Versión 7.5

SOFTWARE DE ADMINISTRACIÓN DE RIESGOS PARA PROCESOS Y TECNOLOGIA DE INFORMACION

PRESENTACION DEL PRODUCTO

CONTROLRISK ®

AUDITORÍA INTEGRAL Y SEGURIDAD DE SISTEMAS DE INFORMACIÓN "AUDISIS"
Servicios Especializados de Prevención y Reducción de Riesgos, Seguridad y Auditoría de Sistemas.
Calle 53 No. 27 - 33 Oficina 602 – Bogotá, D.C. Colombia PBX: (571) 3470022 Tels. (571)2556717, (571) 3099764
E-Mail audisis@audisis.com web site: www.audisis.com www.softwareaudis.com
AUDISIS: 33 años - Fundada en 1.988

Contenido

1. QUÉ PUEDE HACER CON LA POTENCIA DE CONTROLRISK.

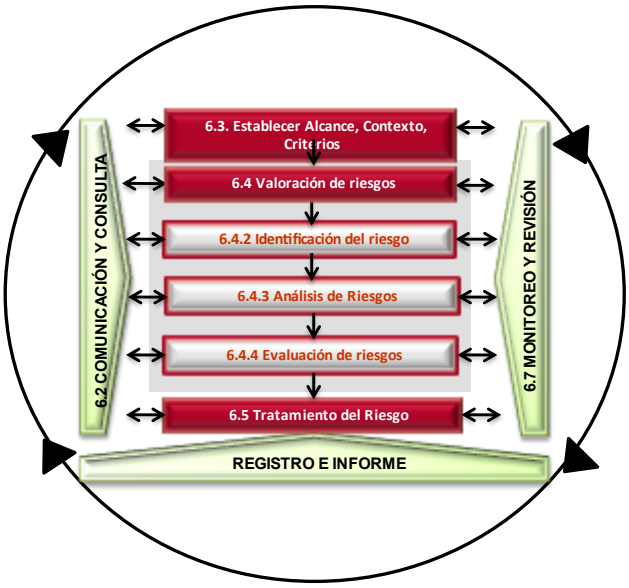
CONTROLRISK es un software en tecnología Web que provee funcionalidades ***para implantar y mejorar continuamente la Gestión de Riesgos Empresariales en los Procesos de la Cadena de Valor y la Tecnología de Informacion de las Empresas, con una visión a corto, mediano y largo plazos;*** las funcionalidades del software están alineadas con las buenas y mejores prácticas de Gestión de Riesgos y Control Interno recomendadas por ISO 31000: 2018, el marco de referencia ERM (Enterprise Risk Management), COSO 2013, COBIT, ISO 27001 y otras normas nacionales de Gestión de Riesgos expedidas por las Superintendencias y el Departamento Administrativo de la Función Pública (DAFP).

Figura 1: Menú Principal de CONTROLRISK

El software CONTROLRISK provee funcionalidades para desarrollar las siguientes actividades de la Gestión de Riesgos por procesos:

a) Implantar la Gestión de Riesgos Empresariales en los procesos de la cadena de valor (estratégico, misional y de soporte), los procesos de TIC (por ejemplo de COBIT) y las aplicaciones de computador o módulo de ERPs que soportan procesos CORE del negocio y la norma ISO 27001.

ISO 31000: 2018 - Elementos del Proceso de Gestión del Riesgo



ControlRisk: Software de Administración de Riesgos Empresariales

Este proceso de implantación de la Gestión de Riesgos en CONTRORISK comprende siete (7) etapas:

- **Etapa 1 - Definición del Contexto del Estudio de Gestión de Riesgos -EGR.** El software provee funcionalidades para documentar las características esenciales y el ambiente de operación del proceso o sistema objeto de la Gestión de Riesgos (denominado EGR: Estudio de Gestión de Riesgos), las cuales servirán como marco de referencia para ***identificar, analizar, controlar y monitorear*** los riesgos inherentes de cada proceso (de la cadena de valor ó de TI o dominio de ISO 27001) y sistema de información de negocios (aplicación de negocios o módulo de ERP).

- **Etapa 2- Identificación y Análisis de Riesgos Inherentes.** La identificación del inventario de eventos de riesgo inherente que pudieran presentarse se realiza por actividades del proceso o sistema y dentro de éstas por categorías o clases de riesgo. A través de una metodología de análisis de riesgo cuantitativo el software conduce el análisis y documentación de los seis (6) elementos por cada evento de riesgo entre los que se destacan la valoración de los activos impactados, la frecuencia anual de ocurrencia y la estimación de la pérdida anual estimada (PAE), los que se utilizan como base para estimar el nivel de severidad de los riesgos y construir los mapas o matrices de riesgo inherente del proceso completo y por cada una de las clases de riesgo, actividades del proceso y áreas organizacionales y terceros que intervienen en el proceso.

- **Etapa 3 – Documentar Cubo de Riegos Inherentes del Proceso.** La documentación del análisis de riesgo se complementa con la descripción de la forma como pueden ocurrir las clases o categorías de riesgo críticas del proceso, en tres matrices que despliegan el **Cubo de Riesgos del proceso:** a) categorías de riesgo Vs Actividades del proceso; b) categorías de riesgos Vs dependencias y c) actividades del proceso Vs dependencias. También asiste la **definición de objetivos de control** que deberán satisfacerse en cada una de las actividades (escenarios de riesgo) del proceso o sistema objeto del Estudio de Gestión de Riesgos (EGR).

- **Etapa 4 – Control y Tratamiento de Riesgos.** En esta etapa el software CONTROLRISK provee funcionalidades para construir y generar *cuestionarios o guías de controles*[1] con las buenas prácticas de Controles *que deberían utilizarse* para reducir el nivel de severidad para los riesgos inherentes del proceso o sistema a niveles aceptables de riesgo residual, los que se utilizan como ayuda para identificar los controles utilizados. También provee funcionalidades y criterios para *evaluar la efectividad individual (once criterios) y colectiva (dos alternativas) de los Controles utilizados por la administración por cada evento de riesgo*. Como resultado o entregable esta etapa, genera **Mapas de Riesgos Residuales** antes de tratamientos, identifica los tratamientos requeridos, asiste el diseño de los tratamientos, la elaboración de plan de implantación, asigna responsables de implantar los tratamientos y realizar seguimiento a su implantación. Para los cargos asignados emite correos electrónicos de notificación.

- **Etapa 5- Análisis Costo/ Beneficio y Especificaciones de los Controles.** En esta etapa, las funcionalidades del software CONTROLRISK asisten la documentación de los controles y tratamientos diseñados o seleccionados en la etapa 4 y a calcular la relación costo / beneficio de los controles por cada evento de riesgo inherente.

- **Etapa 6 - Asignación de Responsabilidades por la Ejecución y Supervisión de los Controles.** En esta etapa, el software asiste la asignación de *cargos responsables de ejecutar y supervisar los controles establecidos* para los eventos de riesgo inherentes del proceso o sistema, en cada una de las áreas organizacionales y terceros que intervienen en el manejo de las operaciones del proceso o sistema. Además genera *reportes y Guías de Autocontrol* con destino a los cargos asignados como responsables de ejecutar y supervisar los controles.

- **Etapa 7- Monitoreo (Aseguramiento) de Controles y del Riesgo Residual.** El software produce *Guías de Autoevaluación / autoaseguramiento de Controles (en inglés CSA: Control Self Assessment)* con las cuales, periódicamente, los jefes de las áreas que intervienen en el proceso monitorean el cumplimiento y efectividad de los controles establecidos. El software provee funcionalidades para asistir el ingreso y procesamiento de las respuestas y con los resultados del monitoreo recalcular la protección ofrecida por los controles, el riesgo residual y generar *indicadores* sobre protección existente y riesgo residual por eventos de riesgo inherentes en cada una de las dimensiones del cubo de riesgos del proceso: Áreas Organizacionales, Escenarios de Riesgo y Categorías de Riesgo. El software mantiene un registro histórico de los resultados de los últimos doce (12) monitoreos realizados al proceso. Con los resultados de cada monitoreo se generan Planes de Mejoramiento del sistema de gestión de riesgos del proceso o sistema.

b) **Consolidar el Perfil del Riesgo de los Procesos de la Organización.** Con base en las calificaciones del nivel de severidad de los eventos de riesgo inherente obtenidas en

[1] Estos cuestionarios tienen formato de ***Control Self Assessment – CSA-*** para ser diligenciado por los dueños o responsables del proceso.

la implantación de la gestión de riesgos en los procesos y sistemas de la empresa, *el software provee funcionalidades para calcular el promedio de riesgo inherente de los eventos de riesgo de todos los procesos, consolidar el Perfil de riesgo inherente de la Empresa de identificar los riesgos transversales en todos los procesos de la organización.* Con las calificaciones de protección existente (PE) y riesgo residual (RR) de los eventos de riesgo en los últimos monitoreos de cada proceso*, el software generan matrices y perfiles consolidados del estado de protección existente (PE) y Riesgo Residual (RR) de la Empresa, identifica los riesgos y controles que se utilizan en varios procesos.* Estos perfiles de riesgo se visualizan por tipos de procesos (estratégicos, misionales y de soporte) y por categorías de riesgos, por procesos y por áreas organizacionales de la Empresa.

c) **Soportar la Actualización y Mejoramiento Continuo de la Gestión de Riesgos en los procesos.** En cualquier tiempo, el software provee funcionalidades para adicionar, modificar o suprimir riesgos, controles, áreas organizacionales, cargos y terceros que intervienen en la gestión de riesgos de los procesos y sistemas de la Empresa.

d) **Crear y mantener actualizada** la Base de Datos de "Eventos de Riesgo Ocurridos" (RERO) de la Empresa. El software provee un módulo para poblar la base de datos de eventos materializados, **analizar** las causas de su ocurrencia, diseñar acciones correctivas, asignar responsables de implantarlas, asignar responsables de implantarlas, notificar por correo electrónico las asignaciones y **ejecutar seguimiento** a la implantación de las acciones correctivas de remediación.

e) **Monitorear periódicamente el Plan de Continuidad del Negocio.** Comprobar periódicamente la disponibilidad de las estrategias de continuidad previstas en el BCP, a través de las repuestas a **guías de autoaseguramiento** que se responden en las áreas responsables de la disponibilidad de las estrategias y planes de continuidad establecidos..

f) **Auditar el SARO.** Verificar el cumplimiento y validez de las políticas, normas y procedimientos de gestión de riesgos establecidos en la empresa, el funcionamiento del RERO y del BCP .

La información generada en la implantación de la Gestión de Riesgos de los procesos y servicios de sistemas de la empresa se guarda y administra en un repositorio denominado *Base de Datos de Conocimientos de Gestión de Riesgos y Controles de la Empresa*. Esta base de datos crece continuamente en la medida que se avanza en la implantación de la Gestión de Riesgos en la Empresa, hasta llegar a convertirse en un repositorio único de toda la información de riesgos y controles de la Empresa.

Esta **Base de conocimientos de Gestión de Riesgos se entrega poblada por el proveedor del software,** con numerosas *"mejores y buenas prácticas*" universalmente aceptadas sobre

clases de riesgos utilizadas por el SARO, SARLAFT, MECI y el SGSI (ISO 27001), eventos de riesgo inherente (amenazas) que pueden originar las clases de riesgo (por ejemplo, eventos de riesgo que podrían generar fraude interno, Sanciones Legales, etc), relaciones entre *clases de riesgos y riesgo inherentes* (por ejemplo, riesgos que podrían generar la clase de riesgo "Fraude Interno"), controles, *relaciones entre riesgos y controles* (por ejemplo, los controles aplicables al riesgo "Destrucción de la información por incendio accidental") y objetivos de control aplicables a procesos de TI (COBIT e ISO 27001) y aplicaciones de computador.

Los procedimientos de *identificación, análisis, control y monitoreo de riesgos* utilizados por CONTROLRISK, están alineadas con estándares internacionales y nacionales de Gestión de Riesgos, Control Interno Organizacional (COSO, COBIT y MECI) y utilizan buenas prácticas administrativas tales como los principios de "Pareto" y del "Poder del 3", el enfoque Proactivo y preventivo de los Controles en lugar del enfoque *reactivo* o "a posteriori" y la implantación de "*los 3 anillos de seguridad ó tres Barreras de Control*" *por cada evento de riesgo,* como requisito para asegurar la *efectividad* de los controles por cada riesgo inherente (amenaza).

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

El software se oferta por equipo servidor y cantidad de usuarios en dos (2) modalidades de licenciamiento: a) Licencias de Uso a perpetuidad y b) licencias por Suscripción Anual.

También se ofrece el servicio de Asesoría para la implantación del software en el proceso de Gestión de Riesgos de la Empresa.

2. TIPOS DE USUARIOS.

CONTROLRISK provee perfiles de acceso ara tres (3) tipos de usuarios: a) **Administradores de Riesgos** de la Empresa con derechos de acceso a todas las funcionalidades del software; y b) **Dueños de Procesos**, con derechos de acceso limitado a las funcionalidades del software, como responsables implantar los planes de tratamiento, de la auto-evaluación en el monitoreo de riesgos y controles y de implantar los planes de mejoramiento que resultan de cada monitoreo; y **c) Auditores**, con acceso a funcionalidades del módulo de auditoría y consulta a los demás módulos del software.

Perfil Administrador de Riesgos: Con acceso a todas las Funcionalidades del Software**.**

- ❑ Gerente de Riesgos.
- ❑ Analista de Riesgos.
- ❑ Administrador RERO.
- ❑ Administrador BCP.

Perfil Dueño de Procesos: con derechos de acceso limitados al monitoreo de riesgos y controles, Registro de Eventos de Riesgo Ocurridos (RERO), monitoreo del Plan de Continuidad de Negocios (BCP), implantación de Acciones de Tratamiento (AT), Acciones de Mejoramiento (AM) y Acciones Correctivas (AC).

- ❑ Administrador de EGRs (Estudios de Gestión de Riesgos).
- ❑ Auto-evaluador .
- ❑ Monitoreo de riesgos, CSA.
- ❑ Auxiliar de RERO: ingreso de eventos de riesgo ocurridos
- ❑ Auto-evaluador del BCP.
- ❑ Implantador Acciones Correctivas – RERO y BCP, Acciones de Tratamiento de Riesgos y Acciones de Mejoramiento por Monitoreos.
- ❑ Comité de Riesgos de la Empresa.

Perfil Auditor, con derechos de acceso a todas las funcionalidades del módulo de auditoría y acceso solo consulta a los demás módulos del software.

- ❑ Gerente de Auditoría.
- ❑ Auditor.
- ❑ Comité de Auditoría

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

3. PROPUESTA DE VALOR DEL SOFTWARE "CONTROLRISK" .

Las siguientes son características de CONTROLRISK que generan valor para las empresas usuarias del software:

1) El software **CONTROLRISK** satisface los lineamientos y estándares recomendados para Gestión de Riesgos Empresariales en los marcos de referencia internacionales *ISO 31000:2018, ERM (Enterprise Risk Management – Integrated Framework), ISO 27005 y otros nacionales establecidos por las Organismos de Control del Estado (Superintendencias) y el Departamento Administrativo de la Función Pública (DAFP)*.

2) *El software CONTROLRISK* ***es multiempresa,*** es decir, con una sola licencia puede administrar la gestión de riesgos operativos de múltiples empresas.

3) CONTROLRISK soporta la **evolución de la Gestión de Riesgos** a corto, mediano y largo plazos. Los productos generados por el software se conservan y administran en una *Base de Datos de Conocimientos de Gestión de Riesgos y Controles de la Empresa que se actualiza continuamente con adiciones, modificaciones y eliminaciones de registros***.** Esta Base de Datos "contiene *el inventario de riesgos inherentes que pudieran presentarse en los procesos y sistemas de la organización" y* crece continuamente en la medida que se avanza en la implantación de la Gestión de Riesgos.

4) CONTROLRISK provee funcionalidades que permiten la **interacción entre la Gerencia de Riesgos de la Empresa y los Dueños de Procesos**, para implantar y realizar seguimiento a planes de tratamiento de riesgos, planes de mejoramiento de la gestión de riesgos que resultan de cada monitoreo periódico y de las acciones correctivas por efecto del análisis de los riesgos ocurridos o materializados.

5) ***La Gestión de Riesgos es PROACTIVA Y PREVENTIVA****,* es decir, se anticipa a la ocurrencia de los riesgos mediante el establecimiento de controles para prevenirlos y reducirlos a nivel tolerable de riesgo residual. *El objetivo es "Administrar el inventario de riesgos inherentes de la Empresa, que pudieran presentarse en los diferentes procesos y sistemas, para* ***reducir*** *la posibilidad de ocurrencia y/o el impacto en caso de presentarse".*

6) *El software CONTROLRISK, genera* ***numerosos reportes resumidos y detallados*** *que constituyen el Manual de Gestión de Riesgos de cada proceso de la Empresa.* Estos reportes son exportables a diferentes formatos de archivo (PDF, Excel, etc) e incluyen gráficas, tablas y un lenguaje cromático para identificar los diferentes niveles de severidad de los eventos de riesgo inherente antes de controles (mapa de riesgos inherentes) y mapas de riesgo residual para los eventos de riesgo en tres momentos: a) después del diagnóstico sobre la efectividad de los controles existentes; b) después de implantar los tratamientos a los riesgos; y c) después de cada monitoreo periódico de los riesgos y controles.

7) El software CONTROLRISK **"genera"** cuestionarios para apoyar la implantación de la gestión de riesgos por cada proceso: a) para identificar los riesgos inherentes que podrían presentarse en los procesos; b) para identificar los controles aplicables *que deberían existir* por cada riesgo; y c) Guías de Autoevaluación o Auto-aseguramiento de controles (del inglés CSA: Control Self Assessment), para realizar el monitoreo periódico de la gestión de riesgos. Por ejemplo, el software genera cuestionarios de riesgos inherentes que pudieran presentarse por cada una de las siguientes categorías de riesgo del modelo SARO: Fraude Interno, Fraude Externo, Daños a Activos Físicos,

Problemas Laborales, Fallas en atención a los clientes, fallas tecnológicas y errores en el diseño y operación de los procesos*.*

8) Utiliza métodos de ***análisis cuantitativo*** *de los* riesgos inherentes por cada proceso o sistema. Por cada riesgo, el *software provee funcionalidades para documentar el análisis de al menos seis (6) elementos del 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) la frecuencia anual de ocurrencia (FAO); e) la pérdida simple por cada ocurrencia; f) la pérdida anual estimada (PAE); g) evaluación de la severidad o nivel de exposición (con base en estimaciones de la frecuencia anual de ocurrencia y del impacto financiero y operacional); h) fuentes del riesgo (actividades del proceso y áreas que intervienen en las operaciones del proceso), i) las consecuencias en caso de ocurrir, e j) el propietario del riesgo.

9) El software mide o califica la severidad o nivel de exposición de cada riesgo inherente 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 aprobado por la Gerencia (color verde). Los riesgos, después de evaluada su severidad, se ubican en el **Mapa de Riesgos Inherentes** (una matriz de 5 x 5), el cual se muestra en pantalla y en reportes y gráficos para las tres (3) dimensiones del **Cubo de Riesgos del proceso**: a) por clases o categorías de riesgo, b) por Dependencias (áreas de la estructura de organización o terceros) y c) por actividades del proceso.

10) **El software provee criterios para evaluar (medir) la efectividad individual y colectiva de los controles** por cada riesgo inherente. Ofrece diez (10) de criterios de evaluación individual de los controles y dos (2) alternativas para evaluar la efectividad colectiva de los controles por riesgo inherente.

11) ***CONTROLRISK*** *aplica tres (3) criterios para ASEGURAR un apropiado diseño de los controles por cada evento de riesgo inherente: a) Eliminan las vulnerabilidades que pudieran crear el ambiente* propicio para la ocurrencia de los eventos de riesgo; b) *bloquean o neutralizan los agentes generadores* que pudieran explotar las vulnerabilidades y c) reducen el impacto o consecuencias del riesgo en caso de materializarse.

12)

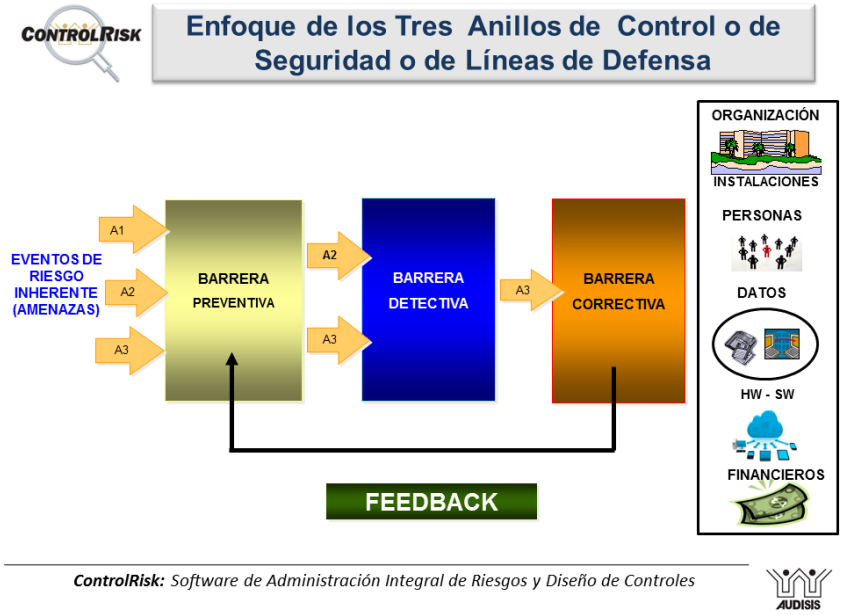


Figura 3: Enfoque de los 3 Anillos de Seguridad o Líneas de Defensa de los Controles.

13) Para *evaluar la efectividad (eficacia + eficiencia) colectiva de los controles* por cada riesgo inherente, CONTROLRISK ofrece dos alternativas. **La primera** aplica tres criterios como se ilustra en la figura 3: a) Los controles satisfacen al menos una vez los "*tres anillos de seguridad o barreras de defensa y hacen sinergia*"; b) La efectividad promedio de los controles individuales que actúan sobre el riesgo es superior a un valor numérico especificado por la Gerencia y c) La relación costo / beneficio de los controles es razonable. La **segunda alternativa** considera tres (3) criterios de evaluación por evento de riesgo: a) Se utiliza un número plural de controles para gestionar el riesgo y estos actúan antes que ocurra el riesgo; b) La efectividad promedio de los controles individuales que actúan sobre el riesgo es superior a un valor numérico especificado por la Gerencia y c) La relación costo / beneficio de los controles es razonable.

14) Para evaluar la eficiencia de los controles por riesgo, el software utiliza dos criterios: a) los controles reducen la pérdida anual estimada (PAE) al menos en un 70%; y b) el costo de los controles que no excede del 7% del valor de los activos protegidos.

15) *CONTROLRISK evalúa y mide cualitativamente la "efectividad Colectiva de los controles para reducir el riesgo".* La escala de calificaciones de efectividad de los controles es la siguiente: 5- Apropiada, 4-Mejorable, 3-Insufiicente, 2- Deficiente y 1-Muy deficiente.

16) *CONTROLRISK provee funcionalidades para identificar* las debilidades de control que presentan los riesgos inherentes que presenten efectividad de los controles MEJORABLE, INSUFICIENTE, DEFICIENTE Y MUY DEFICIENTE, para las cuales se requieren acciones de tratamiento. Los tratamientos son controles adicionales que se necesitan para asegurar que la severidad del riesgo inherente se reduzca a niveles aceptables de riesgo residual.

17) *CONTROLRISK provee funcionalidades para diseñar el plan de tratamiento de los riesgos, planear su implantación, comunicar por correo electrónico la asignación de cargos responsables de implantar los tratamientos y la fecha límite para su implantación, ejecutar seguimiento a la implantación y enviar correos electrónicos de recordatorio* a los responsables de implantar, supervisar y verificar la implantación. Para este fin, el software ofrece funcionalidades que permiten la interacción permanente a través de correos electrónicos entre Administradores de Riesgos y Dueños de Procesos.

18) El software produce *Mapas de Riesgos Residuales después de tratamientos,* para las tres dimensiones del cubo de riesgos del proceso o sistema objeto de gestión de riesgos*.* También genera reportes y gráficos para visualizar la comparación de la severidad de los riesgos inherentes antes de controles y después de tratamientos y numerosos reportes resumidos y detallados de los controles y tratamientos requeridos para reducir los riesgos inherentes a nivel aceptable de riesgo residual.

19) CONTROLRISK conduce la generación de **Guías de Autocontrol por cada una de las áreas que intervienen en las operaciones del proceso o sistema**. Estas asignan los *cargos responsables de ejecutar y supervisar los controles establecidos* por cada riesgo inherente. Para los controles manuales, se asignan cargos responsables de ejecutar y supervisar los controles; para los controles automatizados, que son ejecutados por la máquina o el software de las aplicaciones, únicamente se asignan responsables de supervisar el funcionamiento de los controles.

20) Para el monitoreo periódico de la Gestión de Riesgos de cada proceso o sistema, CONTROLRISK genera ***Guías de Autoevaluación o Auto-aseguramiento de Controles*** *(en inglés CSA: Control Self Assessment)* para ser respondidas en cada una de las Areas Organizacionales que intervienen en las operaciones del proceso o sistema. También provee funcionalidades para ingresar y procesar las respuestas y generar *indicadores de Gestión de Riesgos* sobre protección existente y riesgo residual por cada riesgo inherente y por cada una de las dimensiones del cubo de riesgos del proceso: Áreas Organizacionales, Escenarios de Riesgo y Categorías de Riesgo. El software mantiene un registro histórico de los resultados de los últimos doce monitoreos efectuados.

21) En el monitoreo de la Gestión de Riesgos de cada proceso, por cada riesgo inherente CONTROLRISK **mide** el cumplimiento de los controles con una escala de cinco

calificaciones, así: 5- Apropiada (cumplimiento superior al 80%); 4- Mejorable (cumplimiento entre el 60% y 80%), 3- Insuficiente (cumplimiento entre 40% y 60%): 2: Deficiente (cumplimiento entre 20% y 40%); y 1 - Muy deficiente (cumplimiento entre 0% y 20%). A cada uno de estos niveles de cumplimiento de los controles corresponde un nivel de riesgo residual, así: 1- Bajo (cumplimiento superior al 80%); 2- Moderado (cumplimiento entre el 60% y 80%), 3- Alto (cumplimiento entre 40% y 60%): 4: Extremo (cumplimiento entre 20% y 40%); y 5- Extremo (cumplimiento entre 0% y 20%).

22) En cada monitoreo de la Gestión de Riesgos por proceso, para los riesgos que presentan resultados no satisfactorios (cumplimiento menor del 80%), CONTROLRISK provee funcionalidades para ***coordinar y realizar seguimiento a la implantación de planes de mejoramiento:*** *definir acciones de mejoramiento a implantar, comunicar por correo electrónico la asignación de cargos responsables de implantar las acciones de mejoramiento y fecha límite para su implantación, ejecutar seguimiento a la implantación y enviar correos electrónicos de recordatorio* a los responsables de implantar, supervisar y verificar la implantación de las acciones de mejora. Para este fin, el software permite interacción continua a través de correos electrónicos entre los Administradores de Riesgos y Dueños de Procesos.

23) *CONTROLRISK consolida el Perfil de Riesgo Operativo de la Empresa*. El software **provee funcionalidades para consolidar a nivel Empresa**, los perfiles de riesgo Inherente y Residual de todos los procesos de la organización (estratégicos, misionales, de apoyo y de evaluación y mejora) para los cuales se haya implementado el SARO. La consolidación se realiza por los siguientes conceptos: a) por tipos de procesos (misionales, estratégicos y de soporte), b) por áreas organizacionales y c) por categorías de riesgo.

24) ***Registro de Eventos de Riesgo Ocurridos (RERO).*** *CONTROLRISK crea, mantiene actualizada y explota una Base de Datos con el Registro de Eventos de Riesgo Ocurridos o Materializados en cada empresa*. Esta base de datos es un registro histórico de los eventos de riesgo ocurridos, los cuales una vez reportados se analizan y confrontan con los eventos de riesgo inherentes registrados en la *base de conocimientos de Gestión de Riesgos y Controles de la Empresa*, con el fin de evaluar la validez, robustez y valor preventivo de la información existente en esa base *de Conocimientos y de la metodología y los procedimientos definidos en el marco de referencia (framework) de la gestión de riesgos en la empresa.*

25) ***Monitorea el Plan de Continuidad del Negocio (BCP)****.* El software ofrece un módulo para verificar la disponibilidad de recursos requeridos por el Plan de Continuidad del Negocio (BCP), las estrategias de continuidad implementadas en la organización y el estado de preparación para ejecutar los procedimientos de administración de crisis, el plan de respuesta a emergencias y el plan de retorno a la normalidad.

26) *CONTROLRISK* ***provee funcionalidades para Auditar el SARO.*** Estas funcionalidades permiten a auditores internos y externos *evaluar y verificar* el cumplimiento de los procedimientos de gestión de riesgos de los siguientes componentes del SARO: a) El cumplimiento del Framework o marco de referencia de la gestión de riesgos y la calidad de la información de la base de conocimientos de gestión de riesgos y controles de la empresa; b) El Registro de Eventos de Riesgo Ocurrido (RERO) – Auditoria a la exactitud y calidad de la información de los eventos ocurridos, al seguimiento de los planes de acciones correctivas y al cumplimiento de los procedimientos de reporte, registro y análisis de eventos ocurridos; y c) Verificar el estado de preparación de las áreas que intervienen en cada proceso, para aplicar los procedimientos y estrategias de contingencia previstos en Plan de Continuidad del Negocio (BCP).

27) ***Gestión de Conocimientos***. La base de conocimientos de CONTROLRISK crea una excelente oportunidad para gestionar los conocimientos adquiridos en el desarrollo del proceso de Gestión de riesgos Empresariales; ahora la Gerencia Corporativa de Riesgos y los dueños de procesos pueden registrar en una base de datos los conocimientos de la organización adquiridos o generados sobre los riesgos que pudieran presentarse y los controles necesarios para gestionarlos, mantenerlos actualizados, socializarlos a través de la red de datos de la empresa y convertirse en la línea base para garantizar la continuidad del proceso de gestión de riesgos de la Empresa a través del tiempo. La gestión del conocimiento es una nueva cultura empresarial, una manera de gestionar las organizaciones que sitúa los recursos humanos como el principal activo y sustenta su poder de competitividad en la capacidad de compartir la información y las experiencias y los conocimientos individuales y colectivos.

28) El software CONTROLRISK fomenta y estimula la creación de una nueva cultura en la organización, en los gestores de riesgos y dueños de proceso, para migrar del estado de *"consumidores de conocimientos" al estado de "generadores de conocimiento y de valor para las organizaciones".*

4. MODULOS COMPONENTES DEL SOFTWARE CONTROLRISK

El software CONTROLRISK consta de siete (7) módulos interrelacionados (ver figura 4):

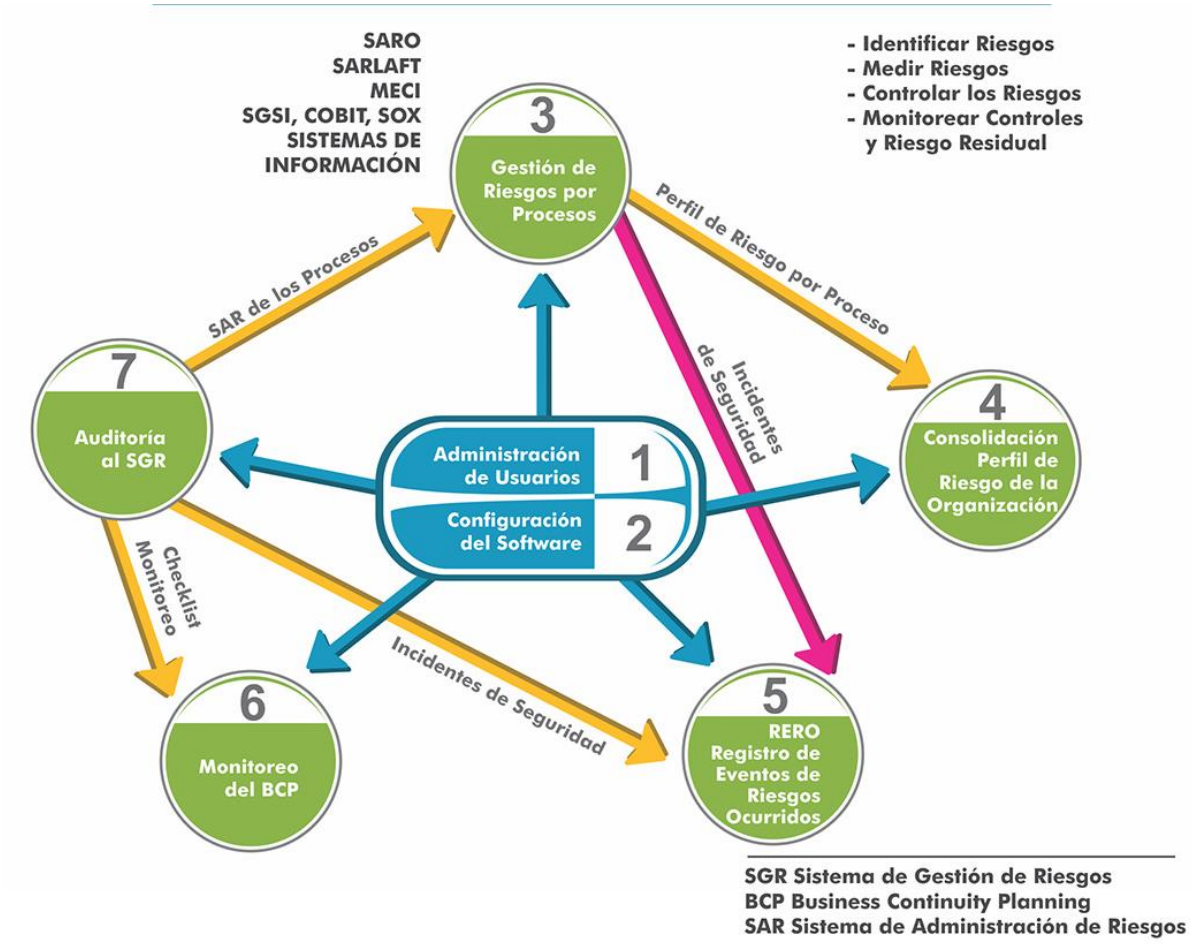


Figura 4: Módulos componentes de CONTROLRISK

MÓDULO 1: ADMINISTRACIÓN DE USUARIOS.

Este módulo de CONTROLRISK ofrece funcionalidades para administrar las cuentas de los usuarios de la aplicación (crear, activar, inactivar usuarios y cambiar los passwords) y asignar los permisos de acceso a los diferentes módulos del software (ver figura 3).

Figura 5: Módulo Administración de Usuarios

Los perfiles de acceso se establecen para tres (3) tipos de usuarios: a) **Administradores de Riesgos** de la Empresa con derechos de acceso a todas las funcionalidades del software; y b) **Dueños de Procesos**, con derechos de acceso limitado a las funcionalidades del software, como responsables implantar los planes de tratamiento, de la auto-evaluación en el monitoreo de riesgos y controles y de implantar los planes de mejoramiento que resultan de cada monitoreo; y **c) Auditores**, con acceso a funcionalidades del módulo de auditoría y consulta a los demás módulos del software.

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

MODULO 2: CONFIGURACION DEL SOFTWARE.

CONTROLRISK provee funcionalidades para configurar los estándares del marco de referencia que serán utilizados para *implantar la gestión de riesgos empresariales y monitorear el cumplimiento de los controles y el riesgo residual (ver figura 4)*. Por ejemplo:

- Criterios para evaluar cualitativamente *el impacto financiero y operacional* de los eventos de riesgos inherentes. Provee una escala de valores numéricos y rangos de valor monetario para evaluar el impacto de los eventos de riesgo.
- Criterios para estimar cualitativamente la *frecuencia anual de ocurrencia* de los eventos de riesgo inherentes y su *probabilidad de ocurrencia*. Provee una escala de valores numéricos para la frecuencia y probabilidad de ocurrencia de los eventos de riesgo.
- Escala de valores y criterios para evaluar cualitativamente *la Severidad o nivel de exposición* de los eventos de riesgo inherentes.
- Criterios para evaluar la efectividad de los controles sobre los eventos de riesgo inherentes y valorar el riesgo residual después de controles y tratamientos.
- Escala de Puntajes para valorar las respuestas de las *Guías de Monitoreo de Riesgos y Auto-aseguramiento* de Controles (en Ingles CSA: Control Self Assessment) en los procesos y sistemas de la Empresa.
- Criterios para evaluar el *cumplimiento de los controles y el riesgo residual*, según los resultados del Monitoreo de Riesgos y de Controles.

Figura 6: Elementos de Configuración del Sistema

El software provee funcionalidades para poblar con información de la Empresa, algunas tablas de la **Base de Datos de Conocimientos de Gestión de Riesgos y Controles,** suministrada por CONTROLRISK. Por ejemplo:

- Categorías o clases de Riesgo del *Universo de riesgos de la Empresa*.
- Agentes Generadores de Riesgo / Factores de Riesgo.
- Activos de la empresa que pueden ser impactados por los eventos de riesgo inherentes.
- Macroprocesos.
- Procesos del Modelo de Operación.
- Sistemas de Información – Aplicaciones de Computador.
- Areas Organizacionales - Estructura de organización de la empresa.
- Estructura de Cargos de la Empresa.
- Nombres de los Funcionarios de la Empresa.
- PUC.
- Líneas de Negocio.

El software también ofrece funcionalidades para *configurar el correo electrónico corporativo de la Unidad de Gestión de Riesgos y el envío automático de mensajes de recordatorio o alertas tempranas* dirigidos a los funcionarios responsables de implantar, supervisar la implantación y hacer seguimiento a las *acciones de tratamiento* de los riesgos y las *acciones de mejoramiento* que resultan de los monitoreos periódicos de los controles y los riesgos residuales por cada proceso o sistema.

MÓDULO 3: GESTIÓN DE RIESGOS POR PROCESOS.

El Ciclo PHVA de la Gestión de Riesgos por cada Proceso o Sistema.

En "CONTROLRISK", la "*Implantación del Sistema de Gestión de Riesgos"* tienen como objetivo conducir el desarrollo del ciclo PHVA (Planear, Hacer, Verificar, Actuar) de la **Gestión de Riesgos por cada proceso o sistema de información de la Empresa** (ver figura 7).

Figura 7: Ciclo PHVA del proceso Gestión de Riesgos

Este módulo de CONTROLRISK ofrece funcionalidades para desarrollar el ciclo PHVA de la gestión de riesgos por cada proceso o sistema. Para desarrollar la gestión de riesgos de cada proceso o sistema de negocios se crea un ***Estudio de Gestión de Riesgos (EGR)***; *por* consiguiente un EGR en CONTROLRISK, puede ser:

1) Un proceso del modelo de operación de la empresa (estratégico, misional, de soporte y de supervisión y control);

2) Un Proceso de Gestión de Tecnología de Información y comunicaciones (de los modelos COBIT, ITIL);

3) Los dominios de Seguridad de la Informacion considerados por ISO 27001 (Sistema de Gestión de Seguridad de la Informacion; y

4) Los Sistemas de información automatizados (aplicaciones de computador ó Módulos de ERPs).

Etapas de la Metodología para Implantar la GESTION DE RIESGOS en los procesos y Sistemas de la Empresa.

Por cada proceso o sistema, el software CONTROLRISK provee funcionalidades para conducir la implantación de la Gestión de Riesgos, a través de ocho (8) etapas que se muestran en la figura 8 y se describen a continuación:

Figura 8: Etapas de Implantación de la Gestión de Riesgos por proceso o sistema

Las ocho etapas del Ciclo PHVA implementadas en el software corresponden a las dos fases de "*la Gestión de Riesgos por proceso*":

- **Fase 1, Estática o Estructural, compuesta por las etapas 1 a 5:** Elaborar Contexto de Riesgos del Proceso; Identificación y análisis de Riesgos; Elaborar Cubo de Riesgos del proceso; Análisis Costo / beneficio y Especificaciones de los Controles; y Evaluación y Tratamiento de Riesgos.

- **Fase 2, Dinámica u Operativa, compuesta por etapas 6, 7 y 8:** Asignación de responsabilidades por los controles; Monitoreo y Auto-aseguramiento de los Controles; y Generación del Manual de Gestión de Riesgos del proceso.

PLANEAR (P) la Gestión de Riesgos del Proceso.

Etapa 1 - Definición del Contexto del Estudio de Gestión de Riesgos -EGR.

El software provee funcionalidades para documentar las características y el ambiente de operación del proceso o sistema objeto del EGR, las cuales servirán como marco de referencia de conocimientos para desarrollar el ciclo PHVA de la gestión de riesgos.

Etapa 2- Identificación y Análisis de Riesgos Inherentes.

Apoyándose en la base de datos de conocimientos suministrada por CONTROLRISK, el software conduce a identificar, analizar y estimar la severidad de los eventos de riesgo inherentes (amenazas) que podrían presentarse y obstaculizar la consecución de los objetivos de la empresa y causar daño a los activos del proceso o sistema objeto del EGR.

Por cada categoría de riesgo ***crítica*** aplicable al proceso o sistema, el software genera un cuestionario con los *eventos de riesgo inherentes negativos* que podrían ocurrir y causar daño a uno o más activos del proceso. De estas el dueño del proceso selecciona las que sean aplicables y adiciona las que pudieran faltar. Estos eventos de riesgo inherente también se denominan **amenazas.**

Para analizar los eventos de riesgo inherente identificados, el software conduce a documentar al menos 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) frecuencia anual de ocurrencia; e) pérdidas estimadas por cada ocurrencia; f) severidad o nivel de exposición (con base en estimaciones de la frecuencia anual de ocurrencia y del impacto financiero y operacional por cada ocurrencia); g) fuentes del riesgo (actividades del proceso y áreas que intervienen en las operaciones del proceso); h) las consecuencias en caso de ocurrir; i) el propietario del riesgo; y j) el indicador de ocurrencia del evento.

Como entregables de esta etapa, el software produce el *mapa de riesgos inherentes del proceso* (una matriz de 5 x 5 en la que se localizan las amenazas según su evaluación de probabilidad de ocurrencia e impacto), el perfil de riesgos del proceso (por categorías de riesgo, por área organizacional, por actividad del proceso y el mapa general) y la definición de las alternativas de manejo o tratamiento de riesgos (acciones de respuesta a riesgos) a emplear para mitigar los riesgos inherentes.

Etapa 3 – Documentar Cubo de Riegos Inherentes del Proceso.

En esta etapa, el software CONTROLRISK conduce la documentación detallada del mapa de riesgos inherentes, describiendo la forma como podrían ocurrir las categorías de riesgo críticas del proceso, en tres matrices que despliegan el **Cubo de Riesgos del proceso:** a) categorías de riesgo Vs Actividades del proceso; b) categorías de riesgos Vs dependencias y c) actividades del proceso Vs dependencias. También asiste la **definición de los objetivos de control** que se deberán satisfacer en cada una de las actividades (escenarios de riesgo) del proceso o sistema objeto del Estudio de Gestión de Riesgos (EGR) y los relaciona con los riesgos inherentes.

Para el proceso o sistema objeto de EGR se construye un CUBO DE RIESGOS como base para proyectar la gestión de riesgos del proceso (ver figura 9). Las tres dimensiones del **cubo de riesgos del proceso** son:

a) **Las categorías de Riesgos críticas en el proceso**. Esta dimensión está representada por las *clases o categorías de riesgos que sean aplicables y críticas para el proceso*, es decir, las que podrían ocurrir y ocasionar un impacto significativo económico y operacional en el proceso. Estas se seleccionan del *universo de clases de riesgo* aplicables a la empresa o de las clases de riesgo utilizadas en el SARO o del modelo de control interno MECI (para el sector público colombiano);

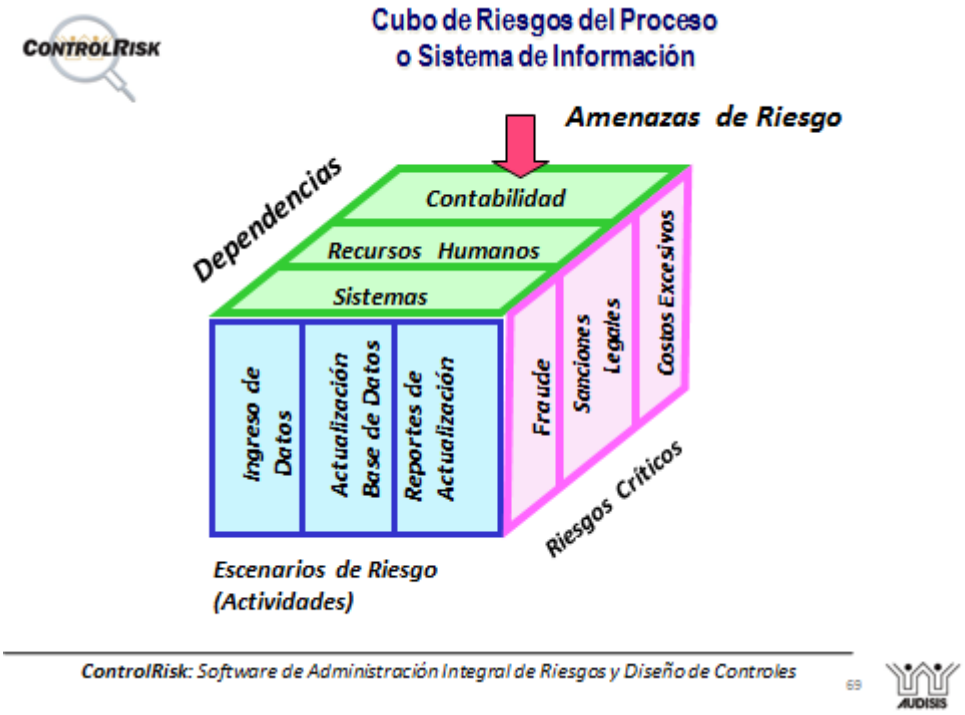


Figura 9: Cubo de Riesgos del Proceso o Sistema de Información

b) **Las actividades que constituyen el ciclo PHVA del proceso, también llamadas "Escenarios de Riesgo".** Está representada por las actividades o nombres de procedimientos que se constituyen el ciclo PHVA del proceso. Un proceso se define como "el conjunto de actividades interrelacionadas que transforman los insumos en un producto que puede ser un bien o un servicio".

c) **Las Dependencias (áreas de la estructura de organización y terceros) que intervienen en el manejo de las operaciones del proceso**. Los procesos son transversales en la estructura de organización de las empresas, lo cual significa que en

un proceso normalmente intervienen varias áreas de la estructura de organización de la empresa o terceros (outsourcing) que desarrollan algunas actividades del proceso. En los procesos que se soportan en sistemas de información automatizados, el área de sistemas siempre será una de las dependencias a considerar en la construcción del cubo del proceso, y

HACER (H) o Implementar la Gestión de Riesgos del Proceso.

Etapa 4 – Control y Tratamiento de Riesgos.

En esta etapa el software CONTROLRISK genera *cuestionarios o guías de controles*[2] con las buenas prácticas de Controles *que deberían existir* para reducir el nivel de severidad de los riesgos inherentes, como ayuda para identificar los controles utilizados en las operaciones del proceso o sistema. También provee funcionalidades para *evaluar la efectividad de los Controles por cada evento de riesgo,* es decir, la capacidad para reducir la severidad del riesgo a un nivel de riesgo residual aceptable. Como resultados o entregables de esta etapa, el software genera **Mapas de Riesgos Residuales** antes de tratamientos.

Como resultado de evaluar la efectividad de los controles, el software genera reportes y gráficos con *mapas de riesgo residual antes de tratamientos*, para las tres dimensiones del **cubo de riesgos del proceso o sistema objeto del EGR**: a) las clases de riesgo críticas; b) las actividades del proceso y c) las dependencias (áreas de la organización y terceros) que intervienen en el proceso.

Para los eventos de riesgo inherentes que presentan debilidades de control (riesgo residual con severidad diferente de Bajo o Tolerable), CONTROLRISK conduce el **diseño de las acciones de Tratamiento,** es decir, de los controles adicionales necesarios para reducir la severidad el riesgo inherente a un nivel aceptable de riesgo residual.

El software CONTROLRISK conduce la elaboración del plan de implantación de tratamientos y la ejecución de múltiples seguimientos a este plan, por cada evento de riesgo que lo requiera, según los resultados de la evaluación de efectividad de los controles. Se asignan cargos responsables de implantar, supervisar la implantación, ejecutar seguimiento y una *fecha límite* para implantar los tratamientos; por correo electrónico se comunican esta asignación y las credenciales para ingresar al sistema e informar los avances de implantación. Por cada seguimiento y hasta que sean implantadas todas las acciones de tratamiento, el software provee funcionalidades para ***configurar y enviar correos electrónicos de recordatorio*** de fechas límite próximas a vencerse y vencidas,

[2] Estos cuestionarios tienen formato de ***Control Self Assessment – CSA-*** para ser diligenciado por los dueños o responsables del proceso.

con destino a los cargos funcionarios asignados como responsables de implantar, supervisar la implantación y efectuar seguimiento a las acciones de tratamiento.

Para finalizar esta etapa, el software CONTROLRISK produce *Mapas de riesgos residuales después de tratamientos* para las tres dimensiones del cubo de riesgos del proceso o sistema objeto de gestión de riesgos. También genera reportes y gráficos para visualizar la comparación de la severidad de los riesgos inherentes antes de controles y después de tratamientos y numerosos reportes resumidos y detallados de los controles y tratamientos requeridos para reducir los riesgos inherentes a nivel aceptable de riesgo residual.

Etapa 5- Análisis Costo/ Beneficio y Especificaciones de los Controles.

En esta etapa, las funcionalidades del software CONTROLRISK conducen la documentación de los controles y tratamientos diseñados o seleccionados en la etapa 4 y a calcular la relación costo / beneficio de los controles por cada evento de riesgo inherente.

Etapa 6 - Asignación de Responsabilidades por la Ejecución y Supervisión de los Controles.

En esta etapa, el software asiste la asignación de *cargos responsables de ejecutar y supervisar los controles establecidos* para los eventos de riesgo inherentes del proceso o sistema, en cada una de las áreas organizacionales y terceros que intervienen en el manejo de las operaciones del proceso o sistema. Para los controles manuales, se asignan responsables de ejecutar y supervisar los controles; para los controles automatizados, que son ejecutados por la máquina o el software de las aplicaciones, se asignan responsables únicamente para supervisar el funcionamiento de los controles. Además genera *reportes y Guías de Autocontrol* con destino a los cargos asignados como responsables de ejecutar y supervisar los controles.

VERIFICAR (V) para monitorear la Gestión de Riesgos y ACTUAR (A) para efectuar mejoras a la Gestión de Riesgos.

Etapa 7- Monitoreo (Aseguramiento) de Controles y del Riesgo Residual.

El software produce *Guías de Autoevaluación de Controles (en inglés CSA: Control Self Assessment)* con las cuales se monitorea (auto-aseguramiento) el cumplimiento de los controles establecidos y verifica el nivel de riesgo residual aceptable por cada uno de los eventos de riesgo inherente. Estas guías se responden en cada una de las dependencias que intervienen en el proceso. El software también conduce el ingreso y procesamiento de las respuestas y genera *indicadores de Gestión de Riesgos* sobre protección existente y

riesgo residual por eventos de riesgo inherentes y por cada una de las dimensiones del cubo de riesgos del proceso: Áreas Organizacionales, Escenarios de Riesgo y Categorías de Riesgo. El software mantiene un registro histórico de los resultados de los últimos doce (12) monitoreo realizados al proceso.

El cumplimiento de los controles y el riesgo residual por cada evento de riesgo inherente se mide con una escala de cinco calificaciones, así: 5- Apropiada (cumplimiento superior al 80%); 4- Mejorable (cumplimiento entre el 60% y 80%), 3- Insuficiente (cumplimiento entre 40% y 60%): 2: Deficiente (cumplimiento entre 20% y 40%); y 1- Muy deficiente (cumplimiento entre 0% y 20%). A cada uno de estos niveles de cumplimiento de los controles corresponde un nivel de riesgo residual, así: 1- Bajo (cumplimiento superior al 80%); 2- Moderado (cumplimiento entre el 60% y 80%), 3- Alto (cumplimiento entre 40% y 60%): 4: Extremo (cumplimiento entre 20% y 40%); y 5- Extremo (cumplimiento entre 0% y 20%)

Para los eventos de riesgos que presenten porcentaje de cumplimiento de controles menor del 80%, el software asiste el **diseño de las *Acciones de Mejoramiento*** necesarias para corregir las falencias identificadas en el monitoreo y mejorar la gestión de riesgos del proceso.

El software CONTROLRISK también provee funcionalidades para diseñar, planear y ejecutar múltiples seguimientos del **Plan de Mejoramiento de la Gestión de Riesgos del EGR** por cada evento de riesgo inherente que lo requiera, según los resultados del monitoreo. Se asignan cargos responsables de implantar, supervisar la implantación, ejecutar seguimiento y una *fecha límite* para implantar los mejoramientos o ajustes requeridos; por correo electrónico se comunican esta asignación y las credenciales para ingresar al sistema e informar los avances de implantación. Por cada seguimiento y hasta que sean implantadas todas las acciones de mejora, el software provee funcionalidades para ***configurar y enviar correos electrónicos de recordatorio*** de fechas límite próximas a vencerse y vencidas, con destino a los cargos funcionarios asignados como responsables de implantar, supervisar la implantación y efectuar seguimiento a las acciones de tratamiento.

Para finalizar esta etapa, el software CONTROLRISK produce *Mapas de riesgos residuales REALES después de cada monitoreo,* para las tres dimensiones del cubo de riesgos del proceso o sistema objeto de gestión de riesgos. También genera reportes y gráficos para visualizar la comparación de la severidad de los riesgos inherentes *después de tratamientos y después del monitoreo* y numerosos reportes resumidos y detallados de las Acciones de Mejora requeridas para reducir los riesgos inherentes a nivel aceptable de riesgo residual.

Etapa 8 - Generar Manual de Gestión de Riesgos.

Esta etapa el software permite generar y visualizar la documentación detallada del sistema de gestión de riesgos de cada proceso o sistema de información objeto del EGR. Se producen reportes de todos los productos generados en cada una de las siete (7) etapas de implantación de la gestión de riesgos.

MÓDULO 4: CONSOLIDACIÓN DEL PERFIL DE RIESGOS DE LA ORGANIZACIÓN.

En este módulo **el software CONTROLRISK** provee funcionalidades para CONSOLIDAR a nivel Empresa los **perfiles de riesgo Inherente y Residual** de todos los procesos de la organización (estratégicos, misionales, de apoyo y de Evaluación y Mejora) para los cuales se haya desarrollado el ciclo PHVA de la gestión de riesgos en el módulo 4 de CONTROLRISK, en la forma como se ilustra en la Figura 10.

El software presenta el perfil de riesgos por tres conceptos: a) Por Categorías de Riesgo del universo de riesgos de la empresa y dentro de estas por procesos; b) por Areas Organizacionales y dentro de estas por categorías de riesgo y c) Para todos los procesos de la organización, por tipos de Procesos (Estratégicos, Misionales y de Soporte). Por cada concepto el software presenta la cantidad de amenazas y el valor promedio del Riesgo Inherente (RI) en cada proceso. Estos valores se obtienen con el promedio de riesgo inherente de las amenazas identificadas en cada proceso, en la etapa 2 del módulo 1.

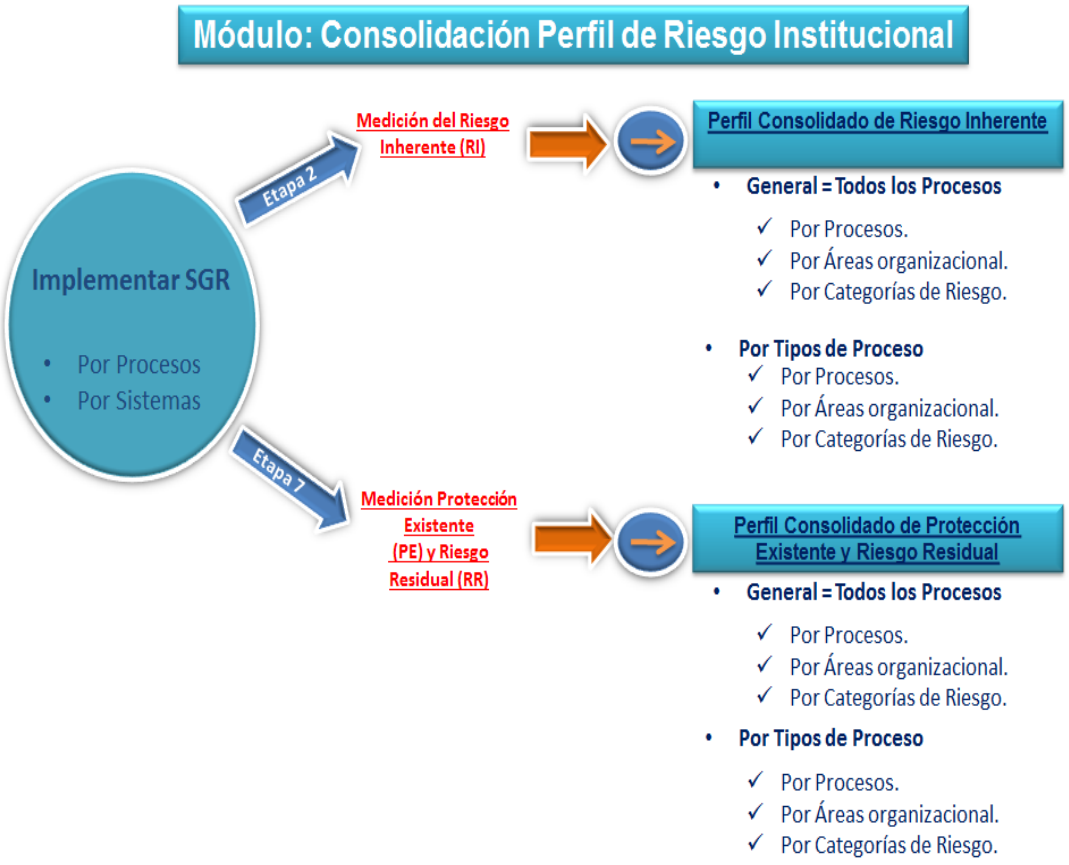


Figura 10: Funcionalidades del Módulo de Consolidación del Perfil de Riesgo

a) El Perfil de Riesgo Inherente Consolidado de la Organización (ver figura 11).

Nombre Empresa: Morraos de Colombia
Consolidado Perfil de Riesgo Inherente por Tipo de Proceso

Consolidado de Riesgo Inherente - Categorías de Riesgo

Tipo de Proceso: De Soporte

Id	Categoría de Riesgo	Total Amenazas	Riesgo Inherente (RI)	Significado RI	Acción
17	Daño y destrucción de activos	2	3	Alto	Ver
18	Hurto / fraude	2	3	Alto	Ver
19	Sanciones Legales	4	3	Alto	Ver
20	Pérdida de Credibilidad, reputación e imagen corporativa	3	4	Extremo	Ver
21	Decisiones Erróneas	4	4	Extremo	Ver
23	Costos Excesivos	2	3	Alto	Ver

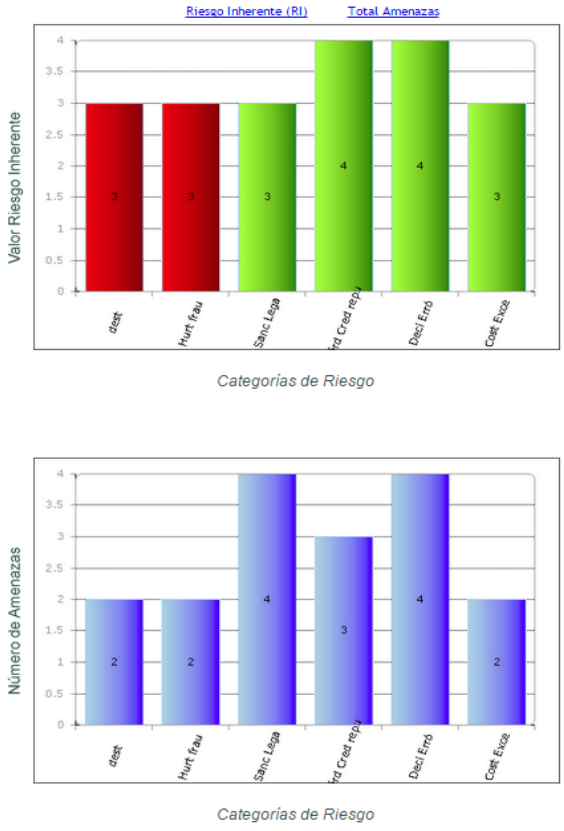


Figura 11: Consolidado del Perfil de Riesgo Inherente – Categorías de Riesgo

b) El Perfil de Protección Existente y Riesgo Residual Consolidado de la Organización (ver figura 12).

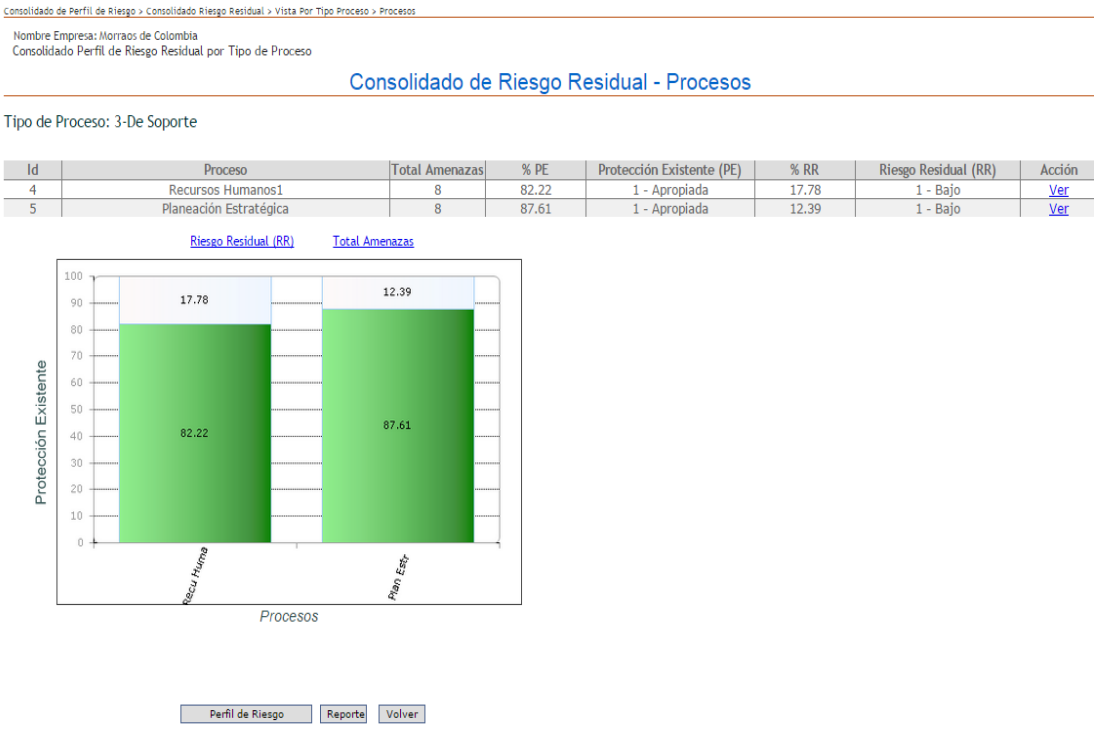


Figura 12: Consolidado del Perfil de Riesgo Residual – Procesos

Para este perfil, el software calcula indicadores (porcentajes) de los niveles de protección que ofrecen los controles establecidos sobre los eventos de riesgo inherentes y del riesgo residual según los resultados del último monitoreo, en todos los procesos a los cuales se ha implantado la gestión de riesgos. Con la información del *último monitoreo efectuado a* cada proceso, el software calcula y presenta el *porcentaje promedio* de *Protección Existente – PE (% de cumplimiento de los controles establecidos) y del Riesgo Residual – RR (el complemento a 100% de la PE)*, calculado con el porcentaje de cumplimiento de los controles por cada evento de riesgo inherente. Esta información se puede visualizar organizada por tres conceptos: a) Para todos los procesos que tienen implementada la gestión de riesgos; b) Por categorías de Riesgo y dentro de estas por procesos y c) Por áreas organizacionales y dentro de estas por categorías de riesgo.

El software genera reportes detallados y de Alto Nivel para los Ejecutivos de la Empresa.

MÓDULO 5: ADMINISTRACION Y ANALISIS DEL REGISTRO DE EVENTOS DE RIESGO OCURRIDOS (RERO).

Figura 13: Ingreso de Registro de Eventos de Pérdida Ocurridos

CONTROLRISK provee funcionalidades para conducir el ingreso (ver figura 13), cargue y análisis de información de los eventos de riesgo ocurridos en cualquier sitio de la empresa, en la **base de datos de Eventos de Riesgo Ocurridos en la organización.** Esta base de datos es un registro histórico de los eventos de riesgo ocurridos, los cuales después de su ingreso a la base de datos, se analizan y confrontan con los eventos de riesgo inherentes registrados en la *base de conocimientos de Gestión de Riesgos y Controles de la Empresa*, con el fin de evaluar la validez, robustez y valor preventivo de la información existente en esa base *de Conocimientos y de la efectividad de la metodología y los procedimientos utilizados para la gestión de riesgos en la Empresa (los que están definidos en el marco de referencia – framework de la gestión de riesgos en la empresa).*

La base de datos de RERO está estructurada de acuerdo con los requerimientos del modelo Basilea II y de los organismos de supervisión del Estado (por ejemplo, la Superintendencia Financiera de Colombia).

El software CONTROLRISK produce reportes impresos y en pantalla, con información detallada y resumida para consulta, análisis a alto nivel y soporte de las decisiones de los

Ejecutivos de la Empresa, respecto a la efectividad de los *procedimientos y estándares definidos en el marco de referencia (framework) de la gestión de riesgos en la empresa.*

Para el análisis de los eventos de riesgo ocurridos (ver figura 12), **CONTROLRISK** provee funcionalidades que ayudan, al analista de eventos ocurridos, a contrastar las características de ocurrencia del evento con la información disponible en la *Base de conocimientos de la Gestión de Riesgos y Controles de la Empresa* poblada durante la implementación de la gestión de riesgos. En esta base de conocimientos está disponible la información del *inventario de eventos de riesgo negativos que podrían presentarse (amenazas) en la empresa*, junto con las vulnerabilidades que podrían generar el ambiente propicio para la ocurrencia del evento, los agentes generadores del riesgo que podrían explotar esas vulnerabilidades, la acción de respuesta a riesgos implementada y los controles establecidos para gestionar el evento de riesgo.

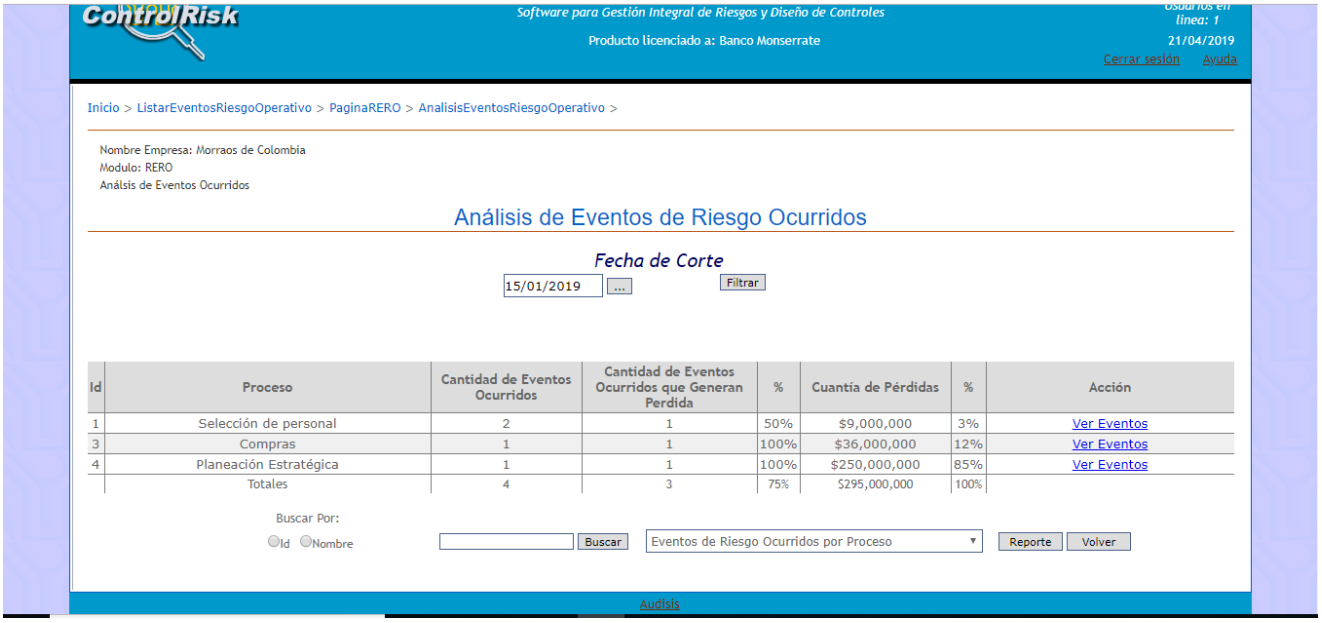


Figura 14: Análisis de Eventos de Riesgo Ocurridos

Con los resultados del análisis de cada evento ocurrido, la Gerencia y los Administradores de riesgos de la Empresa pueden tomar decisiones respecto a las medidas correctivas necesarias para *mejorar el valor preventivo* de la información del análisis de riesgos realizada durante la implantación de la gestión de riesgos y los controles establecidos, para reducir la posibilidad de que vuelva a presentarse el evento de riesgo.

Cuando un evento de riesgo ocurrido *no estaba registrado* en la base de conocimientos de gestión de riesgos de la empresa, significa que durante el proceso de implementación de la gestión de riesgo se omitió la identificación de ese evento. El evento *debe adicionarse a la base de conocimientos de Gestión de Riesgos* con la información sobre agentes generadores

del riesgo, vulnerabilidades que permitieron su ocurrencia, la acción de respuesta que ha de implementarse, los controles requeridos y el cargo asignado como responsable o dueño del riesgo.

Cuando un evento de riesgo ocurrido *estaba registrado* en la base de conocimientos de gestión de riesgos de la empresa, significa que los controles establecidos no fueron efectivos para controlar el evento de riesgo o que los controles fueron omitidos en forma accidental o intencional por las personas asignadas para ejecutarlos y supervisarlos. La Gerencia debería revisar la opción de respuesta a riesgos asignada al evento ocurrido y decidir si deben modificarse los procedimientos de gestión para este evento.

MÓDULO 6: MONITOREO DEL PLAN DE CONTINUIDAD DEL NEGOCIO (BCP).

CONTROLRISK provee funcionalidades para verificar la disponibilidad de recursos requeridos por el Plan de Continuidad del Negocio (BCP), las estrategias de continuidad implementadas en la organización y el estado de preparación para ejecutar los procedimientos de administración de crisis, el plan de respuesta a emergencias y el plan de retorno a la normalidad.

Figura 15: Configuración de Elementos del Módulo Monitoreo del BCP

El software tiene opciones para crear y mantener actualizada una lista de comprobación de los elementos claves del Plan de Continuidad del Negocio (BCP), para ser diligenciada por los

jefes o funcionarios de mayor jerarquía dentro de las áreas organizacionales de la Empresa (ver figura 13).

Algunas funcionalidades de este módulo son:

- Poblar / Cargar en la base de datos, los requerimientos que debe satisfacer el BCP.
- Verificar el estado de preparación de las áreas organizacionales para operar en caso de interrupciones.
- Generar checklist – Guías de Autoaseguramiento (CSA: Control Self Assessment) para medir porcentualmente (%) el cumplimiento de los procedimientos y controles del BCP.
- Generación Indicadores de Cumplimiento / preparación para trabajar en modo contingencia.
- Genera Reportes del Monitoreo.

MÓDULO 7: AUDITORÍA AL SISTEMA DE GESTIÓN DE RIESGOS EMPRESARIALES.

La figura 14 muestra el menú principal del módulo de Auditoría al sistema de gestión de riesgos.

Figura 16: Módulo Auditoría al Sistema de Gestión de Riesgos

CONTROLRISK ofrece funcionalidades para satisfacer las actividades de los auditores internos o externos, orientadas a *evaluar y verificar la calidad y cumplimiento* de los siguientes componentes del sistema de Administración de Riesgos (SAR):

a) Auditoría al cumplimiento del Framework o marco de referencia de la gestión de riesgos en la Empresa y la exactitud y calidad de la información de la base de conocimientos de gestión de riesgos y controles de la empresa..

b) El sistema de Gestión de Riesgos y el Diseño de controles para uno más procesos o sistemas de información.

c) Registro de Eventos de Riesgo Ocurrido (RERO) – Auditoria a la exactitud y calidad de la información de los eventos ocurridos, al seguimiento de los planes de acciones correctivas y al cumplimiento de los procedimientos de reporte, registro y análisis de eventos ocurridos.

d) Verificar Plan de Continuidad del Negocio (BCP). Pruebas de cumplimiento y sustantivas a los procedimientos y controles establecidos para el BCP.

e) Realizar Auditorías a la calidad y cumplimiento de los sistemas de gestión de riesgos SARO Y SARLAFT.

Figura 17: Pasos para ejecución de la Auditoría a cada componente del SAR

Para realizar la auditoría a cada componente del SAR, el software ofrece funcionalidades para ejecutar las cuatro fases del proceso de auditoría (ver figura 17):

1. Planeación de la Auditoría.
2. Ejecución de la Auditoría.
3. Comunicación de los resultados.
4. Seguimiento a recomendaciones de la Auditoría.

5. A QUIENES SIRVE LA METODOLOGIA Y EL SOFTWARE CONTROLRISK?

La metodología del software **CONTROLRISK** está orientada a apoyar el trabajo de:

- Gerentes y Analistas de Riesgos.
- Administradores de Seguridad en Tecnología de Información.
- Auditores Internos y Externos, para auditar la Gestión de Riesgos.
- Funcionarios con responsabilidades de Diseño / Evaluación del Sistema de Control Interno.
- Gerentes y Analistas de Proyectos.
- Funcionarios de Gestión de la Calidad o de Organización y Métodos.
- Equipos de Desarrollo de Sistemas.

5. ELEMENTOS QUE RECIBE EL USUARIO DE CONTROLRISK

5.1 ADQUISICIÓN DE LICENCIAS DE USO DEL SOFTWARE CONTROLRISK, A PERPETUIDAD.

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

✓ Un Link para descargar:

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

✓ Derecho a recibir soporte para operación del software y 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.
✓ La posibilidad de renovar el servicio anual de soporte y actualización del software y de la metodología. Para este fin debe pagar el valor del servicio a las tarifas vigentes.

5.2 ADQUISICION DE LICENCIAS POR SUSCRIPCION ANUAL DEL SOFTWARE CONTROLRISK.

Link para descargar:

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

✓ Derecho a recibir soporte para operación y actualización del software durante la vigencia de la suscripción.

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

✓ En caso de no renovarse la suscripción antes de la fecha de vencimiento, la operación del software deja de funcionar.

6. SERVICIO ANUAL DE SOPORTE TÉCNICO Y ACTUALIZACIONES.

Para las licencias a perpetuidad, AUDISIS ofrece el servicio anual de soporte técnico y actualización del software, el cual incluye soporte telefónico o vía internet al usuario para resolver inquietudes relacionadas con la operación y funcionamiento de la metodología **CONTROLRISK.**

Los desarrolladores y analistas de soporte funcional de **CONTROLRISK** se encuentran disponibles para interacción con los usuarios y generar nuevas versiones que pueden ser suministradas vía Internet en su página www.audisis.com.

El acuerdo anual de servicios de soporte técnico y actualización incluye:

✓ Soporte técnico ofrecido por funcionarios de AUDISIS especializados en CONTROLRISK.

✓ 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 CONTROLRISK, en la página web de AUDISIS.

7. REQUERIMIENTOS DE HARDWARE Y SOFTWARE PARA EL FUNCIONAMIENTO DE "CONTROLRISK".

- ✓ **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 CONTROLRISK

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.

Actualmente ofrece nueve (9) tipos de servicios y productos especializados que se presentan a continuación:

1) Interventoría en Proyectos de Tecnología de Información.

2) Servicios de Consultoría en Auditoría de Sistemas y Auditoría de Procesos de Negocio.

3) Consultoría en Gestión de Riesgos, Seguridad y Control Interno en procesos de negocio y en tecnología de información.

4) Fabricación, suministro e implantación de "CONTROLRISK": Software de Administración de Riesgos Empresariales.

5) Fabricación, suministro e implantación de "AUDIRISK": Software de Auditoría Interna y de sistemas basada en riesgos.

6) Fabricación, suministro e implantación de "AUDIT IP ": Software de Seguimiento a Hallazgos de Auditorias efectuadas por terceros o para terceros.

7) Representación, suministro e implantación de "IDEA": Software de Análisis de Datos y Automatización de Pruebas de Auditoría.

8) Representación, suministro e implantación de "ASD AUDITOR": Software de Auditoría Financiera y Análisis Financiero.

9) Educación continuada en Gestión de riesgos, controles, seguridad y auditoría de sistemas de información.

9. EMPRESAS QUE UTILIZAN EL SOFTWARE “CONTROLRISK”.

SECTOR FINANCIERO

- CREDISERVIR – Cooperativa de Ahorro y Crédito – Ocaña.
- PROGRESSA Entidad Cooperativa de Ahorro y Crédito.
- CONFIAR – Cooperativa Financiera- Medellín.

CAJAS DE COMPENSACIÓN FAMILIAR.

- Caja De Compensación Familiar Del Tolima – COMFENALCO TOLIMA.
- Caja de Compensación Familiar de la Guajira – Comfaguajira.
- Caja de Compensación Familiar de Arauca – COMFIAR.

ENTIDADES DEL GOBIERNO.

- OCENSA, Oleoducto Central de Colombia.
- Contraloría General De La República de Colombia. Dirección de Control Interno.
- ESSA. Empresa Electrificadora de Santander. Oficina de Control Interno.

SECTOR INDUSTRIAL.

- AVESCO – Grupo KoKorico. Contraloría Interna.
- LAFAYETTE. Industria Textilera.

SECTOR EDUCATIVO.

- Universidad La Gran Colombia – Bogotá. Facultad de Contaduría.

- Universidad Central de Bogotá. Facultad de Contaduría.
- Universidad Autónoma de Colombia. Facultad de Contaduría.
- Universidad Militar Nueva Granada. Bogotá. Facultad de Ciencias Económicas.
- Universidad Panamericana. Bogotá - Facultad de Contaduría.
- Universidad Santo Tomas – Bucaramanga – Facultad de Contaduría.
- Universidad Católica de Colombia – Bogotá. Facultad de ingeniería de sistemas.
- Universidad Pedagógica y Tecnológica de Colombia. UPTC – Tunja.

CLIENTES EN OTROS PAISES.

En Ecuador

- **Banco Central del Ecuador.** Auditoría.

En Bolivia

- **Banco Santacruz. Auditoría**

En Honduras

- **Banco Centroamericano de Integración Económica (BCIE).** Contraloría y Auditoría Interna.

En Perú

- Contraloría General de la República del Perú.
- Universidad Unión Peruana. Lima Perú.