CAPITULO I

AUDITORIA DE APLICACIONES

1.1 Definición

Es la revisión que se dirige a evaluar los métodos y procedimientos de uso de aplicaciones o sistemas de información en una entidad, con el propósito de determinar si su diseño y aplicación son correctos y comprobar el sistema de procesamiento de información como parte de la evaluación de control interno; con el fin de identificar aspectos susceptibles para mejorar o eliminarse.

Las aplicaciones o sistemas de información son uno de los productos finales que genera la infraestructura de la Tecnología Informática en las organizaciones y por ende son el aspecto de mayor visibilidad desde la perspectiva de negocio.

La importancia de una auditoría de aplicaciones según lo expuesto anteriormente radica en el control, eficiencia y eficacia de los sistemas informáticos.

1.2 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 u/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.
- 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.

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 puede ser garantizada. Además la profesionalidad no inmuniza

contra el cansancio y el estrés. Asumiendo 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. [1]

Y no son éstas las únicas amenazas al normal cumplimiento de la finalidad de las aplicaciones.

- La posibilidad de fallo en cualquiera de los elementos que intervienen en el proceso informático.
- La conexión cada vez más generalizada de las empresas a entornos abiertos como el internet multiplica los riesgos que amenazan la confidencialidad e integridad de la información de nuestros sistemas.

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.

1.3 Tipos de controles

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.
- **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.

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 cualquier criterio que ayude a

[1] Introducción, tipos de amenazas, mitos sobre seguridad Auditing Web Applications, NileshChaudhari. Pag145

asegurar la corrección formal y verosimilitud de los datos (la exactitud solo la garantiza el usuario).

- **Controles detectivos:** Tratan de descubrir a posteriores errores que no haya sido posible evitar.
- **Controles correctivos:** Tratan de asegurar que se subsanen todos los errores identificados mediantes 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 realizada.
- En la generación de informes y resultados de salida.

CAPITULO II

ETAPAS DE LA AUDITORÍA DE UNA APLICACIÓN INFORMÁTICA:

2.1 Recogida de información y documentación sobre la aplicación.

Antes de plantear el alcance de los trabajos de auditoría sobre aplicaciones informáticas se necesita disponer de un conocimiento básico de la aplicación y de su entorno. Realizar un estudio preliminar en el que se recoge toda aquella información que 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.

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.

2.2 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. 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 asignaciones 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.
    - 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 salidas: Clasificación y verificación de las salidas, presentación distribución, diseño, y forma de los listados.
    - Pistas para el control y auditoría.
    - Salvaguardias.
- Test de confirmación, test 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.

2.3 Objetivos de auditoría de aplicaciones.

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.
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.

3. Emitir opinión sobre la idoneidad del sistema de control de accesos de la aplicación.
4. Verificar el grado de fiabilidad de la información.
5. Llevar a cabo la revisión de los métodos utilizados para el desarrollo del sistema computacional de una empresa
6. Evaluación del Control Interno de las Aplicaciones, el cual debe permitir el diseño de nuevos programas desarrollados a la medida de la empresa.
7. Evaluación de todo sistema computacional, en cuanto a la funcionalidad y objetividad del mismo, dado que este debe ser aprobado por el usuario; quien será el responsable de su mantenimiento y desarrollo.
8. Evaluación de la administración adecuada de las bases de datos, puesto que estas contienen información vital de toda empresa, las cuales deben tener ciertas restricciones de acceso.
9. Aumento de la productividad, toda evaluación debe buscar la objetividad de los sistemas computacionales, y estos a su vez, deben ser productivos y ser capaces de contribuir al aumento de la productividad de las empresas que los utilizan.
10. Evaluar la seguridad de los sistemas, esto con el afán de evitar fraudes que representen pérdidas significativas para la empresa.
11. Evaluación de aspectos técnicos del sistema, mediante una serie de técnicas que el auditor debe diseñar, y dar el alcance necesario, para que su trabajo satisfaga las necesidades de la auditoría.

2.4 Planificación de 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 alegar 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. 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, procesamientos 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 ponga, en base a razones por las que estime puedan aportar mayor valor al trabajo.

- Debe conseguirse cuanto antes, solicitándolo ya en la primera toma 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.

2.5 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.

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, a cometer otras no previstas y concluir alguna antes de su final.

Una recomendación a esta etapa es la de plantearse la mínima utilización de papeles de trabajo, en el sentido literal, físico, potenciando la utilización de computadoras 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 solo 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.

En cuanto a la etapa de implantación de las mejoras identificadas en la auditoría; 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, ésta es la mejor señal de valoración positiva por parte de una organización a un trabajo de auditoría.

La función de desarrollo es una evolución del llamado análisis y programación de Sistemas y Aplicaciones. Esta auditoría engloba muchas áreas de las empresas, sectores formales e informales de la misma y recorre las siguientes fases:

- Prerrequisitos del usuario y su entorno.
- Análisis funcional
- Diseño
- Análisis orgánico (Pre-programación y Programación)
- Pruebas

- Entrega a explotación y alta para el proceso.

Estas fases deben estar sometidas a un exigente control interno, caso contrario, además del disparo de los costes, podrá producirse la insatisfacción del usuario.Finalmente, la auditoría deberá comprobar la seguridad de los programas en el sentido de garantizar que los ejecutados por la maquina sean exactamente los previstos y no otros.

Una auditoría de Aplicaciones pasa indefectiblemente por la observación y el análisis de cuatro consideraciones:

1. Revisión de las metodologías utilizadas:

   Se analizaran éstas, de modo que se asegure la modularidad de las posibles futuras ampliaciones de la Aplicación y el fácil mantenimiento de las mismas.

2. Control Interno de las Aplicaciones:

   Se deberán revisar las mismas fases que presuntamente han debido seguir el área correspondiente de desarrollo.

3. Satisfacción de usuarios:

   Una aplicación técnicamente eficiente y bien desarrollada, deberá considerarse fracasada si no sirve a los intereses del usuario que la solicitó; la colaboración del usuario proporciona grandes ventajas posteriores, ya que evitará reprogramaciones y disminuirá el mantenimiento de la Aplicación.

4. Control de Procesos y Ejecuciones de Programas Críticos:

   El auditor no debe descartar la posibilidad de que se esté ejecutando un módulo que no se corresponde con el programa fuente que desarrolló, codificó y probó el área de Desarrollo de Aplicaciones.

CAPITULO III

ENFOQUES PARA LA COMPROBACION DE CONTROLES

Existen dos principales enfoques alternativos para probar los controles de aplicación: Probando los resultados y probando el procesamiento.

3.1 PROBANDO LOS RESULTADOS:

El probar los resultados proporciona una inferencia de que si los resultados son correctos, los controles esenciales están funcionando adecuadamente, por ejemplo, si las cuentas por cobrar se confirman a una fecha intermedia y no se encuentran excepciones significativas, podemos inferir que los controles respecto de la actualización del archivo de cuentas por cobrar en cuanto a facturas y pagos, está funcionando adecuadamente.

La desventaja de este enfoque es que las pruebas de resultados pueden dar lugar a que, injustificadamente, se suponga que debido a que las cosas están bien ahora, seguirán estándolo. Esto puede propiciar que ocurran causas de riesgo que podrían haberse conocido con anticipación si los controles hubiesen sido verificados más minuciosamente.

Por muchos años se han utilizado ampliamente tres técnicas en la auditoria no computarizadas de las aplicaciones. Estas técnicas se utilizan principalmente como pruebas sustantivas y pueden llevarse a cabo manualmente o con ayuda del computador.

3.1.1. Confirmación

Se lleva a cabo mediante correspondencia directa con terceros, para corroborar transacciones o saldos.

El ejemplo más común de pruebas de resultados, es la confirmación de las partidas de un archivo de una organización, con los registros de otra persona u organización. Las partidas pueden incluir todo el archivo o una muestra representativa. Típicamente: depósitos en efectivo, cuentas por cobrar, inventarios en consignación, proveedores y otros pasivos.

Los resultados satisfactorios de la confirmación de tales partidas normalmente proporciona bastante seguridad de que el archivo que se está examinando se actualiza correctamente; sin embargo, debe tomarse en consideración que la confirmación es solamente una de las pruebas que integran el procedimiento que se aplicara al archivo de que se trate, es decir, que solamente es un elemento de juicio mas para determinar la razonabilidad del concepto que se esté examinando.

3.1.2 Comparación

Consiste en comparar las partidas que contiene un archivo, con otro archivo independiente o con las partidas físicas que representan.

Un ejemplo frecuente de este tipo de verificación, es la comparación de los archivos de nominas con los registros de personal; en forma similar, los registros en un archivo pueden compararse con las partidas físicas que representan, tales como inventarios, activos fijos, inversiones, etc.

3.1.3. Pruebas de edición y de razonabilidad

La ultima técnica para probar resultados, consiste en la aplicación de una amplia variedad de pruebas de razonabilidad y edición sobre las partidas que se encuentran dentro de los archivos. Con frecuencia tales pruebas sirven para detectar condiciones que no deberían existir si los controles de prevención fuesen efectivos. Si el auditor determina que es posible aplicar, pruebas de edición y razonabilidad para efectos de su auditoria, deberá de preguntarse si también sería útil tenerlas como controles regulares en una aplicación.

La naturaleza especifica de las pruebas de razonabilidad y edición, puede variar ampliamente dependiendo de la imaginación del auditor, de su comprensión de la información y de la importancia que esta tiene para la organización.

3.2 PROBANDO EL PROCESAMIENTO:

La norma internacional ISO-9001 define al proceso como “una actividad que utiliza recursos, y que se gestiona con el fin de permitir que los elementos de entrada se transformen en resultados”.

En ellos se observan numerosas actividades que en realidad están interrelacionadas según una secuencia predeterminada. Estas actividades se realizan de un modo determinado en cada organización, es decir con una determinada metodología.Esa forma de realizarse cada una de esas actividades es lo que se denomina procedimiento en sí. Se dice que cuando el mismo se formaliza en algún medio está documentado. Este conjunto de procedimientos es la base de una organización para el logro de sus objetivos.

La naturaleza, oportunidad y alcance de sus procedimientos dependerán del análisis de riesgos de los procesos sustantivos que hubiera realizado previamente, y más puntualmente en aquellas actividades críticas del proceso.

El “input” es el plan de auditoría y los recursos necesarios para cumplir con los objetivos de la auditoria. El “output” es el conjunto de elementos de prueba válidos y suficientes que permiten respaldar la opinión del auditor de sistemas. El informe de auditoría de sistemas (con las observaciones y recomendaciones) es otro de los “outputs” y el que se constituye en el producto final principal de todo el proceso de auditoría visto integralmente.

Cuando se prueba el procesamiento real, las funciones y controles clave se verifican individualmente. Los porcentajes de error que se detectan en estas funciones y controles se utilizan posteriormente para pronosticar el riesgo.

Las pruebas del proceso real proporcionan un mejor conocimiento de la confiabilidad de cada control individual importante. El principal problema con este enfoque radica en convertir el porcentaje de errores observado; en un riesgo cuantificado.

3.3 Los Procesos y el Auditor de Sistemas

1) Planificación de sus actividades basado en un enfoque de procesos con sus respectivos riesgos.

2) Ejecutar las actividades focalizando en los procesos más críticos para la organización auditada, es decir aquellos vitales para el desempeño normal de la operatoria.

3) Controlar lo planificado vs. Lo realizado. El output del primero de los procesos y el detalle de las actividades realizadas con sus resultados generarán el “input” para este proceso.

4) Mejora continua de los propios procesos de auditoría y respectivas actividades. El “input” de este proceso lo constituye todo el análisis realizado en el proceso anterior y la transformación consiste en el propio rediseño de actividades que permitan incrementar la efectividad. El “output” lo constituye el rediseño de los propios procesos de auditoría.

Ejemplo

El Dr. Leopoldo Pérez trabaja en el área de “Recaudación Tributaria” de un organismo. Es especialista en todo lo referido a Administración Tributaria. Necesita una PC para trabajar. Y con determinados programas instalados. Necesita un acceso a la red corporativa y a un servidor de archivos donde almacena toda la información de su gestión. A un servidor de aplicaciones donde están las aplicaciones que alguien desarrollo para que realice sus actividades. Y que alguien mantiene cuando Leopoldo requiere alguna modificación por alguna nueva ley o cambio en la normativa aplicable. Esta aplicación almacena información de la cual él es propietario y que no puede perder.

También tiene que tener certeza que solo él puede acceder o en todo caso, a quien el designe. Necesita una impresora en su estación de trabajo para imprimir listados de cuentas corrientes de los contribuyentes o acceso a un servidor de impresión donde podrá localizar alguna de las impresoras a las cuales enviar su solicitud de impresión. Necesita una cuenta de correo electrónico.

Leopoldo necesita poder realizar sus operaciones de modo eficiente y eficaz.

Este proceso primario (“Recaudar tributos”) necesita del apoyo de otros tipos de procesos: pero son de incumbencia del área de Sistemas

CAPITULO IV

TECNICAS PARA EVALUAR LOS CONTROLES DE APLICACIONES

Se orientan básicamente a verificar cálculos en aplicaciones complejas comprobar la exactitud del procesamiento en forma global y especifica y verificar el cumplimiento de los controles preestablecidos.

4.1 Auditoria alrededor del computador

Al auditar alrededor del computador, los resultados del procesamiento por computador se verifican manualmente contra los datos fuente alimentados al computador. La verificación se lleva a cabo sin que el auditor participe directamente en el procesamiento dentro del computador.

Este tipo de técnica se aplica sobre la base de muestreo o mediante la comparación de saldos totales; normalmente la misma es eficiente, siempre y cuando exista documentación que pueda verificarse externamente, o bien dicha documentación pueda crearse fácilmente.

- Determinar que existan datos de salida.

- En cada paso importante del procesamiento deben existir listados de transacciones y de datos de cifras de control del archivo que se está procesando, tanto antes como después de la actualización del archivo. Normalmente el listado previo al procesamiento anterior.

- Desarrollar métodos para obtener muestras representativas de las transacciones.

- El muestreo es normalmente necesario, ya que la presencia misma del computador índice que los volúmenes de transacciones son demasiado

grandes para duplicar el procesamiento en forma manual. Las técnicas de muestreo deben asegurar que se prueban tanto las transacciones representativas como las no usuales.

- Verificar manualmente cada control o paso de procesamiento en el que el auditor desee confiar.

  La principal ventaja de la auditoria alrededor del computador es que el personal de auditoría necesita poco entrenamiento técnico de procesamiento electrónico de datos pues el examen se realiza básicamente a nivel lógico. También con este enfoque, no existen limitaciones logísticas relacionadas con el centro de procesamiento de datos, porque no se hace uso del computador y consecuentemente todo el personal de auditoría puede entender fácilmente la documentación y técnicas asociadas a este tipo de auditoría.

Las principales desventajas del enfoque de auditoría alrededor del computador, son que mientras más grande sea el sistema computarizado, menos detallados serán los datos de salida impresos; por lo tanto, será menos factible pretender auditar a su alrededor, pues la auditoria alrededor del computador requiere reportes impresos detallados en cada paso del procesamiento. Cuando los reportes impresos están orientados hacia las excepciones, las pruebas externas detalladas pueden no ser factibles. Cuando la variedad o el volumen de las transacciones es grande, las condiciones a probarse pueden exceder la posibilidad de efectuar pruebas manuales, aun si se utilizan técnicas de muestreo estadístico para seleccionar las transacciones y los datos de salida para su verificaron.

Al aplicar la técnica de auditoría alrededor del computador, el auditor debe hacer lo siguiente:

- Definir los procesos y los controles que van a probarse.

  Como en toda auditoria, es necesario iniciar una auditoria alrededor del computador definiendo los objetivos específicos del trabajo. Con este enfoque el auditor tiene mucha más flexibilidad que con los procedimientos de verificación utilizando el computador, ya que conserva el control sobre sus pruebas y puede aumentar o reducir el alcance de las mismas con base en resultados intermedios.

- Seleccionar las partidas de prueba

  El auditor debe principiar por seleccionar los datos de salida que van a probarse. Después, examina los datos de entrada correspondientes a la aplicación, para determinar la razonabilidad y exactitud de los datos de salida seleccionados. Debe probarse cada dato de salida que sea de interés para el

trabajo de auditoría, incluyendo los listados de excepciones, que indican la efectividad de muchos de los controles de aplicación.

Al auditar alrededor del computador, es deseable probar los datos de entrada hacia atrás, hasta el inicio de las partes de manuales del procesamiento, de modo de probar tanto estas como las partes computarizadas del procesamiento.

- Reprocesar las partidas de prueba

  Una vez que ha identificado los datos de salida y obtenido los datos de entrada correspondientes, el auditor esta lista para efectuar los cálculos de la aplicación. Esto requiere un entendimiento detallado de que debe hacerse y que resultados deben obtenerse.

- Resolver las excepciones

  Si se identifican excepciones en el procesamiento una vez que las pruebas han sido terminadas, el auditor debe darles seguimiento para determinar sus causas y establecer si son resultados de deficiencias de control o de rutinas de procesamiento incorrectas.

4.2 Datos de prueba

Este procedimiento ejecuta programas o sistemas usando conjuntos de datos de prueba (Test decks) y verifica el procedimiento en cuanto a su exactitud comparando los resultados del proceso con los resultados de prueba predeterminados. Los auditores usan esta técnica para probar la lógica del proceso seleccionado, los cálculos y las características del control en el programa.

Tales pruebas pueden incluir cálculos brutos, cálculos de intereses, o validaciones de la entrada de transacciones. Una de las ventajas de estos datos de prueba es que su uso inicial puede estar limitado a funciones de programas específicos, minimizando así, el alcance de la prueba y asimismo su complejidad.

Esta técnica es una buena herramienta de aprendizaje para los auditores[2] porque su uso inicial requiere un mínimo de conocimiento en procesamiento electrónico de datos. Debe aplicarse con mucho cuidado para asegurar que el alcance de la prueba sea él suficiente para proveer evidencia consistente con los objetivos de la auditoria.

Ventajas:

[2] Marvin Cifuentes Velásquez, Diplomado de Auditoría Interna 2008 IGCPA

- Poca experiencia pero debe estar muy familiarizado con la lógica del programa y controles del mismo.

Desventajas:

- Difícil de prever todas las circunstancias.
- Limitan a probar situaciones preconcebidas.
- Un programa diferente podría sustituirse fraudulentamente por el real para satisfacer al auditor y aparentar ser apropiado.

Aplicación de la técnica

a. Define objetivos

- Verifica únicamente aquellas características o controles que el auditor designa en forma explícita.

b. Prepara los datos de prueba

- Desarrolla el o los archivos maestros con las características apropiadas y las transacciones a probar.

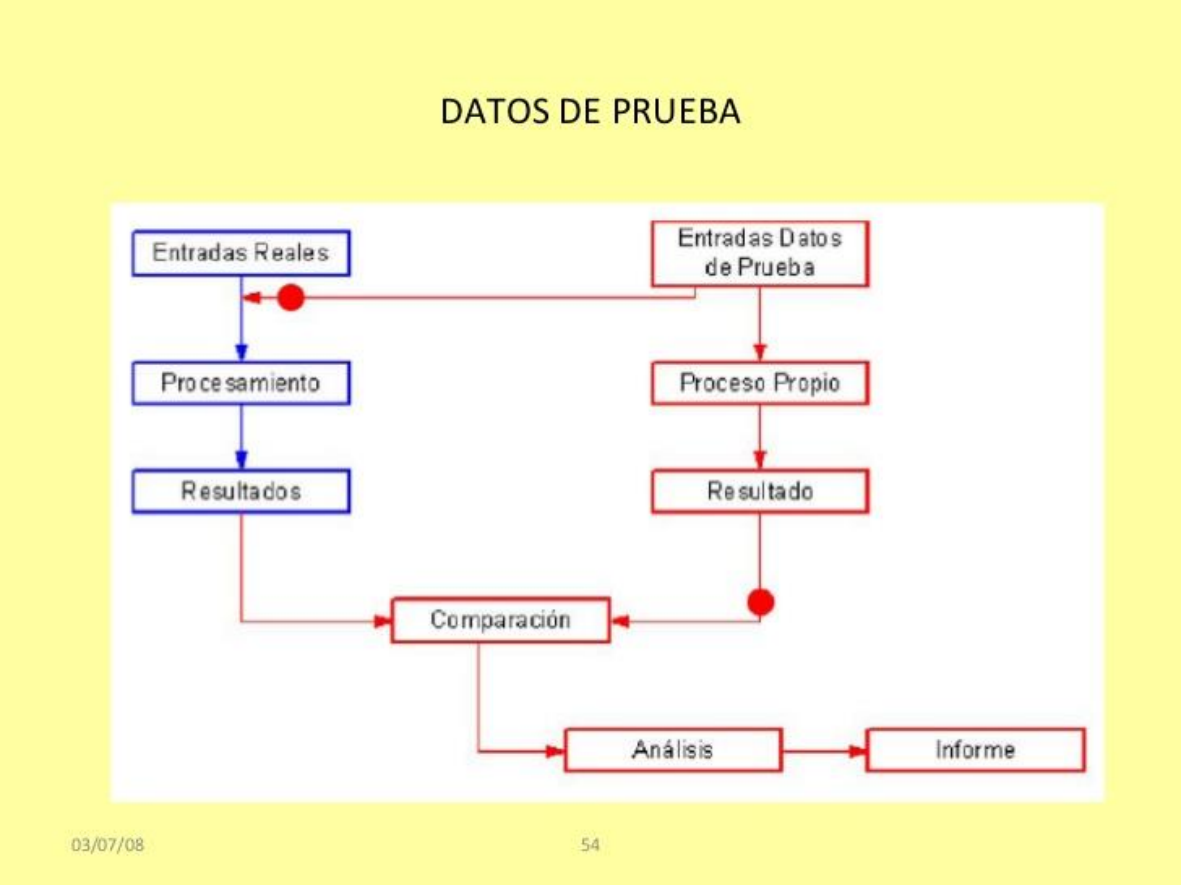
c. Calcula los resultados previstos para el procesamiento

- Efectúa el cálculo previo de los resultados previstos para el procesamiento. Esto se hace mediante uso de datos reales y falsos que se quieren probar.

d. Procesa los datos de prueba a través del computador.

e. Compara los resultados manuales contra los producidos por el computador

f. Resuelve excepciones.



Fuente: www.firma-e.com Proyectos y formación.

4.3 ITF (Instalación De Prueba Integrada)

(I.T.F. =Integrated Test Facility)

Es una técnica para probar los sistemas de aplicación en producción con datos reales evaluándolo en un ambiente normal de producción. Se procesan las transacciones de prueba de una entidad ficticia junto con las transacciones reales de producción. Por esta razón se llama prueba integrada.

Este es un procedimiento para procesar datos de prueba a través de los sistemas concurrente con el proceso de producción y subsecuentemente comparar los resultados de la prueba con los resultados de los datos de prueba predeterminados. Los procedimientos usados en la implementación de una ITF deben ser cuidadosamente planeados para asegurar que los resultados de la producción y que los archivos de datos de la producción no sean efectuados por los datos de prueba.

El alcance de una ITF puede ser limitado para pruebas específicas de funciones de procesamiento o calculo o puede ser diseñada para probar toda la lógica en una aplicación. La característica esencial de una ITF es que la prueba ocurre con el procesamiento de la producción de los datos. Esta técnica tiene la ventaja de permitir pruebas periódicas sin necesidad de procesos separados de prueba. Debe tomarse cuidado, sin embargo, para asegurar que los datos de prueba se aíslen de los datos de producción o que a la inversa se eliminen los datos de prueba en los archivos de producción.

Su objetivo es conocer que hace el programa y la acción de los controles implementados sin detener el funcionamiento normal de la instalación, mezclando los datos de prueba con los datos reales, en la misma aplicación.

Uso:

- Evaluación de controles específicos.
- Verificación de validaciones.
- Prueba de perfiles de acceso.
- Prueba a transacciones seleccionadas.

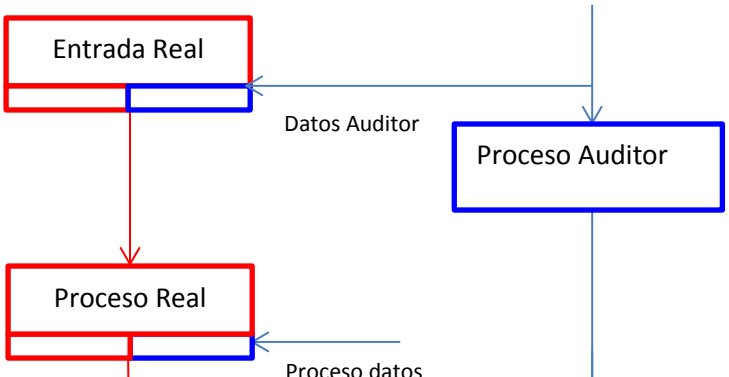
Ventajas:

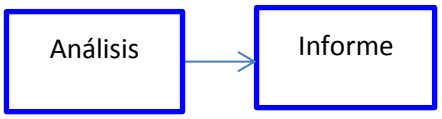
- Se requiere poco entrenamiento técnico.
- Costo de procedimiento bajo debido a que los datos de prueba se procesan junto con los datos de entrada normales.
- Posibilidad de probar el sistema real, tal como opera normalmente.

Desventajas:

- Las transacciones de datos de prueba deben ser eliminadas de los registros de control de la empresa, utilizando modificaciones a los programas.
- Alto costo si los programas deben modificarse para eliminar los efectos de los datos de prueba.
- Posibilidad de destruir archivos.

Diagrama de ITF.





Fuente: www.firma-e.com Proyectos y formación.

CAPITULO V

TECNICAS PARA ANALISIS DE TRANSACCIONES

Tienen como objetivo la selección y análisis de transacciones significativas de forma permanente, utilizando procedimientos analíticos y técnicas de muestreo.

5.1 SCARF (Método Del Archivo De Revisión De Auditoria Como Control Del Sistema)

(SCARF= System Control Audit Review File)

Este procedimiento usa software de auditoría para sustraer y seleccionar transacciones de entrada y transacciones generadas en los sistemas durante el

proceso de producción. Tales subrutinas de auditoría están incluidas en aplicaciones huésped[3].

Las actividades de control, muestreo y reportes de excepción, son controladas por parámetros. El diseño e implementación de tales módulos son altamente dependientes de la aplicación y son generalmente ejecutados como una parte integral del proceso de desarrollo de aplicación. Este método es generalmente referido como SCARF, que significa Sistema Control AuditReview File.

Tiene la ventaja de proveer muestras y estadísticas de producción, incluyendo la entrada y las transacciones generadas internamente. La principal desventaja es su alto costo de desarrollo y mantenimiento y las dificultades asociadas con la independencia del auditor.

Implica la incorporación de controles requeridos por el auditor en los programas de procesamiento normal. Los resultados de esas pruebas se trasladan al auditor para su revisión y posible investigación. Estos controles se establecen en la fase de desarrollo del sistema.

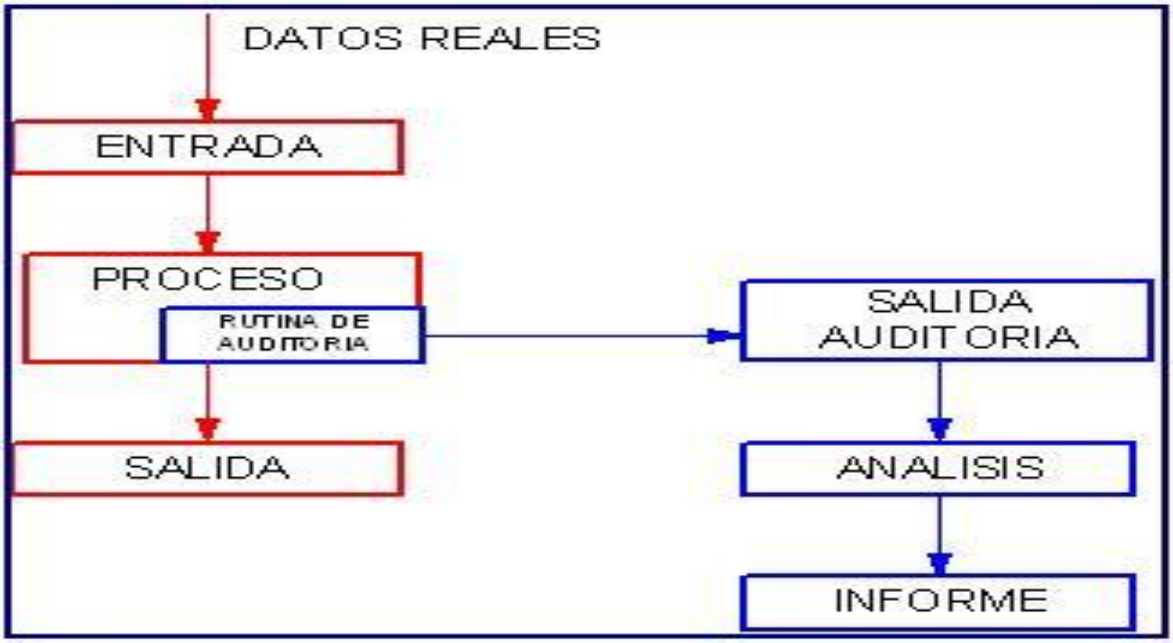
Implantación de la técnica SCARF

a. Los requerimientos del auditor se implantan en los programas de aplicación, junto con el resto del desarrollo de la aplicación.

b. Una vez que se ha implantado el nuevo sistema las excepciones a estas pruebas se registran en un archivo.

c. El archivo de excepciones de auditoría es revisado por el auditor utilizando técnicas manuales o ayudadas por el computador.

d. El auditor sigue la acción que considera apropiada, basado en las excepciones que descubre.



Fuente: www.firma-e.com Proyectos y formación.

En resumen los paquetes de auditoría son usados para control de secuencias, búsquedas de registros, selección de datos, revisión de operaciones lógicas y muestreo

5.2 Etiquetado

(TAGGING – SNAPSHOP)

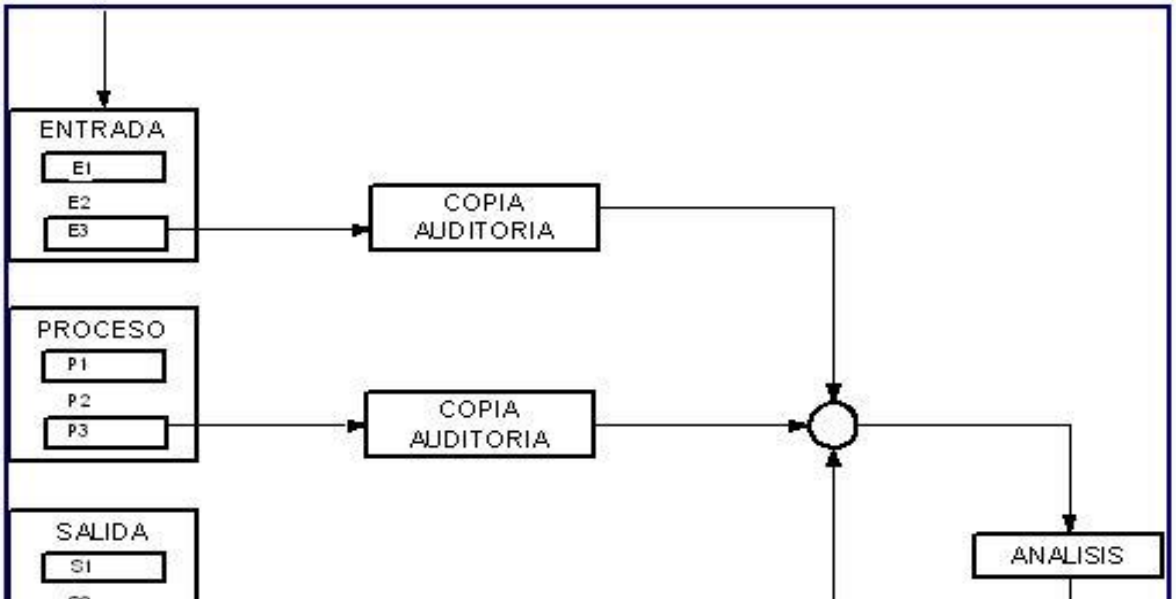
Estas instrucciones de programas o subrutina, reconocen y registran el flujo de las transacciones diseñadas en programas de aplicación. Esta técnica es usada por los auditores para rastrear transacciones específicas por medio de los programas de computador y asegurar la evidencia documental de las relaciones lógicas, condiciones de control y frecuencias de procedimientos. La técnica tiene la ventaja de verificar el flujo de la lógica del programa y consecuentemente ayuda a los auditores en el entendimiento de los pasos del proceso en los programas. Tiene la desventaja de requerir extensos conocimientos de computación y programación, y es generalmente un procedimiento que consume mucho tiempo del auditor.

Esta técnica consiste en:

1. Se marcan algunas transacciones (con una “X” por ejemplo)

2. Se hace que cada vez que estas transacciones pasan por un punto dado del programa, un vuelco instantáneo de unas partes seleccionadas de la memoria del computador que contiene datos relevantes sea y tales datos sean listados.

3. se analiza el comportamiento del programa al trabajar tales transacciones.



Fuente: www.firma-e.com Proyectos y formación.

CAPITULO VI

TECNICAS ADMINISTRATIVAS

Permiten al auditor establecer el alcance de la revisión, definir las áreas de interés y la metodología a seguir para la ejecución del examen.

6.1 Selección del área a auditar

Mediante esta técnica el auditor establece las aplicaciones críticas o módulos específicos dentro de dichas aplicaciones que necesitan ser revisadas periódicamente, que permitan obtener información relevante respecto a las operaciones normales del negocio.

Esta técnica es muy utilizada por los auditores internos de empresas corporativas grandes o medianas con un alto volumen de transacciones y exige que el departamento de auditoría interna construya sus propios aplicativos (con la ayuda

del departamento de sistemas), para que puedan realizar su trabajo de manera eficiente.

Entre los beneficios que se pueden obtener al seleccionar el área específica para auditar destacan:

- Facilitar la organización de las actividades respecto de los objetivos de auditoría.
- Concentración en la identificación y evaluación de lo importante, en base a los riesgos y controles existentes.
- Contribuir a la racionalización de los recursos humanos, técnicos y financieros.
- Fijar líneas de acción para ejecutar programadamente las labores en terreno.
- Guiar la obtención de evidencia de auditoría adecuada y suficiente para respaldar el contenido del informe.
- Presentar evidencia objetiva de la programación de las actividades.
- Explicar la labor del auditor frente a cuestionamientos externos.
- Documentar los procedimientos utilizados.

Las áreas que se pueden seleccionar corresponden con las sujetas a las condiciones de aplicación señaladas a continuación:

- Gestión de Datos.
- Control de Operaciones y aplicaciones.
- Control y utilización de recursos materiales y humanos.
- Interfaces y relaciones con usuarios.
- Planificación.
- Organización y administración.

Supuestos de aplicación:

En función de la definición dada, la selección de áreas es aplicable más a deficiencias organizativas y gerenciales que a problemas de tipo técnico, pero no cubre cualquier área de un Centro de Procesos de Datos.

La selección de áreas puede aplicarse cuando se producen algunas de las situaciones que se citan:

- Se detecta una mala respuesta a las peticiones y necesidades de los usuarios.
- Los resultados del Centro de Procesos de Datos no están a disposición de los usuarios en el momento oportuno.
- Se genera con alguna frecuencia información errónea por fallos de datos o proceso.
- Existen sobrecargas frecuentes de capacidad de proceso.
- Existen costes excesivos de proceso en el Centro de Proceso de Datos.

Efectivamente, son éstas y no otras las situaciones que el auditor de aplicaciones informáticas encuentra con mayor frecuencia. Aunque pueden existir factores técnicos que causen las debilidades descritas, hay que convenir en la mayor incidencia de fallos de gestión.

Objetivos:

La selección del área para realizar la auditoria tiene como objetivo fundamental evaluar el grado de bondad o ineficiencia de los procedimientos y métodos de gestión que se observan en un centro de proceso de datos. Las recomendaciones que se emitan como resultado de la aplicación de dicha selección, tendrán como finalidad algunas de las que se relacionan:

- Identificar y fijar responsabilidades.
- Mejorar la flexibilidad de realización de actividades.
- Aumentar la productividad.
- Disminuir costes
- Mejorar los métodos y procedimientos de Dirección.

Alcance:

Se fijarán los límites que abarcará la selección del área, antes de comenzar el trabajo.

Se establecen tres clases:

- Reducido. El resultado consiste en señalar las áreas de actuación con potencialidad inmediata de obtención de beneficios.

- Medio. En este caso, la selección ya establece conclusiones y Recomendaciones, tal y como se hace en la auditoría informática ordinaria.

- Amplio. La selección incluye Planes de Acción, aportando técnicas de implementación de las Recomendaciones, a la par que desarrolla las conclusiones.

6.2 Simulación y modelación

6.2.1 Simulación

Es un medio que experimenta con un modelo detallado de un sistema real para determinar cómo responderá el sistema a los cambios en su estructura o entorno, se podría afirmar que la simulación permite experimentar con un modelo del sistema para comprender mejor los procesos, con el fin de mejorar la actividad en las empresas. Esta pretende imitar el comportamiento del sistema real, evolucionando como éste, pero lo más frecuente es estudiar además la evolución del sistema en el tiempo.

A nivel de planificación y control estratégicos de una empresa, los modelos de simulación insertan varios inputs a un sistema y proporcionan un modelo para evaluar o volver a diseñar y medir o cuantificar factores tan importantes como la satisfacción del cliente, la utilización de recursos, el proceso de reingeniería y el tiempo invertido en todo ello.

Esta herramienta es una de las más utilizadas para el análisis y diseño de sistemas, pero también puede ser de mucha utilidad para la auditoria de sistemas computacionales, ya que mediante el uso de un modelo, conceptual o físico, se simula el comportamiento de un sistema computacional, de un programa, de una base de datos, de una operación, de una actividad o de cualquier tarea de sistemas que tenga que ser revisada, con el propósito de investigar cuál es, fue o será el comportamiento del fenómeno de sistemas en estudio, bajo ciertas condiciones y características concretas, en las que se presentan todas las simulaciones necesarias que se asemejen al medio ambiente real en donde actúa dicho fenómeno para valorar su auténtico aprovechamiento, sus eficiencias y deficiencias del funcionamiento, sus principales problemas, etcétera.

El uso de esta técnica de simulación es indispensable para el trabajo de los desarrolladores de nuevos sistemas, ya que permite elaborar un ambiente análogo al del nuevo sistema, con el fin de estudiar su posible comportamiento.

Una vez estudiado el posible comportamiento del sistema se puede sacar conclusiones para corregir sus fallas de funcionamiento, así como sus principales problemas antes de implantar dicho sistema. De hecho, todos los analistas de sistemas utilizan modelos conceptuales antes de programar (codificar) un sistema computacional, mientras los programadores elaboran su programación con base a estos modelos.

Tipos de simulación que se pueden aplicar en una auditoria de sistemas:

Simulación a través de modelos de metodología de sistemas.

- Ciclo de Vida de los Sistemas
- Metodología de Kendall & Kendall
- Fases del desarrollo, según James Martín
- Ciclo de vida de los sistemas, según Yourdon
- Análisis y diseño, según Jackson
- Las fases de un proyecto para MERICE
- Metodología SSADM
- Simulación a través de diagramas de flujo de sistemas.
- Simulación a través del diseño de circuitos lógicos.
- Simulación a través de otros documentos gráficos.

6.2.2 Modelación

Esta técnica es muy similar a la de selección de áreas de auditoría, cuya diferencia radica en los objetivos y criterios de selección de las áreas de interés; ya que esta técnica tiene como objetivo medir la gestión financiera de la organización y todo lo que ello involucra

6.3 Punteo Scoring

Aborda situaciones de incertidumbre o con pocos niveles deinformación.Usa una función de valor para cada una de las alternativas. Supone la transitividad de preferencias o la comparabilidad.Completamente compensatorio, y puede resultar dependiente, y manipulable, de la asignación de pesos a los criterios o de la escala de medida de las evaluaciones.

Es un método fácil y utilizado ampliamente en el mundo

Este enfoque es puramente aritmético, y se basa en la percepción realizada por el equipo evaluador sobre la importancia asignada a cada elemento - impacto y probabilidad en el análisis. Una vez que se determinan los puntajes para cada riesgo, pueden ordenarse de mayor a menor para establecer un orden de prioridad.

La puntuación puede computarse de diversos modos:

• Un simple promedio de impacto y probabilidad;

• El producto de multiplicar impacto por probabilidad;

• Un promedio ponderado, donde a uno de los criterios se le asigna mayor peso que al otro.

Etapas

El método del Scoring es una manera rápida y sencilla para identificar la alternativa preferible en un problema de decisión multicriterio.

Las etapas del método son los siguientes:

1. Identificar la Meta General del Problema

2. Identificar las Alternativas

3. Listar los Criterios a emplear en la toma de decisión

4. asignar una ponderación para cada uno de los Criterios

5. Establecer en cuanto satisface cada Alternativa a nivel de cada uno de los Criterios

6. Calcular el Score para cada una de las Alternativas

7. Ordenar las Alternativas en función del Score. La Alternativa con el Score más alto representa la Alternativa a recomendar.

Este método parte del supuesto de que podemos dividir el universo auditable en un conjunto de unidades auditables que pueden ser empresas, procesos o proyectos o áreas objeto de estudio. El método nos permite establecer una calificación del riesgo de cada una de tales unidades, lo cual posteriormente veremos tiene varias aplicaciones muy útiles para la planificación del trabajo de la auditoría.

Otro de los supuestos del modelo es que es posible establecer un conjunto de criterios o factores de riesgo que podemos utilizar para calificar cada uno de las unidades auditables del universo elegido. Tales criterios deben ser los mismos para todas las unidades que estamos calificando.

Habiendo definido un conjunto de áreas auditables y un conjunto de criterios o factores de riesgo, contamos con un modelo para medir los riesgos. Este modelo podemos detallarlo rigurosamente mediante las siguientes etapas[4]:

- Etapa 1: Diseño del Modelo de Riesgo mediante Consenso

Sub-etapa 1.1: Identificar y elegir los Criterios / Factores de Riesgo

- Los criterios a utilizar deben ser acordes con la naturaleza de la organización.
- Medir Riesgos Potenciales / Reales críticos del Negocio.
- Deben reflejar las expectativas de la Alta Gerencia.
- Deben ser aplicables a todo el universo auditables.

Sub-etapa 1.2: Identificar rangos de valoración y puntajes

- Deben definirse a la medida de la organización.
- Debe utilizarse valoración semi-cuantitativa. Esto significa que va a exigir calificaciones en una escala por ejemplo de 1 a 5, pero se van a definir esos valores con base en los rangos de una variable objetiva.

[4]Gonzales, 2000, Auditoria de aplicaciones informáticas. Pags. 56-57

- Deben ser suficientes como elemento diferencial.
- Los rangos y puntajes deben ser los mismos para todos los criterios.

Sub-etapa 1.3: Identificar y Determinar Factores de Ponderación.

- Se asignará un factor de ponderación para cada criterio de riesgo elegido que sea proporcional a la importancia que tenga este criterio para el negocio.
- Para establecer la importancia del criterio de riesgo se pueden determinar las consecuencias y probabilidad estimadas de que se materialicen los riesgos asociados a cada criterio.

- Etapa 2: Levantamiento y Proceso de la Información

Sub-etapa 2.1: Seleccionar los evaluadores y calificar

- Se seleccionan las personas que van a hacer la evaluación (evaluadores) que sean expertos en los procesos a auditar. En esta evaluación pueden participar funcionarios que laboren en las áreas auditables.
- Se les suministra el modelo a los evaluadores y se les brinda asesoría en su utilización.
- Se documentan las fuentes e información de soporte de las calificaciones realizadas.
- Se revisan, validan y consolidan las calificaciones individuales.

Sub-etapa 2.2: Obtención del Mapa de Riesgos

- Se clasifica cada Unidad Auditable por nivel de Riesgo.
- Se realiza la presentación del Mapa de Riesgos y de hallazgos a la Alta Gerencia y propietarios de los procesos, y con base en sus comentarios se realizan los ajustes finales.

Sub-etapa 2.3: Elaboración del Plan Anual de Auditoría

- Se diseña el plan de auditoría.
- Se somete el plan a validación y aprobación de la Alta Gerencia.

A continuación presentamos un cuadro con las categorías genéricas de criterios de riesgo con que podemos contar y algunas de las variables que nos pueden servir para medir dichas categorías de riesgo:

Clasificación general de los criterios/factores de riesgo	
Criterios genéricos de riesgo	Variables de medición
Efecto en el Servicio	• Número de clientes • Tipo de clientes • Número / tipo de reclamos • Efecto en la oportunidad del servicio • Número de usuarios
Materialidad (Pérdidas estimadas)	• Negociabilidad de las transacciones • Estimaciones • Liquidaciones • Valor de los fraudes • Valores controlados • Valor / costo de recuperación del recurso
Efectos en la Gestión	• Impacto en los planes • Valor agregado • Contribución / comportamiento de

	los costos • Efecto en viabilidad del negocio a mediano y largo plazo • Valor competitivo • Indicadores de desempeño
Regulación Estado (Imagen)	• Efecto en la imagen o la credibilidad • Sanciones potenciales o reales • Número de reportes a entidades reguladoras • Impacto en imagen ante entidades reguladoras.
Sensibilidad (de las transacciones)	• Número de transacciones monetarias / no monetarias • Valor (impacto de los errores en el proceso) • Rutinarias / Estimaciones
Auditabilidad	• Facilidades de bitácoras, rutinas y utilitarios de monitoreo de transacciones • Herramientas de “software” en uso o disponibles para hacer auditorías • Antigüedad, alcance y resultado de la última auditoría realizada
Relativos a la Información	• Valor de la información para el negocio • Importancia de la información en términos de confidencialidad /

	privacidad • Número / tipo de puntos de acceso • Arquitectura (centralizada versus distribuida) • Costo de recuperación de la información

Fuente: González, 2000, págs. 56-57

6.4 Software De Auditoria Multisitio

Es una técnica aplicable a organizaciones que tienen centros de procesamiento electrónico de datos regionales o remotos y un staff centralizado para el desarrollo de sistemas. Esta técnica implica la preparación y distribución centralizada de software de auditoría en forma descentralizada en las diferentes dependencias.

Esta técnica se aplica en organizaciones multinacionales que tienen diferentes centros de procesamiento electrónico de datos. Consiste en instalar un programa o grupo de programas de auditoría en varios centros de procesamiento electrónico de datos para que sean utilizados por los auditores regionales.

Se basa sobre el mismo concepto de los sistemas distribuidos, en el que una organización con varias sucursales u oficinas remotas, dispone de un software de auditoría capaz de ser utilizado en dichas sucursales y a la vez pueda actualizar y almacenar información resultante en una base de datos principal generalmente ubicada en la matriz de la organización.

6.5 Centro De Competencia

Consiste en centralizar la información que va a ser examinada por el auditor, a través de la designación de un lugar específico que recibirá los datos provenientes de todas las sucursales remotas y que luego serán almacenadas, clasificadas y examinadas por el software de auditoria

6.6 Análisis Matricial De Riesgos

Este método utiliza una matriz para mostrar gráficamente tanto las amenazas a que están expuestos los sistemas computarizados como los objetos que

comprenden el sistema. Dentro de cada celda se muestran los controles que atacan a las amenazas.

Una matriz de riesgo constituye una herramienta de control y de gestión normalmente utilizada para identificar las actividades (procesos y productos) de una empresa, el tipo y nivel de riesgos inherentes a estas actividades y los factores exógenos y endógenos relacionados con estos riesgos (factores de riesgo). Igualmente, una matriz de riesgo permite evaluar la efectividad de una adecuada gestión y administración de los riesgos que pudieran impactar los resultados y por ende al logro de los objetivos de una organización.

La matriz debe ser una herramienta flexible que documente los procesos y evalúe de manera integral el riesgo de una institución, a partir de los cuales se realiza un diagnóstico objetivo de la situación global de riesgo de una entidad. Aparte de lo ya mencionado la matriz de riesgos constituye una herramienta clave en el proceso de supervisión basada en riesgos, debido a que la misma nos permite efectuar una evaluación cualitativa o cuantitativa de los riesgos inherentes de cada actividad en estudio y la determinación del perfil de riesgo del proceso.

Los beneficios de la matriz entre otros, son los siguientes:

- Permite la intervención inmediata y la acción oportuna.
- Evaluación metódica de los riesgos.
- Promueve una sólida gestión de riesgos en las industrias.
- Monitoreo continuo.

De esta manera la matriz de riesgo permite establecer de un modo uniforme y consistente el perfil de riesgo de cada una de los proceso y permite profundizar en el propósito de establecimiento de planes de supervisión a fin de que se ajusten a las características específicas de cada empresa.

Formato de matriz utilizado.

Al realizar una matriz de riesgo nos permitirá tener un conocimiento amplio de cada una de las actividades y procesos de la industria en estudio, el formato de las matrices no es estandarizado pudiendo el personal que realice el estudio de riesgos tomar su propio formato y realizar su investigación. Deeste modo se ha realizado un formato de matriz que se adapte de manera apropiada al proceso de obtención de dato y a las labores cotidianas de la empresa.

Partes que debe incluir un análisis matricial de riesgos:

- Nombre de la empresa en estudio.
- Objetivo de la matriz

- Alcance de la matriz
- Proceso al cual estará relacionada la matriz.
- Código de la matriz.
- Numero de actividad.
- Actividades del proceso.
- Responsable de las actividades
- Peligro de la actividad.
- Acciones tanto correctivas como preventivas.

Entre los procedimientos establecidos, se incluye la confección de la Matriz de Riesgos, herramienta fundamental, para evaluar los controles que deben de estar presentes tanto en las aplicaciones como en su entorno. Seleccionadas aquellas funciones que constituyen riesgos y causas de riesgo, pueden ser evaluados con precisión, el éxito alcanzado por cada control, determinando aquellos, que por débiles o insuficientes, actúan adversamente o con un efecto inversamente proporcional al esperado (causas de riesgos).

A manera de ejemplo, se anexa una Matriz de Riesgo que muestra algunas de las relaciones existentes entre controles, causas de riesgos y grado de efectividad que cada uno de ellos posee con distinta probabilidad; de igual forma, se muestra como varias causas de riesgos con distintas probabilidades pueden provocar un riesgo.

El empleo de la Matriz de Riesgo permite obtener señales y advertencias concluyentes sobre los controles existentes y su efectividad real respecto a la esperada. A partir de sus resultados se aplican procedimientos de simulación y comprobación sustantiva, para evaluar controles, sistemas, procedimientos, grado de efectividad de políticas y medidas instrumentadas por la organización en lo que se refiere a garantizar la seguridad física y lógica del hardware y software; confiabilidad de los sistemas; adecuado empleo de los niveles de acceso; mantenimiento sistemático; respaldo de los sistemas; así como efectividad de los planes de medidas contra contingencia, a fin de minimizar riesgos tales como retraso o interrupción del trabajo, mala toma de decisiones, desastres, delitos y otros.

6.6.1 Realización del análisis matricial de riesgos

Clasificación de los riesgos

Evaluación.- Es el resultado de comparar los niveles de riesgo establecidos, con los criterios que se tienen preestablecidos para su evaluación. En este caso los criterios son los siguientes:

a) Probabilidad de ocurrencia del Riesgo

b) Impacto ante la ocurrencia del Riesgo.

Para ello:

- Las probabilidades de ocurrencia deberán determinarse en:

  a. Poco Frecuente (PF): cuando el Riesgo ocurre sólo en circunstancias excepcionales.

  b. Moderado (M): Puede ocurrir en algún momento.

  c. Frecuente (F): Se espera que ocurra en la mayoría de las circunstancias.

- El Impacto ante la ocurrencia sería considerado de:

  a. Leve (L): Perjuicios tolerables. Baja pérdida financiera.

  b. Moderado (M): Requiere de un tratamiento diferenciado: Pérdida financiera media.

  c. Grande (G): Requiere tratamiento diferenciado. Alta pérdida financiera.

La evaluación del Riesgo sería de:

Aceptable: (Riesgo bajo). Cuando se pueden mantener los controles actuales, siguiendo los procedimientos de rutina.

Moderado: (Riesgo Medio). Se consideran riesgos aceptables con medidas de control. Se deben acometer acciones de reducción de daños y especificar las responsabilidades de su implantación y supervisión.

Inaceptable: (Riesgo Alto). Deben tomarse de inmediato acciones de reducción de impacto y probabilidad para atenuar la gravedad del riesgo. Se especificará el responsable y la fecha de revisión sistemática.

Si se quisiera evaluar el impacto de los riesgos en un subproceso, se utiliza un estándar el que se muestra a continuación:

Para evaluar, se utiliza el estándar, donde se identifican todos los riesgos de cada uno de los subprocesos diagnosticados anteriormente, y se evalúan en conformidad con lo previsto anteriormente.

UAI: _____	Clasificación del Riesgo									
No.	Riesgo	E	I	Impacto (6)			Probabilidad (7)			Nivel de Riesgo
				L	M	G	F	M	PF	

Fuente: González, 2000, pág. 60

La evaluación de riesgos proporciona la lista de prioridades para el tratamiento de los riesgos por medio de las acciones a seguir en cada caso.

Se deben tener en cuenta los objetivos de la organización y el grado de oportunidad que se puede alcanzar como resultado de tratar el riesgo. Se tendrá en cuenta, también, el grado de beneficio para las partes involucradas.

6.6.2 Mapa de los Riesgos

Luego de evaluado todos los riesgos, se sitúan en el cuadrante del Mapa que le corresponde según la Matriz. Resulta una técnica conocida y muy usada, como herramienta de trabajo, la representación gráfica.

Se ilustra a continuación:

	MATRIZ DE RIESGOS			
PROBABILIDAD	Frecuente	Inaceptable	Inaceptable	Inaceptable
	Moderado	Moderado	Moderado	Inaceptable
	Poco Frecuente	Aceptable	Moderado	Inaceptable
		Leve	Moderado	Grande
		IMPACTO		

González, 2000, pág. 61

6.6.3 Niveles del análisis matricial

Como puede observarse, el gráfico anterior ilustra los cuadrantes donde según su impacto y probabilidad de ocurrencia se sitúan estos riesgos, y su color identifica la evaluación del mismo, lo que no significa que en el pplan de medidas no se tengan en cuenta todos los riesgos, pues deberá mantenerse el seguimiento de todos los identificados y el plan de acción de cada uno.

Las opciones a tener en cuenta para realizar acciones de reducción de riesgos pueden ser:

- Evitarlo
- Reducir probabilidad de ocurrencia
- Reducir consecuencias
- Transferir el riesgo
- Retener el riesgo

Luego estas opciones deberán evaluarse y tener en cuenta el costo beneficio de la decisión de tratamiento del riesgo.

Se confeccionarán planes de tratamiento de riesgos. En los mismos se tendrá en cuenta:

- El riesgo en orden de prioridad
- Opciones posibles de tratamiento
- Nivel que adquiere el riesgo luego de ser tratado
- Resultado del análisis costo beneficio
- Responsable de acometer la acción
- Calendario de implementación
- Forma en que se va a monitorear

El Plan de Acción estaría en correspondencia con el tipo de riesgo, con la organización donde se realiza el servicio, con el tipo de auditoría, con el subproceso que se realice y por supuesto con el auditor o auxiliar que la ejecute.

Vital importancia reviste el dominio de la actividad, el monitoreo en la ejecución sucesiva sobre el manejo de futuras acciones y la supervisión sistemática en diferentes momentos de realización de las auditorías en correspondencia sobre la incidencia de los riesgos pasados o reiterados en los subprocesos con mayores impactos. Las organizaciones de auditoría deben elaborar planes de acción que contribuyan a la preparación del auditor sobre el cumplimiento del ejercicio de la profesión.

6.6.4 Plan de Acción

El plan de acción estaría en correspondencia con el tipo de riesgo, con la organización donde se realiza el servicio, con el tipo de auditoría, con el subproceso que se realice y por supuesto con el auditor o auxiliar que la ejecute. Vital importancia reviste el dominio de la actividad, el monitoreo en la ejecución sucesiva sobre el manejo de futuras acciones y la supervisión sistemática en diferentes momentos de realización de las auditorías en correspondencia sobre la incidencia de los riesgos pasados o reiterados en los subprocesos que mayores impactos se han observados.

Por el impacto que hoy produce la ocurrencia de los riesgos observados en la investigación, debe elaborarse un plan de acción en el que se proponga, fundamentalmente.

- El diseño de un sistema organizativo de ejecución para cada uno de los subprocesos de la auditoría.
- Capacitar a los profesionales de la auditoría en la formación teórico-práctica que garantice la calidad en el ejercicio de sus funciones.
- Evaluar los resultados de las supervisiones
- Mantener la vigilancia de la posible comisión de riesgos en el desarrollo sistemático del ejercicio de las auditorías.

Responsables:

- Departamento de Auditoría
- Supervisor
- Jefe de Grupo
- Auditor

Estándares:

Consiste en Guías, con determinado aspectos a evaluar, por cada subproceso, el cual debe concluir con una evaluación, la que deberá clasificar según la probabilidad de ocurrencia y el Impacto ante la misma.

- Deberá además de resumirse, representarse en un gráfico, con el fin de elaborar el consecuente plan de acción para reducir la probabilidad de ocurrencia.

Controles:

Frecuentemente debe evaluarse el comportamiento de cada subproceso y por cada área de trabajo.

Resulta importante establecer un sistema de control en esa cadena de valores, donde todos los subprocesos en Auditoría son necesarios para lograr un servicio eficaz, y eficiente, con los requerimientos de calidad esperada. Una administración eficiente de los riesgos, sería entonces una aproximación científica de su comportamiento, anticipando posibles pérdidas accidentales con el diseño e implementación de procedimientos que minimicen la ocurrencia de pérdidas o el impacto financiero de las pérdidas que puedan ocurrir.

CAPITULO VII

HERRAMIENTAS

7.1 Observación O Monitoreo

Es la aplicación de diversas técnicas y métodos de observación que permiten recolectar directamente la información necesaria sobre el comportamiento del sistema, del área de sistemas, de las funciones, actividades y operaciones del equipo procesador o de cualquier otro hecho, acción o fenómeno del ámbito de sistemas.

A fin de recolectar los datos suficientes, se hace necesario, precisamente, observar los fenómenos en cuestión con objeto de determinar si existe.

Existen distintas formas de Observación siendo las principales:

- Observación Directa
- Observación Indirecta
- Observación Oculta
- Observación Participativa
- Observación No Participativa
- Introspección
- Experimentación
- Observación Histórica
- Observación Controlada
- Observación Natural

7.2 Observación Directa

Es la inspección hecha directamente en el contexto donde se presenta el hecho o fenómeno observado, a fin de contemplar todos los aspectos inherentes al comportamiento, conducta y características de ese ambiente.

En otras palabras el auditor ve directamente los procesos o procedimientos del objeto observado. Hay dos formas en que el auditor realiza esta tarea: de forma aislada solamente observando o de forma participativa formando parte del proceso.

7.3 Observación Indirecta

Es la observación del hecho o fenómeno en estudio, pero sin que el observador ingrese en contacto directo con el aspecto observado, sino que lo examina por medios indirectos, ya sea por referencias o comparaciones; para lograr lo anterior.

De esta forma el auditor puede saber exactamente cuál es la forma en que se desarrollado realmente algún sistema o gestión de informática.

7.4Observación Oculta

Es cuando el observador, por las necesidades propias de la evaluación, permanece oculto para observar el fenómeno que está auditando, sin que los involucrados noten su presencia.

Relacionada con la observación indirecta lo que se pretende con este tipo de observación es que el sistema y sus operadores se desarrollen en el ambiente normal o cotidiano, para que no sufra ninguna alteración.

7.5 Introspección

En una auditoria se entiende como la observación interna del fenómeno, es decir es la investigación en la que se observa desde el interior del propio hecho en estudio. Su propósito es entender mejor el comportamiento del fenómeno, sus características y su desenvolvimiento.

La introspección pues es el estudio de la estructura de un sistema computacional a fin de evaluar su calidad y capacidad de procesamiento de información. Buscando detectar cualquier deficiencia para ser corregida y así poder tener la seguridad de la información que se procesa.

7.6Experimentación o Simulación

Ésta es una de las herramientas más utilizadas en cualquier tipo de auditoría y una de las que más ayudan al auditor a recopilar la información que se requiere para realizar una auditoría de sistemas; el auditor puede aplicar esta herramienta por sí mismo o ayudándose de algún instrumento de registro, en el que recopilará los datos que le servirán para la evaluación.

Existen varios tipos de experimentos entre los que podemos mencionar:

- Experimentos Exploratorios
- Experimentos Confirmatorios
- Experimentos Cruciales

- Experimentos Exploratorios

Son los experimentos cuyo objetivo fundamental no es demostrar una suposición del comportamiento del fenómeno o sistema en evaluación, sino investigar si las técnicas, métodos procedimientos que serán usados serán útiles para llevar a cabo una evaluación correcta.

Lo que se busca con este tipo de simuladores es analizar y examinar los sistemas que serán evaluados, antes de iniciar con el estudio formal.

- Experimentos Confirmatorios

Mediante los experimentos confirmatorios se pueden corroborar o desmentir las sospechas de desviaciones que dieron origen a la realización de la auditoría. Es importante establecer que con este tipo de experimentación se busca confirmar los resultados de la suposición inicial de una desviación, ya sea para probar que ésta existe o para refutar su presencia en el ambiente de sistemas auditado.

- Experimentaciones Cruciales

Este tipo de experimentaciones pone a prueba algunas de las suposiciones planteadas en el programa de auditoría, las cuales se supone que son de los aspectos relevantes del ambiente de sistemas que será evaluado. Es importante recalcar que con las experimentaciones bajo estas circunstancias se busca obtener un verdadero conocimiento del sistema en evaluación, a fin de comprobar o desmentir cualquier situación mediante la experimentación.

El más claro ejemplo que existe de este tipo de experimentación, es la que se debió realizar para verificar el funcionamiento de los sistemas para el año 2000, ya que fue necesario analizar todos los aspectos cruciales que hubieran podido repercutir en el funcionamiento de los sistemas.

Entre los aspectos que intervienen en la experimentación entre los más destacados podemos determinar los siguientes:

- ✓ Constante
- ✓ Variable
- ✓ Variables independientes
- ✓ Variable independiente

- ✓ Variables recurrentes
- ✓ Variables ajenas
- ✓ Variables discretas
- ✓ Causalidad
- ✓ Temporalidad
- ✓ Control de los factores de causalidad
- ✓ Variaciones concomitantes
- ✓ Comparabilidad
- ✓ Fuentes de invalidación
- ✓ Factores ambientales
- ✓ Medición
- ✓ Instrumentación
- ✓ Maduración
- ✓ Regresión
- ✓ Selección
- ✓ Deserción

CONCLUSIONES

Se ha analizado simplemente algunos de los múltiples aspectos relativos a la seguridad en las aplicaciones web. Se cubrieron las partes más importantes del tema, siendo suficiente para comprobar lo fácilmente que puede ser vulnerada una aplicación cuando no se le asigna una prioridad adecuada a los controles de seguridad en las distintas etapas de desarrollo.

La presente realidad de las entidades conlleva a implementar los controles mediante la auditoria de aplicaciones en forma adecuada, en particular la creciente complejidad y variedad de tecnologías incrementa de la misma forma la variedad de puntos vulnerables y técnicas. Muchas de las vulnerabilidades que se pueden presentar son propias de la plataforma sobre la que se desarrolla la aplicación, como el sistema operativo, software de bases de datos, herramientas de desarrollo, otras son negligencia por parte de jefes de proyecto o de departamentos, arquitectos, diseñadores, programadores, administradores y usuarios del sistema.

Se desarrollaron varias medidas de control, que deben ser implementadas en el marco de políticas de seguridad establecidas en la entidad, ejecutadas en varias fases distintas del ciclo de vida de la aplicación, y controladas por un auditor, que permiten disminuir considerablemente los riesgos e impacto de estas amenazas vistas, aunque difícilmente sea posible asegurar la invulnerabilidad de una aplicación.

La auditoría de aplicaciones se desarrolla en un campo amplio la cual puede tener diferentes enfoques y puede ser utilizada de diferentes maneras las cuales dependerán de los objetivos que se pretende alcanzar y de las delimitaciones que establecidas por el alcance, así mismo, el auditor debe de establecer las mejores herramientas y técnicas que deben de ser utilizadas para la realización del trabajo de campo, por otra parte se debe de tener en cuenta las delimitaciones o problemas que se enfrentaran al momento de realizar la auditoria y estos deben de ser planteados desde la planeación del proyecto.

RECOMENDACIONES

Para el buen desempeño de la auditoria de aplicaciones recomendamos:

- Capacitar de manera adecuada al personal que realizara las auditorias, así mismo, asignar los adecuados recursos que serán utilizados.

- Realizar una adecuada delimitación del objetivo y resultado que se espera alcanzar para que el trabajo se ajuste a las necesidades que se pretenden cubrir.

- Que el auditor unifique y utilice técnicas y procedimientos como la auditoria sin computadora y con computadora, así mismo, la auditoría de gestión informática.

- Evaluación de los niveles de seguridad de las aplicacionesweb de la organización.

- Mejorar de la seguridad en empresas convencionalesreduciendo el riesgo derivado de una intrusiónque permita el sabotaje o robo de información.

- Aplicar la auditoria de aplicaciones para ahorrar tiempo y dinero al afrontar y corregirsituaciones negativas antes de que sucedan.

- Tener un adecuado mantenimiento y mejorar de la imagen corporativa y revalorización de la confianza en la empresa delos clientes, proveedores y empleados al garantizarla continuidad de negocio.

ANEXOS

RESUMEN

AUDITORIA DE APLICACIONES

Es la revisión que se dirige a evaluar los métodos y procedimientos de uso de aplicaciones o sistemas de información en una entidad, con el propósito de determinar si su diseño y aplicación son correctos y comprobar el sistema de procesamiento de información como parte de la evaluación de control interno; con el fin de identificar aspectos susceptibles para mejorar o eliminarse. Las aplicaciones o sistemas de información son uno de los productos finales que genera la infraestructura de la Tecnología Informática en las organizaciones y por ende son el aspecto de mayor visibilidad desde la perspectiva de negocio. La importancia de una auditoria de aplicaciones radica en el control, eficiencia y eficacia de los sistemas informáticos.

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.
- **Controles automáticos:** Incorporados a los programas de la aplicación.

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.
- **Controles detectivos:** Tratan de descubrir a posteriores errores que no haya sido posible evitar.
- **Controles correctivos:** Tratan de asegurar que se subsanen todos los errores identificados mediantes controles detectivos.

Objetivos de auditoría de aplicaciones.

12. Emitir opinión sobre el cumplimiento de los objetivos, planes y presupuestos
13. Evaluar el nivel de satisfacción de los usuarios del sistema
14. Emitir opinión sobre la idoneidad del sistema de la aplicación.
15. Verificar el grado de fiabilidad de la información.

Etapas de la auditoría de una aplicación informática:

- Planificación de auditoría
- Recogida de información y documentación sobre la aplicación: Determinación de los objetivos y alcance de la auditoría
- Trabajo de campo, informe e implantación de mejoras

Una auditoría de Aplicaciones pasa indefectiblemente por la observación y el análisis de cuatro consideraciones:

4. Revisión de las metodologías utilizadas
5. Control Interno de las Aplicaciones
6. Satisfacción de usuarios
7. Control de Procesos y Ejecuciones de Programas Críticos

ENFOQUES PARA COMPROBACION DE CONTROLES

Existen dos principales enfoques alternativos para probar los controles de aplicación: Probando los resultados y probando el procesamiento.

- **Probando los resultados**
- **Probando el procesamiento**

TECNICAS PARA EVALUAR LOS CONTROLES DE APLICACIONES: Se orientan básicamente a verificar cálculos en aplicaciones complejas comprobar la exactitud del procesamiento en forma global y específica y verificar el cumplimiento de los controles preestablecidos. Las cuales incluyen:

- **Auditoria alrededor del computador:** Al auditar alrededor del computador, los resultados del procesamiento por computador se verifican manualmente contra los datos fuente alimentados al computador. La verificación se lleva a cabo sin que el auditor participe directamente en el procesamiento dentro del computador.

- **Datos de prueba:**Este procedimiento ejecuta programas o sistemas usando conjuntos de datos de prueba y verifica el procedimiento en cuanto a su exactitud comparando los resultados del proceso con los resultados de prueba predeterminados.

- **ITF (Instalación De Prueba Integrada):** Es una técnica para probar los sistemas de aplicación en producción con datos reales evaluándolo en un ambiente normal de producción.

TECNICAS PARA ANALISIS DE TRANSACCIONES: Tienen como objetivo la selección y análisis de transacciones significativas de forma permanente, utilizando procedimientos analíticos y técnicas de muestreo.

- **SCARF (Método Del Archivo De Revisión De Auditoria Como Control Del Sistema):** Este procedimiento usa software de auditoría para sustraer y

seleccionar transacciones de entrada y transacciones generadas en los sistemas durante el proceso de producción.

- **Etiquetado:**Estas instrucciones de programas o subrutina, reconocen y registran el flujo de las transacciones diseñadas en programas de aplicación. Esta técnica es usada por los auditores para rastrear transacciones específicas por medio de los programas de computador

TECNICAS ADMINISTRATIVAS: Permiten al auditor establecer el alcance de la revisión, definir las áreas de interés y la metodología a seguir para la ejecución del examen**.**

- **Selección del área a auditar:** Mediante esta técnica el auditor establece las aplicaciones críticas o módulos específicos dentro de dichas aplicaciones que necesitan ser revisadas periódicamente, que permitan obtener información relevante respecto a las operaciones normales del negocio.

- **Simulación:** Es un medio que experimenta con un modelo detallado de un sistema real para determinar cómo responderá el sistema a los cambios en su estructura o entorno.

- **Modelación:** Esta técnica es muy similar a la de selección de áreas de auditoría, cuya diferencia radica en los objetivos y criterios de selección de las áreas de interés; ya que esta técnica tiene como objetivo medir la gestión financiera de la organización y todo lo que ello involucra

- **Punteo Scoring:** Aborda situaciones de incertidumbre o con pocos niveles de información. Usa una función de valor para cada una de las alternativas.

- **Software de auditoría Multisitio:** Esta técnica implica la preparación y distribución centralizada de software de auditoría en forma descentralizada en las diferentes dependencias.

- **Centro de competencia:** Consiste en centralizar la información que va a ser examinada por el auditor, a través de la designación de un lugar específico que recibirá los datos provenientes de todas las sucursales remotas y que luego serán almacenadas, clasificadas y examinadas por el software de auditoría.

- **Análisis matricial de riesgos:** Este método utiliza una matriz para mostrar gráficamente tanto las amenazas a que están expuestos los sistemas computarizados como los objetos que comprenden el sistema. Dentro de cada celda se muestran los controles que atacan a las amenazas.

REFERENCIAS BIBLIOGRAFICAS

- Auditoria En sistemas Computacionales, 1ra edición 2002, Carlos Muñoz Razo, Grupo Editorial Pearson Educación de México, S.A. de C.V.

- Auditoría Informática, Un Enfoque Practico 2da edición 2001, Mario Gerardo Piattini / Emilio del Peso, Editorial Alfaomega Grupo Editorial, S.A. de C.V.

- Marvin Cifuentes Velásquez, Diplomado de Auditoría Interna 2008 IGCPA

- Introducción, tipos de amenazas, mitos sobre seguridadAuditing Web Applications,NileshChaudhari.

- Tergiversar Aplicaciones Web,Joel Scambray and Mike Shema McGraw-Hill/Osborne 2002

- González, 2000, Auditoria en Aplicaciones Informáticas, Novena edición.