto

El término «control» designa todos los conceptos, procedimientos, prácticas y estructuras de organización que permiten verificar con una seguridad razonable la realización de los objetivos de la entidad y la prevención o la identificación y la corrección de acontecimientos no deseables.

Los controles internos relativos a los procesos informáticos comprenden tanto los controles generales que afectan al entorno informatizado en su conjunto como los controles específicos de las distintas aplicaciones de negocio relacionadas con la información financiera.

Cuando se evalúa la fortaleza de un control, se clasifica como preventivo, detectivo o correctivo, de acuerdo con las siguientes características:

Preventivo	• Detecta los problemas antes de que sucedan • Monitoriza tanto las operaciones como los inputs • Pretende predecir problemas potenciales antes de que ocurran y permite hacer los ajustes oportunos • Previenen errores, omisiones o actos malintencionados
Detectivo	• Detectan e informan de la ocurrencia de un error, omisión o acto malintencionado
Correctivo	• Minimiza el impacto de una amenaza • Resuelve problemas descubiertos por los controles detectivos • Identifica la causa de un problema • Corrige los errores producidos por un problema • Modifica el sistema de proceso para minimizar las probabilidades de suceso futuro del problema

Figura 3.4

A las tres clases de controles anteriores cabe añadir los compensatorios. Un control compensatorio, si es efectivo, puede limitar la gravedad de una deficiencia de control interno y prevenir que se convierta en una deficiencia significativa o en una debilidad material. Estos controles limitan la gravedad de una deficiencia, pero no la eliminan.

3.5.2. Tipos de controles

a) Controles generales

Los controles generales son las políticas y procedimientos que se aplican a la totalidad o a gran parte de los sistemas de información de

una entidad, incluyendo la infraestructura y plataformas informáticas de la organización auditada.

En el modelo de la figura 3.1, vemos, a la izquierda, que los controles generales afectan a todos los niveles de los sistemas de información, si bien están relacionados con mucha mayor intensidad con aquellos niveles de carácter general que afectan a toda la organización (nivel entidad) o a los sistemas informáticos de base y la infraestructura informática (nivel de sistemas TI).

De esta forma, para su estudio, diremos que una entidad puede establecer controles generales a los siguientes niveles:

— a nivel de la entidad,

— a nivel de los sistemas TI, y

— a nivel de aplicación.

Los controles generales pueden incluir:

– Controles de organización y dirección

– Controles sobre operaciones realizadas a través del ordenador.

– Controles sobre el software de los sistemas.

– Controles de entrada de datos y de programa.

– Continuidad de las operaciones.

En el apartado 5.4.2 se amplían los comentarios sobre los controles generales

b) Controles de aplicación

Dado que la mayor parte de los procesos de negocio de una entidad están soportados por aplicaciones informáticas, muchos de los controles internos están automatizados en ellas. El objetivo de los, denominados controles de aplicación en un entorno informatizado es establecer procedimientos de control específicos sobre las aplicaciones de negocio con el fin de asegurar razonablemente que todas las transacciones son autorizadas y registradas, y que son procesadas de forma completa, adecuada y oportuna.

Los controles de aplicación garantizan la realización de los objetivos definidos y deben ayudar a garantizar la validez, integridad, exactitud y confidencialidad de las transacciones y datos durante todo el procesamiento de la aplicación.

Estos controles tienen por finalidad asegurar un procesamiento adecuado y seguro de las transacciones y de garantizar la exactitud de los resultados. En consecuencia, los controles juegan un papel central en la realización de los objetivos de la entidad, de la protección del

patrimonio, de la exactitud y de la fiabilidad de la contabilidad y del respeto a las normas.

En el capítulo 5.5.2 se estudian en profundidad los controles de aplicación.

c) Controles de usuario

Los controles de usuario son aquellos realizados por personas que interactúan con los controles de los SI. La eficacia de los controles de usuario generalmente depende de la exactitud de la información proporcionada por el sistema de información, como por ejemplo los informes de excepción u otros informes. Si se da esta dependencia de los SI, los controles de usuario son controles de sistemas de información.

Si el auditor espera que la eficacia de un control de usuario reduzca el riesgo de manifestaciones erróneas significativas, el auditor deberá entender el diseño de cualquier control relacionado que pueda influir en la exactitud de la información contenida en los informes utilizados como parte del control de usuario y comprobar dicho control.

Por ejemplo, si un control de usuario consiste en la revisión de un informe de excepción, el auditor deberá entender el diseño de los controles de la aplicación directamente relacionados con la elaboración de ese informe y comprobar su funcionamiento, así como los controles generales y otros controles de aplicación de los que depende la fiabilidad de la información contenida en el informe. Esta comprobación incluirá los controles del correcto funcionamiento de la aplicación del proceso de negocios que produjo el informe de excepción y la fiabilidad de los datos utilizados para generar ese informe. Además, el auditor deberá comprobar la eficacia del control de usuario (es decir, la revisión de la gestión y el seguimiento de los puntos contenidos en el informe de excepción).

Los controles de usuario pueden ser unos controles manuales utilizados para observar el eficaz funcionamiento de los sistemas de información y los controles de los sistemas de información. Por ejemplo, un control de usuario podría ser comprobar manualmente la exactitud e integridad de las transacciones procesadas por los sistemas de información comparándolas con unos registros elaborados manualmente.

3.5.3. Evaluación del control interno en un entorno informatizado

Con carácter general, el auditor debe obtener una comprensión del control interno suficiente para planificar la auditoría, realizando procedimientos para comprender:

1. el diseño de los controles relevantes para una auditoría de los estados financieros y
2. si los controles están siendo operativos.

Esta comprensión incluirá la consideración de los métodos que una entidad usa para procesar la información, porque dichos métodos influyen en el diseño del control interno.

La extensión con que los sistemas informáticos son utilizados en aplicaciones contables importantes,[41] así como la complejidad de dicho proceso pueden además influir en la naturaleza, calendario y alcance de los procedimientos de auditoría.

La Norma técnica del ICAC sobre auditoría en entornos informatizados, establece que en la planificación de los aspectos de la fiscalización susceptibles de ser influidos por el entorno informático de la entidad auditada, el auditor deberá tener en cuenta la importancia y la complejidad de los sistemas informáticos de dicha entidad, así como la disponibilidad de datos que puedan ser utilizados en la fiscalización.

Así el auditor deberá tener en consideración cuestiones como las siguientes:

- La importancia de los componentes de las cuentas anuales afectados por el procesamiento informático. Una aplicación contable significativa a efectos de la auditoría se relaciona con información contable que puede afectar materialmente a las cuentas anuales auditadas.
- La complejidad. Una aplicación contable debe considerarse significativa cuando, por ejemplo:
  - El volumen de transacciones es tal que sus usuarios pueden encontrar difícil identificar y corregir errores en el procesamiento.
  - El ordenador genera automáticamente transacciones significativas o entradas directas en otra aplicación.
  - El ordenador lleva a cabo operaciones complicadas de información financiera y/o genera automáticamente transacciones significativas o entradas que no pueden ser (o no son) validadas independientemente.

41. Las aplicaciones significativas son aquellas que se relacionan con información contable que puede afectar materialmente a los estados financieros que el auditor está auditando. Las aplicaciones contables significativas pueden incluir además de aplicaciones financieras, aplicaciones de otros sistemas, como sistemas de información a la dirección, o sistemas de revisión de cumplimiento, si proporcionan datos para saldos materiales, transacciones, o revelaciones en las cuentas anuales.

— Se intercambian electrónicamente transacciones con otras organizaciones (como en los sistemas de intercambio electrónico de datos) sin revisión manual de su adecuación o razonabilidad.

- La estructura organizativa de las actividades de los sistemas informáticos de la entidad.
- El grado de concentración o distribución del proceso informatizado en la entidad, especialmente en cuanto puede afectar a la segregación de funciones (mainfranes, redes, intranet, web).
- La disponibilidad de los datos.

Deben considerarse los tipos y adecuación de la evidencia a conseguir, en formato electrónico o en papel, para lograr los objetivos de auditoría.

Fuentes de documentos, ciertos archivos informáticos y otras materias relacionadas con la evidencia necesaria para el auditor pueden existir solo durante un corto período de tiempo o únicamente en soportes de lectura informática.

La posibilidad de utilizar técnicas de auditoría asistida por ordenador puede permitir aumentar la eficiencia de los procedimientos de auditoría, o hacer posible la aplicación, sin excesivo coste, de algunos de ellos al conjunto completo de saldos o transacciones.

De acuerdo con lo anterior, cuando el sistema informático sea significativo, el auditor debe obtener el necesario conocimiento del entorno del mismo, y de su influencia en la evaluación del riesgo inherente y de control.

De acuerdo con las normas técnicas de auditoría, en la planificación de la auditoría, el auditor debe documentar en los papeles de trabajo:

1. su comprensión de los componentes del control interno de una entidad relativos a las aplicaciones informáticas que procesan información usada en la preparación de los estados financieros de la entidad,
2. las bases de su valoración del máximo riesgo de control para las afirmaciones relativas a saldos materiales, clases de transacciones, o revelaciones de los estados financieros cuando dichas afirmaciones dependen significativamente de los sistemas de información computerizados, y
3. la consideración de que los procedimientos planificados de la auditoría son diseñados para conseguir los objetivos de auditoría y reducir el riesgo de auditoría a un nivel aceptable.

4

Enfoque y planificación de la auditoría de sistemas de información integrada en una auditoría financiera

4.1. El enfoque de Auditoría Basado en el Análisis de los Riesgos

4.1.1. Las normas técnicas de auditoría del ICAC

Las Normas Técnicas de Auditoría del ICAC tienen implícito un concepto fundamental: el auditor, al planificar una auditoría, debe realizar un análisis de los riesgos de auditoría que pueden existir al ejecutar el trabajo y emitir su informe, y teniendo en cuenta ese análisis debe diseñar un conjunto de procedimientos de forma que los riesgos queden reducidos a un nivel aceptable a la hora de emitir el informe de auditoría.

Dichas normas, en su apartado 2.4.20, establecen:

«El planteamiento conceptualmente lógico de la evaluación que hace el auditor del control interno, consiste en aplicar a cada tipo significativo de transacciones y a los respectivos activos involucrados en la auditoría, los siguientes criterios:

a) Considerar los tipos de errores e irregularidades que puedan ocurrir.

b) Determinar los procedimientos de control interno contable que puedan prevenir o detectar errores o irregularidades.

c) Determinar si los procedimientos necesarios están establecidos y si se han seguido satisfactoriamente.

d) Evaluar cualquier deficiencia, es decir, cualquier tipo de error o irregularidad potencial no contemplada por los procedimientos de control interno existentes, para determinar:

   1. La naturaleza, momento de ejecución o extensión de los procedimientos de auditoría a aplicar, y

   2. Las sugerencias a hacer al cliente.»

La realización de estos procedimientos requiere el juicio profesional del auditor para la interpretación de los resultados, y la adaptación o extensión de las pruebas de auditoría, para que resulten apropiadas a las circunstancias.

La revisión que haga el auditor del sistema de control interno y sus pruebas de cumplimiento deben relacionarse con cada uno de

los objetivos que se pretenden alcanzar mediante la evaluación del sistema.

Los controles y deficiencias que afecten a cada una de las manifestaciones en las cuentas anuales y a los tipos de transacciones deben ser evaluados independientemente y no son compensatorios en su efecto.

Manifestaciones en las cuentas anuales

Al elaborar las cuentas anuales de conformidad con el marco conceptual correspondiente (contabilidad privada o pública) los cuentadantes realizan manifestaciones implícitas o explícitas en relación con la existencia, acaecimiento, integridad, valoración, medición, presentación y desgloses de los distintos elementos de las cuentas anuales.

Según el apartado 2.5.22 de las Normas técnicas de auditoría del ICAC,[42] el auditor deberá obtener evidencia mediante pruebas substantivas en relación con las siguientes afirmaciones (también denominadas manifestaciones o aserciones) de la Dirección contenidas en las cuentas:

- Existencia

  Los activos y pasivos existen en una fecha dada.

- Derechos y obligaciones

  Los activos son bienes o derechos de la entidad y los pasivos son obligaciones a una fecha dada.

- Acaecimiento

  Las transacciones o hechos registrados tuvieron lugar.

- Integridad

  No hay activos, pasivos o transacciones que no estén debidamente registrados.

- Valoración

  Los activos y pasivos están registrados por su valor adecuado.

- Medición

  Una transacción se registra por su justo importe. Los ingresos y gastos han sido imputados correctamente al período.

- Presentación y desglose

  Las transacciones se clasifican, de acuerdo con principios y normas contables generalmente aceptados y la Memoria

42. Resolución de 19 de enero de 1991 del Instituto de Contabilidad y Auditoría de Cuentas, BOICAC n.º 4 de enero de 1991.

contiene la información necesaria y suficiente para la interpretación y comprensión adecuada de la información financiera auditada.

Por otra parte, de acuerdo con las definiciones incluidas en la *Guía de auditoría* del Registro de Economistas Auditores, una manifestación errónea significativa es una incorrección de importancia relativa en las cuentas anuales que se deriva de errores o irregularidades. Se usa el término de manifestación errónea porque la incorrección se refiere a una de las afirmaciones contenidas en las transacciones, hechos contables o los saldos de cuentas que integran las cuentas anuales.

El riesgo de manifestaciones erróneas significativas (RMES) es el riesgo de que al menos una de las manifestaciones contenidas en las transacciones, hechos contables, saldos de cuentas o revelaciones en la memoria que integran las cuentas anuales sea errónea y cuyo efecto, individual o acumulado, afecte de forma significativa a las cuentas anuales.

4.1.2. El enfoque ABAR según las Normas internacionales de auditoría

Las Normas Internacionales de Auditoría revisadas y las International Standards of Supreme Audit Institutions (ISSAI) 1315 y 1330 emitidas por INTOSAI (que se basan en aquéllas), explicitan mucho más este concepto y exigen que el auditor realice sus auditorías basándose en el *risk-based approach to auditing* o enfoque de auditoría basado en el análisis de los riesgos (ABAR).

De acuerdo con este enfoque,[43] en una ABAR, el objetivo del auditor es obtener una seguridad razonable de que no existen manifestaciones erróneas significativas en las cuentas anuales causadas por errores o irregularidades. Esto implica tres pasos:

1. Evaluar el riesgo de manifestaciones erróneas significativas en las cuentas anuales;
2. Diseñar y ejecutar los procedimientos de auditoría precisos en respuesta a los riesgos evaluados y reducir el riesgo a un nivel aceptablemente bajo, y
3. Emitir un adecuado informe escrito basado en la evidencia de auditoría obtenida y en las incidencias de auditoría detectadas.

43. Véase la *Guide to Using International Standards on Auditing in the Audits of Small- and Mediumsized Entities* (página 27) de la IFAC.

La *seguridad razonable* se refiere al conjunto del proceso de la auditoría, es un alto nivel de seguridad, pero no es absoluto ya que el auditor nunca podrá obtener una seguridad absoluta debido a las limitaciones propias del trabajo realizado, a los juicios profesionales realizados y a la naturaleza de la evidencia examinada.

Bajo este enfoque el auditor debe evaluar el riesgo de manifestaciones erróneas significativas a dos niveles. El primero es al nivel de las cuentas anuales en conjunto, y se refiere al RMES que afectan a las cuentas anuales como un todo y pueden afectar potencialmente a varias manifestaciones.

El segundo se refiere a riesgos identificables con manifestaciones específicas al nivel de las clases de transacciones, saldos de cuentas o revelaciones.

Para simplificar su análisis, en este apartado sintetizamos estas manifestaciones (vistas en el capítulo 4.1.1) en cuatro:

- E Existencia (incluye acaecimiento)
- I Integridad
- F Fiabilidad (incluye presentación y desglose, derechos y obligaciones, y medición)
- V Valoración

Para cada clase de transacción, saldo de cuenta o revelación, debe realizarse una evaluación del riesgo (como Alto, Moderado o Bajo) para cada una de las manifestaciones (E, I, F, y V de la figura 4.1).

Al analizar los RMES el auditor clasifica las manifestaciones en tres tipos: sobre los saldos de las cuentas a la fecha de cierre del periodo auditado, sobre las clases de transacciones y acontecimientos del periodo auditado y sobre la presentación y revelaciones.

La siguiente figura muestra gráficamente la diferencia entre la evaluación de riesgos en ambos niveles.

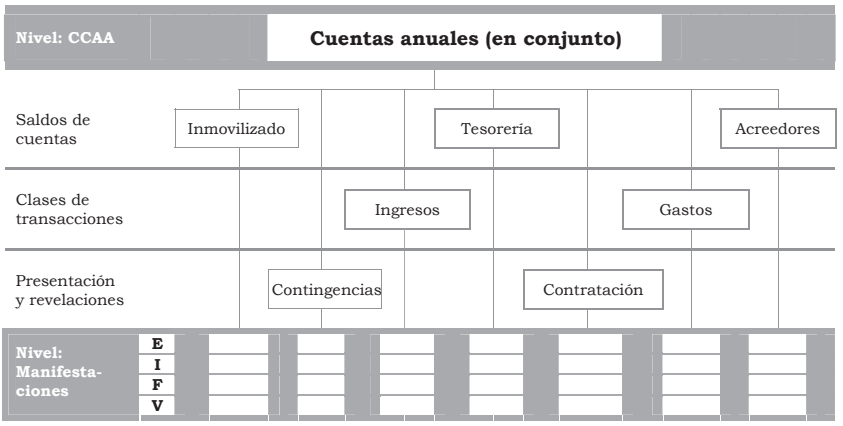


Figura 4.1

Se analizarán las cuentas anuales para orientar los procedimientos de auditoría sobre los procesos de negocio y las correspondientes aplicaciones informáticas que guarden relación con áreas significativas de las cuentas anuales auditadas y sus riesgos asociados. Este análisis liga las principales áreas contables a los procesos de negocio pertinentes, y determina los flujos de tratamiento de los datos y las principales aplicaciones que soportan esos flujos de datos.

Una vez identificadas las principales aplicaciones, el auditor se interesará en la calidad del sistema de control. En primer lugar analizará si su diseño está adaptado a la situación real de los riesgos de los procesos de negocio y finalmente si los controles previstos están implementados y funcionan con eficacia.

La evaluación del sistema de control interno de los procesos de negocio significativos para la auditoría permite al auditor saber si puede apoyarse y confiar en los procedimientos de elaboración de las cuentas anuales y en función de los resultados de las pruebas de cumplimiento, definir la extensión de los procedimientos sustantivos de auditoría suplementarios que deberá efectuar.

4.1.3. Enfoque integrado y equipo pluridisciplinar

En una entidad que opera en un entorno informatizado, la calidad de la información financiera depende en gran medida de la calidad de los procesos de negocio y de los flujos de procesamiento de los datos relacionados. Es por tanto lógico que el auditor centre su trabajo sobre los procesos de negocio que sean significativos

y en la revisión de los controles internos e integre la revisión de las aplicaciones informáticas que los soportan en su enfoque de auditoría.

En esas situaciones, con carácter previo a la revisión de los controles de las aplicaciones de negocio significativas, el auditor debe evaluar y probar de forma sistemática los controles generales embebidos en el sistema de información a fin de definir una estrategia de pruebas adaptada a las circunstancias para la revisión de los controles de las aplicaciones.

Así, en el marco de los procedimientos de una auditoría financiera basada en el análisis de riesgos, es preciso tomar en cuenta los aspectos específicos del entorno informatizado que tengan influencia sobre los objetivos de la auditoría.

En estas circunstancias es necesario que colaboren estrechamente tanto el auditor financiero como el informático, con sus conocimientos y experiencia complementarios, ya que en caso contrario el riesgo de auditoría será alto, tanto más elevado cuando más complejo sea el entorno informatizado.

El enfoque de auditoría que se expone a lo largo de todo este trabajo, pretende ser integrado y orientar los procedimientos de auditoría de forma más eficaz y centrada sobre los riesgos, integrando en la auditoría financiera la revisión de los procesos de negocio y de las aplicaciones informáticas correspondientes. Se comenzará con el análisis de las cuentas anuales de la entidad y se terminará por la valoración de los resultados de la auditoría sobre dichas cuentas y la emisión del correspondiente informe.

Tal como se destaca en el apartado 2.6.1 el auditor financiero debe tener el conocimiento suficiente de los sistemas informáticos que le permita planificar, dirigir, supervisar y revisar el trabajo realizado. Debe evaluar si es necesario para la auditoría disponer de conocimientos especializados sobre esta materia que permitan:

a) Entender suficientemente los sistemas contables y de control interno afectados por el entorno informatizado.
b) Determinar el efecto del entorno informatizado en la evaluación del riesgo global y del riesgo a nivel de saldos contables y de tipos de transacciones.
c) Diseñar y aplicar las adecuadas pruebas de cumplimiento de los controles generales y controles de aplicación y los procedimientos sustantivos.

Si el auditor estima que se requieren conocimientos específicos para cubrir los aspectos anteriormente indicados, deberá obtener asesoramiento de otros profesionales que los posean, bien de su propia organización o bien ajenos a la misma.

Normalmente se requerirá la colaboración de un auditor de sistemas de sistemas de información en situaciones donde:

- Los sistemas informatizados de la entidad, los controles automatizados o la forma en la que son usados para gestionar la actividad de la entidad es compleja.
- Se han hecho cambios significativos en los sistemas informatizados existentes o se han implementado otros nuevos.
- La información está muy compartida entre las distintas aplicaciones.
- La entidad utiliza el comercio electrónico.
- La entidad utiliza tecnologías emergentes.
- Evidencia de auditoría significativa existe solo en formato electrónico.

Un problema bastante frecuente en las colaboraciones entre los auditores financieros y los auditores informáticos radica en las dificultades de comunicación entre ellos, debido a los diferentes lenguajes utilizados (marcadamente económico y contable uno, y muy técnico el otro). Para mejorar la eficacia de las auditorías es necesario que ambos auditores mejoren su mutua comunicación.[44]

Para mejorar y hacer más fluida esta comunicación es muy importante que el auditor financiero tenga los suficientes conocimientos para:

1. comunicar los objetivos del trabajo al auditor de sistemas (ver capítulo 4.4),
2. evaluar si los procedimientos a realizar cubren los objetivos de auditoría, y
3. evaluar los resultados de las pruebas realizadas.

En el caso de que el auditor financiero obtenga asesoramiento de otros profesionales externos especializados, se deberá tener en cuenta el contenido de la Norma técnica de auditoría sobre la utilización del trabajo de expertos independientes por auditores de cuentas.[45]

44. *Comment intégrer l'audit informatique?*, Michel Huissoud, L'Expert-comptable suisse, 9/94.

45. ISA 620 Norma técnica de auditoría del ICAC sobre *Utilización del trabajo de expertos independientes.*

4.1.4. Diligencia profesional y escepticismo profesional

La norma 2.2.3 de los Principios y Normas de Auditoría del Sector Público de los OCEX establece que «la ejecución de los trabajos y la emisión de los informes se llevará a cabo con el debido cuidado profesional», que impone al auditor el cumplimiento de las normas técnicas de auditoría.

Aunque es un concepto no recogido expresamente en los Principios y Normas de Auditoría del Sector Público, la realización de las auditorías con un razonable grado de escepticismo profesional es un elemento esencial de la diligencia profesional. Dicho concepto, consustancial a la actividad auditora, ha adquirido una importancia creciente en los últimos años, recogiéndose de forma expresa en las Normas Técnicas de Auditoría del ICAC sobre cumplimiento de la normativa y sobre errores e irregularidades y en las Normas Internacionales de Auditoría.

El escepticismo profesional es una actitud que requiere mentalidad o espíritu crítico y una evaluación crítica de la evidencia de auditoría. Significa no confiar únicamente en las manifestaciones del auditado y no dar por sentado que los registros proporcionados por el auditado son auténticos sin otra evidencia corroborativa.[46]

Esto puede plantear problemas a veces, cuando los registros informáticos (evidencia informática de transacciones o saldos) sólo pueden ser corroborados por otra evidencia informática. En estos casos su autenticidad y fiabilidad puede ser difícil o imposible de verificar sin comprender y verificar los controles informáticos relacionados.

Hay que tener presente que los listados en papel o en formato digital, sobre los que se hacen determinadas comprobaciones son tan sólo una visualización física, en papel o en la pantalla, de una evidencia informática, que puede ser fácilmente alterada para engañar al auditor.

El apartado 5.3.10 de las Normas de Auditoría del Sector Público de la IGAE recoge esta idea y dice que «Cuando se emplee evidencia informática, o datos procedentes de sistemas informáticos del auditado, los auditores deberán evaluar la fiabilidad de esta evidencia, y no darla nunca por supuesta a priori.»

46. Según Isaac Jonas: «Se trata, en definitiva, de evitar caer en la simplificación de asumir que todo lo que está informatizado es correcto, y de aplicar el escepticismo profesional que debe regir toda actuación del auditor también al proceso realizado en los propios sistemas de información, y por supuesto a los resultados obtenidos en los mismos, ...»; Jonás González, Isaac; *La auditoría de cuentas en entornos informatizados*, *Partida Doble*, n.º 156, junio de 2004.

Cuanto más complejo sea el entorno informático mayor será el grado de escepticismo profesional requerido.

Dicho todo lo anterior, debe tenerse claro que un auditor no tiene que ser necesariamente competente (especialista) en la obtención y examen de la evidencia informática para darse cuenta que la información proporcionada por los ordenadores no es fiable si no hay otra evidencia corroborativa, o si no se ha realizado y documentado una revisión de los controles generales y de aplicación. Sólo tiene que actuar con la debida diligencia y escepticismo profesional y hacerse, entre otras, las siguientes preguntas:

> ¿Cuál es la probabilidad de que un listado u otro documento informático sea erróneo, tanto accidental como intencionadamente?
>
> ¿Quiénes, de la organización auditada, tienen la oportunidad y el incentivo para alterar los datos electrónicos por algún motivo?
>
> ¿Puede alterarse la evidencia informática sin dejar pistas de auditoría o rastros del cambio?
>
> ¿Hay una pista de auditoría que liga claramente la evidencia informática al hecho que la generó y en algunos casos hacia su inclusión en las cuentas anuales?
>
> ¿Contiene la evidencia informática información que identifique quién generó la entrada y cuándo?
>
> ¿Qué controles existen para prevenir cambios no autorizados en la evidencia informática después de su correcta generación?
>
> ¿Quién tiene derechos de acceso para cambiar la evidencia informática?
>
> ¿Cómo sabe el auditor que la evidencia informática no ha sido intencionadamente alterada para engañar o llevar a conclusiones equivocadas?
>
> ¿Tienen el sistema un «log» de auditoría adecuadamente establecido para registrar los intentos de acceso (éxitos y fracasos) a la evidencia informática?
>
> ¿Han sido revisados los «log» de auditoría por alguien independiente?

La respuesta a estas cuestiones ayudará al auditor a evaluar la fiabilidad de los datos informáticos, el riesgo de que existan incidencias significativas y a planificar pruebas de auditoría más eficaces, incluyendo la necesidad de que participe un experto en auditoría informática.

4.2. Fases de una auditoría de sistemas de información

Como en cualquier otra actividad auditora, la auditoría de sistemas de información consta de las tres fases siguientes:

Planificación: El auditor determina la forma más efectiva y eficiente de obtener la evidencia necesaria para alcanzar los objetivos de la auditoría de sistemas de información y respaldar el informe de auditoria. (Se estudia esta materia en el capítulo 4.3).

Ejecución: El auditor de sistemas probará la efectividad de los controles TI que sean relevantes para los objetivos de la auditoría. (Se estudia esta materia en el capítulo 5).

Informe: El auditor concluirá sobre el efecto de cualquier debilidad detectada en los controles TI relacionados con los objetivos de auditoría e informará sobre los resultados de su auditoría. (Se estudia esta materia en el capítulo 6).

4.3. Planificación de la auditoría

4.3.1. Tipos de planificación

Antes de empezar a tratar los aspectos más relevantes de la planificación de una auditoría de sistemas de información, consideramos pertinente realizar algunas observaciones sobre los distintos niveles de planificación existentes, los cuales deben realizarse de forma coordinada para obtener el máximo grado de eficacia:

- Planificación estratégica del departamento de auditoría informática.
- Planificación anual del OCEX/órgano auditor.
- Planificación plurianual de cada ente a fiscalizar.
- Planificación de una auditoría.

1. Planificación estratégica del departamento de auditoría informática del órgano auditor

En esta planificación a largo plazo se deben plasmar las metas y los objetivos para el departamento de auditoría informática fijados por el superior órgano de gobierno del OCEX/órgano auditor para un periodo de 3 a 5 años.

Este plan debe abarcar todos los entes sujetos a fiscalización por el órgano auditor y se deben considerar aspectos como:

– Objetivos a largo plazo del OCEX/órgano auditor.
– Elaboración de un mapa general de riesgos, en el que estén incluidos todos los entes sujetos a fiscalización potencial.
– Prioridades de auditoría y criterios para establecerla.
– Cómo reorientar los métodos y técnicas de auditoría para alcanzar los objetivos de auditoría en un entorno dinámico.
– Necesidades humanas y materiales.
– Colaboraciones externas.
– Necesidades de formación.

2. Plan anual del OCEX/órgano auditor

Traslada el plan a largo plazo del órgano auditor a un plan operativo de trabajo para un ejercicio.

Este plan definirá los objetivos y alcances para cada uno de las entidades a fiscalizar en el ejercicio siguiente, teniendo en cuenta los recursos humanos disponibles del órgano auditor y las disponibilidades presupuestarias para contratar colaboraciones externas de expertos en auditoría de sistemas de información.

3. Planificación plurianual de cada ente a auditar

Las posibles actividades de auditoría informática derivadas del gran número, extensión y complejidad de los sistemas de información en una entidad media o grande, es muy elevada, lo que en general hace inviable para un órgano auditor razonablemente dimensionado abarcar todo el Universo TI[47] relevante.

De esta circunstancia se deriva la necesidad de elaborar un plan de trabajo para un periodo de tres años para los entes fiscalizados recurrentemente (que normalmente serán los más importantes en el ámbito de actuación del órgano auditor).

Este plan abarcará los sistemas y las aplicaciones relevantes de la entidad, e incluirá la programación y el alcance de las revisiones a efectuar en el periodo y la fundamentación para el enfoque planeado. Este plan debe revisarse anualmente en función de los resultados de cada auditoría y si se producen cambios significativos en el entorno TI de la entidad.

En los casos en los que se aplique un plan de pruebas o de auditoría plurianual, al realizar la planificación anual se debe documentar la conclusión del auditor sobre si en el año corriente puede depositarse confianza en la evidencia obtenida en años anteriores sobre la eficacia de los controles internos.

47. Ver capítulo 4.4.

En aquellas fiscalizaciones que realizan los OCEX de carácter no recurrente, no será necesario ni eficiente realizar un plan plurianual detallado.

4.3.2. Planificación de una auditoría individual

Todo trabajo de auditoria individual, de unas determinadas cuentas anuales (incluyendo la parte correspondiente a la revisión de los sistemas de información) debe planificarse adecuadamente y documentarse en una memoria de planificación.

La planificación de la auditoría informática es el primer paso para realizar una auditoría efectiva de los sistemas de información. Debe realizarse conjuntamente y de forma integrada con la planificación de la auditoría financiera.

En una auditoría financiera, de acuerdo con la ISSAI 1300 / ISA 300[48] el auditor desarrollará una estrategia global de auditoría y un plan de auditoría.

La estrategia global describirá el alcance, el momento y el enfoque de la auditoría, así como las directrices de actuación de la auditoría. Para ello el auditor.

- Identificará las características del trabajo, que condiciona su alcance.
- Concretará los objetivos para el informe para organizar el calendario de la auditoría y el tipo de comunicaciones.
- Considerará los factores que según su juicio profesional son significativos para focalizar los esfuerzos del equipo de auditoría.
- Determinará la naturaleza, calendario y extensión de los recursos necesarios para realizar el trabajo.

Además el auditor desarrollará un plan de auditoría que incluirá una descripción de:

- La naturaleza, momento y extensión de los procedimientos planeados para la evaluación del riesgo.
- La naturaleza, momento y extensión de los procedimientos sustantivos planeados.

Una adecuada planificación ayuda a:

- Dirigir y controlar el trabajo de auditoría.

48. ISSAI 1300: Norma Internacional de las Entidades Fiscalizadoras Superiores - Planificación de una auditoría de los estados financieros.

ISA 300: Norma Internacional de Auditoría - Planificación de una auditoría de los estados financieros.

– Identificar las áreas relevantes.
– Asignar los recursos (escasos) a las áreas más importantes.
– Establecer el calendario de trabajo y los plazos para revisar el trabajo.
– Obtener evidencia de auditoría suficiente, fiable y relevante.
– Efectuar recomendaciones para mejorar la gestión.

El plan contendrá una descripción detallada de la organización de la entidad auditada incluyendo la descripción preliminar del sistema de control interno y de los principales elementos del sistema de información.

Si la auditoría informática se realiza en el marco de una auditoría financiera, se deberá obtener una comprensión suficiente del control interno relacionado con la información financiera que permita evaluar el riesgo, con origen en las tecnologías de información, de manifestaciones erróneas significativas en las cuentas anuales y diseñar las pruebas basadas en esta evaluación. Esto incluirá procedimientos para evaluar el diseño de los controles relevantes para la auditoría financiera y para comprobar si los controles han sido implementados y funcionan eficazmente.

También se justificará la extensión de la colaboración necesaria de los auditores informáticos y la distribución del trabajo entre el auditor financiero y el auditor informático.

Esta fase del trabajo es muy importante para el adecuado desarrollo de la auditoría y representa un elevado porcentaje del presupuesto de horas, especialmente en las primeras auditorías. Si no hay cambios en la organización o en los sistemas de información, en años sucesivos disminuirá el peso de esta fase en el conjunto de la auditoría.

El plan se documentará en una **memoria de planificación**, cuyo propósito es:

– Definir el alcance de la auditoría informática.
– Describir la justificación del enfoque de auditoría adoptado.
– Describir cómo debe avanzar la auditoría.
– Proporcionar un medio para comunicar el plan de auditoría a los otros miembros del equipo.

El contenido de la memoria de planificación será:

– Antecedentes e información relevante sobre la entidad auditada.
– Los objetivos de la auditoría.

- El alcance de la auditoría.
- Las áreas críticas a estudiar.
- Procedimientos principales.
- Personal necesario.
- Etc. (ver apartado 4.7).

Actividades de planificación

La planificación es un proceso iterativo que debe mantenerse abierto durante toda la auditoría (por ejemplo, los resultados de alguna prueba de auditoría pueden hacer cambiar determinado enfoque de auditoría; se podía haber previsto confiar en los controles clave, pero los resultados han sido malos y se decide aumentar el alcance de las pruebas sustantivas).

No obstante, las actividades de planificación se concentran al principio del trabajo, en la fase de planificación, durante la cual el objetivo es obtener una adecuada comprensión de la entidad y de sus actividades, incluyendo su sistema de control interno, identificar y evaluar los riesgos, y diseñar la naturaleza, extensión y el momentos para ejecutar los procedimientos de auditoría.

Entre las actividades a realizar (relativas a los sistemas de información), están:

- Comprender los objetivos globales y el alcance de la auditoría de sistemas de información.
- La comprensión de la actividad de la entidad, de los principales procesos de negocio y del sistema de control interno.
- Obtener una comprensión general de la estructura de las redes de la entidad.
- Identificar las áreas clave de interés para la auditoría (archivos, bases de datos, aplicaciones, sistemas).
- Evaluar el riesgo preliminar de los sistemas de información.
- Identificar puntos críticos de control.
- Obtener una comprensión preliminar de los controles TI.
- Estudiar la necesidad de que participen expertos en auditoría de sistemas de información (internos o externos).
- Hacer un plan de revisiones plurianual.

Normalmente todas estas actividades no se podrán realizar en el orden anterior, sino en función de las circunstancias

El auditor planifica su trabajo para definir un método efectivo y eficiente para obtener la evidencia necesaria que respalde los obje-

tivos de la auditoría y las conclusiones que se reflejen en el informe de auditoría.

El tipo y la extensión de los procedimientos para planificar un trabajo varían en cada auditoría dependiendo de varios factores: tamaño y complejidad de la entidad y de sus sistemas de información, la experiencia y el conocimiento que tenga el auditor de la entidad.

Un elemento clave para realizar una auditoría de calidad es que los miembros del equipo de auditoría con más experiencia (tanto el auditor financiero como el informático) se involucren en la planificación.

El auditor también debe coordinarse estrechamente con la entidad auditada.

Al evaluar el sistema de control interno se estudiará como afecta el uso de TI a los controles relevantes para la auditoría.

4.4. Determinación del alcance del trabajo del auditor de sistemas de información en una auditoría financiera

Tal como hemos comentado en el capítulo 2.1, el ámbito de trabajo de un auditor de sistemas de información es, con carácter general, muy amplio ya que puede abarcar múltiples áreas y componentes, que potencialmente pueden formar parte de una auditoría informática. Sin ánimo de ser exhaustivo, se pueden citar:

- Auditoría de la administración electrónica.
- Auditoría de gestión de datos personales.
- Auditoría sobre la accesibilidad de páginas web.
- Auditoría forense.
- Auditoría de gestión.
- Auditorías específicas sobre adquisición de equipos y sistemas.
- Auditoría de seguridad informática.
- Auditoría de aplicaciones informáticas y sistemas de información.
- Auditorías limitadas sobre controles generales y de aplicación.
- Auditoría de redes y comunicaciones.
- Auditoría de sistemas de información realizada en el marco de una auditoría financiera.

Cada una de las posibles áreas señaladas, podría, a su vez, ser dividida en diversas áreas de trabajo de auditorías específicas.

A todo este vasto conjunto de posibles áreas de trabajo del auditor informático lo denominaremos «Universo TI» y lo representaremos en la figura siguiente como un conjunto de color amarillo.

Para realizar una auditoría informática el auditor de sistemas debe trabajar basándose en un marco de actuación profesional, como por ejemplo Cobit, que es una metodología adecuada a esa tarea e internacionalmente reconocida.

Pero en el contexto de una auditoría financiera, realizar todos los procedimientos Cobit resultaría sin duda excesivo e innecesario.

Los auditores informáticos impulsados por su diligencia profesional pueden sentir la «tentación» de aplicar sus conocimientos y experiencia a su «Universo TI», establecer prioridades de acuerdo con sus criterios (cuya perspectiva será fundamentalmente técnica) y definir el alcance de su trabajo de forma no coordinada con el auditor financiero. De esta forma se corre el riesgo de realizar más procedimientos de auditoría de los necesarios para los objetivos de una auditoría financiera.

Este es uno de los riesgos derivados del problema de comunicación entre auditores financieros y auditores informáticos que ya hemos mencionado.

Un buen sistema para determinar el alcance preciso del trabajo del auditor de sistemas de información en el marco de una auditoría financiera, que no sea ni excesivo, ni insuficiente, es aplicando el enfoque de Auditoría Basada en el Análisis de los Riesgos (ABAR), que se ha descrito en el capítulo 4.1.2.

Una ABAR comienza identificando los distintos aspectos relacionados con la información financiera (representados con un conjunto azul en la siguiente figura).

Por ejemplo, se debe averiguar, entre otras cuestiones:

- ¿Qué sistemas manuales o automatizados están relacionados con la elaboración de la información financiera?
- ¿Qué cuentas y clases de transacciones están relacionadas con la elaboración de la información financiera?
- ¿Qué procesos manuales o automatizados ocurren en el ciclo de elaboración de la información financiera?

A continuación el auditor de sistemas de información, conjuntamente con el auditor financiero, evalúa qué componentes del Universo TI son relevantes a los efectos de la información financiera. En el gráfico siguiente esos componentes estarían representados por la intersección de los conjuntos amarillo y azul.

En ese subconjunto intersección, se incluirán los datos asociados con la información financiera y los componentes TI relacionados con la captura, procesamiento, almacenamiento y manipulación de dichos datos. Estos componentes del Universo TI serán relevantes para la información financiera.

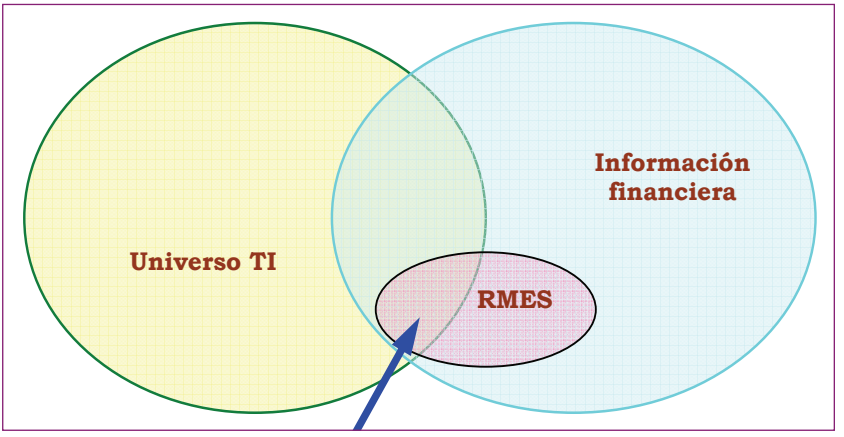


Figura 4.2. Alcance de la auditoría de SI en una auditoría financiera[49]

Pero todavía debe acotarse con mayor exactitud el alcance de la auditoría de SI considerando los riesgos de manifestaciones erróneas significativas (RMES, representados en la figura anterior con un círculo rosado). Estos riesgos incluyen los riesgos inherentes y de control asociados a las TI.

En esta fase la responsabilidad del auditor informático consiste en determinar:

a) Qué riesgos existen debido a la utilización de las TI en el proceso de elaboración de la información financiera.

   Estos riesgos dependerán, entre otras cuestiones, de la complejidad del entorno TI.

b) Además debe determinar cuáles de esos riesgos son relevantes, es decir cuáles pueden ocasionar un riesgo de manifestaciones erróneas significativas (RMES). En el gráfico anterior están representados por la intersección de los tres conjuntos (señalada con una flecha azul).

49. *What every auditor IT should know about scoping an IT audit*, Tommie W. Singleton, ISACA Journal, vol 4, 2009.

Los demás serán riesgos irrelevantes y no deberán ser objeto de mayor atención por parte del auditor informático en el marco de la auditoría financiera.

Llegados a este punto debe destacarse que un riesgo considerado irrelevante a los efectos de la auditoría financiera puede, sin embargo, ser muy importante en una auditoría informática independiente. No obstante el auditor de sistemas de información debe centrar sus procedimientos (el alcance de su trabajo) de auditoría, exclusivamente, en aquellos componentes del «Universo TI» incluidos en el subconjunto intersección con RMES.

La determinación del alcance de la auditoría con este enfoque permite realizar una auditoría más eficaz (ya que se abordan los riesgos importantes) y más eficiente (ya que no se realizarán procedimientos de auditoría innecesarios).

4.5. Materialidad

4.5.1. Concepto

La materialidad o importancia relativa puede considerarse[50] como la magnitud o naturaleza de un error (incluyendo una omisión) en la información financiera que, bien individualmente o en su conjunto, y a la luz de las circunstancias que le rodean hace probable que el juicio de una persona razonable, que confía en la información, se hubiera visto influenciado o su decisión afectada como consecuencia del error u omisión. El concepto de importancia relativa, necesariamente habrá de ser contemplado tanto en el desarrollo del plan de auditoría como en el proceso de formación de la opinión del auditor.

Al planificar la auditoría de sistemas de información, el auditor utiliza el concepto equivalente a la materialidad de la auditoría financiera para planificar procedimientos de auditoría que sean eficaces y eficientes.

El principio subyacente en la materialidad es que el auditor no necesita dedicar recursos (horas de profesional) en aspectos de poca importancia, es decir aquellos que no afectan al juicio o conducta de un usuario razonable del informe de auditoría. Basándose en este principio el auditor puede decidir que algunas áreas de la auditoría de sistemas de información no son materiales o significativas y dedicarles poca o nula atención.

50. Apartado 2.5.16 de las Normas Técnicas de Auditoría del ICAC.

La materialidad incluye factores tanto cuantitativos como cualitativos relativos al objeto de la auditoría. Por ejemplo, un sistema puede procesar transacciones de importes muy bajos, pero puede contener información confidencial o proporcionar vías de acceso a otros sistemas que contienen información confidencial o quizá significativa; ambas cuestiones deben ser consideradas al decidir si una posible incidencia es material.

A los efectos de la revisión de controles internos, se utilizarán los siguientes conceptos y definiciones: [51]

Deficiencia de control interno

Una deficiencia de control interno existe cuando el diseño o el funcionamiento de un control no permite al personal de la entidad o a su dirección, en el curso ordinario de las operaciones, prevenir o detectar errores o irregularidades en un plazo razonable:

- Existe una *deficiencia en el diseño* del control cuando: (a) un control necesario para alcanzar el objetivo de control no existe o (b) un control existente no está adecuadamente diseñado de forma que si funciona como está diseñado, la actividad de control no siempre se realiza.
- Existe una *deficiencia de funcionamiento* cuando un control adecuadamente diseñado no opera tal como fue diseñado o cuando la persona que lo ejecuta no posee la necesaria autoridad o cualificación para realizarlo eficazmente.

Deficiencia significativa

Una deficiencia significativa es una deficiencia en el control interno, o una combinación de deficiencias, que afectan adversamente la capacidad de la entidad para iniciar, autorizar, registrar, procesar o reportar información financiera de forma fiable de conformidad con los principios o normas contables y/o presupuestarias aplicables, y existe una probabilidad que es más que remota,[52] de que una manifestación

51. Basados en el *Statement on Auditing Standards No. 115, Communicating Internal Control Related Matters Identified in an Audit* y utilizados en el FAM de la GAO.

52. El término «más que remota» significa lo mismo que «al menos razonablemente posible». Deben tenerse presentes las siguientes definiciones (basadas en el Financial Accounting Standards Board Statement No. 5, Accounting for Contingencias): 1) Remoto: La probabilidad de que ocurran determinados hechos futuros es mínima; 2) Razonablemente posible: La probabilidad de que ocurran determinados hechos futuros es más que remota pero menos que probable; 3) Probable: Cuando la probabilidad de que ocurra el acontecimiento futuro es superior a la de su no ocurrencia.

errónea en las cuentas anuales, que no es claramente trivial,[53] no sea prevenida o detectada por los empleados de la empresa en el curso normal de ejecución de las funciones que les fueron asignadas.

Debilidad material

Una debilidad material es una deficiencia significativa en el control interno o una combinación de ellas, respecto de las que existe una razonable posibilidad (si tuviéramos que concretarla diríamos que la probabilidad es superior al 50%) de que una manifestación errónea significativa en las cuentas anuales no sea prevenida o detectada y corregida en plazo oportuno.

4.5.2. Relación entre la importancia relativa, el riesgo de auditoría y la extensión de los procedimientos de auditoría

Los criterios que afectan a la «cantidad» (suficiencia) y a la «calidad» (adecuación) de la evidencia a obtener y, en consecuencia, a la realización del trabajo de auditoría, son los de «importancia relativa» y «riesgo probable».

Estos criterios deben servir, asimismo, para la formación del juicio profesional del auditor.

La consideración del riesgo de auditoría supone la posibilidad de que el auditor no detecte un error significativo que pudiera existir en las cuentas, por la falta de evidencia respecto a una determinada partida o por la obtención de una evidencia deficiente o incompleta sobre la misma.

Los conceptos de materialidad y riesgo están interrelacionados y a veces se confunden. El auditor utiliza ambos conceptos para

1. determinar la naturaleza, extensión y momento para realizar los procedimientos de auditoría, y
2. evaluar el resultado de las pruebas.

La evaluación del riesgo normalmente no afecta a la materialidad. Sin embargo el riesgo sí afecta a la extensión requerida de las pruebas. Cuanto mayor sea la evaluación del riesgo de incidencias materiales, mayor será el nivel requerido de procedimientos sustantivos, es decir mayor deberá ser el tamaño de las muestras examinadas, pero

53. Incidencias «claramente triviales» son aquellas cuestiones sin trascendencia a nivel individual y de conjunto, ya sean juzgadas con criterios de cuantía, de naturaleza o atendiendo a las circunstancias que las rodean. (Fuente: Manual de fiscalización de la Sindicatura de Cuentas de la Comunidad Valencia – Sección 230. www.sindicom.gva.es/web/valencia.nsf/documento/manual_de_fiscalizacion)

no se modificará el error tolerable ni el nivel de importancia relativa o materialidad.

4.6. Pasos para evaluar controles de los sistemas informatizados en una auditoría financiera

Los siguientes flujogramas ilustran las etapas o pasos a seguir por el auditor financiero y por el auditor de sistemas de información para comprender y evaluar los controles de los sistemas de información en el contexto de una auditoría financiera realizada con el enfoque ABAR.

En primer lugar se realizarán los procedimientos iniciales de planificación y conocimiento de la entidad y análisis de los controles generales:[54]

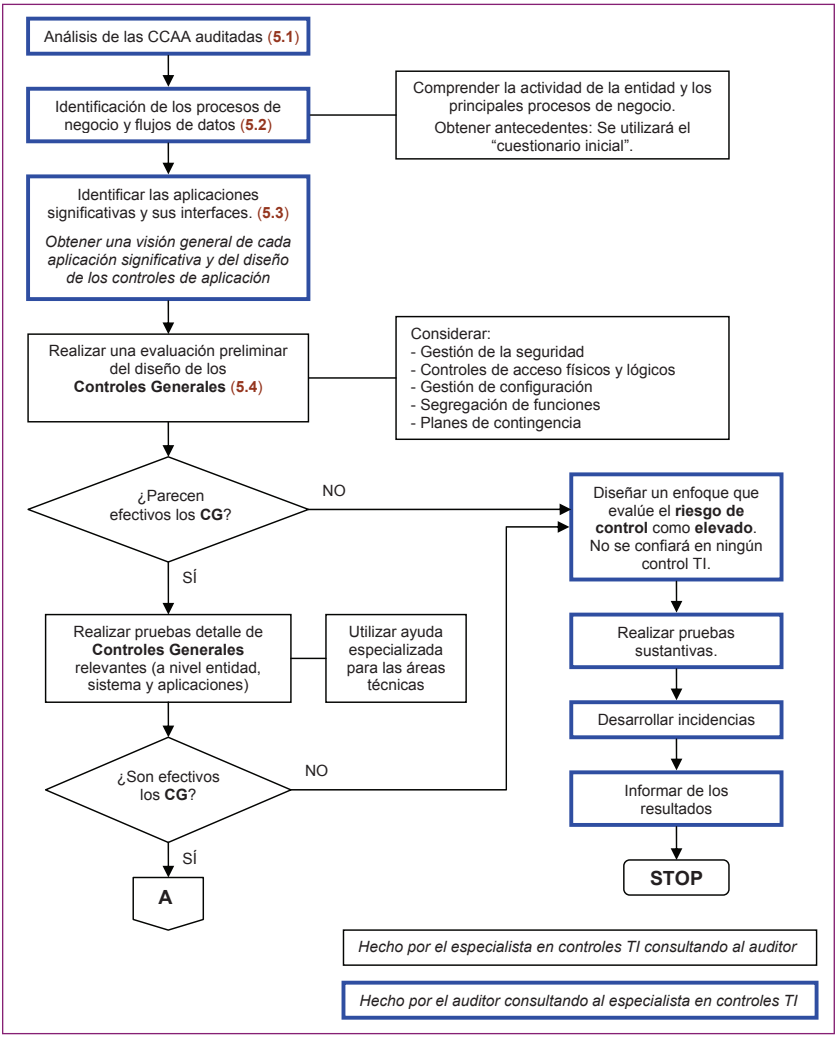


Figura 4.3: Pasos para evaluar controles generales

Los números entre paréntesis hacen referencia a los correspondientes capítulos de este trabajo.

54. Basado en FISCAM, página 527 y 528.

A continuación, para las aplicaciones significativas se darán los siguientes pasos para revisar los controles clave identificados:

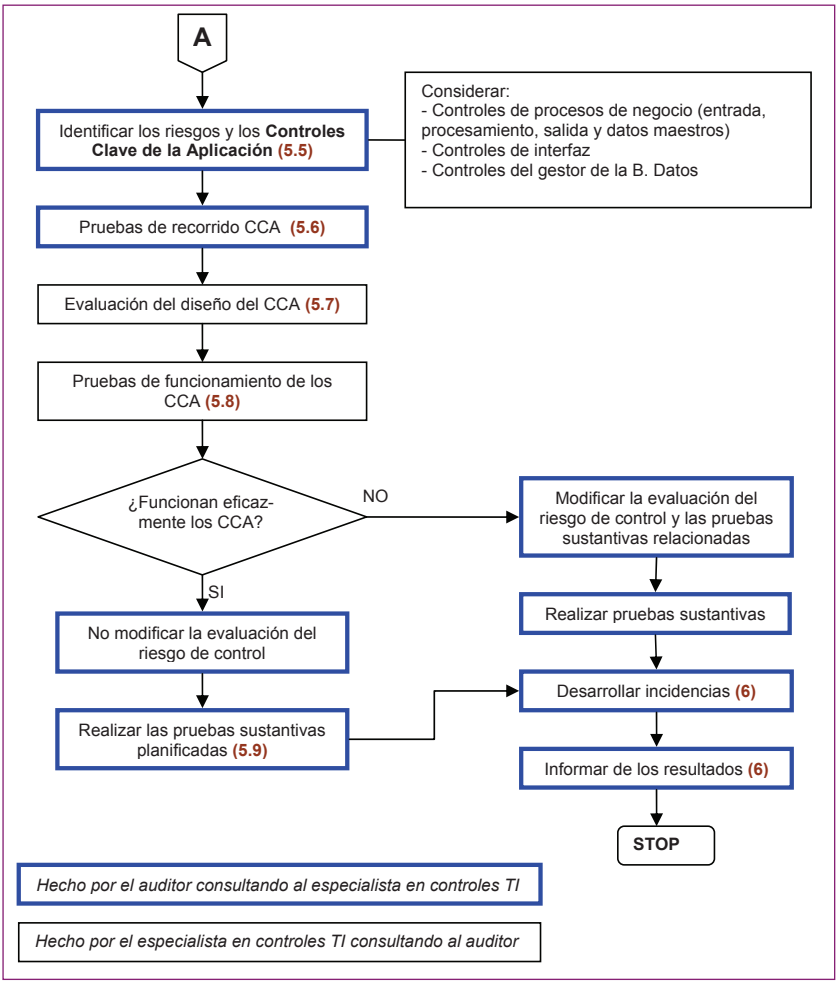


Figura 4.4: Pasos para evaluar los CCA

El auditor puede decidir comprobar la efectividad de los controles generales (figura 4.3) incluso si no es probable que sean efectivos o revisar los controles de aplicación (figura 4.4) incluso cuando los controles generales no sean efectivos, con objeto de hacer recomendaciones para subsanar las debilidades de control.

4.7. Documentación de la planificación

El auditor debe documentar la siguiente información desarrollada en la fase de planificación:

- Los objetivos de la auditoría de sistemas de información y, si forma parte de una auditoría más amplia, una auditoría de financiera de cuentas anuales en el caso más frecuente, una descripción del modo en que tales objetivos apoyan los objetivos globales de la auditoría financiera.
- El alcance de la auditoría de los sistemas de información.
- La comprensión del auditor de las operaciones de la entidad y de los procesos de negocio clave, incluyendo, en la medida en que estén relacionados con los objetivos de la fiscalización, los siguientes aspectos:
  - la importancia y la naturaleza de los programas y funciones respaldados por los sistemas de información;
  - los procesos de negocio clave relevantes para los objetivos de la auditoría, incluidas las reglas de gestión, los flujos de transacciones, así como la interacción de los módulos de aplicaciones y programas informáticos;
  - solicitud de antecedentes;
  - los factores internos y externos importantes que podrían influir en los objetivos de auditoría de sistemas de información;
  - un organigrama detallado, especialmente los componentes de los sistemas informáticos y de los sistemas de información;
  - los cambios significativos en el entorno/arquitectura informática o en las aplicaciones importantes implementadas durante los dos últimos años o que hayan sido planificadas para los próximos dos años; y
  - la confianza/dependencia de la entidad en terceros para proveer servicios informáticos.
- Una comprensión general de la estructura de las redes de la entidad y de sus componentes, como base para poder planificar la auditoría de controles de los sistemas de información, incluidos unos esquemas de alto nivel y también detallados de las redes relevantes para los objetivos de la fiscalización.
- Las áreas clave de interés para la auditoría, incluidos los sistemas de apoyo generales y las aplicaciones y ficheros más importantes. Esto incluye (1) las ubicaciones operativas de cada sistema o fichero clave, (2) los componentes fundamentales de hardware y software asociados (por ejemplo, cortafuegos,

routers, servidores, sistemas operativos), (3) otros sistemas o recursos a nivel de sistema que respalden las áreas clave de interés para la auditoría, y (4) problemas surgidos en auditorías anteriores.

- Una evaluación preliminar de los riesgos de los sistemas de información relacionados con las áreas clave de interés para la auditoría así como su fundamentación. Para cada riesgo identificado, el auditor deberá documentar la naturaleza y alcance del riesgo; las condiciones que causaron dicho riesgo así como la información u operaciones específicas afectadas (si no están generalizadas). El auditor deberá además documentar otros factores que puedan atenuar los efectos de los riesgos detectados.
- La comprensión preliminar de los controles de los sistemas de información, incluida la organización, plantilla, responsabilidades, permisos y recursos de la función de gestión de seguridad de la entidad. El auditor deberá incluir la siguiente información en la documentación de la comprensión preliminar del diseño de los controles de los sistemas de información, en la medida en que sean relevante para los objetivos de la auditoría:
  - Identificación de los controles a nivel de la entidad en su conjunto (así como los adecuados controles a nivel de sistemas) diseñados para llevar a cabo las actividades de control para cada elemento crítico dentro de cada área de controles generales y la decisión sobre si han sido diseñados de manera eficaz e implementados (puestos en funcionamiento), incluida la identificación de las actividades de control para las que no hay controles al nivel de la entidad o éstos son ineficaces así como los riesgos relacionados;
  - Identificación de los controles al nivel de los procesos de negocio para las aplicaciones clave identificadas como de interés para la fiscalización, determinación del lugar donde esos controles son implementados (puestos en funcionamiento) dentro de los sistemas de la entidad, así como la conclusión del auditor sobre si los controles han sido diseñados eficazmente, incluida la identificación de las actividades de control para las cuales no hay controles o de haberlos, éstos son ineficaces y los riesgos relacionados, así como el posible efecto de cualquier debilidad

de diseño identificada sobre la completitud, exactitud, validez y confidencialidad de los datos de la aplicación;

— Cualquier revisión interna o externa de los sistemas de información, auditorías, o pruebas especializadas (p. ej. tests de intrusión, pruebas de recuperación de desastres, así como pruebas sobre aplicaciones específicas) realizadas durante el año anterior;

— Planes de actuación de la dirección e hitos, o sus equivalentes, que identifican las actuaciones correctivas planificadas para abordar las debilidades conocidas de control de los sistemas de información;

— Situación de las incidencias de auditoría de años anteriores;

— Documentación de cualquier incidente significativo informado durante el año anterior relacionado con la seguridad informática;

— Planes de seguridad documentados;

— Evaluaciones documentadas de los riesgos para los sistemas relevantes (p.ej. sistemas de apoyo generales y aplicaciones más importantes)

— Certificación de sistemas y documentación de acreditación o equivalente para los sistemas relevantes;

— Planes documentados de continuidad de negocio y planes de recuperación de desastre; y

— Una descripción del uso por parte de la entidad de servicios informáticos externos.

– Leyes y normativa y su relación con los objetivos de la auditoría, incluida cualquier documentación de consultas a un asesor jurídico.

– Una descripción de los procedimientos utilizados por el auditor para considerar el riesgo de fraude, cualquier factor de riesgo de fraude que el auditor considere que podría influir en los objetivos de la auditoría y en los procedimientos de auditoría planificados para detectar cualquier fraude que pueda ser importante para los objetivos de la auditoría.

– Recursos (personal, herramientas) de auditoría planificados.

– Planes actuales de pruebas para varios años.

– Documentación sobre los contactos establecidos con la dirección de la entidad.

- Si los controles de los sistemas informáticos son llevadas a cabo por empresas de servicios, las conclusiones sobre si dichos controles son significativos para los objetivos de la fiscalización y cualquier procedimiento de auditoría que se lleve a cabo con respecto a tales controles.
- Si el auditor planea utilizar el trabajo de expertos, las consideraciones sobre dicha colaboración planificada y cualquier procedimiento previsto con respecto a la utilización del trabajo de expertos internos o externos.
- Una memoria de planificación que describa adecuadamente los objetivos, el alcance y la metodología de auditoría.
- Cualquier decisión que se haya adoptado para reducir la comprobación de los controles de los sistemas de información como consecuencia de la detección de debilidades significativas en el control de dichos sistemas.

5

Metodología de auditoría de sistemas de información

5.1. Análisis de las cuentas anuales auditadas

5.1.1. Introducción

El análisis del balance, de la cuenta de pérdidas y ganancias y/o de la liquidación del presupuesto u otros estados auditados (en adelante cuentas anuales) es el procedimiento inicial, básico, en una auditoría financiera basada en el análisis de los riesgos, y sirve para identificar los epígrafes del balance, de la cuenta de pérdidas y ganancias y/o del presupuesto sobre los que focalizar el esfuerzo de la auditoría.

Esta actividad conlleva el conocimiento de la actividad y entorno de la entidad durante el ejercicio auditado.

El análisis proporciona al auditor información sustancial para la identificación de los riesgos y de las aplicaciones informáticas con influencia en las cuentas anuales.

Sirve también como instrumento de planificación, ya que ayuda en el proceso de identificar los principales controles internos y los métodos de comprobación a utilizar.

5.1.2. Objetivos

Los objetivos de esta etapa de la auditoría son:

a) Identificar las cuentas y grupos de cuentas significativos a los efectos de la fiscalización o auditoría financiera a realizar.

b) Identificar las transacciones (operaciones comerciales) o clases de transacciones que impactan en las cuentas significativas identificadas.

c) Adquisición de un conocimiento general de la entidad.

5.1.3. Procedimientos de auditoría

a) Adquisición de un conocimiento general de la entidad

El análisis de las cuentas anuales y la identificación de los componentes significativos a los efectos de la fiscalización, es uno de los

pasos iniciales, fundamentales, para planificar eficazmente la fiscalización.

Para realizar este análisis con la máxima solvencia es preciso adquirir un conocimiento de carácter general de la entidad, de su organización y del entorno en el que desarrolla su actividad; conocimiento que en las siguientes etapas irá haciéndose más profundo especialmente en lo relativo a los sistemas contable, presupuestario y de control interno. En las organizaciones modernas, en la medida en que éstos se encuentran soportados por sistemas informáticos cada vez más complejos, se les debe prestar la máxima atención profesional, ya que la complejidad de un sistema de información es un elemento esencial para determinar si es necesario o no la colaboración de un auditor informático en los trabajos de fiscalización.

Debe tenerse presente que la planificación de una fiscalización no es un proceso discreto, sino un proceso continuo en el que si bien la mayor parte de las actividades de planificación se realizan en las primeras etapas de la auditoría, debe reajustarse, siempre que sea necesario, a lo largo del trabajo.

El auditor debe tener en cuenta los principales acontecimientos de la entidad que hayan tenido influencia sobre las cuentas o clases de transacciones seleccionadas. Por ejemplo: la introducción de una nueva aplicación informática; la migración de aplicaciones o de datos, etc.

En esta primera etapa de la auditoría se mantendrán reuniones con el personal de la entidad fiscalizada para explicarles los objetivos y alcances de la auditoría de sistemas de información y se les hará entrega de un cuestionario inicial (ver un modelo en el Anexo 1) para que lo cumplimenten, en el que se solicita una serie de información y documentación relativa a distintos aspectos técnicos y organizativos de los sistemas de información de la entidad.

b) Identificación de las cuentas y grupos de cuentas significativos

Se deben identificar las cuentas y grupos de cuentas significativos (superiores al umbral de importancia relativa fijado en la planificación) y aquellas cuya existencia o evolución futura comportan riesgos específicos a considerar en la fiscalización.

El auditor efectuará una evaluación de los riesgos inherentes y de control que puedan tener una influencia sobre las cuentas anuales y orientará sus procedimientos de auditoría sobre esos riesgos.

c) Identificación de transacciones y de clases de transacciones[55] significativas

Una vez identificadas las cuentas o los grupos de cuentas significativas, sobre las que focalizará su auditoría, el auditor analizará las transacciones que tienen un impacto significativo sobre dichas cuentas, aquellas que generan los importes o saldos que lucen las mismas. La ventaja de este enfoque es que excluye las clases de transacciones no significativas resultantes de la subdivisión de procesos.

Una vez que el auditor conoce las clases de transacciones significativas y las operaciones que las generan, puede proceder al análisis de riesgos en las diferentes fases del proceso de negocio en el que se producen tales operaciones, tal como se describe en el capítulo siguiente.

A los efectos de la auditoría de sistemas de información y la revisión de las aplicaciones TI, el auditor se concentrará generalmente en las transacciones ordinarias o recurrentes puesto que la mayoría son generadas por esas aplicaciones y en ellas tienen lugar la mayoría de controles automatizados ligados a los sistemas informáticos.

Las transacciones no rutinarias, como las estimaciones, operaciones de consolidación, etc. son revisadas normalmente mediante procedimientos sustantivos.

5.2. Identificación de los procesos de negocio de la entidad y de los flujos de datos

5.2.1. Introducción

Las cuentas anuales de una empresa o entidad son el resultado de la agregación de múltiples actividades que se pueden agrupar en procesos, éstos pueden ser muy diferentes unos de otros (procesos complejos, limitados en el tiempo, procesos que pueden afectar a varias transacciones, etc.).

Si existieran debilidades en los procesos de negocio significativos podría cuestionarse la fiabilidad de las cuentas anuales. Por ello resulta indispensable la identificación minuciosa de los procesos de

55. Clases o tipos de transacciones se refieren a las derivadas de actividades de explotación (básicamente ingresos, compras de bienes y servicios, y las del personal), de inversión o de financiación. Suelen ser repetitivas y, a efectos de auditoría, pueden agruparse en ciclos o fases desde el inicio hasta la terminación, o ser tratadas por separado (como por ejemplo cobros o pagos).

Fuente: *Guía de auditoría* del REA.

negocio y de los flujos de procesamiento de datos para poder identificar y evaluar los riesgos en el seno de cada uno de ellos.

La trazabilidad y la fiabilidad de la información producida por un sistema de información financiera son dos elementos clave de los sistemas de control interno. Con esa finalidad hay que conocer a fondo, entre otros, los aspectos siguientes:

- Identificar los flujos de datos. Es necesario tener una visión global de la circulación de los datos a lo largo de todo el proceso analizado, desde su captura inicial, tratamientos, hasta su archivo final. Esta visión se desprende del análisis de los procesos, incluyendo la identificación de las bases de datos que intervienen y las operaciones que se realizan para transferir los datos procesados y las operaciones que se realizan para transferir los datos de una base de datos a otra.
- Identificar los controles. A lo largo del flujo de los datos a través del proceso se establecen una serie de controles sobre la integridad, confidencialidad y disponibilidad de los datos (este aspecto se estudia en los siguientes capítulos de este trabajo).
- Revisar pistas de auditoría (trazabilidad). La finalidad es localizar una información o un dato a partir de otro, resultante de una aplicación informática lógica y físicamente alejada. Así, es posible por ejemplo, a partir del saldo de una cuenta del balance, obtener un detalle de sus movimientos, y de cada uno de éstos el apunte contable realizado y la referencia a los documentos que originaron el movimiento contable. La ausencia de pistas de auditoría es una debilidad del control interno.

5.2.2. Objetivos

Los objetivos de esta etapa de la auditoría son:

- Comprender la actividad de la entidad y los principales procesos de negocio.
- La identificación de los procesos de negocio que están en el origen de las transacciones y clases de transacciones significativas identificadas en la etapa anterior.

5.2.3. Definiciones

Un proceso de negocio o proceso de gestión consiste en una serie de actividades, operaciones o funciones (manuales, semiautomáticas o

automatizadas) llevadas a cabo por una entidad, que sirven para llevar a cabo su misión y desarrollar su actividad (la elaboración de productos o el suministro de servicios) o el tratamiento de la información. Un proceso tiene un punto de inicio y otro de finalización claros y generalmente intervienen varios departamentos de la entidad.

Los procesos de negocio pueden clasificarse en tres grupos:

- Procesos relacionados con la misión o actividad de la entidad: gestión de subvenciones, gestión de historias médicas, tramitación del IRPF, matriculación universitaria, compras, ventas, etc.
- Procesos financieros: cobros, pagos, nóminas, etc.
- Procesos de apoyo: que agrupan todas las funciones de apoyo a la puesta en marcha y a la explotación de los procesos operativos: gestión de recursos humanos, mantenimiento de inventario de inmovilizado, contabilidad, etc.

Un subproceso o función es un subconjunto de actividades o tareas, realizadas por un empleado o funcionario para llevar a cabo una parte de sus responsabilidades, que producen un resultado u output.

Por procesos de negocio significativos, a los efectos de la auditoría, se entiende los principales procesos que tienen una influencia directa sobre el flujo de tratamiento contable y la formación o valoración de componentes significativos de las cuentas anuales.

Una aplicación de negocio es una combinación de hardware y software usada para procesar información de la actividad de la entidad. Puede dar soporte a uno o varios procesos de negocio.

5.2.4. Procedimientos de auditoría

a) Comprensión de la actividad de la entidad

Comprender la actividad y el funcionamiento de la entidad (tarea ya iniciada en la etapa anterior) y de los principales procesos de negocio, incluye entender cómo se emplean las aplicaciones informáticas para soportar los procesos de negocio, ya que tiende a variar de una entidad a otra.

b) Identificación de los procesos de negocio significativos

Partiendo de las clases de transacciones significativas identificadas en la etapa anterior, el auditor debe identificar los procesos de negocio significativos que influyen en sus importes o en sus saldos contables.

El concepto de materialidad tratado en el capítulo 4.5, puede ayudar al auditor a determinar qué componentes de las cuentas anuales y que aplicaciones relacionadas son significativas para los objetivos de la auditoría.

Para comprender mejor la actividad de la entidad es conveniente desagregar los procesos complejos en subprocesos.

Veamos varios ejemplos:

Procesos	*Subprocesos*
Gastos de personal	Aprobación RPT Modificación RPT Altas de personal Elaboración de la nómina Pago nómina Contabilización de la nómina
Compras	Gestión de datos maestros de proveedores Gestión de datos maestros de materiales Mantenimiento de contratos marco Gestión de compras Entrada de mercancías Recepción de facturas Gestión de pagos Contabilización de compras Imputación de costes
Concesión de subvenciones[56]	Inicio Instrucción Finalización Pago
Ventas-facturación	Gestión de datos maestros de clientes Gestión de datos maestros de productos Mantenimiento de contratos marco Gestión de ventas Gestión de inventario y entrega Emisión de facturas Gestión de cobros Contabilización de ventas
Concesión de préstamos	Solicitud Aprobación Transferencia del efectivo

El análisis a realizar se extiende, tanto al proceso contable mismo como al proceso puntual de cierre de las cuentas anuales; a proce-

56. Obtenido de un caso real. Véase la página 508 del informe de auditoría de los sistemas de información de la gestión de las subvenciones en 2007 del IMPIVA elaborado por la Sindicatura de Cuentas de la Comunidad Valenciana, (www.sindicom.gva.es).

sos de negocio complejos como el de ventas-facturación, que tiene influencia en el flujo de mercancías y en el flujo financiero (en este caso varias cuentas del balance y de la cuenta de pérdidas y ganancias tienen el mismo proceso como fuente u origen de sus datos); y a los procesos de apoyo, como por ejemplo los del área de recursos humanos.

Los procesos pueden ser representados como un mapa de procesos en un gráfico o en una tabla. Estas formas de presentación tienen ventajas que puede ser útil combinar cuando se presentan interacciones complejas entre distintos procesos.

Al realizar este análisis, se debe aprovechar la documentación descriptiva de los procesos de negocio que exista en la empresa o entidad auditada. Normalmente esta documentación se centra en las actividades y es preciso completarla para cada etapa del proceso con las entradas de datos, los tratamientos de datos y los resultados, así como los roles de los distintos agentes que intervienen.

En general, la documentación de la empresa no señalará los riesgos de los procesos y ni los controles clave, que deberán ser identificados y documentados por el auditor en una fase posterior, al analizar los controles de las aplicaciones.

c) Presentación de la información en forma de tabla

Esta forma de presentación puede ser aplicable en procesos de negocio y en entornos informatizados simples.

Ejemplo: En una empresa distribuidora de un producto

Epígrafe de las CCAA	Importe (Mill. euros)	Proceso	Input	Output
Ventas	650,7	Ventas/ Facturación	Contratos y pedidos	Facturas
Compras	390,0	Aprovisionamiento	Pedidos	Alta inventario
Gastos de personal	92,1	Gestión personal	Plantilla	Nómina
Amortizaciones	20,0	Cierre contable	Inventario de inmovilizado	Amortizaciones

Figura 5.1

d) Presentación gráfica mediante un mapa general de procesos

Un mapa general de procesos es una descripción de las actividades, funciones y procesos de negocio llevados a cabo por la entidad auditada.

Es una herramienta que facilita la comprensión por todos los miembros del equipo de auditoría de las actividades que desarrolla la entidad auditada y de los flujos de documentos y datos. También facilita la posterior identificación y evaluación de los riesgos y controles clave que existen en un determinado proceso o función.

Al preparar los mapas de procesos, hay que tener presente cuál es el propósito de su elaboración:

- Si se está elaborando el mapa de procesos general de la entidad, cuyo propósito principal es servir para la planificación del trabajo, solo recogerá los principales procesos, no se requiere un detalle excesivo, y puede caber en una página.
- Si se va a elaborar el mapa de un proceso de negocio en particular, que va a ser objeto de revisión, el grado de detalle e información requerido es muy superior.

Los mapas generales de procesos y los mapas individuales de un proceso/subproceso también denominados *flujogramas* pueden usarse para:

- Facilitar la comprensión de la actividad de la entidad
- Establecer alcances al planificar auditorías basadas en el enfoque de riesgos
- Identificar riesgos
- Identificar y documentar los controles internos
- Servir para la formación del personal
- Aumentar la eficiencia en el diseño de controles
- Puede también usarse por la entidad para tomar decisiones relacionadas con el diseño de nuevos sistemas y con cambios y reorganizaciones de determinadas actividades.

Elaboración de un mapa general de procesos y aplicaciones

Adquirir un conocimiento profundo de un proceso de negocio implica documentarlo teniendo en cuenta su complejidad, para ello se debe:

1.º Elaborar un mapa general de procesos, que permite tener una visión de conjunto de la actividad y del funcionamiento de la entidad.

2.º Elaborar una representación detallada de cada proceso, mediante diagramas que muestran el encadenamiento de las actividades y los principales flujos de datos, las tareas manuales y automatizadas.

Conviene distinguir los procesos de negocio (p.e. ventas) de los procesos financieros y de apoyo, a veces muy puntuales (p.e. consolidación mensual de las cifras de delegaciones; cálculo anual de las amortizaciones). Ambas categorías de procesos comportan riesgos susceptibles de materializarse en las cuentas anuales.

Aunque la elaboración de un mapa general de procesos y aplicaciones puede realizarse de distintas formas, siempre debe hacerse de forma conjunta por el auditor financiero y el auditor informático, ya que es necesario adoptar un enfoque pluridisciplinar para obtener la máxima comprensión del sistema de información financiera auditado.

La documentación debe elaborarse con claridad, de forma consistente, empezando por una visión general y ampliando el grado de detalle hasta llegar a la descripción de los procedimientos de control.

Cuestiones a preguntar

Para documentar el trabajo y elaborar un mapa de procesos se debe obtener información mediante entrevistas a los responsables de los principales procesos de negocio y al personal que interviene en los mismos. Estas últimas es mejor posponerlas hasta que se haya obtenido una visión de alto nivel de cada proceso completo; si se entrevista al personal que interviene en un proceso antes de que el auditor lo comprenda, se corre el riesgo de describir mucha más información de la necesaria, perder mucho tiempo y ser ineficiente.

En las entrevistas iniciales es necesario que las preguntas se dirijan a obtener información relevante, que permita comprender el negocio y crear un diagrama completo y de alto nivel del proceso revisado.

Se deberá obtener una visión global de los objetivos del negocio o actividad de la entidad, sus principales funciones, principales sistemas, relaciones críticas, interdependencias, cómo se generan los ingresos, principales tendencias de la actividad.

Un inventario así elaborado constituye una base de trabajo indispensable que permitirá a los auditores financieros e informáticos poner en común sus análisis de los riesgos, identificar los flujos de datos e información, iniciar la elaboración del mapa de procesos y concretar los procedimientos de auditoría a efectuar.

Uso de cuestionarios o checklist

En lo que respecta al auditor informático, lo más efectivo es, tras la reunión inicial con los máximos responsables de la entidad, incluyendo el departamento TI, entregar un cuestionario con aspectos generales de la función informática adaptado a la entidad, para que el responsable del departamento de sistemas informáticos lo cumplimente (ver un modelo general en el Anexo 1). Posteriormente la información se completará con otras entrevistas.

Este cuestionario también será útil para la posterior revisión de los controles generales.

Aspectos técnicos

Para efectuar un mapa general es conveniente identificar el perímetro de las funcionalidades instaladas y parametrizadas por la entidad:

- Se puede revisar la documentación proporcionada por el fabricante del ERP e identificar con la empresa los módulos que han sido instalados y parametrizados. Algunos ERP, proporcionan esta información en un módulo de administración.
- También se puede revisar el contrato de licencia, que generalmente detalla los módulos adquiridos y puede también proporcionar información sobre los perfiles de usuario (parametrizaciones, utilización, consultas). Algunos ERP son instalados de forma estándar con todos los módulos, incluso si la empresa solo utiliza una parte.

La información obtenida permite identificar los elementos sensibles que pueden ser objeto de una revisión más detallada, por ejemplo los puntos de integración entre los distintos módulos (también denominados interfaces internas, para diferenciarlas de las interfaces externas que permiten a un ERP comunicarse con otros sistemas).

Ejemplo de Mapa general de procesos de una empresa, en un caso de interacciones complejas:[57]

57. Fuente: *Prise en compte de l'environnement informatique et incidence sur la démarche d'audit*, Collection guide d'application, Compagnie Nationale des Commissaires aux Comptes, abril de 2003.

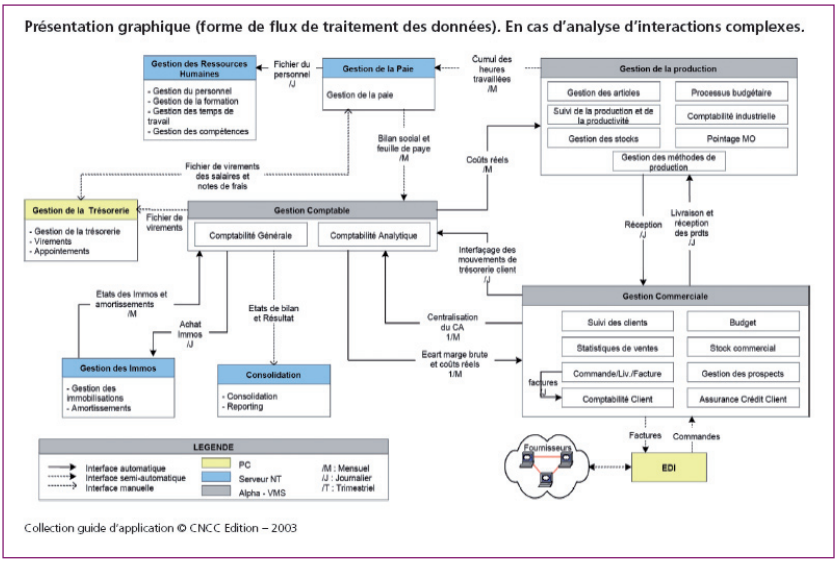


Figura 5.2

e) Obtención de un conocimiento general de la estructura de redes y comunicaciones de la entidad

Debe obtenerse y documentarse un conocimiento general de la estructura de redes y comunicaciones de la entidad de forma que se pueda planificar la revisión de los controles generales.

Este conocimiento incluirá una visión de alto nivel de la arquitectura de las redes que utiliza la entidad en sus procesos de negocio significativos y ayudará al auditor de sistemas de información a evaluar los riesgos, identificar posibles controles clave, identificar las tecnologías que pueden ser objeto de auditoría y, en su caso, los centros a visitar.

Normalmente en la primera petición de información se incluirá la relativa a estas cuestiones, en particular esquemas generales y detallados sobre la estructura de redes y comunicaciones e información como la siguiente:

- Presencia en Internet.
- Firewalls, routers y switches.
- Sistemas de detección y prevención de intrusiones.
- Sistemas críticos: web, correo electrónico, FTP, etc.
- Sistemas de gestión de la red.
- Conexiones a otros sitios internos o entidades externas.

– Acceso remoto (VPN y dial-in).
– Conexiones wireless.

Se solicitarán y/o elaborarán diagramas de la estructura de redes y comunicaciones de la entidad.

Ejemplo de diagrama de una red sencilla:

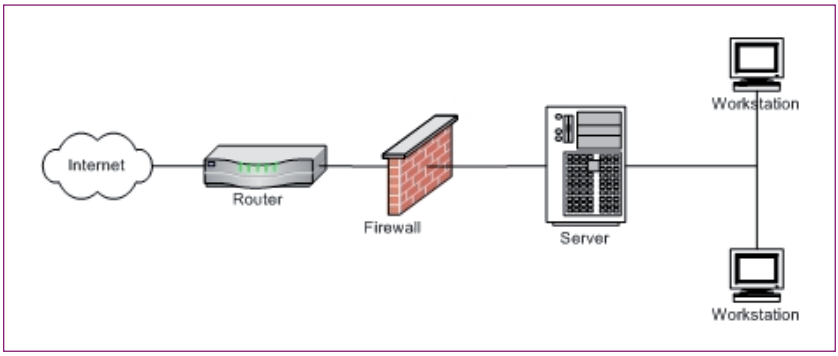
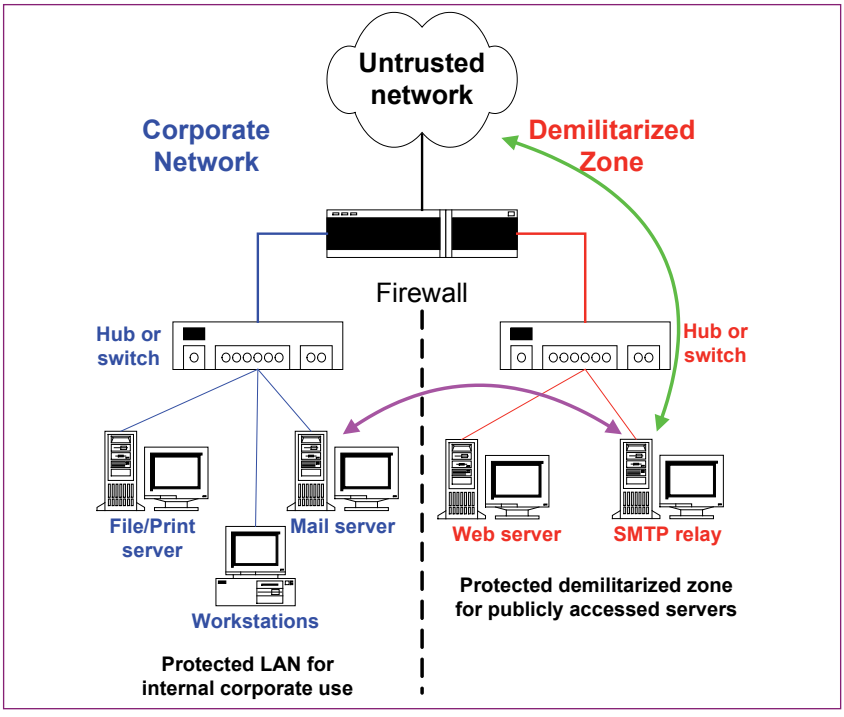


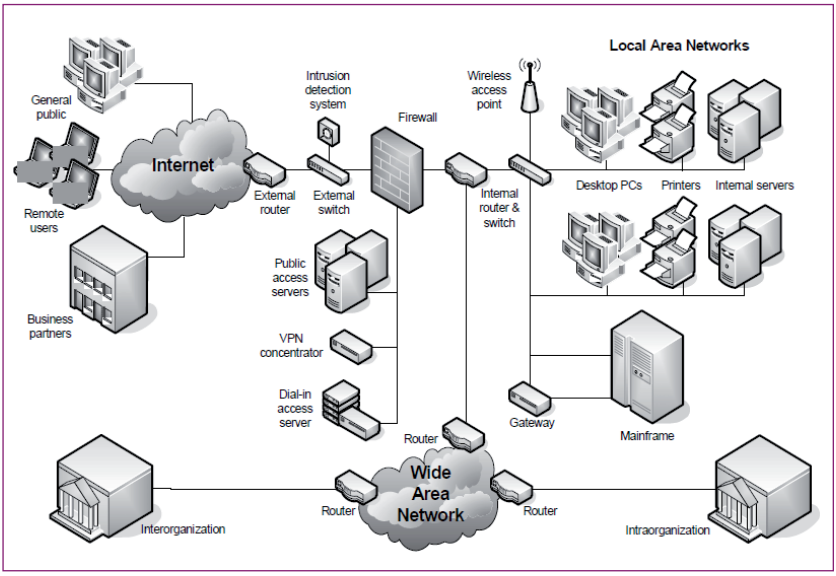
Figura 5.3

Ejemplo de diagrama de una instalación media:



Fuente: NAO Audit Briefing: Firewalls, enero 2004
Figura 5.4

El siguiente esquema representa una instalación típica de una entidad de mayor tamaño:



Fuente: FISCAM GAO, página 35.
Figura 5.5

5.3. Identificación de las aplicaciones de negocio significativas y de las principales interfaces

5.3.1. Introducción

Los procesos de negocio, tal como se han definido en el capítulo anterior, están soportados por aplicaciones informáticas, que pueden tener una mayor o menor complejidad y grado de integración, según los casos.

La automatización e integración de las distintas fases de los procesos de negocio y de numerosos controles internos en un sistema de información plantea riesgos inherentes adicionales. Pueden presentarse, por ejemplo, dificultades para implementar una adecuada segregación de funciones; también si el nivel de integración es muy elevado, los datos se procesan en tiempo real o se aplica el principio de «entrada única de datos», se generarán procesos y registros automáticos de transacciones que provocarán que pueda ser imposible que existan controles humanos (ver capítulo 3.4.5).

Las aplicaciones de gestión integradas, en particular los ERP, condicionan profundamente la manera de trabajar y determinan la

forma en la que se hacen los intercambios entre los distintos agentes, contribuyendo a la estructuración de los procesos de negocio.

La identificación de las aplicaciones de negocio significativas para los propósitos de la auditoria financiera, sus características y sus interfaces, se debe hacer lo antes posible, ya que esta información permitirá definir de forma detallada el diseño, alcance y la extensión de las pruebas de auditoría, el grado de participación requerido del auditor informático y la elaboración de los programas de auditoría.

Las interfaces entre aplicaciones y entre bases de datos requieren una atención especial, en particular las relacionadas con aquellas aplicaciones con impacto en las cuentas anuales.

5.3.2. Objetivo

El objetivo de esta etapa de la auditoría es:

– La identificación de las aplicaciones de negocio significativas para los objetivos de la fiscalización y de sus interfaces.

5.3.3. Procedimientos de auditoría

a) Identificar las aplicaciones significativas y sus interfaces

Aplicaciones de negocio

Una aplicación de negocio es una combinación de hardware y software usada para procesar información de la actividad de la entidad y da soporte a uno o varios procesos de negocio.

Una aplicación es por lo general significativa a los efectos de la auditoría financiera si procesa transacciones agregadas superiores al nivel de importancia relativa fijado en la memoria de planificación o si respalda un saldo contable significativo de las cuentas anuales auditadas.

Un sistema de información financiera generalmente comprende varias aplicaciones contables informáticas.

El auditor también puede identificar aplicaciones contables como significativas basándose en consideraciones cualitativas. Por ejemplo, sistemas que respaldan la planificación financiera, los informes de gestión y actividades presupuestarias; sistemas que gestionan y proporcionan datos e información de costes; y sistemas que gestionan aspectos relacionados con el cumplimiento de la legalidad (contratación, subvenciones, etc.).

El sistema de información financiera de la entidad puede ser visto como una serie de agrupamientos lógicos de transacciones y activi-

dades relacionadas y de aplicaciones informáticas. Cada partida presupuestaria o cuenta significativa puede estar afectada o influida por inputs de una o varias aplicaciones (origen de cargos y abonos).

Interfaces

Un análisis completo de un sistema de información debe tener en cuenta tanto los flujos de datos y documentos como las interfaces.

Una interfaz es una conexión entre dos dispositivos, aplicaciones o redes, mediante la que se intercambia información. También se utiliza este término para referirse a la parte de un programa que interactúa con el usuario (la interfaz de usuario).

El objetivo de esta etapa de la auditoría es comprender los flujos de la información y de los datos entre distintas funciones, aplicaciones o sistemas, no solo electrónicos sino también manuales. Las interfaces entre aplicaciones y entre bases de datos requieren una atención especial, en particular las relacionadas con aquellas aplicaciones con impacto en las cuentas anuales.

Incluso los entornos ERP muy integrados a menudo requieren complicadas interfaces para intercambiar información con otras aplicaciones distribuidas, como los sistemas de internet.

Las interfaces suelen ser gestionadas con tecnología middleware,[58] que actúa como un elemento central de comunicación y coordinación de aplicaciones, bases de datos e interfaces.

A pesar de que las interfaces y el middleware juegan un importante papel en el proceso de las transacciones, en muchos casos no se incluyen, erróneamente, en el plan de la auditoría. Debe tenerse presente que su mal funcionamiento puede afectar a todo el sistema, lo que representa un riesgo a considerar.

b) Información a obtener sobre las aplicaciones de negocio e interfaces

Basándose en entrevistas mantenidas con el personal de la entidad y con otra información obtenida, el auditor determinará las aplicaciones TI que son la fuente de la información de las cuentas anuales.

Por ejemplo, las aplicaciones que contienen registros auxiliares de las cuentas a cobrar, inmovilizado y cuentas a pagar, por lo general ofrecen información detallada para pruebas y respaldo para los saldos

58. Middleware: Software que permite la compatibilidad entre las infraestructuras tecnológicas (fundamentalmente los SGBD) y las aplicaciones de negocio. También permite la intercomunicación de datos entre aplicaciones o sistemas diferentes.

de los libros mayores, si se llevan a cabo unos controles (por ejemplo: reconciliaciones) adecuados.

Cuando una cuenta significativa tiene más de una fuente de información financiera, el auditor debe considerar las distintas fuentes y determinar cuál de ellas es la más apropiada para los propósitos de la auditoría financiera. El auditor debe evaluar la probabilidad de manifestaciones erróneas y la auditabilidad al elegir la fuente que va a utilizar. Para los propósitos de la auditoría, la mejor fuente de información financiera a veces puede ser información operativa elaborada fuera del sistema contable.

El auditor debe obtener un conocimiento suficiente de los sistemas de información relevantes para la información financiera para entender el diseño de los procedimientos. Debe obtener y revisar documentación, como pueden ser documentos de diseño, proyectos, procedimientos de los procesos de negocio, manuales de usuario, etc. Debe también entrevistarse con el personal con conocimientos a fin de obtener una comprensión general de cada aplicación de negocio significativa para los objetivos de la auditoría.

Después de identificar las aplicaciones significativas e interfaces, el auditor debe obtener un conocimiento suficiente de las mismas y de los procedimientos (incluyendo los componentes del control interno) mediante los cuales las transacciones son iniciadas, registradas, procesadas y presentadas desde el momento en que acontecen hasta que son incluidas en las cuentas anuales y documentar los siguientes aspectos:

Para cada aplicación significativa

- Procedimientos por los que se inician las transacciones, se autorizan, registran, procesan, acumulan y se muestran en las cuentas anuales, incluyendo el tipo de archivos informáticos y la forma en que se puede acceder a ellos, actualizarlos y borrarlos.
- Naturaleza y tipo de los registros, listados contables, documentos fuente y cuentas relacionadas.
- Entorno técnico y sistemas informáticos asociados a cada aplicación.
- Procedimientos para subsanar el procesamiento incorrecto de transacciones.
- Procesos por los que se capturan hechos y condiciones diferentes de los ordinarios.

– Estimación de los volúmenes tratados.
– Tipo de control de acceso.
– Persona responsable de la aplicación.
– Los flujos de transacciones (estudio detallado de los controles internos de la entidad sobre una categoría concreta de hechos que identifica todos los procedimientos y controles clave relacionados con el procesamiento de transacciones), y
– La interacción de la aplicación y software (las transacciones dejan un sistema para ser procesadas por otro, por ejemplo, interfaces de tarjetas de registro horario de personal con el fichero de salarios y complementos para determinar la información de la nómina.

Alcanzar una comprensión de todo esto es fundamental para poder evaluar el riesgo del sistema de información, comprender los controles de aplicación, así como desarrollar los procedimientos de auditoría pertinentes.

Además de efectuar una nota descriptiva, será útil completar una tabla resumen con la información que se muestra en el ejemplo de la figura siguiente.

Cuentas anuales		Aplicaciones				Bases de datos		Sistemas operativo		Plataforma hardware
Epígrafe	Importe (Millones de euros)	Proceso	Aplicación utilizada	Tipo de aplicación	Responsable	Versión	Administrador	Versión	Responsable	
Ventas - Facturación	650,7	Ventas/ Facturación	Ticketing	Desarrollo propio	J. Gómez	Oracle 9i v9.2.0		Solaris 3.2		HP9000
Contabilidad	—	Contabilidad	SAP R/3	Estándar	A. Arias	DB2 400		OS400		AS400
Compras	390,0	Aprovisionamiento	SAP R/3	Estándar	M. Pérez	DB2 400		OS400		AS400
Gastos de personal	92,1	Gestión personal	People Soft	Estándar adaptada	A. Martín	Oracle 9i v9.2.0		W Server 2003		HP9000
		Control de presencia	WinPlus	Estándar	A. Martín	Oracle 9i v9.2.0		W Server 2003		HP9000
Amortizaciones	150,0 20,0	Cierre contable	Access 2007	Ofimática	A. Arias	Access 2007		W Vista		PC

Figura 5.6. Ejemplo de inventario de aplicaciones y capas tecnológicas

En esta tabla se intentará relacionar las principales cuentas o epígrafes de las cuentas anuales con su correspondiente proceso de

negocio, las aplicaciones de negocio que lo soportan y otros datos relacionados.

Para cada interfaz:

- Tipo (manual o automática).
- Aplicaciones origen (de los datos) y destino.
- Frecuencia de uso (diario, mensual, anual).
- Controles implantados para detectar anomalías.
- Otros aspectos relevantes (ver capítulo 7.4).

Para su análisis inicial y documentación puede realizarse un inventario de las principales interfaces mediante una tabla:

Nombre de interfaz	Tipo	Aplicaciones		Tipo de flujo	Frecuencia	Listas de error	Evaluación de los riesgos
		Origen	Destino				

Figura 5.7

5.3.3. Documentación del trabajo

a) Memorandos o notas descriptivas

El auditor debe preparar suficiente documentación, que describa claramente el sistema de información contable, y que incluya evidencia sobre la implementación de los controles.

Para cada proceso o aplicación significativa, el auditor preparará unas notas descriptivas, que podrán incluir tablas informativas y flujogramas (o mapas de procesos).

Una buena descripción debe:

- Identificar el proceso de negocio y las aplicaciones informáticas que lo soportan.
- Describir las interfaces con otros procesos/aplicaciones
- Identificar los epígrafes de las cuentas anuales, manifestaciones y cuentas afectadas por el proceso.
- Describir las políticas y procedimientos de la entidad relacionadas con el proceso de negocio descrito.
- Identificar (de forma preliminar) los principales controles internos.

Se podrán utilizar tablas para reflejar esta información, como las vistas en el apartado anterior.

b) Presentación de la información en forma de flujogramas o mapas de procesos

Los sistemas de información complejos pueden ser difíciles de entender si no se describen mediante un mapa general de procesos/aplicaciones y con flujogramas o mapas individuales detallados. Por eso, normalmente la mejor forma de describir un sistema es mediante el uso de memorandos o notas descriptivas, que pueden incluir tablas informativas, a las que se adjuntarán las representaciones gráficas del sistema.

Los flujogramas o mapas individuales de aplicaciones son un buen mecanismo para documentar un proceso y el flujo de transacciones a través del sistema, complementando la información descrita en los memorandos o notas descriptivas y resume los flujos en términos de:

- Inputs.
- Informes emitidos.
- Pasos del procesamiento de los datos
- Archivos y bases de datos usadas.
- Unidades involucradas.
- Interfaces con otros procesos y aplicaciones.
- Principales controles.

Son herramientas que permiten tener una visión general del sistema de información de la entidad, con la finalidad de comprender su funcionamiento más fácilmente y ayudan a diseñar los procedimientos de auditoría a efectuar.

Un mapa de procesos proporciona una sinopsis de las actividades clave realizadas en el proceso revisado y debe permitir identificar los principales riesgos y las funciones que requieren atención especial. Pueden abarcar varios departamentos.

Pueden acompañarse de información complementaria sobre los controles (como una tabla de segregación de funciones). La combinación de ambas herramientas (gráfico y tabla) proporciona una gran información sobre un determinado proceso.

Un ejemplo de flujograma que representa un proceso específico puede verse en las figuras 4.3 y 4.4, que representan el proceso de una auditoría.

La elaboración de un mapa de procesos (general o específico) es un proceso iterativo que se inicia elaborando un borrador y puede

ir perfeccionándose a lo largo de la auditoría. No debe esperarse obtener un mapa completo al primer intento.

Grado de detalle

Como ya hemos señalado en el capítulo anterior, la elaboración de un mapa de procesos puede realizarse con carácter general cuando abarca todo el sistema de información de una entidad, y será necesariamente de carácter menos detallado, o puede tratarse de un mapa específico de un proceso o aplicación en particular que contendrá un mayor grado de detalle, que es el que se va a comentar aquí.

A la hora que obtener información hay que buscar un equilibrio en cuanto a la cantidad a manejar, ya que una descripción muy general de un proceso de negocio hace difícil la identificación de los riegos y llegar a conclusiones precisas.

Inversamente un alto grado de detalle puede volver los flujogramas confusos y difíciles de seguir, perjudicando su lectura, comprensión y análisis posterior, además de hacer perder tiempo y dinero innecesariamente.

El grado de detalle requerido variará en función de los objetivos del trabajo, del tamaño y complejidad de la entidad auditada; debe ser el suficiente para:

- Describir el proceso de negocio de principio a fin en una hoja de papel.
- Permitir la identificación de los principales riesgos y controles.
- Permitir el diseño de una prueba de recorrido para comprobar la exactitud de la descripción.
- Desarrollar los distintos pasos de las pruebas a realizar.
- Concretar el alcance del trabajo y la participación de personal especializado.

Según la complejidad de un proceso puede ser útil dividir el mapa del proceso en subprocesos.

Deben priorizarse los procesos y controles de la entidad auditada, y documentar con mayor detalle los más relevantes para la información financiera.

Cómo elaborar un mapa de procesos

Al elaborarlo, se tendrán en cuenta las siguientes consideraciones:[59]

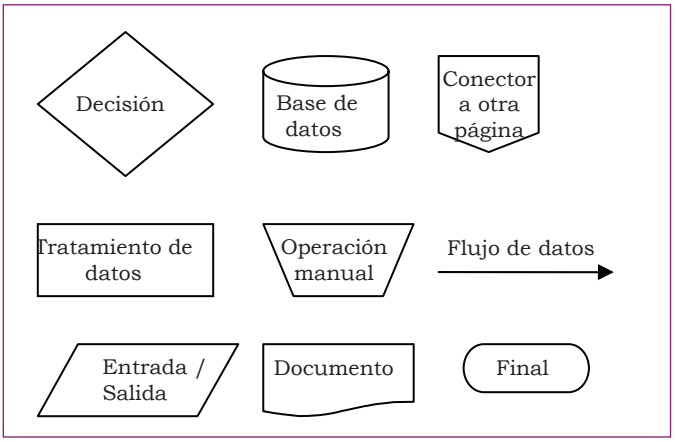
59. *Process mapping – The updated form of flowcharting*, Ann Butera, The Whole Person Project Inc., 2003.

- Definir el proceso que se va a representar, con base en la información obtenida de la entidad.
- Hay que tener y dejar claro el proceso a revisar, ya que esto ayuda a determinar su punto inicial y final.
- Pensar cuidadosamente sobre el grado de detalle que se quiere dar a cada actividad importante. Los procesos (representados por cuadrados) en un mapa general (ver figura 5.2), normalmente se podrán representar mediante un flujograma detallado y se corresponderán con áreas de auditoría. Los departamentos de la entidad no se corresponden con los cuadrados.
- Al elaborar un mapa individual, hay que determinar cómo (y cuánto) se desea desagregar las funciones o subprocesos que forman el proceso auditado. Una función[60] consta típicamente de los siguientes atributos:
  - — Como un proceso, tiene un punto de inicio y otro de terminación, así como inputs y outputs.
  - — Puede transcurrir de forma independiente o simultánea con otras actividades.
  - — Consiste en múltiples y distintas actividades o pasos.
  - — Las actividades que forman una función son, de ordinario, la responsabilidad de una persona en concreto o de un equipo de trabajo.
- Se debe comenzar dibujando los principales pasos que forman el proceso:
  - — Hay que identificar el punto de inicio del proceso y los inputs principales.
  - — Hay que identificar el punto final del proceso y los outputs principales.
  - — Hay que identificar, en orden secuencial, las principales actividades u operaciones que se producen entre los dos puntos anteriores, incluyendo los sistemas informáticos usados en el proceso. Se representan con cuadrados.
  - — Se debe documentar solo las funciones o actividades reales, no las planeadas o previstas.

60. Una función o subproceso es un subconjunto de actividades o tareas realizadas por un empleado para llevar a cabo una parte de sus responsabilidades, y producen un resultado o output.

— Se puede documentar con descripciones o símbolos, o una mezcla de ambos, que resulta más recomendable.

– Los símbolos más usualmente utilizados son los siguientes:



Además de estos símbolos que representan los distintos puntos y actividades del proceso de negocio, posteriormente, al identificar los riesgos y controles, se deberá señalar su ubicación en el proceso/flujograma, por ejemplo así:

Riesgo: **R001**

Control clave: **C001**

En ambos casos se deben marcar con un código que permita identificarlos y describirlos posteriormente.

– Determinar si el flujograma contiene suficiente información para planificar el trabajo. Revisarlo y completarlo cuando sea necesario. Considerar las decisiones básicas que son adoptadas en las principales actividades. Si no se está seguro se debe consultar al personal responsable de la entidad.

– Considerar si la información que contiene el mapa del proceso es adecuada para proceder a la siguiente fase de la auditoría: la evaluación de los riesgos.

– En cada mapa de procesos debe señalarse claramente cuál es el proceso o función representado. También debe documentarse las personas que han intervenido en su elaboración y la fecha de creación y modificación.

– Una vez completado, debe contrastarse la exactitud del mapa revisándolo con las personas que realizan las actividades descritas en el mismo. Se debe contrastar con todos los depar-

tamentos afectados. Si se trata de mapas generales se deben comentar con los máximos responsables de la entidad.

– Identificar los «huecos» en el proceso por existir funciones desconocidas. Estas áreas deben completarse hablando con el personal de las mismas. Si los huecos no pueden completarse son indicios de posibles problemas de auditoría.
– Comparar el mapa con los procedimientos escritos.

Ejemplo de flujograma para un subproceso de solicitud de ayudas en un ayuntamiento:

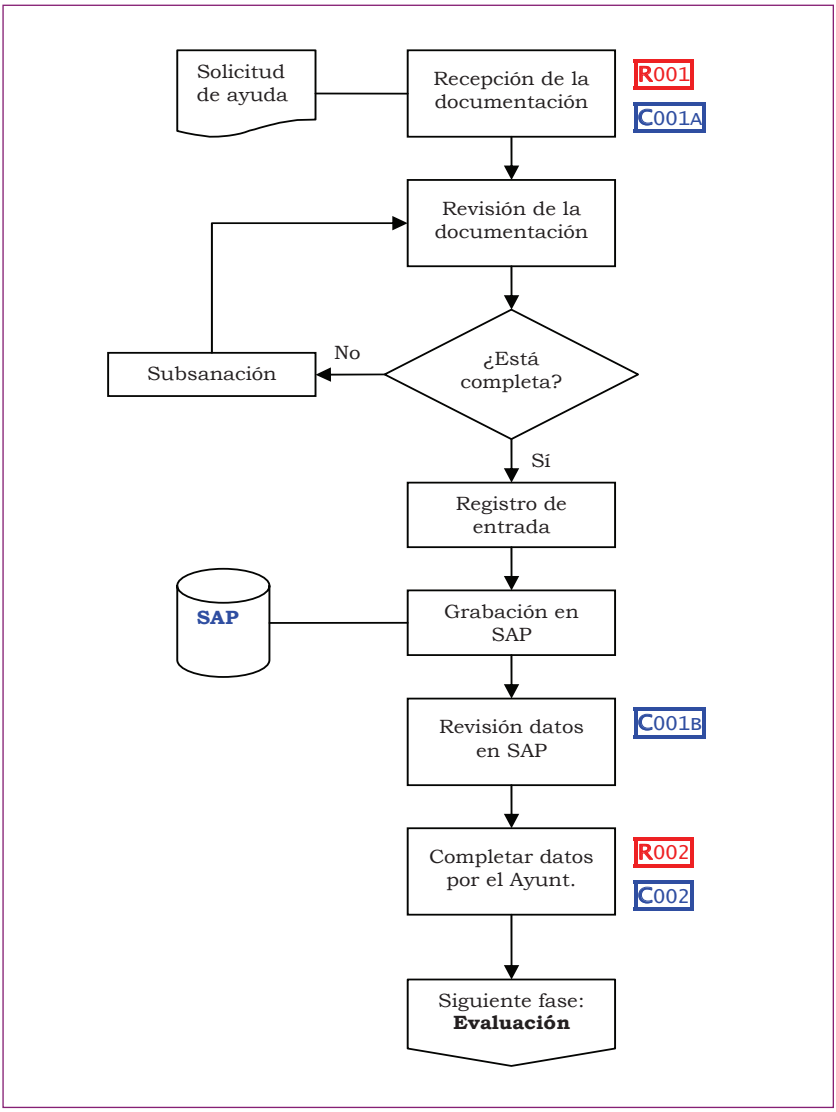


Figura 5.8

Deben señalarse en el flujograma y anotarse para su posterior análisis los riesgos y controles identificados en esta fase. Posteriormente se completará esta información.

Riesgos		Controles clave	
R001	Los datos introducidos en la solicitud no son válidos	C001A	El formulario que debe utilizarse, se descarga de la página web y tiene controles para la mayoría de campos.
		C001B	Una vez registradas las solicitudes se realiza una revisión de los todos los datos para comprobar su validez.
R002		C002	

Figura 5.9

5.3.4. Otros aspectos a considerar

a) Externalización y descentralización

La externalización de áreas de actividad o de procesos de negocio comporta riesgos inherentes y riesgos de auditoría suplementarios considerando la delegación o transferencia de responsabilidad. En estos casos deberá aplicarse la Norma Técnica de Auditoría sobre consideraciones relativas a la auditoría de entidades que exteriorizan procesos de administración aprobada el 26 de marzo de 2004 por Resolución del ICAC.

Otro aspecto a considerar es que la utilización descentralizada de una aplicación comporta riesgos inherentes y riesgos de auditoría suplementarios que aumentan la complejidad de la auditoría.

b) Tipos de aplicaciones significativas para los propósitos de la auditoría financiera

Se pueden distinguir los siguientes tipos de aplicaciones de negocio:

- Aplicaciones estándar.
- Aplicaciones estándar muy adaptadas.
- Desarrollos internos.

Considerando que sus perfiles de riesgo son muy diferentes, conocer los tipos y características de las aplicaciones implicadas es una información importante para la planificación y la realización de la auditoría.

En el capítulo 7 se analizan las diferencias entre los distintos tipos de aplicaciones.

c) Gestión de los parámetros y de los datos maestros

En ciertos procesos de negocio, es aconsejable considerar la gestión (primera grabación, cambios y borrados) de los parámetros y de los datos maestros como dos subprocesos distintos.

Los datos maestros son los atributos permanentes de un objeto (p.e. datos maestros de clientes, de proveedores, de productos en existencias, etc.).

En el capítulo 7.5.2 se estudia la importancia de la parametrización sobre los riesgos y los controles en los actuales sistemas ERP y por tanto la atención que requieren en los procedimientos de auditoría.

5.4. Revisión de los controles generales

5.4.1. Introducción

Una vez adquirido un conocimiento general de la entidad, de los procesos y de las aplicaciones significativas a los efectos de la auditoría financiera y antes de iniciar la revisión de las aplicaciones de negocio y de sus controles, se debe revisar la situación de los controles generales, ya que el grado de confianza en los mismos determinará la posterior estrategia de auditoría.

Los controles generales ayudan a asegurar el correcto funcionamiento de los sistemas de información mediante la creación de un entorno adecuado para el correcto funcionamiento de los controles de aplicación. Su evaluación favorable da confianza sobre los controles automatizados embebidos en las aplicaciones de negocio (controles de aplicación).

La eficacia de los controles generales es un factor significativo a la hora de determinar la eficacia de los controles de aplicación y ciertos controles de usuario. Sin unos controles generales efectivos, los controles de aplicación pueden dejar de ser efectivos ya que resultará mucho más fácil eludirlos. Por ejemplo, la producción y revisión de un informe especial de elementos no coincidentes (desparejados) puede ser un control de aplicación efectivo; no obstante, dicho control dejará de ser efectivo si los controles generales permitiesen realizar modificaciones no autorizadas de los programas, de forma

que determinados elementos quedasen excluidos del informe de manera indebida.

Si no existen controles generales o no son efectivos, será necesario adoptar un enfoque de auditoría basado exclusivamente en procedimientos sustantivos, siguiendo el razonamiento lógico representado en la figura 4.3.

5.4.2. Objetivo

El objetivo de esta etapa de la auditoría es:

- Identificar y comprobar el adecuado funcionamiento de los controles generales.

5.4.3. Concepto

Los controles generales son las políticas y procedimientos que se aplican a la totalidad o a gran parte de los sistemas de información de una entidad, incluyendo la infraestructura y plataformas TI de la organización auditada.

En el modelo representado por la Figura 3.1, vemos a la izquierda, que los controles generales afectan a todos los niveles de los sistemas de información, si bien están relacionados con mucha mayor intensidad con aquellos niveles de carácter general que afectan a toda la organización (nivel entidad) o a los sistemas informáticos de base y la infraestructura informática (nivel de sistemas TI).

Para su estudio, diremos que una entidad puede establecer controles generales a los siguientes niveles:

— a nivel de la entidad,

— a nivel de los sistemas TI, y

— a nivel de aplicación.

Al evaluar los controles generales a nivel de la entidad o de sistema, el auditor financiero y el auditor informático examinarán los controles de acceso generales.

Cuando son examinados los controles generales a nivel de aplicación, el auditor y el auditor de sistemas pueden evaluar los controles de acceso que limitan/restringen el acceso a determinadas aplicaciones y ficheros relacionados (como, por ejemplo, el fichero maestro de empleados y los ficheros de transacciones de nóminas) a usuarios autorizados.

Por último, el auditor y el auditor de sistemas pueden evaluar la seguridad establecida en la propia aplicación para restringir el acceso

en mayor medida. Esta seguridad normalmente se consigue mediante creación de usuarios con palabra clave de acceso y otras restricciones programadas en el software de la aplicación como los perfiles de usuario. Así, un empleado responsable de las nóminas puede tener acceso a las aplicaciones sobre nóminas pero puede tener restringido el acceso a una determinada función, como puede ser la revisión o actualización de datos de las nóminas sobre los empleados del propio departamento de nóminas.

El propósito de los controles generales de un entorno informatizado es establecer un marco conceptual de control general sobre las actividades del sistema informático y asegurar razonablemente la consecución de los objetivos generales de control interno y el correcto funcionamiento de los controles de aplicación.

Como ya se ha señalado, unos controles generales ineficaces pueden impedir que los controles de aplicación funcionen correctamente y permitir que se den manifestaciones erróneas y que éstas no sean detectadas.

5.4.4. Clases de controles generales

Los controles generales de un entorno informatizado pueden incluir:

a) Controles de organización y dirección

Diseñados para establecer el marco general de organización de las actividades del sistema informático, incluyendo:

- Políticas y procedimientos relativos a funciones de control y gestión de seguridad que proporcione un marco y un continuo ciclo de actividad para gestionar el riesgo, desarrollar unas políticas de seguridad, asignar responsabilidades y controlar la correcta aplicación de los controles de la entidad relacionados con los sistemas informáticos.
- Adecuada segregación de funciones incompatibles (preparación de transacciones de entrada, programación y explotación).

  Incluye contar con políticas, procedimientos y una estructura organizativa para gestionar quién puede controlar los aspectos clave de las transacciones relacionadas con los sistemas informáticos y de ese modo evitar realizar acciones no autorizadas o conseguir acceso no autorizado a activos o registros.
- Controles de acceso lógicos y físicos que restrinjan/limiten o detecten el acceso a los recursos informáticos (datos, pro-

gramas, equipos e instalaciones), a través de los cuales estos recursos queden protegidos contra cualquier modificación no autorizada, pérdida o revelación.

Los controles lógicos de acceso requieren que los usuarios se identifiquen (mediante el uso de claves u otros identificadores) y limitan los ficheros y otros recursos a los que los usuarios autenticados pueden acceder y las acciones que pueden realizar.

Las políticas de contraseñas deben establecerse de forma general y aplicarse en todos los niveles y plataformas de los sistemas de información: sistemas operativos, sistemas de red, aplicaciones, bases de datos, etc. El auditor al revisarlas puede elaborar un cuadro como el del ejemplo siguiente, en el que junto con la recomendación según las mejores prácticas, se indicará la situación real observada en la entidad en los componentes del sistema de información objeto de revisión:

Política de Contraseñas					
Parámetro	Recomendación	Dominio Windows Server	SAP	DB2	Linux
Longitud mínima	6	6	6	N.D.	N.D.
Caducidad	90 días	62	720	N.D.	N.D.
Histórico	4 contraseñas recordadas	5	Deshabilitado	N.D.	N.D.
Complejidad	Números, letras y alfanuméricos	Deshabilitado	Deshabilitado	N.D.	N.D.
Cambio en primer inicio de sesión	Sí	Sí	Sí	N.D.	N.D.
Máximo número accesos erróneos	5 accesos erróneos	3	5	N.D.	N.D.
Suspensión de cuenta tras inactividad	Después de 90 días sin uso	Deshabilitado	Deshabilitado	N.D.	N.D.
Tiempo de inactividad para bloqueo	10 minutos	10 minutos	3 minutos	N.D.	N.D.

N.D. No definido
Figura 5.10

Los controles de acceso físicos implican restringir el acceso físico a los recursos informáticos y protegerlos de cualquier pérdida o deterioro intencionado o no intencionado. Se realizará una inspección física en el centro de proceso de datos, utilizando un checklist como el que se adjunta en el Anexo 2.

b) Controles sobre operaciones realizadas a través del ordenador

Diseñados para controlar las operaciones que se realizan desde el sistema y para asegurar razonablemente que:

- El sistema se está utilizando exclusivamente para propósitos autorizados.
- El acceso a las operaciones realizadas desde el ordenador está restringido a personal autorizado.
- Sólo se utilizan programas autorizados.
- Se detectan y corrigen los errores de procesamiento.

c) Controles sobre el software de los sistemas.

Diseñados para asegurar razonablemente que el software de los sistemas se ha adquirido y desarrollado de forma autorizada y eficiente, incluyendo:

- Autorización, aprobación, pruebas, implantación y documentación de los nuevos software de sistemas y de sus modificaciones.
- Restricción de acceso al software de sistemas y documentación al personal autorizado.
- Gestión de configuración que impida realizar cambios no autorizados en los recursos de los sistemas de información (programas informáticos, configuraciones y componentes de hardware) y que proporcione una seguridad razonable de que los sistemas están bien configurados y funcionan correctamente y tal como estaba previsto
- Adquisición de aplicaciones de terceros.

d) Controles de entrada de datos y de programa.

Diseñados para asegurar razonablemente que:

- Se ha establecido una adecuada estructura de autorización sobre las transacciones a introducir en el sistema.
- El acceso a los datos y programas se encuentra restringido al personal autorizado.

e) Continuidad de las operaciones

Existen otras salvaguardas que contribuyen a la continuidad de las operaciones de procesamiento en entornos TI. Entre estas se pueden citar:

- Mantenimiento de copias de seguridad externas de los datos y de los programas informáticos.
- Procedimientos de recuperación aplicables en el caso de robo, pérdida o destrucción accidental o intencionada.
- Establecimiento de centros alternativos de procesamientos en el caso de catástrofes.
- Planificación de contingencias a fin de que cuando ocurran hechos inesperados, las operaciones críticas puedan continuar sin interrupción o ser inmediatamente reanudadas y quede protegida la información importante y confidencial.

5.4.3. Procedimientos de auditoría

Para la revisión de los controles generales puede utilizarse como elemento básico la metodología COBIT.[61] COBIT es un sumario de objetivos de control y mejores prácticas que, si se encuentran implementadas en una entidad, proporciona una seguridad razonable de que la gobernanza TI soporta los objetivos del negocio, utilizando los recursos tecnológicos con eficacia para gestionar y reportar información fiable.

El Tribunal de Cuentas Europeo ha desarrollado para aplicar esta metodología la herramienta ECACOBIT.[62]

La metodología COBIT se debe complementar con programas de trabajo específicos según el tipo de aplicaciones ERP que se estén revisando.

5.5. Identificación de los riesgos y de los controles clave de las aplicaciones

5.5.1. Introducción

Una vez identificados los procesos y las aplicaciones de negocio que tienen carácter significativo en relación con la formulación de las cuentas anuales, que por tanto van a ser objeto de revisión por el auditor informático, y hecha la revisión de los controles generales con resultado satisfactorio (es decir son confiables), se pasa a la siguiente etapa de la auditoría (ver figura 4.4).

61. Los usuarios registrados de la herramienta de papeles de trabajo electrónicos TeamMate, que utilizan muchos auditores públicos en España e internacionalmente, pueden descargarse todos los programas de auditoría Cobit.

62. Ver *Guidelines on how to integrate IT AUDIT within the audit. Process – ECA-COBIT*, Tribunal de Cuentas Europeo.

En esta etapa se debe delimitar el alcance de la auditoría a realizar sobre la aplicación de negocio seleccionada previamente. Teniendo en cuenta la complejidad de los procesos y de las aplicaciones de negocio, es importante centrarse en lo esencial, por ello la identificación de los riesgos y de los controles clave constituye la base para una auditoría eficaz.

Todo el trabajo de auditoría en esta fase debe centrarse en los controles clave, ya que son los únicos que proporcionan al auditor la seguridad razonable suficiente de que, si funcionan eficazmente, el riesgo de auditoría quedará reducido a un nivel aceptable.

Posteriormente, los controles clave identificados por el auditor serán comparados con los controles efectivamente implementados y evaluada la eficacia de su funcionamiento.

5.5.2. Objetivo

El objetivo de esta etapa de la auditoría consiste en:

- Definir para cada riesgo significativo identificado, los posibles escenarios de errores, con objeto de evaluar la forma en que pueden ser mitigados por controles clave.

  También debe analizarse el impacto de los riesgos sobre las manifestaciones en las cuentas anuales.

5.5.3. Los controles de aplicación

a) Concepto

El propósito de los controles de aplicación en un entorno informatizado es establecer procedimientos de control específicos en las aplicaciones de negocio con el fin de asegurar razonablemente que todas las transacciones son autorizadas y registradas, y que son procesadas de forma completa, adecuada y oportuna.

Cada aplicación y cada proceso específico tienen incorporados controles que garantizan la realización de los objetivos definidos. Estos controles son llamados «controles de aplicación» (a veces controles de procesos de negocio) y deben ayudar a garantizar la validez, integridad, exactitud, confidencialidad y disponibilidad de las transacciones y datos durante todo el procesamiento de la aplicación.

Es evidente que cada tipo de aplicación exige controles diferentes, ya que cada proceso de negocio o actividad comercial, industrial, o de

servicio específica, comporta riesgos diferentes, inherentes a esa actividad y susceptibles de perjudicar o impedir alcanzar los objetivos.

Los controles de aplicación tienen por finalidad asegurar un procesamiento adecuado y seguro de las transacciones y de garantizar la exactitud de los resultados. En consecuencia, los controles juegan un papel central en la realización de los objetivos de la entidad, de la protección del patrimonio, de la exactitud y de la fiabilidad de la contabilidad y del respeto a las normas.

Con los controles aplicativos la entidad garantiza la captura exhaustiva, exacta y verificable de todas las transacciones así como el tratamiento, registro y la edición de estas por el sistema de información.

Estos controles se extienden sobre el conjunto del proceso de negocio o actividad cubierto por la aplicación. Su comprobación proporcionará confianza únicamente sobre aquellas transacciones concretas procesadas por esa aplicación.

b) Exhaustividad de la revisión de los controles

La identificación de los controles existentes en las aplicaciones no es suficiente por sí mismo; es necesario considerar también los riesgos inherentes y los controles existentes en las interfaces, en los parámetros y en los datos maestros.

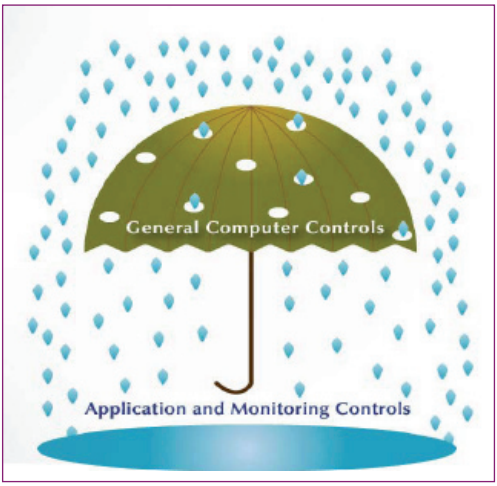
Todos los controles importantes ligados a las aplicaciones, que tengan una influencia directa sobre el resultado del proceso, deben ser tenidos en cuenta, tanto los manuales como los automáticos.

También debe ser evaluada con carácter previo la eficacia de los controles que tengan una influencia indirecta sobre el funcionamiento de los controles clave de la aplicación (principalmente los controles generales TI).

c) Dependencia de los controles generales

La eficacia de los controles de aplicación depende de la eficacia de los controles generales al nivel de la entidad y al nivel del sistema. Debilidades en los controles generales a esos niveles pueden permitir cambios no autorizados en las aplicaciones de negocio y en los datos que pueden perjudicar la eficacia de los controles de aplicación.

De una forma visual, vemos que unos controles generales débiles no protegen ni posibilitan de forma eficaz el buen funcionamiento de los controles de las aplicaciones:



Sin embargo unos controles generales sólidos y eficaces, proporcionan un entorno adecuado para el buen funcionamiento de los controles de las aplicaciones:

Por ejemplo: los controles de una aplicación de ventas-facturación pueden estar bien diseñados y correctamente implementados, pero si no hay controles sobre los accesos directos a las tablas de las bases de datos que soportan y registran los datos y transacciones de la aplicación, aquellos controles son inútiles.

La ISA 330 establece[63] que al diseñar y ejecutar pruebas de controles el auditor determinará si los controles a comprobar dependen a su vez de otros controles (controles indirectos), y si es así, si es

63. ISA 330, párrafo 10 (b).

necesario obtener evidencia adicional de auditoría que acredite el funcionamiento efectivo de dichos controles indirectos.

Por ejemplo: Cuando el auditor decide comprobar la eficacia de un control consistente en la revisión manual de un informe de excepción sobre ventas que hayan excedido los límites de crédito autorizados. La revisión del responsable y el consiguiente seguimiento es el control relevante para el auditor. Los controles sobre la precisión de la información incluida en los informes (por ejemplo los controles generales) se denominan controles indirectos.

d) Controles clave

Los controles clave son un elemento fundamental en la auditoría basada en el análisis del riesgo, ya que buena parte de los procedimientos de auditoría gira a su alrededor.

En esta fase, de todos los controles que haya en las aplicaciones revisadas, solo nos interesan aquellos más importantes, los que si están bien diseñados e implantados y funcionan con eficacia, permiten concluir al auditor que los riesgos de auditoría de que existan errores o irregularidades no detectados por el sistema de control interno están controlados en un nivel aceptable.

Todo el trabajo de auditoría en esta fase debe centrarse en dichos controles clave, ya que todo trabajo que se realice sobre los otros controles existentes no aporta satisfacción o utilidad adicional de auditoría, y será un trabajo ineficiente.

e) Objetivos de control

Los objetivos de control se deducen de los riesgos. Un objetivo de control se define como una manifestación relativa al resultado deseado (objetivo) que debe alcanzarse gracias a la implementación del control. Los objetivos de control son así a menudo riesgos «invertidos», dicho de otra forma, tienen por función disminuir un riesgo dado.

5.5.4. Tipos de controles de aplicación

Desde el punto de vista de la auditoría de sistemas de información, los controles pueden clasificarse de distintas formas:

- Controles preventivos o controles detectivos: según que el objetivo del control sea impedir que ocurran errores o detectarlos.
- Controles manuales o automáticos: según el control se realice manualmente o esté automatizado en una aplicación.

– Controles del proceso de negocio, de la interfaz y del gestor de base de datos.

Los controles de aplicación programados o automáticos son aquellos efectuados automáticamente por los programas o aplicaciones en cada una de las diferentes etapas del tratamiento de la información. Así, de acuerdo con la etapa del proceso en la que se encuentre la información, los controles se clasifican de la siguiente forma:

a) Creación y autorización

Los principales objetivos relativos a la creación y autorización son los siguientes:

- Minimizar los errores y las omisiones
- Identificar, documentar, comunicar y corregir los errores y las irregularidades desde su aparición
- Verificar la exactitud de las corrección de errores por un servicio o persona independiente
- Las transacciones solo son realizadas por personas autorizadas y según procedimientos autorizados
- Las personas responsables de la captura de las transacciones son identificadas por el sistema
- Los justificantes de captura proporcionados son exhaustivos y transmitidos en tiempo útil
- Los justificantes de captura se conservan durante el periodo y en la forma legalmente exigidos o pueden ser reconstituidos por la organización

Los controles más usuales relativos a la creación y autorización son los siguientes:

- Perfiles de competencias para la emisión de documentos contables (p.e. regulación de las firmas) y puesta en práctica de un control de las autorizaciones por sistemas de gestión de acceso.
- Segregación de las funciones de creación y de validación de documentos contables
- Visé o firma sobre los justificantes de captura de datos
- Formularios de captura de datos comprensibles y útiles (p.e. con campos predefinidos)
- Procesos de identificación precoz y de tratamiento de los errores e irregularidades.

- Archivo sistemático de los documentos contables
- Digitalización de los justificantes y conservación adecuada

b) Captura y registro de datos

Los principales objetivos de la captura y registro de datos son los siguientes:

- Solo las personas autorizadas o los procesos autorizados pueden grabar los datos
- La exactitud, exhaustividad y la validez de los campos importantes son controlados en las pantallas o programas superpuestos al proceso de captura
- Los errores y las anomalías de captura y registro son identificados, documentados, comunicados y corregidos en tiempo útil.
- La exactitud de la corrección de los errores se verifica por un servicio o persona independiente.

Los controles típicos de captura y registro de datos son los siguientes:

- Perfiles de competencias para la captura/registro de las transacciones y puesta en práctica a través de un control de las autorizaciones por sistemas de gestión de accesos.
- Máscaras de captura comprensibles y amigables con controles de formato de datos integrados (p.e. campos de fecha, numéricos, campos obligatorios, etc y lista de valores predefinidos y recurrentes).
- Control automático profundo de los valores introducidos (p.e. superación de valores límites, control de factibilidad (credibilidad) de los contenidos, sincronización con los datos archivados).
- Despliegue de etiquetas de código completas después de la grabación del código (p.e. la designación de un artículo se muestra al grabar el número del artículo).
- Comparación de datos capturados, es decir comparación de los datos a capturar con los datos visibles en la pantalla (teniendo en cuenta el coste, solo es justificable para transacciones críticas como cambios en datos maestros).
- Totales de control por lotes: número de documentos (p.e. facturas), suma de zonas de valores visibles en los documentos o sumas numéricas (importes, cantidades), suma de control.

- Control secuencial de documentos contables numerados correlativamente para identificar los faltantes o duplicados en las grabaciones.
- Comparación de datos capturados con valores registrados.
- Captura de control (llamada también doble captura, control de los 4 ojos); captura doble de valores importantes por diferentes personas o por una misma persona.
- Control visual de valores capturados por una segunda persona; conviene para los casos críticos y un pequeño número de transacciones.
- Proceso de identificación precoz y de tratamiento de errores y de anomalías, las transacciones corregidas deben ser enteramente verificadas de nuevo.

c) Procesamiento de los datos

Los principales objetivos del procesamiento de datos son los siguientes:

- Las transacciones (cálculos, totalizaciones, consolida-ciones, análisis, etc), incluidas las que genera el propio sistema, son adecuadamente procesadas por el ordenador.
- Las transacciones no son objeto de pérdida, duplicación, manipulación o alteración.
- La exhaustividad, exactitud y la validez del procesamiento realizado son verificados según un procedimiento de rutina;
- Los errores de procesamiento son identificados rápidamente, documentados y corregidos en tiempo útil.
- La corrección de transacciones erróneas se efectúa sin interrumpir inútilmente el procesamiento de las demás transacciones.
- La separación de funciones está garantizada incluso durante el procesamiento de los datos.
- Las transacciones generadas automáticamente por la aplicación (p.e. intereses periódicos de préstamos, órdenes al sobrepasar umbrales de stocks) son objeto de los mismos controles de exhaustividad, exactitud y de validez que las transacciones aisladas.
- Las decisiones importantes basadas en cálculos automáticos son adoptadas y verificadas por personas.

Los controles típicos del procesamiento de datos son los siguientes:

- Un gran número de los controles descritos precedentemente para la captura y la creación de datos pueden ser aplicados para el procesamiento (p.e. comparación de campos individuales, sincronización automática de libros principales y auxiliares). No obstante, es importante que los documentos y los totales utilizados para los controles correspondan a los resultados de fin de procesamiento.
- Comparación de los datos tratados en el sistema con confirmaciones externas (p.e. inventarios físicos, confirmación de saldos bancarios y de saldos de clientes y proveedores).

d) Salida de los datos

Las salidas u outputs son el resultado del procesamiento de los datos.

Los principales objetivos de la salida de datos son los siguientes:

- Los resultados (integridad y exactitud) del procesamiento son adecuados.
- El acceso a los datos de salida del sistema está restringido al personal autorizado.
- Los datos de salida del sistema llegan al personal autorizado en tiempo oportuno, de conformidad con los procedimientos definidos.
- El tratamiento, la conservación y la destrucción de output son conformes con las exigencias de las normas de protección de datos y de seguridad (antes y después de su difusión entre los usuarios).
- Las informaciones impresas se conservan de conformidad con las disposiciones legales.

Los controles típicos de la salida de datos son los siguientes:

- Los controles de envío y de recepción regulan las modalidades de comunicación de listados y otros output (quién, cuándo, qué, cómo y cuántos ejemplares).
- Los sistemas de gestión de acceso garantizan la trazabilidad de los accesos de los usuarios a consultas en pantalla o a listados.
- Los controles de numeración y de exhaustividad garantizan que la gestión, edición, restitución, recepción y destrucción (p.e. en caso de copia de control) de outputs críticos (p.e. cheques, vales, etc) se efectúan de conformidad con los procedimientos.

– La exactitud y la exhaustividad de las impresiones periódicas (p.e. listados semestrales o anuales) son controlados mediante muestreos.

e) Interfaces

Las interfaces de entrada y de salida de una aplicación deben ser consideradas como fuentes de riesgo. Es importante identificarlas y revisarlas (ver el capítulo 7.4).

Los controles de interfaz son aquellos diseñados para el procesamiento de información oportuno, exacto, y completo entre aplicaciones y otros sistemas emisores y receptores de información.

Los principales objetivos relativos a los interfaces son los siguientes:

– La autenticidad y la integridad de las informaciones provenientes de fuentes externas a la organización son controladas cuidadosamente antes de emprender cualquier acción potencialmente crítica, independientemente del medio de recepción (teléfono, fax, email, etc).
– Las informaciones sensibles están protegidas durante su transmisión por medidas adecuadas contra accesos no autorizados, modificaciones o envío a destinatarios erróneos.

Los controles típicos al nivel de las interfaces son los siguientes:

– Un gran número de los controles existentes previamente para la captura y registro de datos pueden también ser utilizados para el control de las interfaces (p.e. comparación de saldos individuales, totales de control de lote, controles de numeración, comparación de datos).
– Autenticación de cada mensaje por procedimientos criptográficos.
– Encriptación de cada mensaje importante para garantizar la confidencialidad e integridad del contenido y la identidad del que lo envía.

Un gran número de controles realizados al nivel de las interfaces se refieren principalmente al transporte y la transmisión, así como al registro electrónico de los datos; se trata en general de controles no ligados a una aplicación.

f) Datos maestros

Los datos maestros son los datos permanentes utilizados por el sistema y participan en la correcta ejecución de los tratamientos de datos realizados por las aplicaciones.

Los principales objetivos relativos a los datos maestros son los siguientes:

- Las modificaciones deben ser realizadas por personas autorizadas. Deben ser registradas y archivadas de forma que se mantenga la pista de auditoría.

Los controles típicos son los siguientes:

- Existen procedimientos para las modificaciones.
- Las actualizaciones se realizan de forma simultánea en todo el sistema de información.
- Sólo las personas autorizadas pueden modificarlos.
- Se mantiene un fichero histórico con todos los cambios en los datos maestros incluyendo quién los realizó.

5.5.5. Procedimientos de auditoría

a) Aspectos generales

Para las aplicaciones de negocio significativas objeto de auditoría, el auditor debe obtener un adecuado conocimiento de los distintos controles existentes en ellas.

En las auditorías de sistemas, integradas en las auditorías financieras, solo se evaluará la efectividad de aquellos controles que tengan relevancia a efectos de la auditoría financiera, circunstancia que deberá ser definida por el auditor financiero con la colaboración del informático. Los controles clave de un proceso de negocio a los efectos de la auditoría financiera, incluirán tanto controles automatizados como manuales.

En general, para el análisis y evaluación del riesgo de las aplicaciones se seguirán las siguientes actividades:

- Realización de un mapa del proceso/aplicación o flujograma (visto en el capítulo 5.3).
- Identificación de riesgos posibles relacionados con las manifestaciones de las cuentas anuales y su probabilidad de suceso (apartado b siguiente).
- Identificación y evaluación de los controles clave (manuales y automatizados) implantados por la entidad para cubrir los riesgos existentes (apartado c siguiente).
- Evaluación del riesgo de control (capítulos 5.6, 5.7 y 5.8).

b) Identificación de los riesgos

Se deben identificar los *riesgos* existentes en los principales procesos y sistemas implicados, que dará una idea general de los riesgos susceptibles de impedir la consecución de los objetivos del proceso de negocio o que puedan entrañar inexactitudes importantes en las cuentas anuales. Este análisis de los riesgos permite también definir la extensión de los procedimientos de auditoría.

Se partirá del estudio y descripción mediante un flujograma (que ya se ha visto cómo elaborar en el capítulo 5.3) del proceso/aplicación a analizar, y de cualquier otra documentación o información disponible del proceso/aplicación, incluyendo entrevistas con los usuarios o responsables de la entidad

Normalmente, al realizar el estudio y descripción de un proceso mediante un flujograma, se incluye una «primera versión» de los riesgos y controles clave identificados, que serán confirmados después al realizar las pruebas de recorrido.

La identificación de los riesgos posibles se realiza contando con los distintos usuarios o responsables del proceso de negocio auditado y analizando los distintos componentes aplicativos que intervienen en el proceso:

- Las interfaces (datos entrantes y salientes)
- Los datos maestros
- Los permisos o autorizaciones
- El procesamiento de datos

En el siguiente cuadro[64] se muestra el grado de importancia que desempeña cada componente aplicativo con relación a las manifestaciones de las cuentas anuales:

	Interfaces	Datos maestros	Permisos	Procesamiento
Integridad	***	*	***	*
Existencia	**	*	***	*
Valoración	*	***	***	***

(*** Mucha; ** Media; * Poca)
Figura 5.11

Según este cuadro, los permisos y las interfaces son los principales factores a considerar en materia de integridad. El procesamiento afecta principalmente a la valoración, etc.

64. Fuente: *Prise en compte de l'environement informatique et incidente sur la démarche d'audit*, CNCC, 2003, (pag. 65).

El énfasis en cada componente aplicativo se efectuará en función de la manifestación revisada.

Las características de las interfaces afectan a la evaluación del riesgo. Las manuales presentan un mayor riesgo de errores (de captura de datos, por omisión de operaciones, duplicados, etc.) que las automáticas. En las interfaces automáticas debe comprobarse la existencia de logs o informes que permitan comprobar la correcta ejecución del procesamiento (informes de anomalías, informes de ejecución que permitan comparar los datos que entran y salen de la interfaz); los informes deben ser analizados y dar lugar a las acciones correctoras que procedan.

La fiabilidad de una interfaz se analiza estudiando las condiciones de implementación, de funcionamiento y de actualización. A priori una interfaz nueva, no testeada completamente, tiene más posibilidades de funcionar mal.

c) Identificación de controles clave

A continuación el auditor debe distinguir entre controles clave y otros controles.

Los controles clave, individuales o combinados entre ellos, son indispensables para la reducción de los riesgos a un nivel aceptable. Son los que permiten reducir los RMES descritos en el capítulo 4 (ver figura 4.2) a un nivel aceptablemente bajo.

Los controles clave identificados por el auditor deben ser contrastados con los controles efectivamente implantados y la cobertura de los riesgos es evaluada a la vista del conjunto de los controles clave existentes en el proceso de negocio analizado.

Constituyen el elemento fundamental del sistema de control y deben ser, pues, objeto de comprobación prioritaria; los otros controles tienen menos importancia para el auditor. Si el auditor no se concentra sobre los controles clave, la auditoría corre el riesgo de ser demasiado general e ineficaz.

No es aconsejable una descripción demasiado detallada de los controles, pues ello acarrearía costes adicionales y no generaría un beneficio adicional.

Para la comprensión de los controles clave de las aplicaciones y en particular para la evaluación posterior de su diseño, es importante efectuar una adecuada documentación de los mismos.

La documentación debe permitir al auditor comprender cuáles son las «reglas de gestión» que deben ser garantizadas por el control.

Además debe recoger los aspectos ligados al diseño del control desde la perspectiva de su implementación. Deben reflejarse los parámetros o ajustes personalizables para que el control pueda funcionar conforme a las reglas de gestión definidas:

Control clave		Regla de gestión	Diseño del control
C001	*3-way-match*	No se paga ninguna factura si no concuerdan el pedido, albarán y factura (tolerancia 10%)	Referencia a la función *3-way-match* de los ERP
C002	Segregación de funciones	Segregación de funciones entre contables, deudores y acreedores. Las personas que pagan las facturas no pueden crear nuevos proveedores.	Roles separados de los que contabilizan deudores y acreedores de los que gestionan datos maestros. Documentación de una matriz de segregación de funciones.

Figura 5.12 Ejemplo de documentación de controles

d) Evaluación y análisis de los riesgos y de los controles clave

El diseño de los mapas de procesos o flujogramas vistos en el capítulo 5.3, en los que, además deben indicarse los principales riesgos y los controles clave (representados por símbolos), debe complementarse con documentos en los que se describan en detalle estos aspectos.

Para cada proceso de negocio significativo analizado, debe cumplimentarse un formulario de análisis de riesgos (FAR) en el que debe resumirse el trabajo realizado para identificar y evaluar los riesgos y controles clave relacionados, como el modelo de la figura siguiente.

Se identificarán los epígrafes de las cuentas anuales (partida presupuestaria, cuenta y revelación significativa de la memoria), afectados por procesos de negocio (como ingresos, subvenciones, compras y producción) y las aplicaciones específicas significativas que afectan a esas partidas presupuestarias, cuentas y declaraciones.

Un formulario FAR proporciona una forma práctica y útil de documentar los riesgos específicos de manifestaciones erróneas significativas de las partidas presupuestarias o cuentas significativas, que se deben tener en cuenta a la hora de determinar la naturaleza, alcance y momento de ejecución de los procedimientos de auditoría.

En la figura siguiente puede verse un modelo de FAR:

Formulario de Análisis de Riesgos Entidad: Ayuntamiento de X Y Z
Proceso de negocio: *Contratación de inversiones* Subproceso: *Adjudicación* Cuentas relacionadas: Capítulo 6 y acreedores Aplicación informática: *SAP*

Riesgo	Control clave	Tipo de control	Respon-sable	Eficacia del control	Riesgo de control	RMES (1)	Impacto (1)
(Describir el riesgo y asignar un identificador secuencial)	(Describir el CC y asignar un identificador secuencial. Para cada riesgo puede haber más de un control)	Señalar si es: Manual/ Automático Detectivo/ Preventivo	(Indicar el responsable del control)	Señalar si es: Efectivo/ No efectivo (en este caso describir la incidencia observada)	Bajo Medio Alto	Bajo Medio Alto	Describir (señalar la cuenta y la manifestación afectada) y cuantificar (si es posible) cuál podría ser el resultado posible del mal funcionamiento del control
R001-Descripción	C001A-Descripción						
R002-Descripción	C002A -Descripción						
	C002B -Descripción						

(1) Esta columna se cumplimentará tras realizar las pruebas de cumplimiento de los controles, cuyo resumen se plasmará en el cuadro de la figura 5.14.

Figura 5.13 Formulario de análisis de riesgos

5.6. Pruebas de recorrido o walkthrough

5.6.1. Concepto

Una prueba de recorrido consiste en reproducir y documentar las etapas manuales y automáticas de un proceso o de una clase de transacción, sirviéndose de una transacción utilizada como ejemplo.

Sirve para verificar la comprensión del proceso de negocio, subproceso o actividad analizada, los riesgos y los controles clave relacionados.

Se deben realizar pruebas de recorrido para todas las aplicaciones significativas y así obtener evidencia sobre el funcionamiento de esas aplicaciones y de los controles clave.

La prueba debe permitir que el auditor comprenda los principales riesgos que pueden existir en el proceso revisado, y orientar en consecuencia sus pruebas sustantivas.

Antes de realizar una prueba de recorrido, debe comprenderse el proceso global, del principio al fin. No obstante, en las pequeñas entidades, las pruebas de recorrido pueden realizarse al mismo tiempo que se obtiene la comprensión del sistema de control interno.

En la práctica con esta prueba se efectúa a menudo la evaluación del diseño del control y, en el caso de controles automáticos, de la comprobación de su funcionamiento. Ambas cuestiones se analizan en los dos capítulos siguientes.

Debe tenerse cuidado al realizar estas pruebas de no descuidar la inclusión de las interfaces que enlacen varios subprocesos o varias aplicaciones individuales.

5.6.2. Objetivos de una prueba de recorrido

La prueba de recorrido permite:

- Confirmar que la comprensión del proceso por el auditor es completa y correcta.
- Verificar la existencia de controles clave en las actividades ordinarias y el funcionamiento de los controles clave automáticos.
- Confirmar la comprensión por el auditor del diseño de los controles clave identificados.
- Verificar la consistencia y pertinencia de la documentación elaborada hasta el momento, incluyendo los diagramas de flujo existentes.

5.6.3. Cómo realizar una prueba de recorrido[65]

a) Recorrer el proceso completo

Para cada uno de los procesos revisados, se debe seguir el flujo de procesamiento de una transacción real, utilizando los mismos documentos y operaciones informáticas que utiliza el personal de la entidad. No se deben revisar copias de documentos proporcionados por una única fuente o que pretendidamente están en uso.

El auditor analiza una transacción a través del proceso global, empezando por el inicio de la transacción, su autorización, registro,

65. Basado en *Guide to Using International Standards on Auditing in the Audits of Small- and Mediumsized Entities*, página 360.

procesamiento, hasta su contabilización e inclusión en las cuentas anuales. El proceso o clase de transacción analizada debe seguirse a partir del hecho generador, después a través de las distintas etapas de procesamiento en la aplicación. En el desarrollo del proceso, son verificados los controles existentes y es analizada la selección de controles clave previamente realizada por el auditor.

b) Grado de detalle requerido

El grado de detalle con el que se desarrolla una prueba de recorrido depende de la intención del auditor financiero de apoyarse o no sobre el sistema de control interno existente:

- Si el auditor tiene la intención de apoyarse sobre los controles clave, analizará detalladamente el funcionamiento de los diferentes controles al realizar esta prueba para saber si cubren eficazmente o no los riesgos existentes.
- Si el auditor no tiene la intención de apoyarse sobre la eficacia de los controles, bastará una prueba menos detallada. En determinados casos podrá incluso prescindirse de estas pruebas.

c) Implicar al personal de la entidad

En esta prueba, el personal de la entidad debe ser interrogado sobre su comprensión de las descripciones de su función y de las instrucciones para la realización de los controles, especialmente en lo que respecta al tratamiento de las excepciones en el procesamiento o de los errores.

No deben limitarse las preguntas a una sola persona.

d) Preguntar sobre la comprensión del personal

En cada punto que ocurra o suceda algún procedimiento o actividad de control importante, se debe preguntar al personal de la entidad sobre su conocimiento y comprensión de lo que deben hacer y si hacen habitualmente lo que está previsto.

Hay que estar atento a posibles excepciones sobre los procedimientos y actividades de control previstas.

No se deben hacer pruebas de controles (pruebas de cumplimiento) sobre procedimientos que no son realizados de forma regular.

e) Cuestiones a considerar

En estas pruebas se deberá tener en cuenta:

- ¿A quién recurrir para obtener explicaciones de los detalles?

- ¿De quién y de dónde proceden los documentos, informes, diagramas de flujo, etc. existentes?
- ¿Qué actividad de control tiene lugar en el curso de las diferentes actividades?
- ¿El control se realiza para evitar un error o para detectarlo?
- ¿Cómo y con qué frecuencia se efectúa el control (automático o manual)?
- ¿El control automático está realmente operativo?
- ¿Qué pistas deja el control (trazabilidad)?

f) Corroborar

Se deben corroborar las informaciones en varios puntos de la prueba de recorrido preguntando al personal que describa su conocimiento de la parte anterior y posterior del proceso o actividad de control interno y que demuestre lo que hace.

Es preciso pedir al personal que enseñen lo que hacen, más que se lo digan al auditor.

g) Hacer preguntas de seguimiento

Debe preguntarse y obtener evidencia que pueda ayudar a identificar abusos del control interno o indicadores de fraude. Por ejemplo:

- ¿Le han pedido alguna vez que evite o fuerce el procedimiento de control interno? Si es así describa la situación, porqué ocurrió y qué sucedió.
- ¿Qué sucede cuando usted encuentra un error?
- ¿Cómo determina si ha ocurrido un error?
- ¿Qué clase de errores suele encontrar?
- ¿Cómo se solucionan los errores?

Si nunca se ha detectado un error, el auditor debe evaluar si es debido a buenos controles preventivos o si las personas que realizan los controles internos adolecen de las necesarias habilidades para identificar un error.

h) Tratamiento de las incidencias detectadas

Un control interno indebidamente diseñado puede representar una debilidad significativa en el sistema de control interno de la entidad.

Se debe considerar su comunicación a los responsables de la entidad. El informe que resuma las deficiencias de control interno

detectadas y las recomendaciones para su subsanación se hará por escrito.

i) Documentación

Se obtendrá documentación suficiente y adecuada que proporcione evidencia de que los objetivos del walkthrough se han alcanzado.

La documentación de las pruebas de recorrido consiste normalmente en descripciones, diagramas de flujo, impresiones de pantalla, copias de documentos, notas de las conversaciones con el personal de la entidad, etc.

El grado de confianza en el trabajo realizado por otros se documentará junto con una evaluación de su competencia profesional y objetividad.

5.7. Evaluación del diseño de los controles

En las etapas anteriores el auditor ha identificado los principales riesgos y controles clave relacionados y ha adquirido una comprensión profunda del proceso de negocio auditado mediante las pruebas de recorrido.

En esas etapas ya ha sido objeto de un primer examen la adecuación de los diferentes controles, tomados individualmente.

En la evaluación del diseño de los controles se examina la adecuación (cobertura de los riesgos, exhaustividad, actualidad) y la eficacia económica (redundancias, solapamientos) del conjunto del sistema de control interno.

Solo una comprensión profunda del diseño de los controles permite definir una estrategia de auditoría adecuada para la evaluación del funcionamiento de los controles mediante el diseño y ejecución de pruebas de cumplimiento.

5.7.1. Objetivos

Los objetivos de esta etapa de la auditoría consiste en:

- Evaluar la efectividad del diseño de los controles clave. Es decir, determinar si cada uno de los controles clave, individualmente o en combinación con otros controles, es capaz de prevenir, detectar y corregir de forma efectiva errores o irregularidades materiales.
- Alcanzar la máxima cobertura de controles con el mínimo coste.

5.7.2. Procedimientos y consideraciones de auditoría

a) Evaluación del diseño de los controles

Un sistema de control interno se presume efectivo si los controles son respetados y dan una seguridad razonable de que no habrá errores o irregularidades que afecten de manera significativa a los estados financieros.

Ciertos procedimientos, en una auditoría basada en el análisis de los riesgos, están concebidos para confirmar que el diseño de los controles permite identificar, evitar y corregir errores importantes.

El diseño de los controles, especialmente su situación en el proceso de negocio, debe ser evaluado para saber si:

- Los riesgos identificados son cubiertos completamente.
- Los objetivos de control definidos pueden ser realmente alcanzados por los controles implantados.
- Los controles permiten realmente reducir los riesgos de errores y de irregularidades.
- La cobertura de los riesgos se realiza de forma eficaz y económica (eficiencia).
- Otro control o combinación de controles, son más eficaces para realizar el mismo objetivo de control.

Un análisis minucioso del diseño de los controles permite:

- Identificar las lagunas, los solapamientos y los duplicados en materia de controles.
- Evitar la realización onerosa de controles por la empresa.
- Evitar las pruebas de cumplimiento o funcionamiento efectivo por el auditor cuando los controles son inadecuados o ineficaces.
- Considerar si el mismo resultado o aún mejor, puede ser obtenido con la utilización o adaptación de otros controles, especialmente con otros ya establecidos.

La evidencia probatoria de la eficacia de los controles durante todo el periodo revisado solo puede ser obtenida en la etapa siguiente «Comprobación del funcionamiento de los controles».

b) Cuestiones relativas a la evaluación del diseño de los controles

Las entrevistas con empleados del área auditada, con ayuda de algunas preguntas o cuestionarios predefinidos, permiten a veces, identificar debilidades importantes en la estructura del control.

Deben considerarse los aspectos siguientes:

- ¿Las etapas del proceso y los controles relacionados están organizados en un orden lógico y razonable?
- ¿Está definida sin ambigüedad la responsabilidad de la realización de los controles?
- ¿Pueden realizarse los controles de forma correcta y razonable?
- ¿Son reemplazados los controles híbridos o manuales, en la medida de lo posible, por controles automatizados?
- ¿Los controles detectivos son reemplazados si es posible por controles preventivos?
- ¿Son conformes los controles a las exigencias de las directivas y procedimientos de trabajo?
- ¿Están disponibles las instrucciones e informaciones necesarias para la realización del control?
- ¿Los controles son realizados por una persona cualificada?
- ¿Los controles son realizados con un retraso razonable y con una frecuencia apropiada?
- ¿El diseño de los controles puede ser puesto en marcha en el marco de restricciones organizativas y financieras de la entidad?

En este análisis debe tenerse presente que los controles automáticos son más eficaces y eficientes que los controles manuales pues tienen un funcionamiento continuo en el tiempo y un coste único de implementación. Además su eficacia es más estable en tanto no se efectúen modificaciones significativas en la aplicación.

Como regla general, una frecuencia elevada de controles manuales o semiautomáticos ocasiona costes y retrasos más elevados respecto a controles automáticos cuya frecuencia no tiene prácticamente influencia sobre los costes de explotación. Por el contrario una frecuencia de ejecución baja de un control manual o semiautomático puede perjudicar su eficacia.

Está generalmente admitido que los controles preventivos permiten alcanzar más fácilmente los objetivos de control que los controles detectivos.

Un control que cubre varios objetivos de control o diferentes riesgos se considera en principio más eficaz, más fiable y más económico que un control centrado sobre un solo riesgo.

En entornos ERP complejos, al evaluar el diseño de controles aplicativos, el auditor debe clarificar las condiciones técnicas requeridas para que el control se desarrolle de la forma prevista. El auditor se planteará principalmente las cuestiones siguientes:

- ¿Puede eludirse o forzarse (rodeo, procedimiento de excepción, superusuario) el control?
- ¿En qué medida depende el control de la parametrización?
- ¿En qué medida depende el control del sistema de derechos o permisos de acceso?
- ¿Quién controla el sistema de derechos de acceso?
- ¿En qué medida depende el control de los datos maestros?
- ¿Quién controla los datos maestros?
- ¿Puede registrarse el funcionamiento del control para comprobaciones posteriores (logs, pistas de auditoría)?

c) Procedimientos de auditoría

Los procedimientos de auditoría para la evaluación del diseño de los controles incluyen preguntas, observaciones, pruebas de recorrido, revisión de documentación y la evaluación de controles específicos.

El auditor formará su opinión sobre el diseño de los controles:

- Interrogando a los miembros de la dirección de la empresa, a los empleados que tengan tareas de supervisión, así como a los empleados implicados en la realización del control.
- Consultando los documentos relativos a las transacciones y otros documentos importantes de la empresa.
- Observando las actividades específicas de ejecución y de control.
- Siguiendo las transacciones individuales en el sistema de información (mediante las pruebas de recorrido vistas en el capítulo anterior).

De conformidad con las normas técnicas de auditoría, los procedimientos para la evaluación del diseño de los controles deben estar respaldados por evidencia de auditoría y adecuadamente documentados.

Cuando tras una prueba de recorrido (*walkthrough*) y el análisis del diseño de los controles, se llega a la conclusión de que el esfuerzo de auditoría a efectuar para verificar un control clave es despropor-

cionado, se debe realizar una adaptación de la selección de controles clave para hacer un esfuerzo viable.

También, al analizar el diseño de los controles, si el auditor identifica controles clave que considera inoperantes, el sistema de control evaluado presenta entonces una laguna. Para cubrirla debe identificar otros controles clave o controles compensatorios y evaluar su eficacia. En este caso, el auditor debe tener presente la selección completa de controles clave para evitar crear redundancias costosas en los procedimientos de auditoría.

d) Considerar el potencial de optimización

Al analizar la eficiencia del sistema de control, hay que preguntarse si los controles definidos son necesarios y si se solapan con otros controles del proceso o por controles al nivel de la entidad o si son redundantes.

Ya se ha indicado que los controles preventivos y los controles automáticos representan un potencial de economía considerable y proporcionan una seguridad más elevada.

Para identificar el potencial de mejora del diseño de los controles conviene utilizar el conocimiento y las experiencias del personal de la entidad auditada, así como las consideraciones de la dirección.

El análisis de los controles generales al nivel de la entidad ofrece un potencial de mejora considerable en el diseño de los controles, debido a su influencia global sobre el conjunto de los procesos. Este potencial optimiza los diferentes controles del proceso, los completa o incluso los reemplaza, ya que a veces, los objetivos de control son realizados de forma redundante en el marco de controles de proceso y de controles generales al nivel de la entidad.

Hay que verificar si los controles al nivel de la entidad aseguran una reacción inmediata o si no están en condiciones de aportar una respuesta adecuada más que a medio plazo.

5.8. Comprobación del funcionamiento de los controles clave mediante la realización de pruebas de cumplimiento

5.8.1. Introducción

Las pruebas de cumplimiento se realizan para obtener evidencia sobre la eficacia de los controles clave para prevenir, o detectar y corregir, errores o irregularidades significativas al nivel de las manifestaciones de las cuentas anuales.

Solo las pruebas del funcionamiento de los controles proporcionan al auditor la evidencia necesaria para evaluar el funcionamiento real de los controles durante todo el periodo auditado, la cobertura de los riesgos identificados y si se han alcanzado los objetivos de control.

La evaluación del funcionamiento de los controles mediante las pruebas de cumplimiento permite al auditor formarse una opinión sobre el sistema de control interno.

Si el auditor en las etapas iniciales de la auditoría ha considerado que los controles no están bien diseñados e implementados, no está obligado a comprobar su funcionamiento. Así los controles que no tienen un diseño efectivo o que según comprobaciones de años anteriores, no funcionan adecuadamente, y no se han introducido cambios para subsanar la deficiencia no es necesario probarlos.

Por el contrario, si se considera que los controles clave tienen un diseño efectivo y están implementados, el auditor debe realizar las suficientes pruebas de cumplimiento sobre su funcionamiento para respaldar la evaluación del riesgo de control que se haya realizado en la fase de planificación. En los casos que sea factible se deberá efectuar una planificación plurianual de las pruebas a realizar.

Debe tenerse presente que en determinados entornos informatizados complejos la sola aplicación de procedimientos sustantivos no proporcionará evidencia de auditoría suficiente para reducir el riesgo de auditoría a un nivel aceptable y será necesario realizar la evaluación del control interno y comprobar su adecuado funcionamiento mediante las pruebas de cumplimiento.

5.8.2. Objetivos

El objetivo de esta etapa de la auditoría consiste en:

- Comprobar el funcionamiento de los controles para determinar su eficacia, comprobando si el control funciona como estaba previsto y si ha sido ejecutado completamente por una persona cualificada y autorizada, durante todo el período auditado.

5.8.3. Procedimientos de auditoría

a) Aspectos generales

La comprobación del funcionamiento de los controles comprende las etapas siguientes:

- Selección de los controles clave a revisar (no deben comprobarse todos los controles). Tema tratado en el capítulo 5.5.
- Elección de la estrategia de pruebas (definir la mezcla de pruebas de cumplimiento y procedimientos sustantivos) en función de la confianza preliminar en el sistema de control interno.
- Selección de las pruebas de cumplimiento a efectuar y especialmente del tamaño de la muestra.
- Realización de las pruebas de cumplimiento.
- Evaluación de las incidencias detectadas, de la importancia de los errores y debilidades observadas y su incidencia en la estrategia de auditoría adoptada.

Estas pruebas, denominadas pruebas de controles o pruebas de cumplimiento, se realizan para obtener evidencia de auditoría sobre la efectividad operativa de los controles clave identificados previamente. Los controles seleccionados serán aquellos que respondan a riesgos identificados de manifestaciones erróneas significativas o aquellos que las prevengan o detecten y corrijan.

Esta evidencia no se refiere a las transacciones o hechos contables, sino a la efectividad operativa de los controles clave que están dirigidos a obtener seguridad de la correcta valoración de todas las transacciones y hechos ocurridos en el periodo y su registro e integración en las cuentas anuales.

En principio, aunque a los efectos de la auditoría financiera las pruebas de control son menos directas y eficaces que los procedimientos sustantivos, en general son necesarias, bien porque sea la única forma de obtener evidencia (como en los casos de entornos informatizados complejos) o porque suelen ser más eficientes cuando la población de transacciones es elevada y repetitiva y la valoración sencilla y de reducido valor unitario. En estos casos, no obstante, se requieren también pruebas sustantivas, por lo que la estrategia de auditoría debe ser combinada, incluyendo ambos tipos de procedimientos.

Cuando se auditan entidades de pequeño tamaño debe tenerse en cuenta que determinados controles internos no son practicables. Así una segregación de funciones insuficiente puede ser reemplazada por un control directo fuerte de la dirección (control compensatorio); o el auditor puede compensar la ausencia de evidencias de control con pruebas sustantivas.

La naturaleza de los procedimientos de control interno y la evidencia disponible sobre su cumplimiento determinan, necesariamente, la naturaleza de las pruebas de cumplimiento e influyen sobre el momento de ejecución y extensión de tales pruebas. Las pruebas de cumplimiento están íntimamente interrelacionadas con las pruebas sustantivas y, en la práctica algunos procedimientos de auditoría suministran, al mismo tiempo, evidencia de cumplimiento de los procedimientos de control interno contable, y evidencia sustantiva.

b) Estrategia de auditoría a adoptar

La decisión de confiar o no en los controles clave que responden a los riesgos identificados, la selección de los procedimientos (de cumplimiento o sustantivos) y el nivel de seguridad de la evidencia de las pruebas de control depende del juicio del auditor, al que las siguientes consideraciones pueden serle de utilidad:

- La evidencia que se obtiene de las pruebas de los controles se refiere a su efectividad operativa, pero no es directa[66] como la que se obtiene en las pruebas sustantivas. En todo caso, suministran evidencia sobre la información generada por el sistema de información.
- Puede proporcionar un alto grado de confianza sobre los controles clave que se prueban y se puede medir la efectividad operativa de los mismos.
- El control interno está condicionado por factores externos, entre los que destacan la posibilidad de la dirección de eludirlo.

El auditor, al decidir una estrategia de confianza en los controles, debe tener una idea muy clara de lo que se quiere probar, que las pruebas planificadas responden a lo que se quiere probar y que son conformes a las normas de auditoría. Ello requiere un claro conocimiento de los procedimientos de control a probar y una seguridad adecuadamente fundamentada de que la prueba de los mismos es lo más apropiado.

Si el auditor no tiene una idea clara de todo lo anterior corre el riesgo de que la estrategia de control sea no solo ineficiente sino también ineficaz (si la evidencia obtenida no es relevante o fiable).

66. No se refieren a un saldo contable o al importe de una cuenta de ingresos y gastos, por ejemplo.

En todo caso, si no se considera práctico establecer una estrategia basada en la confianza en los controles, y el auditor decide basarse fundamentalmente en la evidencia obtenida mediante procedimientos sustantivos, siempre debe tenerse en consideración la evidencia obtenida del conocimiento del control interno, de forma que sea posible evaluar y dar la respuesta más adecuada, a los riesgos identificados de manifestaciones erróneas significativas.

c) Diseño de las pruebas de cumplimiento

Al diseñar las pruebas de los controles que responden a los riesgos de las manifestaciones contenidas en las transacciones, hechos contables y saldos de cuentas, puede ser de utilidad para el auditor la consideración, entre otras cuestiones, de:

1. Lo que se ha de probar

Lo que normalmente se ha de probar son los controles existentes sobre el correcto registro de las transacciones y de los hechos contables. Entre dichos controles sólo suministran evidencia de auditoría relevante aquellos que previenen o detectan y corrigen manifestaciones erróneas; el resto de los controles o no suministran evidencia, o la evidencia que suministran no es lo suficientemente clara o útil. Los primeros son los controles clave.

Conviene distinguir entre controles de transacciones, hechos contables, registros contables y mantenimiento del control responsable de los saldos de cuentas, ya que esto proporciona una mayor claridad de lo que se ha de probar.

Procedimientos de control de transacciones.

Cuando se establece una estrategia de confianza en el control interno, normalmente se efectúa sobre las principales clases de transacciones (no sobre todas), ya que generalmente reúnen las condiciones en las que una estrategia de confianza en el control interno es más eficiente. Suelen constituir las partidas más representativas de las actividades de la entidad y ser de valor unitario relativamente reducido, repetitivas y fácilmente medibles.

Procedimientos de control sobre hechos contables

Cuando se trate de hechos contables cuya población no sea elevada o no sean repetitivos, suele ser más efectivo el uso de pruebas sustantivas sobre su valoración y acaecimiento, especialmente cuando sea compleja y, en todo caso, limitar las pruebas de control a la manifestación de integridad.

De todos modos, el auditor puede considerar necesaria o más adecuada una estrategia de confianza en los controles sobre la valoración del hecho en las siguientes situaciones:

- Dado que para obtener evidencia de la correcta valoración de un hecho contable, se requiere la evaluación de información generada por el sistema de información de la entidad (en cuyo caso el auditor debe obtener evidencia sobre la exactitud e integridad de la misma), puede ser necesario o más práctico establecer una estrategia de confianza en los controles existentes sobre dicha información.
- En el caso de que la acumulación de hechos de la misma naturaleza fuese representativa, y los hechos fuesen de valor unitario relativamente reducido, repetitivos y fáciles de medir.

2. Procedimientos de auditoría para obtener evidencia sobre la confianza en los procedimientos de control

Los procedimientos a diseñar y ejecutar son aquellos que suministran evidencia sobre la efectividad operativa de los controles durante todo el periodo auditado.

La eficacia y eficiencia de los procedimientos de auditoría para obtener evidencia sobre la confianza en los procedimientos de control son un factor determinante que condiciona la estrategia de auditoría. Estos procedimientos están condicionados por el entorno informatizado del sistema de información.

En un entorno informatizado simple es posible obtener evidencia mediante pruebas de los controles manuales. Para la obtención de evidencia en un entorno informático complejo se requerirá una confianza previa de dicho entorno (mediante la revisión de los controles generales de los sistemas de información) y las pruebas, a nivel de aplicación, diseñadas sobre los controles dependerán del tipo de control (manual o informatizado).

d) Tipos de pruebas para los controles de aplicación

Los procedimientos para obtener evidencia son la inspección de los controles documentados en registros y documentos y la observación del funcionamiento operativo de los controles mediante alguno de los tipos de pruebas siguientes:

- Test único:

  Un control programado debe ser, en principio, probado una sola vez. Después de lo cual se considera que funciona de manera eficaz, a condición de que el entorno TI sea estable

y que los controles generales TI hayan funcionado durante todo el periodo auditado. El auditor debe comprobar que el control probado funciona como está previsto en el conjunto de las situaciones razonablemente posibles.

– Test directo:

  El funcionamiento del control se comprueba sobre la base de una muestra o por el análisis de transacciones.

– Pruebas masivas de datos:

  En estos casos la eficacia de un control es comprobada mediante un análisis de los datos con ayuda de CAAT.

  El uso de técnicas de auditoría asistida por ordenador posibilita una mayor extensión de las pruebas sobre transacciones electrónicas y archivos contables, que puede ser útil cuando el auditor decida modificar la extensión de las pruebas, por ejemplo, en respuesta a los riesgos de manifestaciones erróneas de la dirección de carácter significativo debido irregularidades. Estas técnicas pueden usarse para seleccionar muestras de transacciones de archivos electrónicos clave, para filtrar transacciones con características específicas, o comprobar toda una población en lugar de una muestra.[67]

  Un ejemplo típico se puede encontrar al auditar los gastos de personal de un ayuntamiento. Además de revisar la aplicación informática que soporta ese proceso e identificar controles clave, se deben realizar pruebas de cumplimiento de los mismos. Algunas de las pruebas de cumplimiento, que tradicionalmente se realizan sobre una muestra seleccionada aleatoriamente o mediante muestreo estadístico, actualmente si se dispone de herramientas CAAT puede hacerse un planteamiento diferente y decidir hacer la comprobación sobre el 100% a partir de la Relación de Puestos de Trabajo del Ayuntamiento. Está prueba aportará al auditor tanto evidencia de cumplimiento de los controles como sólida evidencia sustantiva.

  Es decir, este tipo de pruebas pueden realizarse como pruebas de cumplimiento de los controles, como procedimientos sustantivos o con carácter mixto.

  En el capítulo 8 se describe in extenso las posibilidades de utilización de los CAAT.

67. ISA 330, párrafo A16.

– Muestreo

El muestreo estadístico es, en principio, el medio idóneo para expresar en términos cuantitativos el juicio del auditor respecto a la razonabilidad, determinando la extensión de las pruebas y evaluando su resultado.

Las pruebas de cumplimiento deberán aplicarse a las transacciones ejecutadas durante el período que se está revisando, de acuerdo con el concepto general de muestreo, que implica que las partidas que vayan a ser examinadas deben seleccionarse del conjunto de datos a los cuales deben aplicarse las conclusiones resultantes. Deberá dejarse constancia en los papeles de trabajo del criterio utilizado en la selección de la muestra.

La determinación de una muestra representativa depende del juicio del auditor, especialmente si la población es relativamente reducida. En casos de probación elevada, es de utilidad para el auditor usar como referencia los criterios estadísticos que se aplicarían de la determinación del tamaño de la muestra, por la eficiencia de poder obtener conclusiones con la muestra más reducida posible.

En las pruebas de la efectividad operativa de los controles sobre documentos contables, lo más apropiado es la aplicación del muestreo de atributos cuando la población es elevada. En el muestreo de atributos el tamaño de la muestra viene determinada en una tabla cuyos parámetros están basados en la conclusión que el auditor pretenda obtener, con un nivel determinado de seguridad (90% ó 95%), que el número de errores o incumplimiento de los atributos para cada uno de los controles probados no excederá de un máximo que considere aceptable.

En las pruebas sustantivas, lo más apropiado para la determinación del tamaño de la muestra cuando la población es elevada, es la aplicación del método de unidad monetaria. Mediante dicho método el tamaño de la muestra viene determinado por la siguiente fórmula:

$$TM = P / (ET/FC)$$

Donde:

TM = Tamaño de la muestra
P = Importe monetario de la población
ET = Error tolerable
FC = Factor de confianza
ET / FC = Intervalo de muestreo

– Selección sobre bases subjetivas

  Cuando se utilicen bases subjetivas se deberá dejar constancia en los papeles de trabajo de las razones que han conducido a tal elección, justificando los criterios y bases de selección, y determinando el grado de confianza a depositar en el control interno.

e) Cuestiones relativas a la evaluación del funcionamiento de los controles

Los siguientes factores pueden influir en el procedimiento de comprobación y en el nivel de seguridad obtenido por el auditor:

– Frecuencia de realización del control:

  Cuanto más baja sea la frecuencia de realización de un control manual menor es la cantidad de casos a comprobar.

– Importancia del control:

  Cuanto más se apoye el auditor en un control para formar su opinión de auditoría, más debe ser comprobado ese control.

– Validez del justificante del control:

  Si el control genera evidencias ligadas a la eficacia de su funcionamiento (trazabilidad, exhaustividad, exactitud, sellado de tiempo), la cantidad de casos a comprobar puede ser menor que en caso de controles sin justificantes documentados.

– Importancia relativa de las incidencias:

  Depende de la importancia, la complejidad y la cantidad de transacciones tratadas.

– *Management override*:

  Evaluación de la probabilidad de eludir o de forzar un control por una persona con responsabilidad.

– Frecuencia de cambio de los controles:

  La eficacia del control puede ser considerablemente influida por cambios en el control mismo o en el proceso en el que está implantado.

f) Evaluación de las incidencias detectadas

Cuando el auditor encuentra una excepción, en relación con el resultado esperado de la prueba, debe establecer si se trata de un caso aislado, estadísticamente previsible y por tanto aceptable.

Si por el contrario no era previsible ninguna diferencia o si las diferencias surgen frecuentemente, conviene analizar su origen.

Para comprobar si el número de incidencias no sobrepasa un límite aceptable, es posible, por ejemplo, ampliar los muestreos.

Si el resultado de la prueba muestra los controles como inoperantes, se deberán identificar controles compensatorios. Si no se identifica ningún control compensatorio, deberá revisarse la evaluación preliminar del riesgo, su efecto en los procedimientos y en las conclusiones de la auditoría.

El auditor calificará el riesgo de auditoría como alto cuando los controles no pueden evitar, identificar y corregir una anomalía importante.

5.8.4. Documentación de las pruebas

En los papeles de trabajo se deberá documentar lo siguiente:

- El objetivo de las pruebas, el auditor que las ejecuta y la fecha.
- Los controles (incluida versión) y objetivos de control revisados.

  Se describirán las técnicas de control utilizadas por la entidad para llevar a cabo las actividades de control pertinentes. Se detallará por nivel (por ejemplo, a nivel de la entidad, del sistema, proceso de negocio), así como por subnivel de sistema (p. ej. red, sistema operativo, middleware, SGBD, aplicaciones).
- Procedimiento utilizado (muestreo, totalidad de casos, ...).
- Tipo de pruebas realizadas, calendario, alcance de las pruebas y resultados.
- Los suficientes detalles para que un tercero experto en la materia pueda comprender la eficacia de las pruebas realizadas en términos de evaluación del riesgo de auditoría.
- Evidencia que justifique que las técnicas de control son aplicadas de manera eficaz o evidencia que justifiquen que éstas no existen (p. ej. resúmenes que describan los procedimientos, resultados y output de las herramientas y otros análisis relacionados);
- Si una actividad de control no se lleva a cabo, cualquier control compensatorio que exista, así como la fundamentación para determinar si éstos son efectivos;

- Las conclusiones del auditor sobre la eficacia de los controles de los sistemas de información de la entidad a la hora de realizar la actividad de control propiamente dicha.
- Descripción de las incidencias, recomendación efectuada, prioridad, responsable del control y de aplicar la recomendación situación de la puesta en práctica de medidas de mejora o cualquier información cualitativa complementaria.
- En caso de incidencias importantes, el auditor debe proporcionar la siguiente información: tamaño de la muestra (si procede), número de excepciones o de pruebas con error, tipo y causa de la incidencia.

  Para cada debilidad detectada, se señalará, si se trata de una deficiencia significativa, o una debilidad material, así como los criterios, condiciones, su causa y efecto.

Finalmente, el trabajo realizado se resumirá en un cuadro como el de la figura siguiente para facilitar su comprensión (tanto por el auditor como por el personal de la entidad al que se le comunique la incidencia) y la emisión posterior del informe.

Pruebas de cumplimiento Entidad: Ayuntamiento de X Y Z
Proceso de negocio: *Contratación de inversiones* Subproceso: *Adjudicación* Cuentas relacionadas: Aplicación informática: *SAP*

Control clave	Prueba realizadas	Resultado	Responsable del control	Aplicación o sistema afectado	Recomendación	Prioridad	Referencia
(Describir el CC e indicar su identificador secuencial)	Describir sucintamente	Describir sucintamente	Indicar	(Si hubiera más de una aplicación soportando el proceso)	Describir	Alta Media Baja	Referencia al papel de trabajo
C001A-Descripción							
C001A-Descripción							
C001B-Descripción							

Figura 5.14

5.9. Procedimientos sustantivos

La combinación adecuada de las pruebas de auditoría permite al auditor minimizar el riesgo final mediante un adecuado equilibrio entre pruebas de cumplimiento y pruebas substantivas.

El peso relativo atribuible a las respectivas fuentes de confianza y la estrategia de auditoría, son materias que deben decidirse de acuerdo con el criterio del auditor y según las circunstancias.

La amplitud de las pruebas substantivas a realizar sobre los distintos componentes de las cuentas anuales, así como su naturaleza y el momento de su aplicación, será tanto menor cuanto mayor sea la confianza obtenida de las pruebas de cumplimiento del control interno.

5.9.1. Objetivo

El objetivo de esta etapa de la auditoría consiste en:

– Obtener evidencia de auditoría respecto de todas las clases de transacciones, saldos de balance y revelaciones en las cuentas anuales.

5.9.2. Procedimientos de auditoría

Los procedimientos sustantivos están diseñados para responder a los riesgos evaluados de que existan errores o irregularidades significativas al nivel de las manifestaciones.

Hay dos tipos de procedimientos sustantivos:

a) Pruebas de detalle sobre clases de transacciones, hechos contables, saldos de cuentas y revelaciones en la memoria.

   Estas pruebas están diseñadas para obtener evidencia que respalde un importe (saldo, clase de transacción o revelación) de las cuentas anuales. Se usan para obtener evidencia sobre ciertas manifestaciones, como existencia, exactitud y valoración.

b) Procedimientos analíticos.

   Estos procedimientos están diseñados para comprobar relaciones predecibles entre magnitudes financieros y no financieras. Se aplican principalmente a grandes volúmenes de transacciones que tienden a tener un comportamiento predecible a los largo del tiempo.

6

Conclusiones generales y emisión de informe

6.1. Introducción

Si las deficiencias de los controles pueden afectar significativamente a la exactitud de la opinión de auditoría sobre las cuentas anuales, y si este riesgo no puede ser compensado por otros controles, debe evaluarse el impacto de las debilidades significativas sobre el informe de auditoría.

Esta evaluación se hará considerando las tres cuestiones siguientes:

- ¿Se trata de un hecho que afecta a la situación financiera y a la opinión de auditoría?
- ¿Se trata de un incumplimiento de una norma?

El tratamiento por parte del auditor público en su informe dependerá del tipo de informe que deba emitir: informe de auditoría de cuentas anuales o informe «corto» o informe de regularidad contable o informe «largo»:

- Si se emite un informe «corto», el auditor de sistemas emitirá un memorándum interno para documentar su trabajo, pero normalmente el informe de auditoría solo recogerá alguna incidencia que tenga un efecto material sobre las cuentas anuales y provoque una salvedad en el mismo.

  En estos casos podría emitirse un informe adicional o carta de recomendaciones sobre aspectos de control interno y recoger las principales incidencias o debilidades de control derivadas de la auditoría de sistemas de información, incluyendo recomendaciones para su subsanación.
- Si se emite un informe «largo», que es lo más habitual entre los auditores externos públicos, se podrá incluir un apartado dedicado a exponer los resultados de la auditoría de los sistemas de información, donde se recogerán las debilidades materiales y las deficiencias significativas, incluyendo recomendaciones para su subsanación.

6.2. Objetivos

Los objetivos de esta etapa son:

- Considerar el efecto de los hallazgos de la auditoría de sistemas en la opinión de auditoría financiera.
- Emitir, en su caso, un informe de auditoría de sistemas o un informe sobre recomendaciones de control interno.

6.3. Procedimientos de auditoría

a) Evaluación de los resultados obtenidos

Después de finalizar la ejecución del trabajo de campo y de completar las pruebas de auditoría, el auditor debe resumir los resultados de la auditoría, redactar las conclusiones individuales de las debilidades de control detectadas en el sistema de información, considerar su efecto agregado, y redactar el informe de auditoría.

En esta evaluación se debe considerar:

1. El efecto de las debilidades identificadas por el auditor en las pruebas realizadas.
2. El seguimiento de las debilidades incluidas en informes anteriores.

El auditor concluirá sobre si las debilidades de control consideradas individualmente o de forma conjunta, constituyen una deficiencia significativa o una debilidad material de la información financiera. Esta evaluación debe hacerse coordinadamente con el equipo de auditoría financiera. Para realizar esta evaluación es necesario tener claros los siguientes conceptos y definiciones anticipados en el capítulo 4.5:

- Una deficiencia de control interno existe cuando el diseño o el funcionamiento de un control no permite al personal de la entidad o a su dirección, en el curso ordinario de las operaciones, prevenir o detectar errores o irregularidades en un plazo razonable. Pueden ser deficiencia de diseño del control (cuando un control necesario para alcanzar el objetivo de control no existe o no está adecuadamente diseñado) o deficiencias de funcionamiento (cuando un control adecuadamente diseñado no opera tal como fue diseñado o la persona que lo ejecuta no lo realiza eficazmente).
- Una deficiencia significativa es una deficiencia en el control interno, o una combinación de deficiencias, que afectan ad-

versamente la capacidad de la entidad para iniciar, autorizar, registrar, procesar o reportar información financiera de forma fiable de conformidad con los principios o normas contables y/o presupuestarias aplicables, y existe una probabilidad que es más que remota, de que una manifestación errónea en las cuentas anuales, que no es claramente trivial, no sea prevenida o detectada.

– Una debilidad material es una deficiencia significativa en el control interno o una combinación de ellas, respecto de las que existe una razonable posibilidad de que una manifestación errónea significativa en las cuentas anuales no sea prevenida o detectada y corregida en plazo oportuno.

Para determinar si una deficiencia de control, individualmente o junto con otras, constituye una deficiencia significativa o una debilidad material, el auditor considerará varios factores, incluyendo los siguientes:[68]

– La probabilidad de que una persona pueda obtener acceso no autorizado o ejecutar actividades no autorizadas o inapropiadas en sistemas críticos de la entidad o archivos que puedan afectar a la información con efecto en las cuentas anuales. Esto puede incluir (1) la habilidad para tener acceso a sistemas en los que residen aplicaciones críticas y que posibilita a usuarios no autorizados a leer, añadir, borrar, modificar o extraer información financiera, bien directamente o a través de la utilización de software no autorizado; (2) la habilidad para acceder directamente y modificar ficheros que contengan información financiera; o (3) la habilidad para asignar derechos de acceso a las aplicaciones a usuarios no autorizados, con la finalidad de procesar transacciones no autorizadas.

– La naturaleza de los acceso no autorizados que pueden conseguirse (por ejemplo: limitados a programadores del sistema o de las aplicaciones o a administradores del sistema; a todos los usuarios autorizados del sistema; a alguien externo a través de acceso no autorizados por Internet) o la naturaleza de las actividades no autorizadas o inadecuadas que pueden llevarse a cabo.

– La probabilidad de que importes de las cuentas anuales estén afectados de forma significativa.

68. FISCAM página 123.

- La probabilidad de que otros controles incluyendo los controles de aplicación puedan prevenir o detectar accesos no autorizados. Generalmente, si la efectividad de esos controles depende de la información procesada por el sistema, es improbable que pueda prevenir eficazmente o detectar dichos accesos; salvo que la debilidad de control identificada, razonablemente, no sea capaz de comprometer la eficacia de los otros controles.
- El riesgo de que la dirección de la entidad pueda burlar los controles (por ejemplo, mediante derechos de acceso excesivos).

Basándose en estas consideraciones el auditor determinará si las deficiencias de control son, individualmente o en conjunto, debilidades materiales o deficiencias significativas. El auditor también debe determinar si las deficiencias significativas son en conjunto debilidades materiales.

Si las deficiencias de control constituyen debilidades materiales, el auditor concluirá que los controles internos no son eficaces.

b) Formulación de las conclusiones

Se deben compilar los resultados individuales de los procedimientos de auditoría realizados a lo largo del trabajo de auditoría. Debe evaluarse el impacto sobre los estados financieros de los controles inexistentes, los mal diseñados y los que no han funcionado de forma efectiva durante el periodo auditado.

A pesar de los medios auxiliares existentes, las conclusiones de los trabajos requieren necesariamente la aplicación del juicio profesional del auditor para tener en cuenta las peculiaridades de la entidad, las exigencias relacionadas con los procesos y aquellas específicas de los riesgos. Esto exige una discusión profunda en el seno del equipo auditor para definir si fueran necesarios procedimientos de auditoría suplementarios.

Las deficiencias identificadas en la evaluación de los controles clave y no corregidas por controles compensatorios deben ser evaluadas, por definición, de forma más crítica que las deficiencias de los otros controles.

Como paso final de la auditoría de sistemas de información se debe concluir sobre el efecto acumulado de las debilidades de control de las aplicaciones de negocio que se hayan detectado a lo largo del trabajo.

Se deberá tener en cuenta las interdependencias potenciales de los controles (p.e. los controles cuya efectividad depende de de la efectividad de otros controles).

En esta etapa de formulación de las conclusiones se evalúan los resultados de las anteriores etapas de la auditoría y se sintetizan en una evaluación global en función de su influencia sobre las cuentas anuales.

En el informe se pueden incluir recomendaciones para la introducción de medidas correctoras.

El auditor puede, en algunos casos, emitir una opinión sobre la adecuación del sistema de control interno y su capacidad para evitar errores significativos en las cuentas anuales con un nivel de seguridad razonable.

Si el auditor emite un informe «largo» o un informe adicional de control interno, se emitirá una valoración general sobre:

- Las debilidades existentes en los controles generales TI.
- La medida en que la aplicación revisada soporta el proceso de negocio (diseño y funcionamiento de los controles).
- La presencia de lagunas de control significativas en la aplicación.
- El impacto de las lagunas de control sobre los procesos de la aplicación y sobre el proceso global así como sobre las manifestaciones relacionadas de los estados financieros.
- La presencia en el proceso de negocio de controles que compensen el impacto de las debilidades de control detectadas en la aplicación y las comprobaciones y procedimientos sustantivos de auditoría adicionales que sean necesarios.

Terminología utilizada

Es importante que el informe se redacte utilizando una terminología que sea comprensible para personas que tienen un conocimiento limitado en lo que se refiere a los sistemas informatizados. Con este fin, puede ser conveniente incluir en el informe una definición de los términos técnicos y se debe evitar jerga y abreviaturas y acrónimos no definidos.

Al presentar los resultados es importante señalar el marco de referencia utilizado en la auditoría y redactar las conclusiones y recomendaciones sobre esa base, para evitar componentes de subjetividad.

Por ejemplo, será más efectivo decir «la gestión de passwords no es conforme con la norma sobre seguridad de la información

ISO27001» que «la seguridad de los passwords puede ser mejorada».

c) Comunicación y discusión del borrador de informe

Antes de realizar el informe se deben comentar con los responsables de la entidad fiscalizada las debilidades significativas detectadas, para obtener su conformidad con los hechos descritos y tener la oportunidad de conocer sobre la existencia de aspectos adicionales de relevancia para la evaluación de los efectos de cada debilidad observada.

La comunicación a los gestores de las debilidades observadas generalmente incluirá la siguiente información:

- Naturaleza y amplitud del riesgo.
- Objetivos de control.
- Actividad de control.
- Incidencia detectada (incluyendo descripción, criterio de referencia, causa y efecto si es posible).
- Recomendaciones.

d) Confidencialidad

En todo caso, el auditor de sistemas de información tendrá especial cuidado en no desvelar en sus informes información confidencial o sensible relativa a los sistemas de información (información técnica relativa a las debilidades en los controles de acceso podría facilitar acceso no autorizados de terceros). Con esta finalidad, para evitar desvelar información confidencial, el auditor proporcionará un borrador del informe a la entidad para que revise dichos aspectos de seguridad y confidencialidad.

Se tendrá especial cuidado en la distribución de borradores y se controlarán todas las copias emitidas.

Si el informe finalmente contiene información que puede afectar a la seguridad o a aspectos confidenciales, no se deberán publicar en la página web ni de la entidad auditada ni de la entidad auditora. No obstante se deberá atender a las exigencias legales aplicables en cada caso.

En determinados casos puede ser adecuado la realización de un resumen ejecutivo del informe de la auditoría de sistemas de información, que será público, y un informe detallado de carácter restringido.

6.3. Tipos de informe a emitir

Dependiendo del tipo y objetivos de la auditoría (auditoría de cuentas anuales, auditoría de regularidad contable, etc), la legislación reguladora del auditor público y las normas técnicas de auditoría que se apliquen, la plasmación del trabajo del auditor de sistemas de información en el informe final puede ser muy diferente. A modo de síntesis, pueden señalarse varias situaciones:

a) Auditoría de cuentas anuales

Este tipo de auditoría es la misma en el sector público o privado, y el auditor financiero emite un «informe corto» sobre si las cuentas anuales auditadas reflejan la imagen fiel del patrimonio, la situación financiera y los resultados del ejercicio.

El trabajo del auditor de sistemas de información se habrá condensado en un informe interno o memorando, que contendrá las conclusiones sobre la confiabilidad de los controles revisados y su incidencia en el riesgo de manifestaciones erróneas significativas en las cuentas anuales. El auditor financiero habrá evaluado (junto con el auditor de sistemas) el efecto de estas conclusiones sobre la estrategia de pruebas sustantivas planificada, adoptado las modificaciones que procedan y considerado el efecto final de la evidencia obtenida sobre la opinión de auditoría financiera.

Podrá emitirse adicionalmente una carta de recomendaciones de control interno en la que se incluyan las debilidades detectadas y recomendaciones para su mejora.

b) Auditoría de regularidad contable

En estos casos, normalmente, los informes son largos, con descripción detallada del trabajo realizado y de las incidencias detectadas.

El trabajo de la auditoría de sistemas de información en estos casos puede ser similar al señalado en el apartado anterior, o disponer de un apartado propio en el informe en el que se detallen los aspectos más relevantes del trabajo realizado, señalando las debilidades de control detectadas, sus efectos, y proponiendo recomendaciones para su mejora.

En estos casos debe tenerse cuidado con los aspectos relacionados con la seguridad y confidencialidad que se mencionan más adelante.

Analizados los cuatro informes publicados hasta la fecha, señalados en el apartado 1.1, por la Sindicatura de Cuentas de la Comunidad

Valenciana (los otros no pueden considerarse de auditorías de sistemas de información integradas en auditorías financieras, que es el objeto de este trabajo) vemos que tienen la siguiente estructura y contenido:

1. Estructura de los informes

Con ligeras variaciones los informes de fiscalización analizados[69] tienen la siguiente estructura general:

- Apartados 1-2-3 con los objetivos, alcances y conclusiones generales.
- Apartado 4 dedicado a la revisión financiera.
- Apartado 5 dedicado a la revisión de algún área legal (normalmente contratación o subvenciones).
- Apartado 6 de dedicado a la auditoría de sistemas de información:
  a) Introducción.
  b) Área de controles generales de los sistemas de información.
  c) Área de controles sobre procesos de negocio y aplicaciones informáticas.
- Apartado 7 Recomendaciones.

2. Contenido

En figura siguiente se ha elaborado un cuadro resumen con las principales deficiencias de control mencionadas en los cuatro informes analizados:

Tipo de deficiencia de control	Informe			
	A	B	C	D
Área de controles generales TI:				
Plan de continuidad de negocio y Plan de recuperación de desastres.	X	X	X	X
Autenticación de usuarios y seguridad lógica.	X	X		X
Política de formación-concienciación en seguridad.		X	X	X
Riesgos físicos del CPD.	X		X	X
LOPD	X	X	X	
Políticas generales y la normativa de seguridad.	X	X		
Gestión de usuarios y privilegios.	X	X		
Metodología de desarrollo.			X	X

69. Accesibles en la página web de la Sindicatura: www.sindicom.gva.es/web/wdweb.nsf/menu/informes.

Vulnerabilidad accesos remotos.			X	X
Procedimientos de desarrollo y cambios (seguridad y segregación de funciones).	X	X		
Procedimiento formal de copias de seguridad.	X			
Política general del departamento de informática.	X			
Dependencia de outsourcers.			X	
Organigrama del departamento TI y funciones y responsabilidades de su personal.	X			
Área de controles aplicativos:				
Gestión de perfiles de usuarios	X	X		
Segregación de funciones	X	X		
Incidencias particulares de la aplicación revisada	X			

Figura 6.1

c) Recomendaciones

Los auditores desarrollarán los elementos de las incidencias de auditoría, con la extensión requerida por los objetivos de la auditoría. De acuerdo con esos objetivos se desarrollarán también recomendaciones para la introducción de medidas correctoras.

Es conveniente seguir una serie de criterios generales en la formulación de las recomendaciones:[70]

- Deben ser claras y concretas.
- Deben evitarse las recomendaciones genéricas, procurando identificar el departamento o cargo concreto responsable de su adopción.
- Ser convincentes en el fondo y en la forma. Para ello deben estar sólidamente soportadas por hechos y argumentarse de un modo lógico.
- Estar formuladas de manera positiva y constructiva, evitando el tono negativo o recriminatorio hacia los gestores públicos. Evitar expresiones tajantes en su formulación.
- Ser coherentes con recomendaciones formuladas en informes anteriores.
- Ser relevantes y, en todo caso, derivarse de su aplicación beneficios potenciales, superiores al coste que conlleve su puesta en práctica.

70. Fuente: Manual de fiscalización de la Sindicatura de Cuentas de la Comunidad Valencia – Sección 703. www.sindicom.gva.es/web/valencia.nsf/documento/manual_de_fiscalizacion.

- Normalmente solo se redactarán las recomendaciones cuando se hayan encontrado soluciones admisibles y con un coste-beneficio razonable, a las debilidades detectadas.
- Debe darse especial atención a las recomendaciones más importantes, que se enfatizarán de alguna forma (p.e. ordenándolas según su importancia). Se debe de centrar la atención en aquellas que se consideren más relevantes.
- Es deseable que sean asumidas por los gestores públicos durante la realización del trabajo de campo asegurando así, en la medida de lo posible, su adopción futura.

Siempre deben ser comentadas junto con el resto del informe, con carácter previo, con los responsables de las entidades fiscalizadas.

6.4. Documentación en la fase de elaboración del informe

El auditor deberá documentar la siguiente información desarrollada en la fase de elaboración del informe:

1. La conclusión del auditor sobre la eficacia de los controles de los sistemas de información (en relación con los objetivos de la auditoría de los sistemas de información) y la fundamentación de la conclusión, incluidos los factores que el auditor consideró oportunos.
2. En caso de que forme parte de una auditoría más amplia, las consecuencias que las debilidades detectadas en el control de los sistemas de información puedan tener en la consecución de los objetivos globales de la auditoría.
3. Copias de los informes o cualquier comunicación por escrito elaborada con relación a la auditoría, y los comentarios o alegaciones emitidos por la dirección de la entidad sobre dichos informes y comunicaciones.
4. Para las auditorías financieras, la decisión del auditor sobre si las debilidades detectadas representan debilidades materiales o son deficiencias significativas, y la fundamentación de las conclusiones del auditor.
5. Cualquier otra documentación que sea requerida por las políticas y procedimientos de auditoría de la entidad auditora, incluidos los procesos de garantía de calidad.
6. Los resultados de los procedimientos llevados a cabo para detectar cualquier fraude que sea significativo para los objetivos de la auditoría y el impacto sobre la auditoría.

7. Los resultados de los procedimientos de seguimiento para determinar si han sido aplicadas medidas correctivas, basándose en análisis de riesgo y de coste-beneficio, con la finalidad de subsanar las debilidades de control de los sistemas de información que hayan sido incluidas en informes anteriores.

A efectos internos se debe elaborar un memorando que incluya una descripción del sistema, mapa de aplicaciones, flujogramas, riesgos, controles cuya utilidad principal sea servir de Archivo permanente para futuras auditorías.

7

Sistemas de información integrados y aplicaciones de negocio

7.1. Aspectos generales

7.1.1. Introducción

Actualmente existe en el mercado un amplio abanico de sistemas informáticos integrados, con un mayor o menor grado de complejidad y de estandarización (ver capítulo 7.5.1 para mayor detalle), que ofrecen una variedad de funcionalidades y servicios a las empresas y organizaciones públicas y privadas, impensable hace unos años.

Cada configuración posible de un sistema informático, presenta unas características propias en cuanto a seguridad, funcionamiento, controles, etc. que condiciona el trabajo de auditoría, exigiendo la adaptación de los procedimientos que debe aplicar el auditor de sistemas de información.

Así, como complemento a la metodología general expuesta en los capítulos anteriores, en el presente capítulo vamos a dar un repaso a diferentes aspectos relacionados con las características particulares de los distintos componentes de un sistema de información. También comentaremos algunas de las características relevantes de los principales y más usuales entornos comerciales ERP con los que sin duda cualquier auditor público se va a encontrar en el desarrollo de sus trabajos.

7.1.2. Tipos de aplicaciones de negocio

Comenzaremos familiarizándonos con algunas siglas habituales cuando se estudia o analiza esta materia; cada una de ellas representa un tipo de herramienta informática o aplicación de negocio que hoy en día puede encontrase en cualquier plataforma o sistema informático comercial:

- ERP Enterprise Resource Planning / Planificador de recursos de la empresa

  Los ERP permiten a las empresas y entidades llevar a cabo tareas financieras, gestión de recursos humanos, compras y logística, desarrollo de productos y producción, ventas, etc.

  Los ERP incrementan la eficiencia dentro de la organización y ayudan a extender desde extremo a extremo los procesos

de negocio, desde los proveedores a los clientes, pasando por toda la cadena de producción de un bien o servicio.

Esta es la herramienta que normalmente va a ser objeto de análisis en una auditoría de sistemas de información integrada en una auditoría financiera, ya que incluye e integra los procesos y aplicaciones relacionadas con la formulación de las cuentas anuales.

- CRM Customer Relationship Management / Gestor de relaciones con clientes

  Con los CRM las entidades son capaces de conseguir y mantener clientes, adquirir un conocimiento más profundo de sus clientes y mercados, y alinear la organización hacia estrategias orientadas a sus clientes.

- PLM Product Lifecycle Management / Gestor del ciclo de vida de productos

  Un PLM ayuda a los fabricantes proporcionándoles una única fuente para toda la información relacionada con los productos y la producción, necesaria para colaborar con los proveedores y gestionar eficazmente la producción.

- SCM Supply Chain Management / Gestor de la cadena de aprovisionamientos

  Ayuda a las empresas a mejorar la flexibilidad operativa y proporciona información en tiempo real de clientes y proveedores.

- SRM Supplier Relationship Management / Gestor de relaciones con los proveedores

  Con estas herramientas clientes y proveedores pueden colaborar estrechamente e integrar procesos con aplicaciones interempresas para mejorar la transparencia y reducir costes.

- HRM Human Recurse Management / Gestor de Recursos Humanos

  Gestiona todos los aspectos relacionados con los recursos humanos de una entidad. Junto con los ERP y CRM son de las aplicaciones más utilizadas actualmente.

7.1.3. Situación global del mercado de las aplicaciones de negocio

Según el *SAP Annual Report 2008* el mercado de aplicaciones de negocio (concepto que incluye ERP, PLM, HRM, CRM, etc) ha tenido la siguiente distribución, por proveedores:

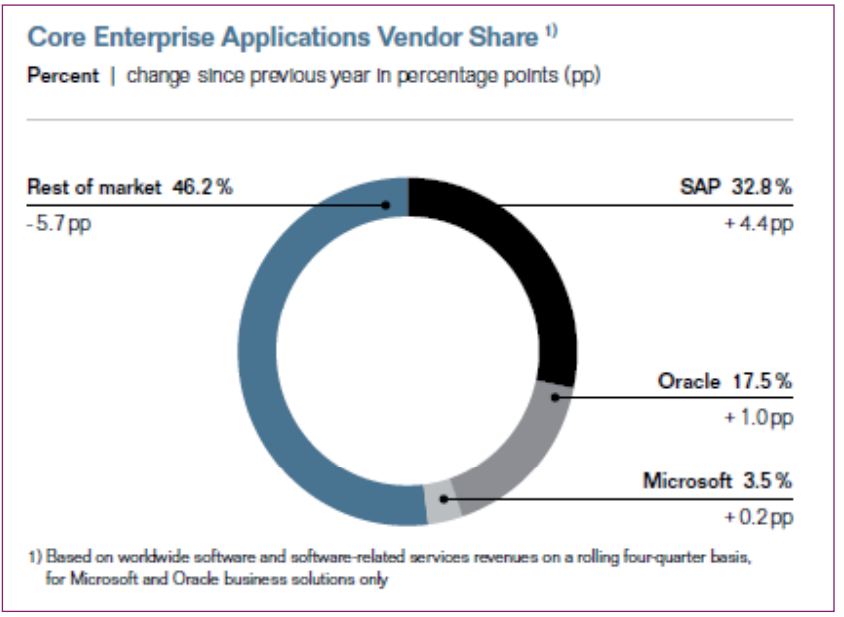


Figura 7.1

Puede observarse que SAP mantiene una posición dominante a nivel mundial con casi un tercio del mercado de las aplicaciones de negocio. Oracle, aunque en el sector de aplicaciones de negocio solo cubre un 17,5% de cuota de mercado, domina en otros apartados como el de las bases de datos o el de middleware. Otro actor importante en el mundo del software, Microsoft, que es un relativamente recién llegado al mercado de las aplicaciones de negocio, solo alcanza un 3,5% de cuota de mercado.[71]

7.1.4. Situación en España de las aplicaciones de negocio

Los ERP y herramientas similares como los CRM, son cada vez más utilizados en nuestro país. Según el *informe eEspaña 2009*,[72] dos de las soluciones de gestión más ampliamente utilizadas por las empresas son los sistemas CRM y ERP (ver figura siguiente, extraída del mismo informe).

71. Según el estudio de AMR Research, *The Global enterprise Market Sizing Report 2008-2013*, en 2008 las empresas Sage Group, Infor, Dassault Systemes y Siemens PLM, tuvieron una cuota de Mercado superior a la de Microsoft. En conjunto esas cuatro empresas alcanzaron una cuota de casi el 16% de mercado según AMR Research. El resto de mercado está muy atomizado.

72. Informe anual sobre el desarrollo de la sociedad de la información en España *(Informe eEspaña 2009)*, Fundación Orange, 2009

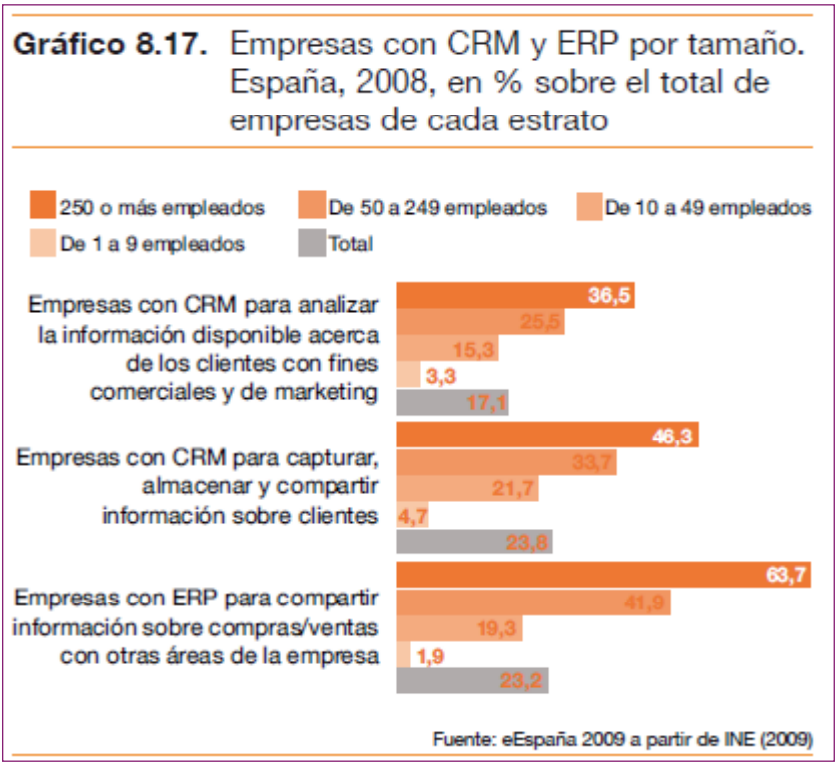


Figura 7.2

Ambas herramientas han experimentado un notable crecimiento en relación con los datos del año anterior (17,96% y 12,53% para ERP y CRM, respectivamente) según la misma fuente.

Al igual que en otras tecnologías, persiste el notable desequilibrio en la utilización de estas soluciones entre empresas grandes y microempresas, que presentan valores muy bajos.

Por sector de actividad, el CRM es la herramienta mayoritaria en los sectores con mayor contacto con el consumidor final (sector financiero, servicios, construcción), mientras que el ERP predomina en el resto de sectores, como los industriales.

En cualquier caso, según la misma fuente, es el sector financiero el que muestra mayor disposición al uso de ambas soluciones tecnológicas:

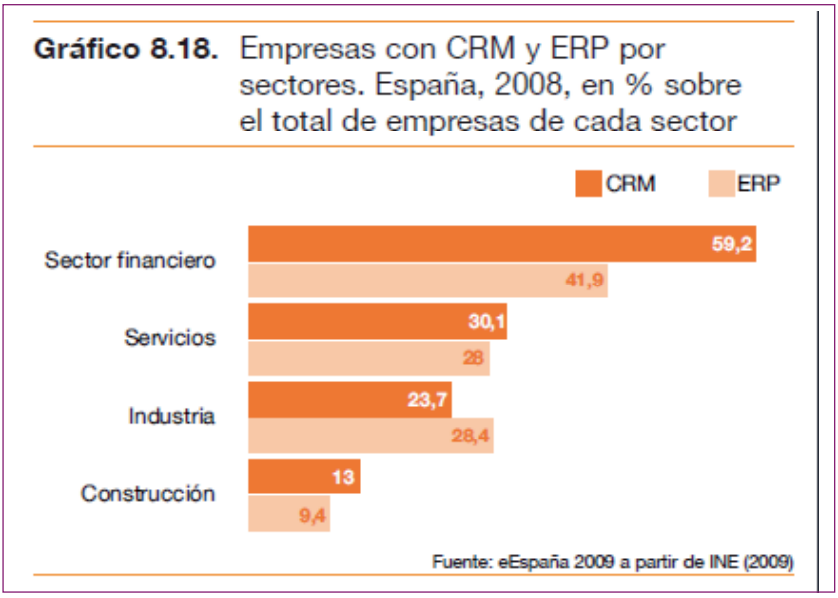


Figura 7.3

Aunque no existe una estadística fiable sobre la utilización y distribución por fabricante de software o tipo de ERP utilizada por las distintas administraciones en España, es una evidencia claramente perceptible que las principales administraciones públicas utilizan complejas aplicaciones informáticas para desarrollar las misiones encomendadas legalmente, en todos los estratos de las Administraciones públicas (central, autonómica y local) y entidades satélites (fundaciones, empresas, agencias, consorcios, etc).

7.1.5. Esquema de un sistema de información complejo

En el capítulo 3.1.2 vimos que, esquemáticamente, en un modelo simplificado, el sistema de información de una entidad consta de varios niveles superpuestos.

La *Global Technology Audit Guide n.º 5: Developing the IT Audit Plan*, publicada por *The Institute of Internal Audit*, también representa los sistemas de información mediante un esquema similar al representado en la figura 3.1:

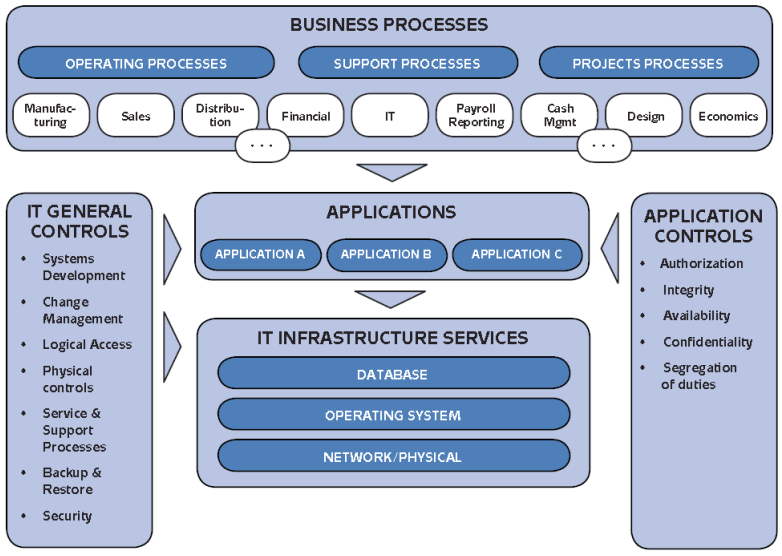


Figure 3. Understanding the IT environment in a business context

Figura 7.4

Aun manteniendo este esquema general, en la realidad las interacciones son más complejas, y los sistemas y aplicaciones comerciales que un auditor va a tener que revisar, pueden presentarse desplegados con muy distintas configuraciones, teniendo cada producto y versión de software sus propias características diferenciadoras que el auditor de sistemas debe conocer con una cierta profundidad y el auditor financiero al menos en sus aspectos principales.

A efectos del análisis posterior de los productos concretos que pueden encontrarse con mayor frecuencia en instalaciones del sector público, dividimos un sistema integrado en las siguientes capas o niveles básicos:

- Sistema operativo.
- Base de datos.
- Middleware.
- Aplicaciones.

En los siguientes capítulos se va a hacer un análisis de estos niveles desde el punto de vista del auditor.

7.1.6. Consideraciones iniciales de auditoría

La existencia de un ERP en una entidad, ya esté plenamente operativo o en proceso de implantación, requerirá del auditor que realice

determinados procedimientos específicos, ya que dada su complejidad comprender su funcionamiento requiere un esfuerzo adicional.

En una primera aproximación un ERP parece un sistema cerrado, que hace complicada la revisión de los controles internos. El conocimiento del sistema por los empleados de la entidad es a veces limitado por distintas razones, principalmente por una insuficiente formación. También es frecuente que los usuarios no comprendan todas las consecuencias y las múltiples incidencias a que pueden dar lugar sus acciones sobre el sistema y sobre los datos contables.

Hay tres grandes grupos de sistemas integrados, que se describen en el capítulo 7.5.1, y lo primero es saber a qué tipo pertenece el de la entidad que se va a auditar.

Luego hay que obtener información general sobre las características del ERP utilizado en particular (marca y versión) por la entidad.

La primera vez que se audita una entidad con un ERP o cuando una entidad ya auditada va a implantar uno, es conveniente conocer qué estrategia de implantación se ha adoptado:

- Revisión completa de sus procesos de negocio para adaptarse a la estructura y funcionalidades del ERP (sin duda la mejor estrategia para productos poco flexibles como SAP).
- Adaptación del ERP a las peculiaridades de la organización de la entidad (en determinados ERP muy estandarizados, cuanto mayores sean las adaptaciones y cambios del software, mayores serán los riesgos inherentes derivados del sistema informático).

La fase de implantación de un ERP condiciona la posterior fortaleza o debilidad del sistema de control de una entidad y ha dado lugar a abundante literatura al respecto. Aunque es un tema que excede los objetivos de este trabajo, solo citaré un artículo[73] publicado en la revista Information Systems Control Journal, en el que se señalaba, entre otras cosas, que «un problema común que se encuentra durante la implantación de un sistema ERP es la eliminación de controles tradicionales sin su reemplazo por nuevas medidas de control efectivas… Algunos sistemas como SAP permiten introducir controles que crean pistas de auditoría y permiten seguir y verificar todas las entradas de datos… No obstante, todos los maravillosos mecanismos de control disponibles en SAP R/3 son efectivos solo si se instalan correctamente.»

Por otra parte, ya se ha señalado que cada configuración posible de un sistema informático, presenta características propias que condicionan

73. *Implementation of ERP Systems: accounting and auditing implications*, de Benjamin Bae y Paul Ashcroft, Information Systems Control Journal, volumen 5, 2004

el trabajo de auditoría, exigiendo la adaptación de los procedimientos que deben aplicarse. Por esta razón en los próximos apartados de este capítulo 7 se va a dar repaso general a los distintos componentes de dichos sistemas y a las principales consideraciones de auditoría.

7.2. Sistemas operativos

7.2.1. Concepto

Un sistema operativo (SO) es software que controla la ejecución de otros programas de ordenador, programa tareas, distribuye el almacenamiento, gestiona las interfaces con hardware periférico y muestra la interfaz por defecto con el usuario cuando no hay funcionando ningún otro programa.

Es muy importante realizar determinados procedimientos de auditoría sobre los sistemas operativos y los controles existentes a este nivel, ya que vulnerabilidades en los SO tienen un impacto potencial en todo el sistema de información (aunque las aplicaciones y las bases de datos tengan buenos controles, si un intruso pudiera penetrar sin restricciones en el sistema operativo y su sistema de carpetas, podría provocar graves daños en los datos y sistemas de la entidad).

7.2.2. Situación global del mercado

Según el informe *Server workloads forecast and analisis study, 2005-2010* publicado por IDC, el mercado de sistemas operativos para servidores de bases de datos y de aplicaciones de negocio (concepto que incluye ERP, PLM, HRM, CRM, etc) tuvo en 2005 la siguiente distribución:

TABLE 10

Worldwide Database and Application Server Revenue by Operating System, 2005

	Revenue ($M)			Share (%)		
	Database	Application	Total	Database	Application	Total
Windows	3,881	15,317	19,197	22.7	40.6	35.0
NetWare	119	948	1,067	0.7	2.5	1.9
Linux	1,064	4,986	6,050	6.2	13.2	11.0
Unix	7,739	11,084	18,823	45.3	29.3	34.3
i5/OS	883	1,211	2,095	5.2	3.2	3.8
z/OS	2,343	2,526	4,868	13.7	6.7	8.9
Other	1,053	1,698	2,751	6.2	4.5	5.0
Total	17,082	37,770	54,852	100.0	100.0	100.0

Source: IDC, 2006

Figura 7.5

En la siguiente figura se ven gráficamente los anteriores datos.

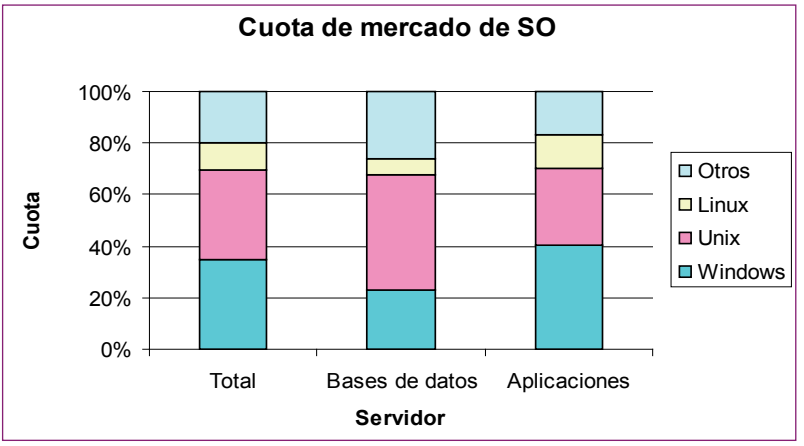


Figura 7.6

Puede observarse que predominan las instalaciones basadas en Unix/Linux con un 45,3%, seguidas de Windows con un 35%.

7.2.3. Situación del mercado en España

De acuerdo con los datos ofrecidos por el *Informe IRIA 2008*, los sistemas operativos instalados en sistemas grandes[74] en la Administración del Estado, en 2007 tenían la siguiente distribución:

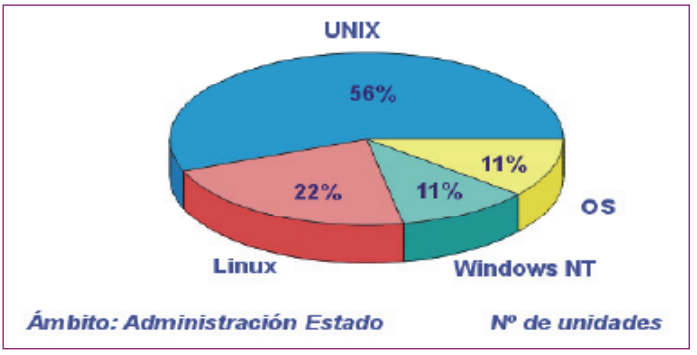


Figura 7.7

74. Según el Informe IRIA 2008:

Sistemas Grandes: También conocidos como mainframes, cuya unidad central tiene un precio igual o superior a 601.012 euros, sin incluir unidades de almacenamiento asociadas. Se incluyen en esta categoría los equipos multiprocesador.

Sistemas Medios: Equipos informáticos con unidad central, mono o multiprocesador, de precio que oscila entre 60.101 y 601.012 euros. Como en los sistemas grandes, no se incluyen las unidades de almacenamiento.

Sistemas Pequeños: Con un precio entre 6.010 y 60.101 euros, en esta categoría se incluyen unidades multiprocesador y las unidades de almacenamiento se consideran parte del sistema (quedan excluidos los ordenadores personales).

La distribución de los sistemas operativos instalados en sistemas medios en la Administración del Estado, en 2007:

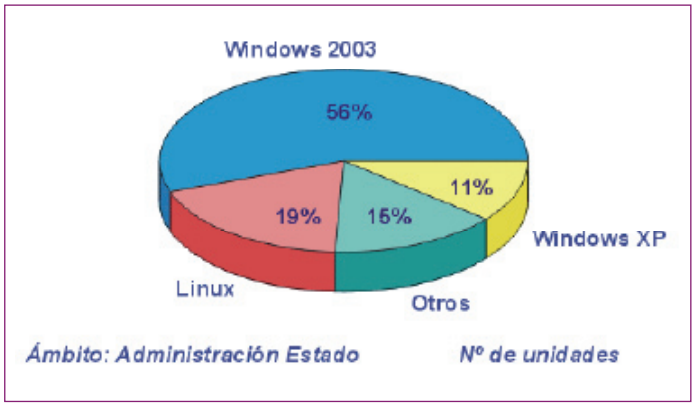


Figura 7.8

La Figura 7.9 muestra la distribución de los sistemas operativos instalados en sistemas pequeños en la Administración del Estado, en 2007, era la siguiente:

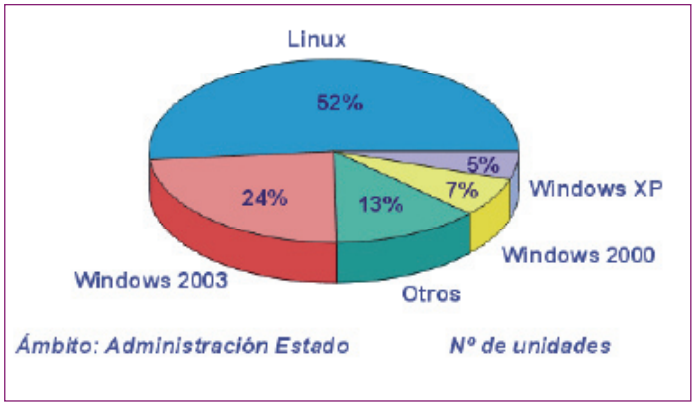


Figura 7.9

7.2.4. UNIX-Linux

a) Conceptos básicos

UNIX es un sistema operativo portable, multitarea y multiusuario desarrollado en 1969 por un grupo de empleados de los Laboratorios Bell de AT&T. El sistema UNIX fue comercializado e implantado en empresas y administraciones públicas, sobre todo a partir de 1980.

La evolución del sistema a lo largo de su historia ha dado lugar a numerosas variantes. En la actualidad la empresa propietaria de

la marca es The Open Group, que certifica que los productos de otras empresas, cumplen con los estándares UNIX que aquella ha establecido.

Existen numerosas variantes registradas de UNIX, algunas de las más conocidas son:

- Sun Microsystems, Inc.: Solaris 10
- IBM Corporation: AIX 6
- Hewlett-Packard Company: HP-UX 11i
- Apple Inc.: Mac OS X Version 10.5 Leopard

En 1994 Linus Torvalds, un estudiante de la Universidad de Helsinki, diseñó y distribuyó un sistema operativo, similar a UNIX y de libre distribución, que se denominó Linux. También existen muchas variantes de Linux pero las características básicas desde el punto de vista de la auditoría de sistemas son las mismas. Entre las más conocidas se encuentran:

- Red Hat
- Debian
- Suse
- Gentoo
- Ubuntu
- Oracle Enterprise Linux (es la distribución Oracle de Linux; es 100% compatible con la variante Red Hat Enterprise Linux)

b) Consideraciones de auditoría

Linux es un sistema operativo similar a UNIX, por lo que el enfoque de la auditoría de sistemas es el mismo que para los sistemas UNIX y requiere tener en cuenta, entre otras, las consideraciones que se hacen en este capítulo.

La seguridad no fue una de las principales preocupaciones en los primeros diseños del sistema UNIX. Aunque algunas distribuciones del sistema UNIX son seguras después de una correcta instalación, se deberá prestar especial atención a las especificaciones de seguridad del sistema sujeto a revisión, verificando que está configurado con parámetros que sean seguros.

La información a obtener debe ser facilitada por los responsables del departamento de sistemas. En general, el auditor no ejecutará directamente los comandos a que hacemos referencia en este capítulo.

El acceso al sistema UNIX se consigue introduciendo una cuenta de usuario y el sistema la reconoce como un número. Para UNIX todos los usuarios que tienen asignado el condigo 0 se comportarán como el usuario *root*, que es el superusuario de UNIX que tiene las más amplias capacidades de gestión del sistema.

El sistema UNIX configura una estructura jerárquica de directorios y carpetas. Cada carpeta y archivo tiene definidos permisos para el propietario, grupo y otros.

A su vez, existen tres tipos diferentes de accesos a estos elementos: lectura, escritura y ejecución.

Si solicitamos la información de permisos y vemos que una carpeta o fichero está configurada con los siguientes parámetros:

rwxrwxrwx

indica que la autorización para el *propietario* (posiciones 1 a 3) es de lectura, escritura y ejecución (las 3 primeras posiciones son: r read, w write, x execute; en binario situando un 1 dónde hay una letra y un 0 si no la hay, sería 111; en decimal esto sería 7).

Lo mismo para el *grupo* (posiciones 4 a 6) y lo mismo para el resto de usuarios u *otros* (posiciones 7 a 9).

Los expertos dirían que esta carpeta tiene una configuración 777 que significa la menor restricción posible y por tanto la mayor vulnerabilidad.

Una configuración 740 sería mucho más restrictiva y segura:

rwxr-----

Las siguientes carpetas de sistema contienen información relevante sobre usuarios, grupos de usuarios y contraseñas:

/etc/passwd	Contiene información sobre los usuarios del sistema.
/etc/shadow	Contiene información sobre contraseñas.
/etc/group	Contiene información sobre grupos de usuarios.

Se deberá tener en cuenta, siempre, si existen mecanismos de gestión centralizada de usuarios (NIS, NIS+, LDAP).

NIS (Network Information System) permite a los equipos de una red compartir información de configuración, incluyendo las palabras clave. NIS no está diseñado como mecanismo de seguridad. Para visualizar los archivos de password se usa el comando *ypcat passwd*.

NIS y NIS+ han sido reemplazados por LDAP (Lightweight Directory Access Protocol)

LDAP (*Lightweight Directory Access Protocol*) es un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red.

Un directorio es un conjunto de objetos con atributos organizados en una manera lógica y jerárquica. Un árbol de directorio LDAP a veces refleja varios límites políticos, geográficos y/o organizacionales, dependiendo del modelo elegido. Los despliegues actuales de LDAP tienden a usar nombres de Sistema de Nombres de Dominio (DNS por sus siglas en inglés) para estructurar los niveles más altos de la jerarquía. Conforme se desciende en el directorio pueden aparecer entradas que representan personas, unidades organizacionales, impresoras, documentos, grupos de personas o cualquier cosa que representa una entrada dada en el árbol (o múltiples entradas).

LDAP habitualmente, almacena la información de autenticación (usuario y contraseña) y es utilizado para autenticarse aunque es posible almacenar otra información (datos de contacto del usuario, ubicación de diversos recursos de la red, permisos, certificados, etc). A manera de síntesis, LDAP es un protocolo de acceso unificado a un conjunto de información sobre una red.

c) Procedimientos de auditoría

Se deberá prestar atención especial, diseñar y ejecutar procedimientos de auditoría que cubran las siguientes áreas:

1. Gestión de usuarios y contraseñas

- Revisar los procedimientos establecidos para gestionar las altas y bajas de usuarios.
- Asegurar que los identificadores de usuario son únicos. En caso contrario los usuarios podrían acceder a las información de aquellos con la misma denominación de usuario (también que no hay dos usuarios con el mismo código numérico de usuario).
- Asegurarse que las contraseñas están encriptadas.
- Revisar los permisos de las carpetas *passwd* y *shadow*.

  El acceso a estas carpetas da capacidad para la gestión de contraseñas. El archivo *passwd* debería ser accesible con capacidad de escritura sólo por el *usuario root* y el archivo *shadow* sólo debería ser accesible con capacidad de lectura por *root*.

Al ejecutar la siguiente instrucción: *ls -l /etc/passwd* el resultado esperado sería *r--r--r-- 1 root sys*

Al ejecutar la siguiente instrucción: *ls -l /etc/shadow* el resultado esperado sería *r-------- 1 root sys*

- Evaluar la fortaleza de la composición de las contraseñas
- Evaluar el uso de los grupos de usuarios para ver si se gestiona restrictivamente.
- Verificar si se comparten cuentas de usuarios
- Evaluar la necesidad de que existen todos los usuarios con capacidad de superusuario (cuando haya varios).
- Revisar las seguridad de las rutas de acceso por defecto y de las rutas de acceso root.
- Revisar la seguridad de las carpetas home de usuario y de las carpetas de configuración.

2. Seguridad de las carpetas y ficheros

- Revisar la seguridad de las carpetas con información crítica:

  /bin, /usr/bin, /sbin, /usr/sbin, /usr/local/bin (programas para la interpretación de comandos).

  /etc (ficheros con información sobre usuarios, gurpos, contraseñas, …).

  /usr o /var (logs)

  Kernel (centro del sistema operativo).

  La información clave del servidor sobre el que se está haciendo la revisión del sistema operativo

Los comandos *ls –ld* y *ls –l* nos darán la información sobre directorios y ficheros.

- Verificar la existencia de directorios abiertos «777». Analizar los riesgos en función del tipo de directorio. Utilizar el comando *find / -type d –perm -777*.
- Evaluar la seguridad de los ficheros SUID, que permiten ser ejecutados por usuarios distintos a su propietario. Ejecutar *find/ -perm u+s.*

  (*Setuid*, también llamado a veces «*suid*», y «*setgid*» son permisos de acceso que pueden asignarse a archivos o directorios. Se utilizan principalmente para permitir a los usuarios ejecutar binarios con privilegios elevados temporalmente para realizar una tarea específica).
- Revisar la configuración de permisos por defecto.

– Revisar las carpetas que tienen programadas tareas (*crontab*).

3. Seguridad de la red

– Evaluar la necesidad y seguridad de los servicios que se encuentran activados en el sistema operativo. Usar el comando «*nestat –an*» para verificar los servicios activos.

  Si un servicio no es necesario debe deshabilitarse. Existen servicios que si no están adecuadamente controlados suponen vulnerabilidad para el sistema: FTP, TFTP, Telnet, rlogin, NIS, NFS, …

  Ejecutar una herramienta de detección de vulnerabilidades.

– Evaluar la seguridad y necesidad de accesos remotos configurados como accesos de confianza (ver ficheros */etc/hosts.equiv* y *.rhost*). Comprobar que existen procedimientos de autorización y control.

– Verificar si se usan ficheros *.netrc* para configurar accesos automatizados y su razonabilidad y seguridad.

– Verificar si se usan modems para acceso remoto al servidor (son más seguros sistemas como VPN o RAS).

4. Auditoría (logs)

– Evaluar el contenido, seguridad, seguimiento, y periodo de retención del sistema de almacenamiento de datos de acesos (logs).

  Revisar las carpetas: *sulog, sudolog, syslog, loguinglog, wtmp, utmp*.

5. Seguimiento de la seguridad y controles generales

– Revisar los procedimientos establecidos para el control de la situación de seguridad del sistema.

– Revisar los procedimientos para las configuraciones iniciales de los sistemas verificando las configuraciones de seguridad.

– Verificar que existen controles físicos y de ejecución de operaciones que aseguren la protección y disponibilidad del sistema: seguridad física, control de temperatura y humedad, planificación de la capacidad del sistema, procedimientos de gestión de cambios, seguimiento del desempeño del sistema, procedimientos de recuperación y copias de seguridad.

Existen numerosas aplicaciones libres, disponibles en internet que, usadas con las debidas precauciones por los auditores, pueden ayudar a detectar vulnerabilidades de los sistemas UNIX, ente otras: COPS, para identificar debilidades y hallar soluciones, Crack, para adivinar contraseñas, Npaswd, para configurar normas en el establecimiento de contraseñas, Satan, para localizar vulnerabilidades, Tripwire, para verificar la integridad de ficheros, etc.

7.2.5. Windows Server

a) Conceptos básicos

Windows Server 2003 se introdujo en el mercado en abril de 2003, como evolución del sistema operativo Windows 2000 Server e introdujo mejoras significativas desde el punto de vista de la seguridad y de las posibilidades de gestión del sistema.

Windows 2000 Server fue a su vez fue una evolución del Windows NT (New Technology) introducido en el mercado por Microsoft en 1993. Windows NT ya supuso una mejora sustantiva en cuanto a seguridad, al estar basado en el sistemas de ficheros NTFS (NT File Sistem) frente al sistema FAT (File Alocation Table) que utilizaban los sistemas operativos basados en DOS.

En 2008 Microsoft ha lanzado al mercado una nueva versión de su sistema operativo, Windows Server 2008, que está basado en el esquema del Windows Vista y aporta nuevas funcionalidades. Dado que esta versión no se encuentra todavía muy extendida, las referencias y las cuestiones de auditoría las realizamos sobre el más extendido Windows server 2003.

Algunas de sus funciones son:

- Servidor de archivos e impresión.
- Servidor Web y aplicaciones Web.
- Servidor de correo.
- Terminal Server.
- Servidor de acceso remoto/red privada virtual (VPN).
- Servicio de directorio, Sistema de dominio (DNS), y servidor DHCP.
- Servidor de transmisión de multimedia en tiempo real (Streaming).
- Servidor de infraestructura para aplicaciones de negocios en línea (tales como planificación de recursos de una empresa y software de administración de relaciones con el cliente).

b) Cuestiones y procedimientos de auditoría

De forma abreviada, los aspectos básicos de auditoría sobre el sistema operativo Windows Server 2003 son los siguientes:

1. **Obtención de la información:**

   Para llevar a cabo la auditoría necesitaremos obtener la información básica sobre el sistema utilizando dos procedimientos:

   1.a Solicitud al responsable del departamento de sistemas de la información sobre configuración de seguridad del dominio (obtendremos evidencia copiando en un documento las impresiones de pantalla de la configuración de seguridad del sistema operativo: Directiva de contraseñas, Directiva de bloqueo de cuentas, configuración protector de pantalla, …).

   1.b Solicitud al responsable del departamento sistemas para que ejecute la aplicación de libre distribución Dumpsec que contiene comandos para la extracción de toda la información que vamos a necesitar sobre los usuarios del dominio, contraseñas y accesos.

2. **Revisión de la configuración de auditoría del sistema**

– Verificar que la auditoría del sistema esta habilitada.
– Verificar que los logs de auditoría se almacenan en carpetas protegidas.
– Verificar que la auditoría para intentos de acceso está habilitada.

3. **Verificación de la configuración de los accesos al sistema y su gestión**

– Los derechos de acceso al directorio activo deben estar restringidos al personal autorizado. Los derechos de acceso deben ser concedidos por pertenencia a un grupo antes que individualizadamente.
– Los directorios más críticos del directorio activo deben estar protegidos:

%systemroot%\sysvol
%systemroot%\security
%systemroot%\ntds
%systemroot%\ntfrs

– Revisión de las capacidades de compartir (concede capacidades de acceso remoto a la red): comando «net Share».

Solo deben existir para el controlador de dominio. Obtener justificación de la existencia de esta funcionalidad de todas las que no correspondan al controlador del dominio y evaluar su necesidad.

4. Controles de red

– Solo deben permitirse relaciones de confianza de una sola dirección y creadas automáticamente de acuerdo con las necesidades del negocio. No se deber permitir terceros de confianza. Verificar en el directorio activo del dominio la pestaña «Confianza» y verificar la necesidad y conveniencia de todas las existentes.

– Verificar que no está activo el servicio telnet por los riesgos sobre accesos indebidos que conlleva. Comando Open regedit.

– Verificar que el servicio SNMP está deshabilitado para gestión remota del servidor. Si no lo está porque es necesario verificar que está configurado de forma que no esta disponible para usuarios no autorizados. Comprobar en el directorio de políticas de grupo en el directorio activo, pestañas de configuración, carpetas administrativas, red y SNMP. Verificar si está habilitado.

5. Configuración del sistema

– La posibilidad de ignorar las políticas de contraseñas no debe estar habilitada. Abrir el directorio activo, usuarios y ordenadores. Seleccionar la carpeta de usuarios y hacer doble click en cada usuario para verificar.

– Debe estar configurada la opción para los nuevos usuarios de cambiar la contraseña en el primer acceso. La contraseña inicial no debe ser fácil de adivinar. Verificar con el administrador del sistema.

– Verificar que el sistema operativo tiene instalados los últimos parches.

6. Gestión de usuarios

– Verificar que las cuentas por defecto de administrador, soporte e invitado están configuradas de modo seguro. Verificar que han sido renombradas. Si es posible, utilizar un programa para descifrar contraseñas para verificar su robustez.

– Los derechos de acceso a los objetos del directorio activo deben estar restringidos. Ir al directorio activo y seleccionar los objetos, presionar botón derecho y seleccionar propiedades, pestaña seguridad.

- Verificar que los usuarios pertenecientes al grupo de administradores lo necesitan para sus tareas. En el directorio activo, ir a la carpeta de grupo de administradores. Revisar las funciones de los usuarios del grupo. Ídem para grupo de administradores del dominio. Ídem para administradores de la empresa.
- Debe regir el principio de las mínimas autorizaciones para realizar las tareas encomendadas.
- Las cuentas de administración no deben tener el acceso a administrar desde la red y sólo deben administrar desde la consola del servidor. El abrir el editor de políticas de grupo e ir a la carpeta de «asignación de derechos de usuario» en la carpeta de «configuración». Ver si esta marcado el tilde de limitación de acceso.
- La gestión de usuarios debe realizarse sólo desde el controlador del dominio, no en los pc o servidores. Fuera del dominio solo deben existir las cuentas internas de administración de los equipos y las de invitado. Verificar en la carpeta de usuarios de una muestra de los equipos.
- Debe estar habilitado el bloqueo de cuenta para un número de intentos de acceso fallidos. Verificar en la directiva de bloqueo de cuentas.
- Verificación de la existencia de usuarios inactivos.

7. Gestión de contraseñas

- Verificar en la directiva de contraseñas que la configuración de contraseñas a utilizar por el usuario está debe ajustarse a las buenas prácticas: No repetición contraseñas, vigencia máxima de contraseñas de utilización de contraseña (al menos 90 días), longitud mínima contraseñas (al menos 6 caracteres), complejidad de la contraseña (letras, mayúsculas y minúsculas, números,…).
- Verificar que la contraseña del usuario administrador se cambia de acuerdo con las políticas aprobadas.
- Verificar que las fechas de cambio de contraseñas reales se corresponden con las políticas aprobadas.

7.3. Sistemas de Gestión de Bases de Datos (SGBD)

7.3.1. Conceptos básicos

El SGBD es uno de los niveles básicos en los modernos sistemas de información (ver esquema en la figura 7.4). Dada su importancia

dentro de esos sistemas y la repercusión que tiene sobre la evaluación del riesgo y en el diseño de los procedimientos de auditoría vamos a estudiar con detalle esta materia.

Al ser el principal repositorio de los datos más valiosos de la entidad, las bases de datos son probablemente el área más sensible del universo TI, siendo vulnerables a ataques externos vía aplicaciones web e internos de empleados que se aprovechen indebidamente de privilegios de acceso excesivos.

En un sistema de información medianamente complejo, la estructura del sistema está diseñada de forma que la misma base de datos puede dar soporte a varias aplicaciones. Así, el concepto de datos compartidos por muchos usuarios y distintas aplicaciones es esencial para comprender un Sistema de Gestión de Base de Datos.

En estos sistemas, los programas de aplicación no acceden a los datos o realizan directamente funciones de gestión de los mismos; en lugar de ello, el SGBD actúa como una interfaz para todos los programas que acceden los datos.

Un SGBD permite:

a) La independencia de los datos

   Los datos de la entidad están integrados y disponibles para todas las aplicaciones que utilizan la base de datos.

   Esto altera la relación tradicional existente entre los programas y los datos, en sistemas no integrados, en los que se crean ficheros de datos concretos para cada programa.

b) Compartir los datos

   Las bases de datos de la organización ya no son propiedad de una aplicación en concreto.

   Pueden ser utilizados por muchas aplicaciones y los usuarios y proveedores de datos pueden ser distintos. Por ejemplo, determinados usuarios sólo podrán recuperar datos, en tanto que otros pueden estar autorizados para añadir, eliminar o modificarlos. Finalmente, ciertos usuarios pueden no tener permisos de acceso a los datos por no ser necesario para su trabajo.

c) La manipulación de datos

   Los requerimientos de procesamiento (lectura, actualización, inserción, eliminación) de los programas se realizan por medio de rutinas de manipulación de datos que son parte del SGBD.

Establecer quién puede acceder a los datos y quién puede llevar a cabo funciones de manipulación (añadir, cambiar y eliminar) es una importante consideración de auditoría.

La relación entre funciones, transacciones, programas y datos puede no quedar establecida con tanta facilidad como en el caso de los sistemas de ficheros tradicionales.

Procesamiento por lotes frente a procesamiento en línea

El procesamiento por lotes es el procesamiento de transacciones a intervalos fijos o después de haberse acumulado cierto número de transacciones.

Muchos entornos tienen a la vez aplicaciones por lotes y en línea. Estas últimas consisten con frecuencia en consultas a las bases de datos o en la captura en línea de datos. La actualización o el mantenimiento se plantean a menudo como una aplicación por lotes, con frecuencia después de haber incluido y acumulado transacciones vía entrada de datos en línea, dado que es más fácil controlar el procesamiento por lotes.

Como una de las razones de la existencia de un SGBD es disponer de datos puntuales y actuales, la actualización en línea, en tiempo real, se utiliza en los sistemas que lo necesitan, tales cómo los sistemas de reserva de líneas aéreas o de aprobación de créditos.

La introducción del procesamiento de transacciones en línea significa que la seguridad deberá incluir controles adecuados para el acceso a la red de teleproceso en línea. En un SGBD, el acceso se encuentra frecuentemente controlado por medio de contraseñas de usuarios, códigos o contraseñas de transacción y comandos de terminal gestionados por un administrador de seguridad de datos.

7.3.2. Controles sobre la base de datos y procedimientos de auditoría

a) Controles de acceso

Dado que los SGBD proporcionan un almacenamiento de datos integrado, se hace necesario establecer controles en torno a quién puede acceder a qué elementos de los datos.

Por ejemplo, un sistema de cuentas a cobrar puede compartir una base de datos de clientes con un sistema de servicio al cliente. Las cuentas de los clientes se actualizan con las facturas y pagos introducidos por el departamento de cuentas a cobrar y con las transacciones que resultan de la anotación, por parte del departamento de servicio al cliente, de mercancías devueltas y abonos.

El control del acceso en este ejemplo significa que sólo esos dos departamentos pueden modificar los saldos de los clientes. El departamento de ventas también tiene acceso a la base de datos, pero si bien puede incluir pedidos de venta, no podrá introducir pagos o facturas. La preocupación de la auditoría está en que se hayan implantado unos controles adecuados para garantizar que el departamento de ventas no dispone de acceso a la información que refleja las cuentas a cobrar o que tiene capacidad para incluir transacciones no autorizadas.

La eficacia de los controles del acceso viene determinada por el modo en que se implanta el ambiente de control y por las normas que se aplican para mantener los controles establecidos.

El impacto del SGBD en los controles generales varía dependiendo de las funciones de la base de datos, de la complejidad y alcance del uso de la misma, de la utilización de las telecomunicaciones y de la medida en que los procedimientos de la aplicación garantizan la fiabilidad de los datos.

Será necesario aplicar controles de validación sobre los datos de entrada. Como un mismo dato será utilizado por diversos programas, un error aislado puede tener consecuencias múltiples. Esto es lo que comúnmente se denomina «error acumulado» o «en cascada».

El análisis de la auditoría sobre los controles de acceso a los datos incluidos en un sistema de base de datos puede dividirse como sigue:

1. Control del acceso

Puede proporcionarse seguridad para los entornos de base de datos en línea en tres niveles fundamentales:

– Inicio de una sesión identificándose

Identificación y autentificación de los usuarios durante el inicio de una sesión.

– Protección de las transacciones

La utilización de la seguridad nativa de las bases de datos y/o de seguridad externa para limitar las transacciones con arreglo a la función asignada.

– Protección de comandos

Cuando se define que un comando necesita una contraseña, el sistema no debe permitir al usuario ejecutar la operación a menos que la contraseña se introduzca correctamente.

2. Granularidad del acceso[75]

Las personas y programas autorizados sólo deben acceder a las entidades necesarias para realizar su función laboral o procesar las tareas asignadas.

La base de datos está diseñada para ayudar a proporcionar un adecuado control del acceso a las entidades pertinentes tales como elementos de datos, tablas, capacidades, etc.

El diseño de la estructura de la base de datos y de los requerimientos de acceso del usuario a la base de datos son tareas complicadas. Por consiguiente, es probable que el auditor se encuentre con bases de datos que no disponen de los adecuados controles de acceso o que no están adecuadamente configurados.

3. Separación de pruebas y producción

El control del acceso a los datos durante la producción normal es una preocupación importante, pero el control del acceso durante las pruebas de los programas y aplicaciones es igualmente importante.

Las pruebas deben realizarse utilizando una base de datos de prueba para garantizar que no se distorsiona la producción de datos y que los datos confidenciales no corren riesgo de exposición. Por lo tanto, el auditor deberá comprobar si durante el desarrollo de las aplicaciones se utilizan bases de datos de prueba y no se trabaja en un entorno de producción.

b) Otros controles sobre el SGBD

1. Principales procedimientos de control

Para garantizar que los controles sobre el SGBD minimizan los riesgos adicionales inherentes en las bases de datos se pueden introducir los siguientes procedimientos de control interno:

– Definición del «sub-esquema» de cada usuario, que limita la capacidad del mismo para realizar consultas, dar altas, modificaciones o bajas de datos. Los «sub-esquemas» deben ser definidos por el administrador de base de datos. El SGBD tendrá que controlar cada solicitud de datos consultando una tabla de niveles de protección, a fin de garantizar que el usuario, según se identificó con su contraseña, tiene derecho a leer la información y a ejecutar las funciones solicitadas.

75. Granularidad es el nivel de detalle al cual se identifican los componentes de un documento o la estructura de una base de datos. Se refiere a la especificidad a la que se define un nivel de detalle en una tabla.

- Inclusión de un programa de utilidad en el SGBD para controlar la consistencia de los indicadores internos y avisar de cualquier inconsistencia (enlaces rotos).
- Inclusión en el SGBD de un control sobre cada solicitud para dar de baja datos a fin de garantizar que ninguno de los ítems subordinados a ese dato se volverán así inaccesibles.
- Procedimientos de bloqueo que permitan al SGBD evitar o detectar automáticamente la actualización concurrente que puede ocurrir cuando dos usuarios tratan de tener acceso al mismo dato de forma simultánea.
- Registros de archivo de transacciones y de reenganche separados de la base de datos en forma física y lógica.
- Barrido periódico del contenido de la base de datos por medio de un programa que acumule valores de registros individuales para después conciliarlos con un registro de control.

2. Controles compensatorios e importancia de las debilidades

La falta de restricciones a la capacidad de procesamiento de los usuarios y de los programas, deja a la base de datos sin ninguna protección contra modificaciones accidentales o no autorizadas. Resulta improbable que la evidencia de auditoría y los respectivos procedimientos del usuario para la conciliación de la entrada/salida permitan detectar alteraciones accidentales, ya que las mismas pueden no tener un impacto inmediato en los datos de salida.

Igualmente, encontrar el origen de un error en un sistema de base de datos constituye una tarea compleja debido a las interrelaciones lógicas entre los diferentes datos. Frecuentemente, en tales situaciones no existe un control compensatorio adecuado.

La falta de verificación de la consistencia de los indicadores internos podría ser compensada por severos controles del usuario sobre la actualización de la base de datos y la conciliación de los totales de control. Este control no es viable en grandes bases de datos.

3. Procedimientos de auditoría

- En combinación con pruebas del software del SGBD o el diccionario de datos, se debe verificar si los niveles de protección para determinados datos específicos son apropiados.
- Hacer una prueba de los procedimientos de bloqueo, intentando dos actualizaciones simultáneas a través de terminales adyacentes.

– Utilizar herramientas CAAT o las utilidades existentes, para poner a prueba la consistencia de los indicadores internos.

c) La función de administración de la base de datos

Esta función permite garantizar la existencia de controles adecuados sobre el desarrollo y uso de la base de datos y una adecuada coordinación entre los usuarios.

El establecimiento de un SGBD implica que la entidad debe hacer frente a una serie de complejidades técnicas del sistema y se debe controlar y coordinar las actividades y las comunicaciones entre las diversas aplicaciones y departamentos que comparten los recursos de la base de datos.

Una de las características básicas de un sistema de base de datos es que éstos son compartidos por todos los usuarios. De ahí que puedan surgir conflictos entre los diferentes usuarios, que requerirán un arbitraje adecuado. Alguien debe dar una perspectiva global de los objetivos de la base de datos de modo que el usuario más poderoso no pueda ejercer una influencia desmedida.

Esas funciones son normalmente desempeñadas por un administrador de bases de datos (ABD) y un administrador de seguridad de los datos.

El ABD planea y gestiona las necesidades globales de recursos de datos y puede ocuparse de la disciplina y de establecer normas para las bases de datos. Actúa de forma independiente tanto de los usuarios como de los programadores. En un entorno de grandes dimensiones, el ABD puede ser más de una persona.

El administrador de seguridad es habitualmente responsable de determinar y vigilar los controles de acceso a los datos.

El ABD es un factor importante en la revisión y evaluación de los controles por parte del auditor, que obtiene una gran parte del conocimiento acerca de cómo se utiliza la base de datos y de cuáles son los controles que se emplean, hablando con él y revisando sus actividades. La ausencia de una estructura coordinada para desempeñar esas responsabilidades puede constituir en sí misma una debilidad del control.

El ABD dispone de herramientas que le ayudan a cumplir sus responsabilidades; algunas de esas herramientas también pueden ser utilizadas por el auditor. Una de las más importantes y útil es el diccionario de datos, que organiza y mantiene información sobre las relaciones, atributos y definiciones de los elementos de datos exis-

tentes en las bases de datos. Su ausencia también puede constituir una debilidad del control.

En el caso de bases de datos pertenecientes a instalaciones pequeñas, no existirá por lo general una función separada y permanente de ABD. La misma será normalmente parte de las responsabilidades de un analista de sistemas senior.

Procedimientos de control

- Existencia de un ABD cuyas responsabilidades serán:
  - Justificación de costes y planificación.
  - Diseño del «esquema» de la base de datos, incluyendo contenido de los datos, estructura de los datos, y relación entre los datos, así como métodos de almacenamiento y acceso.
  - Procedimientos de desarrollo e implantación del SGBD.
  - Diseño y mantenimiento de un diccionario de datos.
  - Especificación de procedimientos de control y normas de documentación, incluyendo copias de seguridad, vuelco de copias, reinicios y reenganches.
  - Control del procesamiento de la base de datos, y preparación de informes para la dirección del departamento TI.
  - Enlace con los usuarios y los auditores, incluyendo el suministro de información referente a definiciones, modos de acceso y procedimientos de protección.
  - Puesta a punto del funcionamiento de la base de datos.
  - Pruebas de la base de datos para garantizar su integridad.
- Separación de las tareas del ABD, de las siguientes áreas:
  - Control operativo del funcionamiento diario del SGBD.
  - Implantación y ejecución de procedimientos de seguridad.
  - Ejecución de procedimientos de reenganche.
  - Diseño y codificación de programas.
  - Implantación de definiciones de la base de datos.
  - Análisis de sistemas y programación.

Controles compensatorios e importancia de las debilidades

A falta de una función de ABD independiente y eficaz, debemos identificar los controles compensatorios impuestos por los usuarios individualmente y por el departamento TI. Si no existen tales controles, necesitaremos aumentar el alcance de los procedimientos de auditoría.

Procedimientos de auditoría

- A través de la discusión con la dirección TI, evaluar el grado de independencia que la función de administración de la base de datos tiene con respecto a los departamentos usuarios y al desarrollo de las aplicaciones.
- Examinar la evidencia documental del trabajo del ABD, tal como manuales de procedimientos, informes periódicos y anotaciones relacionadas con las reuniones realizadas.

d) ¿Proporciona el sistema de manejo de la base de datos, o el diccionario de datos, un registro de la estructura de la base de datos?

La estructura lógica de una base de datos es definida mediante la utilización de «esquemas» y «subesquemas», que son procesados por el SGBD a fin de permitir que los programas realicen el procesamiento de los datos acumulados en la base de datos.

El «esquema» representa la estructura lógica de toda la base de datos, mientras que cada «subesquema» contiene únicamente los elementos necesarios para el funcionamiento del programa para el cual fue proyectado.

Algunas organizaciones utilizan un sistema de **diccionario de datos** para facilitar la documentación de la estructura de la base de datos. El mismo proporciona una descripción de los datos a los cuales se podrá tener acceso y que podrán ser actualizados, y cuáles son los usuarios autorizados a hacerlo. También muestra la interrelación entre los diferentes datos. Esto puede constituir una importante herramienta de control y auditoría.

La función de administración de la base de datos, los usuarios, y el personal del departamento TI, deben tener una idea exacta de la estructura de la base de datos y de los datos que la misma contiene.

Este conocimiento debería reducir la posibilidad de errores en el análisis de sistemas o en la programación. También evitará una confianza exagerada por parte de los usuarios en los controles incorporados en los programas.

Procedimientos de control

- Documentación clara de la base de datos, incluyendo:
  - Descripciones de cada elemento (definiciones de datos) en lenguaje que pueda ser entendido por los usuarios.
  - Origen y formato de los datos.
  - Programas relacionados con cada dato y tipo de registro.
  - Interrelaciones entre los datos y tipos de registro.
  - Controles de validación para cada tipo de dato de entrada.
  - Usuarios autorizados a tener acceso a los datos o realizar su actualización.
- Archivo cuidadoso de la información para facilitar su consulta, tomándose cuidado de mantener la información antigua de forma separada como referencia histórica.
- Tratamiento confidencial de la información, con el acceso a la misma restringido únicamente a aquellos que realmente la necesitan y están autorizados.
- Asignación a la función de manejo de la base de datos de la responsabilidad de garantizar la exactitud de la información contenida en el diccionario.

Controles compensatorios e importancia de las debilidades

Una información inexacta puede conducir a errores de programación o hacer que el usuario confíe en controles programados inexistentes.

Estas posibles debilidades podrán ser parcialmente compensadas mediante la participación del usuario en los procedimientos de prueba de los sistemas.

Sin embargo, si los programadores no cuentan con una visión exacta de la interrelación entre los diferentes datos, podrán introducir errores de lógica que afectarán otras aplicaciones, además de aquella que están programando. En ese caso, las pruebas por ellos proyectadas pueden no ser capaces de detectar tales errores. El DBA puede ser responsable de esta área. A falta de documentación exacta, se debe procurar depositar una confianza relativamente mayor en los controles del usuario sobre los datos de entrada y salida.

La falta de protección de la información confidencial podrá llegar a permitir el acceso y actualización no autorizada de la base de datos. El acceso no autorizado podrá ser detectado mediante el

examen de los registros de acceso de las terminales, mientras que las actualizaciones no autorizadas podrán ser descubiertas mediante la conciliación por el usuario de los datos de entrada/salida, siempre y cuando exista adecuada evidencia de auditoría.

Procedimientos de auditoría

- Examinar los tipos de información proporcionados por el diccionario, y verificar para ítems específicos si los niveles de protección son adecuados.
- Utilizar CAAT para repetir las pruebas de validación descritas en el diccionario.
- Analizar con los funcionarios responsables de la administración de la base de datos, los procedimientos existentes para dar información a los usuarios y programadores, y los procedimientos para la actualización del «esquema», «subesquemas» y el diccionario de datos.

e) Riesgos de seguridad más frecuentes

En una reciente presentación[76] realizada por una empresa especializada en bases de datos, se exponía de forma resumida bajo el sugestivo título *¿Por qué todavía no son seguras las bases de datos en 2008?* de forma resumida los principales problemas que afectan a la seguridad de las bases de datos y sus posibles soluciones:

Problema	Motivo	Solución
BD antiguas, sin actualizar	Muchas entidades están todavía usando versiones antiguas de BD y por tanto vulnerables	Actualizar a una versión con soporte para cubrir fallos de seguridad
Uso de passwords entregados por defecto o bien débiles	Muchas BD siguen usando los passwords que vienen predefinidos u otros débiles	Implantar unas normas estrictas de uso de passwords
Configuración poco segura, muchos privilegios	Falta de conocimiento y/o aplicaciones de terceros	Formación de los administradores de las BD
Código inseguro	Desarrolladores sin formación específica	Formación de los desarrolladores
Sin herramientas de auditoría interna	Temor al impacto en el rendimiento	Utilización de herramientas especializadas con bajo impacto en el rendimiento

Figura 7.10

76. *Trends in Oracle Security*, Alexander Kornbrust, Red Database Security Gmbh, 29 de mayo de 2008.

7.3.3. Principales SGBD

Según un informe de IDC sobre el año 2007,[77] el mercado mundial de SGBD estaba distribuido de la siguiente forma:

Oracle	44,3%
IBM DB2 e Informix	21,0%
Microsoft SQL Server	18,5%
Otros	16,2%

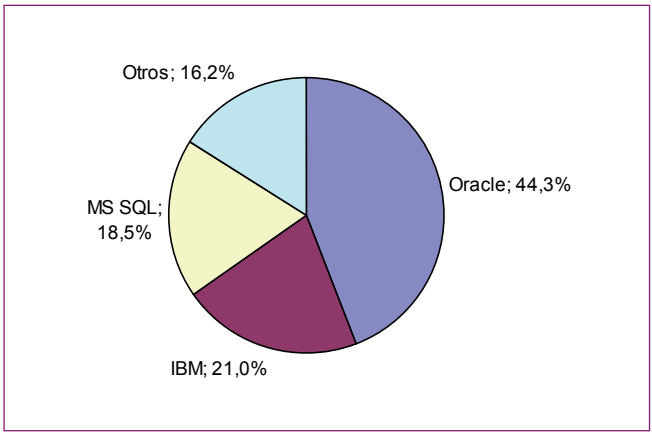


Figura 7.11

Aunque no se dispone de datos fiables, en el sector público español predominan las bases de datos de Oracle y MS SQL.

A nivel mundial la base de datos con mayor cuota de mercado en sistemas ERP es Oracle. Es una base de datos neutra respecto de la plataforma en la que opera. El soporte de Oracle a las principales plataformas Unix, Windows y Linux da a los usuarios la garantía de que pueden cambiar de proveedores de hardware y sistemas operativos sin problemas.

En buena medida la gran penetración de Oracle en el mercado se debe a su relación con SAP, que se remonta al año 1988, cuando SAP R/3 inició su desarrollo. Durante casi 20 años Oracle ha sido la base de datos sobre la que se han desarrollado principalmente las aplicaciones SAP. De hecho Oracle tiene un equipo de desarrollo en la sede central de SAP en Walldorf (Alemania). En noviembre de 1999 se firmó un contrato para garantizar la cooperación entre

77. *World wide Relational Database Management Systems 2007 Vendor Shares*, Carl W. Olofson, IDC, junio 2008.

Oracle y SAP y la situación privilegiada de la base de datos Oracle en los sistemas SAP. El contrato fue renovado en enero de 2008.

No obstante, en los últimos años, a raíz de la entrada de Oracle en el mercado de las aplicaciones de negocio (principalmente tras la compra de JD Edwards, Siebel, PeopleSoft, etc) la perspectiva de SAP respecto de Oracle ha evolucionado desde la consideración como un socio privilegiado a un competidor.

Casi dos tercios de las implementaciones SAP están basadas en BD Oracle,[78] indistintamente con sistemas operativos Unix, Linux y Windows.

7.4. Interfaces y middleware

7.4.1. Interfaces

Los entornos TI complejos generalmente requieren interfaces complejas para integrar sus aplicaciones de negocio críticas. Incluso los entornos ERP muy integrados a menudo requieren complicadas interfaces para otras aplicaciones distribuidas, como los sistemas de internet.

Las interfaces entre aplicaciones y entre bases de datos requieren una atención especial, en particular las relacionadas con aquellas aplicaciones con impacto en las cuentas anuales. Estas interfaces pueden ser gestionadas con tecnología middleware, que actúa como un elemento central de comunicación y coordinación de interfaces.

A pesar de que las interfaces y el middleware juegan un importante papel en el proceso de las transacciones, en muchos casos no se incluyen, erróneamente, en el plan de la auditoría.

Como mínimo mueven información de un sistema a otro, pero también pueden ser responsables de cálculos o de modificar datos de acuerdo con algún algoritmo. Además el riesgo de su mal funcionamiento puede afectar a todo el sistema.

Se deben evaluar los riesgos de interfaz (pérdida de datos por interrupción de las comunicaciones, duplicación de datos en el sistema de destino, actualización del sistema de destino con datos de un período incorrecto, etc) y los controles establecidos para mitigarlos.

78. *Oracle Database: The Database of Choice for Deploying SAP Solutions*, Abdelrani Boukachabine, agosto 2009.

Los controles de interfaz pueden ser manuales (p.e. mediante reconciliaciones manuales) o estar automatizados (los datos de ambos sistemas se concilian automáticamente).

7.4.2. Middleware

Las aplicaciones de negocio actuales tienen los componentes de la interfaz de usuario, el procesamiento de datos y el almacenamiento de datos ubicados en distintos servidores, a menudo usando diferentes sistemas operativos.

Hacer trabajar todos los componentes juntos se consigue normalmente mediante el uso de software especializado en transporte de datos y comunicaciones comúnmente conocido como middleware. También se usa para conectar diferentes aplicaciones en distintas arquitecturas.

El middleware proporciona unas comunicaciones robustas y potencialmente seguras entre aplicaciones a través de capas de funciones en distintos servidores y tecnologías de red.

Ejemplo de middleware son los productos Oracle Fusión, SAP NetWeaver y WebSphere de IBM.[79]

7.4.3. Consideraciones de auditoría

Cualesquiera que sean las ventajas de un ERP y la voluntad de la entidad de implantar un sistema integrado, el sistema de información está a menudo constituido de varias aplicaciones heterogéneas. Los procedimientos de auditoría se harán sobre cada una de las aplicaciones pero también sobre las interfaces que posibilitan la transferencia de datos.

79. En Forrester.com, se publicó en agosto de 2009 un informe elaborado por Jeffrey S. Hammond y John R. Rymerm, titulado *With «11g,» Oracle Steps Out Of IBM's Middleware Shadow. New Release Will Also Blast Past SAP NetWeaver And Challenge Microsoft,* que ilustra sobre la orientación del middleware y los principales competidores en ese mercado; en su reseña señala:

«The latest release of Oracle Fusion Middleware 11g, establishes Oracle as the innovator among Java platform vendors. The first modules of Oracle Fusion Middleware 11g — the core Java application server, development tools, service-oriented architecture (SOA), and portal platforms — exhibit a high degree of integration and the first comprehensive declarative development environment for Java from a major vendor. IBM and SAP, the other big Java vendors, are behind Oracle in providing this level of platform integration and Java-development innovation. Application development and enterprise architecture professionals with significant commitments to enterprise Java should now reevaluate their strategic vendors and decide whether or not to follow Oracle's new path with Java platforms. In considering this path, they should be wary of the high potential cost of Oracle Fusion Middleware 11g as well as the high potential for customer lock-in with Oracle's approach.»

Las interfaces deben ser descritas teniendo cuidado de identificar los aspectos señalados en el apartado 5.3.3 h) de este trabajo.

Las intervenciones del usuario pueden ser muy variadas:

- integración o exportación de un fichero con descripción del formato de entrada o salida (estos casos más que interfaces, son ficheros de intercambio).
- Desencadenamiento manual de un proceso automático
- Simple verificación del tratamiento de las excepciones o de los rechazos de la interfaz

Se debe indagar si existe un módulo específico para la gestión de interfaces. Generalmente existen para las interfaces salientes vía las funcionalidades de exportación de datos. Respecto de la importación de datos, conviene averiguar las funcionalidades que permiten a los usuarios seguir el buen funcionamiento de las interfaces, por ejemplo: el seguimiento de los procesos (situación, cumplimiento de la frecuencia prevista,…), identificación de los posibles rechazos, la posibilidad de conocer la causa de los rechazos y de volver a tratar los datos afectados.

Es necesario identificar el tipo de interfaz que tiene el ERP, en particular para las interfaces entrantes.

Se pueden clasificar las interfaces según cuatro categorías principales:

- Interfaces utilizando un lenguaje o un modulo específicamente propuesto por el fabricante del ERP. Este módulo utiliza generalmente las funciones del ERP; los datos integrados por la interfaz se someten a los mismos controles que los datos registrados manualmente por el usuario.
- Las interfaces que utilizan el lenguaje o un módulo proporcionado por el SGBD. En estos casos, si los datos se someten a los controles propios del SGBD (control de coherencia de datos) no serán sometidos a los controles funcionales de las aplicaciones. Estos controles más ricos pueden afectar por ejemplo a las verificaciones de cálculos (tipo de retención IRPF, tipo de IVA, etc).
- Interfaces que utilizan un lenguaje normalizado como en el caso de los intercambios EDI. Se puede usar este tipo de intercambio entre dos sistemas internos de la misma empresa.
- Otros interfaces utilizando distintos medios no previstos por el fabricante del ERP (modificación de los programas, escrituras directas en las tablas de la base de datos, …).

La revisión de las interfaces pasa por la comprensión del tipo de interfaz analizada, para identificar los tipos de controles internos a aplicar y para detectar los riesgos asociados. Se considera en general que una interfaz estándar situada al nivel de la aplicación presenta pocos riesgos, puesto que los datos integrados que provengan de una aplicación externa se someten a los mismos controles que los datos capturados directamente por la aplicación.

7.4.4. Procedimientos de auditoría

Si los métodos de revisión varían según el tipo de interfaz, el objetivo es el mismo en todos los casos.

Se trata de comprobar el funcionamiento de los controles implantados por la entidad (verificación del tratamiento de la interfaz según la frecuencia prevista, seguimiento de los controles realizados sobre los datos, de los rechazos y su tratamiento, etc.).

Los controles de interfaz pueden ser manuales (p.e. mediante reconciliaciones manuales) o estar automatizados (los datos de ambos sistemas se concilian automáticamente).

Se deben evaluar los riesgos de interfaz (pérdida de datos por interrupción de las comunicaciones, duplicación de datos en el sistema de destino, actualización del sistema de destino con datos de un período incorrecto, etc) y los controles establecidos para mitigarlos.

La interrogación de ficheros y bases de datos utilizando CAAT es un procedimiento que proporciona confianza sobre la integridad de la información transmitida entre distintos sistemas.

7.5 . Aplicaciones de negocio integradas

7.5.1. Tipos de ERP o de aplicaciones significativas para los propósitos de la auditoría financiera

Se pueden distinguir los siguientes tipos de ERP o aplicaciones de negocio integradas:

- aplicaciones estándar
- aplicaciones estándar muy adaptada
- desarrollos propios

Considerando que sus perfiles de riesgo son muy diferentes, el conocimiento de los tipos y características de las aplicaciones objeto de revisión es una información importante para la planificación y la realización de la auditoría.

a) Aplicaciones estándar

Las aplicaciones estándar maduras presentan generalmente una gran cantidad de controles integrados.

El siguiente cuadro muestra unos ejemplos de controles básicos destinados a asegurar la integridad de las transacciones procesadas:

Una aplicación de contabilidad estándar debería disponer, entre otras, de las funcionalidades siguientes	**Estas funcionalidades ofrecen o requieren los controles siguientes**
Fechado automático de las operaciones y de las transacciones por el sistema.	Protección del acceso a los parámetros de la fecha del sistema.
Identificación de los usuarios con mecanismos de autenticación.	Encriptado de passwords. Control de la sintaxis de passwords. Control de la validez de passwords. Histórico de intentos de conexión no válidos.
Parametrización de las autorizaciones.	Mecanismos de protección de acceso mediante perfiles de grupo o por autorizaciones individuales.
Prohibición de eliminar.	El programa no debe disponer de la posibilidad de eliminar datos.
Trazabilidad de los cambios de parámetros y datos maestros (parámetros de seguridad, plan de cuentas, datos maestros de deudores y acreedores, etc.).	Registro automático de valores antiguos en un fichero histórico (con fecha de validez: válido desde/hasta) fecha de los cambios e identificación del usuario que ha efectuado la modificación. Protección de los accesos a los parámetros y al fichero histórico.

Figura 7.12

Además, también son muy importantes los siguientes controles:

- Validar los datos (p.e. listas de selección, fórmulas de validación, etc.)
- Dirigir el procesamiento (control de trabajos, orden de proceso diaria, mensual, etc.)
- Desarrollo de las transacciones (p.e. gestión de flujo de trabajo, control de límites, firma electrónica, comprobación de la concordancia entre pedido/albarán/factura).
- Gestionar los gastos (disponibilidad de informes, etc).

Al evaluar las aplicaciones estándar conviene responder a las siguientes preguntas:

- ¿Qué tipo de aplicación estándar usa la entidad?
- ¿Está difundida en su sector de actividad?

- ¿Está certificada?
- ¿Se trata de una aplicación nueva o es conocida y está probada?
- ¿Existen fuentes de información sobre la aplicación y sobre las posibles debilidades de seguridad o de proceso conocidas (las aplicaciones estándar contienen a veces errores y el auditor debe disponer de un conocimiento suficiente sobre las fuentes de error conocidas).
- ¿Dispone el auditor de conocimiento y experiencia en esa aplicación?

Las respuestas a estas preguntas sirven para identificar las áreas que requieren una atención o unos conocimientos particulares y proporcionan al auditor una visión general de los riesgos inherentes a la aplicación utilizada.

Si el auditor concluye que la aplicación estándar revisada no presenta debilidades conocidas en las áreas auditadas, puede limitar sus esfuerzos en las etapas siguientes del trabajo de auditoría sobre identificación de riesgos y posterior evaluación de los controles.

Como mínimo el auditor debe asegurarse que:

- Los controles en los que piensa confiar existen y funcionan.
- Sobre los parámetros de la aplicación, que estaban activos durante el periodo auditado.

Dentro de este grupo de aplicaciones estándar se encontrarían, típicamente, y entre estas probablemente las más extendidas en el sector público sean SAP R/3 o SAP ERP 6.0.

b) Aplicaciones estándar muy adaptadas

Son las aplicaciones cuyo objetivo principal es ofrecer disponibilidad de funcionalidades de base y herramientas de creación de procesos y de flujos de trabajo, y cuya parametrización permite la implantación de soluciones específicas que respondan a las necesidades de la empresa o entidad.

El auditor se enfrenta aquí a un gran desafío, en la medida que, incluso si dispone de informaciones sobre la fiabilidad de los componentes de las aplicaciones y sistemas a auditar, no los tiene sobre la interacción de estos componentes con las posibles configuraciones y programación suplementaria en el entorno específico de la entidad.

En semejantes situaciones, el auditor deberá prever tiempo adicional para identificación de los riesgos y la evaluación de los controles pertinentes.

Cuanto mayor sea la adaptación de una aplicación estándar a las especificaciones de una empresa/entidad, mayor deberá ser el análisis de los parámetros, de la gestión de los flujos de datos y de las adaptaciones técnicas de los programas.

Dentro de este grupo probablemente la aplicación más extendida, sobre todo en implantaciones recientes en empresas y fundaciones pequeñas y medianas sea Microsoft Dynamics NAV (antes comercializada con el nombre de NAVISION).

c) Desarrollos propios

En el caso de desarrollos propios, el auditor no puede apoyarse en informaciones y experiencias de conocimiento general y debe adaptar sus procedimientos de auditoría a la aplicación correspondiente.

Las aplicaciones desarrolladas internamente por la entidad auditada generalmente exigen un trabajo de auditoría más importante. En estas situaciones, la colaboración entre el auditor, el responsable de la aplicación, o en su defecto, el desarrollador de la misma, tiene una gran importancia.

En el caso de aplicaciones estándar muy adaptadas y de desarrollo propio, el auditor se apoyará, por razones de eficacia, en la medida de lo posible, sobre pruebas realizadas y documentadas en el seno de la empresa. Si las pruebas no existen o no son pertinentes (el concepto o la documentación de las pruebas contiene lagunas, errores no corregidos después de los test, etc.), el auditor realizará las pruebas necesarias para alcanzar sus objetivos de auditoría.

En el caso de desarrollos propios se debe prestar mayor énfasis a la evaluación de riesgos y controles generales de estas tres áreas:

- Desarrollo y pase a producción (o cambios a programa).
- Controles de acceso a la aplicación.
- Segregación de funciones.

En las Administraciones públicas de tamaño mediano o grande, será habitual encontrar una o varias aplicaciones significativas desarrollada ad hoc, bien con medios propios o, frecuentemente, con la colaboración parcial o total de empresas externas.

7.5.2. Algunos aspectos de los ERP relevantes para la auditoría

a) Los derechos de acceso

La gestión de los permisos o derechos de acceso es un área que debe ser estudiada sistemáticamente.

La implantación de un ERP lleva a reunir en el seno de la misma aplicación numerosas funcionalidades que antes podían estar repartidas entre varios sistemas. Por ejemplo, la gestión del proceso de compras puede integrar las funcionalidades siguientes:

— el mantenimiento de proveedores
— la gestión de pedidos
— la comprobación de albaranes
— la contabilización de facturas
— el pago de facturas

El principio de segregación de funciones es más fácil de respetar en una empresa que utiliza diferentes sistemas, dando por ejemplo acceso a una persona a la aplicación contable y a otra distinta a la de mantenimiento de proveedores. En un ERP integrado todas las funcionalidades están en la misma aplicación y la entidad debe establecer la separación de funciones con la ayuda de la gestión de derechos de acceso y perfiles de usuario.

La gestión de derechos es un elemento esencial de la seguridad lógica y permite por lo general definir perfiles de acceso tipo. Conviene conocer:

- La forma en que se realiza la gestión de los derechos, pues ciertas entidades pueden haber dado los mismos permisos a todos los usuarios.
- La documentación del ERP.

También es necesario comprobar los parámetros generales de seguridad. Su ausencia es una debilidad del sistema:

- Gestión de contraseñas (longitud, frecuencia de cambio, ..)
- Protección del puesto de los usuarios (bloqueo en caso de intentos de conexión, desconexión automática transcurrido un tiempo sin utilización).
- Histórico de las operaciones realizadas por los usuarios.

b) Parametrización

Una de las características principales de un ERP es la capacidad de parametrización de sus aplicaciones. La parametrización permite,

en cierta medida, adaptar el sistema al funcionamiento a las peculiaridades de la entidad. Si las posibilidades de parametrización pueden ser muy desarrolladas, las diferencias en la forma de funcionamiento y de organización de las entidades de un mismo sector pueden ser numerosas.

Las empresas generalmente modifican la parametrización estándar del ERP e intentan adaptarlo a su modo de funcionamiento.

Así, antes de analizar la parametrización de un ERP, es necesario conocer las condiciones en las que ha sido instalado y las adaptaciones que ha experimentado:

- Una adaptación o una modificación de las funcionalidades de parametrización por la empresa será objeto de un análisis idéntico a la que será realizada si se revisara un software desarrollado internamente: análisis de las necesidades, de los programas, de la estructura de ficheros, etc.
- Una utilización estándar de las funcionalidades de la parametrización por la entidad permitirá comprobaciones simplificadas.

La revisión de la parametrización debe empezar por:

- El análisis de la documentación disponible necesaria para una buena comprensión del funcionamiento de un ERP
- El análisis de las áreas sensibles de un ERP que se correspondan con las áreas analizadas en el marco de la auditoría financiera. La complejidad de un ERP hace absolutamente imposible la realización de una revisión completa de la parametrización.

La revisión de la parametrización consiste en estudiar las reglas de gestión operativas y las reglas de gestión financieras:

- Reglas de gestión operativas.

  Se refieren a los módulos relacionados con los procesos de negocio (compras, ventas, concesión de subvenciones, …). Las selecciones realizadas por la empresa y la existencia de anomalías de parametrización tienen incidencia directa en la generación de las cuentas, por eso es necesario no limitar las comprobaciones únicamente a las aplicaciones contables.

- Reglas de gestión contables y financieras.

  El análisis de las reglas de gestión contable en un ERP se refiere no solo a los parámetros estándar comunes a toda aplicación contable (plan de cuentas, aplicación del IVA, criterios

de facturación, etc) sino también a los puntos de integración o interfaces internas, que permiten la transferencia de datos entre los distintos módulos.

Si no existen reglas generales para las interfaces internas, es corriente encontrar las siguientes situaciones:

a. Los parámetros que permiten la integración entre dos módulos se definen generalmente en el módulo origen (ejemplo: los parámetros de la contabilidad de compras se gestionan en el módulo de pedidos). La parametrización consiste a menudo en la definición de un tipo o de una categoría (por ejemplo una clase de compra, un tipo de pedido). En estos casos se revisará la forma en la que estos parámetros se definen y el enlace que tiene con el módulo de contabilidad.

b. Los enlaces entre los módulos pueden ser realizados:

   b.1 Por una tabla de correspondencias (por ejemplo entre un tipo de compra y una cuenta del grupo 6) que permite el paso automático de los datos entre dos módulos.

   b.2 Por una parametrización al nivel de la transacción, es decir que el dato, por ejemplo el pedido, contiene los diferentes parámetros (tipo de compra, número de cuenta). Los datos son entonces directamente accesibles por los diferentes módulos.

c) Datos maestros

Son bases de datos de carácter permanente utilizadas en los programas. Puede haber varios grupos de datos maestros y darse las siguientes situaciones:

- El repositorio de datos maestros de la entidad es común al conjunto de los módulos para hacer posible su integración.
- Los repositorios son especializados por módulo.

Sea cual sea el ERP, el análisis del repositorio de datos maestros consiste en investigar la utilización que de ellos se hace en los distintos módulos. Si un repositorio puede compartirse por varios módulos, normalmente no lo utilizarán de la misma forma. El repositorio de clientes está gestionado normalmente por el módulo de gestión comercial, aunque ciertas informaciones pueden ser utilizadas por otros módulos (por ejemplo la contabilidad auxiliar de clientes).

Ciertos ERP complejos prevén compartir los datos maestros entre distintos módulos dando a cada módulo la posibilidad de gestionar los datos propios, enlazando estos a los datos centrales del repositorio.

Este análisis debe efectuarse a la vista del estudio de los derechos de acceso para conocer los derechos de acceso dados a los usuarios de los datos maestros.

d) Segregación de tareas

Una adecuada segregación de tareas incompatibles es un aspecto importante para determinar si las actividades de control de una entidad son eficaces para alcanzar los objetivos de control interno.

El concepto básico subyacente en la segregación de tareas es que ningún empleado, funcionario o grupo de ellos, está en disposición de cometer y ocultar errores o irregularidades en el normal desempeño de sus tareas. En general, las principales tareas incompatibles que deben estar segregadas, son:

- Custodia de activos.
- Autorización o aprobación de transacciones relacionadas con dichos activos.
- Registro y soporte de transacciones relacionadas.

Los sistemas tradicionales de control interno confiaban en asignar estas tareas a diferentes personas, segregando funciones incompatibles. Dicha segregación de tareas pretende prevenir que una persona tenga tanto acceso a los activos y disponibilidad sobre ellos como responsabilidad en su contabilidad.

En un entorno informatizado la segregación de tareas es tradicionalmente considerada como un elemento crítico de los controles generales TI y revisada acorde con esa importancia. Por ejemplo, las entidades implementan controles que restringen la capacidad de una persona de pasar programas a producción. También se segregan tareas de solicitud y concesión de accesos a los sistemas y datos.

Una adecuada segregación de tareas es también crítica al nivel del proceso y aplicación de negocio. Una de las principales cuestiones a determinar es cuáles son esas tareas incompatibles en el nivel de las aplicaciones, ya que, la segregación de tareas, que era relativamente fácil de diseñar e implementar con los antiguos sistemas informáticos requiere ser refinada en un entorno ERP integrado.

En el diseño de los sistemas ERP se ha puesto especial énfasis en proporcionar al usuario potentes instrumentos de gestión, fa-

cilitando que tengan acceso a las diversas funciones del negocio o actividad a través de la entidad, o a manejar activos físicos y registrar sus movimientos directamente en el ordenador y en los sistemas contables. En este entorno actual, la noción de segregación de tareas debe ser desarrollada incluyendo la perspectiva de gestión de los riesgos.

El análisis de la segregación de tareas implantada en los sistemas es un procedimiento a realizar en todas las fiscalizaciones y para realizar esta revisión y evaluar la eficacia de control y los riesgos relacionados se elaborará una matriz de segregación de tareas incompatibles.

7.5.3. SAP ERP

a) Breve apunte de la evolución histórica y características básicas

SAP es uno de los fabricantes de ERP cuyos productos están más extendidos en España y en todo el mundo, especialmente entre las grandes organizaciones. Dado que fue uno de los creadores del concepto ERP vamos a dar unas breves pinceladas de la evolución histórica de este producto.

En 1972 cinco antiguos empleados de IBM crearon en Alemania la compañía Systems Applications and Products in Data Processing, conocida por su acrónimo SAP, con el objetivo de desarrollar aplicaciones informáticas estándar.

En 1973 SAP desarrolló y comercializó el sistema R/1 de contabilidad financiera.

En 1979 publicó el sistema SAP R/2 que funcionaba sobre un *mainframe* y soportaba distintos lenguajes y monedas.

SAP R/3 se publicó en 1992. Este producto dio el salto de la estructura basada en *mainframe* a la arquitectura cliente-servidor de tres niveles. La «R» de SAP R/3 es la inicial de *realtime* (tiempo real) y el número 3 se refiere a la arquitectura de 3 niveles o capas:

- Capa de la aplicación

  Es el nivel en el que se procesan todos los datos almacenados en las bases de datos de acuerdo con las peticiones de los usuarios.

- Capa de base de datos

  Esta capa es el SGBD utilizado por la aplicación. El Servidor de Base de Datos procesa los pedidos SAP de los programas de aplicación y devuelve los datos requeridos. SAP soporta las principales bases de datos existentes en el mercado.

– Capa de presentación

La presentación de la aplicación es igual para todas las plataformas. Constituye la interfaz gráfica del sistema, es decir, la imagen de la aplicación.

SAPGUI es el nombre del software que se instala en cada ordenador de usuario. En las últimas versiones de SAP ERP la interfaz con el usuario puede hacerse a través de un navegador web.

Gráficamente:

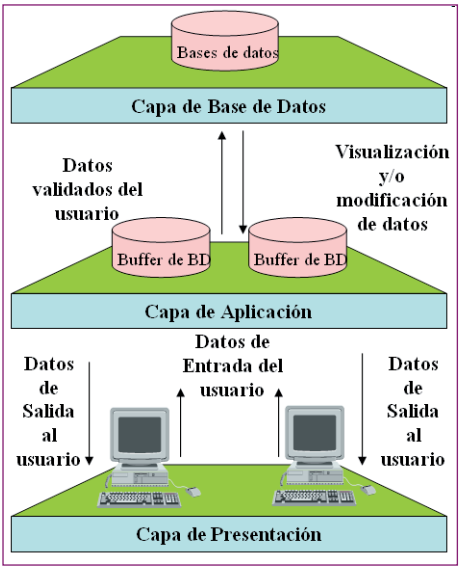


Figura 7.13. Arquitectura de tres niveles de SAP R/3

Los componentes de cada capa pueden, cada uno, ser gestionados por equipos diferentes. Además, SAP puede funcionar sobre una gran diversidad de hardware, sistemas operativos y bases de datos:

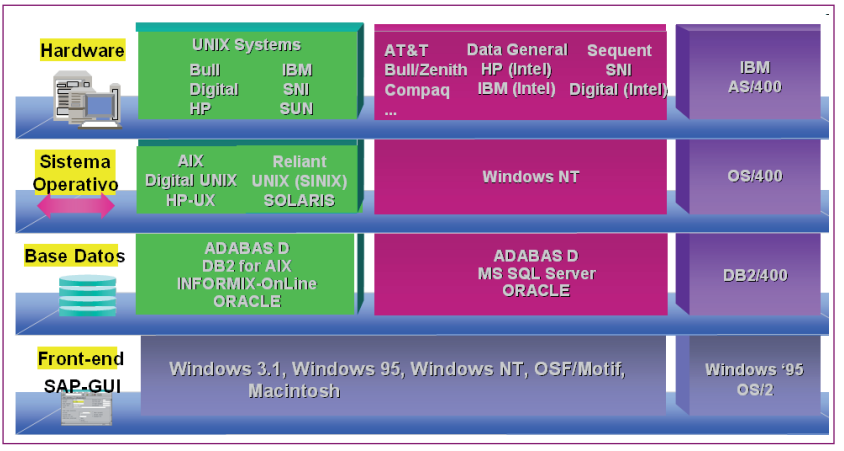


Figura 7.14

Con R/3 se introdujo el concepto cliente-servidor, un uso coherente de las bases de datos relacionales y la capacidad de funcionar en ordenadores de diferentes fabricantes, estableciendo unos estándares que todavía se mantienen en lo sustancial.

SAP R/3, hasta la Version 4.6C, consistía en varias aplicaciones funcionando sobre SAP Basis, que es un conjunto de programas y herramientas middleware, sobre el cual se construye una estructura modular, lo cual le proporciona una gran flexibilidad y dinamismo a la hora de adaptarse a las necesidades funcionales de diversos sectores y entidades (ver figura siguiente).

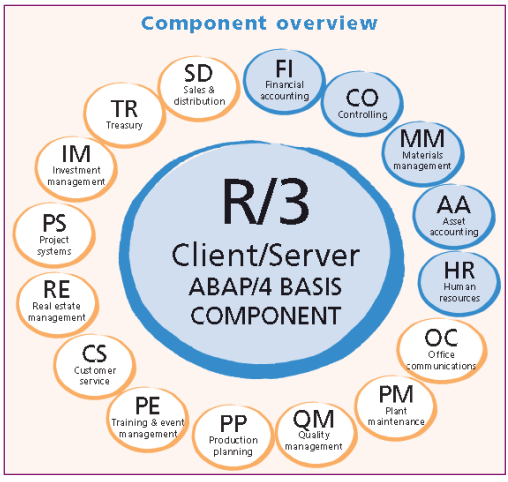


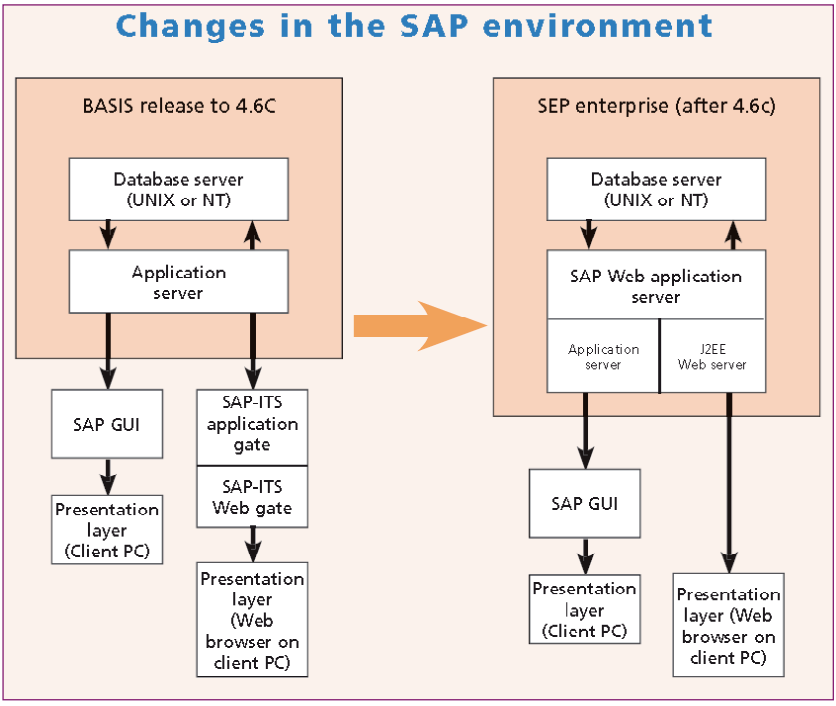
Figura 7.15 Componentes o módulos de SAP R/3

El módulo Basis proporciona la arquitectura básica para R/3 y abarca el software de sistema y los servicios que subyacen bajo las aplicaciones R/3. Es el módulo que se debe usar cuando se implementa cualquier nueva aplicación (SAP tiene muchos módulos y submódulos de aplicaciones). Tiene las siguientes funciones y características:

- Configuración de funciones vía control central de tablas, sin modificación de programas.
- Provee herramientas para crear y modificar tablas, cambiar diseños de pantallas y mejorar el sistema.
- Provee la habilidad para implementar la seguridad de los diferentes módulos, incluido Basis.
- Mantenimiento de la base de datos y el diccionario ABAP/4.
- Contiene herramientas para la administración del sistema, esto permite al administrador de Basis mantener la integridad y el rendimiento del sistema SAP.

– Soporte para intercambio electrónico de datos.
– Documentación on line de información de Ayuda.

Cuando SAP R/3 Enterprise (*release 4.6C*) fue publicado en 2002, todas las aplicaciones fueron construidas sobre *SAP Web Application Server. Extension sets* eran utilizados para proporcionar nuevas funciones y mantener el núcleo lo más estable posible. El *Web Application Server* contenía todas las capacidades de *SAP Basis* y permitía la utilización de tecnologías web. En la siguiente figura se refleja gráficamente la evolución.



Fuente: Security and Control for SAP R/3 Handbook Update, ANAO
Figura 7.16 Cambios en el entorno SAP

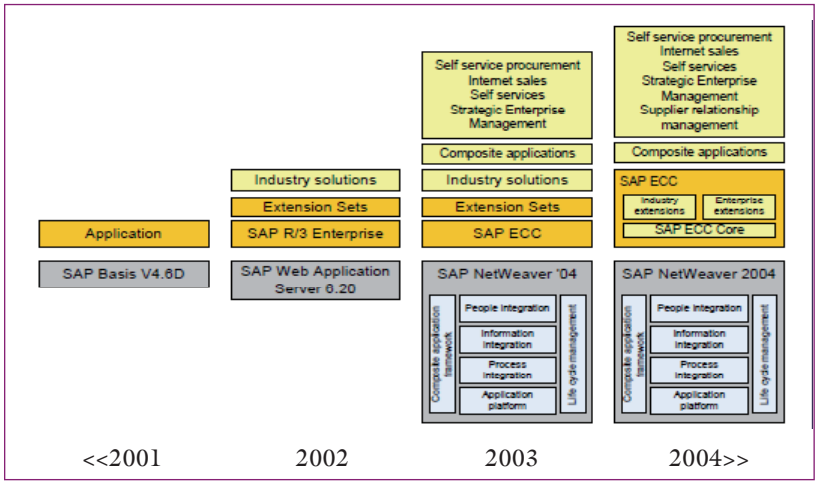
La primera edición de mySAP ERP fue lanzada en marzo de 2003 e incluía una serie de, hasta entonces, productos separados, como SAP R/3 Enterprise, *SAP Strategic Enterprise Management*, y *extension sets*. El *SAP Web Application Server* fue empaquetado dentro de NetWeaver,[80] también fue introducido en 2003; mySAP tenía una nueva plataforma (NetWeaver), nueva tecnología del in-

80. NetWeaver es un conjunto de herramientas y tecnologías middleware que proporciona a los usuarios una interfaz unificada entre Java y sistemas SAP basados en el lenguaje de desarrollo ABAP propio de SAP.

terfaz de usuario, nuevas herramientas analíticas y muchas nuevas funcionalidades.

SAP NetWeaver ofrecía un completo conjunto de tecnologías de software incluyendo funcionalidades de infraestructura de portal, *business warehousing*, integración de aplicaciones, servidor de aplicaciones Web, tecnologías móviles, etc. Esta nueva plataforma está en el centro de la estrategia a largo plazo de SAP.

En 2004 tuvo lugar un cambio de arquitectura con la introducción de mySAP ERP 2004. R/3 Enterprise fue reemplazado con la introducción de *ERP Central Component* (SAP ECC). El *SAP Business Warehouse, SAP Strategic Enterprise Management*, e *Internet Transaction Server* fueron también integrados en SAP ECC, permitiendo a los usuarios hacerlos funcionar desde una única ubicación lógica (instancia en la terminología SAP). También se realizaron cambios en la arquitectura para soportar la transición a la denominada *Service-oriented architecture*.[81]



Fuente: SAP Backup using Tivoli Storage Manager, June 2009
Figura 7.17 Evolución SAP R/3 – SAP ERP

mySAP ERP 2004 incluía nuevas funcionalidades adicionales, e integraba y expandía la utilización de la plataforma SAP NetWeaver (que amplía el concepto sobre el que se basaba el módulo Basis) comparado con la versión de 2003.

81. Service-oriented architecture (SOA) es un modelo para una arquitectura TI adaptable, flexible y abierta, para desarrollar soluciones de negocio modulares orientadas al cliente.

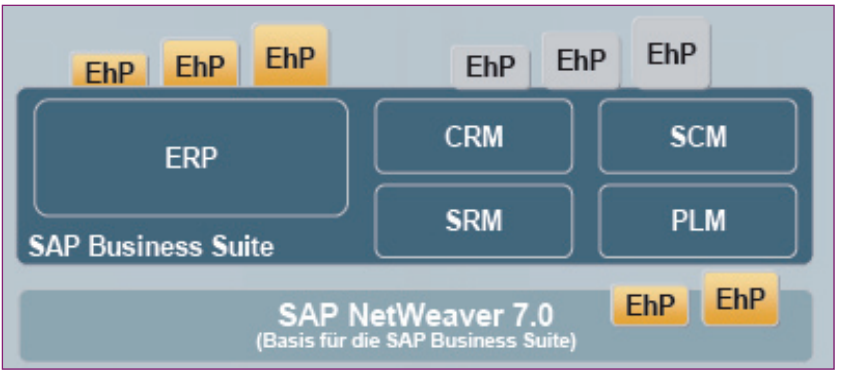
Es en este último punto donde SAP se encuentra enfrentada con Microsoft e IBM, en lo que se conoce como «la guerra de las plataformas». Microsoft ha desarrollado una plataforma basada en la web llamada .NET, mientras que IBM ha desarrollado otra llamada WebSphere. También compite con el middleware Fusion Oracle.

Esta plataforma tecnológica convierte a SAP en un programa con el que se puede trabajar con SAP mediante cualquier navegador de internet si se tienen los componentes apropiados de SAP NetWeaver (SAP Portals).

NetWeaver permite gestionar la base de datos con el *Computing Center Management System* (CCMS). Con CCMS, se pueden tener amplias funciones de administración de la base de datos y gestionarlas desde NetWeaver. CCMS es un componente estándar de NetWeaver.

SAP ERP 6.0 fue lanzado en junio de 2006 (funcionando sobre NetWeaver 7.0) y en junio de 2009 fue lanzado el denominado «SAP enhancement pack 4 for SAP ERP 6.0» (los enhancement pack – EhP, incorporan nuevas funcionalidades y son equivalentes a la versión del software).

Como los otros grandes fabricantes de software, que también se mencionan en este trabajo, ofrece una SAP Business Suite compuesta por una familia de aplicaciones informáticas, con un alto grado de integración y funcionalidades específicas para distintas industrias, preparada para colaborar con terceros a través de Internet. Todos los productos SAP están focalizados en el principal producto de la compañía: SAP ERP.



Fuente: SAP
Figura 7.18 Esquema de SAP Business Suite

Las aplicaciones incluidas en SAP Business Suite proporcionan un completo soporte a los procesos de negocio, información finan-

ciera y analítica. Sus aplicaciones principales, aplicaciones sectoriales y suplementarias están movidas por la plataforma tecnológica NetWeaver.

SAP Business Suite incluye las siguientes aplicaciones:

- Enterprise Resource Planning (ERP)

  Incluye cuatro soluciones individuales para sendas áreas funcionales: SAP ERP Financials, SAP ERP Human Capital Management, SAP ERP Operations, y SAP ERP Corporate Services.
- Customer Relationship Management (CRM)
- Product Lifecycle Management (PLM)
- Supply Chain Management (SCM)
- Supplier Relationship Management (SRM)

Simultáneamente a la más reciente versión de SAP ERP, también se comercializan dos productos destinados a la mediana empresa: SAP All-in-One, que incorporar soluciones especializadas para los distintos sectores industriales; y a la pequeña empresa: SAP Business One que es una aplicación que reside en un servidor basado en Windows y que soporta las bases de datos MS SQL e IBM DB2.

Además, la versión anterior SAP R/3 4.6C está todavía operativa en muchas organizaciones y soportada por SAP. Por tanto en las fiscalizaciones actuales pueden encontrarse y revisarse cualquiera de las versiones mencionadas.

b) Procedimientos de auditoría específicos para entornos SAP

Al diseñar la auditoría de sistemas de información en un entorno SAP se debe tener en cuenta su diseño específico, que brevemente se ha repasado en los apartados anteriores. Muy esquemáticamente diremos que la auditoría comprenderá dos bloques:

Auditoría de controles generales de la plataforma TI:

- Bases de datos.
- Sistemas operativos.
- Redes y comunicaciones.
- Aspectos físicos y organizativos del entorno de TI.

Para auditar estas áreas servirá la metodología general descrita en este trabajo.

Auditoría específica del entorno SAP:[82]

- Plataforma SAP: Módulo Basis o NetWeaver
- SAP R/3 ó 6.0: módulo específico, normalmente Financials
- Proceso de negocio y estructura organizacional.

Para revisar todas estas áreas se podrán seguir los siguientes procedimientos principales:

1. Planificación de la auditoría

Objetivo

Establecer, y coordinar con los responsables de la Entidad, la planificación de las actividades y los recursos necesarios para un desarrollo eficaz de la auditoría.

Actividades y tareas a desarrollar

- Definición detallada de los objetivos de la auditoría.
- Identificación de los principales interlocutores.
- Establecimiento del calendario de la auditoría.
- Establecimiento del equipo de trabajo.
- Exposición del proyecto y metodología.
- Presentación del equipo de trabajo.

2. Identificación y evaluación preliminar del entorno informático

Objetivo

Identificar los procesos críticos de negocio, la estructura organizativa y las plataformas tecnológicas que soportan los sistemas de información de la entidad.

Actividades y tareas a desarrollar

- Identificación de los procesos significativos y de los riesgos derivados de la actividad.
- Identificación de la plataforma tecnológica que soporta las aplicaciones revisadas:
  - — Versión de los sistemas operativos y Base de Datos.
  - — Herramientas de administración de gestión de usuarios.
  - — Herramientas de administración de gestión de cambios a programas.

82. Para la auditoría específica de entornos SAP son de especial interés los tres manuales sobre esta materia publicados por la Australian Nacional Audit Office que se reseñan en la bibliografía.

- Entendimiento de la estructura organizativa:
  - Análisis del organigrama de sistemas de información.
  - Análisis de las funciones de sistemas de información y su adecuada distribución entre los integrantes del área.
- Evaluación del marco procedimental:
  - Políticas de seguridad.
  - Procedimientos de control de acceso a los sistemas de información.
  - Procedimientos de control de cambios en los sistemas de información.
  - Procedimientos relacionados con otras operaciones de TI (Gestión de incidencias, gestión de copias de resguardo y restauración).
- Elaborar resumen detallado de procesos críticos/plataforma tecnológica.
- Elaborar resumen de debilidades identificadas.

3. Auditoría de los Controles Generales de la Plataforma SAP

3.1. Gestión de cambios a programas

Objetivo

Evaluar los controles existentes en el procedimiento de Gestión a cambios a programas (nuevos desarrollos, mantenimientos, parametrizaciones) en la aplicación SAP.

Actividades y tareas a desarrollar

- Análisis de las metodologías y procedimientos vigentes para el proceso de Gestión de cambios a programas en las aplicaciones SAP revisadas, considerando:
  - La formalización de la solicitud de cambio.
  - Esquema de aprobación formal del usuario.
  - Tipos de pruebas que deben efectuarse y documentarse.
  - Niveles de autorización requeridos.
  - Diferentes circuitos y niveles para cada tipo de cambio.
- Identificación de los responsables involucrados en el proceso de Gestión de cambios a programas y parametrizaciones en la aplicación SAP.
- Definición de los controles claves involucrados en los controles claves del proceso de Gestión de cambios a programas y parametrizaciones en la aplicación SAP.

- Evaluación del esquema de separación de entornos establecidos en la aplicación SAP (mandantes): Desarrollo, Testing y Producción.
- Evaluación del esquema de separación de funciones del personal involucrado en el Desarrollo, Mantenimiento e Implementación de los cambios en el entorno de Producción.
- Ejecución de una prueba de recorrido (Walkthrough) del proceso Gestión de cambios a programas y parametrizaciones en la aplicación SAP, de manera de evaluar el grado de cumplimiento de los Controles Claves identificados.
- Ejecución de una prueba de cumplimiento del proceso de Gestión de cambios a programas y parametrizaciones en la aplicación SAP, donde se analiza la existencia de documentación de respaldo relacionada con:
  - Existencia de una solicitud formal de cambio.
  - Existencia de una aprobación formal de los cambios solicitados.
  - Existencia de un plan de pruebas y de una participación del usuario solicitante.
  - Existencia de aprobaciones de traspaso entre los distintos entornos SAP.

  Para la validación mencionada se seleccionará una muestra.
- Evaluación de los resultados de las pruebas de cumplimiento y en caso de identificar controles que no funcionen según su propósito y diseño, identificar si existieran controles compensatorios y/o factores mitigantes.
- Elaborar resumen de debilidades de control identificadas en el procedimiento de Gestión de Cambios a programas.

3.2. Gestión de usuarios y controles de acceso

Objetivo

Evaluar los controles existentes en el procedimiento de gestión de usuarios en la aplicación SAP.

Actividades y tareas a desarrollar

- Análisis de las metodologías y procedimientos vigentes para el procedimiento de Gestión de usuarios y perfiles en la aplicación SAP, considerando:
  - Formalización de la solicitud de Alta, Baja o Modificación de cuentas de usuario.

— Esquema de Aprobación por parte del responsable funcional.
— Involucramiento del departamento de Recursos Humanos en el proceso de baja de cuentas de usuario.
— Diferentes circuitos y niveles de autorización para cada tipo de usuario.

- Identificación de los responsables involucrados en el proceso de Gestión de usuarios y perfiles en la aplicación SAP.
- Definición de los controles clave involucrados en el proceso de Gestión de usuarios y perfiles en la aplicación SAP.
- Ejecución de una prueba de recorrido (Walkthrough) del proceso de Gestión de usuarios y perfiles en la aplicación SAP, de manera de evaluar el grado de cumplimiento de los controles clave.
- Ejecución de una prueba de cumplimiento del proceso de Gestión de usuarios y perfiles en la aplicación SAP, donde se analiza la existencia de documentación de respaldo relacionada con:
  — Existencia de una solicitud formal de Alta, Baja o Modificación de usuario.
  — Existencia de una aprobación formal de la solicitud de Alta, Baja o Modificación.
  — En caso de Alta o Modificación, se evaluará si los perfiles solicitados corresponden con los realmente definidos en la aplicación SAP.
  — En caso de Baja se evaluará si los perfiles han sido eliminados o bloqueados en la aplicación SAP.

Para la validación mencionada se seleccionará una muestra.

- Evaluación de los resultados de las pruebas de cumplimiento y en caso de identificar controles que no funcionen según su propósito y diseño, identificar si existieran controles compensatorios y/o factores mitigantes.
- Elaborar resumen de debilidades de control identificadas en el proceso de Gestión de usuarios y perfiles en la aplicación SAP.

3.3. Controles de seguridad lógica.

Objetivo

Evaluar las medidas de seguridad en los entornos de procesamiento que soportan la aplicación SAP.

Actividades y tareas a desarrollar

- Identificar el tipo y las versiones de los Sistemas Operativos, Base de Datos y herramientas de gestión (en caso de existir) que soportan la aplicación SAP.
- Ejecutar *scripts* para la obtención de informes de seguridad en los Sistemas Operativos y Base de Datos identificados.
- Mediante la ejecución del programa de trabajo correspondiente, se llevará a cabo la evaluación de seguridad considerando los siguientes aspectos:

Sistemas Operativos

- Configuración de los parámetros de seguridad.
- Parámetros para la construcción de contraseñas (longitud, rotación, etc.).
- Perfiles de administración y críticos.
- Perfiles de usuarios y grupos.
- Autorizaciones sobre directorios y ficheros.
- Configuración de log de auditoría.
- Elaborar resumen debilidades de seguridad identificadas en el Sistema Operativo.

Base de Datos

- Configuración de los parámetros de seguridad.
- Parámetros para la construcción de contraseñas.
- Perfiles de administración y críticos.
- Perfiles de usuarios y grupos.
- Autorizaciones sobre directorios y ficheros.
- Configuración de log de auditoría.
- Elaborar resumen debilidades de seguridad identificadas en la Base de Datos.

Herramientas de gestión

- En caso de existir, se evaluarán las herramientas de gestión de solicitudes que soportan los procesos de administración de usuarios y cambios en la aplicación SAP, considerando los aspectos de configuración de los parámetros de seguridad y los perfiles de administración definidos.
- Elaborar resumen de debilidades de seguridad identificadas en las herramientas de gestión.

4. Evaluación de la seguridad de la aplicación SAP.

Objetivo

Evaluar las medidas de seguridad establecidas en la aplicación SAP.

Actividades y tareas a desarrollar

- Evaluación de la configuración de los parámetros de seguridad del sistema SAP R/3 con el objetivo de verificar si la compañía ha establecido mecanismos de seguridad efectivos.
- Evaluación de las medidas de seguridad relacionadas con la identificación y autentificación de usuarios.
- Análisis de la asignación de las transacciones de sistema críticas (administración de usuarios, de la gestión de cambios así como de la planificación de tareas programadas).
- Evaluación de la segregación de funciones dentro de los procesos de sistemas de información y de negocio, entre otras (solo un breve ejemplo) presentan incompatibilidad las siguientes transacciones:

Transacciones – Procesos de Sistemas de Información	
SCC4	Acceso a los parámetros de configuración Cliente
SM30	Acceso para actualizar directamente tablas
STMS	Acceso para realizar los Pasos a Producción

Transacciones – Procesos de Negocio	
AS02	Modificar un Activo Fijo
FSP0	Modificación Cuenta Libro Mayor (a nivel de Plan de Cuenta)
OB52	Abrir/Cerrar períodos contables (tabla T001B)

- Identificación y evaluación de los controles de aplicación (automáticos y manuales) que soportan los procesos de negocio bajo alcance, mediante la ejecución de:
  - Pruebas de cumplimiento.
  - Pruebas sustantivas y/o controles compensatorios que mitiguen los riesgos.
  - Técnicas de reprocesamiento y análisis de datos (evaluación: integridad y exactitud).
- Elaborar matriz para la evaluación de segregación de funciones en SAP.

5. Revisión de los controles en la aplicación (procesos SAP)

Para el análisis de cada módulo SAP (un proceso de negocio puede implicar la intervención varios módulos) se sigue la metodología resumida en las figuras 4.3 y 4.4. No obstante dada la particular naturaleza de SAP habrá que identificar y analizar los siguientes aspectos particulares:

- La arquitectura específica instalada del módulo de SAP revisado.
- La estructura y datos organizacionales de SAP.
- Tablas maestras de datos involucradas en el proceso.
- Los tipos de documentos y rangos de los mismos.
- Las transacciones empleadas en el proceso y autorizaciones sobre las mismas.
- Los controles automáticos estándar (y aquellos específicos) incluidos en el flujo del proceso y en la generación de cálculos e informes.
- Las parametrizaciones y «customizaciones» o adaptaciones respecto del estándar del proceso.

Concretamente las pruebas sobre los controles de aplicación en SAP, se realizarán de diversos modos:

- En casos donde la validación de los cálculos generados en un proceso sea crítico, se realizarán pruebas de recálculo que permitan validar las que son actualmente realizadas por el sistema, para ello se procederá de la siguiente manera:
  - Mediante el uso de CAAT se realizarán recálculos de las transacciones así como la simulación del propio proceso con datos reales del sistema.
  - Se analizarán los datos a lo largo del proceso de negocio para supervisar la integridad de la información y controles del proceso.
- Verificación de las parametrizaciones y customizaciones del sistema SAP para validar los controles automáticos implantados (*3-way matching* en el proceso de facturación, períodos de apertura y cierre de ejercicios contables, cuentas preconfiguradas para contabilizaciones automáticas, etc.).
- Seguimiento in-situ del flujo del proceso para verificar on-*line*, recolectando pruebas y simulando situaciones posibles (en algunos casos en entornos de preproducción) que los controles están implantados y funcionan correctamente.

c) Herramientas de auditoría

Herramientas SAP

En los últimos años se han desarrollado herramientas para automatizar las tareas de auditoría que permiten extraer y analizar los datos centrales de SAP (perfiles de seguridad, configuraciones, etc) utilizados para configurar el sistema de forma más eficaz y eficiente que utilizando procedimientos de muestreo y probar que SAP ha sido configurado de la forma prevista.

Utilizar estas herramientas permite al auditor analizar y obtener conclusiones relativas a toda la población en lugar de extrapolar los resultados obtenidos de una muestra.

- AIS (Audit Information System)

  AIS proporciona a los auditores una herramienta que ayuda a comprender y cumplimentar determinadas tareas de auditoría en el complejo entorno SAP. Suministra un repositorio centralizado para informes, *queries* y vistas de datos que tienen implicación en los controles, y permite trabajar en línea, en producción.
- SUIM (User Information System Management)

  Información sobre las cuentas de usuario SAP y sus permisos de acceso.
- IMG (Implementation Management Guide)

  Herramientas de configuración y personalización de SAP.
- PFCG (Profile Generator)

  Mantenimiento de roles de usuario en SAP.
- STMS (SAP Transport Management System)

  Para la gestión de cambios a programa.
- SAP Query

  Para generar consultas específicas no existentes en caso necesario.

Otras herramientas

Otras herramientas que se pueden utilizar son las mencionadas en el capítulo 8 sobre los CAAT: ACL, IDEA, ACL Direct Link

7.5.4. ORACLE

a) Breve apunte de la evolución histórica

Otro actor importante en el mundo de las aplicaciones informáticas es la empresa Oracle, que fue creada en 1977.

La primera versión comercializada de su base de datos fue llamada Oracle Version 2 (la empresa decidió llamarla versión 2 en lugar de versión 1 porque creían que los clientes no se decidirían a comprar la versión 1 de un producto).

La Oracle Version 3, lanzada en 1983 es el primer SGBD que funcionó tanto en mainframes, como en minicomputadores y PCs, dando a los clientes la capacidad de usar el software en casi cualquier entorno informático.

En 1987 ya era el fabricante de bases de datos más importante del mundo.

En 1989, tras entrar en el mercado de las aplicaciones de negocio lanza Oracle Financials y en 1990 lanza la Oracle Applications Release 8, que incluye programas de contabilidad diseñados para el entonces emergente mercado de los entornos cliente-servidor.

En 1998 con Oracle 8 Database y Oracle Applications 10.7, Oracle utiliza e integra el lenguaje de programación Java.

En 2000 se publica Oracle E-Business Suite Release 11i, su *suite* integrada de aplicaciones de negocio.

En 2005 Oracle compra a su rival en el mercado de las aplicaciones de negocio PeopleSoft, al que sigue la adquisición de Siebel Systems, J.D.Edwards, etc.

Según su web, Oracle E-Business Suite es un conjunto de aplicaciones que permiten a las empresas y entidades seguir de forma eficiente la información detallada de las transacciones y convertirlas en información para la toma de decisiones. Incluye el subconjunto de aplicaciones Oracle Financials diseñadas para capturar y analizar los datos con relevancia financiera. Oracle Public Sector Financials, es otro componente de la Suite, diseñado para gestionar presupuestos y controlar los gastos en las administraciones públicas.

En las figuras 7.11 y 7.1 puede verse cual es su posición en el mercado de las bases de datos y de las aplicaciones de negocio respectivamente.

b) Conceptos básicos de Oracle E-Business Suite

Oracle tiene su propia arquitectura de aplicaciones (Oracle Applications Architecture) que es un sistema multinivel, de procesamiento distribuido que soporta las aplicaciones y productos Oracle.

Como en la estructura general por niveles de un sistema de información que ya hemos mencionado a lo largo de este trabajo, en

este modelo, varios servidores (o servicios) están distribuidos en tres niveles (o *tiers* en la terminología de Oracle).[83]

La arquitectura de tres niveles que comprende una instalación de **Oracle** E-Business Suite está formada por:[84]

- La capa de base de datos (*database tier)*, que soporta y gestiona la base de datos Oracle;
- La capa de aplicación (*application tier)*, que soporta y gestiona los distintos componentes de las aplicaciones, y a veces se le conoce como el nivel medio, y
- La capa de usuario (*desktop tier)*, que proporciona el interfaz de usuario mediante un componente añadido al navegador web estándar.

De forma gráfica:

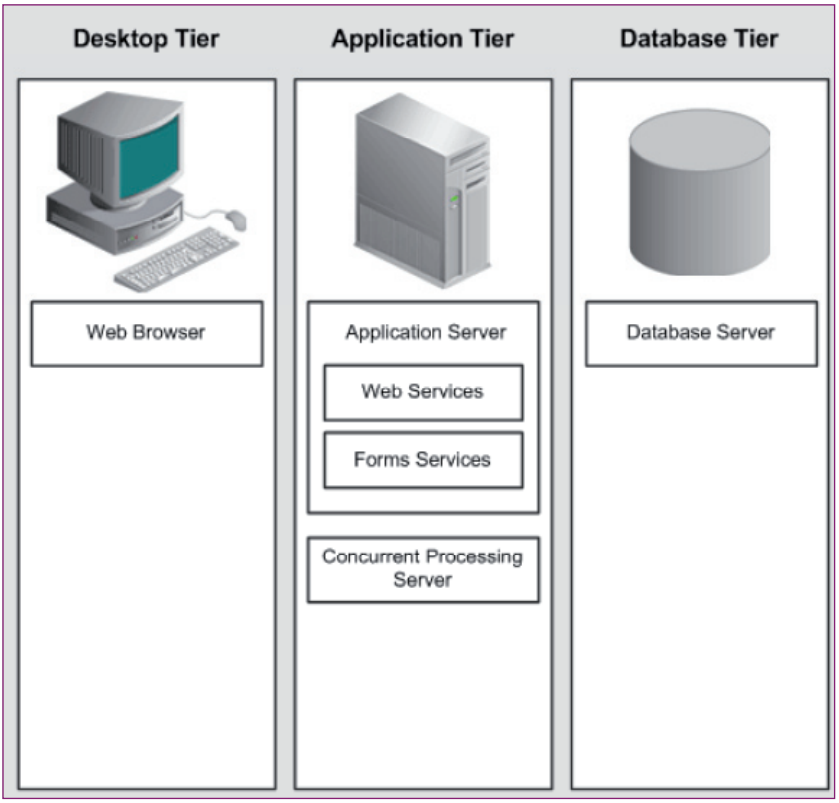


Figura 7.19

83. Un nivel o capa es una agrupación lógica de servicios que puede extenderse a través de varias máquinas físicas.

84. *Oracle Applications Concepts*, Oracle, marzo 2009.

Un servidor (o servicio) es un proceso o grupo de procesos que funciona en una máquina y proporciona una funcionalidad específica. Por ejemplo, *Web services* procesa solicitudes HTTP, y *Forms services* procesa solicitudes relacionadas con *Oracle Forms*.

Una máquina puede ser denominada como «nodo», en particular en el contexto de un grupo de ordenadores que trabajan en conjunto en un *cluster*.

Cada capa puede consistir en uno o más nodos y cada nodo puede potencialmente acomodar más de una capa. Por ejemplo, la base de datos puede residir en el mismo nodo que alguna aplicación. Hay que destacar que un nodo es también un concepto lógico (de software) que se refiere a una agrupación lógica de servidores.

Al centralizar el software de las aplicaciones Oracle en la capa de aplicaciones se elimina la necesidad de instalar y mantener software de las aplicaciones en cada ordenador, y permite escalar fácilmente las aplicaciones cuando se producen aumentos de las cargas de trabajo.

La conexión entre el nivel de las aplicaciones y el nivel del usuario puede realizarse a través de internet.

La capa de aplicaciones tiene un rol dual:

a) contiene los diversos servidores y servicios que procesan las aplicaciones, y

b) gestiona las comunicaciones con los otros dos niveles.

La configuración básica de esta capa la forman tres grupos de servidores o servicios: *Web services, Forms services* y *Concurrent Processing Server*. En la Release 12, *Web and Forms services* son facilitados por *Oracle Application Server 10g*. Ya no hay servidores en el sentido de ser un proceso único, como sucedía en las versiones anteriores.

La capa de la base de datos contiene el servidor de la base de datos, que almacena todos los datos mantenidos por las aplicaciones Oracle. También se almacena el sistema de información y ayuda en línea de las aplicaciones Oracle. Más específicamente, este nivel contiene los archivos del *Oracle data server* y la base de datos de los ejecutables de las aplicaciones Oracle que físicamente guardan las tablas, índices y otros objetos (de base de datos) por el sistema.

En esta capa cada vez se usa más el *Oracle Real Application Clusters (Oracle RAC)*, por el cual múltiples nodos soportan una sola base de datos proporcionando mayor disponibilidad y escalabilidad.

c) Cuestiones de auditoría

Aunque Oracle tiene productos ERP estándar (de acuerdo con la tipología descrita en el capítulo 7.5.1), en el sector público español las aplicaciones desarrolladas e implantadas con las herramientas Oracle hay que considerarlas, en general, como desarrollos a medida, y en consecuencia la metodología de auditoría a aplicar debe adaptarse a cada implantación, no pudiendo apoyarse el auditor en controles estándar predefinidos.

1. Principales debilidades de seguridad

Como en la auditoría de cualquier ERP, un área fundamental es la revisión de la seguridad de los datos. En las grandes organizaciones tanto la dirección, como los funcionarios, auditores y otros usuarios, utilizan y confían en los datos gestionados por el ERP, por tanto, su integridad y fiabilidad es un aspecto crítico que depende de la existencia de un bien diseñado e implantado sistema de seguridad y de buenos controles funcionando eficazmente. Todos los aspectos relacionados con la seguridad del sistema deben ser considerados en las auditorías financieras.

A pesar de ser un elemento crítico como en cualquier sistema complejo, existen una serie de debilidades que se presentan con una cierta recurrencia. En este sentido, en la revista del Grupo de trabajo de auditoría informática de INTOSAI se publicó un artículo[85] en el que se enumeraban las cinco principales debilidades relacionadas con la seguridad en un entorno Oracle (que, por otra parte, son comunes a cualquier ERP):

- Los accesos del equipo de soporte son a menudo excesivos, con demasiados perfiles de acceso que infringen el tradicional principio de segregación de funciones.
- Muchas organizaciones no tienen definidas las políticas de segregación de funciones. Cuando están definidas, muchas organizaciones no tienen controles preventivos o detectivos para hacer respetar esas políticas.
- Oracle no proporciona informes estándar para identificar conflictos de segregación de funciones (aunque existen herramientas que pueden adquirirse por separado). Pocas organizaciones han definido sus propios informes a la medida para hacer frente a este problema.

85. *Oracle Applications: The benefits of using automated audit tools*, Will Drew and Anirvan Banerjee, intoIT n.º 28.

– Pocas organizaciones configuran procedimientos de auditoría para registrar cambios en información de riesgo alto, como, por ejemplo, cuentas bancarias de proveedores.
– Muchas organizaciones no tienen definidos informes de excepción para identificar y seguir excepciones o incidentes de seguridad.

2. Accesos indebidos a las bases de datos

Además de las debilidades al nivel de las aplicaciones, la seguridad en las bases de datos es otra área crítica que es a menudo pasada por alto al auditar una implantación.

Toda la información en las aplicaciones Oracle es mantenida en una base de datos subyacente. Si la base de datos no está adecuadamente securizada, puede accederse a la información y modificarse en el nivel de la base de datos, saltándose todos los controles de las aplicaciones.

Además del riesgo de accesos maliciosos, los manuales de Oracle[86] advierten de los riesgos de pérdida de información si se producen accesos directos a las bases de datos utilizando gestores de base de datos en lugar de utilizar las aplicaciones Oracle. Al igual que en SAP, se recomienda modificar los datos solo a través de las aplicaciones.

Aspectos comunes relacionados con la seguridad de las bases de datos (vistos en detalle en el capítulo 7.3) incluyen el uso de cuentas de

86. *Oracle Applications Concepts*, Oracle, March 2009:
«Do Not Use Database Tools to Modify Oracle Applications Data
Oracle STRONGLY RECOMMENDS that you never use SQL*Plus, Oracle Data Browser, database triggers, or any other tool to modify Oracle Applications data unless otherwise instructed.
Oracle provides powerful tools you can use to create, store, change, retrieve, and maintain information in an Oracle database. But if you use Oracle tools such as SQL*Plus to modify Oracle Applications data, you risk destroying the integrity of your data and you lose the ability to audit changes to your data.
Because Oracle Applications tables are interrelated, any change you make using an Oracle Applications form can update many tables at once. But when you modify Oracle Applications data using anything other than Oracle Applications, you may change a row in one table without making corresponding changes in related tables. If your tables get out of synchronization with each other, you risk retrieving erroneous information and you risk unpredictable results throughout Oracle Applications.
When you use Oracle Applications to modify your data, Oracle Applications automatically checks that your changes are valid. Oracle Applications also keeps track of who changes information. If you enter information into database tables using database tools, you may store invalid information. You also lose the ability to track who has changed your information because SQL*Plus and other database tools do not keep a record of changes.»

usuario genéricas, controles de passwords inadecuados e inexistencia de control de la actividad de los administradores[87] de las bases de datos.

3. Control de los usuarios privilegiados

Respecto de los usuarios privilegiados, debe revisarse que la entidad tenga establecidos controles de acceso a los datos sensibles, incluyendo a los ABD. Como un producto separado existe la herramienta *Oracle Database Vault*, que previene que usuarios privilegiados puedan acceder a los datos de las aplicaciones, los ABD pueden continuar realizando sus tareas pero no pueden acceder o modificar los datos confidenciales. También refuerza las políticas de la organización sobre quién puede acceder, cuándo, cómo a qué aplicaciones, bases de datos y datos. Obviamente para que estos controles funciones deben estar instaladas y activadas esas herramientas.

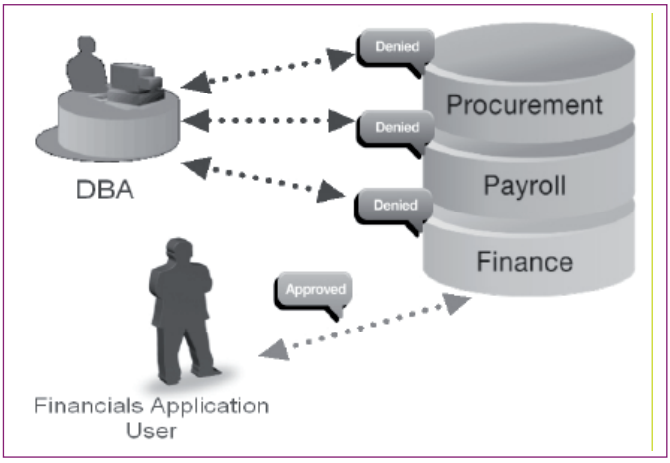


Figura 7.20

4. Herramientas de auditoría

«Muchos entes fiscalizadores están evolucionando hacia un enfoque de auditoría integrado en el que especialistas en auditoría informática efectúan su trabajo para dar soporte en las auditorías financieras. Debido al tamaño y complejidad de los sistemas Oracle, incluso auditores informáticos cualificados pueden encontrar difícil realizar revisiones efectivas de seguridad y controles».[88]

87. Según *Oracle Applications Concepts*, un administrador de base de datos (ABD) es la persona que prepara el servidor BD y las herramientas Oracle para la instalación de las aplicaciones, lleva a cabo tareas de mantenimiento con posterioridad y tiene elevados privilegios de acceso a la base de datos vía las cuentas SYSTEM y SYS.
88. *Oracle Applications: The benefits of using automated audit tools*, Will Drew and Anirvan Banerjee.

Si se adopta un enfoque «manual» para auditar en un entorno Oracle, normalmente se efectúan pruebas limitadas sobre los controles generales TI (como por ejemplo los relativos a la aplicación de las políticas de contraseñas).

Realizar pruebas avanzadas resulta complicado debido a lo limitado de los informes estándar de que dispone Oracle y la complejidad técnica de las aplicaciones. Esta misma dificultad hace que, a veces, las mismas entidades que operan Oracle tengan dificultades para conocer con exactitud la situación de sus controles. Así, obtener una seguridad razonable de auditoría sobre los controles de seguridad puede llevar mucho trabajo de auditoría y requerir mucha colaboración del personal del departamento de sistemas de la entidad auditada.

Para abordar este problema se han desarrollado herramientas automatizadas que ayudan al auditor a revisar entornos Oracle. Sus ventajas son:

- Son rápidas de utilizar y requieren menos tiempo de colaboración del personal de la entidad auditada.
- Proporcionan información más detalla de la que puede ser obtenida manualmente.
- No requieren, necesariamente, la colaboración de expertos en auditoría informática de entorno Oracle.
- Permiten incrementar la cobertura de las pruebas y la calidad de las recomendaciones.

Por mencionar solo dos de ellas: la herramienta desarrollada por Deloitte U.K.: Oracle Application Security Integrity Suite (OASIS) la comercializada por la misma Oracle: Oracle Audit Vault.[89]

Además, también se pueden automatizar muchas pruebas utilizando herramientas estándar como ACL o IDEA.

7.5.5. Microsoft Dynamics NAV

a) Historia y características

La empresa NAVISION (fabricante del software del mismo nombre) fue creada en 1984 en Dinamarca y, tras fusionarse con otra compañía, fue adquirida por Microsoft en 2002.

Tras varios cambios, en 2007 Microsoft cambio definitivamente el nombre al producto denominándolo Microsoft Dynamics NAV.

89. Oracle Audit Vault es un producto que permite proteger y centralizar datos de auditoría para su análisis y reporte posterior, mediante alertas de seguridad por accesos no autorizados, revisión centralizada de configuraciones, etc. Debe adquirirse separadamente.

En noviembre de 2008 Microsoft publicó Dynamics NAV 2009, con una nueva interfaz de usuario

Actualmente Microsoft comercializa cuatro sistemas ERP (Dynamics AX, Dynamics NAV, Dynamics GP y Dynamics SL) con el mismo interfaz de usuario, sistema de reporting y de análisis basado en MS SQL, portal basado en SharePoint e integrados con Microsoft Office.

En la siguiente figura puede verse la arquitectura propuesta por Microsoft en la solución para la Administración local:[90]

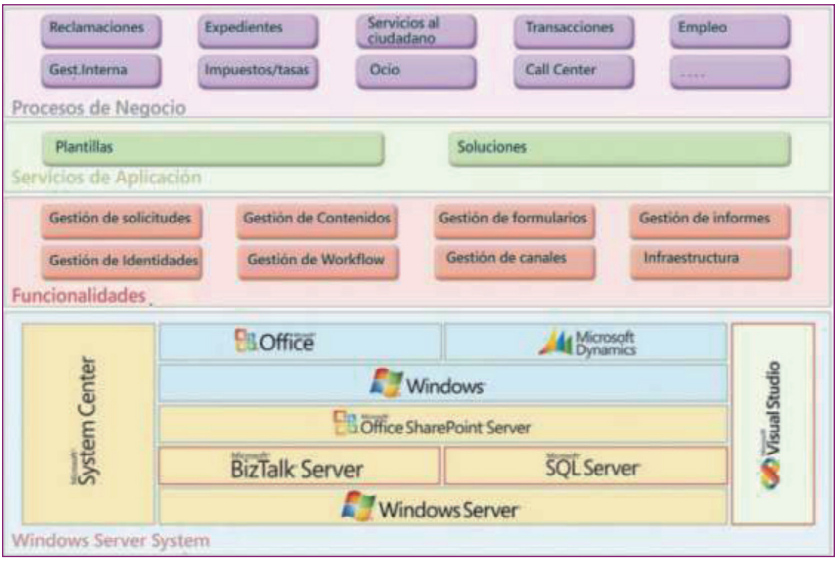


Figura 7.21. Arquitectura Microsoft propuesta para el sector local

Microsoft Dynamics NAV es un ERP que permite y facilita un alto grado de adaptación a las necesidades de los usuarios. Es un ERP compuesto por módulos, que a su vez se subdividen en «gránulos». Este diseño ofrece flexibilidad, permitiendo realizar las personalizaciones que en cada caso se entiendan oportunas y añadir posteriormente funciones según necesidades del usuario.

Microsoft Dynamics NAV es una solución de gestión empresarial integrada que incluye funciones de gestión financiera, fabricación, distribución, gestión de relaciones, de servicios, comercio electrónico y análisis. Está compuesto por las siguientes funcionalidades:

Gestión financiera

Ventas y cobros

90. Fuente: *La Plataforma para Servicios de Administración Local. Desarrollo de la plataforma de Microsoft de servicios al ciudadano*, Microsoft.

Compras y pagos

Gestión de stocks

Producción

Gestión de servicios

Gestión de proyectos

Microsoft Dynamics NAV es un ERP que también tiene una estructura de tres capas:

- La capa de cliente incluye acceso integrado adaptado a funciones a datos y procesos.
- La capa de servidor de Microsoft Dynamics NAV está integrada por completo en Microsoft.NET Framework e incluye servicios web configurables para lograr integraciones más rápidas y económicas con otras aplicaciones.
- En la capa de base de datos Microsoft Dynamics NAV permite la opción de usar una base de datos nativa denominada 'Classic' o Microsoft SQL Server como SGBD. SQL es más adecuada para gestionar grandes bases de datos que la nativa. También se hace referencia a Classic como C/SIDE que significa *Client/Server Integrated Development Environment.*

Gráficamente:

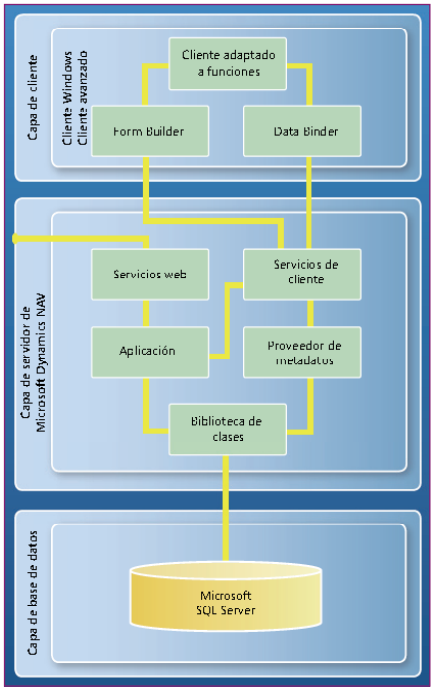


Figura 7.22

b) Cuestiones de auditoría

Al auditar la aplicación Microsoft Dynamics NAV, habitualmente no estamos auditando un programa estándar, sino un programa implantado en una empresa o entidad muy adaptado para gestionar unos procesos de negocio muy concretos relacionados con la actividad del ente y que normalmente abarcan la mayoría de los ámbitos de gestión de la entidad: contabilidad, financiero, personal, compras, ventas, almacén, etc.

Por ello, la comprensión del diseño del proceso de negocio en la entidad concreta y su configuración en la aplicación será fundamental para el desarrollo de la auditoría.

Los pasos para el adecuado desarrollo de la auditoría son, en muy grandes líneas, los siguientes:

- Planificación y definición de la auditoría. En base al análisis previo de la actividad, la organización y los sistemas de información de la entidad, definiremos exactamente sobre que procesos gestionados por Microsoft Dynamics NAV vamos a realizar la auditoría.

  La planificación deberá prever, en su caso, la utilización de CAATs y por lo tanto la obtención de la información necesaria en soporte informático. Estas herramientas nos permitirán verificar la integridad de la información obtenida de las bases de datos sobre las que trabaja Microsoft Dynamics NAV.
- Análisis de riesgos. Evaluaremos el nivel de riesgo de cada uno de los procesos de negocio que vayamos a auditar y los controles generales y de aplicación existentes según la metodología vista en este trabajo.
- La gestión de accesos y perfiles, como siempre, es muy importante. Se hará un análisis de la segregación de funciones en los diferentes procesos definidos sobre la aplicación. Dada la cobertura Microsoft Dynamics NAV a la totalidad del proceso de negocio, es necesario analizar que ningún usuario tenga niveles de autorizaciones sobre transacciones incompatibles desde el punto de vista de la segregación de funciones. En caso de que no exista segregación de funciones y no sea posible implementarlas se recomendarán controles alternativos sobre la actividad de esos usuarios.

  El nivel de autorizaciones sobre transacciones debe respetar el principio de otorgar las mínimas capacidades de autorización necesarias para llevar a cabo las tareas asignadas.

Deberemos verificar la adecuada configuración de los niveles de autorizaciones a los usuarios están adecuadamente asignados en Microsoft Dynamics NAV.

- Comprobación del adecuado funcionamiento de interfaces con aplicaciones externas a Microsoft Dynamics NAV.
- Verificación de las actualizaciones llevadas a cabo.

8

Técnicas y herramientas de auditoría asistida por ordenador (CAAT)

8.1. Introducción

Como se ha expuesto en los capítulos precedentes de este trabajo, en los últimos veinte años, la potencia y capacidad de tratamiento de datos, la capacidad de almacenamiento, y las capacidades de interconexión, han crecido de forma espectacular. Para acompañar al auditor en sus tareas profesionales en este nuevo entorno, los programas informáticos de auditoría también han experimentado una notable evolución.

Hasta los años 1990 las principales plataformas para el tratamiento de la información eran los grandes ordenadores centrales o *mainframes* y las utilidades para el auditor se reducían, básicamente, a las aplicaciones en COBOL o EasyTrieve ejecutadas en esos equipos.

Con la llegada de los miniordenadores (IBM S/36, S/38, AS/400 o DEC VAX), se desarrollaron programas para esos entornos.

La introducción de los ERP dio lugar a nuevos retos para los auditores, como la creación de sistemas y bases de datos complejas y la pérdida de las pistas de auditoría.

Por otra parte, a medida que los ordenadores personales fueron consolidándose como herramientas de gestión e incrementando su capacidad de almacenamiento y de proceso, mucho software de gestión ha ido desplazándose hacia estos equipos. Los auditores también vieron en los ordenadores personales un buen instrumento para desarrollar su trabajo y se desarrollaron herramientas informáticas de auditoría como ACL e IDEA.

Como organización pionera en el ámbito del estudio de la interrelación entre las TIC y la auditoría, el *Instituto Canadiense de Auditores de Cuentas* (CICA), creó en 1987 un programa de extracción y análisis de información, como respuesta a la creciente automatización informática de la contabilidad de las empresas. A partir de esta semilla nacieron dos empresas en Canadá: ACL Services Ltd e IDEA; ambas empresas continúan siendo líderes hoy día en el mercado de herramientas informáticas para la auditoría.

Tanto los productos de ACL como los de IDEA tienen unas funcionalidades muy similares y son herramientas utilizadas por la mayor parte de los auditores públicos y privados de todo el mundo.

Actualmente existe en el mercado un amplio abanico de sistema informáticos integrados con un mayor o menor grado de estandarización, que ofrecen una variedad de funcionalidades y servicios a las administraciones y empresas impensable hace unos pocos años.

Aunque los objetivos generales y el alcance de una fiscalización no cambian al realizarse en un contexto informatizado; no obstante, el auditor al determinar los procedimientos de auditoría más eficaces en este entorno deberá tener en cuenta la posibilidad de aplicar técnicas que utilizan al ordenador como una herramienta de auditoría. Este tipo de herramientas se conocen como técnicas de auditoría asistida por ordenador (Conocidas por el acrónimo inglés de computer assisted audit technics – CAAT).

Las técnicas de auditoría asistida por ordenador son un conjunto de técnicas de auditoría que emplean herramientas informáticas (programas, utilidades…) a lo largo de las distintas fases (planificación, ejecución e informe), o dentro de las distintas funciones (dirección, administración y ejecución) de un auditoría.

Así definidas, estas técnicas son aplicables en todos y cada uno de los distintos tipos de auditoría (financiera, operativa, de legalidad, informática, etc.).

Las CAAT constituyen un medio, sin ser un fin en sí mismas; la utilización de CAAT debe planificarse y emplearse sólo cuando aporten un valor añadido o cuando los procedimientos manuales no puedan aplicarse o sean menos eficientes.

El objetivo final será obtener evidencia informática, tal como queda definido este término en las Normas de Auditoría del Sector Público de la IGAE: Información y datos contenidos en soportes electrónicos, informáticos y telemáticos, así como elementos lógicos, programas y aplicaciones utilizados en los procedimientos de gestión del auditado.

8.2. Tipos de CAAT

Aunque en la introducción solo se ha hecho referencia a dos herramientas concretas (IDEA y ACL), la realidad es que existen muchas herramientas informáticas que ayudan al auditor a desempeñar su trabajo, que podrían clasificarse de la siguiente forma:

1. Programas de gestión de la auditoría (papeles de trabajo electrónicos).

Según una encuesta internacional[91] las principales herramientas informáticas utilizadas para este propósito son

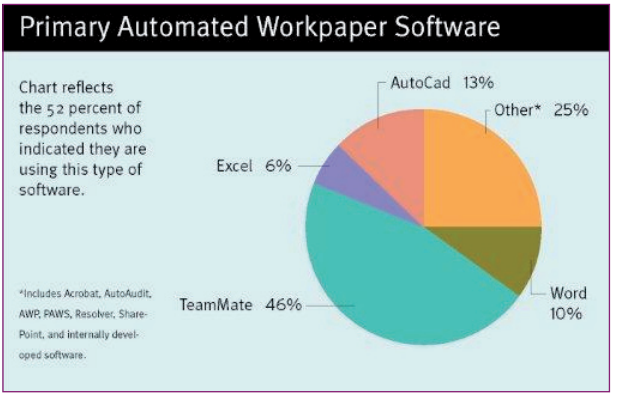


Figura 8.1

2. Programas ofimáticos
   - — Hojas de cálculo.
   - — Procesadores de textos.
   - — Gestores de bases de datos.
   - — Programas de presentaciones.
   - — Programas para el diseño de procesos.
3. Herramientas de análisis y extracción de datos.

   Según la misma encuesta las principales herramientas informáticas utilizadas en el mundo para este propósito son

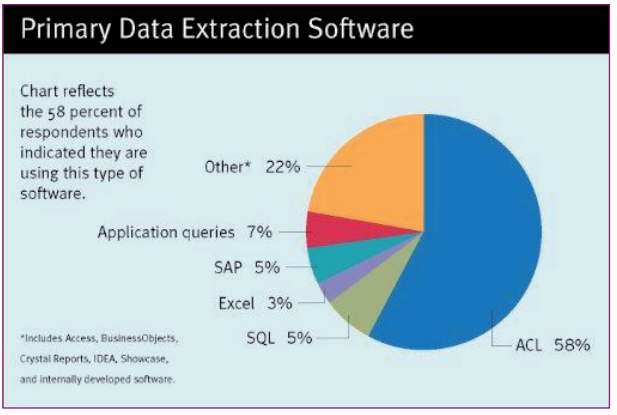


Figura 8.2

91. Fuente: *Software trend spotting* publicado por Neil Baker en la revista *Internal audit* de agosto 2009. Según encuesta a nivel mundial realizada en 2009 por The IIA.

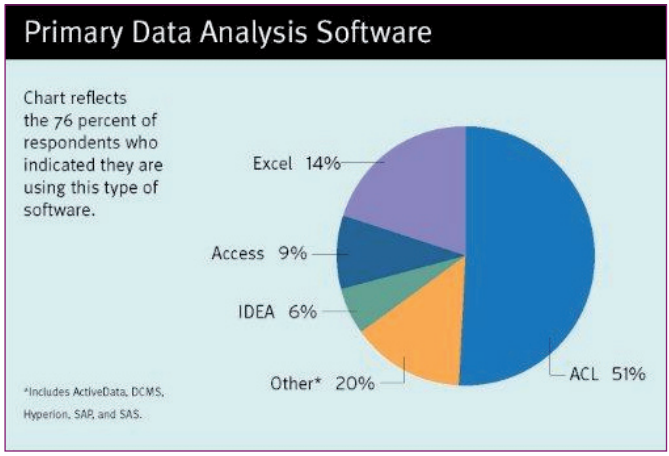


Figura 8.3

4. Módulos de auditoría de los ERP.

   Son las utilidades o módulos de auditoría incluidos de forma estándar o previa adquisición en los principales ERP del mercado. Ya se ha citado en un capítulo anterior de este trabajo a Audit Vault de Oracle y A.I.S de SAP.

   Además fabricantes de software independientes han desarrollado gran número de herramientas de auditoría para los principales ERP.

5. Programación y control de tiempos y trabajos.

   TeamMate Suite tiene un módulo con esta funcionalidad.

6. Herramientas de análisis y gestión de riesgos

   TeamMate Suite también tiene un módulo con esta funcionalidad.

7. Paquetes estadísticos

   Existen numerosos productos estadísticos, entre los más conocidos: SPSS (Statistical Package for the Social Sciences), SAS (Statistical Analysis System) y Statgraphics. ACL e IDEA incluyen sencillos, pero útiles, módulos estadísticos.

En la siguiente figura puede verse la utilidad que para distintos propósitos pueden tener para el auditor los distintos paquetes de software, en este caso los disponibles en el Tribunal de Cuentas Europeo:[92]

92. Según *Guidelines on computer assisted audit tools (CAATS)*, del Tribunal de Cuentas Europeo, 2006.

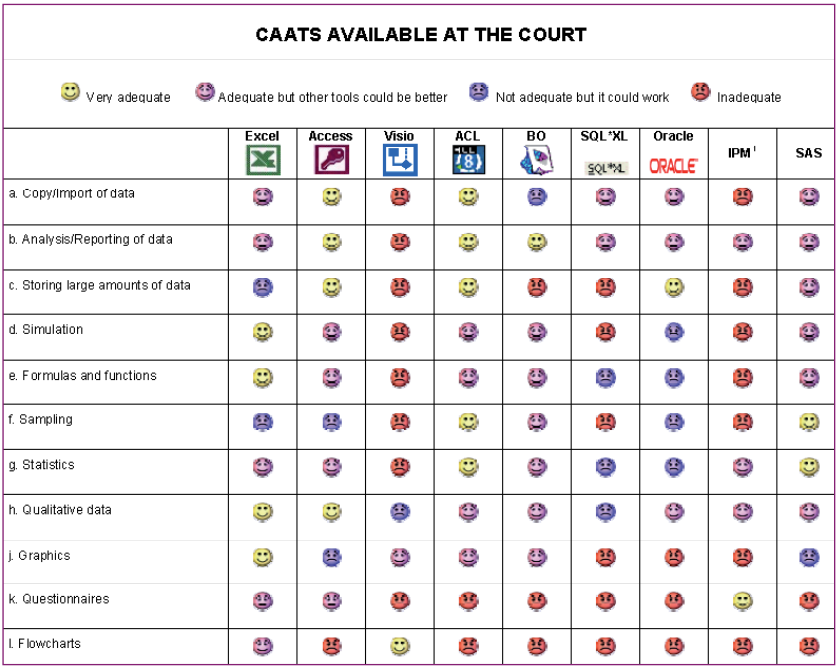


Figura 8.4 Herramientas utilizadas en el TCE

Aunque los auditores utilizarán gran parte de los tipos de herramientas vistas en este apartado, en este trabajo, nos centraremos en el análisis de los programas o Herramientas de Análisis y Extracción de Datos (HAED), ya que son programas creados específicamente para ayudar al auditor a cumplimentar más eficaz y eficientemente sus pruebas de auditoría.

8.3. Herramientas de análisis y extracción de datos

8.3.1. Características principales

Las dos principales herramientas de auditoría existentes en el mercado para el análisis y extracción de datos (HAED) son ACL e IDEA. En este capítulo 8 nos referiremos básicamente a las características y funcionalidades de estas dos herramientas que son muy similares y permiten analizar los datos en casi todos los formatos, de prácticamente todas las plataformas, así como procesar grandes volúmenes de datos.

Para entornos *mainframe* y muy grandes volúmenes de datos (entidades financieras) es muy utilizada la herramienta CA-Easytrieve.

Las HAED son herramientas de apoyo en labores de análisis de información, extrayendo la información de la empresa y generando documentación de los resultados del estudio de la información contable.

Aunque sería casi interminable enumerar todas las funciones de estas herramientas, algunas de sus características principales son:

a) Funciones de extracción

Permiten extraer registros de un archivo mediante algoritmos de extracción. El programa es capaz de generar los algoritmos interactivamente con el usuario, o dejar a éste la labor de confección. Una función adicional permite almacenar algoritmos importantes en un catálogo para su uso posterior. Se genera un nuevo archivo virtualmente con los registros de interés, pero físicamente, lo que realmente se almacena en disco, es la definición lógica y no la información. De esta forma se evita duplicar información.

b) Indexación y clasificación

Son dos formas de reorganizar la información de un archivo, que no estaba en el orden adecuado, utilizando claves de ordenación. La Clasificación genera un archivo equivalente con el orden deseado. La Indexación, menos costosa, genera simplemente un archivo índice de referencias al original.

c) Funciones de análisis

Engloba un conjunto de funciones, utilizadas a menudo, en el análisis de información. Algunas de estas funciones son:

— Resumir campos clave
— Estratificación de ficheros
— Gráficos de barras
— Estadísticas de campos
— Análisis de antigüedad
— Comparación de dos archivos
— Detección de espacios vacíos

d) Funciones de muestreo

Permiten utilizar distintos métodos de muestreo: sistemático, aleatorio, generación de números aleatorios, muestreo de atributos y de unidades monetarias.

e) Funciones de manipulación de campos

Permite modificar la información una vez ésta ha sido importada. Entre otras, tenemos la posibilidad de fusionar archivos,

modificar y eliminar campos, así como introducir campos de control virtuales.

f) Funciones de preparación de informes

Permiten la confección y edición de informes con los resultados del trabajo, que se incorporarán en la documentación de las auditorías.

g) Imprimir/Visualizar ficheros

Permite lo propio con cualquier información o resultado de análisis manejados por el programa.

8.3.4. Usos y aplicaciones de las CAAT

Las CAAT pueden ser usadas para ejecutar diversos procedimientos de auditoría, entre los que se incluyen:

- Verificación de la integridad de la información financiera que se va a analizar. Cuadres libros diarios y mayores con estados financieros aprobados.
- Comprobaciones de detalle en transacciones y saldos (por ejemplo, para comprobar la totalidad o una muestra de las transacciones en un archivo contable).
- Procedimientos de revisión analítica (por ejemplo, para identificar partidas o fluctuaciones inusuales).
- Pruebas de cumplimiento de los controles informáticos generales (por ejemplo, el uso de verificaciones de datos para comprobar los procedimientos de acceso a las bibliotecas de programas).
- Pruebas de cumplimiento de los controles informáticos sobre aplicaciones (por ejemplo, el uso de verificaciones de datos para comprobar el funcionamiento de un procedimiento o prueba previamente programados).
- Detección de valores erróneos.
- Detección de valores extraordinarios.
- Comprobación del registro o del resumen de las operaciones.
- Repetición del tratamiento informatizado (por ejemplo, conversión de divisas, reelaboración de la nómina, etc).
- Comparación de datos de diferentes archivos.
- Estratificación.
- Verificación de cálculos.
- Automatización de las rutinas.

- Identificación de los riesgos excedidos.
- Identificación de los desfases en los gastos.
- Identificación de duplicidades en pagos.
- Identificar tendencias, señalando excepciones y áreas que requieren mayor atención
- Localizar errores y posibles irregularidades, comparando y analizando los archivos según criterios especificados por el auditor.
- Recalcular y verificar saldos.
- Analizar y determinar la antigüedad de cuentas a cobrar, cuentas a pagar y otras transacciones.
- Evitar pérdidas de ingresos, detectando pagos duplicados, secuencias numéricas incompletas en la facturación, servicios no facturados.
- Cuadre entre los documentos contables y los documentos del área de contrataciones.
- Detección del posible fraccionamiento analizando las facturas de un mismo proveedor en un determinado período.
- Detección de las facturas imputadas al ejercicio actual que corresponden a ejercicios anteriores.
- Pagos realizados a cuenta o direcciones distintas de las del proveedor.
- A partir de las bases de datos de documentos contables se elaboran las hojas sumarias de cada área de la auditoría, se recalcula la ejecución de los presupuestos por conceptos o de los balances y cuenta de pérdidas y ganancias.
- Selección en cada área de la muestra de documentos contables a revisar, mediante muestreo estadístico o sistemático.
- En el área de subvenciones se realiza una extracción de los ficheros de los mayores de gastos para obtener las subvenciones concedidas y contabilizadas en el ejercicio fiscalizado a cada beneficiario (obteniendo todos los documentos contables relacionados con los CIFs de los beneficiarios).
- En la revisión de los expedientes de subvenciones se pueden realizar extracciones de todos los documentos contabilizados en los mayores de gastos relacionados con los expedientes seleccionados, cuando se ha dispuesto de la codificación adecuada para realizar la extracción.

– Conversión y análisis de los ficheros de procesos de pagos de la entidad.
– Comprobación de la nómina.
– Aplicación del análisis de Benford a los gastos corrientes en los centros fiscalizados.

8.3.5. Consideraciones sobre el uso de CAAT

Al planificar la auditoría, el auditor debe considerar la combinación más apropiada de técnicas manuales y asistidas por ordenador. Para determinar si es conveniente el uso de CAAT, los factores a considerar son, entre otros:

a) Conocimientos informáticos, pericia y experiencia del auditor

El auditor deberá poseer los suficientes conocimientos para planificar, ejecutar, valorar y utilizar los resultados de las CAAT empleadas en su trabajo. El nivel de conocimientos exigidos depende de la complejidad y naturaleza de las CAAT y del sistema contable de la entidad. De acuerdo con ello, se deberá ser consciente de que el uso de CAAT, en ciertas circunstancias, puede exigir unos conocimientos informáticos y una pericia significativamente mayores que en otras.

b) Disponibilidad de CAAT y de otros medios informáticos

El auditor tendrá en consideración la disponibilidad de CAAT, y de otros medios informáticos. La cooperación del personal de la entidad puede ser requerida para asistir al auditor en actividades tales como cargar o aplicar las CAAT en el sistema informático de la entidad o para suministrar copias de archivos de datos en el formato exigido por el auditor.

c) Impracticabilidad de comprobaciones manuales

Muchos sistemas contables informatizados ejecutan tareas para las que no existe disponible ninguna evidencia visual y, en tales circunstancias, puede ser impracticable para el auditor la realización de comprobaciones manuales y solo pueden aplicarse CAAT.

d) Efectividad y eficiencia

Al obtener y evaluar la evidencia de auditoría, la efectividad y eficiencia de los procedimientos pueden ser mejoradas mediante el uso de CAAT; así, por ejemplo:

— Algunos tipos de transacciones pueden ser verificadas más eficientemente, con un coste similar, utilizando el ordenador para

examinar la totalidad de las mismas o, al menos, un mayor número de transacciones que las seleccionadas por otros medios.

— Al aplicar procedimientos de revisión analítica, los detalles de las transacciones o saldos pueden ser revisados más eficientemente mediante el uso del ordenador que manualmente, logrando más fácilmente información sobre partidas inusuales.

— El uso de las CAAT en los procedimientos sustantivos proporciona evidencia adicional de calidad a los procedimientos de cumplimiento relacionados con ellos.

e) Tiempo

Ciertos registros pueden ser retenidos sólo por períodos cortos de tiempo y pueden no estar disponibles de forma legible para cuando se los necesita. Por ello, el auditor precisará tomar medidas para ordenar la retención de los datos que va a necesitar, o bien para alterar la programación de la parte del trabajo que requiera tales datos.

f) Uso creciente de ERPs

El incremento exponencial del número de las transacciones que se producen en las empresas y entidades, la generación de transacciones automatizadas, la ausencia de documentos de entrada en soporte tradicional de papel o la falta de rastro visible pueden exigir, **exigen**, el uso de CAAT en la aplicación de procedimientos sustantivos y de cumplimiento.

8.3.6. Ventajas e inconvenientes de la utilización de CAAT

a) Ventajas

Las CAAT facilitan la labor del auditor y permiten incrementar la calidad de los trabajos, aportando indudables ventajas en términos de productividad y eficacia. Entre las principales ventajas, puede citarse:

1. La primera es que permiten al auditor extraer datos de grandes bases de datos y analizarlos sin necesitar ayudas externas.
2. La obtención de una evidencia de auditoría de mejor calidad que la obtenida manualmente especialmente en grandes clientes y entorno informáticos complejos, ya que posibilita leer y analizar ficheros y bases de datos completas, en lugar de una muestra, permitiendo analizar todos los datos, reprocesar tareas al 100% y extraer todas las excepciones, en lugar de realizar una proyección de los resultados estadísticos obtenidos de un muestreo.

3. El uso de CAAT incrementa la eficacia y eficiencia del trabajo de auditoría.
4. Permite realizar análisis cualitativos complejos (por ejemplo hacer un análisis de la segregación de funciones implantada en un aplicación SAP, revisando los usuarios autorizados para series de transacciones con incompatibilidades).

b) Inconvenientes

La introducción de CAAT entre las herramientas de los auditores públicos no ha sido todo lo rápido ni extenso que hubiera sido conveniente,[93] circunstancia que podría achacarse a las siguientes razones (comunes tanto para los auditores públicos como privados):

1. La ausencia de una clara relación entre la eficacia y el coste.
2. La complejidad técnica (especialmente los problemas relacionados con el acceso a los datos del ente auditado).
3. La falta de formación y experiencia del auditor (miedo a lo desconocido, comodidad, falta de planificación por parte de los órganos de dirección para organizar las actividades formativas precisas).
4. Preocupación del auditado por la seguridad de los datos solicitados por el auditor.

   Es necesario tener conversaciones previas con el auditado, al nivel adecuado, para garantizarle la confidencialidad y seguridad respecto de los datos analizados. Debe explicarse cuales son los objetivos del trabajo y el procedimiento que se va a seguir. Nunca se debe trabajar con los datos de explotación, siempre con copias.
5. Disponibilidad de HAED adecuadas en el ente auditor.

8.4. Etapas para trabajar con un CAAT[94]

8.4.1. Planificar el proyecto

Ante una prueba de auditoria que contemple la utilización de un volumen importante de datos deberemos plantearnos si la utilización de la herramienta nos va a reportar beneficios en términos de ahorro

93. A juzgar por las presentaciones que se pueden consultar en las páginas web de los tres Foros tecnológicos de los OCEX celebrados hasta la fecha.

94. Puede consultarse también la *IS Auditing Guideline G3 Use of computer-assisted audit techniques (CAATs)* de ISACA.

de tiempo de realización de la prueba, más posibilidades en cuanto a pruebas a realizar o más seguridad en el trabajo realizado, no sólo a corto plazo sino también a largo plazo, en el caso en el que la prueba o el trabajo sea recurrente.

Los CAAT van resultar de utilidad en muchas pruebas de auditoría, sobre todo una vez se ha adquirido experiencia en su utilización.

Algunos especialistas sostienen que los pasos más importantes de un proyecto de análisis de datos preceden al uso de la HAED. Con una planificación cuidadosa, se puede establecer con claridad los objetivos y evitar posibles dificultades técnicas. Esto es cierto en todas las pruebas de auditoría, pero los errores y aciertos en este aspecto destacan más con las HAED.

Al preparar el proyecto de análisis de datos, se deben identificar los objetivos, los requisitos técnicos y los procedimientos analíticos a efectuar.

a) Identificar los objetivos del proyecto

Dependerán de la prueba de auditoría que en la que se esté trabajando.

Debe estar claro el objetivo de la prueba para evaluar las necesidades de información y los criterios para el tratamiento de los datos en CAAT. Hay que redactar enunciados claros y precisos de los objetivos. Cuanto más específico sea el enunciado, con mayor facilidad se podrán detallar los pasos necesarios y lograr el objetivo.

A medida que se articulan las metas específicas, es posible que se descubra que se puede aportar más claridad al proceso.

Se pueden redactar varios objetivos simultáneamente siempre que aseguremos que los enunciados son específicos y no generales.

En los enunciados, se debe identificar el proceso que se auditará y la información que espera encontrar. Por ejemplo (1), un objetivo del proyecto podría ser: «Identificar los proveedores que cobran importes superiores a los acordados en los contratos».

Otro ejemplo (2): Comprobar que la liquidación del presupuesto de gastos es la que resulta de procesar todos los documentos contables tramitados.

Los objetivos también influyen en los requisitos técnicos del proyecto. Si se desea incluir determinada información en el informe final, hay que asegurarse que los campos de datos pertinentes forman parte de los datos que adquiere para el proyecto.

b) Identificar los requisitos técnicos

Una vez redactados claramente los objetivos, se deben definir los pasos técnicos que permitirán lograrlos. Por lo general, la evaluación técnica incluye estas actividades:

Evaluar la factibilidad

Se puede determinar si el tipo de análisis es factible teniendo en cuenta los enunciados de los objetivos, que identifican el tipo de información (la entrada) y el resultado deseado (la salida). En algunos casos es posible que no haya datos suficientes como para lograr los objetivos.

Por ejemplo, para alcanzar el objetivo del ejemplo (2) anterior se necesita una tabla que contenga todos los registros / documentos contables con los campos siguientes:

n.º documento

fecha

tipo de documento contable: A, D, O, K, P, /A, /D, /O….

importe

aplicación económica y funcional

Identificar los archivos de datos necesarios

Identifique los archivos de datos que contienen los campos necesarios.

Por ejemplo, para comparar el precio contratado con un proveedor con el precio facturado, se necesitarán archivos con los precios contractuales y las facturas con los detalles de cada producto.

Es posible que se necesite más de un archivo de datos para obtener todos los campos requeridos.

Se debe determinar el nombre exacto de los archivos que contienen los datos necesarios.

Garantizar la disponibilidad de recursos para los archivos de datos

Se debe estimar lo mejor posible el tamaño aproximado de los datos que se solicitan y hay que considerar el soporte en el que se solicitarán y recibirán los datos y la capacidad del servidor de red o la unidad de disco local. El auditor debe asegurarse de que tiene la capacidad para almacenar y procesar los datos que se solicitan.

c) Identificar los procedimientos analíticos

Una vez determinados los objetivos y los datos fuente necesarios, se debe planificar cómo lograr cada objetivo. Esto significa especificar

los datos de origen, los comandos, las expresiones y las variables que se utilizarán.

Para lograr un objetivo es posible que se necesite más de un paso, de manera que deberá articularse y revisarse un enfoque detallado paso a paso antes de comenzar. Este proceso ayudará a garantizar que no se produzcan eventos imprevistos durante el procesamiento y que se consideren todos los resultados posibles.

Además, ofrece una visión integral que permite identificar los procesos que pueden ejecutarse con mayor eficiencia con otra funcionalidad.

No siempre es factible planificar con total detalle, sobre todo en los primeros años de uso de un CAAT, ya que es un proceso que se va perfeccionando con la experiencia adquirida. Cuando ya se tiene una experiencia sólida es posible planificar con mucha mayor precisión y eficiencia.

8.4.2. Adquirir los datos

Hay que obtener acceso físico y lógico a los datos de origen necesarios, identificando su ubicación y formato. Según el tipo de análisis que se pretenda realizar, es posible que se tenga que depender de terceros para que suministren los datos que se necesitan.

Los datos de origen pueden encontrarse en un mainframe, un servidor de red o en un ordenador personal.

Pueden tener cualquier estructura de registro, ser de diversos tipos y estar almacenados en discos duros, CD u otros dispositivos de almacenamiento.

Es necesario que se planifique el proceso para obtener los datos requeridos. Puede necesitarse la ayuda o el permiso de terceros para acceder a determinados datos, especialmente si se trata de un sistema importante.

a) Pautas para adquirir datos

Independientemente de cómo se obtengan los datos, se pueden seguir las pautas que se indican a continuación:

1. Solicitar los datos como ODBC o como archivo plano

Si bien ODBC representa un método válido para acceder a los datos, los archivos planos secuenciales constituyen otra alternativa muy adecuada. Si los datos están en una base de datos relacional, conviene convertirlos a un archivo plano antes de descargarlos o copiarlos. En esta fase se requerirá la ayuda de un informático de la entidad fiscalizada.

2. Utiliar datos no procesados

IDEA o ACL son compatibles con todos los tipos de datos de mainframe y minicomputadoras, y leen texto EBCDIC y ASCII con la misma facilidad.

3. Solicitar una copia de los datos

Solicitar una copia auténtica, no una de seguridad, del archivo original. La única forma en que puede usar una copia de seguridad consiste en restaurar los datos en un archivo común y luego hacer una copia para usarla con CAAT.

b) Solicitar archivos y diseños

Los archivos y diseños que se necesitan para el proyecto, se deben pedir a la persona adecuada por escrito. La solicitud debe indicar el diseño de archivo solicitado, con al menos la siguiente información:

- Nombre del archivo de datos
- Longitud de registro
- Nombre de campo
- Posición inicial del campo
- Longitud de campo
- Tipo de campo
- Formato de campo
- Descripción del campo

Esta información ayudará a crear la tabla para cada archivo de datos.

Si es un fichero Access o Dbase, ya va incorporada la información sobre formatos.

8.4.3. Acceder a los datos

Se deben agregar los datos al proyecto en forma de tablas, que definen la manera en que se leen los datos de origen.

Para poder trabajar con un archivo de datos nuevo es necesario indicar a la HAED cómo debe leer e interpretar los datos del archivo facilitado por la entidad.

El formato de una tabla describe la estructura y el contenido de los datos de origen, y especifica el lugar en el que se encuentran dichos datos. Describe los datos de cada campo, identifica los campos que desea analizar y explica cómo mostrar e imprimir la información.

Normalmente, con ficheros ACCESS, EXCEL, TEXTO DELIMITADO y DBASE el asistente actúa automáticamente detectando las características del fichero, y no necesitaremos añadir ninguna información al incorporar el fichero.

Si es un fichero de TEXTO sin caracteres de separación de los campos se debe introducir esta información (sobre las características de los campos) a la HAED, para lo cual debe haberse obtenido del suministrador del fichero.

También se puede definir o redefinir las características de los campos ya incorporados a una tabla, manualmente.

8.4.4. Verificar la integridad de los datos

Una de las primeras tareas en el análisis de datos es garantizar que los datos con los que se está trabajando son completos y válidos (fiables).

La verificación es muy importante al trabajar con archivos de datos que no contienen información sobre su propio diseño de registro.

Al solicitar las bases de datos con la información a la entidad auditada, se solicitará al mismo tiempo la siguiente información sobre cada uno de los ficheros que vayan a facilitar: n.º de registros del fichero, totalización de uno de los campos numéricos, denominación y descripción de cada una de los campos y, en su caso (para ficheros de texto no definidos), las longitudes de los campos.

Se pueden usar distintos métodos de prueba, como por ejemplo contar los registros, totalizar los campos y verificar los datos a fin de garantizar que:

- los archivos contienen el número correcto de registros, son correlativos, no hay faltantes ni duplicados.
- los totales numéricos corresponden a los totales de control proporcionados por los propietarios de los datos.
- los campos contienen solo datos válidos.

8.4.5. Analizar los datos

Las etapas anteriores son preparatorias, para obtener los datos a auditar y comprobar que no ha habido errores o fallos en su obtención y que son fiables.

Ahora toca auditarlos utilizando toda la potencia analítica de estas herramientas. Algunos de los usos posibles se han indicado en el apartado 8.4.3.

La lista de funciones posibles que tienen herramientas como ACL o IDEA es casi inagotable.

8.4.6. Generar informes de los resultados y documentar el trabajo

Es la fase de preparación de los resultados para su presentación formal y la elaboración de las conclusiones de la prueba. Al documentar los resultados obtenidos y las conclusiones se incluirá al menos la siguiente información:

- Fichero base utilizado
- Tabla de ACL
- Script o instrucciones utilizadas
- Resultado obtenido
- Conclusión de la prueba.

No existe una normativa específica que regule como documentar el trabajo realizado con los CAAT. Los criterios que regulen su documentación en el trabajo de auditoría deben ser los de carácter general, adaptados a las circunstancias de su utilización.

Por tanto es imprescindible documentar adecuadamente los aspectos señalados en el apartado anterior.

El Manual de fiscalización (sección 230) de la Sindicatura de Cuentas de la Comunitat Valenciana, Documentación de la auditoria: Apartado 12, sobre evidencia informática señala:

Cuando se emplee evidencia informática, o se utilicen técnicas o herramientas de auditoría asistida por ordenador los documentos mediante ellas generados se integrarán en los papeles de trabajo, así como la descripción manual o automatizada, de los procesos y tratamientos efectuados para llegar a los resultados finales partiendo de la evidencia primaria.

8.5. Herramientas de análisis digital

8.5.1. La Ley de Benford

La Ley de Benford o Análisis de Frecuencia Digital es una técnica de análisis utilizada para detectar configuraciones anómalas de los datos en agrupaciones de datos que cumplen determinados criterios.

Si tenemos un conjunto de datos numéricos, financieros o de otro tipo, cuyas características permiten deducir que cumplen los parámetros de la Ley de Benford, al aplicar este análisis sobre estos datos, obtendremos como resultado aquel conjunto de datos que no encajan en la composición típica de esos datos.

La extracción de estos datos «atípicos», su análisis y el análisis de su documentación soporte nos permitirá concluir si se trata de datos correspondientes a anomalías o irregularidades o bien se apartan de la tipicidad por motivos justificados.

Esta Ley sostiene que los números correspondientes a medidas de fenómenos o sucesos naturales del mismo tipo, relacionados entre ellos, tienen mayor probabilidad de empezar por el dígito 1 que por el 2, por el 2 mayor probabilidad que por el 3, y así sucesivamente.

La Ley se basa en la observación del comportamiento de magnitudes mesurables en la naturaleza, realizada inicialmente por Simon Newcomb, matemático que en 1881 observó que los libros de logaritmos que utilizaban para sus cálculos estaban más desgastados en las primeras páginas que en las últimas.

A partir de esta observación dedujo que la frecuencia del dígito «1» como primer dígito de cualquier magnitud mesurable de un objeto de la naturaleza era muy superior a las frecuencias de los otros dígitos «2», «3», … Newcomb publicó esta observación en el American Journal of Mathematics, pero no aportó verificación empírica de la regla.

Más tarde, un físico de la General Electric Company, Frank Benford, sin tener conocimiento de las observaciones de Newcomb, realizó la misma observación sobre los libros de logaritmos, obteniendo la misma conclusión.

Benford realizó verificaciones sobre colecciones de datos (longitudes de ríos, población en regiones, números de calles de direcciones, etc.) para validar sus observaciones y en 1938 cuantificó las frecuencias de los primeros dígitos.

Obtuvo las siguientes probabilidades de ocurrencia para los nueve primeros dígitos en estos tipos de conjuntos de datos:

Primer dígito	Frecuencia
1	30,10%
2	17,61%
3	12,49%
4	9,69%
5	7,92%
6	6,69%
7	5,80%
8	5,12%
9	4,58%

Benford obtuvo una ecuación matemática para el cálculo de la probabilidad de que el primer dígito de una magnitud sea un dígito determinado.

Esta propiedad, con distintas probabilidades, se da también para la frecuencia de aparición en este tipo de conjuntos de datos de magnitudes que empiecen por dos o tres dígitos concretos.

No obstante, para poder aplicar correctamente este análisis, los conjuntos de datos deben cumplir los siguientes requisitos:[95]

- Los datos deben ser numéricos.
- Estos datos deben estar relacionados de alguna forma entre ellos y pertenecer al mismo fenómeno. Debe existir alguna causa subyacente que motive la aparición de estas magnitudes (un fenómeno o suceso).
- Las magnitudes no deben estar restringidas a un determinado rango de máximos o mínimos.
- Las magnitudes deben crearse o suceder de forma natural y no deben ser inventadas o asignadas (n.º de teléfono o números identificativos).
- Deben ser números de cuatro o más dígitos. No obstante, si son de menos dígitos se puede utilizar el análisis sobre los dos primeros.
- No deben ser números aleatorios.
- Debe ser un conjunto de datos elevado, en general, superior a 1.000 elementos.
- Debe haber mayor número de valores pequeños que grandes y con un elevado coeficiente de apertura (el valor mayor dividido por el menor debe dar un cantidad superior a 100)

8.5.2. Aplicaciones prácticas

La aplicación del análisis de Benford para la detección de fraudes o irregularidades se inició en 1994 por Mark Nigrini, que lo aplicó a conjuntos de datos de deducciones fiscales.

¿En qué casos puede servir el análisis de frecuencia digital o Ley de Benford en auditoría?

a) Puede ser útil cuando se trabaja con datos financieros para detectar datos manipulados o inventados ya que este tipo de datos, en series que sí cumplen la ley de Benford, normal-

95. *El análisis de frecuencia digital como instrumento analítico en control financiero*, Pablo Lanza, Cuenta con IGAE, n.º 9, 2004.

mente no la cumplirán y, por tanto, se podrán aislar como incumplimientos de la Ley.

b) También en series de datos financieros, por ejemplo facturas justificantes de gastos, en los casos en que determinados valores de esos gastos se repiten anómalamente respecto a la Ley de Benford, bien por condicionantes de las normas o bien para eludir determinados límites impuestos por las normas.

   Por ejemplo para detectar fraccionamientos de contratos o facturas falsas.

   Podremos extraer estos justificantes y verificar si el comportamiento anómalo es justificado y se ajusta a las normas de gestión y a los principios contables.

c) En general, nos sirve para detectar en un conjunto de datos aquéllos que aparecen en una proporción que no es probable de acuerdo con la Ley de Benford.

Los motivos para que se aparten de las probabilidades esperadas pueden estar justificados (criterios de gestión documentados, actividades típicas y repetitivas, …) o no justificados (datos inventados, prácticas de gestión no reguladas, irregularidades…).

8.5.3. Pruebas de auditoría[96]

El análisis de frecuencia digital se puede realizar usando CAAT que tienen preconfigurado este tipo de análisis entre sus opciones (tanto ACL como IDEA ofrecen esta opción).

El análisis de frecuencia digital sobre un conjunto de datos puede hacerse sobre el primer dígito, los dos primeros o los tres primeros. En la mayor parte de los análisis lo más fructífero resulta hacerlo sobre los dos primeros dígitos.

Una vez verificado que el conjunto de datos puede ser candidato a ser tratado mediante análisis de frecuencia digital y efectuada la fase de planificación del uso de las CAAT, los pasos que se siguen son:

a) Obtención de la información en soporte informático accesible, información sobre su diseño y datos de comprobación.

b) Acceder a los datos con ACL/IDEA

c) Verificación de la integridad

96. En las páginas web de los tres Foros tecnológicos de los OCEX celebrados hasta la fecha se pueden consultar numerosos casos prácticos sobre la utilización de ACL e IDEA, incluyendo la aplicación de la Ley Bendford.

d) Realizar el análisis de Benford y detectar los datos anómalos

f) Documentar el trabajo

A través de las opciones se puede indicar en el papel de trabajo: Fecha del trabajo, tablas utilizadas en el análisis, comandos utilizados para la extracción de datos y fichero de destino del resultado del trabajo, de forma que el que realiza la revisión del trabajo puede ver detalladamente todos los pasos y, en su caso, reproducir la prueba.

g) Solicitar justificación a los auditados sobre los datos anómalos: facturas, resoluciones, expedientes de subvención o de contratación,…

La tabla que hemos obtenido de datos anómalos la imprimiremos o la exportaremos a un fichero Excel, Access y solicitaremos los justificantes de los datos que consideramos que no son normales y puedan contener incidencias.

i) Concluir sobre si las anomalías respecto a la Ley de Benford constituyen o no anomalías contables, legales o de gestión y si estas son relevantes para la auditoría.

Anexos

Anexo 1. Modelo de cuestionario inicial

Instrucciones para cumplimentar el cuestionario

La finalidad del cuestionario es de disponer del mayor nivel de información y documentación posible para realizar una planificación preliminar eficiente.

Para cumplimentar el cuestionario no es necesario que la entidad genere documentación adicional a la ya disponible. La idea es disponer de la documentación existente en la entidad en el momento de inicio del trabajo de campo, con el fin de optimizar el tiempo invertido por ambas partes.

El trabajo de campo se desarrollará principalmente mediante entrevistas de las que podrán surgir necesidades adicionales de información.

En el caso de que exista documentación descriptiva de los procedimientos, se adjuntarán al cuestionario.

No se debe adjuntar aquella información que la entidad considere de carácter confidencial, bastará inicarlo en el cuestionario.

Este es un cuestionario inicial. A lo largo de la fiscalización se irá solicitando información y documentación adicional.

Toda la información obtenida a partir de este cuestionario o en el curso de la fiscalización será tratada de forma confidencial de acuerdo con las directivas de seguridad de la información aprobadas por *el órgano auditor*.

Para cualquier duda, no dude en ponerse en contacto con personal del equipo de fiscalización.

Cuestionario cumplimentado por:

Nombre: _____

Cargo: _____

Entidad: _____

Fecha: _____

1. Inventario de aplicaciones

Para cada uno de los siguientes ciclos de negocio, identifique la aplicación/es que los soportan:

- Contabilidad
- Ingresos
- Tributos
- Concesión subvenciones
- Compras
- Existencias
- Tesorería
- Recaudación
- RRHH
- Activos Fijos
- Gestión de proyectos
- Contratación

Alguna de las anteriores actividades es realizada por alguna organización externa (OE) a su entidad y con una infraestructura tecnológica propia? ¿Cuál? Para cada una de ellas, identifique:

- Nombre y ubicación de la OE
- Descripción del servicio externalizado
- Contrato con la organización externa. Alcance del mismo.
- ¿Cuánto tiempo se lleva trabajando con esta OE?
- Informes de control recibidos de la OE (contenido, periodicidad, acciones derivadas de los mismos, valoración general del grado de satisfacción del cliente, problemas significativos durante el servicio prestado, etc.)
- Informes de los auditores de la OE
- Accesos remotos / conexiones que se mantienen entre dicha organización y su entidad

Para cada una de las aplicaciones identificadas, describa el entorno tecnológico que la soporta:

- Departamento responsable de la aplicación (usuario principal).
  - Usuario Responsable
  - Jefe de Proyecto de Desarrollo
- Infraestructura tecnológica que soporta la aplicación
  - Servidor/es

- Software de Aplicación
- Sistema Operativo
- SGBD

— Principales flujos de información que mantiene la aplicación
  - Entre los usuarios y la aplicación
  - Con otras aplicaciones dentro de la entidad
  - Con entidades fuera de la entidad (otros organismos, proveedores, clientes, etc.)

2. Organización y personal del entorno del Proceso Informático

Describa la estructura del área de TI de la entidad. Para cada una de las áreas relevantes, identifique el número de personas y el nombre y cargo del personal clave:

Departamento/ U. Negocio	# Personas	Nombre y cargo personal clave

Indique el número de miembros externos que componen cada una de las áreas anteriormente identificadas.

Describa brevemente, las principales funciones asignadas a cada una de las áreas identificadas.

¿Existe alguna actividad relacionada con la gestión de los SSII (desarrollo, administración de sistemas, plan de recuperación de desastres, etc.) realizada por alguna organización externa a su entidad? Identifique actividad y proveedor.

¿Se han establecidos unos niveles de servicios mínimos a cumplir por los proveedores de Outsourcing (externalización de servicios informáticos)?

Incluye el acuerdo de externalización mecanismos de control sobre el servicio prestado:

— Procedimientos de control (parámetros de calidad del servicio, acuerdos de nivel de servicio establecidos, procedimientos de seguimiento, etc.).

— Derecho para realizar auditorías.

— Certificación SAS70.

Documentación necesaria:

— Organigrama general de la entidad (incluyendo el área de tecnología)

— Organigrama del área de tecnología

— Documento de funciones y responsabilidades de cada una de las subáreas de tecnología

— Contrato con proveedores de outsourcing

— Informes de calidad de servicio. ¿Se han definido unos parámetros que permitan cuantificar el grado de cumplimiento de los niveles de servicio establecidos?

3. Estrategia y planificación de las fuentes de información

¿Dispone la entidad de un plan estratégico de los sistemas de información?

¿Dispone la entidad de un presupuesto anual de inversión en materia tecnológica?

Describa brevemente, los principales proyectos tecnológicos acometidos durante el úlitimo ejercicio y enumere los principales proyectos previstos para el próximo ejercicio.

Documentación necesaria:

— Copia del Plan Estratégico de Sistemas de Información

4. Planificación continuada del negocio

¿Dispone la entidad de un Plan de Recuperación de Desastres?

Describa brevemente la estrategia de recuperación de los SSII implantada en la entidad:

— Identificación de los sistemas críticos.

— Arquitecturas de Alta Disponibilidad.

— Acuerdos de Reposición

— Ubicaciones alternativas de procesamiento

— Generación de Copias de Respaldo

  – Alcance de las copias

  – Periodicidad de ejecución

  – Tipo de copia (total/incremental)

  – Herramienta/s empleada/s para la generación de las copias de respaldo

- Lugar de almacenamiento
- Política de Archivo

¿Se realizan pruebas periódicas del Plan? ¿Con qué frecuencia?

¿Al margen del Plan de Recuperación ante Desastre, dispone la entidad de un Plan de Continuidad de Negocio?

Documentación necesaria:

— Copia del Plan de Recuperación de Desastres.

— Copia del Plan de Continuidad de Negocio.

— Copia de los resultados de las úlitimas pruebas del Plan.

5. Operación de los Sistemas de Información (Mantenimiento)

Describa brevemente los principales procedimientos de las operaciones de los SSII:

— Planificación de tareas
  - Describa brevemente los principales procesos que se ejecutan de manera planificada
  - Describa la herramienta de planificación empleada
  - Identifique al personal encargado de planificar los trabajos y de monitorizar su ejecución

— Administración de sistemas
  - Describa los procedimientos gestión de la capacidad de los servidores
  - ¿Dispone de procedimientos formalizados de instalación de servidores/productos?
    - ¿Dispone de guías de configuración segura del sistema operativo?
    - ¿Existe un procedimiento de actualización del sistema operativo?
  - Identifique al personal encargado de planificar los trabajos y de monitorizar su ejecución

— Administración de usuarios. Para cada uno de las aplicaciones identificadas, describa el procedimiento de gestión de usuarios:
  - Responsable de administración de usuarios (departamento usuario vs sistemas).
  - Procedimiento de gestión de peticiones (alta/baja/modificación).

- Perfiles definidos dentro de cada aplicación y permisos asociados.
- Procedimiento de asignación de usuarios a perfiles.
- Procedimiento de revisión de usuarios y perfiles.

— Pases a producción. Para cada una de las aplicaciones identificadas, describa el procedimiento de pase a producción de cada cambio/actualización:
- Herramienta de gestión de versiones empleada.
- Procedimiento de solicitud y autorización de pases a producción.
- Herramienta de automatización del pase a producción.

Documentación necesaria:

– Copia de los manuales de procedimientos relacionados con la operación de los SSII.

6. Seguridad de la información

Describa brevemente la naturaleza y el alcance de las políticas y procedimientos para la seguridad de la información.

¿Se dispone de un programa para que los usuarios conozcan las políticas de seguridad respecto a la información, procedimientos y el uso?

Documentación necesaria:

— Copia del Documento de Seguridad Reglamento de medidas de seguridad (RMS)- Ley Orgánica de Protección de Datos (LOPD).

— Copia de los procedimientos relacionados con la seguridad de la información, tales como:
- Procedimientos de Gestión de Usuarios.
- Procedimientos de Configuración Segura.
- Gestión de Vulnerabilidades.
- Procedimiento de Gestión de Copias de Seguridad.
- Procedimiento de Gestión de Incidencias.

7. Seguridad lógica

Identificación

— ¿Existe un estándar para la construcción de los identificadores de usuario en los sistemas de información?

— Describa, para cada una de las aplicaciones identificadas, el estándar de nomenclatura definido.
— ¿Se permite, en algún caso, la utilización de cuentas de usuario genéricas por parte de los usuarios finales?

Autenticación

— Describa las técnicas que se utilizan para verificar la autenticidad de la identidad de los usuarios que intentan acceder al sistema. A dos niveles:
  – Del sistema operativo (de red y de los servidores).
  – A nivel de aplicación (para cada una de las aplicaciones identificadas).
— En el caso de que el mecanismo de autenticación se base en usuario y contraseña, describa:
  – Características de las contraseñas (longitud mínima, complejidad, vigencia máxima, vigencia mínima, histórico de contraseñas, posibilidad de cambio antes de que caduquen, bloqueo de cuenta por número de intentos fallidos de acceso, etc.)
  – Procedimiento de asignación, distribución y almacenamiento de contraseñas (quién las entrega, método de asignación, canal definido para el envío, acuse de recibo en la recepción de las contraseñas)

Documentación necesaria:

— Pantallazos de la configuración de la política de autenticación en cada uno de los entornos principales.
— Listados de usuarios para cada uno de los entornos de autenticación definidos.

8. Protección frente a Software Malicioso

— Describa las soluciones de antivirus implantadas en la entidad.
— Describa los principales mecanismos de gestión:
  – Mecanismos de actualización
  – Periodicidad de actualización
    ▪ De la BBDD de Firmas
    ▪ De los puestos cliente

— Principales funcionalidades instaladas
  – Opción de Firewall personal
  – Escaneo bajo demanda.
  – Etc.
— Prevención de equipos sin software de antivirus instalado

9. Mapa de Comunicaciones

Describa brevemente, o facilite documento descriptivo sobre el mapa de comunicaciones que soporta los flujos de información de su entidad. Contemple, al menos, los siguientes aspectos:

— Redes de servidores

  Identifique las redes de servidores de producción y los procedimientos de segmentación:

  ▪ Respecto a las redes de usuarios.
  ▪ Respecto a los entornos de prueba.

— Redes de usuarios (entorno LAN)
  – Identifique las principales sedes desde las que se conectan lo usuarios (edificios centrales, oficinas, accesos remotos, etc.).
  – ¿Se aplican restricciones en el acceso a la red de usuarios: bocas de los swithces deshabilitadas por defecto, filtrado por MAC's, etc.).
  – ¿Existen redes WLAN?
— Redes WAN
  – Describa las principales conexiones entre los diferentes centros de trabajo de su entidad.
  – Describa la solución empleada para las conexiones WAN:
    ▪ Protocolo
    ▪ Proveedor
    ▪ Caudales
    ▪ Mecanismos de respaldo
  – ¿Se aplican restricciones de conexión en el entorno WAN?
— Conexiones con terceros. Identifique las conexiones con terceros que se establecen desde sus SSII. Considere, entre otros:
  – Conexiones con organismos públicos.

- Conexiones con proveedores de servicios TI.
- Conexiones con proveedores.
- Conexiones con clientes.

Para cada uno de ellos, describa finalidad de la conexión y protocolo de comunicación empleado.

— Accesos remotos. Identifique los diferentes mecanismos de acceso remoto establecidos actualmente en su entidad:
  - Por tipología de usuario (administradores TI, proveedores, usuarios en movilidad, oficinas remotas, etc.).
  - Por protocolo de conexión (RAS, VPN). Identifique la solución empleada en cada caso.
  - ¿Se aplican restricciones de acceso en las conexiones remotas?
  - Describa los mecanismos de autenticación de usuarios en cada caso y los procedimientos de gestión de usuarios.

— Red de navegación.
  - Describa la solución empleada para facilitar acceso a Internet a los usuarios: proxy, ADSL's, modems, etc.
  - Identifique todos las salidas a Internet que proporciona la entidad a sus usuarios.
  - Se otorga acceso a Internet a todos los usuarios de la entidad.
  - Se aplican restricciones en el acceso a Internet

— Red de servidores internet.
  - ¿Qué tipo de servicios están disponibles en la página del cliente?
    - Descripción a grandes rasgos de la página Web
    - Funcionalidades (sólo publicación de contenidos o el usuario tiene posibilidad de interactuar)
    - Se tiene un área restringida para los empleados? Mecanismo de identificación y autenticación?
    - Se tiene un área restringida para los clientes? Mecanismo de identificación y autenticación?
    - Localización del servidor Web. Diseño, mantenimiento y soporte de la página Web (interno / externo)
  - Descripción de la arquitectura Internet:
    - WEB: Apache (UNIX), IIS (MS).

- Aplicación: IAS (Oracle), Weblogic (BEA), Websphere (IBM).
- BBDD: Oracle, SQL Server, Sybase, DB2.

— Arquitectura de Alta Disponibilidad. Para cada uno de los entornos anteriores, identifique las soluciones de alta disponibilidad implantados:
  – De conexión.
  – De equipos.
— Arquitectura de Seguridad. Describa la infraestructura de seguridad desplegada en sus redes de comunicaciones:
  – Firewalls: solución empleada, ubicación, alta disponibilidad.
  – IDS/IPS
  – ACL's en los routers
  – VLAN's en los siwtches.

Documentación necesaria:

— Mapa de Red
— Procedimientos de operación elementos de comunicaciones

10. Seguridad física

Enumera los Centros de Procesos de Datos en los que se ubican los servidores de la entidad. Para cada uno de ellos, describa:

Inventario de Servidores

— Listado no exhaustivo de servidores ubicados en cada CPD

Controles de acceso

— Ubicación
— Personal autorizado a acceder al mismo
— Método de control de acceso
— Procedimiento de acceso del personal externo (mantenimiento, limpieza, etc.)?
— Enumeración de grupos internos y externos autorizados al acceso físico al entorno de proceso informático.

Controles ambientales

— Detección y extinción de incendios
— Controles de temperatura

— Controles de humedad
— Sistemas alternativos de suministro de energía
— SAI
— Falso suelo / Falso techo

Documentación necesaria:

— Será necesario realizar una visita a los CPD's de la entidad

11. Implantación y mantenimiento de los sistemas de la aplicación

Clasifique cada una de las aplicaciones identificadas que soportan los principales procesos de negocio, según la siguiente clasificación:

— Software propio desarrollado por la organización
— Software comprado con pequeñas o ninguna personalización
— Software comprado con personalización significativa
— Software propiedad de una empresa de Outsourcing

¿Disponen de acceso a una copia actualizada del código fuente de todas las aplicaciones significativas? ¿De cuáles no?

¿Se dispone de una metodología para el desarrollo y mantenimiento de las aplicaciones? Si no es así, describa las principales tareas que se realizan en cada una de las fases típicas del Ciclo de Vida de Desarrollo:

— Análisis de requerimientos: cómo se reciben las peticiones de los usuarios, quién las evalúa, cómo se aprueban, etc.
— Análisis funcional.
— Desarrollo.
  – Herramienta de gestión de versiones empleada
  – ¿Existe un entorno de desarrollo separado del entorno de producción?
— Prueba
  – ¿Existe entorno de pruebas?
  – Tipos de pruebas a considerar:
    - Unitaria.
    - Integración.
    - Certificación.

— Pase a producción
  – ¿Se producen accesos de los analistas/desarrolladores a producción?
  – ¿Quién tiene acceso para actualizar las bibliotecas de código fuente de los programas?
  – ¿Quién tiene acceso para actualizar las bibliotecas ejecutables de los programas?
  – Herramienta de automatización de pase a producción
— Mantenimiento
  – Gestión de incidencias

Documentación necesaria:

— Copia de la Metodología de Desarrollo de la Entidad

12. Implantación y mantenimiento de las bases de datos

Enumere las diferentes soluciones de software gestor de bases de datos (SGBD) que utilizan las aplicaciones informáticas dentro del entorno de procesamiento e indique las aplicaciones correspondientes:

SGBD	Aplicaciones

Describa brevemente las principales funciones realizadas en cuanto a la gestión/administración de las BBDD de su entidad y el responsable de llevarlas a cabo.

¿Se dispone de un diccionario de datos?

13. Soporte del software

Describa brevemente los procedimientos para adquirir, poner en marcha y mantener el software de sistemas, incluyendo las funciones y responsabilidades de las personas o grupos involucrados en este proceso. Considerar los siguientes tipos de procedimientos si aplican:

— Realización de pruebas del nuevo software de sistemas o modificaciones del existente.

— Evaluación del efecto del nuevo software de sistemas o modificaciones sobre el procesamiento de aplicaciones informáticas.
— Aprobación de la puesta en marcha de nuevo software y/o modificaciones del existente.
— Implantación de los programas nuevos o modificados desde la fase de desarrollo/pruebas a producción.
— Validación de la integridad y precisión de procesamiento del software nuevo o modificado.

14. Soporte del hardware

Para el ordenador/servidor central y otros equipos significativos (no sólo los que soportan las aplicaciones identificadas) dentro del entorno de proceso informático, facilite la siguiente información:

Fabricante y modelo	S.O. y versión	Ubicación	Año

Describa el ciclo de vida estimado de los equipos (servidores, PC's, comunicaciones):

— Plan de reposición de equipos.
— Política de reuso de equipos.
— Procedimientos para la destrucción de equipos e implicaciones en cuanto a seguridad.

¿Se encuentran todos los equipos dentro de acuerdos de mantenimiento con los fabricantes? ¿Se encuentra algún equipo fuera del periodo de soporte del fabricante?

Documentación adicional a solicitar:

— Informes realizados por los auditores internos relacionado con los sistemas informáticos.
— Informes realizados por consultores/auditores externos trabajo relacionado con las aplicaciones informáticas.

Anexo 2. Check list para la revisión física del Centro de Procesos de Datos

REQUERIMIENTO	SÍ	NO	COMENTARIOS
Detección de Incendios			
Detectores de Temperatura			
Detectores de Humo			
Detectores por debajo de Suelo Técnico			
Sistemas de Alarma (La alarma debería estar conectada a un panel fuera del área protegida para ayudar a localizar el origen de la alarma.)			
Sistema de Extinción de Incendios • CO2 • Halon • FM200 • H20 • Dry pipe with H20			
Las paredes de la Sala de Servidores se extienden hasta el techo real			
Aire Acondicionado			
Aire acondicionado adecuado			
Si hay ventanas, estás securizadas y reforzadas?			
Ventanas ciegas para reducir la visión y el calor			
Agua			
Tanques de Agua en la proximidad			
Tuberías por encima de la Sala			
Baños en la proximidad			
Cubiertas Antigua disponibles			
Sala de Servidores en Planta Baja			
Si es así, riesgos de inundaciones (terreno hundido, río cercano, incidentes en el pasado)			

Infraestructura de Red			
El acceso al armario de cableado es seguro?			
Es el armario de cableado fácilmente identificable?			
Está el cableado y el equipamiento organizado y etiquetado?			
El equipo se encuentra convenientemente mantenido?			
Suministro Eléctrico			
SAI es utilizado en caso de corte o interrupciones del suministro eléctrico			
Duración del SAI			
SAI sometido a pruebas periódicas?			
Grupo electrógeno sometido a pruebas periódicas y con depósito lleno			
Equipamiento debidamente conectado a tierra			
General			
Acceso controlado a la Sala de Servidores • Acceso mediante tarjeta • Cámara de Seguridad • Guardia de Seguridad • PBX Securizada?			
Seguridad del entorno de la Sala de Servidores correcta?			

Anexo 3. Bibliografía

AENOR:

- Norma UNE_ISO/IEC 17799, Tecnología de la Información, Código de buenas prácticas para la Gestión de la Seguridad de la Información, 2002.
- Norma UNE 71502, Especificaciones para los Sistemas de Gestión de la Seguridad de la Información, 2004

AMR RESEARCH: *The Global enterprise Market Sizing Report 2008-2013*. Boston, 2009.

Bae, Benjamin y Ashcroft, Paul: *Implementation of ERP Systems: accounting and auditing implications*, Information Systems Control Journal volumen 5, Rolling Meadows, 2004.

Baker, Neil: *Software Trend Spotting*. Internal Audit, Altamonte Springs, 2009.

Bernal Montañés, Rafael y Contell Simón, Óscar: *Auditoría de los sistemas de información*. Universidad Politécnica de Valencia, Valencia, 1996.

Boukachabine, Abdelrani: *Oracle Database: The Database of Choice for Deploying SAP Solutions*, Oracle, Redwood Shores, 2009.

Butera, Ann: *Process mapping – The updated form of flowcharting*. The Whole Person Project Inc., Elmont, 2003.

Cerillo, Virginia y Michael: *Impact of SAS n.º 94 on Computer Audit Techniques*. Information Systems Control Journal, volumen 1, 2003.

Calleja Ruiz, Ignacio: *Fiscalización en un entorno de @-Administración*, presentación en el VII Seminario «La E-Administración en la función de control - La fiscalización electrónica, y la evaluación de políticas públicas», que se celebró los días 16 y 17 de julio de 2009, en Maspalomas, organizado por la Audiencia de Cuentas de Canarias.

CASTER, Paul y VERARDO, Dino: *Technology Changes the Form and Competence of Audit Evidence*. The CPA Journal, 2007

CENTER FOR AUDIT QUALITY: *Performing an audit of internal control in an integrated audit – Lessons learned*. Center for Audit Quality, Washington, 2009.

CODERRRE, David G.: *CAATTs and other BEASTs for Auditors*: Ekaros Analytical Inc., Vancouver, 2005.

COMPAGNIE NATIONALE DES COMMISSAIRES AUX COMPTES: *Prise en compte de l'environnement informatique et incidence sur la démarche d'audit*, Collection guide d'application, Paris, 2003.

CONSEJO SUPERIOR DE ADMINISTRACIÓN ELECTRÓNICA: *Informe IRIA 2008 Las Tecnologías de la Información y las Comunicaciones en las Administraciones Públicas*. Ministerio de administraciones Públicas, Madrid, 2008.

CRASWELL, Lesa y FOX, Amy: *Assuring SAP*, intoIT 27, Londres, 2008.

DREW, Will y BANERJEE, Anirvan: *Oracle Applications: The benefits of using automated audit tools*, intoIT n.º 28, Londres, 2008.

ÉMOND, Caroline: *Electronic Audit Evidence*. Research Report, The Canadian Institute of Chartered Accountants, Toronto, 2003.

EUROSAI: *La Administración electrónica desde una perspectiva de auditoría, Informe del Grupo de Trabajo de sobre TI*, Madrid, 2005.

FUNDACIÓN ORANGE:

- *Análisis del uso de los procedimientos básicos de eAdministración en las CCAA por parte de los ciudadanos y las empresas*, Madrid, 2009.
- *Estudio Comparativo 2009 de los Servicios Públicos on-line en las Comunidades Autónomas Españolas*, Madrid, 2009.
- Inf*orme anual sobre el desarrollo de la sociedad de la información en España (Informe eEspaña 2009)*. Madrid, 2009

HUISSOUD, Michel: *Comment intégrer l'audit informatique?*. L'Expert-comptable suisse, n.º 9, Zurich, 1994.

INTERNATIONAL FEDERATION OF ACCOUNTANTS:

- *Guide to Using International Standards on Auditing in the Audits of Small- and Mediumsized Entities*. New York, 2007.
- *Implementing International Education Guideline 11 Information Technology in the Accounting Curriculum*. New York, 1996.

– *International Education Guidelines IEG11 - Information Technology for Professional Accountants*. New York, 2003.
– *International Education Guideline n.º 11 (Information Technology in the Accounting Curriculum)*. New York, 2007.
– *Tone at the Top and Audit Quality*. New York, 2007.
– ISA's 315, 330 y 401

INTERVENCIÓN GENERAL DE LA ADMINISTRACIÓN DEL ESTADO:
– *Normas de Auditoría del Sector Público*. Aprobadas el 14 de febrero de 1997 por el Interventor General de de la Administración del Estado.
– Circular 2/2009 de 16 de septiembre, *sobre auditoría pública*.

INTOSAI
– *Auditing e-Government*. The INTOSAI Standing Committee on IT Audit, 2003.
– *E-government in an audit perspective*. Eurosai IT Working Group, 2004.
– *Guía para las normas de control interno del sector público* (INTOSAI GOV 9100). aprobada por el XVIII INCOSAI en 2004.
– Informe del 18º Seminario interregional naciones Unidas/ INTOSAI «*Simposio sobre la aplicación de las Tecnologías de Información y de comunicación a la auditoría del gobierno electrónico: una estrategia para la eficiencia, la transparencia y la rendición de cuentas*», Viena 2005.
– *ISSAI 5310 Information System Security Review Methodology. A Guide for Reviewing Information System Security in Government Organisations*. Issued by EDP Audit Committee, 1995.

ISACA:
– *IS Auditing Guideline G3 Use of computer-assisted audit techniques (CAATs)*.

IT GOVERNANCE INSTITUTE:
– *CobiT 4.1 (Control Objectives for Information and Related Technology)*. Rolling Meadows, 2005.
– *IT Control Objectives for Sarbanes-Oxley. The importance of IT in the design, implementation and sustainability of internal control over disclosure and financial reporting*. Segunda edición, Rolling Meadows, 2006.

JONÁS GONZÁLEZ, Isaac: *La auditoría de cuentas en entornos informatizados*. Partida Doble n.º 156, Madrid 2004.

KERKVLIET, Matthijs y WIJSMAN, Thomas: *Dutch experiences with ERP SAP systems*. intoIT 28, Londres, 2009

KPMG: *Internal Control: A Practical Guide*. Londres, 1999.

KRIEL, Eckhardt J.: *Application des techniques de verification informatisée*. L'Institut Canadien des Comptables Agrées, Toronto, 2007.

KORNBRUST, Alexander: *Trends in Oracle Security*, Red Database Security Gmbh, Neunkirchen, 2008.

LANZA SUÁREZ, Pablo:

- *El análisis de frecuencia digital como instrumento analítico en control financiero*. Cuenta con IGAE, n.º 9, 2004.
- *Iniciación a la Auditoría de Sistemas de Información*. Intervención General de la Administración del Estado – Oficina Nacional de Auditoría, Madrid, 2000.
- *La evidencia informática*. Auditoría Pública n.º 11, 1997.
- *La informática en el trabajo de auditoría*. Auditoría Pública n.º 13, 1998.
- *Técnicas de auditoría asistida por ordenador*. Instituto de Estudios Fiscales, Madrid, 2000.

LAVIGNE, Andrée y ÉMOND, Caroline: *Going electronic*. intoIT n.º 19, Londres, 2004.

L'ASSOCIATION FRANÇAISE DE L'AUDIT ET DU CONSEIL INFORMATIQUES (AFAI): *Contrôle interne et système d'information*, 2ème edition, Neuilly sur Seine, 2008,.

MEDINA JÁBER, Rafael: *Iniciativas para la gobernanza. Hacia un nuevo modelo de control de las finanzas públicas*. Auditoría Pública, n.º 47, Sevilla, 2009.

MICROSOFT: *La Plataforma para Servicios de Administración Local. Desarrollo de la plataforma de Microsoft de servicios al ciudadano*, 2008.

MINGUILLÓN ROY, Antonio: *La fiscalización en entornos informatizados*, Auditoría Pública n.º 40, 2006.

ORACLE: *Oracle Applications Concepts*, Oracle, Redwood Shores, 2009.

ÓRGANOS DE CONTROL EXTERNO DE ESPAÑA: *Principios y Normas de Auditoría del Sector Público*, elaborados por la Comisión de Coordinación de los Órganos de Control Externo de España, 1991.

POLO GARRIDO, Fernando y MARTÍN YESTE, Ana María: *Introducción a la auditoría del Sector Público*. Ed. Universidad Politécnica de Valencia, Valencia, 2008.

PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD (PCAOB):

- *An audit of internal control over financial reporting that is integrated with an audit of financial statements (Auditing Standard n.º 5)*. Washington, 2007.
- *An audit of internal control over financial reporting that is integrated with an audit of financial statements: Guidance for auditor of smaller public companies*. Washington, 2009.

REGISTRO DE ECONOMISTAS AUDITORES: *Guía de Auditoría*. Madrid, 2005.

SAP: *Annual Report 2008*. www.sap.com.

SILON LOUIE, Denise: *Guidelines for reviewing the appropriateness of user access*. Proviti KnowledgeLeader, 2008

SINDICATURA DE COMPTES DE LA COMUNITAT VALENCIANA:

- *Plan Trienal 2008-2010 de la Sindicatura de Comptes*. Valencia, 2008.
- *Manual de fiscalización de la Sindicatura de Comptes*. Solo accesible on line en www.sindicom.gva.es/web/valencia.nsf/documento/manual_de_fiscalizacion.

SINGLETON, Tommie W.: *What every auditor IT should know about scoping an IT audit*. ISACA Journal, Rolling Meadows, 2009.

THE INSTITUTE OF INTERNAL AUDITORS:

- *GAIT for Business and IT Risk*. Altamonte Springs, 2008
- *GAIT for IT General Control Deficiency Assessment. An approach for evaluating ITGC deficiencies in Sarbanes-Oxley Section 404 assessments of internal controls over financial reporting*. Altamonte Springs, 2008
- *The GAIT Methodology. A risk-based approach to assessing the scope of IT General Controls*. Altamonte Springs, 2007
- *The GAIT Principles*. Altamonte Springs, 2007
- *Global Technology Audit Guide (GTAG) 12: Auditing IT Projects*
- *GTAG 11: Developing the IT Audit Plan*
- *GTAG 10: Business Continuity Management*

– *GTAG 9: Identity and Access Management*
– *GTAG 8: Auditing Application Controls*
– *GTAG 7: IT Outsourcing*
– *GTAG 6: Managing and Auditing IT Vulnerabilities*
– *GTAG 5: Managing and Auditing Privacy Risks*
– *GTAG 4: Management of IT Auditing*
– *GTAG 3: Continuous Auditing*
– *GTAG 2: Change and Patch Management Controls*
– *GTAG 1: Information Technology Controls*
– *2009 IT Audit Benchmarking Study*

TONAREN, John: *Integrated IT audit*. ITAudit, Londres, 1999.

TRIBUNAL DE CUENTAS EUROPEO:

– *Guidelines on computer assisted audit tools (CAATs)*, Luxemburgo, 2006.
– *Guidelines on how to integrate IT AUDIT within the audit process - ECACIT*. Luxemburgo, 2008.

UK NATIONAL AUDIT OFFICE:

– *Audit Briefing: Firewalls*. Londres, 2004.
– *Improving the disposal of public sector Information, Communication and Technology Equipment*. Londres, 2007.

UNIÓN EUROPEA: *Préparer l'avenir numérique de l'Europe. Examen à mi-parcours de l'initiative i2010*. Comunicación de la Comisión de la Unión Europea, abril de 2008.

US Government Accountability Office (GAO):

– *Assessing the Reliability of Computer-Processed Data*. Washington, 2009.
– *Federal Information System Controls Audit Manual (FISCAM)*. Washington, 2009.
– *Financial Audit Manual (FAM)*. Washington, 2008.
– *Information Security Risk Assessment*, *Practices of Leading Organizations*. Washington, 1999.

VALERO TORRIJOS, Julián: *Las garantías jurídicas en la Administración electrónica: ¿Avance o retroceso?*. Revista Cuenta con IGAE, n.º 22, Madrid

WILLIAMSON, A. Louise: *The Implications of Electronic Evidence*. Journal of accountancy, 1997.

Anexo 4. Glosario

ABAP/4

Advanced Business Application Programming. El lenguaje de programación de cuarta generación de SAP.

ABAP/4

Actividades de control

Es una descripción de los requisitos principales de un control.

Control activities

Análisis del riesgo

El proceso para identificar los riesgos de un sistema y estimar la probabilidad de ocurrencia, el impacto posible, y las acciones que lo mitigan.

Risk analysis

Aplicación de negocio

Una aplicación de negocio es una combinación de hardware y software usada para procesar información de la actividad de la entidad y da soporte a uno o varios procesos de negocio.

Pueden clasificarse en tres grupos: procesos relacionados con la misión o actividad de la entidad, financieros, o de apoyo.

Business process application

Control a nivel de entidad (empresa)

Se trata de directivas y de procedimientos internos aplicables a toda la empresa

A la inversa de los controles de procesos, los controles al nivel de la empresa (en general) tienen un alcance abstracto pero más amplio.

Entity level controls

Control compensatorio

Un control interno que reduce el riesgo de una debilidad, real o potencial, existente en otro control, que pudiera resultar en errores u omisiones.

Compensating control

Control de acceso físico

Este tipo de control implica restricciones de acceso físico a los recursos informáticos y protege a esos recursos de pérdidas o deterioros intencionados o accidentales.

Physical access control

Control de integridad

Controles que garantizan que todas las transacciones que han producido han sido registradas en el sistema y procesadas una sola vez.

Completeness control

Control de usuario

Los controles que son llevados a cabo por personas interactuando con controles TI.

User control

Control interno

El control interno es un proceso integral efectuado por la gerencia y el personal, y está diseñado para enfrentarse a los riesgos y para dar una seguridad razonable de que en la consecución de la misión de la entidad, se alcanzarán los siguientes objetivos gerenciales:

- Ejecución ordenada, ética, económica, eficiente y efectiva de las operaciones
- Cumplimiento de las obligaciones de responsabilidad
- Cumplimiento de las leyes y regulaciones aplicables
- Salvaguarda de los recursos para evitar pérdidas, mal uso y daño.

Internal control

Controles de aplicación

Son controles incorporados en las aplicaciones para asegurar la integridad, exactitud, validez, confidencialidad y disponibi-

lidad de transacciones y datos durante el procesamiento de las aplicaciones.

Application controls

Controles de interface

Controles para proporcionar una garantía razonable de que los datos utilizados por las aplicaciones con origen en otros sistemas o aplicaciones han sido adecuadamente convertidos a la aplicación destino.

Interface controls

Controles generales

Los controles generales son las políticas y procedimientos que se aplican a la totalidad o a gran parte de los sistemas de información de una entidad, incluyendo la infraestructura y plataformas informáticas de la organización auditada.

General controls

Controles híbridos

Combinación de controles manuales y automatizados.

Hybrid controls

Datos maestros

Son los atributos permanentes de un objeto, información importante que es relativamente constante y se comparte entre múltiples funciones o aplicaciones (p.e. datos maestros de clientes, de proveedores, de productos en existencias, etc.).

Master data

Debilidad material

Una debilidad material es una deficiencia significativa en el control interno respecto de las que existe una razonable posibilidad (si tuviéramos que concretarla diríamos que la probabilidad es superior al 50%) de que una manifestación errónea significativa en las cuentas anuales no sea prevenida o detectada y corregida en plazo oportuno.

Material weakness

Deficiencia de control

Una deficiencia de control interno existe cuando el diseño o el funcionamiento de un control no permite al personal de la entidad

o a su dirección, en el curso ordinario de las operaciones, prevenir o detectar errores o irregularidades en un plazo razonable

Control deficiency

Deficiencia significativa

Es una deficiencia en el control interno que afecta adversamente la capacidad de la entidad para iniciar, autorizar, registrar, procesar o reportar información financiera de forma fiable de conformidad con los principios o normas contables y/o presupuestarias aplicables, y existe una probabilidad de que una manifestación errónea en las cuentas anuales, no sea prevenida o detectada por los empleados de la empresa en el curso normal de ejecución de sus funciones.

Significant deficiency

Dependencia de control

Existe cuando la eficacia de un control interno depende de la eficacia de otros controles internos.

Control dependency

Diccionario de datos

El diccionario de datos organiza y mantiene información sobre las relaciones, atributos y definiciones de los elementos de datos existentes en las bases de datos, y cómo los datos son usados en los programas y pantallas.

Data dictionary

Dueños de datos

Individuos, por lo general gerentes o directores, que tienen la responsabilidad de la integridad, el uso y el reporte preciso de los datos computarizados

Data owner

Entorno de control

El entorno o ambiente de control es un componente importante del sistema de control interno de una entidad. Establece las condiciones en que los sistemas de control deben operar y como resultado contribuye, positiva o negativamente, a su propia confiabilidad.

Entre los factores que influyen en el entorno de control se incluyen la filosofía de dirección, y el estilo operativo, la estructura organizativa, métodos para asignar responsabilidades, métodos de la gerencia para monitorizar el rendimiento, etc.

Control environment

ERP

Software comercial que integra toda o gran parte de la información que fluye en el seno de una entidad. Los ERP están formados por diferentes módulos funcionales que están integrados dentro del núcleo del sistema o conectados mediante interfaces con sistemas externos.

ERP (Enterprise Resource Planning)

Evaluación por comparación

Un proceso utilizado en administración, en particular en la administración estratégica, en el cual las compañías evalúan varios aspectos de sus procesos de negocio con respecto a las mejores prácticas, por lo general dentro de su propia industria.

Benchmarking

Fiabilidad

La capacidad del sistema de funcionar como los usuarios esperan. y hacerlo consistentemente, sin fallos o comportamientos erráticos

Reliability

Función

Es la tarea que realiza un empleado o funcionario para llevar a cabo una parte de sus responsabilidades.

Es un subconjunto de actividades que producen un resultado u output

Function

Infraestructura TI

Incluye software que es usado para asistir a ejecutar las operaciones del sistema, incluyendo la gestión de los dispositivos de la red. Se incluyen los SGBD, email, plug-in, y aplicaciones no relacionadas directamente con los procesos de negocio.

Infrastructure application

Interfaz

Una interfaz es un elemento del sistema que sirve a la comunicación, al intercambio de informaciones entre diferentes componentes y subsistemas. Una interfaz está definida por una serie de reglas.

Las interfaces entre programas (interfaces externas) y los puntos de integración entre diferentes módulos (interfaces internas) son puntos de contacto lógicos en un sistema de información.

Interface

Manifestación

Afirmación, implícita o explícita contenida en las transacciones realizadas o hechos contables ocurridos, que integran los saldos de cuentas y las revelaciones en la memoria de las cuentas anuales. Se refieren a la existencia, acaecimiento, integridad, valoración, medición, presentación y desgloses de los distintos elementos de las cuentas anuales.

Assertion

Mapa de procesos

Es una descripción gráfica de las funciones o actividades llevadas a cabo por una entidad.

Process mapping

Materialidad

Concepto de auditoría acerca de la importancia relative de un importe en el contexto de las cuentas anuales.

Materiality

Middleware

Software que permite la compatibilidad entre las infraestructuras tecnológicas (fundamentalmente los SGBD) y las aplicaciones de negocio.

También permite la intercomunicación de datos entre aplicaciones o sistemas diferentes.

Middleware

No repudio

La habilidad para prevenir a los que envían un documento que el receptor niegue haberlo recibido y al receptor que se les niegue que lo han recibido.

Nonrepudiation

Objetivos de control

Una declaración del resultado o propósito que se desea alcanzar al implementar procedimientos de control en un proceso en particular.

Control objectives

Parámetro

Valores que se dan a una variable. Proporcionan el medio para adaptar (customizing) una aplicación.

Parameter

Pista de auditoria

Un registro que muestra quién ha accedido a un sistema TI y qué operaciones ha realizado un usuario en un periodo determinado.

Puede usarse para identificar acceso y actividades no autorizadas.

Audit trail

Plan de contingencia

Políticas y procedimientos establecidos por la dirección, diseñados para mantener o restaurar las operaciones de la entidad, incluyendo las informáticas, posiblemente en una ubicación alternativa, en caso de emergencias, fallos de los sistemas o desastres.

Contingency plan

Plan de continuidad de negocio

Un conjunto preestablecido de instrucciones o procedimientos que describen cómo se mantendrán un conjunto de funciones básicas de la entidad durante un periodo de hasta 30 días, en caso de que suceda un desastre, hasta la vuelta a la actividad normal.

Continuity of Operations Plan

Plan de recuperación de desastres

Un plan escrito para poder seguir utilizando las aplicaciones importantes en caso de un fallo generalizado de hardware o de software, o de destrucción de las instalaciones.

Disaster recovery plan

Plataforma

La tecnología fundamental de un sistema informático. Normalmente una combinación específica de hardware y software.

Platform

Proceso

Un proceso consiste en una serie de actividades, operaciones o funciones (manuales, semiautomáticas o automatizadas) llevadas a cabo por una entidad, que sirven para producir un determinado resultado (la elaboración de productos o el suministro de servicios) o el tratamiento de la información.

Process

Proceso de negocio

Consiste en una serie de actividades, operaciones o funciones (manuales, semiautomáticas o automatizadas) llevadas a cabo por una entidad, que sirven para llevar a cabo su misión y desarrollar su actividad (la elaboración de productos o el suministro de servicios) o el tratamiento de la información.

Business process

Propietario

Gerente o director que tiene la responsabilidad de un determinado recurso de TI (SO, SGBD, aplicación, …).

Owner

Regla de gestión

Reglas o instrucciones que deben ser tenidas en cuenta en las especificaciones de una aplicación, su desarrollo e implementación. Tienen un impacto importante en el diseño del sistema de control interno y en la concepción y eficacia de los controles clave.

Business Rule

Prueba de recorrido

Una prueba de recorrido consiste en reproducir y documentar las etapas manuales y automáticas de un proceso o de una clase de transacción, sirviéndose de una transacción utilizada como ejemplo. Sirve para verificar la comprensión del proceso de negocio, subproceso o actividad analizada, los riesgos y los controles clave relacionados.

Walktrough

Repudio

La negación por una de las partes que intervienen en una transacción, de su participación total o parcial en la misma o sobre el contenido de las comunicaciones relacionadas con la misma.

Repudiation

Riesgo de auditoría

El riesgo de auditoría es la evaluación hecha por el auditor del riesgo de que las cuentas anuales contengan un error o irregularidad significativa no detectada una vez que la auditoría ha sido completada.

Audit risk

Riesgo de control

En una auditoría financiera, es el riesgo de que los sistemas de control no puedan evitar o detectar y corregir errores o irregularidades significativas en forma oportuna.

Control risk

Riesgo residual

Riesgo existente después de aplicar las medidas de control.

Residual risk

Segregación/separación de tareas

Un control interno básico que previene y detecta errores o irregularidades por medio de la asignación a individuos diferentes, de la responsabilidad de iniciar y registrar las transacciones y la custodia de los activos.

Segregation / separation of duties

Sistema de información

Un sistema de información consiste en los procedimientos, documentos y registros establecidos para iniciar, registrar, procesar y reportar las transacciones de la entidad (así como los hechos y condiciones) y mantener un control responsable de los activos, pasivos y fondos propios.

Information System

Sistema operativo

Software que controla la ejecución de otros programas de ordenador, programa tareas de la CPU, distribuye el almacenamiento, gestiona las interfaces con hardware periférico y muestra la interfaz por defecto con el usuario cuando no hay funcionando ningún otro programa.

Operating system

SOA

Arquitectura orientada al servicio.

SOA (Service-oriented architecture)

Superusuario

Usuario que tiene las más amplias capacidades de gestión del sistema.

Super user

CAM

Caja de Ahorros
del Mediterráneo

SINDICATURA DE COMPTES
DE LA
COMUNITAT VALENCIANA