



CAATTs
Computer Assisted Audit
Techniques and Tools

Daniel Vargas Madrid

CAATs – Computer Assisted Audit Techniques and Tools

I. INTRODUCCIÓN.....	1
II. NORMAS RELACIONADAS	2
NIA 16 Técnicas de Auditoria con Ayuda de Computadora (TAACs)	2
III. CARACTERISTICAS DESEABLES DE UN SOFTWARE DE AUDITORIA	4
CARACTERÍSTICAS GENERALES	4
CARACTERÍSTICAS DE SEGURIDAD	4
IV. TIPOS DE SOFTWARE DE AUDITORIA	5
1. PLANIFICACIÓN DE LA AUDITORIA	5
1.1. Planning Advisor	5
2. EJECUCIÓN – SUPERVISIÓN	5
2.1. CobiT Advisor	6
2.2. Pro Audit Advisor	6
3. ANÁLISIS DE RIESGOS.....	6
3.1. RISK2K – Pilar - Chinchón	7
3.2. Enterprise Risk Assessor (ERA Lite).....	7
3.3. Risk Assesment Program - RAP	7
3.4. Audicontrol.....	8
4. ANÁLISIS Y EVALUACION DE BASE DE DATOS	9
4.1 ACL: (Audit Command/Control Language)	9
4.2 IDEA: (Interactive Data Extraction and Analysis)	11
4.3 SQL Secure	13
5. HERRAMIENTAS INTEGRADAS	14
5.1. Gestor F1 Audisis.....	14
5.2. Auditor 2000	14
5.2. Audit System 2	15
5.3. TeamMate.....	16
6. PROGRAMAS PARA PROPÓSITOS ESPECÍFICOS.....	17
6.1. Sistema de Auditoria y Seguridad – SAS.....	17
6.2. Statistical Techniques of Analytical Review	18
6.3. DATAS - Digital Analysis Tests And Statistics	18
6.4. Herramientas de Hacking	19

CAATs – Computer Assisted Audit Techniques and Tools

I. INTRODUCCIÓN

Desde el punto de vista de la NIA 16, al hablar de Técnicas de Auditoria con Ayuda del Computador (TAACs), esta parece referirse casi exclusivamente a los programas de “Análisis y Extracción de Base de Datos” como podrían ser desde una planilla electrónica, pasando por un IDEA o ACL y llegando a un nivel de mayor complejidad Access, SQL Server, Oracle por poner algunos ejemplos, reforzando esta impresión que nos da la NIA 16 nos encontramos con una clasificación que realiza Eduardo Leyton Gutierrez al hablar de las CAATs:

BASICOS	INTERMEDIOS	COMPLEJOS
<ul style="list-style-type: none"> • Procesadores de texto (MS Word) • Presentaciones (MS Power Point, FlashMX) • Planillas de cálculo (MS Excel) • Programas estadísticos (SPSS) • Software de producción personal 	<ul style="list-style-type: none"> • ACL (Audit Control Language) • IDEA (Interactive Data Extraction and Análisis) • Productos Methodware: <ul style="list-style-type: none"> ○ Ranking Advisor ○ ProAudit Advisor ○ COBIT Advisor ○ Audit Builder 	<ul style="list-style-type: none"> • ORACLE • SQL Server • Informix • MySQL • MS Access • TOAD

Sin embargo de lo anterior, podemos ser más amplios al hablar de TAACs, y hablar de Técnicas y “**Herramientas**” de Auditoria con Ayuda del Computador, tal como lo expresa el término **CAATs** en inglés. Partiendo de esta ampliación, podemos hacer una nueva clasificación de las TAACs, que desarrollaremos en los apartados III y IV del presente documento que clasifica a las TAACs de acuerdo a las etapas en las que se desarrolla una auditoria: Planificación; Ejecución - Supervisión; Análisis de Riesgos; Análisis y Evaluación de Base de Datos; Herramientas Integradas y Programas para propósitos específicos.

La clasificación mencionada en el párrafo anterior, así como los requisitos generales y específicos de los apartados III y IV, se basan en requisitos técnicos de Licitaciones públicas que establecieron en su momento instituciones como Bancos Centrales y otras organizaciones serias como son: El Banco Central de Nicaragua el 2005; Empresa Portuaria Santo Tomás de Castilla el 2006 (España); Procuraduría de los Derechos Humanos el 2005 (Guatemala); Superintendencia Bancaria de Colombia (2005); Procuraduría General de la Nación el 2005 (Colombia)

II. NORMAS RELACIONADAS

ISA/NIA 15(401): Auditoría en un ambiente de sistemas de información por computadora

ISA/NIA 16(1009): Técnicas de auditoría con ayuda de computadora (TAACs) - **Computer Assisted Audit Techniques. (CAATs)**

ISA/NIA 18(620): Uso del trabajo de un experto

SAS 94: The Effect of Information Technology on the Auditor's Consideration of Internal Control in a Financial Statement audit

Declaración¹ 1: Entornos PED – Microcomputadoras independientes

Declaración 2: Entornos PED – Sistemas de computadoras en línea

Declaración 3: Entorno PED – Sistemas de Base de Datos

Addendum 1 a NIA 6: Evaluación de riesgos y control interno – características y consideraciones de PED

NIA 16 Técnicas de Auditoría con Ayuda de Computadora (TAACs)

La estructura básica de esta NIA se la presenta continuación con una breve descripción de cada punto:

- **Descripción de Técnicas de Auditoría con Ayuda de Computadora (TAACs)**

Software de Auditoría: Son programas utilizados para procesar grandes cantidades de datos generados por la contabilidad de una organización, pueden ser: Programas en paquete, programas escritos para un propósito específico y programas de utilería.

Datos de Prueba: Datos de prueba para probar controles específicos; Transacciones de prueba seleccionada; Transacciones de prueba usadas en una instalación de pruebas integrada

- **Usos de TAACs**

Se pueden utilizar TAACs para:

- Pruebas de detalles de transacciones y saldos
- Procedimientos de revisión analítica
- Pruebas de cumplimiento de controles generales
- Pruebas de cumplimiento de controles de aplicaciones

- **Consideraciones en el uso de TAACs**

Para determinar si se utilizarán TAACs, se deberá considerar:

- Conocimiento, pericia y experticia del auditor en computadoras

¹ Declaración Internacional de Auditoría

- Disponibilidad de TAACs e instalaciones adecuadas de computación
- No factibilidad de pruebas manuales
- Efectividad y eficiencia
- Oportunidad

- **Utilización de TAACs**

Los principales pasos que un auditor debe tomar en cuenta en la aplicación de TAACs son:

- Fijar el objetivo de la aplicación de la TAAC.
- Determinar el contenido y accesibilidad de los archivos de la entidad.
- Definir los tipos de transacción que van a ser probados.
- Definir los procedimientos que se realizarán en los datos.
- Definir los requerimientos de datos de salida.
- Identificar al personal de auditoría y de computación que pueda participar en el diseño y aplicación de la TAAC.
- Refinar los estimados de costos y beneficios.
- Asegurarse de que el uso de la TAAC está controlado y documentado en forma apropiada.
- Organizar las actividades administrativas, incluyendo las habilidades necesarias y las instalaciones de computación.
- Ejecutar la aplicación de la TAAC.
- Evaluar los resultados.

- **Utilización de TAACs en entornos de computadora en negocios pequeños**

El auditor deberá poner especial énfasis en los negocios pequeños en los siguientes aspectos:

- El nivel de controles generales de PED puede ser tal que el auditor deposite menos confiabilidad en el sistema de control interno. Esto dará como resultado:
 - Mayor énfasis en las pruebas de detalles de transacciones y saldos y en los procedimientos de revisión analítica, lo que puede aumentar la efectividad de ciertas TAACs, particularmente del software de auditoría.
 - La aplicación de procedimientos de auditoría para asegurar el funcionamiento apropiado de la TAAC y la validez de los datos de la entidad.
- En casos donde se procesen menores volúmenes de datos, los métodos manuales pueden ser más efectivos en costo.
- La asistencia técnica adecuada puede no estar disponible al auditor por parte de la entidad, haciendo así poco factible el uso de TAACs.
- Ciertos programas de auditoría en paquete pueden no operar en computadoras pequeñas, restringiendo así la opción del auditor en cuanto a TAACs. Sin embargo, los archivos de datos de la entidad pueden copiarse y procesarse en otra computadora adecuada.

III. CARACTERÍSTICAS DESEABLES DE UN SOFTWARE DE AUDITORIA

CARACTERÍSTICAS GENERALES

Las características generales que se deben buscar en un software de auditoria son:

- Manual de Usuario, Manual Técnico y Material de Capacitación.
- Opciones de copiar o exportar cualquier documento como papeles de trabajo a aplicaciones ofimáticas como Word, Excel, Power Point y otros.
- Capacidad de acumular la información histórica, y además de poderla consultar por año.
- Capacidad de poder funcionar como un todo integrado entre las diferentes etapas y procesos de la Auditoria: Planeación; Administración de Riesgos; Ejecución y Administración de Papeles de Trabajo; Evaluación de Administración de TI; Análisis y Evaluación de Base de Datos; Emisión de Informes

CARACTERÍSTICAS DE SEGURIDAD

Las características de seguridad que se deben buscar en un software de auditoria son:

- Posibilidad de definir que usuarios puedan acceder al sistema.
- Administración de los permisos de las opciones a las que tiene derecho un usuario a ejecutar, consultar según su cargo y área a la que pertenezca.
- Opciones de incluir pistas de auditoría en procesos, control de cambios, lectura, escritura y modificación de parte de los usuarios.
- Copias de respaldo de la información mediante BACKUP en medios magnéticos/ópticos y COMPROBAR como recuperar los datos del Backup.

IV. TIPOS DE SOFTWARE DE AUDITORIA

1. PLANIFICACIÓN DE LA AUDITORIA

Algunas características específicas de este tipo de software podrían ser las siguientes:

- Capacidad para ingresar, modificar, eliminar criterios de evaluación de las diferentes modalidades de auditoría existentes (Financiera, Operacional, especiales, integrales y de Sistemas), y así poderlos utilizar en otras auditorías.
- Mantenimiento de las auditorías y de los recursos y así mismo generar mínimamente los siguientes reportes:
 - Utilización de Recursos / Tiempo Libre.
 - Conflictos de asignación.
 - Diagrama de Gantt.
 - Calificaciones de Recursos.
 - Programación de Proyectos.
 - Lista de Recursos.
- Base de datos de mejores prácticas de programas de auditoría, estándares de control y otras normas o estándares internacionales con posibilidad de poder agregar mediante librerías o Base de Datos otros estándares. Algunos ejemplos: COSO - MICIL, COBIT, ISO 27001, ISO 15408, ISO 9126, ITIL, ISO 20000, ISO 13335.

1.1. Planning Advisor

Página web: www.methodware.com

Este programa ayuda a automatizar el proceso de planeación de la auditoría. Utilizando este programa se puede identificar y clasificar las áreas de mayor exposición mediante criterios de evaluación basados en riesgos. Esta herramienta se puede utilizar en combinación con el Pro audit. Advisor como herramienta de ejecución de la planeación. El progreso de toda la planificación de auditoría puede ser monitorizada en forma centralizada por Planning Advisor.

2. EJECUCIÓN – SUPERVISIÓN

Algunas características específicas de este tipo de software podrían ser las siguientes:

- Opciones de administrar pistas de auditoría sobre los documentos que se ingresen al sistema, para cuando se necesite comprobar el origen de determinados cambios sobre los mismos.
- Sistema de referencia que incluya:
 - Referencias automáticas de hallazgos, papeles de trabajo y otra documentación de word o excel que sea parte del programa de trabajo, como por ejemplo los recálculos.
 - Un referenciador de papeles de trabajo que guarda un orden sistemático en toda la base de datos.

- Referencias a posibles archivos de imágenes que formen parte del programa de trabajo.
- Marcas de auditoría integradas y personalizables.
- Personalización de los atributos de los hallazgos de Auditoría de acuerdo a las normas de auditoría.
- Ingreso de notas de revisión, en los papeles de trabajo.
- Repositorio de información histórica de las auditorías realizadas en años anteriores, a su vez de poder consultar los papeles de trabajo e informes emitidos.
- Consolidación de los hallazgos y generación del borrador del informe final, así como el resguardo posterior del informe final.
- Generación de consultas y reportes de recomendaciones realizadas para dar seguimiento por área, rango de fechas, tipo de auditoría y de recomendaciones (emitidas, proceso, cumplidas) según los tipos de auditorías ingresadas al sistema.

2.1. CobiT Advisor

Página web: www.methodware.com

Es un programa que automatiza el marco de referencia CobiT. Permite la definición del personal de trabajo en una auditoría, así como elegir el Dominio en el cual se trabajará es decir Planificación y Organización, Adquisición y Mantenimiento, Desarrollo y Soporte y Monitoreo, así como los subdominios o procesos por cada dominio. También se pueden definir los criterios y recursos de información que se evaluarán. Por cada proceso evaluado se tienen los objetivos de control y las guías de auditoría, así como su respectiva evaluación. Tiene la opción para adjuntar archivos como papeles de trabajo, muestra las evaluaciones en formato gráfico y permite generar reportes exportables a Word.

2.2. Pro Audit Advisor

Página web: www.methodware.com

Es una herramienta de papeles de trabajo electrónicos (digitales). Con esta herramienta se puede: Definir el modelo del negocio en múltiples niveles; Determinar evaluación de procesos, riesgos y control; Identificar y definir riesgos así como el mantenimiento de los controles; Detallar los programas de trabajo en procedimientos individuales y desarrollar los papeles de trabajo apropiados; Analizar los resultados y generar reportes digitales sofisticados en formatos Word o HTML.

3. ANÁLISIS DE RIESGOS

Algunas características específicas de este tipo de software podrían ser las siguientes:

- Automatizar todos los aspectos de riesgos dentro de una herramienta dinámica.
- Base de datos de metodologías/técnicas de Análisis de Riesgos. Algunos ejemplos: Delphi; Análisis por Tablas; MAGERIT; NIST Risk Management Guide; AS/NZS 4360:2004 Risk Management.

- Opciones de realizar análisis de riesgo cualitativo, cuantitativo y mixto.
- Definición de parámetros para el análisis cuantitativo del riesgo.
- Tener un repositorio central y compartido que puede ser accedido por auditores internos y personal externo al área de auditoría que previamente haya sido debidamente autorizado.
- Monitorear y dar seguimiento a la información de las auditorías y al cumplimiento de las recomendaciones.
- Presentación de Registro histórico de auditorías por temas (Consolidación de estudios a través del tiempo).
- Rastrear el rendimiento de los indicadores claves de riesgo.
- Contar con una clara imagen de la información del riesgo en cualquier nivel de la organización; a través de matrices de riesgos y otros gráficos.
- Proveer a la organización un sistema de administración de riesgos, con indicadores de riesgo, eventos de riesgo y tratamientos de riesgo.
- Generar reportes los cuales estén completamente integrados con Microsoft Office.

3.1. RISK2K – Pilar - Chinchón

Estos programas permiten implementar los conceptos y procesos propuestos por la metodología MAGERIT para el análisis y gestión de riesgos. Los objetivos básicos del MAGERIT son estudiar los riesgos y recomendar contramedidas, esto se consigue cargando la base de datos información como: Grupos de activos, Amenazas, Grupos de amenazas, Tipos de amenazas, Funciones de salvaguarda, Tipos de funciones de salvaguarda, Mecanismos de Salvaguarda.

La metodología MAGERIT está compuesta por: Guía de Aproximación, Guía de Procedimientos, Guía Técnica, Guía para desarrolladores de aplicaciones, Guía para responsables del dominio protegible, Referencia de normas legales y Técnicas.

3.2. Enterprise Risk Assessor (ERA Lite)

Página web: www.methodware.com

Es una herramienta para la gestión y control del riesgo, proporciona: Un sistema consistente de gestión de riesgos; Identificación específica de riesgos para la estrategia y contexto organizacional; Gestión para los planes de acción, y monitoreo mediante una base de datos; Evaluación de riesgos, controles y amenazas semi-cuantitativas, a través de análisis de consecuencias; Gráficos de análisis; Reportes de alta calidad alineados a los requerimientos individuales de los negocios.

3.3. Risk Assesment Program - RAP

Página web: www.cosim-ti.com

RAP es un programa de análisis de riesgos y contramedidas basándose en la técnica de Tablas en la que se identifican riesgos y se determina la probabilidad, impacto y en función a estos dos últimos se calcula el Nivel de Riesgo Asociado. Las contramedidas se asignan de acuerdo al mayor Nivel de Riesgo que presenten los Activos de Información de la organización.

RAP le permite:

- Definir los Tipos de Riesgos a los cuales están expuestos los activos de información de una organización.
- Identificar los riesgos específicos que pertenecen a un tipo de riesgo determinado.
- Parametrizar los niveles de probabilidad e impacto.
- Realizar evaluaciones de riesgo por diferentes áreas, departamentos, o empresas, determinando probabilidad de ocurrencia del riesgo, impacto que causaría en caso de producirse el riesgo y cálculo del nivel de riesgo asociado
- Consolidar los resultados de evaluaciones de diferentes áreas, departamentos o empresas
- Asignar contramedidas, priorizándolas en función al mayor nivel de riesgo.
- Exportación de los parámetros, así como de las evaluaciones a diferentes formatos (Word, Excel y otros formatos)
- Generación de Informes sobre evaluaciones tanto individuales como consolidados

3.4. Audicontrolⁱⁱ

AudiControl son metodologías asistidas por computador para evaluar riesgos y establecer controles en sistemas de información automatizados y tecnología relacionada. Consta de dos módulos:

- a) APL, diseño de controles para sistemas de información computarizados, y
- b) FTI, diseño de controles para la función de tecnología de información.

Las metodologías han sido creadas para asistir a los equipos de desarrollo de sistemas o ingeniería de software, a los profesionales encargados de la seguridad informática y a los auditores, en las actividades de evaluación de riesgos y establecimiento de controles internos en cualquier componente de los sistemas de información automatizados. Audicontrol permite el uso de bases de datos de conocimientos que incluyen conceptos y elementos modernos aportados por los modelos *Cobit -Control Objectives for Information and Related Technology ISACA 1998-* y *Coso*. Ayuda a identificar y categorizar los riesgos inherentes a los negocios o servicios de las empresas como lo recomienda *Coso* y permite elaborar el mapa de riesgos con la ubicación física, lógica y funcional de los riesgos en las dependencias y procesos. Ayuda a elaborar las "Guías de Autocontrol" que asignan responsabilidades por la ejecución y/o supervisión de cada control clave en las dependencia que intervienen en los procesos de negocios automatizados, y las "Guías de Autoevaluación del Control" para determinar el riesgo residual en las dependencias de la empresa.

ⁱⁱ Descripción extractada del documento denominado "Software de Auditoria", elaborado por el Lic. Jorge Guevara Espinoza

4. ANÁLISIS Y EVALUACION DE BASE DE DATOS

Algunas características específicas de este tipo de software podrían ser las siguientes:

- Herramienta orientada a la auditoría.
- Facilidad de uso mediante interfaz amigable que le permitan al auditor enfocarse en aplicar su experiencia, en vez de estar aprendiendo a cómo utilizar el software.
- Convierta un conjunto de datos almacenados en un medio digital, en información que sea analizable.
- Importar diversos tipos de archivos mediante un sistema de importación y manejo de especificación de criterios de importación. (Archivos en formato plano y archivos con formato propietario)
- Extracción de datos desde bases de datos relacionales (Oracle, SQL Server 2000, Informix).
- Posibilidad de poder realizar trabajos en línea mediante conexión directa a la Base de Datos del software aplicativo mediante conexiones ODBC.
- Capacidad de análisis interactivo, amigable e intuitiva.
- Manejo de grandes volúmenes de datos no importando su complejidad o configuración sin afectar el rendimiento de la base de datos.
- Capacidad de elaborar diferentes tipos de análisis estadísticos.
- Localizar errores e inconsistencias, comparando y analizando los archivos según los criterios especificados por el usuario.
- Funciones de estratificación, identificación de variaciones y duplicidad de datos, faltantes en datos.
- Archivos de registro (Pistas de Auditoría) que reflejen todo el trabajo realizado
- Posibilidad de desarrollar aplicaciones personalizadas que se puedan ejecutar automáticamente (Macros, Scripts, etc.) creando así una metodología de auditoría continua.
- Capacidad para trabajar simultáneamente con varios archivos.
- Compatibilidad de exportación con aplicaciones ofimáticas, por ejemplo Microsoft Office.

4.1 ACL: (Audit Command/Control Language)

Página web: www.acl.com

ACL (Lenguaje de Comandos de Auditoría) es un software para análisis y extracción de datos más usado en la actualidad.

Con ACL los auditores y profesionales de los negocios pueden transformar grandes cantidades de datos electrónicos en un conocimiento comercial de valor. Es un software, poderoso y fácil de usar, le permite convertir datos en información significativa, lo cual le ayuda a alcanzar sus objetivos de negocios y agregar valor a su organización.

Con ACL se podrá realizar la revisión de datos con una cobertura del **100% de los datos**, esto significa que se pueden hacer auditorías para toda una población entera, y no para pequeñas muestras.

El impacto de ACL se ve en los siguientes aspectos: los ciclos de auditoría más cortos; las investigaciones más detalladas; una confianza completa en sus resultados; un ahorro significativo en sus recursos; un rol mayor de la auditoría en el negocio.

Características generales:

- Permite importar archivos de diferentes fuentes o formatos (archivos planos y de base de datos específicas).
- Los datos importados no son modificados asegurando la integridad e incrementando el nivel de confianza de los datos trabajados
- Generación de pistas de auditoria (Quien, Como, Cuando, Donde)
- Posibilidad de escribir Scripts/Macros que automaticen procedimientos de revisión rutinaria en auditorias recurrentes.
- Incrementar la cobertura de revisión al 100% de datos a analizar

Características específicas:

- Identificar tendencias, señalar excepciones y destacar áreas que requieren atención
- Localizar errores y fraudes potenciales, mediante la comparación y el análisis de archivos según los criterios especificados por el usuario
- Volver a calcular y verificar saldos
- Identificar problemas de control y asegurar el cumplimiento de las normas
- Analizar y determinar la antigüedad de las cuentas por cobrar, cuentas por pagar u otras transacciones a las que afecta el tiempo transcurrido
- Recuperar gastos o ingresos perdidos, detectando pagos duplicados, secuencias numéricas incompletas en la facturación o servicios no facturados
- Detectar relaciones no autorizadas entre el personal de la empresa y los proveedores
- y muchas más
- Funciones específicas para la auditoría: desde comandos tales como Faltantes, Duplicados y Estratificar hasta el importante log de comandos o el historial detallado. La funcionalidad incorporada de revisión de cuentas le permite a auditores y contadores, sin experiencia técnica o de programación, realizar rápidamente análisis e informes sobre datos financieros.
- Procesa rápidamente millones de transacciones, asegurando una cobertura del 100% y una confianza absoluta en sus resultados.
- El Asistente de definición de datos fácilmente selecciona, identifica y da formato a los datos, acelerando su acceso a las poderosas capacidades de análisis y generación de informes de ACL.
- ACL puede leer y analizar cualquier tipo de datos accediendo a cualquier entorno de su organización (tales como Oracle , SQL Server, Informix , AS400, IBM/390, SAP™ R/3™, archivos de informe de longitud variable, archivos privados, archivos tradicionales, archivos de informe y muchos más) .
- Relaciona y trabaja simultáneamente con varios archivos (Modelo Entidad/Relación), para hacer análisis e informes aún más completos.
- Crea informes en HTML para su publicación en Internet o en la Intranet de su organización.
- Automatiza y registra sus pasos y desarrolla aplicaciones especiales, haciendo más productivas las auditorías futuras.
- Permite revisar o imprimir, en cualquier momento, un historial completo de sus archivos, pasos y resultados.

4.2 IDEA: (Interactive Data Extraction and Analysis)

Página web: www.caseware.com

IDEAⁱⁱⁱ es el que utiliza Price WaterhouseCoopers, es una herramienta de PC basada en la Interrogación de Archivos para ser utilizada por auditores, contadores, investigadores y personal de seguridad informática. Analiza los datos de diversas maneras y permite la extracción, el muestreo y la manipulación de datos para identificar errores, problemas, cuestiones específicas y tendencias.

IDEA está diseñado para auditores internos y externos, aunque el uso del software es normalmente diferente.

También es una valiosa herramienta para investigadores de fraude, contadores y administradores.

Puede utilizarse por ejemplo para:

- Identificar elementos excepcionales
- Realizar Análisis
- Comprobar Cálculos
- Coincidencias cruzadas de datos entre sistemas
- Pruebas de Omisiones y Duplicados
- Muestreo

Características Generales:

- Mantiene un registro de todas las acciones realizadas en una base de datos, comenzando con la importación de la base de datos.
- Permite realizar análisis complejos de datos, extracciones de elementos poco usuales, muestras de auditoría, transacciones duplicadas, pruebas de auditoría rutinarias o recurrentes para investigaciones de fraude, auditorías de seguridad y producción de informes de gestión.
- Agregar campos (calculado) virtuales.
- Extracciones de registros según criterios utilizando operadores de comparación (<, >, =, otros), lógicos (y, o, no)
- Realizar pruebas de excepción avanzadas utilizando las funciones incorporadas de IDEA (funciones: Carácter, Numéricas, Coincidencia, Fecha y hora, Condicionales)
- Guardar fórmulas elaboradas con operadores aritméticos, lógicos, y funciones para su posterior uso en trabajos repetitivos o auditorías recurrentes.
- Generar informes con los análisis realizados.
- Genera **Estadísticas de campos: Las Estadísticas Numéricas** incluyendo totales, media, mínimo, máximo y otros valores son útiles para reconciliar los datos importados al ordenador, así como para proporcionar una comprensión del rango de los valores que se están probando.
Las Estadísticas de Fecha incluyendo fecha más temprana y más tardía son útiles para asegurarse que los datos proporcionados pertenecen al periodo correcto de la auditoría, es decir pruebas de corte así como análisis de los datos en un periodo.
- IDEAScript, se utiliza para extender la potencia y funcionalidad del software IDEA es un lenguaje de programación específico para IDEA, similar sino igual a Visual Basic para Aplicaciones (VBA) de los programas Word, Excel o Access de Microsoft.

ⁱⁱⁱ Características y descripción del programa extractado de la Ayuda del Programa **IDEA 2004**

- **Limitaciones de Base de Datos:** 32.167 campos (columnas); 2.1 Billones registros (filas) dependiendo del sistema operativo; 18 EB tamaño de archivo

Objetivos de Auditoría con IDEA

- **Comprobación de Exactitud:** Una de las primeras funciones para las que puede usarse IDEA es para sumar el archivo y comprobar la exactitud de los cálculos. La suma del archivo se lleva a cabo usando la opción Estadísticas de Campo (disponible en Importación de Archivo). Los cálculos pueden verificarse usando la opción de Agregar (en el diálogo Manejar Campos) o usando el botón de Campos Virtuales, en la Barra de Herramientas para crear un cálculo del elemento correspondiente, o mediante una prueba de excepción de cálculos erróneos usando la función de extracción. La exactitud de cualquier informe de dirección puede suponer un uso más extenso de funciones específicas, para lograr el resultado de generar el informe. En estos casos, puede ser necesario llevar a cabo una serie de uniones y/o totalizaciones, o cálculos de antigüedad, como para el caso del análisis de deuda.
- **Revisión Analítica:** IDEA puede ayudar en la preparación de datos para una revisión analítica. En particular, puede generar análisis que no estarían disponibles en otros casos. La opción Estratificación (del menú Análisis) dará un perfil de la población en intervalos de valor, en grupos de códigos, o en fechas. Esto es particularmente útil al auditar activos tales como deudores, inventarios, préstamos o para definir una distribución de las transacciones. Adicionalmente, la información puede resumirse por códigos determinados o por sub-códigos. Las cantidades pueden compararse también con las de años anteriores, para analizar tendencias. Si se necesita un análisis gráfico, puede usarse el Asistente de Gráficos o la opción Gráfico dentro de Ver.
- **Validez (Pruebas de Excepción, Comparaciones y Duplicados):** Las pruebas de Excepción pueden usarse para identificar elementos poco frecuentes o extraños. Estos pueden ser cantidades excepcionalmente grandes, o circunstancias donde dos conceptos de información no se correlacionan debidamente (por ejemplo, salario con categoría). También pueden verificarse campos de información con tablas de valores admisibles (por ejemplo, precios hora estándar).
 - **El Muestreo Estadístico** se usa normalmente para comprobar la validez de datos de tal manera que permite la evaluación de los mismos a través de una población. Los métodos más sofisticados, como el Muestreo por Unidades Monetaria, son difíciles de implantar a mano. Cuando las pruebas se refieren a comprobaciones físicas de documentación o de recursos, en vez de a la comprobación de registros mecanizados, las técnicas de muestreo estadístico son las apropiadas.
 - **Las Pruebas de duplicados** pueden ser muy eficaces en ciertas circunstancias, como en la comprobación de pagos o para buscar entradas de números repetidos durante los recuentos de inventario.
 - Puede ser necesario unir primero dos archivos, para realizar una prueba de validez, como por ejemplo, el archivo de transacciones con el archivo maestro correspondiente.

- **Integridad (Omisiones y Coincidencias):** Para los test de integridad pueden utilizarse la opción de Omisiones (Númericas, de Caracteres y de Fechas, para que esto se pueda hacer debe existir un número secuencial en la documentación original. Los archivos de inventario y de ventas pueden comprobarse para verificar ordenes de entrega con albaranes y pedidos. También puede ser apropiado verificar Omisiones en una secuencia de números de talonarios y de números de identificación del inventario. Otra prueba común que se puede realizar, es la de hacer un cruce entre un archivo maestro (por ejemplo, de contratos de mantenimiento) y uno de transacciones (por ejemplo, facturas), para ver si existen registros en el maestro para los cuales no existen transacciones.
- **Corte de operaciones:** Se pueden realizar comprobaciones de fin de año, sobre el mayor de cuentas, archivos de inventario o archivos de transacciones para analizar elementos con fechas o números de secuencia anteriores o posteriores al corte de fin de año.
- **Detección de Fraudes**, como cruzar archivos de direcciones con los de nómina y libros contables de cuentas a pagar, números duplicados en facturas de proveedores y búsquedas de coincidencias en cuentas bancarias de nómina con archivos maestros correspondientes.
- **Detección de Fraudes y la Ley de Benford^{iv}:** El análisis de la Ley de Benford es efectivo para identificar posibles valores fraudulentos. Si existen valores artificiales o ficticios en una base de datos, la distribución de los dígitos dentro de la base de datos puede ser diferente a la establecida al respecto por la Ley de Benford. Se pueden ver los datos en forma gráfica y comparar los resultados con los establecidos previamente por la Ley de Benford, así como también los límites máximos y mínimos.
- **Otros Objetivos de Auditoría:** IDEA puede proporcionar también información útil en áreas complejas, tales como provisiones y valoraciones, creando varias “vistas” basadas en una serie de parámetros diferentes. Tomando como ejemplo el inventario, se pueden identificar elementos que no se han movido en 3,6,9 y 12 meses; compararlos con las ventas después de fin de año, para ver lo que no se ha vendido, y comprobar el valor neto realizable para aquellos que sí se han vendido; verificar los elementos de inventario, del año pasado, frente a lo que no se ha vendido este año. Cualquier auditoría o investigación de archivos, que tenga necesidad de llevar a cabo análisis de datos, trabajos de cálculo, o pruebas de excepción, se beneficiará con el uso de IDEA.

4.3 SQL Secure

SQL Secure^v, fabricado por BrainTree Security Software, es un conjunto de cuatro herramientas de software que administran todos los aspectos de seguridad y auditoría de la base de datos en ambientes cliente/servidor. Está compuesto de cuatro módulos:

- a) Password Manager, permite definir los estándares para la asignación de passwords.
- b) Audit Manager, para la administración completa de pistas y rastros de auditoría (*audit trail*).

^{iv} Una ejemplificación de la Ley de Benford <http://danielmadv.blogspot.com/2008/01/tecnicas-antifraude.html>

^v Descripción extractada del documento denominado “Software de Auditoría”, elaborado por el Lic. Jorge Guevara Espinoza

- c) Policy Manager, permite evaluar frecuentemente las reglas predefinidas para identificar debilidades de control, y
- d) Database Security Manager, permite la administración de la seguridad de la base de datos.

5. HERRAMIENTAS INTEGRADAS

5.1. Gestor F1 Audisis

Página web: www.yanapti.com

Gestor F1 Audisis^{vi} concentra funcionalidades tanto de gestión de auditoría como de análisis automatizado de datos, en general se puede realizar lo siguiente:

- Análisis de Base de Datos
- Planificación de equipos de Auditoría de Sistemas y Seguridad: COBIT, ISO 17799/27001, COSO
- Control de asignaciones
- Gestión de Riesgos
- Conexiones ODBC
- Módulo de seguridad de accesos y privilegios para usuarios
- Pistas de Auditoría
- Funcionamiento de la herramienta tanto en Intranet como Internet

Módulo de Gestión

- Permite planificar los trabajos de auditoría, llevar costos, responsables, tareas asignadas.
- Permite cargar metodologías, leyes, códigos, reglamentos, políticas de una manera estructurada permitiendo al Auditor Líder planificar las revisiones de campo a ejecutar.
- Contiene las metodologías COBIT, ISO 27001, COSO, y algunas Leyes y reglamentos para su uso

Módulo de Análisis de Datos

- Permite cargar manualmente o ODBC bases de datos y logs con millones de registros, para su análisis.
- Permite efectuar análisis estándar de datos como faltantes, repetidos, muestras, estadísticas, correlativos, etc.
- Permite efectuar consultas libres, añadir y recalcular columnas.
- Registra todas las consultas realizadas y los resultados obtenidos.
- Permite crear bibliotecas de consultas estándares para diferentes procesos

5.2. Auditor 2000

Auditor 2000^{vii} es una solución de metodologías asistidas por computador para auditar sistemas de información automatizados y tecnología relacionada. Consta de tres módulos:

^{vi} **NOBOSTI**, vol.0/08 Edición Especial, La paz 2008. Pág 42

^{vii} Descripción extractada del documento denominado "Software de Auditoría", elaborado por el Lic. Jorge Guevara Espinoza

- a) Audap: auditoría a sistemas de información computarizados;
- b) Audides: auditoría al desarrollo de sistemas; y
- c) Audifti: auditoría a la función de tecnología de información.

Son metodologías maduras y robustas que se apoyan con una herramienta de software amigable y bases de datos con conocimientos sobre riesgos, causas del riesgo, controles, objetivos de control y técnicas de auditoría recomendadas por los estándares Cobit y Coso y las mejores prácticas universalmente aceptadas para el ejercicio profesional de la auditoría de sistemas. Auditor 2000 identifica y evalúa riesgos críticos. Con base en cuestionarios o la técnica Delphy, se identifican y evalúan los riesgos críticos inherentes a los negocios y servicios que se soportan en tecnología de información. Evalúa y califica el nivel de protección que ofrecen los controles establecidos en los procesos manuales y automatizados, relación con las causas de los riesgos críticos asociados con el área objeto de la auditoría. Ayuda a definir y diseñar pruebas de cumplimiento y sustantivas, con base en los resultados de la evaluación del sistema de control interno.

5.2. Audit System 2

Audit System 2^{viii}, el que usa Deloitte Detouche. Esta herramienta es fundamental en la realización de auditoría de empresas donde el control y el registro de las transacciones se efectúa a través de un procesamiento electrónico de datos. Desde el punto de vista de la eficiencia de la auditoría, el Audit System/2TM, es esencial para aquellas organizaciones que procesan un gran conjunto de transacciones similares.

AS/2 ha sido desarrollado por un equipo multinacional de auditores e ingenieros en sistemas de Deloitte Touche Tohmatsu, para cumplir con las diferentes y cambiantes necesidades de sus clientes.

Audit System/2TM, (AS/2) está integrado por hardware, software y profesionales en auditoría. En pocas palabras, representa una reingeniería de las capacidades en servicios de auditoría, integrando el enfoque de Deloitte Touche en la materia y su finalidad es añadir un valor al negocio a sus clientes.

AS/2 ofrece una cobertura de aplicación amplia y profunda, así como un grado de integración de todas las fases del proceso de auditoría (planeación, ejecución e informes), apoyando las habilidades y el tiempo de los profesionales. Contiene funciones para extraer, interrogar, analizar, documentar, revisar, administrar, presentar y comunicar –eficazmente – información del cliente.

^{viii} Descripción extractada del documento denominado “Software de Auditoría”, elaborado por el Lic. Jorge Guevara Espinoza

5.3. TeamMate

TeamMate^{ix} es el que usa Price WaterhouseCoopers, es un facilitador del desarrollo secuencial de la auditoría. Este a su vez facilita la labor de documentación de todas las tareas efectuadas en el proceso de auditoría. Por tanto, TeamMate es un sistema de “archivo electrónico”, una herramienta fundamental para documentar auditorías de diferentes alcances, ayudando a la aplicación de estándares tanto en la documentación como en la revisión. Adicionalmente facilita la generación de informes de auditoría. TeamMate es usado por más de 14,000 auditores en 275 países alrededor del mundo.

Tipos de Auditoría que documenta La aplicabilidad del sistema va desde la documentación de auditorías financieras, de cumplimiento, procedimientos, operacionales, investigaciones, y auditorías de IT. Adicionalmente es utilizado para la documentación de la evaluación de controles, auditorías de contratos y revisiones generales. Con TeamMate se tiene acceso a bases de datos de mejores prácticas, además se aprovecha todo el trabajo realizado en auditorías anteriores, así como las guías de trabajo existentes en Word y Excel. Team Mate permite el seguimiento y firma de los papeles de trabajo, así como el mantenimiento de referencias entre los diferentes documentos como el reporte de auditoría, los hallazgos y las pruebas realizadas.

TeamMate incluye un software de imágenes, el cual permite una sencilla incorporación de imágenes y fotografías escaneadas críticas en los papeles de trabajo.

TeamMate fue desarrollado por el World Research and Technology Centre de PricewaterhouseCoopers en Menlo Park, California. TeamMate fue finalista en la prestigiosa conferencia COMDEX y Windows World Open le dio el premio en 1994 ICAA - Microsoft Innovative Technology Award.

Team Mate ayuda a que el proceso que tradicionalmente lleva más tiempo en la ejecución de la auditoría “la documentación”, se reduzca sustancialmente ayudando a que el auditor se concentre en las actividades de mayor valor agregado

Todos los papeles de trabajo automáticamente son comprimidos y encriptados cuando se cierra una aplicación; de la misma forma se respaldan los trabajos de forma automática cada vez que se termina una sesión de trabajo.

Arquitectura de TeamMate TeamMate posee un poderoso motor de replicación el cual permite el trabajo en equipo tanto en redes de área local como en ambientes de acceso remoto según sea la necesidad. La arquitectura, el modelo de la base de datos y la replicación permite no interrumpir el trabajo durante la etapa de revisión ya que cada uno de los miembros del equipo tiene una copia idéntica (réplica) de la base de datos lo cual permite que el resto de equipo continúe con el trabajo mientras se hace la revisión, TeamMate se integra naturalmente a cualquier sistema de correo electrónico para facilitar la comunicación.

^{ix} Descripción extractada del documento denominado “Software de Auditoría”, elaborado por el Lic. Jorge Guevara Espinoza

6. PROGRAMAS PARA PROPÓSITOS ESPECÍFICOS

6.1. Sistema de Auditoria y Seguridad – SAS

Página web: www.cosim-ti.com

Dentro de las herramientas CAATTs diseñados para un propósito específico se tiene el “Sistemas de Auditoria y Seguridad - SAS”, para uso exclusivo de las Unidades de Control (Auditoria Interna, Gestión de Riesgos operativos y tecnológicos, etc.), que le permite al auditor evaluar los niveles de seguridad de acceso lógico e integridad de datos de Clientes, Cartera, Caja de Ahorro y DPF, incrementando la calidad del control. Esta herramienta trabaja con aplicativos de Instituciones Financieras como son los Bancos, Mutuales, Fondos Financieros y Cooperativas de Ahorro y Crédito.

SAS permite:

- Importa tablas de la BD, exportadas en formato plano.
- Preservar la Integridad y Confiabilidad de las tablas importadas al impedir la modificación de los datos importados.
- Ejecutar auditorias recurrentes a datos.
- Evaluar la integridad de la BD de los módulos: Administración, General, Préstamos, Caja de Ahorro y Depósitos a Plazo Fijo.
- Generar aproximadamente 50 objetivos de control automatizados.
- Los resultados son exportables a los papeles de trabajo o informes (Excel, Word, y otros formatos).
- Combinar tablas automáticamente, generando pruebas de integridad de datos en Préstamos, Caja de Ahorro y DPF.
- Ejecutar Pruebas de cumplimiento y sustantivas que son las recomendadas por la ISO 17799 y COBIT.
- Tener un sistema de alerta preventivo a posibles hechos irregulares o fraudes.

Asimismo el SAS tiene diseñado un módulo adicional denominado **SAS-LOG**, permite monitorear y analizar los eventos del aplicativo, que nos permiten identificar los criterios de una “**pista auditoria**” que nos indicara QUIEN realizo una operación (usuario del aplicativo), COMO se realizo la operación (a través de que menús y submenús a los cuales se accedió), DONDE se realizo la operación (en que oficina y en que modulo del aplicativo), CUANDO se realizo la operación (La fecha y hora en que se realizo el evento). Todos estos aspectos incrementan de gran manera la “**calidad del control**” y garantizan una mayor “**independencia**” respecto al análisis de los datos.

SAS LOG le permite:

- Importa tablas que contengan los eventos del aplicativo, exportadas en formato plano
- Preservar la Integridad y Confiabilidad de las tablas importadas al impedir la modificación de los datos importados.
- Ejecutar auditorias recurrentes a datos.
- Generar pistas de auditoria y objetivos de control automatizados.
- Los resultados son exportables a los papeles de trabajo o informes (Excel, Word, y otros formatos).
- Tener un sistema de alerta preventivo a posibles hechos irregulares o fraudes.
- Analizar los eventos del aplicativo a medida que ocurren.
- Generar evidencia para una posterior revisión.

- Analizar acciones normales, anormales (errores, fraudes) o dañinas, así como la generación de evidencia de auditoría.

6.2. Statistical Techniques of Analytical Review

STAR^x es un programa que usa la regresión analítica para efectuar procedimientos analíticos sustantivos. Este proporciona al auditor la capacidad de realizar un análisis sofisticados de datos financieros e identificar variaciones sutiles, pero significativas en los resultados financieros de una organización, Una característica importante del programa **Star** es su exclusiva “Interfase de Auditoría”, que mide la significancia de las variaciones basado en la materialidad definida para auditoría y la confianza de la auditoría requerida.

6.3. DATAS - Digital Analysis Tests And Statistics

Página web: www.nigrini.com

Este programa permite realizar análisis de un conjunto de datos (una sola columna) que trate de un asunto en particular, por ejemplo transacciones de caja, importes de los asientos contables, reversiones de transacciones, depósitos o retiros de cuentas corrientes, etc. El análisis que realiza el DATAS es mediante la **Ley de Benford** que consiste en:

- Realizar una extracción del primer dígito, segundo dígito, primeros dos dígitos del conjunto de datos a analizar.
- Contar la cantidad de ocurrencias:
 - Para el primer dígito cuántos 1,2, 3,4,5,6,7,8,9 existen en el conjunto de datos a analizar
 - Para el segundo dígito cuántos 0,1,2, 3,4,5,6,7,8,9 existen en el conjunto de datos a analizar.
 - Para los primeros dos dígitos cuántos 10,11,12,13,14,15,16,17.....99 existen en el conjunto de datos a analizar.

Una vez que se tenga el conteo de los dígitos, el DATAS permite guardar esos resultados en un archivo de texto, el cual puede ser exportado a una planilla electrónica (Excel), en la cual podemos ingresar los porcentajes de ocurrencia definidos por la Ley de Benford para los dígitos (primero, segundo, primeros dos) para luego realizar el gráfico respectivo que nos mostrará cumplimiento o desviaciones de la ocurrencia de los dígitos respecto a la Ley de Benford.

Los resultados que arroja esta Ley respecto a la probabilidad de ocurrencia de los dígitos es la siguiente:

Dígitos		0	1	2	3	4	5	6	7	8	9
Primer	Digito %	-	30.10	17.61	12.49	9.69	7.92	6.69	5.80	5.12	4.58
Segundo	Digito %	11.97	11.39	10.88	10.43	10.03	9.67	9.34	9.04	8.76	8.50
Tercer	Digito %	10.18	10.14	10.10	10.06	10.02	9.98	9.94	9.90	9.86	9.83

^x Descripción extractada del documento denominado “Software de Auditoría”, elaborado por el Lic. Jorge Guevara Espinoza

6.4. Herramientas de Hacking

Página web: www.foundstone.com

A continuación se presentan programas que permiten al Auditor de Sistemas y TI realizar auditorías de evaluación de Seguridad de los dispositivos de telecomunicaciones, así como de las PCs conectadas en red tanto en una Intranet como conectadas con Internet.

METODOLOGÍA – TÉCNICAS ^{xi}	HERRAMIENTAS
Rastreo: Búsqueda en la fuentes abiertas Whois, interfaz web a whois, ARIN whois, Transferencia de zona DNS	USENet, motores de búsqueda, Edgar, Cualquier cliente UNIX
Exploración: Barrido ping, Exploración de puertos TCP/UDP, detección del sistema operativo	Fping, icmpenum WS_Ping, ProPackNmap, SuperSacan, fscanNmap, queso, siphon
Enumeración: Lista de cuentas de usuario, lista de archivos compartidos, identificación de aplicaciones	DumpAcl, sid2user, sesiones nulas, OnSite admin.Showmount, Nat, Legion, captura de titulares mediante telnet o netcat, rpinfo
Obtener Acceso: Adivinación de contraseñas, fuerza bruta sobre los archivos compartidos, Captura de archivos de contraseñas, desbordamiento de búferes	Tcpdump, L0phtcrack, readsmb, NAT, Legion, Tftp, pwdump2 (NT), Ttdb, bind, IIS.HTR/ISM.DLL
Escalada de privilegios: Violación de contraseñas, ataques conocidos	John, L0phtcrack, lc_messages, geTADMIN, sechole
Robo (pilfering): Evaluar sistemas de confianza, buscar contraseñas en texto puro	Rhosts, LSA Secrets, Datos de usuario, archivos de configuración, Registro
Eliminación del rastro: Borrar registros, Ocultar herramientas	Zap, GUI del registro de sucesos, rootkits, ocultación de archivos
Creación de puertas traseras: Crear cuentas de usuario falsas, programar trabajos en diferido, Infectar los archivos de inicio, Plantar servicios de control remoto, Instalar mecanismo de supervisión, sustituir aplicaciones con troyanos	Administradores, miembros de la rueda Cron, AT carpeta inicio, rc, claves del registro, Netcat, memote.exe, VNC, B02k, programas de registro de pulsaciones de tecla, añadir cuentas de correo con alias al administrador Logia, fpnwclnt.dll
Denegación del servicio: inundación SYN, Técnicas ICMP, peticiones src/dst, SYN idénticas, solapamiento de fragmentos/errores de desplazamiento, opciones TCP fuera de límites (OOB), DDoS	Synk4ping of death, smurfland, latierra, teardrop, bonk, newtear, supernube.exe, trincoo/TFN/stacheldraht

^{xi} **Stuart McClure y otros**, HACKERS 4, Editorial McGraw-Hill / Interamericana. España. 2003. Pág. 712