Versión 2016

SOFTWARE DE ADMINISTRACIÓN DE RIESGOS EMPRESARIALES Y DISEÑO DE CONTROLES

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 CONTROLRISK?

CONTROLRISK es un software en Tecnología Web (Cloud Computing), ***para conducir y soportar a corto, mediano y largo plazo*****,** de acuerdo con la norma ISO 31000: 2009 y el marco de referencia ERM (Enterprice Risk Management), las siguientes actividades de la **Gestión de Riesgos Empresariales**:

- **Implantar** la Gestión de Riesgos en los Procesos del Modelo de Operación, los procesos de TIC y los Sistemas de Información automatizados de la Empresa.

- **Monitorear** la gestión de riesgos implantada para los procesos y sistemas de la Empresa, respecto al cumplimiento de los controles establecidos y el mantenimiento de los riesgos inherentes dentro de *niveles de severidad tolerables*.

- **Mantener disponible y Actualizada** la Base de Datos de "Conocimientos de Gestión de Riesgos de la Empresa".

- **Soportar el Mantenimiento y Mejoramiento Continuo** del Sistema de Gestión de Riesgos Empresariales.

- **Auditar la Gestión de Riesgos Empresariales.**

El software consta de siete (7) módulos interrelacionados (ver figura 1) que proveen funcionalidades para ***conducir*** *l*as siguientes actividades de Gestión de Riesgos Empresariales:

a) Automatizar las actividades de **implantación, monitoreo, actualización y mejoramiento continuo** de diferentes Sistemas de Gestión de Riesgos (SGR) en la Empresa, como los siguientes: 1) El sistema de administración de riesgos operativos (SARO); 2) El sistema de administración de riesgos de Lavado de Activos y Financiación del Terrorismo (SARLAFT); 3) El Sistema de Gestión de Seguridad de la Información (ISO 27001); 4) El sistema de gestión de riesgos de salud ocupacional; 5) Los sistemas de Gestión de riesgos del sector salud (Resolución 1740 de 2008 MPS) y 6) Otros sistemas de gestión de riesgos utilizados en la industria.

b) ***Diseñar e Implantar la Gestión de Riesgos*** en los procesos individuales del modelo de operación de la empresa, los procesos de gestión de tecnología de información (modelos COBIT o ITIL), los sistemas de información que soportan el desarrollo de las operaciones de la empresa (Módulo 3).

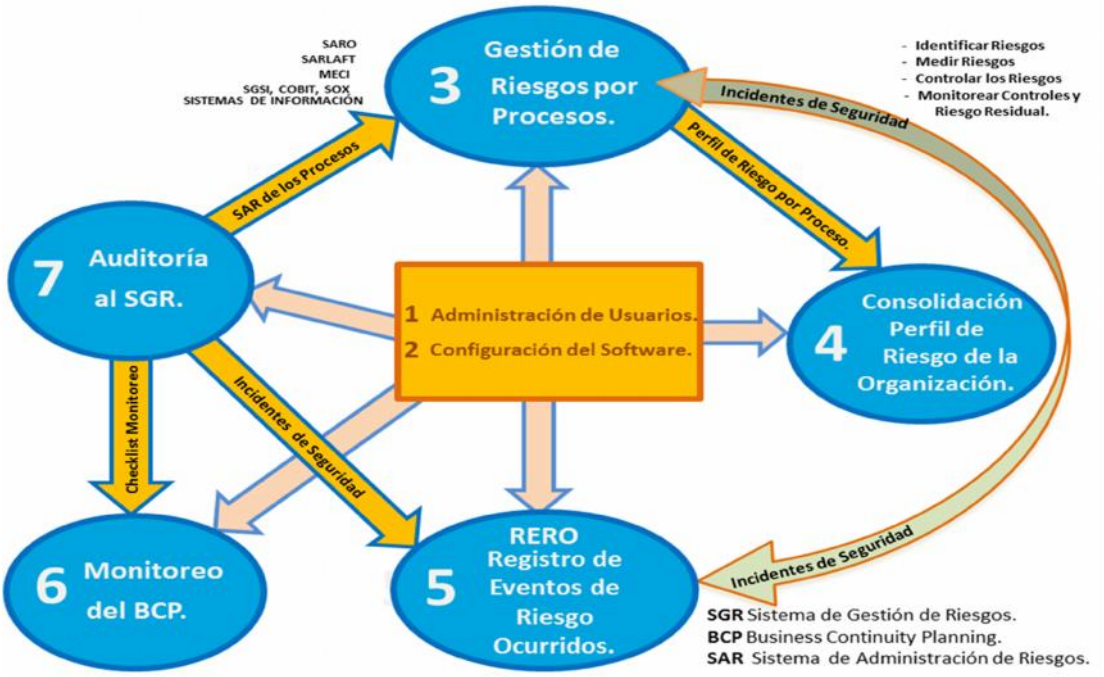


Figura 1: Módulos componentes de CONTROLRISK

c) *Construir el Perfil Consolidado de riesgos inherentes y residuales* de la Organización (por categorías de riesgos, procesos y áreas organizacionales de la Empresa);

d) *Crear, administrar y analizar la base de datos* de Eventos de Riesgo Ocurridos (RERO) en la Empresa;

e) *Monitorear la Operación del Plan de Continuidad del Negocio*; y

f) *Auditar el proceso de Gestión de Riesgos Empresariales*.

Como apoyo para implantar la gestión de riesgos empresariales, CONTROLRISK provee una **Base de Datos de Conocimientos de Gestión de Riesgos**, que contiene numerosas *"mejores y buenas prácticas*" sobre clases o categorías de riesgos (por ejemplo, las consideradas por los modelos SARO, SARLAFT, MECI y AUDIRISK), eventos de riesgo potenciales (amenazas) que pueden originar las clases de riesgo (por ejemplo, eventos de riesgo que podrían generar fraude interno, Sanciones Legales, etc), relaciones entre *categorías de riesgo y eventos de riesgo* (por ejemplo, eventos que podrían generar la clase de riesgo "Fraude Interno"), controles, *relaciones entre eventos de riesgo y controles* (por ejemplo, los controles aplicables al evento "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 productos generados por el software se conservan y administran en un repositorio denominado *Base de Datos de Conocimientos de Gestión de Riesgos y Controles de la Empresa*. Esta Base de Conocimientos crece continuamente en la medida que se avanza en la implantación de la Gestión de Riesgos en los procesos y sistemas de la Empresa, hasta llegar a convertirse en un repositorio único de toda la información de riesgos y controles de la Empresa.

El software **CONTROLRISK** satisface los lineamientos y estándares recomendados para Gestión de Riesgos en los marcos de referencia *ISO 31000:2009, ERM (Enterprise Risk Management – Integrated Framework) y AS/NZ 4360*.

Los procedimientos y guías de *identificación, análisis, control y monitoreo de riesgos* implantados en CONTROLRISK, están alineadas con estándares internacionales y nacionales de 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 o de las tres líneas de defensa*" como requisito para asegurar la *efectividad* de los controles por cada evento de 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 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 al proceso de Gestión de Riesgos de la Empresa.

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

Las siguientes son algunas características de CONTROLRISK que **generan valor para las empresas que adquieren e integran el software a sus procedimientos de Gestión de Riesgos Empresariales:**

1) El software **CONTROLRISK** satisface los lineamientos y estándares recomendados para Gestión de Riesgos en los marcos de referencia *ISO 31000:2009, ERM (Enterprise Risk Management – Integrated Framework) y AS/NZ 4360*.

2) Satisface el objetivo de la Gestión de Riesgos Empresariales. Este *es "Administrar el inventario de riesgos inherentes que pudieran presentarse en los procesos y sistemas de la organización, para **reducir** la posibilidad de ocurrencia y/o el impacto en caso de presentarse".*

3) *La Gestión de Riesgos es PROACTIVA Y PREVENTIVA, es decir, busca anticiparse a la ocurrencia de los eventos de riesgos inherentes para ayudar a prevenirlos y reducirlos a nivel tolerable de riesgo residual. No es REACTIVA ó A posteriori.* Las políticas, normas y procedimientos de Gestión de Riesgos aplican el *enfoque proactivo ó "A priori" de diseño e implantación de los controles,* es decir, estos se diseñan e implantan antes de presentarse los riesgos inherentes.

4) Como apoyo para implantar la gestión de riesgos empresariales, CONTROLRISK provee una **Base de Datos de Conocimientos de Gestión de Riesgos**, que contiene numerosas *"mejores y buenas prácticas*" sobre clases o categorías de riesgos, eventos de riesgo potenciales (amenazas) que pueden originar las clases de riesgo, relaciones de dependencia entre *categorías de riesgo y eventos de riesgo* (por ejemplo, eventos que podrían generar la clase de riesgo "Fraude Interno"), mejores prácticas de control, *relaciones de dependencia entre eventos de riesgo y controles* (por ejemplo, los controles aplicables al evento "Destrucción de la información por incendio accidental") y objetivos de control aplicables a procesos de TI (COBIT e ISO 27001) y aplicaciones de computador.

5) Como ayuda para identificar los eventos de riesgo inherentes, los controles aplicables a los eventos de riesgo y para realizar el monitoreo de la gestión de riesgos, el software **"genera"** cuestionarios o checklists de riesgos, controles, guías de autocontrol y guías de Autoevaluación o Auto-aseguramiento de controles (Del inglés CSAs: Control Self Assessment). *Estos cuestionarios **no son insumos que se preparan anticipadamente para ser ingresados al software**; son productos que genera el software, soportándose en una Base de Datos de Conocimientos de Gestión de Riesgos suministrada por el proveedor, con numerosas "Good and Best practices" sobre clases de riesgos, eventos de riesgo inherentes y controles.* Por ejemplo, el software genera listas de eventos de riesgo inherentes que pudieran generar 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**.**

6) Para identificar los controles necesarios por cada evento de riesgo inherente, *el software genera cuestionarios de controles que "deberían existir" (en formato CSA), en lugar de cuestionarios con los controles establecidos o existentes, los cuales a veces no están documentados ó no son conocidos por los dueños de los procesos y sistemas.* Para este fin, los analistas de riesgos y diseñadores de controles se apoyan en las "best practices" de control documentadas en la *Base de Conocimientos de Gestión de Riesgos* suministrada por el proveedor del software.

7) Para analizar los eventos de riesgos inherentes por cada proceso o sistema, *el software provee formularios para documentar siete (7) 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) 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.

8) Por cada evento de riesgo inherente, *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), el cual se muestra pantalla con reportes y gráficos para las tres (3) dimensiones del **Cubo de Riesgos del proceso**: a) por categorías de riesgo, b) por Dependencias (áreas de la estructura de organización o terceros) y c) por actividades del proceso.

9) *El software provee funcionalidades para asegurar 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.*

10) *Durante la implantación del Sistema de Gestión de Riesgos de cada proceso o sistema, los facilitadores (analistas o asesores de riesgos) actúan como **Agentes de Cambio** de la "Cultura de Riesgos y Controles" de la Empresa para promover el mejoramiento de la consciencia de seguridad, los estándares de diseño de controles internos, el autocontrol y la autogestión.*

11) *La implantación de la Gestión de Riesgos en cada proceso o sistema aplica y promueve el 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.*

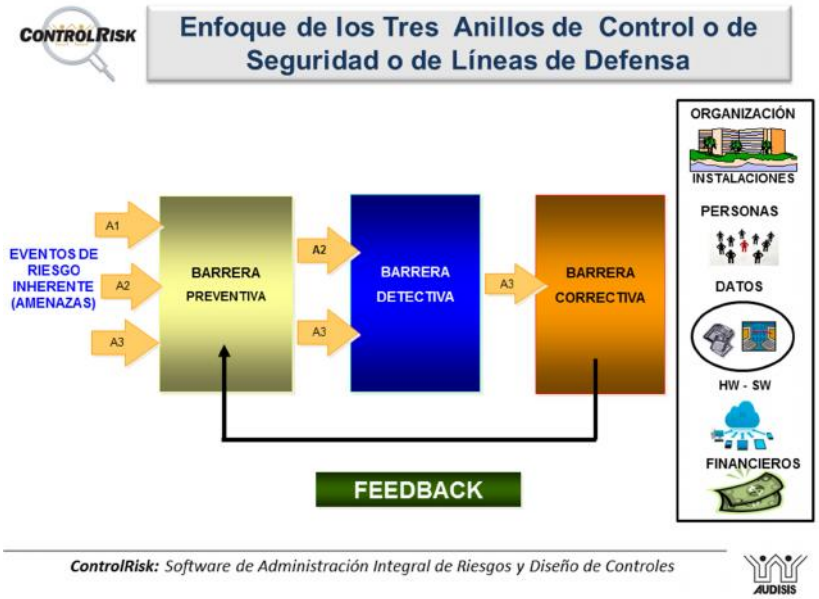


Figura 2: Los 3 anillos de seguridad o líneas de defensa de los controles.

12) 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).

13) *Para gestionar los eventos de riesgo inherentes de cada proceso o sistema, el software evalúa y mide cualitativamente la "efectividad de los controles para reducir el riesgo".* La escala de calificaciones de efectividad de los controles es la siguiente: 1- Apropiada, 2-Mejorable, 3- Insufiicente, 4- Deficiente y 5- Muy deficiente.

14) Para los eventos de riesgo inherentes que presenten efectividad de los controles MEJORABLE, INSUFICIENTE, DEFICIENTE Y MUY DEFICIENTE, *el software conduce el diseño tratamientos del riesgo.* Estos se refieren a los controles adicionales que se necesitan para asegurar que el riesgo inherente se reduce a niveles aceptables de riesgo residual; 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*** a los cargos

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

15) 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.

16) El software conduce la asignación de *cargos responsables de ejecutar y supervisar los controles establecidos* para los eventos de riesgo inherentes de cada 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* para los cargos responsables de ejecutar y supervisar los controles.

17) El software produce *Guías de Autoevaluación de Controles (en inglés CSA: Control Self Assessment)* para monitorear (auto-asegurar) periódicamente el cumplimiento de los controles establecidos y el nivel de riesgo residual aceptable en los eventos de riesgo inherentes, para ser diligenciadas en cada una de las dependencias que intervienen en el proceso. 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 monitoreos.

18) En cada monitoreo, el cumplimiento de los controles y el riesgo residual, por cada evento de riesgo inherente, se mide con una escala de cinco calificaciones, 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%). 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%).

19) Como resultado de cada monitoreo, el software provee funcionalidades para diseñar planes de mejoramiento, planear su implantación, ejecutar seguimientos y enviar correos electrónicos

de recordatorio a los responsables de implantar, supervisar y hacer seguimiento a las acciones de mejora.

20) *Consolidación del Perfil de Riesgo Institucional de la Empresa*. El software CONSOLIDA 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 la gestión de riesgos. 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.

21) *Creación, mantenimiento y explotación del Registro de Eventos de Riesgo Ocurridos*. El software provee funcionalidades para cargar información de los *eventos de riesgo ocurridos* en la empresa, en una **base de datos denominada "Registro de Eventos de Riesgo Ocurridos (RERO)".** 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.*

22) ***Monitoreo del Plan de Continuidad del Negocio***. El software verifica 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.

23) *Auditoría al Sistema de Gestión de Riesgos Empresariales.* El software provee funcionalidades para conducir a las actividades de auditores internos o externos orientadas a *evaluar y verificar* el funcionamiento de los siguientes componentes del sistema de Administración de Riesgos (SAR): a) La Gestión de Riesgos y Diseño de controles para uno más procesos o sistemas de información. Auditoría al cumplimiento del Framework o marco de referencia de la gestión de riesgos y a la exactitud y 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; c) Verificar Plan de Continuidad del Negocio (BCP) (pruebas de cumplimiento y sustantivas a los procedimientos y controles establecidos para el BCP).

24) El software promueve la transición de los analistas de riesgos y diseñadores de controles, del estado de *"consumidores de conocimientos" al estado de "generadores de conocimiento y de valor para las organizaciones".*

25) *El software CONTROLRISK, se generan* ***numerosos reportes resumidos y detallados*** *con los entregables o productos de la implantación de la gestión de riesgos en los procesos y sistemas de información 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 de controles, b) después de implantar los tratamientos y después de cada monitoreo.

3. MODULOS COMPONENTES Y FUNCIONALIDADES DEL SOFTWARE "CONTROLRISK".

MÓDULO 1: ADMINISTRACIÓN DE USUARIOS.

Figura 3: Módulo 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. Los perfiles de acceso en CONTROLRISK son los siguientes:

- ❑ Gerente de Riesgos.
- ❑ Administrador de Usuarios.
- ❑ Administrador de EGR (Estudios de Gestión de Riesgos).
- ❑ Analista de Riesgos.
- ❑ Auto-evaluador - Monitoreo de riesgos, CSA.
- ❑ Administrador RERO.
- ❑ Auxiliar de RERO.

- Administrador BCP.
- Auto-evaluador del BCP.
- Solo Consulta.
- Administrador de Auditoría.
- Auditor.

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.

Figura 4: Elementos de Configuración del Sistema

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*. 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.

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 Y CONTROLES POR PROCESOS Y SISTEMAS DE INFORMACIÓN.

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 5).

Este módulo de CONTROLRISK ofrece funcionalidades para desarrollar el ciclo PHVA de cada proceso o sistema, el cual se denomina ***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 Sistemas de Gestión de la Empresa: El Sistema de Gestión de Seguridad de la Información (ISO 27001), el Sistema de administración de Riesgos Operativos (SARO), el Sistema de riesgos de Lavado de Activos y Financiación del Terrorismo (SARLAFT), el sistema de riesgos de salud ocupacional, riesgos del sector salud (Resolución 1740 de 2008 MPS) y otros modelos de gestión de riesgos utilizados en la industria; y

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

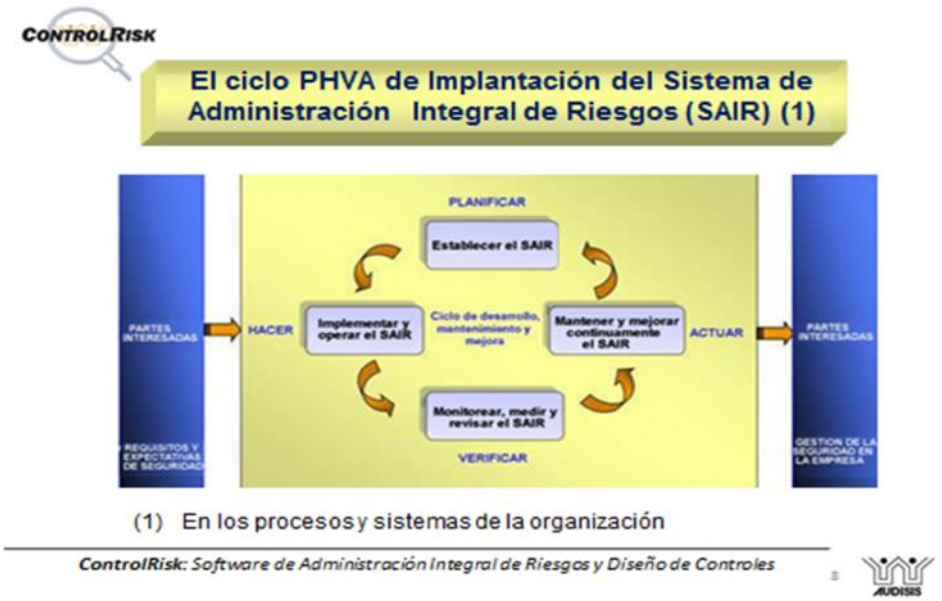


Figura 5: Ciclo PHVA del proceso Gestión de Riesgos

Etapas de la Metodología para Implantar la Gestión de Riesgos en los procesos y Sistemas de la Empresa.

El software CONTROLRISK provee funcionalidades para conducir la implantación de la Gestión de Riesgos de cada proceso o sistema, a través de ocho (8) etapas que se muestran en la figura 6 y se describen a continuación:

Figura 6: Etapas del Proceso de Gestión de Riesgos

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 conducir el ingreso de información que define las características y el ambiente de operación del proceso o sistema objeto del EGR, las cuales servirán como marco de referencia 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, se identifican y analizan los *eventos de riesgo negativos* que podrían ocurrir y causar daño a uno o más activos del proceso (máximo 10, mínimo 6. Estos eventos de riesgo inherente se denominan **amenazas** y se localizan o ubican en el *Mapa de Riesgos Inherentes* del proceso sujeto de EGR.

Para analizar los eventos de riesgo inherente identificados, 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 de riesgo, 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), el cual se muestra pantalla con reportes y gráficos para las tres (3) dimensiones del **Cubo de Riesgos del proceso**: a) por categorías de riesgo, 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), el perfil de riesgos del proceso por diferentes conceptos y la definición de las alternativas de manejo 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. 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 los sistemas de administración de riesgo SARO y SARLAFT ó del modelo de control interno MECI (para el sector público colombiano);

b) **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

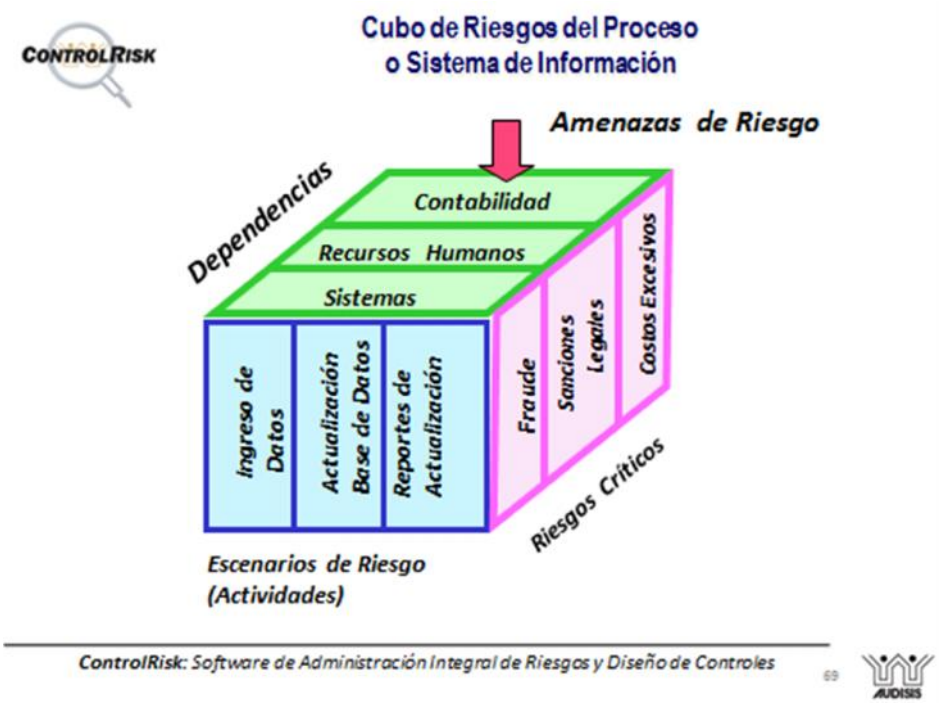


Figura 7: Cubo de Riesgos del Proceso o Sistema de Información

c) **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".

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

Etapa 4 – Evaluación de Riesgos después de Controles y Diseño de Tratamiento de Riesgos.

En esta etapa el software CONTROLRISK genera *cuestionarios o guías de controles*[1] con las buenas prácticas de Controles que deberían existir para reducir la 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.

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).

Para *medir la efectividad de los controles* por cada evento de riesgo inherente, el software utiliza 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). A cada uno de estos niveles de efectividad de los controles corresponde un nivel de riesgo residual, así: 1- Bajo (Si efectividad 1- Apropiada; 2- Moderado (Si efectividad 2 - mejorable); 3- Alto (Si efectividad 3- Insuficiente); 4: Extremo (Si efectividad 4 - Deficiente ó Si Efectividad 5- Muy deficiente).

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 seguimiento y hasta que sean implantadas todas las acciones de tratamiento, el software provee funcionalidades para ***configurar y enviar correos electrónicos de recordatorio*** a los cargos funcionarios asignados como

[1] Este checklist es una forma de ***Control Self Assessment – CSA-*** para ser diligenciado por los dueños o responsables del proceso.

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* para los cargos 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)* para monitorear (auto-asegurar) el cumplimiento de los controles establecidos y el nivel de riesgo residual aceptable en los eventos de riesgo inherentes, para ser diligenciadas en cada una de las dependencias que intervienen en el proceso. 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 monitoreos.

El cumplimiento de los controles y el riesgo residual por cada evento de riesgo inherente se mide con una escala de cinco calificaciones, 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%). 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 ajustar y corregir la gestión de riesgos del proceso en concordancia con las debilidades o deficiencias identificadas en el monitoreo y los cambios en las operaciones de negocio y el soporte tecnológico.

El software CONTROLRISK también provee funcionalidades para diseñar, planear y ejecutar múltiples seguimientos del **Plan de Mejoramiento de la Gestión de Riesgos del EGR** que resulta de cada monitoreo. Para ejecutar los seguimientos, el software asiste la **configuración y envío de correos electrónicos de recordatorio** a los cargos asignados para implantar, supervisar la implantación y efectuar seguimiento a las acciones de mejora.

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.

MÓDULO 4: CONSOLIDACIÓN DEL PERFIL DE RIESGOS INSTITUCIONAL.

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 8.

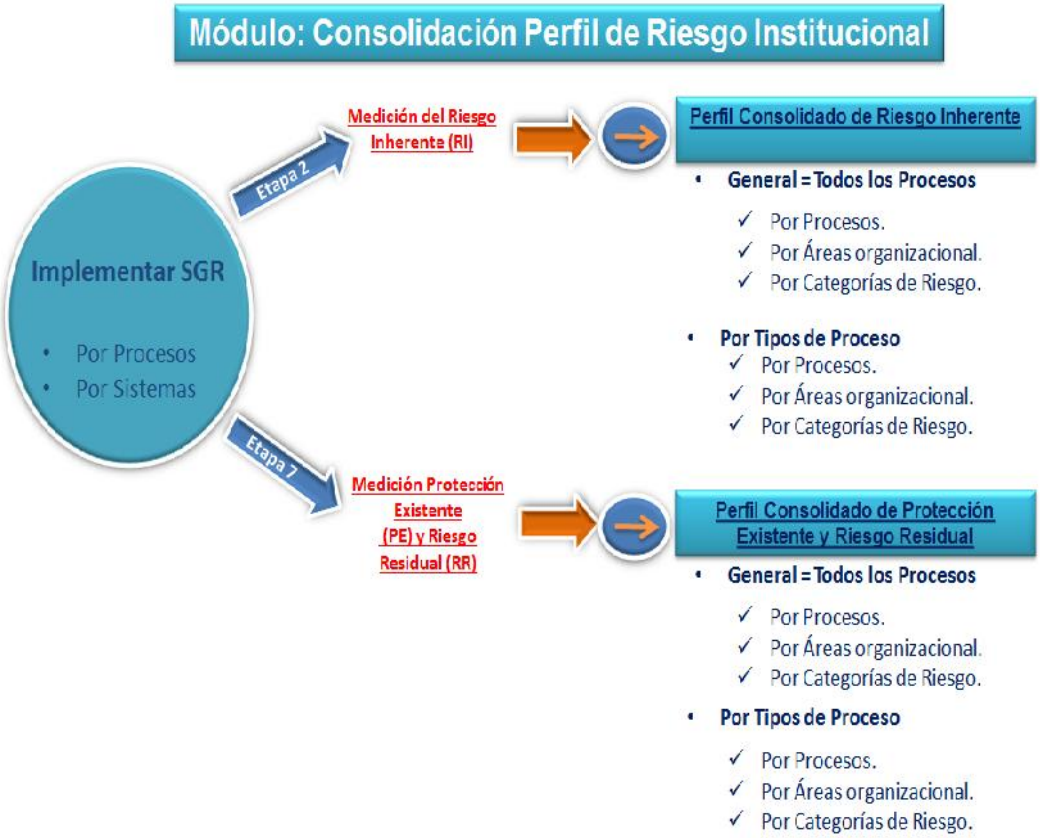


Figura 8: Funcionalidades del Módulo de Consolidación del Perfil de Riesgo

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.

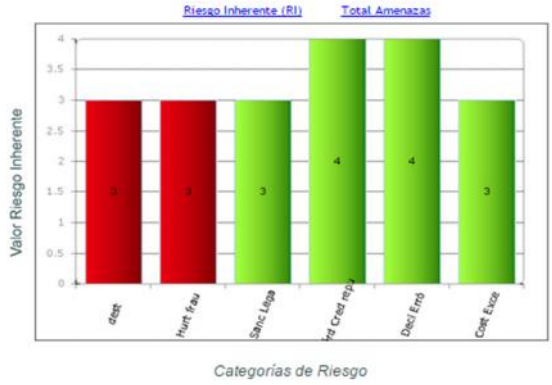
a) El Perfil de Riesgo Inherente Consolidado de la Organización.

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



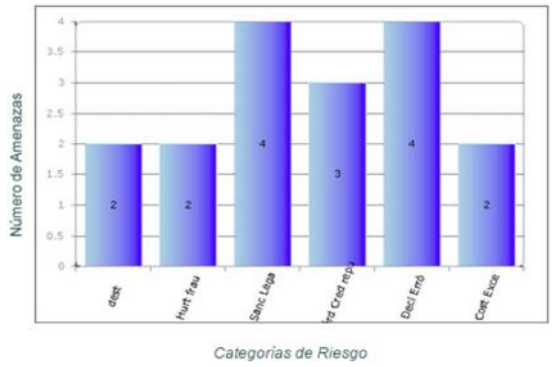


Figura 9: Consolidado del Perfil de Riesgo Inherente – Categorías de Riesgo

b) El Perfil de Protección Existente y Riesgo Residual Consolidado de la Organización.

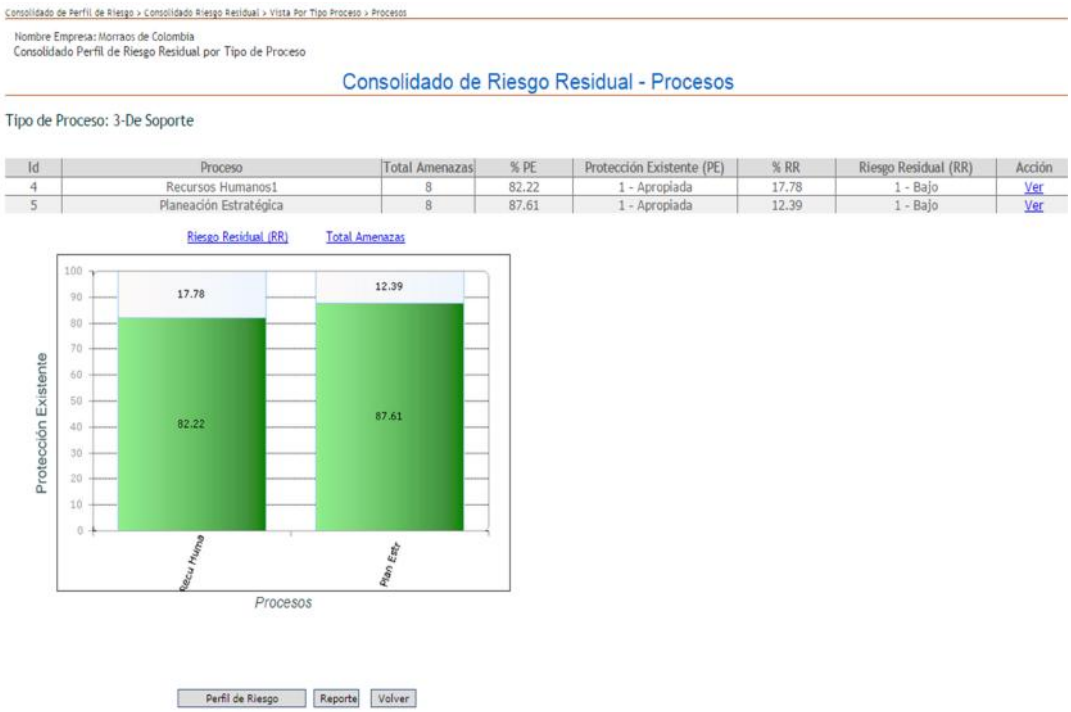


Figura 10: Consolidado del Perfil de Riesgo Residual – Procesos

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).

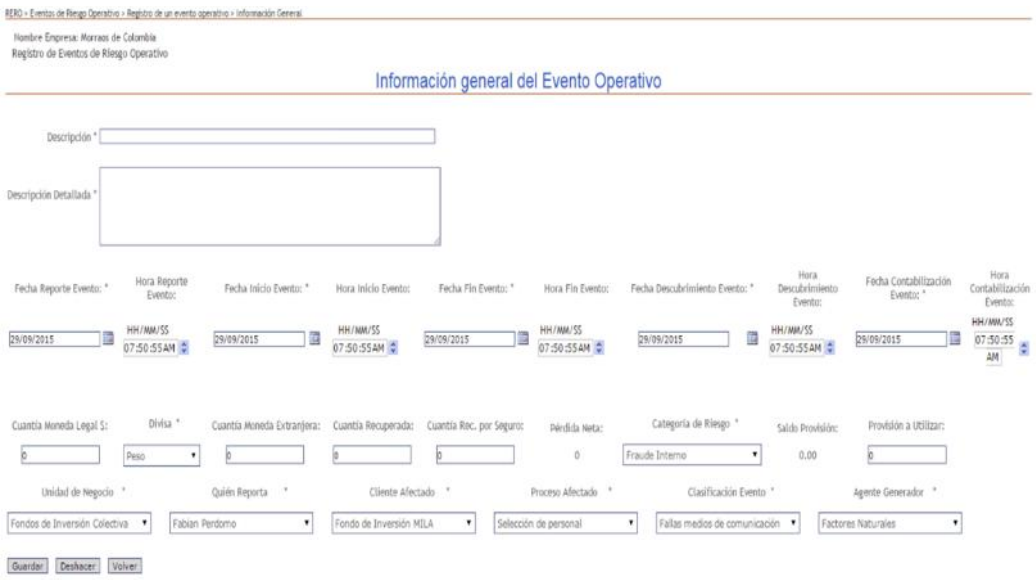


Figura 11: Formulario de Ingreso de Registro de Eventos de Pérdida Ocurridos

CONTROLRISK provee funcionalidades para conducir el ingreso y cargue de información de los eventos de riesgo ocurridos en cualquier sitio de la empresa, en la **base de datos de Registro de Eventos de Riesgo Ocurridos (RERO) en la organización.** 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.*

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, **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. 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 de la base de conocimientos y evitar que el evento de riesgo vuelva a presentarse.

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).

Figura 12: Módulo Plan de Continuidad del Negocio

Figura 13: Configuración de Elementos del Módulo 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.

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.

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.

Figura 14: Módulo Auditoría al Sistema de Gestión de Riesgos

CONTROLRISK ofrece funcionalidades para conducir a las actividades de auditores internos o externos orientadas a *evaluar y verificar* el funcionamiento de los siguientes componentes del sistema de Administración de Riesgos (SAR):

a) Gestión de Riesgos y Diseño de controles para uno más procesos o sistemas de información. Auditoría al cumplimiento del Framework o marco de referencia de la gestión de riesgos y a la exactitud y calidad de la información de la base de conocimientos de gestión de riesgos y controles de la empresa.

b) 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.

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

Figura 15: 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 conducir la ejecución de las cuatro fases del proceso de auditoría:

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

4. 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 de Sistemas – 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 CLIENTE.

5.1 POR LA ADQUISICIÓN DE LICENCIAS DE USO DEL SOFTWARE CONTROLRISK.

Por cada licencia monousuario o en red, el usuario de **CONTROLRISK** 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 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, 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.

5.2 POR EL ARRENDAMIENTO ANUAL DEL SOFTWARE CONTROLRISK.

- Claves de Acceso al Software.
- 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 el período contratado por arrendamiento.

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

6. SERVICIO ANUAL DE SOPORTE TÉCNICO Y ACTUALIZACIONES.

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 **CONTROLRISK.**

Los desarrolladores de **CONTROLRISK** para Windows 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 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.

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

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.

9. EMPRESAS QUE UTILIZAN EL SOFTWARE "CONTROLRISK".

SECTOR FINANCIERO

- **Acciones y Valores S.A.**
- **CREDISERVIR – Cooperativa de Ahorro y Crédito – Ocaña.**
- **PROGRESSA Entidad Cooperativa de Ahorro y Crédito.**
- **CONFIAR – Cooperativa Financiera- Medellín.**
- **Banco Popular. Contraloría.**

CAJAS DE COMPENSACIÓN FAMILIAR.

- **Compensar. Caja de Compensación Familiar. Bogotá.** Auditoría General.
- **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.

- **Comisión Nacional de Televisión – CNTV.**
- **OCENSA, Oleoducto Central de Colombia.**

- **INSTITUTO NACIONAL DE VIAS – INVIAS.** Coordinación Área de Desarrollo Informático. Año 2005.

- **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 Costa Rica

- **Cervecería de Costa Rica.** Contraloría

En Guatemala

- **Superintendencia de Bancos (Guatemala)**

En República Dominicana

- **Banco Central - 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.