Seguridad y Auditoría Informática

Auditoría Informática: Herramientas y Etapas

Ing. Alfredo Pardo

Año 2021

Tabla de Contenidos

Auditoría Informática - Herramientas y Etapas

Herramientas de uso más común en la Auditoría de una Aplicación

Entrevistas

Las entrevistas deben cumplir una serie de requisitos:

- Las personas a entrevistar deben ser aquellas que más pueden 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.
- Debe 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 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 procesos.
- 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.

Encuestas

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

usuarios. La mayor parte de los requisitos enumerados para las entrevistas son también de aplicación para las encuestas.

- En este caso, 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 respuestas 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.
- Aunque no puede ni debe exigirse la identificación personal del encuestado, sí debe hacerse de la organización a la que pertenece. 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.

Observación del Trabajo Realizado por los Usuarios

Es conveniente observar cómo algún usuario hace uso de aquellas transacciones más significativas por 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, 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 que 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.

Pruebas de Conformidad

Son actuaciones orientadas específicamente a comprobar que determinados procedimientos, normas y controles internos, particularmente los que merecen confianza de estar adecuadamente establecidos, cumplen o funcionan de acuerdo con lo previsto y esperado, según lo puntualizado 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 implica evidencia pero, si parten de varias personas, es probable que la organización asuma como válidos dichos testimonios y, por tanto, las consecuencias de que los mismos pudieran derivarse de cara a posibles recomendaciones, ahorrando esfuerzos para tratar de conseguir su confirmación documental.

Pruebas Sustantivas o de Validación

Orientadas a detectar la presencia o ausencia de errores o irregularidades en procesos, actividades, transacciones o controles internos integrados en ellos. 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.
    - Transacciones con información errónea, desde su origen o por alteración posterior, que no refleja la realidad, con posibles consecuencias en:
        - El monto o fechas de vencimiento 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 inventarios.
    - 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 de herramientas informáticas:
        - 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, recibos, etc.) y Confirmación de saldos por parte de terceros (clientes y proveedores).

Uso de Equipos Informáticos

- El uso de computadoras constituye una de las herramientas más valiosas en la realización de la auditoría de una aplicación informática. Nos referimos tanto a los computadoras personales, con las que el auditor informático debe estar familiarizado manejando con soltura las técnicas de edición de textos y presentaciones, hojas de cálculo, gestor de bases de datos, correo electrónico, etc., como a la computadora o computadoras 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 circulares, 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 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 la computadora 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 implementados. 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.

Etapas de la Auditoría de una Aplicación Informática

Obtención 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 obtenemos 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 la organización, para poder transmitir al responsable de la auditoría el conocimiento más

amplio posible sobre 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 del 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 e 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 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 servidores asignados, número de mini o micro computadoras asignadas 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 informáticos, volumen de capturas, volumen de información almacenada en los archivos maestros, seguridades de explotación (accesos, protección, 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 por cada proceso, de tiempos de respuesta de transacciones online, 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.

Determinación de los Objetivos y Alcance de la Auditoría

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.

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 sub-objetivos para cada uno de los objetivos generales.
    - Asociación, a cada sub-objetivo 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.
        - Soporte 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.
    - Protecciones.
- **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.

Planificación de la Auditoría

La auditoría de una aplicación informática debe tener una planificación cuidadosa. Es muy importante elegir el momento adecuado para su realización:

- Por una parte no conviene que coincida con el período de su implementación, especialmente crítico, en que los usuarios no dominan todavía la aplicación y están agobiados con la tarea diaria. En el período próximo a la implementación, 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.
- También hay que establecer el ámbito de actuación: tratándose de organizaciones distribuídas en amplias zonas territoriales, será necesario delimitar el campo de actuación de la mayor parte de las pruebas a realizar a un número reducido 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 costo desproporcionado.
- 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.

- Deben conseguirse las autorizaciones necesarias para que el personal de auditoría pueda acceder a la aplicación y a las herramientas de usuario.

Trabajo de Campo, Informe e Implementación de Mejoras

- 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 ampliar la profundidad de algunas pruebas, a cometer otras no previstas y concluir algunas antes de su final.
- Respecto a la etapa de redacción del informe de auditoría, que recogerá las características del trabajo realizado y sus conclusiones y recomendaciones o propuestas de mejora, inquieta el tiempo que requiere el cual se considera excesivo, tanto en horas de dedicación como en avance del calendario.
- En cuanto a la etapa de implementación de las mejoras identificadas en la auditoría, la situación óptima a alcanzar es conseguir que la organización auditada asuma las propuestas de actuación para implementar las recomendaciones como objetivos de la organización; ésta es la mejor señal de valoración positiva por parte de una organización a un trabajo de auditoría.