CAPÍTULO 19

# AUDITORÍA DE APLICACIONES

*José María Madurga Oteiza*

## 19.1. INTRODUCCIÓN

Qué duda cabe que una meticulosa y exhaustiva auditoría de una aplicación informática de relevancia en una empresa o entidad podría dar pie para poner en funcionamiento la práctica totalidad de la extensa gama de técnicas y rica metodología de la auditoría informática.

Debo, por tanto, aclarar de partida el alcance de este trabajo dentro del contexto de la obra en que se integra: al contar con capítulos específicos dedicados a numerosos aspectos técnicos y al resto de etapas de la vida de un sistema, incluso a su explotación y mantenimiento, mi exposición *se va a centrar en la fase final de la vida de la aplicación informática, la de su funcionamiento ordinario,* una vez superada la crítica etapa de su implantación, que habrá cerrado el ciclo precedido por las de concepción y desarrollo.

También he de confesar mi propósito de que prime la recopilación de experiencias recogidas en los trabajos de este tipo que he tenido ocasión de dirigir, sobre el rigor de una recapitulación de estándares de objetivos de control, que pueden ser localizados sin dificultad a través de numerosas fuentes. Dichas experiencias se han desenvuelto en aplicaciones de gran envergadura y complejidad: utilizadas por un considerable número de usuarios, con gran dispersión geográfica, diversidad de plataformas y compleja red de comunicaciones, lo que debiera haber permitido aflorar mayor número de problemas a tener en cuenta y a los que dar solución.

Así pues, el objeto de este trabajo consiste en *tratar de ayudar a planificar, preparar y llevar a cabo auditorías de aplicaciones en funcionamiento en cuanto al*

*grado de cumplimiento de los objetivos para los que las mismas fueron creadas*: con carácter general, éstos estarán en la línea de servir de eficaces herramientas operativas y de gestión que potencien la más eficiente contribución, por parte de las organizaciones usuarias de las aplicaciones, a la consecución de los objetivos generales de la empresa, grupo o entidad a la que pertenecen.

## 19.2. PROBLEMÁTICA DE LA AUDITORÍA DE UNA APLICACIÓN INFORMÁTICA

Una aplicación informática o sistema de información habitualmente persigue como finalidad:

- Registrar fielmente la información considerada de interés en torno a las operaciones llevadas a cabo por una determinada organización: magnitudes físicas o económicas, fechas, descripciones, atributos o características, identificación de las personas físicas y/o jurídicas que intervienen o guardan relación con cada operación, nombres, direcciones, etc.

- Permitir la realización de cuantos procesos de cálculo y edición sean necesarios a partir de la información registrada, pudiendo, por tanto, almacenar automáticamente más información que la de partida, aunque siempre basada en aquélla.

- Facilitar, a quienes lo precisen, respuesta a consultas de todo tipo sobre la información almacenada, diseñadas en contenido y forma para dar cobertura a las necesidades más comunes constatadas.

- Generar informes que sirvan de ayuda para cualquier finalidad de interés en la organización, presentando la información adecuada: se aplican –según convenga– criterios de selección, ordenación, recuento y totalización por agrupamientos, cálculos de todo tipo, desde estadísticos comunes (media, desviación típica, valores mínimo, máximo, primero y último, etc.), hasta los más sofisticados algoritmos.

Si este planteamiento se consigue trasladar con rigor a una aplicación informática y los usuarios la manejan con soltura y con profesionalidad, la organización a la que pertenecen contará con un importante factor de éxito en el desarrollo de su actividad.

Sin embargo, ni el rigor en la creación de la aplicación ni la profesionalidad en el uso de la misma pueden ser garantizados. Además la profesionalidad no inmuniza contra el cansancio y el estrés. Asumido está también que de humanos es equivocarse, cometer errores y omisiones involuntariamente. Y tampoco es imposible que en un

momento determinado un empleado descontento cometa errores intencionadamente o que otro, en apuros económicos, sucumba a la tentación de intentar un fraude perfecto si considera mínima la probabilidad de ser descubierto, tal y como funciona el sistema y la organización, que puede no estar dando muestras de ejercer un control interno riguroso.

Y no son éstas las únicas amenazas al normal cumplimiento de la finalidad de nuestra aplicación:

- La posibilidad de fallo en cualquiera de los elementos que intervienen en el proceso informático: software múltiple perteneciente a diferentes firmas, computador central y dispositivos periféricos, transmisión de datos (servidores, módems, líneas de comunicaciones, etc.) constituye otra fuente de posibles riesgos.

- La conexión cada vez más generalizada de las empresas a entornos abiertos como la Internet multiplica los riesgos que amenazan la confidencialidad e integridad de la información de nuestros sistemas. Y en este caso el número de interesados en descubrir debilidades que les abran las puertas para enredar y manipular la información a la que sean capaces de acceder no tiene límites.

*Todas esas amenazas y cualquier otra que pueda ser identificada contra el correcto funcionamiento de nuestra aplicación y la consecución de sus objetivos, han debido ser objeto de un análisis minucioso ya desde la fase de su concepción.* Para cada una de ellas se habrán debido estudiar las posibles medidas tendentes a eliminar los riesgos que entrañan o, cuando menos, a reducir la probabilidad de su materialización hasta niveles razonablemente asumibles, siempre teniendo en cuenta el costo de tales medidas (que no cuesten más las cintas que el manto, según el dicho popular).

Dichas medidas son fundamentalmente medidas de control interno que, con carácter general, consisten en los procedimientos para verificar, evaluar y tratar de garantizar que "todo" funciona como se espera: de acuerdo con las políticas, directrices, normas y procedimientos establecidos en los diferentes ámbitos de responsabilidad.

En el terreno de una aplicación informática, el control interno se materializa fundamentalmente en controles de dos tipos:

- ***Controles manuales***: a realizar normalmente por parte de personal del área usuaria: actuaciones previstas para asegurar que –en su caso– se preparan, autorizan y procesan todas las operaciones, se subsanan adecuadamente todos los errores, son coherentes los resultados de salida respecto a referencias disponibles sobre los datos de entrada, y las bases de datos que dan soporte a la aplicación mantienen en los niveles debidos diferentes indicadores de

medición de su integridad y totalidad (número de registros en archivos y/o tablas, de relaciones o índices, totales de magnitudes numéricas, conciliaciones, etc.).

- ***Controles automáticos***: incorporados a los programas de la aplicación que sirvan de ayuda para tratar de asegurar que la información se registre y mantenga completa y exacta, los procesos de todo tipo sobre la misma sean correctos y su utilización por parte de los usuarios respete los ámbitos de confidencialidad establecidos y permita poner en práctica principios generales de control interno como el referente a la segregación de funciones.

Controles que, según su finalidad, se suelen clasificar en:

- **Controles preventivos:** Tratan de ayudar a evitar la producción de errores a base de exigir el ajuste de los datos introducidos a patrones de formato y estructura (dato numérico, fecha válida, etc.), pertenencia a una lista de valores válidos o a un archivo maestro, rango entre límites determinados, incorporación de dígitos de control en datos clave (códigos de identificación, referencias de documentos, nomenclaturas, etc.) y, en general, cualquier criterio que ayude a asegurar la corrección formal y verosimilitud de los datos (la exactitud sólo puede garantizarla el usuario).

  Son de gran utilidad las comprobaciones de conjuntos de datos, buscando su compatibilidad, adecuación y coherencia (por ejemplo, una cuenta de cargo puede no ser compatible con un tipo de instalación).

- **Controles detectivos:** Tratan de descubrir a posteriori errores que no haya sido posible evitar.

- **Controles correctivos:** Tratan de asegurar que se subsanen todos los errores identificados mediante controles detectivos.

Y que pueden ser utilizados:

- En las transacciones de recogida o toma de datos.
- En todos los procesos de información que la aplicación realiza.
- En la generación de informes y resultados de salida.

Pues bien, como apuntábamos hace un momento, ya en el diseño de la aplicación se debió hacer un estudio a conciencia para seleccionar de entre los posibles, y teniendo en cuenta su costo frente a su previsible efectividad contra el riesgo que trata de contrarrestar, los controles considerados idóneos para cada situación planteada en los diferentes pasos de funcionamiento de la aplicación.

Este estudio debió ser propuesto por los responsables del área informática -contando siempre en el diseño con la participación de representantes de la organización usuaria-, *revisado por personal de auditoría interna*, y aprobado en última instancia por la dirección de la organización usuaria, máxima responsable de la aplicación.

Es importante recalcar la conveniencia de la participación de Auditoría interna (con un carácter más general que Auditoría informática) en la revisión de los controles diseñados durante el desarrollo de la aplicación. Sus recomendaciones deben ser consideradas -aunque la decisión final en caso de discrepancia debe radicar en la organización usuaria-. Lo que está fuera de toda duda es que sería tremendamente más costoso, tener que incluir cualquier control una vez finalizado el desarrollo, como modificación, porque se pusiera de manifiesto su necesidad como resultado de una auditoría posterior a la implementación.

La participación de Auditoría interna en el desarrollo de un sistema informático debe tener un alcance más amplio que el referente al sistema informático, ya que debe contemplar no sólo los riesgos relacionados con la aplicación, sino todos los que puedan afectar al proceso completo al que la misma sirve de Herramienta, pudiendo proponer: que la aplicación registre información específica, **"pistas de auditoría"**, para facilitar la futura auditabilidad del proceso respecto a tales riesgos. Lo mismo cabe decir, en cuanto al requerimiento de pistas de auditoría, para facilitar las futuras auditorías informáticas de la aplicación.

Después de lo expuesto, podemos centrar la problemática de la auditoría de una aplicación: se trata de realizar una **revisión de la eficacia del funcionamiento de los controles diseñados para cada uno de los pasos de la misma frente a los riesgos que, tratan de eliminar o minimizar,** como medios *para asegurar la fiabilidad (totalidad y exactitud), seguridad, disponibilidad y confidencialidad de la información gestionada por la aplicación.*

Ello obliga a replantearse nuevamente, y con carácter previo, si los propios riesgos tenidos en cuenta en su momento son todos los posibles o se detectan otros nuevos: unos y otros deben ser evaluados, analizada la probabilidad de su materialización y sus consecuencias previsibles, de cara a reconsiderar si los controles implantados, tal como están actuando, superan con garantías de éxito la exposición a amenazas percibida en la situación actual.

Quede bien entendido que, por muy completa que resulte la revisión que hagamos de una aplicación informática y de los controles que incorpora, no es suficiente para garantizar la seguridad de la misma: ésta se consolida con la realización de una evaluación de los controles generales y una revisión de los controles de la función informática, que estarán recogidos en el Plan de trabajos de auditoría informática.

## 19.3. HERRAMIENTAS DE USO MÁS COMÚN EN LA AUDITORÍA DE UNA APLICACIÓN

Antes de nada conviene hacer hincapié en que la tremenda evolución de las tecnologías, en todo lo referente a los sistemas de información, obliga a un esfuerzo considerable de formación a todo el personal de auditoría interna, y en particular a los especialistas en auditoría informática. Este reto debe estar asumido por la dirección de Auditoría, que debe impulsar la respuesta adecuada al mismo, recogida en un ambicioso **plan de formación**, que incluya la atención a las nuevas tendencias y preocupaciones.

Ello no es óbice para que, dentro de la política de la empresa, se contemple la posibilidad de contratar la realización de determinadas auditorías informáticas muy especializadas *(outsourcing)* o personal auditor que participe en trabajos; pero siempre será conveniente que la dirección de todos los trabajos sea conducida, y con suficiente conocimiento general aun en los temas más especializados, por auditores de la propia empresa.

Haremos un recorrido por las herramientas más comúnmente utilizadas en la auditoría de la aplicación informática dentro del contexto que hemos delimitado en la introducción.

En ocasiones se podrán combinar varias a la vez; por ejemplo se puede, en una entrevista con otro propósito, aprovechar la ocasión para realizar una prueba de conformidad prevista, además de observar la utilización de la aplicación por el entrevistado e incluso, si éste estuviera interesado, rellenar o comentar una encuesta que se le había dirigido.

### 19.3.1. Entrevistas

De amplia utilización a lo largo de todas las etapas de la auditoría, las entrevistas deben cumplir una serie de requisitos:

- Las personas a entrevistar deben ser aquellas que más puedan aportar al propósito pretendido.
- La entrevista debe ser preparada con rigor de cara a sacar el máximo partido de ella.
- Para ello es indispensable escribir el guión de temas y apartados a tratar (no un cuestionario cerrado), para evitar que quede sin tratar algún asunto de interés;

también exige haber alcanzado el nivel de conocimientos sobre la aplicación necesario en ese momento para conducir con soltura la entrevista.

- Ha de ser concertada con los interlocutores con antelación suficiente, informándoles del motivo y las materias a tratar en ella, la duración aproximada prevista y, en su caso, solicitando la preparación de la documentación o información que pueda ser necesario aporten durante la misma; no debe faltar la invitación a colaborar con cuantas sugerencias estimen oportuno, no sólo sobre el propio objeto de la entrevista sino también con miras más amplias en relación con el proceso global desarrollado por la organización y la aplicación informática que apoya el proceso.

- Las jefaturas de las personas a entrevistar deben estar informadas de las actuaciones previstas; en general será positivo que sea el propio jefe quien comunique al interesado la necesidad de participar en la auditoría.

- Durante el desarrollo de la entrevista, el auditor tomará las anotaciones imprescindibles; lo más próximo posible a la finalización de la entrevista el auditor debe repasar sus anotaciones, completando con detalles que pueda recordar aquellas que pudieran haber quedado esbozadas, y reflexionando sobre las posibles implicaciones de las novedades o singularidades que el interlocutor haya podido aportar.

## 19.3.2. Encuestas

Pueden ser de utilidad tanto para ayudar a determinar el alcance y objetivos de la auditoría como para la materialización de objetivos relacionados con el nivel de satisfacción de los usuarios.

Con las lógicas salvedades, la mayor parte de los requisitos enumerados para las entrevistas son también de aplicación para las encuestas.

- En este caso, sin embargo, sí que hay que preparar un cuestionario que pueda ser contestado con la mayor rapidez a base de marcar las respuestas entre las posibles.

- Conviene que todas las preguntas vayan seguidas de un espacio destinado a observaciones, y no sólo las que soliciten descripción cuando la respuesta haya podido ser "Otros", caso de elección entre varias alternativas. Al final del cuestionario hay que solicitar sugerencias u observaciones abiertas, mejor en página exclusiva para ello, que pueda ser fotocopiada por quienes necesiten más espacio para sus comentarios.

- Aunque no puede ni debe exigirse la identificación personal del encuestado, sí debe hacerse de la organización a la que pertenece (Cuidado con los recuentos de resultados de la encuesta por organización que pudieran quedar con una única respuesta: no deben ser obtenidos, limitando, por tanto, la obtención de tales recuentos a la condición de contar con más de una respuesta en el agrupamiento.) Sin embargo, sí puede invitarse a que se identifique quien no tenga ningún inconveniente en ello, lo que permitiría contactos enriquecedores si la encuesta contestada plantea asuntos de interés.

## 19.3.3. Observación del trabajo realizado por los usuarios

Aunque por otros medios puede llegarse a comprobar que la aplicación funciona con garantías de exactitud y fiabilidad, es conveniente observar cómo algún usuario hace uso de aquellas transacciones más significativas por su volumen o riesgo: puede ayudar a detectar que, aunque el resultado final sea bueno y, por tanto, los controles establecidos sean efectivos, la eficiencia no esté en el nivel óptimo; no es infrecuente que un auditor experimentado identifique mejoras en este tipo de observaciones: desde carencias del usuario o vicios adquiridos que pueden denotar falta de formación, hasta mejoras de diseño que puedan aumentar la agilidad y productividad en el uso de la aplicación: recomendaciones de opciones o valores propuestos por defecto, simplificación de pasos, etc.

Debe aprovecharse esta oportunidad para probar también la efectividad de los controles de las transacciones en cuestión, solicitando la simulación de situaciones previsibles de error para comprobar si la respuesta del sistema es la esperada: intento de duplicar una operación real, de cometer errores de diferentes tipos en la introducción de cada uno de los datos, etc.

## 19.3.4. Pruebas de conformidad

De uso general en todo el campo de la auditoría, son actuaciones orientadas específicamente a comprobar que determinados procedimientos, normas o controles internos, particularmente los que merecen confianza de estar adecuadamente establecidos, se cumplen o funcionan de acuerdo con lo previsto y esperado, según lo descrito en la documentación oportuna.

La comprobación debe llevar a la evidencia a través de la inspección de los resultados producidos: registros, documentos, conciliaciones, etc. y/u observación directa del funcionamiento de un control ante pruebas específicas de su comportamiento.

- La evidencia de incumplimiento puede ser puesta de manifiesto a través de informes de excepción.

- Los testimonios de incumplimiento no implican evidencia pero, si parten de varias personas, es probable que la organización asuma como válidos dichos testimonios y, por tanto, las consecuencias que de los mismos pudieran derivarse de cara a posibles recomendaciones, ahorrando esfuerzos para tratar de conseguir su confirmación documental.

## 19.3.5. Pruebas substantivas o de validación

Orientadas a detectar la presencia o ausencia de errores o irregularidades en procesos, actividades, transacciones o controles internos integrados en ellos.

También pertenecen al dominio general de la auditoría.

Están especialmente indicadas en situaciones en las que no hay evidencia de que existan controles internos relevantes, suficientes como para garantizar el correcto funcionamiento del proceso o elemento considerado.

- Todo tipo de error o incidencia imaginable puede ser objeto de investigación en esta clase de pruebas. En el ámbito de la auditoría de una aplicación informática, irregularidades de diversa índole que pueden afectar a las transacciones:

  - Transacciones omitidas, no registradas en el sistema.
  - Duplicadas, registradas más de una vez.
  - Inexistentes indebidamente incluidas.
  - Registradas sin contar con las autorizaciones establecidas.
  - Incorrectamente clasificadas o contabilizadas en cuentas diferentes a las procedentes.
  - Transacciones con información errónea, desde su origen o por alteración posterior, que no refleja la realidad, con posibles consecuencias en:

    - El montante o fechas de devengo incorrectas de derechos y obligaciones de la empresa respecto a terceros.
    - La exactitud de las valoraciones contables o la falta de conciliación con ellas de la contenida en la Aplicación.
    - La exactitud de las mediciones físicas, con posible desajuste respecto a inventarias.

- Infinidad de recursos pueden ser utilizados para detectar indicios, en primera instancia, de posibles errores; indicios cuya presencia deberá llevar a profundizar en la investigación para constatar la existencia real de anomalías. Muchos de ellos se apoyan en la utilización del computador:

  - Análisis de ratios, así como fluctuaciones y tendencias en magnitudes que miden aspectos relacionados con la actividad desarrollada en los procesos.

  - Conciliaciones con partidas que a efectos de control puedan llevarse en la propia aplicación o de otros sistemas, como el económico-financiero.

  - Informes de excepción producidos por la propia aplicación para identificar situaciones que interesa sean objeto de revisión. Aparte de los de obtención rutinaria previstos en el sistema, debiera disponerse de otros específicos para la realización de auditorías, planteados desde la etapa de diseño para poder ejecutar a demanda.

- Otros recursos clásicos utilizados para la detección de errores o sus indicios son de ejecución manual. Normalmente se aplican sobre muestras, estadísticas y no estadísticas.

  - Para las primeras evidentemente son de aplicación las técnicas de muestreo estadístico, que deberán ser respetadas para el cálculo del tamaño de las muestras y su selección en función del nivel de significación y error máximo con que interese trabajar en cada caso.

  - Las muestras no estadísticas, dirigidas, basarán la selección en la búsqueda de las operaciones con mayor probabilidad de error y/o consecuencias más graves, previo análisis de las condiciones de la información disponible que permitan componer un indicador de priorización, asignando puntuaciones al cumplimiento de determinadas condiciones.

- Ejemplos de estos recursos de ejecución manual son: Arqueo, Inventario, Inspección, Comprobación con los documentos soporte de la transacción (factura, albarán, etc.) y Confirmación de saldos por parte de terceros (clientes y proveedores).

## 19.3.6. Uso del computador

- El uso de computadores constituye una de las herramientas más valiosas en la realización de la auditoría de una aplicación informática. Nos referimos tanto a los computadores personales, con los que el auditor informático debe estar

familiarizado manejando con soltura las técnicas de edición de textos y presentaciones, hoja de cálculo, gestor de bases de datos, correo electrónico, etc., como al computador u computadores sobre los que se explota la aplicación objeto de la auditoría.

- Existen en el mercado infinidad de productos de software concebidos para facilitar la tarea del auditor: Herramientas que permiten el acceso generalizado a la información contenida en archivos y bases de datos de forma transparente para el usuario y con independencia de las características de organización y modo de almacenamiento. Muchos de estos productos se presentan como "herramientas de auditoría", ya que incorporan facilidades típicas de esta función como pueden ser la generación de muestras estadísticas, edición de circularizaciones, etc.

- Sin restar su valor a estos productos, y desde la óptica del auditor interno, se pueden obtener resultados similares haciendo uso de herramientas disponibles en la organización y no necesariamente diseñadas para funciones de auditoría. Contando con una herramienta de interrogación, un lenguaje SQL *(Structured Query Language)*, se puede acceder a la información y seleccionar la que interese; su proceso posterior a través de un gestor de base de datos, tipo ACCESS o similar, ofrece un potencial de tratamiento prácticamente ilimitado.

- Las pistas de auditoría de que esté provista la aplicación deben constituir un apoyo importante a la hora de utilizar el computador para detectar situaciones o indicios de posible error. Lo mismo cabe decir de los informes de excepción, particularmente los diseñados específicamente para propósitos de auditoría.

- También hay que considerar la posibilidad de utilizar la propia aplicación, aplicando juegos de ensayo o transacciones ficticias preparadas por los auditores, para verificar la eficacia de los controles implantados. Este tipo de pruebas no es siempre recomendable, sobre todo si no ha sido prevista tal contingencia durante la etapa de diseño de la aplicación.

## 19.4. ETAPAS DE LA AUDITORÍA DE UNA APLICACIÓN INFORMÁTICA

### 19.4.1. Recogida de información y documentación sobre la aplicación

Antes de plantearnos el alcance de los trabajos de auditoría sobre aplicaciones informáticas necesitamos disponer de un conocimiento básico de la aplicación y de su entorno. Realizamos un estudio preliminar en el que recogemos toda aquella información que nos pueda ser útil para determinar los puntos débiles existentes y aquellas funciones de la aplicación que puedan entrañar riesgos.

A través de entrevistas con personal de los equipos responsables de la aplicación, tanto desde la organización usuaria como de la de Sistemas de Información, se inicia el proceso de recopilación de información y documentación que permitirá profundizar en su conocimiento hasta los niveles de exigencia necesarios para la realización del trabajo; y en una primera fase, hasta el nivel de aproximación suficiente para estar en disposición de establecer y consensuar los objetivos concretos de la auditoría.

El primer reto con el que nos encontramos es el de identificar las personas más adecuadas, en cada uno de los ámbitos de organización, para poder transmitir al responsable de la auditoría el conocimiento más amplio posible de la aplicación, sus fortalezas, posibles debilidades, riesgos e inquietudes suscitadas en torno a ella.

Identificadas dichas personas se intenta crear un ambiente de colaboración, con el fin de que transmitan al equipo auditor su visión personal de la situación, aportando cuantas sugerencias estimen de interés, además de suministrar la documentación que se les solicite y estén en disposición de proporcionar.

Para cubrir esta etapa del trabajo de auditoría resulta útil confeccionar unas guías que nos permitan seguir una determinada pauta en las primeras entrevistas y contengan la relación de documentos a solicitar todos aquellos que ayuden a:

- Adquirir una primera visión global del sistema: Descripción general de la aplicación, presentaciones que hayan podido realizarse de la aplicación con distintas finalidades a lo largo de su vida, Plan de Sistemas de la empresa, en lo que respecta a la aplicación a auditar; en él deberán figurar explícitamente sus objetivos, planes y presupuestos. (Un documento de gran trascendencia por su repercusión en la eficacia en el uso de la aplicación es el **"Manual de usuario"**: Concebido como soporte a la formación en el uso de la aplicación informática, debe ser claro, completo y estar bien estructurado para facilitar su

consulta. Es fundamental que esté actualizado al día y en mi opinión imprescindible que los usuarios puedan acceder a él a través de la red.)

- Conocer la organización y los procedimientos de los servicios que utilizan la aplicación. Mediante el examen de lista de personas o dichos servicios, organigrama de los mismos y dependencias funcionales entre ellos, bases de la organización y de la separación de funciones, grado de participación de los usuarios en el desarrollo y en las pruebas de la aplicación, medidas generales de control (protección física, protección lógica), política de formación y sensibilización de los usuarios, grado de satisfacción de los usuarios, etc.

- Describir el entorno en el que se desarrolla la aplicación: conocer recursos de computador central asignados, número de mini o micro computadores asignados total o parcialmente a la aplicación, cantidad de recursos periféricos asignados, configuración de la red y de las líneas de comunicaciones usadas, etc.

- Entender el entorno de software básico de la aplicación, identificando las seguridades que ofrece y los riesgos inducidos.

- Asimilar la arquitectura y características lógicas de la aplicación. Es necesario conocer los principales tratamientos y cómo están estructurados los datos: programas clave de la aplicación, lenguaje y método de programación, archivos maestros, bases de datos y diccionario de datos, modo de captura, de validación y de tratamiento de los datos, informes (listados) generados por la aplicación, así como la periodicidad de los diferentes tratamientos.

- Conocer las condiciones de explotación de la aplicación y los riesgos que se pueden dar. Es decir, si la aplicación la explotan directamente los usuarios o depende de los servicios informativos, volumen de capturas, volumen de información almacenada en los archivos maestros, seguridades de explotación (accesos, salvaguardias, etc.), planificación y organización general de la explotación, características generales; tiempos de respuesta, frecuencia y naturaleza de las incidencias, duración de los procesos *batch*.

- Conocer las condiciones de seguridad de que dispone la aplicación: controles que incorpora, definición de perfiles de acceso a los recursos y a la aplicación, existencia de pistas de auditoría, grado de automatización (mínima intervención humana), documentación.

- Disponer de información relativa a: Estadísticas de tiempos de explotación para cada proceso, de tiempos de respuesta de transacciones on line, de tiempos de reproceso por fallos o errores, tiempos dedicados al mantenimiento, informes de gestión de los accesos, informes de seguimiento

de las salidas, protecciones de los recursos asignados a la aplicación, perfiles de acceso a los recursos de la aplicación.

Resulta conveniente que el auditor solicite los documentos formalmente, facilitando su relación, y que éstos le sean suministrados en soporte informática en la medida de lo posible.

Hemos citado explícitamente sólo unos cuantos documentos, por problemas de espacio, relacionando los lugares comunes que deben cubrir. Adicionalmente cualquier informe, comunicación o acta de grupos de trabajo que puedan estar implicados en tareas de reingeniería de procesos, círculos de calidad, mejora permanente o cualquier otra iniciativa innovadora en el área de negocio a la que sirve la aplicación, serán de gran utilidad para el auditor en su cometido. Procederá en estos casos contactar con los responsables de tales proyectos, para potenciar las sinergias que surgirán, enriqueciendo los resultados de todos.

## 19.4.2. Determinación de los objetivos y alcance de la auditoría

El examen de los documentos recopilados y la revisión de los temas tratados a lo largo, de las entrevistas mantenidas, es decir, las observaciones tras el examen preliminar, la identificación de los puntos débiles y las funciones críticas, deben permitirle al auditor establecer su propuesta de objetivos de la auditoría de la aplicación y un plan detallado del trabajo a realizar. Entendemos que dedicando más recursos cuanto mayor fuera la debilidad o más graves las consecuencias de la amenaza que se somete a revisión.

Es de desear que los objetivos propuestos sean consensuados con el equipo responsable de la aplicación en la organización usuaria.

Es preciso conseguir una gran claridad y precisión en la definición de los objetivos de la auditoría y del trabajo y pruebas que se propone realizar, delimitando perfectamente su alcance de manera que no ofrezcan dudas de interpretación.

En la preparación del plan de trabajo trataremos de incluir:

- **La planificación de los trabajos y el tiempo a emplear,** orden en que se examinarán los diferentes aspectos, centros de trabajo en que se van a desarrollar las pruebas, cargas de tiempos y asignación de los trabajos entre los diferentes colaboradores del equipo.

- **Las herramientas y métodos,** entrevistas con los usuarios y los informáticos, servicios que se van a auditar, documentos que hay que obtener, etc.

- **El programa de trabajo detallado,** adaptado a las peculiaridades de cada aplicación, pero tratando de seguir un esquema tipo:

  - Identificación y clasificación de los objetivos principales de la auditoría.
  - Determinación de subobjetivos para cada uno de los objetivos generales.
  - Asociación, a cada subobjetivo de un conjunto de preguntas y trabajos a realizar teniendo en cuenta las particularidades del entorno y de la aplicación a auditar.

  - Desarrollo de temas como:

    - Modos de captura y validación.
    - Soportes de los datos a capturar
    - Controles sobre los datos de entrada.
    - Tratamiento de errores.
    - Controles sobre los tratamientos: secuencia de programas, valores característicos, controles de versión, exactitud de los cálculos, etc. Controles de las salidas: clasificación y verificación de las salidas; presentación, distribución, diseño y forma de los listados.
    - Pistas para control y auditoría.
    - Salvaguardias.

- **Tests de confirmación, tests sobre los datos y los resultados.** Aquellos que consideramos necesarios para asegurar que los controles funcionan como se han descrito y previsto, y que los controles internos son aplicados.

### Ejemplos de objetivos de auditorías de aplicaciones

A modo de ejemplo, señalaremos las líneas maestras (no servirían como objetivos reales por incumplimiento de los requisitos enunciados) de algunos objetivos que pueden establecerse en este tipo de auditorías de aplicaciones informáticas:

**1. Emitir opinión sobre el cumplimiento de los objetivos, planes y presupuestos contenidos en el Plan de Sistemas de Información sobre la aplicación a auditar**

1.1. Cumplimiento de los plazos previstos en cada una de las fases del Proyecto: Estudio previo, Diseño, Programación, Pruebas, Conversión en su caso, Plan de formación e Implantación.

1.2. Cumplimiento de los presupuestos previstos en cada una de las fases enumeradas y para cada uno de los conceptos manejados: equipos, software, contratación exterior, personal propio, etc.

1.3. Cumplimiento de las previsiones de coste de funcionamiento normal de la aplicación y de su mantenimiento al nivel de desglose adecuado.

**2. Evaluar el nivel de satisfacción de los usuarios del sistema, tanto de la línea operativa como de las organizaciones de coordinación y apoyo respecto a la cobertura ofrecida a sus necesidades de información**

2.1. Nivel de cobertura de funcionalidades implementadas respecto al total de las posibles y deseables en opinión de los usuarios, incluyendo en el concepto de funcionalidad la posibilidad de obtención de informes de gestión y de indicadores de seguimiento de las actividades de la organización usuaria.

2.2. Nivel de satisfacción con el modo de operar las diferentes funcionalidades soportadas por la aplicación, incluyendo los diseños de pantallas e informes de salida, mensajes y ayudas: identificación de mejoras posibles.

2.3. Nivel de satisfacción con la formación recibida para el uso de la aplicación, utilidad del "Manual de usuario" y funcionamiento de los canales establecidos para la resolución de los problemas que surgen en el uso del sistema (¿Línea caliente?).

2.4. Nivel del satisfacción con los tiempos de respuesta de la aplicación y con la dotación de equipos informáticos y sus prestaciones.

2.5. Nivel de satisfacción con la herramienta de usuario para procesar información de la aplicación, en el caso de disponer de ella. (Caso de no estar operativo y haber indicios de su posible conveniencia, el objetivo podría ser el estudio de la conveniencia o no de su implantación.)

**3. Emitir opinión sobre la idoneidad del sistema de control de accesos de la aplicación**

3.1. Evaluar la eficacia y seguridad del Sistema de control de accesos diseñado. (Controles referentes a la identificación de usuario y palabra de paso y posibles intentos reiterados de acceso no autorizado.)

3.2. Analizar si la asignación de operaciones y funcionalidades permitidas a cada uno de los perfiles de usuario diseñados responde a criterios de necesidad para el desempeño del trabajo y segregación de funciones.

3.3. Comprobar que las asignaciones de perfiles a usuarios responden a los puestos que ocupan y se evita la asignación de perfiles a usuarios únicos en cada centro operativo.

**4. Verificar el grado de fiabilidad de la información**

4.1. Revisión de la eficacia de los controles manuales y programados de entrada, proceso y salida: seguimiento de varias operaciones concretas identificables a lo largo del ciclo completo de tratamiento.

4.2. Comprobación por muestreo de la exactitud de la información almacenada en los archivos de la aplicación con respecto a documentos originales.

4.3. Pruebas de validez y consistencia de datos de la aplicación mediante proceso informático de la Base de datos real con herramientas de usuario.

4.4. Pruebas de conciliación de magnitudes totalizadas en la aplicación durante varios períodos de tiempo frente a las disponibles, quizá también a través de utilización de herramientas de usuario, en otros sistemas con los que mantiene relación (sistema contable, almacenes, compras, etc.).

## 19.4.3. Planificación de la auditoría

La auditoría de una aplicación informática, como toda auditoría, debe ser objeto de una planificación cuidadosa. En este caso es de crucial importancia acertar con el momento más adecuado para su realización:

- Por una parte no conviene que coincida con el período de su implantación, especialmente crítico, en que los usuarios no dominan todavía la aplicación y están más agobiados con la tarea diaria. En el período próximo a la implantación, frecuentemente se detectan y solucionan pequeños fallos en la aplicación, situación que convendría esté superada antes de iniciar el proceso de auditoría.

- Por otra parte el retraso excesivo en el comienzo de la auditoría puede alargar el período de exposición a riesgos superiores que pueden y deben ser aminorados como resultado de ella.

En nuestra experiencia, se han manejado períodos de entre 4 y 8 meses desde el inicio de la implantación en función de la magnitud de la aplicación.

- También hay que establecer el ámbito de actuación: tratándose de organizaciones implantadas en amplias zonas territoriales, será necesario delimitar el campo de actuación de la mayor parte de las pruebas a realizar a un reducido número de centros de trabajo. Sin embargo, se ampliará el ámbito, de manera que abarque la representación más extensa posible de usuarios y centros, en aquellas pruebas en que se considere factible, sin incurrir en un coste desproporcionado (encuestas, procesamiento de información, contactos telefónicos, etc.).

- Para la selección de ese limitado número de centros en los que llevar a cabo el trabajo de campo, conviene solicitar a la organización usuaria que los proponga, en base a razones por las que estime puedan aportar mayor valor al trabajo: su participación como pilotos en el desarrollo del sistema o en proyectos de innovación y mejora relacionados con el proceso, haber experimentado recientes cambios organizativos o en su personal directivo que puedan implicar riesgos adicionales, la existencia de indicadores de actividad que se desvíen significativamente de la media general, etc.

- Debe conseguirse cuanto antes, solicitándolo ya en las primeras tomas de contacto, las autorizaciones necesarias para que el personal de auditoría, que está previsto participe en el trabajo, pueda acceder a la aplicación y a las herramientas de usuario. Se solicitará un perfil de auditor –si específicamente se hubiese considerado– o, en otro caso, aquel que ofrezca las mayores posibilidades de sólo consulta: permitirá dedicar a su conocimiento, y a preparar pruebas que puedan precisar su uso, esos tiempos de parada que suelen producirse en el desarrollo de otros trabajos que vayan a ejecutarse durante los meses anteriores al inicio del trabajo de campo de nuestra auditoría de aplicación.

## 19.4.4. Trabajo de campo, informe e implantación de mejoras

En principio las etapas de realización del trabajo de campo, de redacción del informe y de consenso del plan de implantación de mejoras, no ofrecen peculiaridades de relevancia respecto a otros trabajos de auditoría. Es por eso que no vamos a hacer

más referencia a ellas que algún comentario que la experiencia nos sugiere de validez para cualquier auditoría.

- La etapa de realización del trabajo de campo consiste en la ejecución del programa de trabajo establecido. Evidentemente, los resultados que se van obteniendo pueden llevar a ajustar el programa en función de dichos resultados, que pueden aconsejar ampliar la profundidad de algunas pruebas, acometer otras no previstas y concluir alguna antes de su final.

  - Una recomendación de cara a esta etapa es la de plantearse la mínima utilización de "papeles de trabajo", en el sentido literal, físico, potenciando la utilización de PCs portátiles como soporte de la información de las muestras con las que se vaya a trabajar y para la recogida de información y resultados de las diferentes pruebas: no es sólo cuestión de imagen, sino de productividad.

- Respecto a la etapa de redacción del informe de la auditoría, que recogerá las características del trabajo realizado y sus conclusiones y recomendaciones o propuestas de mejora, quiero recoger la inquietud, que compartimos los integrantes de nuestra dirección de Auditoría, por el tiempo que nos está requiriendo: lo consideramos excesivo, tanto en horas de dedicación como en avance del calendario. Son de aplaudir iniciativas como la propuesta en el artículo "The single page audit report", de Francis X. Bossle y Alfred R. Michenzi, publicado en la revista *Internal auditor* de abril de 1997, que por nuestra parte estamos dispuestos a experimentar.

- En cuanto a la etapa de implantación de las mejoras identificadas en la auditoría, simplemente quisiera lanzar un reto: la situación óptima a alcanzar es conseguir que la organización auditada asuma las propuestas de actuación para implantar las recomendaciones como objetivos de la organización, iniciativa con la que gratamente nos hemos visto sorprendidos en un reciente trabajo en nuestra empresa; ésta es la mejor señal de valoración positiva por parte de una organización a un trabajo de auditoría.

## 19.5. CONCLUSIONES

La **creciente importancia asignada a los sistemas de información** como ayuda inestimable e imprescindible en el desarrollo de los procesos de negocio, aportando no ya información, sino conocimiento –se está demandando– que apoye la correcta toma de decisiones *atribuye esa misma importancia a la auditoría de las aplicaciones informáticas*, garantes del correcto cumplimiento de la función encomendada a las mismas. Efectivamente, si la base de la toma de decisiones no es segura, fiable y confidencial los resultados pueden ser exactamente los contrarios a los pretendidos.

Por otro lado **el enorme y continuo avance tecnológico en este terreno y la apertura de los sistemas al exterior, exige un gran esfuerzo de formación a los auditores informáticos,** que debe ser cuidadosamente planificado, para poder seguir ofreciendo las garantías mencionadas en un **entorno cada vez más amenazado por nuevos riesgos,** *entrañados en esas mismas tecnologías.* Téngase en cuenta que las amenazas son de tal calibre, que pueden llegar al extremo de poner en peligro la supervivencia de aquellas empresas que fracasen en el empeño de tener bajo control el conjunto de la función informática que da soporte a sus sistemas de información.

## 19.6. LECTURAS RECOMENDADAS

Manuales de Auditoría informática de las empresas de Auditoría y Consultoría.

Metodología de Auditoría "AUDINFOR", del Instituto de Auditores Internos de España (incluye programa informática).

Handbook of EDP Auditing, de Stanley D. Halper, Glenn C. Davis, P. Jarlath O'Neil-Dunne y Pamela R. Pfau (COOPERS & LYBRAND).

Systems auditability & control, compilado por: The Institute of Intemal Auditors, Inc. Researched by: Stanford Research Institute.

## 19.7. CUESTIONES DE REPASO

1. ¿Qué fines persigue una aplicación informática?

2. Enumere las principales amenazas que pueden impedir a las aplicaciones informáticas cumplir sus objetivos.

3. ¿Qué es una "pista de auditoría"?

4. Explique en qué ocasiones utilizaría la técnica de encuesta frente a la de entrevista.

5. ¿Cuándo se deben llevar a cabo pruebas de conformidad? ¿Y pruebas substantivas?

6. Valore la importancia del manual de usuario para la auditoría de aplicaciones.

7. ¿Qué aspectos se deben considerar en la preparación del plan de trabajo detallado?

8. Proponga técnicas para medir el nivel de satisfacción del usuario con el modo de operar de las aplicaciones.

9. ¿Cómo verificaría el grado de fiabilidad de la información tratada por una aplicación?

10. ¿Cree conveniente que el auditor tenga autorización para actualizar datos de las aplicaciones que está auditando?