AUDISIS

Versión 2016

SOFTWARE DE AUDITORÍA BASADA EN RIESGOS CRITICOS

PRESENTACION DEL PRODUCTO

AUDITORÍA INTEGRAL Y SEGURIDAD DE SISTEMAS DE INFORMACIÓN "AUDISIS"
Servicios Especializados en Prevención y Reducción de Riesgos, Seguridad y Auditoría de Sistemas
Calle 53 No. 27 - 33 Oficina 602 –Tels.: 2556717 – 2556757 – 2556816, PBX: 3470022 – Bogotá, D.C. Colombia
E-Mail audisis@audisis.com web site: www.audisis.com www.softwareaudis.com
AUDISIS: Fundada en 1.988

Contenido

1. QUÉ PUEDE HACER CON LA POTENCIA DE AUDIRISK?

AUDIRISK, Auditoría Basada en Riesgos para procesos y sistemas de información, es un software en tecnología Web (Cloud Computing) diseñado "por auditores para auditores", ***para conducir*** las siguientes actividades de las auditorías internas y externas, de conformidad con las normas y procedimientos de auditoría generalmente aceptados, con las normas de auditoría interna promulgadas por el Instituto de Auditores Internos (IIA) y las normas de auditoría de sistemas emitidas por la Asociación de Control y Auditoría de Sistemas (ISACA):

a) Planeación Anual de la Auditoría Basada en "Valoración de la Exposición a Riesgos". El plan anual se elabora con base en los resultados de "valorar la exposición a riesgos", individualmente para los procesos del modelo de operación de la Empresa, los procesos de a infraestructura de Tecnología de Información y los sistemas de información (aplicaciones y ERPs) que soportan el manejo de las operaciones de negocio y administrativas de la organización.

b) *Desarrollo de auditorías a procesos y sistemas de información, "Basadas en Riesgos Críticos". Comprende:* *a)* Planeación detallada de la auditoría; b) Identificación y evaluación de *una muestra de eventos de riesgo inherentes críticos de* cada proceso o sistema que serán revisados por la auditoría; c) Evaluación de la *efectividad de los controles internos existentes* (eficacia + eficiencia) para mitigar cada evento de riesgo inherente; d) Diseño y evaluación de pruebas de cumplimiento por evento de riesgo inherente, para los controles establecidos cuando éstos son efectivos para mitigar el riesgo; e) Diseño y Evaluación de pruebas sustantivas por cada evento de riesgo inherente para determinar el impacto de las debilidades de control sobre la exactitud de la información que genera el proceso; f) Elaboración de informes para comunicar los resultados de la auditoría (ejecutivos y detallados); y g) seguimiento a los hallazgos de la auditoría y las acciones de mejora que los auditados decidan implementar para atender los hallazgos.

c) G*estionar los Resultados de la Auditoría* - Presentar informes con los resultados obtenidos por la auditoría en fechas de corte determinadas por el auditor, con indicadores de Gestión, estadísticas y gráficos sobre el avance de desarrollo y cumplimiento del plan anual de la auditoría y el estado de atención de los auditados a los hallazgos y acciones de mejora presentadas por la auditoría como necesarias (estado de hallazgos y acciones de mejora).

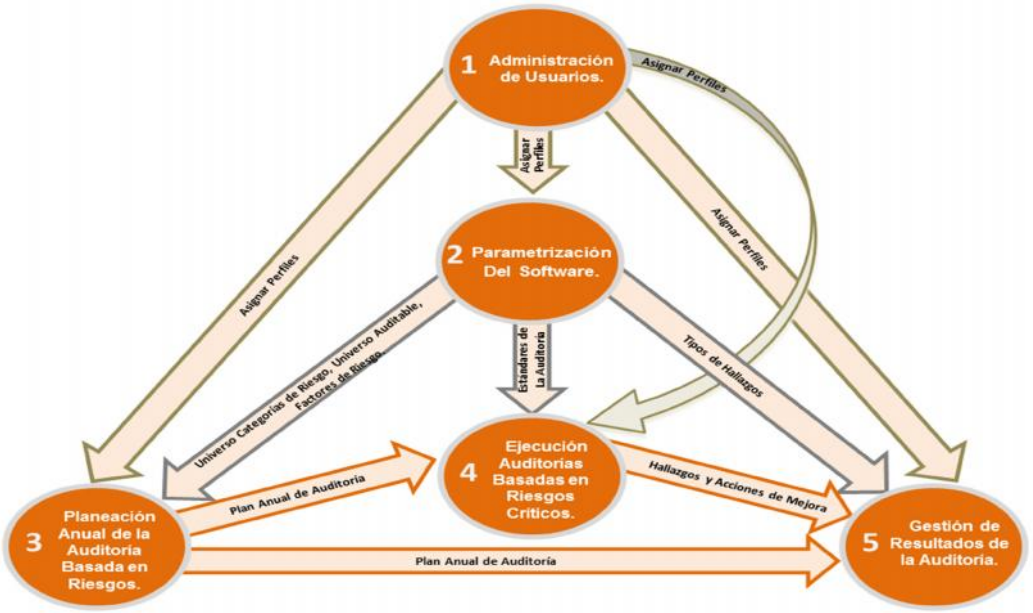

Figura 1: Módulos del software AUDIRISK

El software AUDIRISK puede ser instalado en ambientes WEB (Cloud Computing) en una red interna o en computadores de stand alone.

La **Auditoría Basada en Riesgos Críticos** *"es una forma de conducir las auditorías internas y externas de diferentes tipos (de procesos, de sistemas de información, operativa, de estados financieros, de sistemas de gestión, etc),* ***con enfoque preventivo y proactivo,*** *basando su planeación y desarrollo en* ***una muestra de eventos de riesgo inherentes*** *que pudieran causar el mayor impacto negativo en la organización, para confirmar si el manejo de las operaciones y de la información se realizan de conformidad con las buenas y mejores prácticas de control interno y seguridad, las reglas del negocio y las normas leyes y regulaciones aplicables".*

Como punto de partida y apoyo para planear y realizar las auditorías, AUDIRISK **provee una Base de Datos de Conocimientos de Auditoría** que contiene numerosas *"mejores y buenas prácticas"* sobre: clases o categorías de riesgos[1] (por ejemplo, las clases de riesgo de los modelos SARO, SARLAFT, MECI y AUDISIS); eventos de riesgo negativos (amenazas) que pueden originar las clases de riesgo (por ejemplo, eventos que originan fraude interno, fraude externo, fallas tecnológicas, riesgo estratégico, riesgo reputacional, etc.); mejores prácticas de controles aplicables a los eventos de riesgo negativos; las relaciones entre eventos negativos y controles aplicables (por ejemplo, los controles para el evento de riesgo "Falsificación de documentos de identificación"); Cuestionarios de factores de riesgo

[1] **Clases o Categorías de Riesgo:** Son nombres genéricos utilizados para clasificar y agrupar los eventos de riesgo negativos o amenazas que podrían causar daños a los activos de la empresa y obstaculizar la consecución de los objetivos de la organización. Por ejemplo, para el SARO se establecen siete (7) categorías de riesgo; para SARLAFT 4 categorías y para MECI cinco (5) categorías. En SARO son: fraude interno, fraude externo, daños a activos físicos, fallas en atención a los clientes, fallas en las relaciones laborales, fallas tecnológicas y errores en la administración y ejecución de procesos.

para estimar la exposición a riesgos potenciales; objetivos de control para procesos de TI, dominios de ISO 27001 y aplicaciones de computador; técnicas para realizar pruebas de auditoría (de cumplimiento, sustantivas y de doble propósito); cuestionarios para evaluar los criterios de la información de negocios (eficiencia, eficacia, integridad, disponibilidad, confidencialidad, confiabilidad y cumplimiento).

La *base de datos de conocimientos de Auditoría, suministrada por AUDIRISK,* provee tablas para ser pobladas con información de la empresa, como las siguientes: vulnerabilidades; factores de riesgo; agentes generadores de riesgo; áreas de la estructura de organización de la empresa; procesos del modelo de operación de la empresa (estratégicos, misionales, de soporte y de supervisión y control); estructura de cargos; nombres de los funcionarios y nombres de regionales de la Empresa. Esta base de conocimientos también provee estándares para evaluación y análisis de riesgos, evaluación de control interno y evaluación de resultados de las pruebas de auditoría (de cumplimiento y sustantivas), planeación y seguimiento de los hallazgos de auditoría y de las acciones de mejora adoptadas, y los papeles de trabajo de las auditorías en formato electrónico.

*El contenido de la **Base de Datos de Conocimientos de Auditoría de la Empresa** crece continuamente en la medida que se avanza en la realización de las auditorías a los procesos y sistemas de la Empresa, para convertirse en el repositorio único de los CONOCIMIENTOS GENERADOS POR LA AUDITORÍA y de los papeles de trabajo electrónicos con la información de todas las auditorías realizadas en la Empresa a través del tiempo*.

La propiedad intelectual del software AUDIRISK está registrada a nombre de AUDISIS.

El software se oferta por equipo servidor y cantidad de usuarios en dos modalidades de licenciamiento: a) Adquisición de Licencias de Uso a perpetuidad y b) Arrendamiento Anual. También se ofrece el servicio de Asesoría para la integración del software a los procedimientos del proceso de Auditoría de la Empresa.

2. PROPUESTA DE VALOR QUE GENERA EL SOFTWARE "AUDIRISK"

Las siguientes son algunas características de las auditorías realizadas con AUDIRISK*, que **generan valor percibido** para las Empresas:*

1) El cumplimiento con las normas y procedimientos de auditoría generalmente aceptados, con las normas de auditoría interna emitidas por el IIA, las normas de auditoría de sistemas emitidas por ISACA y con estándares nacionales e internacionales de Control Interno Organizacional (COSO 2013, COBIT, MECI, ISO 27001, ISO 22301) y de Gestión de Riesgos Empresariales (ISO 31000 y ERM).

2) *La Auditoría es PROACTIVA Y PREVENTIVA y tiene como objetivos* ***evaluar y verificar*** *que los procesos y sistemas y de la empresa sean eficaces, eficientes y seguros, es decir, que satisfacen los objetivos de empresa y están adecuadamente protegidos contra los eventos de riesgo críticos que pudieran presentarse en el desarrollo de las operaciones.* ***Estas auditorías se anticipan a la ocurrencia de los eventos de riesgos inherentes para ayudar a prevenirlos.*** El objetivo de la Auditoría **NO ES:** "Detectar e investigar los errores e irregularidades que ocurran o se presenten en la operación de los procesos y sistemas de la organización - **NO ES descubrir, detectar o investigar eventos de riesgo ocurridos**.

3) Como punto de partida y apoyo para planear y realizar las auditorías, AUDIRISK **provee una Base de Datos de Conocimientos de Auditoría** que contiene numerosas *"mejores y buenas prácticas"* sobre: clases o categorías de riesgos, eventos de riesgo negativos (amenazas) que pueden originar las clases de riesgo; mejores prácticas de control aplicables a los eventos de riesgo negativos; las relaciones de dependencia entre eventos negativos y controles aplicables; Cuestionarios de factores de riesgo para estimar la exposición a riesgos potenciales; objetivos de control para procesos de TI, dominios de ISO 27001 y aplicaciones de computador; técnicas de auditoría; y cuestionarios para evaluar los criterios de la información de negocios (eficiencia, eficacia, integridad, disponibilidad, confidencialidad, confiabilidad y cumplimiento).

4) ***Los cuestionarios*** para evaluar la exposición a riesgos de los procesos y sistemas, identificar los eventos de riesgo inherentes que integran la muestra de riesgos seleccionada por la auditoría, identificar los controles establecidos, las listas de comprobación (checklists) de controles y las listas de comprobación de exactitud de la información que pudiera ser impactada por las debilidades de control existentes*,* ***no son insumos que el auditor prepara previamente para ser ingresados al software****; estos son productos generados por el software a la medida de las necesidades identificadas por el auditor en el análisis de los eventos de riesgo inherentes sobre los que se planea y ejecuta cada auditoría.*

5) La auditoría verifica que las políticas, normas y procedimientos de control interno y Gestión de Riesgos de la organización, *utilicen el* ***enfoque proactivo ó "A priori" de diseño e implantación de los controles, es decir, que los controles actúen antes de presentarse los riesgos inherentes****, con el objetivo de reducir la posibilidad y/o el impacto de la ocurrencia de los eventos de riesgo en el ambiente de operación.*

6) Para identificar los controles que el auditor considera necesarios por mitigar cada evento de riesgo inherente, el software provee funcionalidades ***para generar cuestionarios de controles que "deberían existir"****, en lugar de elaborar los cuestionarios con los controles establecidos o existentes, los cuales a veces no están documentados y no son conocidos por los auditados.* Para este fin, la auditoría se apoya en las best practices de control documentadas en la Base de Conocimientos de Auditoría suministrada por el proveedor del software y genera cuestionarios *con formato de Guías de Auto-evaluación o auto-aseguramiento de controles (conocidas por sus siglas en inglés como CSA: Control Self Assessment).*

7) *La auditoría verifica que los controles establecidos por cada evento de riesgo inherente**, satisfagan dos requisitos para ser eficaces:*** a) Eliminan las vulnerabilidades que pudieran crear el ambiente propicio para ocurrencia de los eventos de riesgo y b) bloquean o neutralizan los agentes generadores de los eventos de riesgo.

8) *Cada auditoría evalúa el estado de la "Cultura de Riesgos y Controles" existente en la Empresa y los auditores **actúan como "Agentes de Cambio"** para promover su mejoramiento.*

9) *Cada auditoría aplica y promueve la implantación del enfoque de los "**tres anillos de seguridad o Líneas de defensa" y del nivel de automatización y no discrecionalidad de los controles,*** como factores claves para asegurar la "eficacia" de los controles, es decir, su capacidad para reducir la severidad de los eventos de riesgo inherentes a niveles de riesgo residual aceptables. Para evaluar la "eficiencia de los controles", aplica criterios para asegurar que la relación costo /beneficio de los controles establecidos sea RAZONABLE.

10) *Para los eventos de riesgo inherentes críticos seleccionados por la auditoría, el software evalúa y mide cualitativamente la "efectividad de los controles internos establecidos"**, como base para determinar la naturaleza y extensión de las pruebas de auditoria que deben efectuarse** – de cumplimiento y sustantivas.* La escala de calificaciones de efectividad de los controles es la siguiente: 1- Apropiada, 2-Mejorable, 3-Insufiicente, 4- Deficiente y 5- Muy deficiente.

11) Para los eventos de riesgo inherentes críticos que presentan efectividad de los controles APROPIADA ó MEJORABLE, ***el software genera checklists con formato CSA para comprobar el cumplimiento de los controles establecidos para el proceso en diferentes sitios de prueba***. Con base en estos checklists, la auditoría verifica y mide cualitativamente el porcentaje de "Cumplimiento de los controles internos establecidos" en cada sitio de prueba.

12) Para los eventos de riesgo inherentes críticos que presentan efectividad de los controles INSUFICIENTE, DEFICIENTE Y MUY DEFICIENTE, ***el software genera checklists para comprobar la exactitud de los datos generados por el proceso que pudieran se impactados por las debilidades de control identificadas en el proceso, en diferentes sitios de prueba.*** La auditoría verifica y mide cualitativamente el porcentaje de "Exactitud de los Datos que pudieran ser impactados por los eventos de riesgo con debilidades de control" en cada sitio de prueba.

13) Para los siete (7) criterios que debe satisfacer la información de negocios generada por cada proceso o aplicación de computador*, el software genera cuestionarios (checklists) orientados a "Evaluar y medir cualitativamente el porcentaje de satisfacción de cada uno de los criterios".*

14) *E*l software AUDISIS ***genera los informes con los resultados de la auditoría (ejecutivos y detallados),*** los cuales son exportables a diferentes formatos (PDF y Word entre otros). Estos presentan la opinión, conclusiones, hallazgos y acciones de mejora consideradas como "necesarias" por la auditoría, sobre la evaluación del control interno existente en cada una de las actividades del proceso o sistema que fueron evaluadas y de las pruebas de auditoría

realizadas (de cumplimiento y sustantivas) en los diferentes sitios de prueba y los resultados de estas consolidados a nivel empresa. Estos informes se soportan con tablas que contienen las evaluaciones numéricas y porcentuales para los eventos de riesgo auditados, gráficos y colores para indicar la severidad de los riesgos inherentes auditados antes de aplicar los controles establecidos, después de controles y después de las pruebas de auditoría.

15) AUDIRISK facilita la transición de los auditores, del estado de "*ser y actuar como consumidores de conocimientos"* a convertirse en *"generadores de conocimiento y de valor para las organizaciones".*

16) El software ***genera archivos de papeles de trabajo en formato electrónico (archivo permanente y archivo de papeles de trabajo corrientes).*** El software AUDIRISK, en cada una de las ocho etapas de la Auditoría Basada en Riesgos, genera los papeles de trabajo de la auditoría en formato electrónico y exportable a PDF y otros formatos.

17) ***El software ofrece alternativas para iniciar las nuevas auditorías a partir de los papeles de trabajo de la auditoría anterior.*** El software AUDIRISK permite iniciar nuevas auditorías a un proceso o aplicación de computador, basándose en los papeles de trabajo electrónicos de auditorías anteriores realizadas con AUDIRISK. Esta funcionalidad genera ahorros de tiempo e incrementa la productividad en las auditorías.

3. FUNCIONALIDADES DEL SOFTWARE AUDIRISK.

MÓDULO 1: ADMINISTRACIÓN DE USUARIOS.

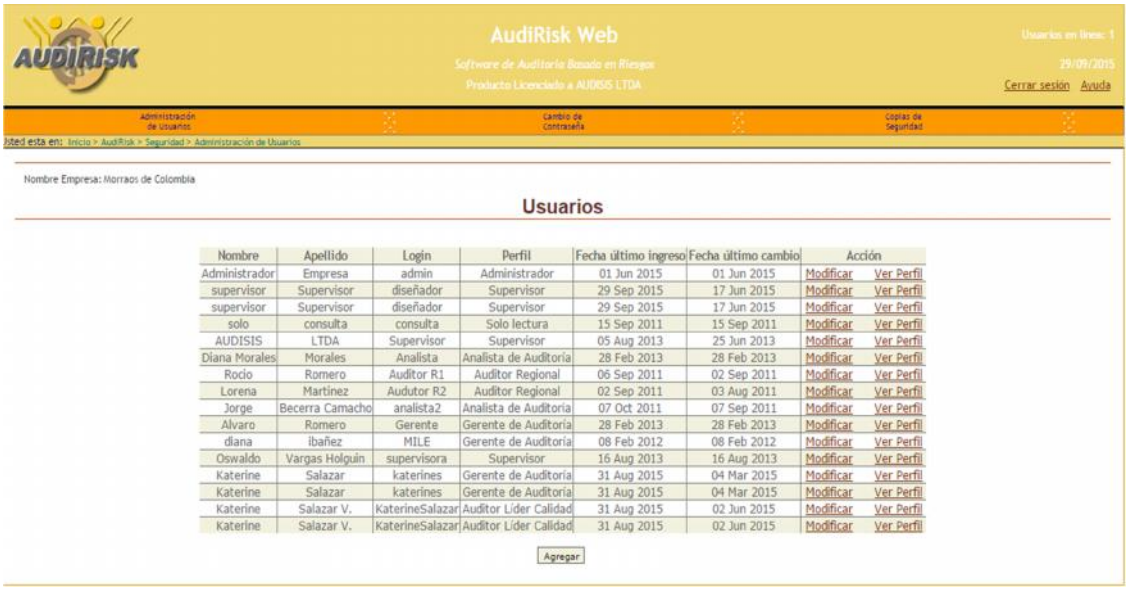

Figura 2: Módulo Administración de Usuarios

Este módulo provee funcionalidades para administrar los usuarios con derechos de acceso a los diferentes módulos del software. Permite adicionar, modificar e inactivar usuarios y establecer el perfil y los privilegios de acceso a cada uno módulos de AUDIRISK. El software maneja los siguientes perfiles:

- Gerente de Auditoría.
- Administrador de Usuarios.
- Supervisor de Auditoría.
- Analista de Auditoría (Auditor de Procesos o de aplicaciones).
- Auditor Regional.
- Solo Consulta.

AUDIRISK ofrece dos opciones de autenticación de usuarios: 1) Autenticación manejada por la aplicación, en la que el administrador del software deberá ingresar los usuarios y 2) Autenticación a través del directorio activo usado en los sistemas operativos Windows.

MODULO 2: PARAMETRIZACIÓN DEL SOFTWARE.

Figura 3: Módulo Parametrización

En este módulo, AUDIRISK provee funcionalidades para *configurar los estándares de trabajo de las Auditorías Basadas en Riesgos* que serán utilizadas en las actividades de análisis y evaluación de riesgos, evaluación de efectividad de los controles establecidos, análisis y evaluación de resultados de pruebas de cumplimiento y sustantivas, evaluación de la satisfacción de los siete (7) criterios de la información de negocios (eficacia, eficiencia, integridad, disponibilidad, confidencialidad, confiabilidad y cumplimiento) y obtener copias de respaldo de la base de conocimientos y de los papeles de trabajo electrónicos de las auditorías realizadas.

El software provee ayudas para *cargar información privada de la Empresa* en la Base de Datos de Conocimientos de Auditoría de la Empresa**.** Por ejemplo: Categorías o clases de Riesgo del *universo de riesgos de la Empresa*; eventos de Riesgo Negativos (Amenazas), *Mejores y Buenas Prácticas de Contro*l, activos impactados por los riesgos, técnicas de Auditoría, Areas Organizacionales, Zonas Geográficas, nombres de los cargos de la empresa, Nombres de los Funcionarios de la Empresa y Objetivos de Auditoría.

También provee ayudas para *configurar el correo electrónico corporativo de la Auditoría, cargar y enviar automáticamente mensajes de recordatorio* dirigidos a los responsables de implantar, supervisar la implantación y hacer seguimiento a las acciones de mejora por hallazgos de Control Interno, de pruebas de cumplimiento, de pruebas sustantivas y de las acciones de mejora por hallazgos de Auditorías Efectuadas por Terceros.

MÓDULO 3: PLANEACIÓN ANUAL DE LA AUDITORÍA, BASADA EN VALORACIÓN DE RIESGOS.

Este módulo de AUDIRISK conduce a elaborar la Planeación Anual de las Auditorías internas y Externas, *basada en la valoración de la Exposición a Riesgos de las operaciones y servicios de las empresas*.

Para las auditorías internas, la "Exposición a riesgos" se valora en los procesos del modelo de operación y los servicios de sistemas de la Empresa. Para las auditorías externas, la "exposición a riesgos" se valora en las operaciones de misión crítica de las empresas (clientes) que serán auditadas, de acuerdo con el sector económico al que correspondan.

En la auditoría interna, los procesos y servicios de sistemas que serán auditados corresponden a procesos del modelo de operación de la empresa (estratégicos, misionales, de soporte y de supervisión y control), procesos de tecnología de información (del modelo COBIT, por ejemplo), aplicaciones de computador o módulos de ERPs y otros trabajos que requieran su atención.

Para las Auditorías Externas (realizadas por firmas de Auditores y entidades de Control y supervisión del Estado), las auditorias se programan por cada entidad o empresa que requiera ser auditada durante el año.

Elaboración del Plan Anual de la Auditoría Interna.

Para las Auditorías Internas, el software AUDIRISK satisface las exigencias de los estándares de auditoría del Instituto de Auditores Internos de los Estados Unidos (IIA) e ISACA (la asociación de Control y Auditoría de Sistemas de Información), los cuales establecen que el plan anual de la auditoría debe realizarse con un enfoque *"basado en valoración de riesgos".*

Figura 4: Planeación Anual de Auditorías Internas

Por cada grupo de trabajos que integran el *universo de auditoría*[2], el software ofrece funcionalidades y el apoyo de la *base de datos de conocimientos de auditoría,* suministrada por AUDIRISK, para diseñar, contestar y procesar cuestionarios con factores de riesgo, estimar la exposición a riesgos (necesidades de seguridad) de cada uno de trabajos candidatos a ser auditados y elaborar el *"panorama de riesgos de la Empresa"*[3] con la estimación porcentual de la exposición a riesgos en los *componentes del universo de auditoría* y los componentes del *universo de riesgos de la Empresa* (por ejemplo: las clases o categorías de riesgo de los modelos SARO, SARLAFT, MECI, AUDIRISK o combinación de las anteriores).

Con los resultados del procesamiento de los cuestionarios, AUDIRISK produce ***matrices de exposición a riesgos*** (factores de riesgo Vs. categorías de riesgo) por cada uno de los procesos del modelo de operación y los servicios de sistemas, en las que se visualizan el puntaje total de exposición a riesgos (en el rango de 1 a 100) y los puntajes obtenidos por las categorías de riesgo aplicables y los factores de riesgo del cuestionario.

Con el agrupamiento de las matrices de riesgo individuales, el software produce ***Matrices de Exposición a Riesgos Consolidadas*** (procesos o sistemas Vs. categorías de riesgo) para tres grupos de trabajos de auditoría: a) Los procesos del modelo de operación de la empresa; b) Los procesos de Tecnología de Información y, c) Las Aplicaciones de Computador de la Empresa. De cada una de estas estas matrices, el software provee dos alternativas para seleccionar los procesos y aplicaciones que serán incluidas en el plan anual de la auditoria. Estas son:

a) Por el puntaje de exposición a riesgos obtenido por cada uno de los procesos o las aplicaciones de computador (en el rango de 1 a 100). Las prioridades para el plan de auditoría se asignan de mayor a menor puntaje, y

b) Por el *puntaje de exposición a riesgos consolidado obtenido por cada una de las clases o categorías de riesgo aplicables* a los procesos (del modelo de operación o de TI) o las aplicaciones de computador. Las prioridades para el plan de auditoria se asignan de mayor a menor puntaje.

Por cada grupo de trabajos del universo de auditoría, el software provee las funcionalidades para generar *"panoramas de riesgos del Universo de Auditoría Interna de la Empresa*[4]*"*. Estos panoramas

[2] **Universo de Auditoría:** Los tres grupos de trabajos que integran el universo de la auditoría son: a) los procesos del modelo de operación; b) los procesos de TI y c) las aplicaciones de computador o módulos de ERPs

[3] **Panorama de Riesgo:** Esta expresión se utiliza para nombrar al análisis que se realiza respecto a la **fragilidad** o a las condiciones más vulnerables de una **organización**. El análisis puede aplicarse sobre distintos aspectos o sectores de la entidad, tales como las operaciones de negocio, lavado de activos y financiación del terrorismo, riesgo laboral, riesgos ambientales y riesgos de la información. Cuando se considera el panorama general de riesgos de la empresa, este hace mención al Universo de Riesgos de la Empresa.

[4] **Panorama de Riesgos del Universo de Auditoría:** Los porcentajes de exposición a riesgos para los componentes de tres grupos de trabajos que integran el universo de la auditoría: a) los procesos del modelo de operación; b) los procesos de TI y c) las aplicaciones de computador. Dentro de cada grupo, los panoramas de riesgo presentan los porcentajes de

de riesgo se producen por tres conceptos: a) Para priorizar los trabajos dentro de los tres (3) grupos de trabajo del universo de auditoría; b) Para priorizar las categorías de riesgo dentro de cada grupo del universo de auditoría y c) Para priorizar las categorías de riesgo aplicables a cada proceso o aplicación de computador.

El software AUDIRISK también provee funcionalidades para incluir en el plan anual de la Auditoría Interna: la programación de auditorías a sistemas de gestión (calidad, ISO 27001, ambiental, riesgos laborales y otras), el seguimiento a los hallazgos de auditorías realizadas por terceros (Revisores Fiscales, Organismos de Control del Estado y Auditores Externos) y otros trabajos que sean asignados a la Auditoría Interna.

Por cada proceso, aplicación de computador o trabajo seleccionado para el plan anual, el software provee funcionalidades para ***programar las auditorías a realizar***. Por ejemplo, programar: evaluación del control interno, pruebas de cumplimiento, pruebas sustantivas, auditoría completa (control interno + pruebas de cumplimiento + pruebas sustantivas), seguimientos a hallazgos de control interno, seguimiento a hallazgos de pruebas de cumplimiento, seguimiento a pruebas sustantivas o seguimiento a la auditoría completa. Porcada auditoría programada se asignan recursos de tiempo, personal y financieros.

Con las auditorías programadas, el software genera el ***plan anual de la auditoría***. Esta opción presenta en pantalla y en forma impresa, el resumen de auditorías programadas y el cronograma correspondiente.

Finalmente, el software provee funcionalidades para conducir el seguimiento a la ejecución del plan anual de la Auditoría Interna.

Elaboración del Plan anual de Auditorías Externas.

Para las empresas candidatas a ser auditadas dentro de cada sector económico, el software ofrece funcionalidades y el apoyo de la *base de datos de conocimientos de auditoría*, suministrada por AUDIRISK, para diseñar, contestar y procesar cuestionarios con factores de riesgo, estimar la exposición a riesgos (necesidades de seguridad) de cada una de las empresas candidatas a ser auditadas y elaborar un "panorama de riesgos" de cada Empresa con la estimación de la *exposición a las clases o categorías del Universo de Riesgos* aplicable a cada sector económico (por ejemplo: las clase de riesgo de los modelos SARO, SARLAFT, MECI, AUDIRISK o combinación de las anteriores).

AUDIRISK provee funcionalidades para realizar la valoración de la exposición a riesgos de las empresas dentro del sector de la economía al que correspondan, priorizar las entidades o empresas que serán

---

exposición a riesgos de cada una de las categorías de riesgo aplicables. Dentro de cada proceso o aplicación de computador, también se muestran los porcentajes de exposición a riesgos de las categorías de riesgo aplicables.

auditadas en el año por sectores, programar las auditorías de cada empresa y asignar recursos de tiempo, personal y financieros. Elabora cronograma anual y conduce el seguimiento a la ejecución del plan anual de auditorías externas.

MÓDULO 4: AUDITORÍAS "BASADAS EN RIESGOS CRÍTICOS" A PROCESOS Y SISTEMAS DE INFORMACIÓN.

Objetivos y Alcance de las Auditorías.

Figura 5: Módulo de Auditoría Basada en Riesgos Críticos

En AUDIRISK, las *"Auditorías Basadas en Riesgos"* tienen como objetivo revisar las actividades, procedimientos, controles e información de un proceso o sistema de información, con el análisis de una muestra *de eventos de riesgo negativos (amenazas)* que podrían presentarse y originar las **clases o categorías de riesgos críticas** en el proceso o sistema sujeto a auditoría. Por ejemplo, en un proceso de cartera las clases de riesgos aplicables son diez (10) y de estas, *las críticas son tres (3)*: Fraude Interno, Fraude Externo y Fallas Tecnológicas; la revisión de la auditoría se ejecutaría para una muestra de treinta (30) eventos de riesgos potencial, diez (10) eventos por cada categoría de riesgo crítica.

Este módulo de AUDIRISK ofrece funcionalidades para planear y desarrollar *cuatro (4) tipos de auditorías basadas en riesgos críticos:*

1) A procesos del modelo de operación de la Empresa (procesos estratégicos, misionales, de soporte y de supervisión y control);

2) A procesos de Tecnología de Información y Comunicaciones (por ejemplo, los procesos COBIT e ITIL);
3) A las aplicaciones de computador en producción (ó módulos de ERPs), y
4) A los componentes clave de la Infraestructura de Tecnología de Información.

Por cada auditoría basada en riesgos, el software ofrece funcionalidades con procedimientos, guías y formatos para conducir el desarrollo de las (4) cuatro fases del proceso de auditoría: 1) Planeación basada en riesgos, 2) Ejecución, 3) Comunicación de resultados y 4) Definición de acciones de mejora por los hallazgos de auditoría, planeación y ejecución de seguimientos. *La figura 6,* ilustra el enfoque de las auditorías realizadas con **AUDIRISK**.

Figura 6: *Las 4 Fases del proceso de Auditoría*

En la fase I, *Planeación detallada de la Auditoría de cada proceso o sistema,* AUDIRISK asiste la definición del memorando de planeación de la auditoría (definición de objetivos, alcance, recursos asignados y programa de trabajo), la comprensión del contexto interno y externo del proceso o sistema y la identificación, análisis y evaluación de severidad de *una muestra de eventos de riesgo inherentes críticos* para los cuales se ejecutarán la evaluación de control interno y las pruebas de auditoría. Con la información obtenida construye un *Cubo de Riesgos de la Auditoría*, el cual incluye el mapeo de la muestra de eventos de riesgo inherentes (amenazas) que podrían originar las clases de riesgos críticas, en las 3 dimensiones del cubo del proceso o sistema sujeto a auditoría: a) las actividades del proceso o sistema (escenarios de riesgo); b) las áreas organizacionales y terceros que intervienen en el proceso; y c) las categorías o clases de riesgos críticos. Este cubo puede considerarse

como una aproximación de la auditoria al *cubo de Control Interno de COSO y ERM (Enterprise Risk Management).*

En la fase 2, *Ejecución de la Auditoría*, por cada proceso o sistema sujeto a auditoría, AUDIRISK conduce a los auditores a la consecución de dos grandes objetivos: **el primero, evaluar la efectividad de los controles establecidos en el proceso o sistema** para una muestra de eventos de riesgo inherente seleccionados según el criterio de la auditoría, **asumiendo que los controles son "un estándar que debe aplicarse en todos los sitios de operación de la empresa"**. El propósito es *evaluar la efectividad (eficacia + eficiencia) de los controles establecidos para reducir el riesgo a niveles aceptables de riesgo residual*; esta evaluación es la base para determinar la naturaleza y extensión de las pruebas de auditoría que deban efectuarse. La evaluación se realiza para cada uno de los eventos de riesgo inherente localizados las actividades (escenarios de riesgo) del proceso o sistema.

El **segundo objetivo de la auditoría es diseñar, planear y ejecutar pruebas de cumplimiento** a los controles de los eventos de riesgo que tienen controles con efectividad "*apropiada"* y **pruebas sustantivas** *a la información que pudiera ser impactada por los eventos de riesgo que presentan debilidades de control (efectividad mejorable, insuficiente, deficiente o muy deficiente)***.** La evaluación del control interno como un estándar en todos los sitios de operación se realiza *una sola vez para todo el proceso*, mientras que las pruebas de auditoría *se ejecutan múltiples veces*, al menos una vez en *diferentes sitios de prueba,* es decir, en cada una de las áreas organizacionales y terceros que intervienen en el proceso o sistema objeto de la auditoría.

En la fase 3, *Comunicación de Resultados,* el software AUDIRISK conduce a los auditores a elaborar cuatro (4) tipos de informes (detallados y ejecutivos) con los resultados de la auditoría de cada proceso o sistema: *Auditoría a la Efectividad del Control Interno Existente; b) Resultados de las pruebas de cumplimiento; c) Resultados de las pruebas sustantivas y d) Satisfacción de criterios de la información de negocios generada por el proceso o sistema auditado*. Por cada uno de estos informes, se presenta la opinión de la auditoría, soportada con mediciones (indicadores) del estado de los eventos de riesgo auditados, gráficas, los hallazgos de la auditoría, el análisis del impacto que podrían causar los hallazgos y las acciones de mejora recomendadas por la auditoría.

La fase 4, *Seguimiento*, AUDIRISK conduce a los auditores en las actividades de elaboración del plan de mejoramiento concertado con los auditados para atender los hallazgos de la auditoría, la planeación del seguimiento, la emisión automática de correos electrónicos de recordatorio a los cargos asignados como responsables de atender los hallazgos de la auditoría (implantar, supervisar implantación y auditor asignado al seguimiento), el registro de resultados del seguimiento y cierre del seguimiento de los hallazgos de cada auditoría.

Metodología de AUDIRISK para planear y desarrollar las Auditorías "Basadas en Riesgos Críticos".

Por cada auditoría, el software **AUDIRISK** ofrece funcionalidades para conducir las cuatro fases del proceso de auditoría, mediante el desarrollo de procedimientos de auditoría de aceptación general, organizadas en un menú de ocho *(8) etapas*, las cuales se describen a continuación y se visualizan en el menú de la *figura 7.*

- **Etapa 1: Pre – auditoría.** El software conduce las actividades para definir los objetivos, alcance, recursos a emplear por la auditoría y el programa de trabajo de la Auditoría. Esta etapa está restringida para ser realizada por el Gerente de Auditoría o el Supervisor de Auditoría.

- **Etapa 2: Comprensión del proceso o sistema (Familiarización).** El software conduce a los auditores en la obtención de la información necesaria para comprender el contexto interno y externo del proceso o sistema objeto de la auditoría y elaborar el archivo permanente o expediente continuo de la auditoría y la caracterización del proceso o sistema sujeto a auditoría. *Este es un paso necesario porque no se puede auditar lo que no se conoce.*

Figura 7: Etapas del proceso de Auditoría Basada en Riesgos críticos

- **Etapa 3: Identificar, analizar y priorizar los Eventos de Riesgo Inherentes Críticos.** Apoyándose en la base de datos de conocimientos suministrada por AUDIRISK, el software conduce actividades para: a) identificar las tres o cuatro categorías de riesgos que sean **críticas** para el proceso o sistema objeto de la auditoría; b) Identificar una muestra de los eventos de riesgo negativos que podrían generar las categorías de riesgo críticas (mínimo 18, máximo 30); c) Documentar, analizar y evaluar la severidad (priorizar) de los eventos de riesgo; d) Elaborar mapas de riesgos inherentes (por categoría de riesgo crítico, escenario de riesgo y área organizacional que interviene en el proceso).

  El análisis de los riesgos inherentes se realiza solamente para una muestra de eventos de riesgo asociados con las tres o cuatro clases de riesgo críticos que podrían presentarse en el ambiente

real de las operaciones del proceso. Por ejemplo, en el proceso de cartera se identifican y analizan diez (10) amenazas por cada una de las tres (3) clases de riesgos críticos: Fraude Interno, Fraude Externo y Fallas Tecnológicas.

Para analizar los eventos de riesgo inherente seleccionados por la auditoría, el software conduce a documentar siete (7) elementos por cada evento de riesgo: a) activos impactados; b) factores de riesgo y agentes generadores de riesgo; c) vulnerabilidades que podrían ser explotadas por los agentes generadores del riesgo; d) evaluación de la severidad o nivel de exposición (con base en estimaciones de la frecuencia anual de ocurrencia y del impacto financiero y operacional); e) fuentes del riesgo (actividades del proceso y áreas que intervienen en las operaciones del proceso), f) las consecuencias en caso de ocurrir, y g) el propietario del riesgo y el indicador de ocurrencia del evento.

Por cada evento, la severidad de la exposición al riesgo se mide con una de las siguientes cuatro (4) calificaciones: E: Extremo (Color rojo); A: Alto (color naranja); M: Moderado (color amarillo) y B: Bajo o dentro del apetito de riesgos de la Gerencia (color verde). Los eventos, después de evaluada su severidad, se ubican en el **Mapa de Riesgos Inherentes** (una matriz de 5x5) y se despliegan organizadamente para las tres (3) dimensiones del **Cubo de Riesgos del proceso** que se está auditando: a) por categorías de riesgo críticas, b) por Dependencias (áreas de la estructura de organización o terceros) y c) por actividades del proceso.

Como entregables de esta etapa, el software produce el *mapa de riesgos inherentes del proceso* (una matriz de 5x5 en la que se localizan las amenazas según su evaluación de probabilidad de ocurrencia e impacto), la documentación del análisis de los eventos de riesgo inherentes, el perfil de riesgos del proceso por diferentes conceptos y la definición de las alternativas de manejo de riesgos (acciones de respuesta a riesgos) que en opinión de la auditoría deberían emplearse para mitigar los riesgos inherentes.

- **Etapa 4: Definir Contexto de Riesgos de la Auditoría**. El Software conduce a completar la documentación del mapa de riesgos inherentes, con funcionalidades que conducen a describir la posible ocurrencia de las categorías de riesgo críticas del proceso, en tres matrices que despliegan el **Cubo de Riesgos de la Auditoría del proceso:** a) categorías de riesgo Vs Actividades del proceso; b) categorías de riesgos Vs dependencias y c) actividades del proceso Vs dependencias.

  También conduce a definir *los objetivos de control* que debería satisfacer el proceso o sistema sujeto a auditoría en cada sus actividades, de acuerdo con los eventos de riesgo considerados por la auditoría.

- **Etapa 5: Evaluar Efectividad del Control Interno Existente**. Para la muestra de eventos de riesgo inherente (amenazas) considerados por la auditoría, el software conduce a *generar cuestionarios (en Ingles CSA: Control Self Assessment)* con las buenas prácticas de Controles

que deberían utilizarse para reducir la severidad de los riesgos inherentes, como ayuda para identificar los controles que se utilizan en las operaciones del proceso o sistema sujeto a auditoría. También provee funcionalidades para ingresar y procesar las respuestas del cuestionario, *evaluar la efectividad de los Controles por cada evento de riesgo,* documentar y analizar los hallazgos de la auditoría de control interno, generar archivos de papeles de trabajo electrónicos y generar el primer informe con los resultados de la auditoría, sobre *evaluación de la efectividad del control interno existente*.

Para *evaluar la efectividad (eficacia + eficiencia) de los controles* por cada evento de riesgo inherente, el software aplica tres criterios: a) Los controles satisfacen al menos una vez los "*tres anillos de seguridad o barreras de defensa y hacen sinergia"*; b) Los controles son eficaces según su nivel de automatización y discrecionalidad; y c) la relación costo / beneficio de los controles es razonable (costo no mayor del 10% del valor de los activos protegidos).

La efectividad de los controles por cada evento de riesgo se mide con una escala de 5 calificaciones: 1- Apropiada (color verde); 2- Mejorable (color amarillo); 3- Insuficiente (color naranja); 4: Deficiente (color rojo) y 5- Muy Deficiente (color rojo). Con los resultados de la evaluación de los controles establecidos, el software produce *Mapas de Riesgos Residuales* con gráficos y detalles de la evaluación de los eventos de riesgos para las tres dimensiones del **cubo de riesgos** en las cuales podrían materializarse los eventos de riesgo: a) en las clases de riesgo críticas; b) en las actividades del proceso y c) en las dependencias (áreas de la organización y terceros) que intervienen en el proceso.

El software elabora papeles de trabajo electrónicos exportables a varios formatos (Word, PDF) con los soportes de los procedimientos ejecutados por la auditoría y produce el primer informe de la Auditoría, *Informe con los resultados de la Evaluación del Control Interno Existente*, *el que mayor valor agregado genera para los auditados y la administración.*

- **Etapa 6: Pruebas de Cumplimiento.** El software AUDIRISK conduce a diseñar estas pruebas, partiendo de los resultados de la evaluación de los controles establecidos; genera checklists de controles por sitio de prueba (en inglés CSA: Control Self Assessment), procesa las respuestas de los checklists, genera hallazgos de auditoría y conduce su análisis, hasta generar *informes (ejecutivo y detallado) con los resultados de las pruebas de cumplimiento.*

Las pruebas de cumplimiento de los controles se realizan en las dependencias que intervienen en el proceso sujeto a auditoría, para los eventos de riesgo inherente (amenazas) que presentan severidad significativa (E: Extremo; A: Alto o M: Moderado) y los controles establecidos en opinión de la auditoría son eficaces y eficientes (efectividad 1- Apropiada ó 2 - Mejorable).

Los resultados de las pruebas se miden con una escala de cinco calificaciones, dependiendo del porcentaje de cumplimiento de los controles establecidos, así: 1- Apropiada (cumplimiento superior al 80%); 2- Mejorable (cumplimiento entre el 60% y 80%), 3- Insuficiente

(cumplimiento entre 40% y 60%): 4: Deficiente (cumplimiento entre 20% y 40%); y 5- Muy deficiente (cumplimiento entre 0% y 20%). Estos resultados se comparan con los de la evaluación de control interno para mostrar las diferencias entre los controles formalmente establecidos y los que realmente se cumplen. Adicionalmente, el software *genera nuevos mapas de riesgos residuales* con los resultados de estas pruebas y el segundo informe con los resultados de la auditoría.

- **Etapa 7: Pruebas Sustantivas**. El software Audirisk conduce a diseñar las pruebas sustantivas o de exactitud de la información que se procesa con el proceso o sistema, de acuerdo con los resultados de la evaluación de la efectividad de los controles establecidos (etapa 5) y de las pruebas de cumplimiento (etapa 6); genera *checklists de datos (cifras) a verificar por sitio de prueba*, procesa las respuestas de los checklists, genera hallazgos de auditoría y conduce su análisis, genera checklists para evaluar la satisfacción de siete (7) criterios de la información de negocios y procesa las respuestas; finalmente, conduce a *generar los informes (ejecutivo y detallado) con los resultados de las pruebas sustantivas y el informe de evaluación de satisfacción de los siete criterios de la información.*

  Estas pruebas se realizan en las dependencias que intervienen en el proceso, para los eventos de riesgo inherente (amenazas) que presentan severidad de exposición a riesgos significativa (E: Extremo; A: Alto o M: Moderado) y en opinión de la auditoría presentan debilidades importantes de control interno (efectividad 3- insuficiente, 4- Deficiente y 5- muy deficiente). Su propósito es verificar el impacto que pudieran tener esas debilidades de control en la integridad de la información de la empresa.

  Los resultados de estas pruebas se miden con una escala de cinco calificaciones, dependiendo del porcentaje de exactitud de los datos verificados por la auditoría, así: 1- Apropiada (exactitud superior al 80%); 2- Mejorable (exactitud entre el 60% y 80%), 3- Insuficiente (exactitud entre 40% y 60%): 4: Deficiente (exactitud entre 20% y 40%); y Muy deficiente (exactitud en entre 0% y 20%). Con los resultados de las pruebas sustantivas, el software genera el tercer informe con los resultados de la auditoría.

- **Etapa 8: Planeación y ejecución de Seguimiento a Hallazgos y Recomendaciones de la Auditoría.** Como paso final de una auditoría basada en riesgos, el software AUDIRISK ofrece funcionalidades para *elaborar concertadamente con el auditado, el plan de acciones para atender los hallazgos de la auditoría que resultaron de la evaluación del control interno, pruebas de cumplimiento y pruebas sustantivas.*

  El software también provee funcionalidades para *planear y ejecutar el seguimiento a los planes de mejoramiento que se elaboren en la empresa para atender los hallazgos de la auditoría y* para generar y enviar **recordatorios por correo electrónico** a los responsables de implantar, supervisar y ejecutar acciones de mejora.

MÓDULO 5: GESTIÓN DE RESULTADOS DE LA AUDITORÍA.

El Software AUDIDIRISK conduce a generar informes con los resultados de evaluar el cumplimiento del plan anual de la auditoría e indicadores de gestión de la Auditoría frente al plan anual y las auditorías desarrolladas con AUDIRISK durante un periodo de tiempo, dentro del año fiscal.

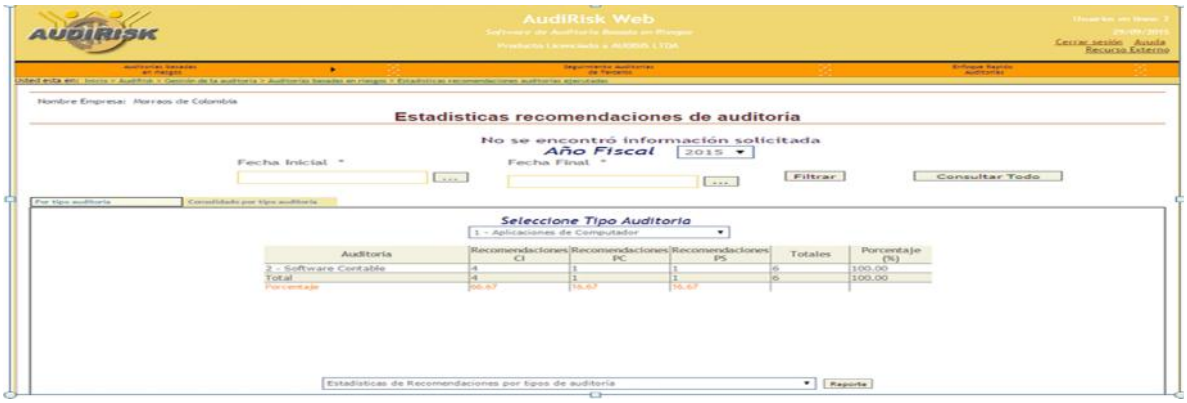

Figura 8: Módulo Gestión de Resultados de la Auditoría

El software ofrece funcionalidades para generar entre otros los siguientes informes de Gestión:

- Estadísticas sobre auditorías desarrolladas en el periodo, programadas y no programadas.
- Estado de ejecución de Auditorías Programadas en el periodo.
- Estadísticas por tipos de hallazgos emitidos (de control interno, pruebas de cumplimiento y pruebas sustantivas), para las auditorías realizadas en el periodo.
- Estadísticas de tipos de hallazgos de auditoría emitidos (de control interno, pruebas de cumplimiento y pruebas sustantivas), clasificados por tipos de auditoría (a procesos del modelo de operación, a procesos de TI, sistemas de información).
- Estadísticas por tipos de hallazgos (de control interno, pruebas de cumplimiento y pruebas sustantivas) sobre el estado de implementación de las acciones de mejora definidas por cada auditoría.
- Estadísticas sobre el estado de implementación de las acciones de mejora (pendientes, en proceso, implantadas, etc) definidas para atender los hallazgos de la auditoría. Se produce por tipos de auditorías realizadas y por dependencias (áreas organizacionales de la Empresa) encargadas de implantarlas.
- Comparación horas programadas y ejecutadas por los auditores asignados, por auditoría y tipos de auditoría.
- Comparación de Costos de personal y otros gastos en la Auditoría, por Auditoría y Tipos de Auditoría.

4. A QUIENES SIRVE LA METODOLOGIA Y EL SOFTWARE AUDIRISK?

El software **AUDIRISK** está diseñado para apoyar el trabajo diferentes grupos de auditores que tienen la responsabilidad de evaluar y verificar el funcionamiento, las operaciones, eficacia, eficiencia y confiabilidad de los procesos y sistemas de las empresas:

- Auditores Internos.
- Auditores Externos.
- Auditores de Sistemas
- Auditores Operativos.
- Auditores Financieros.
- Revisores Fiscales.
- Oficinas de Control Interno Organizacional.
- Auditores de Sistemas de Gestión.

5. ELEMENTOS QUE RECIBE EL CLIENTE.

POR LA ADQUISICIÓN DE LICENCIAS DE USO DEL SOFTWARE AUDIRISK

El licenciamiento del software es a perpetuidad, por servidor y cantidad de usuarios.

Por cada licencia monousuario o en red, el usuario de **AUDIRISK** recibe los siguientes elementos:

✓ Un DVD ROM que contiene:

- El software ejecutable.
- Bases de datos de conocimientos estándar.
- El manual del Usuario del Software (E-book).
- Dos ejemplos de auditorías realizadas con AUDIRISK para la Empresa "Morraos de Colombia" (módulo de prueba y entrenamiento encajado en la estructura de AUDIRISK).

✓ Derecho a recibir soporte para operación, actualizaciones del software y de la metodología durante el primer año, sin costo adicional.
✓ Acceso a preguntas más frecuentes (FAQ: Frequently Asked Questions) en la página web de AUDISIS.

POR EL ARRENDAMIENTO ANUAL DEL SOFTWARE AUDIRISK.

- Claves de Acceso al Software.
- Bases de datos de conocimientos estándar.

- Manual del Usuario del Software (E-book).
- Dos ejemplos de auditorías realizadas con AUDIRISK para la Empresa "Morraos de Colombia" (módulo de prueba y entrenamiento encajado en la estructura de AUDIRISK).

✓ Derecho a recibir soporte para operación y actualización del software durante el período contratado por arrendamiento.

✓ Acceso a preguntas más frecuentes (FAQ: Frequently Asked Questions) en la página web de AUDISIS.

6. SERVICIOS DE SOPORTE TÉCNICO Y ACTUALIZACION.

AUDISIS, ofrece el servicio anual de soporte técnico, mantenimiento y actualización, el cual incluye soporte telefónico o vía internet al usuario para resolver inquietudes relacionadas con la operación y funcionamiento de la metodología **AUDIRISK**.

Los desarrolladores de **AUDIRISK** se encuentran en constante interacción con los usuarios, generando nuevas versiones que pueden ser suministradas a los usuarios vía Internet en su página www.audisis.com o suministradas en formato DVD ROM directamente.

El contrato anual de soporte técnico y actualización incluye:

✓ Soporte técnico ofrecido por funcionarios de AUDISIS especializados en **AUDIRISK**.

✓ Derecho a recibir actualizaciones sin costo adicional, con las nuevas versiones de la metodología cada vez que se produzcan.

✓ Acceso a preguntas más frecuentes (FAQ: Frequently Asked Questions) sobre la operación y uso del software AUDIRISK, en la página web de AUDISIS.

Por el primer año, contado desde la fecha de compra, el contrato de soporte técnico no tiene costo para el usuario de AUDIRISK.

7. REQUERIMIENTOS DE HARDWARE Y SOFTWARE PARA EL FUNCIONAMIENTO DEL SOFTWARE AUDIRISK.

- ✓ **HARDWARE**

Memoria RAM: 1 GB
Capacidad de Disco: 20 GB
Arquitectura: WEB

- ✓ **SOFTWARE**

Sistema Operativo: Windows Server versiones 2003 a 2012; Windows 2000, Vista y Windows 7, 8 y 10.
Internet Information Server (IIS) acorde a la versión de Windows que se encuentra en el servidor.

Motor de Base de Datos: SQL SERVER (versión 2005 o superior), no es necesario adquirir el motor de Base de Datos, debido que puede ser instalado con la versión ***SQL Server Express "de uso gratuito".***

Navegador Web: cualquiera de los existentes. Se recomienda Internet Explorer por sus capacidades visuales.

8. PERFIL DEL PROVEEDOR DE AUDIRISK.

AUDISIS LTDA, **Auditoría Integral y Seguridad de Sistemas de Información Ltda.**, es una firma de Auditores – Consultores Gerenciales, especializada en Gestión de Riesgos, Seguridad y Auditoría de Sistemas de Información, constituida legalmente el 23 de Septiembre de 1.988, Mediante escritura pública No. 5962 de la Notaría 4 del círculo de Bogotá, con registro vigente en la Cámara de Comercio de Bogotá bajo el número de matrícula 346900.

Su misión es *la prestación de servicios profesionales especializados y suministro de herramientas de productividad y soporte administrativo en los campos de Gestión de Riesgos Empresariales, Control interno de Tecnología de Información (TI), Seguridad informática, Auditorías Basadas en Riesgos Críticos a la Tecnología de Información, procesos de negocio, servicios automatizados, Auditorías Basadas en Datos y Auditorías a Sistemas de Gestión (calidad, ambiental, seguridad de la información), utilizando metodologías y herramientas de software de categoría mundial, personal permanentemente capacitado y altos estándares de calidad.*

9. EMPRESAS QUE UTILIZAN AUDIRISK.

EN COLOMBIA.

SECTOR FINANCIERO.

- **Crezcamos S. A. – Cooperativa de Ahorro y Crédito.** Bucaramanga.
- **Crediservir – Cooperativa de Ahorro y Crédito.** Ocaña.
- **Financiera Andina - FINANDINA S.A.** Revisoría Fiscal.
- **FINAGRO. Dirección de Control de Gestión.**
- **Corporación Financiera Colombiana.** Auditoría Interna.
- **Fiduciaria la Previsora S.A.** Oficina de Control Interno.
- **Banco Popular.** Contraloría
- **FMMB. Fundación Mundial de la Mujer. Bucaramanga.** Auditoría Interna

Entidades del Gobierno Colombiano.

- **Policía Nacional – Dirección de Control Interno.**
- **Comisión Nacional de TV – Oficina de Control Interno.**
- **ARMADA NACIONAL. Oficina de Control Nóminas.**
- **CONSEJO SUPERIOR DE LA JUDICATURA.** Unidad de Auditoría.
- **CONTRALORIA GENERAL DE LA REPUBLICA. Dirección De Control Interno.**
- **OCENSA. Oleoducto Central de Colombia. Dirección de Auditoría Interna.**
- **INSTITUTO NACIONAL DE VIAS – INVIAS.** Coordinación Área de Desarrollo Informático.
- **Ministerio de Hacienda y Crédito Público.** Oficina de Control Interno.

- **Secretaría de Hacienda de Bogotá.** Oficina de Control Interno
- **Superintendencia De Notariado Y Registro.** Oficina de Control Interno.
- **ESSA. Empresa Electrificadora de Santander S.A.** oficina de Control Interno.
- **Centrales Eléctricas De Nariño.** Oficina de Control Interno.

CAJAS DE COMPENSACION FAMILIAR.

- **Comfenalco Tolima** – Auditoría Interna.
- **Caja de Compensación Familiar de Arauca – COMFIAR.**
- **COMPENSAR. Caja de Compensación Familiar. Bogotá - Auditoría General.**
- **Caja de Compensación Comfamiliares Caldas.** Auditoría General.

SECTOR INDUSTRIAL.

- **PETROLEOS DEL NORTE - PETRONORTE - Auditoría Interna.**
- **Plastilene S.A – Auditoría Interna**
- **Lafayette S.A. – Auditoría Interna.**
- **OCENSA –** Oleoducto Central de Colombia – Auditoría Interna.
- **CARACOL T.V. Gerencia de Contraloría y Auditoría Interna.**
- **Monómeros Colombo Venezolanos. Auditoría Interna.**

SECTOR COMERCIO.

- **Grupo Casa Toro.** Revisoría Fiscal.

SECTOR SALUD.

- **Salud Vida – EPS – Auditoría Interna.**
- **Famisanar – EPS – Auditoría Interna.**

FIRMAS DE AUDITORES.

- **Colombian Consulting Group.** Firma de Auditoría Externa.
- **Nexia Montes y Asociados.** Firma de Auditoría Externa.
- **Paez y Asociados.** Bogotá. **Firma de Auditores Externos.**

SECTOR EDUCATIVO.

- **Universidad Militar Nueva Granada.** Bogotá. Facultad de Ciencias Económicas.
- **Universidad Pedagógica y Tecnológica de Colombia – UPTC .** Tunja y seccionales.
- **Universidad Francisco de Paula Santander – Ocaña.**
- **Universidad la Gran Colombia- Bogotá.** Facultad de Contaduría.
- **Universidad Católica De Colombia. Bogotá.** Facultad de Ingeniería de Sistemas...
- **Universidad Jorge Tadeo Lozano. Bogotá.** Auditoría de Sistemas
- **CorUniversitaria. Ibagué-** Facultad de Contaduría Pública.
- **Universidad Santo Tomás de Bucaramanga.** Carrera de Contaduría Pública.
- **Universidad Autónoma. Cali,** Dirección de Sistemas.
- **Corporación Universitaria Republicana. Bogotá.**

EN OTROS PAISES

En República Dominicana

- **Banco Central –** Auditoría Interna

En Costa Rica

- **Cervecería de Costa Rica.** Contraloría.

En Guatemala

- **Superintendencia de Bancos (Guatemala)**

En Bolivia

- **Banco Santacruz Bolivia- Auditoría**

En Honduras

- **Cooperativa de Ahorro y Crédito "Sagrada Familia".** Tegucigalpa.
- **Banco Centroamericano de Integración Económica (BCIE).** Tegucigalpa. Contraloría y Auditoría Interna.

En PERÚ

- **Universidad Unión Peruana. Lima Perú.**