Versión 8.0

Software para Gestionar el Sistema de Administracion de Riesgos Operativos (SARO)

Presentación del Software

Agenda

- **Estados Actual y deseado de la Gestión de Riesgos Operacionales.**
- ControlRisk Web: ¿Qué es y para Qué Sirve?.
- Módulos Componentes del Software CONTROLRISK Web.
- Características del Software CONTROLRISK Web que generan valor a las Empresas Usuarias
- Perfiles y Privilegios de Acceso al Software.
- Especificaciones Técnicas y Modalidades de Licenciamiento del Software ControlRisk Web.
- Productos que recibe el usuario por la Compra o Arrendamiento del software.
- Beneficios de Utilizar ControlRisk.
- Empresas Usuarias del software ControlRisk.

Estado Actual de la Gestión de Riesgos

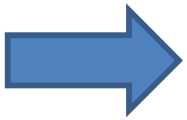
Software y Enfoques Utilizados.

Estado Actual de la Gestión de Riesgos

1) No siempre se soporta en herramientas de software Especializadas en Gestión de Riesgos.

2) Información de la Gestión de Riesgos dispersa, en hojas electrónicas o en herramientas no especializadas.

3) Aplica **Enfoque Reactivo de los Controles.** Estos tienen como propósito detectar la ocurrencia de los riesgos .



Estado Deseado - ControlRisk

1) Se soporta en una herramienta de software Especializada en Gestión de Riesgos Empresariales.

2) Información de la Gestión de Riesgos de los procesos de la empresa **se almacenada en una base de datos única**, que consolida todos los riesgos y controles de la organización.

3) Utilizar ***Enfoque Proactivo y Preventivo de los Controles –*** Todos los controles deben actuar antes de la ocurrencia de los riesgos.

Estado Actual de la Gestión de Riesgos

Estándares utilizados, Monitoreo y Gestión de Riesgo Tecnológico.

Estado Actual de la Gestión de Riesgos

4) Utiliza métodos de análisis de riesgo cualitativo.
5) No utiliza estándares para "Diseñar controles y asegurar efectividad de Controles utilizados, por evento de riesgo".
6) No Ejecutan Monitoreos periódicos a los riesgos y los controles.
7) No mantienen registros actualizados de eventos de riesgo ocurridos.
8) Bajo Enfasis en riesgos y controles de los servicios de Sistemas de la Empresa (TICs).
9) Seguimiento manual a acciones de tratamiento y de mejora

Estado Deseado - Con ControRisk

4) Utiliza métodos de **Análisis de Riesgo Cuantitativo**.
5) Estandariza Criterios para diseño de los controles y asegurar efectividad de los mismos, por evento de riesgo.
6) Realiza monitoreos periódicos y genera indicadores de gestión.
7) Se Mantiene actualizada una base de datos con la historia de eventos de riesgo ocurridos en la Empresa.
8) Enfatiza en los riesgos y controles en la Infraestructura de TI y aplicaciones de Computador.
9) Automatiza seguimiento de Planes de tratamiento y Acciones de mejoramiento y Correctivas.

Agenda

- Estados Actual y deseado de la Gestión de Riesgos Operacionales.
- **ControlRisk Web: ¿Qué es y para Qué Sirve?.**
- Módulos Componentes del Software CONTROLRISK Web.
- Características del Software CONTROLRISK Web que generan valor a las Empresas Usuarias
- Perfiles y Privilegios de Acceso al Software.
- Especificaciones Técnicas y Modalidades de Licenciamiento del Software ControlRisk Web.
- Productos que recibe el usuario por la Compra o Arrendamiento del software.
- Beneficios de Utilizar ControlRisk.
- Empresas Usuarias del software ControlRisk.

ControlRisk Web

¿Qué es y Para Qué Sirve?.

Software Web ***para gestionar la*** **implantación y mejoramiento continuo del Sistema de Administración de Riesgos Operativos (SARO)** en los procesos del modelo de operación y la Tecnología de Información de las Empresas.

1) **Implantar el ciclo PHVA de** la Gestión de Riesgos Operativos en los procesos de la cadena de valor de la empresa, los procesos de TIC, los Sistemas de Información automatizados (aplicaciones de computador ó módulos de ERPs)
2) **Mejorar y actualizar continuamente** la Gestión de Riesgos.
3) **Construir y actualizar el "Perfil Consolidado de Riesgos Operativos de la Empresa".**
4) **Crear y mantener actualizada** *la Base de Datos de Registro de Eventos de Riesgo Ocurridos (RERO) en la organización.*
5) **Monitorear el funcionamiento del Plan de Continuidad del Negocio de la Organización.**
6) **Auditar** la Gestión de Riesgos Operativos de la Empresa.

Concepto de Riesgo Operativo

Se entiende por Riesgo Operativo:

"La posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos. Esta definición incluye el riesgo legal, de custodia y reputacional, asociados a tales factores".

(**Circular Externa 025 de 2020 de la SFC y Guía de Administración del Riesgo, numeral 2.6 ,DAFP, año 2022,).**

Concepto de Riesgo Operativo

Se entiende por Riesgo Operativo:

"La posibilidad de incurrir en pérdidas por deficiencias, fallas, ausencias o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura física o por la ocurrencia de acontecimientos externos. El Riesgo Operativo está asociados al riesgo legal y al riesgo reputacional".

(**Circular Básica Contable y Financiera, Supersolidaria Capítulo IV).**

Sistema de Administración del Riesgo Operativo - “SARO”

Clasificación de los Riesgos Operativos.

1. Fraude Interno

Actos que tienen como resultado defraudar, apropiarse de bienes indebidamente o incumplir regulaciones, leyes o políticas empresariales vigentes en los que se encuentra implicado, al menos, un empleado o tercero contratado para ejecutar procesos a nombre de la entidad.

2. Fraude Externo.

Actos realizados por una persona externa a la entidad, que buscan defraudar, apropiarse indebidamente de activos de la misma o incumplir normas o leyes**, en los que se encuentra implicado un tercero ajeno a la entidad.**

3. Relaciones laborales y Seguridad Laboral.

Actos que son incompatibles con la legislación laboral o con acuerdos relacionados con la higiene o la seguridad en el trabajo, o que versen sobre el pago de reclamaciones por daños personales o casos relacionados con la diversidad y/o discriminación en el ámbito laboral.

Sistema de Administración del Riesgo Operativo - “SARO”

Clasificación de los Riesgos Operativos

4. Clientes, Productos y Prácticas Empresariales.

Incumplimiento involuntario o negligente de una obligación profesional/empresarial frente a clientes o eventos derivados de la naturaleza o diseño de un producto.

5. Daños a activos físicos

Pérdidas derivadas de daños o perjuicios a activos físicos de la entidad como consecuencia de desastres naturales, actos de terrorismo, vandalismo u otros acontecimientos

6. Fallas tecnológicas

Hechos o cambios originados por fallas del hardware, software, telecomunicaciones o servicios públicos que puedan afectar, además de la operación interna de la entidad, la prestación del servicio a los clientes.

Sistema de Administración del Riesgo Operativo - “SARO”

Clasificación de los Riesgos Operativos

7. Ejecución y administración de procesos

Errores en el procesamiento de operaciones o en la gestión de procesos, así como en las relaciones con contrapartes comerciales y proveedores.

8. Riesgo legal.

Es la posibilidad de pérdida en que incurre una entidad al ser sancionada u obligada a indemnizar daños como resultado del incumplimiento de normas o regulaciones y obligaciones contractuales. El riesgo legal surge también como consecuencia de fallas en los contratos y transacciones, derivadas de actuaciones malintencionadas, negligencia o actos involuntarios que afectan la formalización o ejecución de contratos o transacciones.

9. Riesgo Reputacional.

Es la posibilidad de pérdida en que incurre una entidad por desprestigio, mala imagen, publicidad negativa, cierta o no, respecto de la institución y sus prácticas de negocios, que cause pérdida de clientes, disminución de ingresos o procesos judiciales.

Concepto de Riesgo de LA /FT

Se entiende por Riesgo de lavado de Activos y Fin Financiación del Terrorismo (LA/FT):

"La posibilidad de pérdida o daño que puede sufrir una entidad vigilada por su propensión a ser utilizada directamente o a través de sus operaciones como instrumento para el lavado de activos, canalización de recursos hacia la realización de actividades terroristas **y/o financiación de armas de destrucción masiva**, o cuando se pretenda el ocultamiento de activos provenientes de dichas actividades. El riesgo de LA/FT se materializa a través de los riesgos asociados, **estos son: el legal, reputacional, operativo y de contagio,** a los que se expone la entidad, con el consecuente efecto económico negativo que ello puede representar para su estabilidad financiera cuando es utilizada para tales actividades".

(**Circular Externa 027 de 2020, SFC).**

Menú Principal del Software ControlRisk Web

ControlRisk Web

CONTRORISK está alineado con estándares internacionales y nacionales vigentes de Gestión de Riesgos, Control Interno, Seguridad y Calidad

- **ISO / IEC 31000: 2018** Risk Management — Guidelines on principles and implementation of risk management.
- ERM_ 2017 - Enterprice Risk Management.
- Modelos Internacionales y nacionales de Control Interno: COSO 2013, COBIT, MECI, DAFP.
- ISO 27001: 2022 Sistema de Gestión de Seguridad de la Información (SGSI).
- SARO: Sistema de Administración de Riesgo Operativo.
- SARLAFT.: Sistema de Administración de Riesgos de Lavado de Activos y Financiación del Terrorismo.
- ISO 22301: 2019 (BCMS, BCP).
- ISO 9001, ISO 14000, ISO 18000.
- CE 025 de 2020 SFC, CE025 de 2020 de Supersolidaria. Guía de gestión de riesgos del DAFP

Agenda

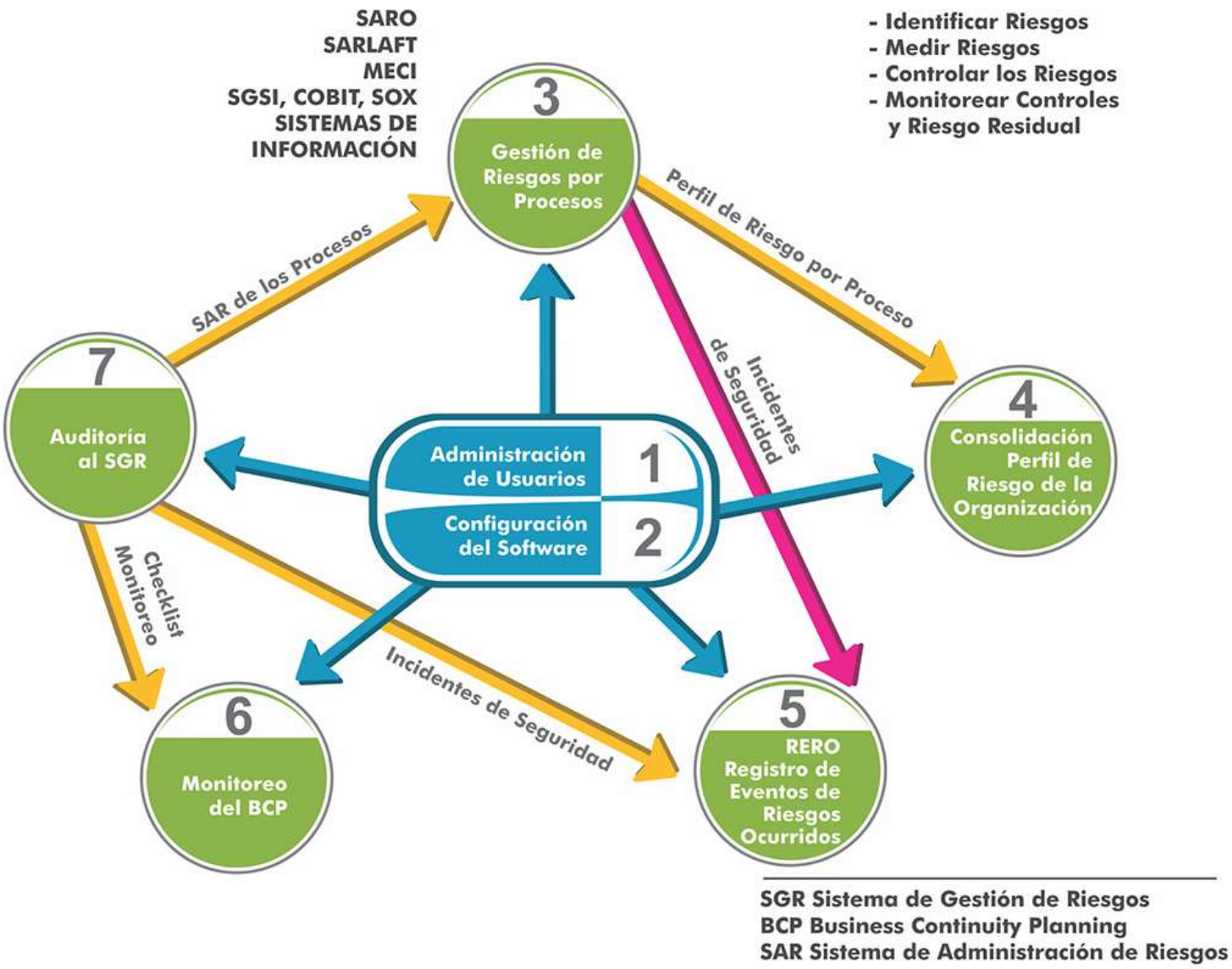
- Estados Actual y deseado de la Gestión de Riesgos Operacionales.
- ControlRisk Web: ¿Qué es y para Qué Sirve?.
- **Módulos Componentes del Software CONTROLRISK Web.**
- Características del Software CONTROLRISK Web que generan valor a las Empresas Usuarias
- Perfiles y privilegios de Acceso al Software
- Especificaciones Técnicas y Modalidades de Licenciamiento del Software ControlRisk Web.
- Productos que recibe el usuario por la Compra o Arrendamiento del software.
- Beneficios de Utilizar ControlRisk.
- Empresas Usuarias del software ControlRisk.

Módulos de CONTROLRISK Web

Módulos Componentes.

1. Administración de Usuarios.
2. Configuración del Software.
3. Gestión de Riesgos Operativos (Operacionales).
4. Consolidación Perfil de Riesgos Operativos de la Organización.
5. Registro de Eventos de Riesgo Ocurridos (RERO).
6. Monitoreo del Plan de Continuidad del Negocio (BCP.
7. Auditoría del SARO.
8. Seguimiento a Acciones de Tratamiento, Acciones de Mejoramiento y Acciones Correctivas

Módulos de CONTROLRISK



Administración de Usuarios

Módulo 1.

CONTROLRISK Ofrece dos opciones de autenticación de usuarios:

1) Autenticación manejada por la aplicación de Gestión de Riesgos ControlRisk y
2) Autenticación a través del directorio activo usado en los sistemas operativos Windows.

Ofrece tres (3) tipos de Usuarios:

a) **Administradores de Riesgos** de la Empresa con derechos de acceso a todas las funcionalidades del software.

b) **Dueños de Procesos:** monitoreo de riesgos y controles, Auxiliares RERO, Implantadores AC, AT y AM .

c) **Auditores**

Los perfiles de acceso son los siguientes:

Administradores de Riesgos

- Gerente de Riesgos.
- Gestor de Riesgos.
- Administrador RERO.
- Administrador BCP.
- Auto-evaluador del BCP.

Dueños de Procesos

- Administrador de EGR (Estudio de Gestión de Riesgos), Auxiliar RERO, Implantadores Acciones de Tratamiento, Mejoramiento y Correctivas.
- Auto-evaluador – Monitoreo de riesgos, CSA.

Auditores.

- Gerente de Auditoría.
- Auditor.

ControlRisk Web

Qué es y para que sirve?

Módulo 2:

Configuración del Software.

CONTROLRISK provee funcionalidades para:

- Poblar la Base de Conocimientos de Gestión de Riesgos con información privada de la Empresa.
- Definir tablas de Frecuencia Anual de Ocurrencia de los riesgos, tipos de impacto, criterios de evaluación individual y colectiva de Controles por riesgo, parámetros de monitoreo.
- Configurar el correo corporativo de la *Unidad de Riesgos y la configuración y envío automático de mensajes de recordatorio por Correo electrónico sobre Acciones de Tratamiento y Acciones de Mejoramiento.*

ControlRisk Web

Qué es y para que sirve?

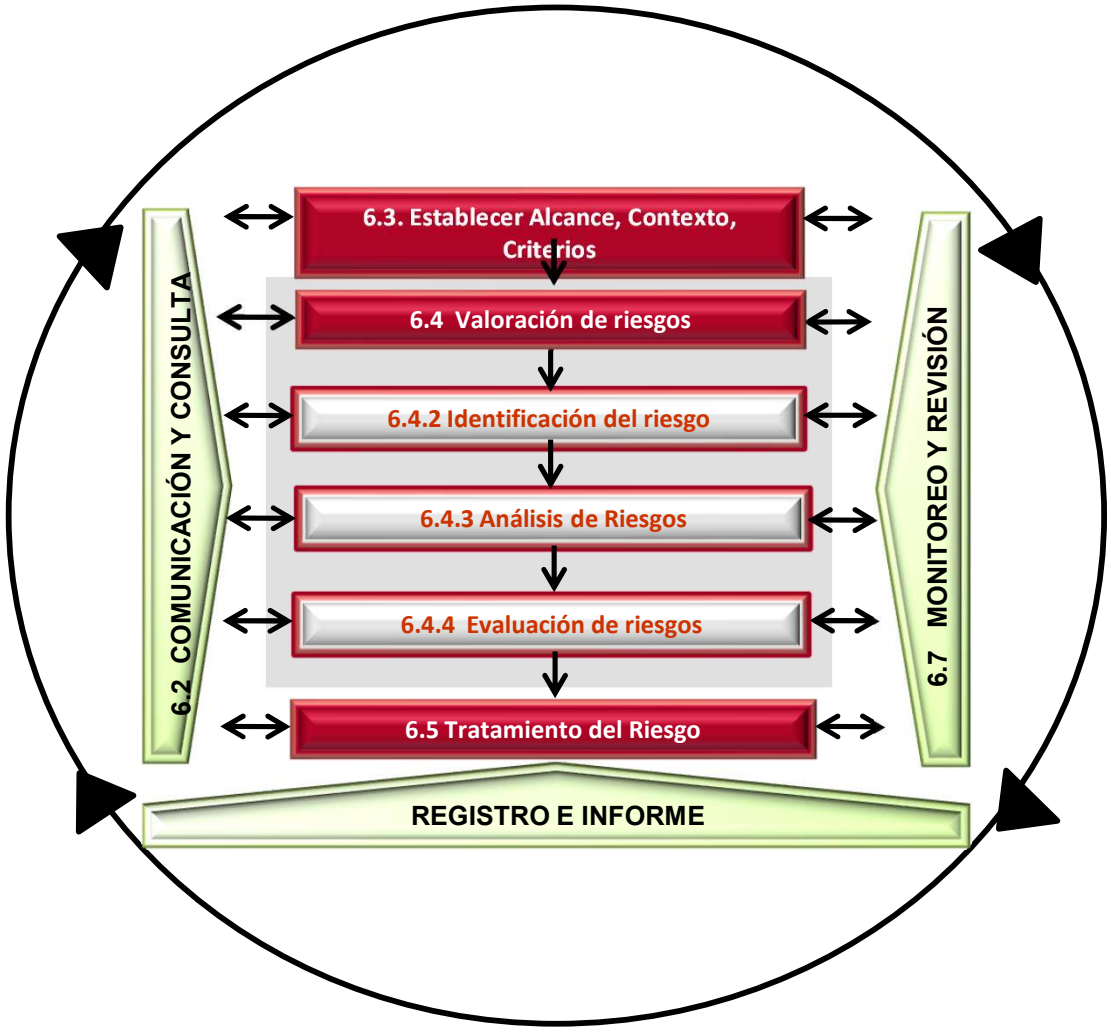
Módulo 3:

Implantar y mejorar continuamente la Gestión de Riesgos por Proceso o Sistema.

CONTROLRISK provee funcionalidades para implantar la Gestión de Riesgos en:

- Los procesos del Modelo de Operación / Cadena de Valor de la Empresa (Estratégicos, Misionales y de Soporte).
- Los procesos de Tecnología de Informacion - Modelos COBIT e ITIL
- Las Aplicaciones de Computador o módulos de ERPs que soporten las operaciones CORE de la empresa.
- El sistema de Gestión de Seguridad de la Informacion (Norma ISO 27001).

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



Módulo 3: Implantar y Mejorar continuamente la Gestión de Riesgos por Proceso / Sistema

1. Provee funcionalidades para desarrollar el ciclo PHVA de la Gestión de Riesgos, por cada proceso o sistema:

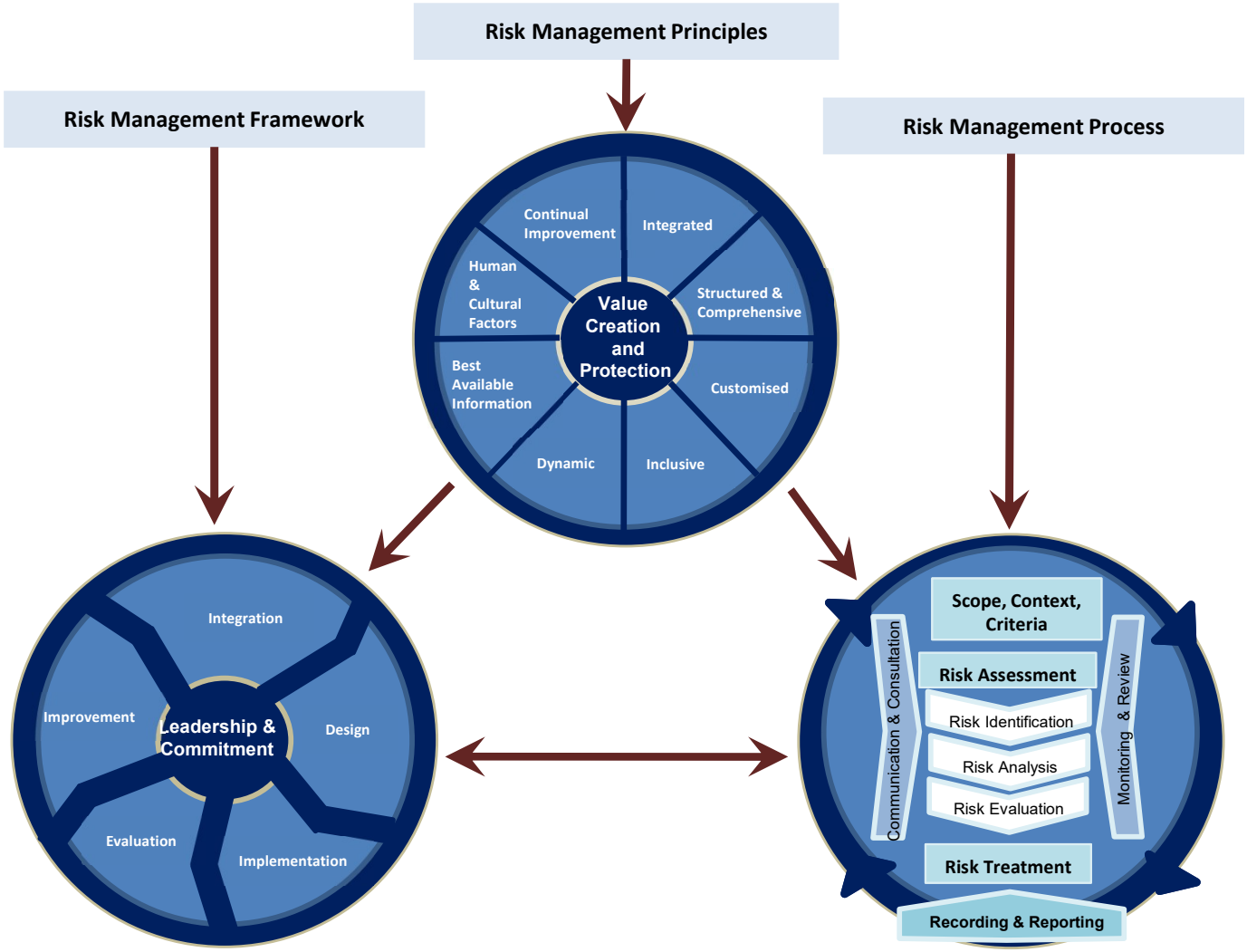
    - **P: Planear-** Identificar, analizar, evaluar los riesgos inherentes; diseñar tratamientos.
    - **H: Hacer-** Implementar procedimientos de gestión de riesgos y el plan de tratamientos.
    - **V: Verificar** - Monitorear periódicamente el funcionamiento de la gestión de riesgos. Generar indicadores de Gestión de Riesgos
    - **A: Actuar / Corregir -** Implantar Acciones de Mejoramiento producto de cada monitoreo.

2. Genera / Actualiza el Manual de Gestión de Riesgos de cada proceso o sistema.

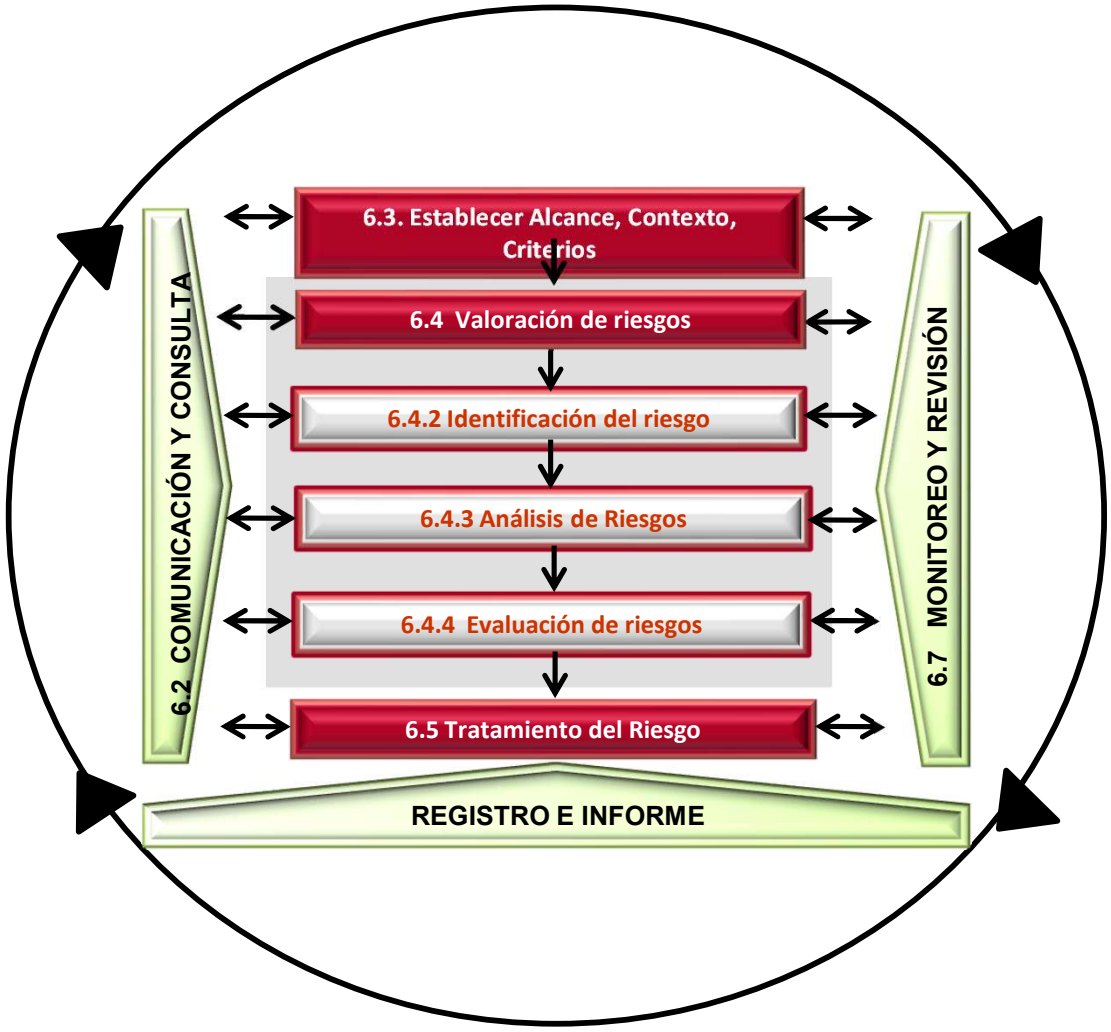
El ciclo PHVA del Proceso de Gestión de Riesgos (1)

(1) En los procesos y sistemas de la organización

Principles, Framework and risk management process from ISO 31000: 2018



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



Módulo 3: Implantar la Gestión de Riesgos

Factores Críticos para la Implantación Exitosa.

1) Obtener el Compromiso y Apoyo de la Gerencia.

2) Definir el Framework o Marco de Referencia de la Gestión de Riesgos Operacionales de la Organización (de acuerdo con ISO 31000 ó ERM).

3) Alinear la Gestión de Riesgos Operacionales con la Estructura del Sistema de Control Interno de la Organización (COSO + COBIT + ISO 27001). En el sector publico de Colombia: MECI + COBIT + ISO 27001. **La Gestión de Riesgos es el Motor del Sistema de Control Interno.**

4) Armonizar la Gestión de Riesgos con el Sistema de Gestión de Calidad (ISO 9001) y otros sistemas de gestión: Ambiental, Salud Ocupacional, gestión de continuidad del negocio – BCP – y el Sistema de Gestión de Seguridad de la Información (ISO 27001).

ControlRisk Web

Qué es y para que sirve?

Módulo 3:

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

Identificar, Analizar, Controlar y Monitorear los Riesgos, de:

ALCANCE DE LA IMPLANTACION.

- **Los Procesos del Modelo de Operación de la Empresa** – Mapa de Procesos de la Cadena de Valor (Estratégicos, Misionales, de Apoyo y de Supervisión y Control).
- **Los procesos de TI (COBIT, ITIL)**
- **Los Dominios de Seguridad de la Informacion – Norma ISO 27001 (SGSI)**.
- **Los Sistemas de Información Automatizados** (Aplicaciones de Computador ó Módulos de ERPs).
- **SARO, SARLAFT, SGSI (Norma ISO 27001), MECI.**

Implantar la Gestión de Riesgos en los procesos y sistemas de la Empresa

Los dos Estados de los Riesgos.

- **Riesgo Inherente (potencial). Riesgo Antes de Controles.** Es el riesgo a cual están expuestos los procesos o las actividades, dada su naturaleza. Es intrínseco, inseparable de las actividades y activos que intervienen en el proceso. Este riesgo no puede evitarse, pero si puede mitigarse. Su SEVERIDAD se evalúa sin tener en cuenta el efecto de los controles establecidos para gestionarlos, si los hubiere.

- **Riesgo residual. Riesgo después de Controles /Tratamientos de riesgo.** Es el riesgo que resta o queda después de aplicar los controles o tratamientos establecidos.

Según ISO 31000: "el ***riesgo residual*** es el riesgo que permanece o persiste después de implementada una opción de tratamiento de riesgos. Este es el riesgo remanente después de que haya reducido el riesgo, removido el origen del riesgo, modificado las consecuencias, cambiado las probabilidades, transferido el riesgo, o retenido el riesgo".

Implantar la Gestión de Riesgos en los procesos y sistemas de la Empresa

Ejemplo: Dos Estados de los Riesgos, por Evento Negativo (Amenaza).

Evento (Amenaza): Robo de dinero en cajero automático (ATM), por suplantación del propietario de la tarjeta.

Riesgo Inherente: Riesgo antes de Controles. (evento) a la que se expone el Banco (usuario), de acuerdo con la naturaleza y modo de operación del cajero automático . En su evaluación no se tienen en cuenta los controles establecidos.

Evaluación: E - Extremo.

Acciones de Respuesta: Reducir (mitigar) el riesgo.

Controles:

- **Preventivos**: Uso de tarjeta y PIN. Políticas de seguridad para uso de cajero automático.
- **Detectivos:** Validar que tarjeta y PIN coincidan. Informar desviación (mensaje) y bloquear.
- **Correctivos:** Reemplazar la tarjeta bloqueada y asignar nuevo PIN.

Riesgo Residual: Riesgo después de Controles y Tratamientos. Amenaza (Evento) no protegida o no cubierta por los controles establecidos. **Evaluación: B - Bajo** (Tolerable).

Implantar la Gestión de Riesgos en los procesos y sistemas de la Empresa

Qué es y para que sirve?

Módulo 3: Implantar la Gestión de Riesgos Operativos . SARO -

Por cada **Proceso ó Aplicación de Computador,** desarrollar el Ciclo PHVA de la gestión de riesgos:

ETAPAS DE LA METODOLOGIA

- **Etapa 1:** Comprender ambiente / Contexto de Riesgos del Proceso.
- **Etapa 2:** Identificar, analizar y documentar los riesgos inherentes que podrían presentarse.
- **Etapa 3:** Elaborar Cubo de Riesgos del Proceso.
- **Etapa 4: Evaluación de Riesgos /** Diagnóstico sobre efectividad Controles Existentes y Tratamiento de los riesgos.
- **Etapa 5:** Evaluación Costo / Beneficio de los Controles.
- **Etapa 6:** Asignar Responsables de Ejecutar y Supervisar los Controles.
- **Etapa 7:** Monitoreo (Autoevaluación) y Mejoramiento de la Gestión de riesgos.

Metodología para Implantar la GR en los procesos y Sistemas de la Organización

Metodología para Implantar la GR en los procesos y Sistemas de la organización

Metodología para Implantar la GR en los procesos y Sistemas de la Organización

Implantar la Gestión de Riesgos
En los procesos y sistemas de la Empresa

Entregables de la Gestión de Riesgos *"por cada proceso o Sistema" – Modelo -*

1) Definición del Contexto Interno y Externo del Proceso.
2) Categorías / Clases de Riesgo Aplicables al Proceso.
3) Identificación de eventos de riesgo negativos (amenazas), por **Categoría** (**clase) de riesgo y factor de riesgo** (el recurso humano, los procesos, la tecnología, la infraestructura y los acontecimientos externos).
4) Análisis de Riesgos Inherentes y Establecer Nivel de Severidad de los Riesgos Inherentes (eventos de riesgo antes de controles).
5) Mapas de Riesgos Inherentes.(por actividad, clase de riesgo y área organizacional)
6) Perfil de riesgo inherente del proceso (por categoría de riesgo, áreas organizacionales y escenarios de riesgo y factores de riesgo).
7) Cubo de Riesgos del proceso.
8) Objetivos de control que deben satisfacerse para el proceso.

Implantar la Gestión de Riesgos en los procesos y sistemas de la Empresa

Entregables de la Gestión de Riesgos *"por cada proceso o sistema"* (Cont).

7) Opciones de manejo del riesgo (acciones de respuesta a riesgos), por cada evento de riesgo inherente (asumir, evitar, mitigar, transferir, distribuir).
8) Identificación Controles establecidos, para los eventos de riesgo inherente (amenazas).
9) Evaluación del **Diseño y Efectividad** de los controles establecidos por Evento de Riesgo (Medición de la Protección Existente y del riesgo residual, después de controles.
10) Definición del Plan de Tratamiento de Riesgos, para Eventos de Riesgo no protegidos apropiadamente.
11) Mapas de Riesgos Residuales – Antes y Después de Tratamientos.
12) Cargos responsables de ejecutar y supervisar los controles.
13) Guías de Monitoreo (autoevaluación o auto-aseguramiento) de los riesgos y de los controles.

ControlRisk Web

Qué es y para que sirve?

Módulo 4:

Consolidar Perfil de Riesgo Operativo de la Organización.

Construye el Perfil de riesgos Operativos a nivel Institucional, con los resultados del último Monitoreo de los procesos.

Entregables

Perfil de Riesgos Inherentes consolidado: a) Por Categorías de Riesgo; b) Por Áreas Organizacionales y c) Por tipos de procesos.

- **Perfil de Riesgos Residuales consolidado:** a) Por Categorías de Riesgo; b) Por Áreas Organizacionales y c) Por tipos de procesos.
- **Perfil de Protección Existente Consolidada**: a) Por Categorías de Riesgo, b) Por Áreas Organizacionales y c) Por tipos de procesos.
- **Matrices Consolidadas de Riesgos Inherentes (RI) y Riesgos Residuales (RR) de los procesos de la Organización.**
- **Genera reportes de Alto Nivel** para los Ejecutivos de la Empresa.

ControlRisk Web

Qué es y para que sirve?

Módulo 5.

Crear / Actualizar Registro de Eventos de Riesgo Ocurridos (RERO)

- **Crear y mantener actualizada** la base de datos con el registro histórico de los Eventos de Riesgo Ocurridos en la Organización.
- **Analiza**r los Eventos de Riesgo Ocurridos, evaluar Eficacia de la Gestión de Riesgos Operativos, diseñar e implantar plan acciones Correctivas..
- **Generar reportes** de eventos de riesgo ocurridos en la organización, por diferentes conceptos.
- **Proveer información de alto nivel** para consulta, análisis y soporte de la decisiones de los Ejecutivos de la Empresa, sobre los Eventos de Riesgo Ocurridos.

ControlRisk Web

Qué es y para que sirve?

Módulo 6.

Monitoreo del Plan de Continuidad del Negocio (BCP) de la Organización.

- Poblar / Cargar en la base de datos, los requerimientos que debe satisfacer el BCP.
- Verifica el estado de preparación de las áreas organizacionales para operar en caso de interrupciones.
- Medir % de cumplimiento de los procedimientos del BCP.
- Generación Indicadores de Cumplimiento / preparación para trabajar en modo contingencia.
- Genera Reportes del Monitoreo.

ControlRisk Web

Qué es y para que sirve?

Módulo 7.

Auditoría al Sistema de Gestión de Riesgos Operativos de la Organización.

- **Auditoría a la Gestión de Riesgos por Procesos:** planeación y pruebas de cumplimiento e informe de la auditoría. Papeles de trabajo.
- **Auditoría al Registro de Eventos de Riesgo Ocurridos:** planeación, pruebas de cumplimiento, pruebas sustantivas, informe de la auditoria y papeles de trabajo.
- **Auditoría al BCP:** Planeación, pruebas de cumplimiento, informe de auditoria y papeles de trabajo.

ControlRisk Web

Qué es y para que sirve?

Módulo 8.

Seguimiento a Implantación de tratamientos de riesgos, Acciones de mejoramiento y acciones correctivas.

- **Acciones de Tratamiento de Riesgos por Proceso:** Avances de implantación, adicionar a controles una vez implantados.
- **Acciones de Mejoramiento por proceso:** Como resultado de cada monitoreo. Adicionar, modificar y eliminar controles por riesgo.
- **Acciones Correctivas por efecto de riesgos materializados:** Adicionar riesgos a la base de datos. Agentes Generadores, vulnerabilidades, controles, reasignar responsables de los controles.

Agenda

- Estados Actual y deseado de la Gestión de Riesgos Operacionales.
- ControlRisk Web: Qué es y para Qué Sirve?.
- Módulos Componentes del software CONTROLRISK Web.
- **Características del Software CONTROLRISK Web que generan valor Agregado a las Empresas Usuarias .**
- Especificaciones Técnicas y Modalidades de Licenciamiento del Software ControlRisk.
- Que recibe el usuario por la Compra o Arrendamiento del software?
- Beneficios de Utilizar ControlRisk.
- Empresas Usuarias del software ControlRisk.

Valor Agregado que genera el Uso de ControlRisk a las Empresas.

El Software ControlRisk:

1) Soporta **Evolución y mejoramiento continuo de la Gestión de Riesgos Operativos (SARO) y de LA/ FT (SARLAFT)**: Implantación, monitoreo periódico y mejoramiento continuo.

2) Provee ***Gestión de Riesgos PROACTIVA Y PREVENTIVA***, *es decir, se anticipa a la ocurrencia de los eventos de riesgos inherentes, para prevenirlos y reducir SEVERIDAD 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 materializarse".*

3) Provee y actualiza una ***Base de Datos de Conocimientos de Gestión de Riesgos y Controles de la Empresa*****.** Esta Base de Datos "*Administra el inventario de riesgos inherentes que pudieran presentarse en los procesos y sistemas de la organización*".

Valor Agregado que genera el Uso del Software a las Empresas.

El Software ControlRisk:

4) ***Es multiempresa,*** es decir, permite realizar la gestión de riesgos operacionales (SARO) de múltiples empresas, con la misma cantidad de usuarios en todas las empresas. Además, con las mismas credenciales y el mismo perfil, un usuario puede realizar la Gestión de Riesgos de múltiples empresas.

5) Provee funcionalidades de **interacción permanente entre los Administradores de Riesgos y los Dueños de Procesos**, a través de correos electrónicos para la implantación y seguimiento de: a) Planes de tratamiento de riesgos; b) Planes de mejoramiento de la gestión de riesgos que resultan de cada monitoreo periódico por proceso; y c) De la implantación de acciones correctivas que resultan del análisis de los eventos de riesgo ocurridos (RERO).

6) *Está alineado con los marcos de referencia ISO 31000: 2018, ERM 2017, COSO 2013, COBIT e ISO 22301: 2019. Hace que la Gestión de Riesgos Empresariales se convierta en* ***el motor*** *del "Sistema de Control Interno de la Empresa".*

Valor Agregado que genera el Uso del Software a las Empresas.

El Software ControlRisk:

7) **Ayuda a Implantar el *Enfoque Proactivo y Preventivo de los Controles, en lugar del enfoque "Reactivo o detrás de los hechos conocidos".*** Es decir, *establece que los controles se diseñen, implanten y actúen antes de materializarse los riesgos inherentes* - **"A priori" respecto a los riesgos**.

8). Genera *Guías y cuestionarios de ayuda* ***para identificar los eventos de riesgo inherentes*** *que pueden presentarse en la operaciones de cada proceso o sistema,* ***por categoría de riesgo****,.*

9) **Estandariza los criterios utilizados en la organización para analizar los riesgos inherentes, diseñar controles y evaluar su efectividad** *(efectividad + eficiencia) para reducir los riesgos inherentes a niveles aceptables de riesgo residual.*

10) Genera *Guías y cuestionarios* ***para identificar los Controles que "deberían existir"*** *por cada riesgo inherente, para reducir su SEVERIDAD a un nivel tolerable de riesgo residual.*

Valor Agregado que genera el Uso del Software a las Empresas.

El Software ControlRisk:

11) ***Por cada proceso o sistema, construye y actualiza el "Cubo de Gestión de Riesgos".*** *Las tres dimensiones del cubo son: a) Categorías de Riesgo Aplicables; b) Actividades que constituyen el Ciclo PHVA del proceso, y c) Areas de la Estructura de organización y terceros que intervienen en el proceso.*

12) *Aplica y promueve la implantación del enfoque de los "**tres anillos ó Barreras de Control", por cada riesgo inherente**.*

13) Genera o 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 o sistema.

Valor Agregado que genera el Uso del Software a las Empresas.

El Software ControlRisk:

14) "Lo que no se mide no puede administrarse". Implementa la cultura de medición en la gestión de riesgos Empresariales:

- Por cada evento de riesgo inherente mide: a) La frecuencia anual de ocurrencia; b) el impacto estimado de cada ocurrencia; c) la perdida anual estimada; y d) La Severidad Estimada con una escala de cuatro (4) calificaciones .
- Mide la **Protección Ofrecida o Efectividad Colectiva de los Controles establecidos** por cada evento de riesgo inherente (amenaza), con una escala de (5) cinco calificaciones.
- Mide la efectividad de los controles por evento de riesgo inherente y del riesgo residual en tres momentos: a) antes de tratamientos; b) después de tratamientos y c) en cada monitoreo.
- Mantiene un registro histórico de las mediciones porcentuales efectuadas a los eventos de riesgo inherentes en los últimos once (11) monitoreos: a) de la protección ofrecida por los controles y b) del riesgo residual.

Valor Agregado que genera el Uso del Software a las Empresas.

El Software ControlRisk:

15) *Consolida* los **perfiles de riesgo Inherente y Residual de los procesos y la TIC de la Empresa**. 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.

16) *Construye y mantiene actualizada la* **base de datos de "Eventos de Riesgo Ocurridos (RERO)" en la organización**, con la que se generan estadísticas e indicadores de riesgo.

17) Monitorea (hace seguimiento) periódico al Plan de Continuidad del Negocio (BCP).

18) Provee funcionalidades para **Auditar el Sistema de Gestión de Riesgos Operacionales (SARO)**.

Valor Agregado que genera el Uso del Software a las Empresas.

19. Provee una **Base de Datos de Conocimientos de Gestión de Riesgos,** con "best practices" universales sobre:

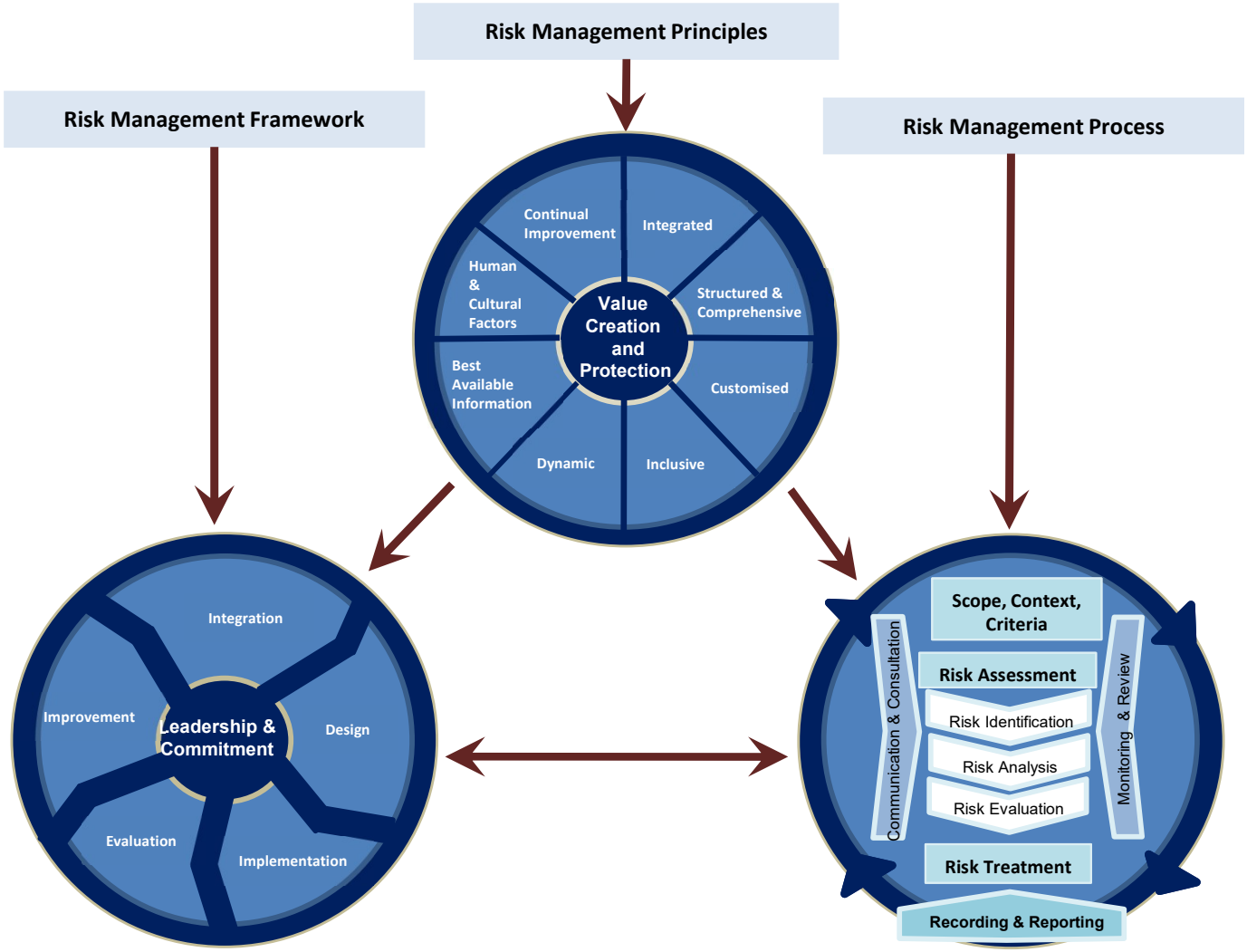
- Clases o Categorías de Riesgos del SARO, SARLAF, Entidades del Sector Publico (MECI / DAFP) y SGSI (ISO 27001), AUDISIS.
- Eventos de riesgo Inherentes (amenazas) que podrían presentarse por cada clase de riesgo.
- Factores y Agentes de Riesgo.
- Tipos y clases de Controles.
- Controles Aplicables.
- Objetivos de control.
- Técnicas y procedimientos de priorización y análisis de riesgos.
- Criterios de medición y aceptación de controles efectivos.
- Cuestionarios de "Best Practices" de Controles aplicables (CSA: Control Self Assessment).
- Guías de Monitoreo o Auto-aseguramiento de Controles (CSA: Control Self Assessment).
- Modelos de Procesos y Escenarios de Riesgo aplicables a TICs según marcos de referencia universales vigentes (COBIT, ISO 27001, Aplicaciones de computador).

Valor Agregado que genera el Uso del Software a las Empresas.

Está alineado con estándares internacionales vigentes de Gestión de Riesgos, Control Interno, Seguridad y Calidad

- ISO / IEC 31000: 2018 Risk Management — Guidelines on principles and implementation of risk management.
- ISO 31010:2019 Risk Management . Risk Assessment Techniques.
- ISO Guide 31073:2022 Risk Management. Vocabulary.
- ERM_ 2017 - Enterprice Risk Management.
- Modelos Internacionales y nacionales de Control Interno: COSO 2013, COBIT, MECI.
- ISO 27001: 2013 Sistema de Gestión de Seguridad de la Información (SGSI).
- ISO 20000: “Best Practices” de Gestión de Tecnologia (ITIL).
- SARO: Sistema de Administración de Riesgo Operativo.
- SARLAFT.: Sistema de Administración de Riesgos de Lavado de Activos y Financiación de l Terrorismo.
- Basilea II.
- ISO 22301: 2019 (BCMS, BCP).
- ISO 9001, ISO 14000, ISO 18000.

Principles, Framework and risk management process from ISO 31000: 2018



Valor Agregado que genera el Uso del Software a las Empresas.

Aplica el enfoque ***"Proactivo y preventivo de los Controles"***, en lugar del enfoque "Reactivo o detrás de los hechos conocidos". *El objetivo de los controles es asegurar el éxito de las operaciones, no es "detectar la ocurrencia de los riesgos".*

Mide la **Capacidad / Efectividad** de los Controles Establecidos (protección que ofrecen) para reducir los riesgos inherentes a niveles aceptables de riesgo residual

- 5: Apropiada, ALTA.
- 4: Mejorable.
- 3: Insuficiente.
- 2: Deficiente
- 1: Muy Deficiente.

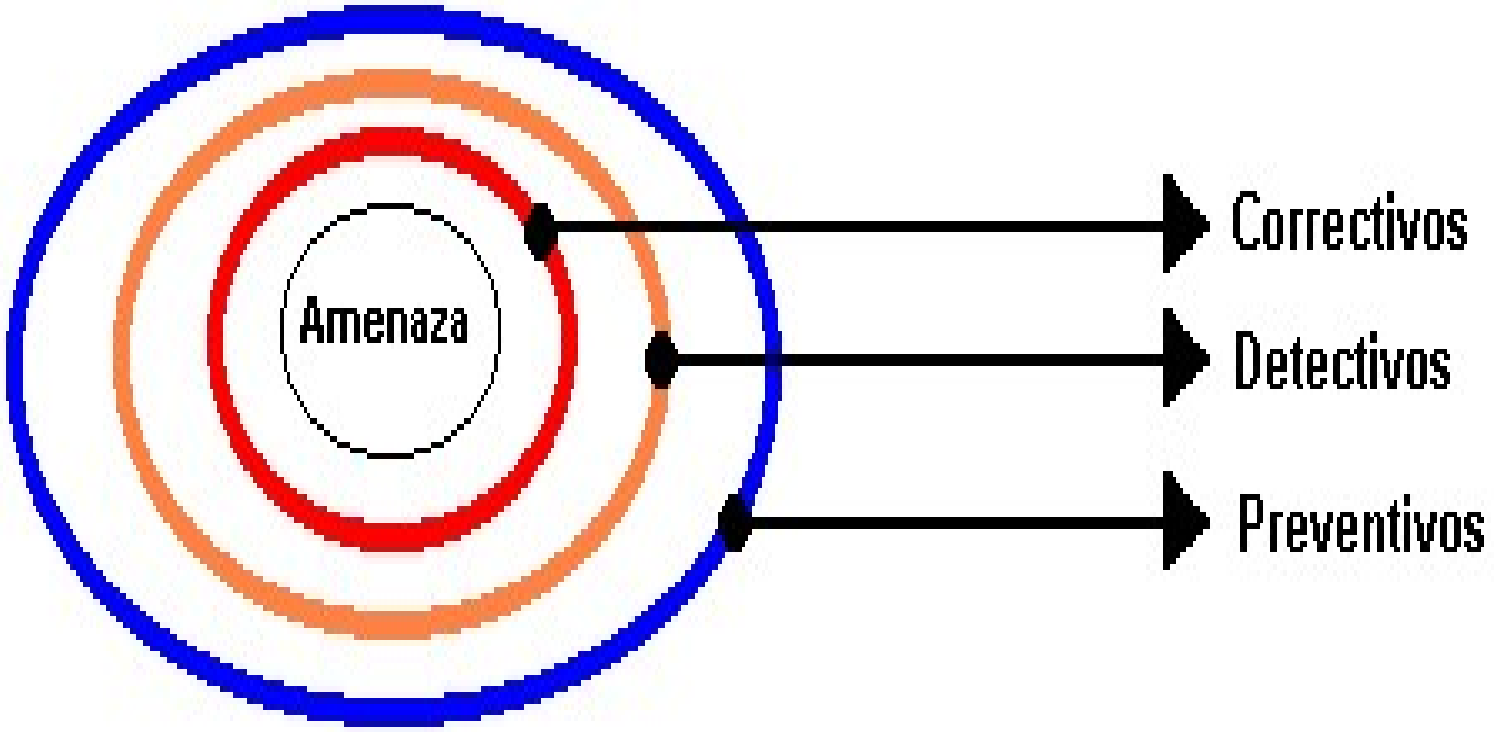
Valor Agregado que genera el Uso del Software a las Empresas.

El Software ControlRisk:

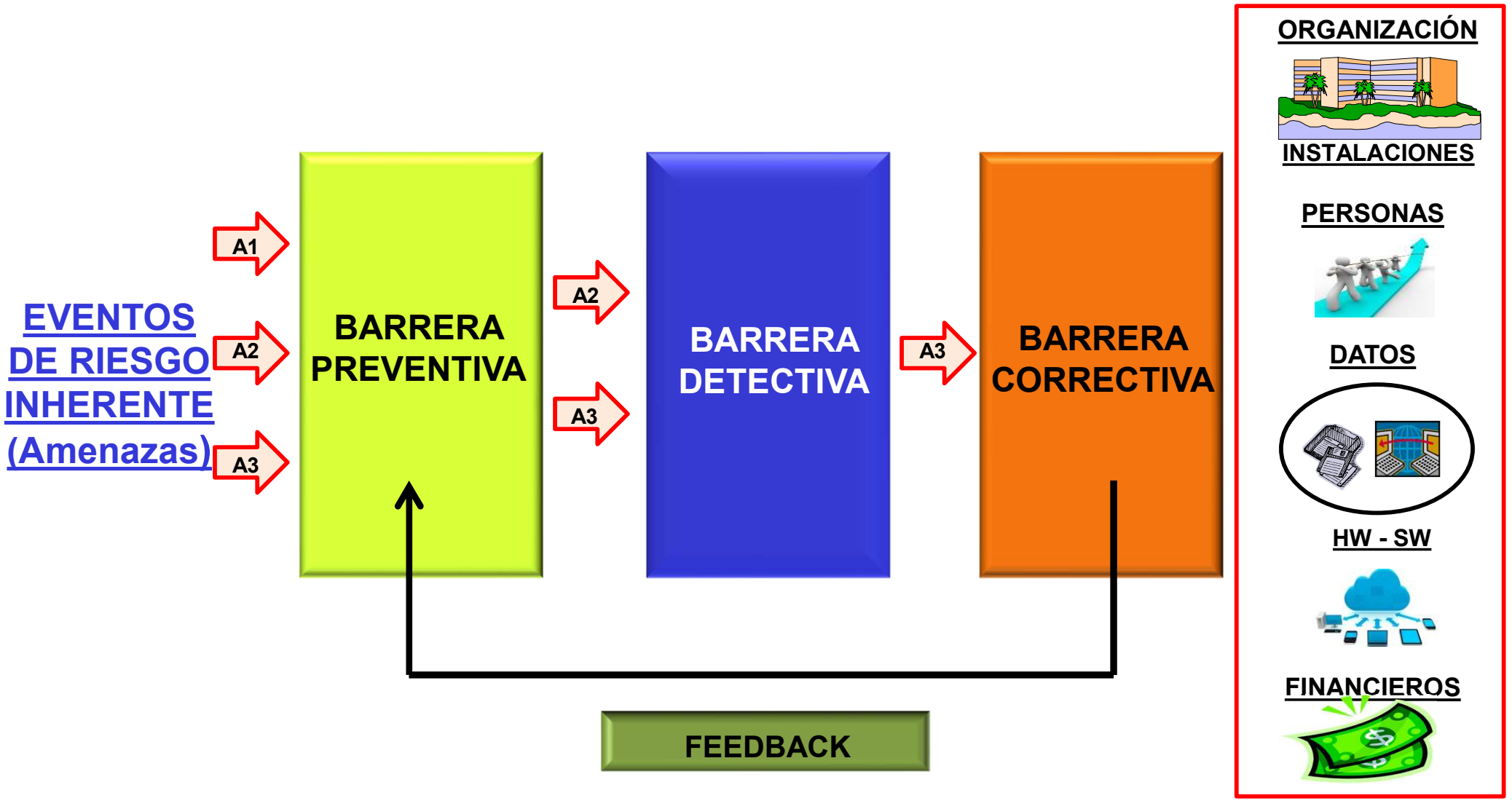
- ✓ Para evaluar la EFICACIA de los controles, a*plica y promueve la implantación del enfoque de los "**tres anillos de seguridad o barreras de Control" por riesgo y el uso de criterios de diseño de controles***

- ✓ *Para evaluar la Eficiencia de los Controles, aplica y promueve la evaluación del Costo / Beneficio de los Controles.*

El enfoque de los 3 Anillos de Control o líneas de Defensa, por Riesgo



Enfoque de los Tres Anillos de Control o de Seguridad o de Líneas de Defensa



El Software ControlRisk

Ejemplo – Aplicación del enfoque de los (3) Anillos de Seguridad o Barreras de Control por Riesgo.

Evento (Amenaza): Robo de dinero en cajero automático (ATM), por suplantación del propietario de la tarjeta.

1. Riesgo Potencial (Inherente): Riesgo antes de Controles. (evento) a la que se expone el Banco (usuario), de acuerdo con la naturaleza y modo de operación del cajero automático . En su evaluación no se tienen en cuenta los controles establecidos.

Evaluación Severidad: E - Extremo.

Acciones de Respuesta: Reducir (mitigar) el riesgo.

Controles:

- **Preventivos**: Uso de tarjeta y PIN. Políticas de seguridad para uso de cajero automático
- **Detectivos:** Validar que tarjeta y PIN coincidan. Informar desviación (mensaje) y bloquear
- **Correctivos:** Reemplazar la tarjeta bloqueada y asignar nuevo PIN.

2. Riesgo Residual: Riesgo después de Controles y de Tratamientos. Amenaza (Evento) no protegida o no cubierta por los controles establecidos. **Evaluación Severidad: B - Bajo** (Tolerable).

El proceso de Evaluación del Riesgo – Por evento de Riesgo Inherente

Cómo Evaluar Efectividad de los Controles Existentes, por Evento de Riesgo Inherente

3.1 Efectividad Individual de los Controles.

Provee once (11) criterios parametrizables para “Evaluar la Efectividad Individual” de los Controles establecidos, por cada evento de riesgo inherente. Estos incluyen criterios de diseño de los controles por riesgo inherente.

3.2 Efectividad Colectiva de los Controles.

Provee dos (2) alternativas para evaluar la Eficacia y Eficiencia de los controles que actúan sobre cada evento de riesgo inherente.

El proceso de Evaluación del Riesgo – Por evento de Riesgo Inherente

Paso 3.1: Evaluar Efectividad Individual de los Controles por Riesgo Inherente.

Criterio No	Descripción del Criterio	Puntaje Máximo Posible (PMP)
1	Tipo de Control	5
2	Clase de Control	5
3	Discrecionalidad del Control	5
4	Obligatoriedad legal	5
5	Evidencias de Aplicación del Control	5
6	Evidencias de Supervisión del Control	5
7	Documentación del Diseño del Control	5
8	Frecuencia de Ejecución del control	5
9	Oportunidad de la acción del control sobre el riesgo	5
10	Efecto del control sobre Probabilidad de ocurrencia o sobre impacto del Riesgo	5
11	Intencionalidad del Diseño del Control	5
12	Costos del Control (Adquisición, implantación, mantenimiento y operación).	5
	Puntaje Máximo Posible	60

El proceso de Evaluación del Riesgo – Eventos de Riesgos Inherentes

Paso 3.1: Evaluar Efectividad Individual de los Controles por Riesgo Inherente.

Provee once (11) criterios parametrizables para “Evaluar la Efectividad Individual de los Controles establecidos, por cada evento de riesgo inherente.

No Estrato	Puntaje obtenido por cada Control Desde – hasta	Efectividad Individual
1	Mayor que 48	5: Muy Alta
2	Mayor que 36 y menor que 48	4: Alta
3	Mayor que 24 y menor que 36	3: Moderada
4	Mayor que 12 y menor que 24	2: Baja
5	Mayor que 0 y menor que 12	1: Muy Baja

El proceso de Evaluación del Riesgo – Eventos de Riesgos Inherentes

Paso 3.2: Alternativa 1 Evaluar Efectividad Colectiva de los Controles Existentes, por Evento de Riesgo Inherente

Alternativa 1:

Criterios para evaluar "Efectividad Colectiva de los Controles" por cada Evento de Riesgo Inherente.

- ***Eficacia de los Controles.***
  - *Satisfacen al menos una vez, los 3 anillos de seguridad o barreras de control o líneas de defensa?.*
  - *El Promedio de Efectividad Individual de los Controles* ***es Aceptable****?.*
- ***Eficiencia de los Controles:*** *La relación Costo / Beneficio* ***es Razonable****.* Reduce la Pérdida Anual Estimada (PAE) mínimo en un 70% y el costo total de los controles no excede del 7.5% del valor total de los activos impactados por el riesgo.

Evaluación de Eficiencia de los controles por Riesgo

Según el costo / beneficio del conjunto de controles que actúan sobre cada riesgo. **Ejemplos:**

Items	Conceptos	Caso 1	Caso 2
1	Valor total de los Activos Impactados	100	100
2	Pérdida Anual Estimada (PAE) antes de controles	90	90
3	Severidad del Riesgo Inherente antes de controles	Extremo	Extremo
4	Costo de los Controles	6	20
5	% costo de los Controles, respecto al valor total de los activos impactados	6%	20%
6	Pérdida Anual Estimada (PAE) después de controles	10	30
7	Reducción de la PAE por efecto de los controles	80	60
8	Riesgo Residual después de Controles	Bajo	Alto
9	Reducción PAE - Costo de los Controles	74	40
10	% Reducción de la PAE	89%	67%
11	Ganancia o Utilidad de la inversión en controles, Costo / Beneficio	1333%	300%
		80 / 6 = 1333%. Por cada peso invertido en controles se ahorran $1333	60 /20 = 300% . Por cada peso invertido en controles se ahorran $300
12	**EFICIENCIA DE LOS CONTROLES**	**ALTA**	**BAJA**

Evaluación de Riesgos Inherentes –

Según la Efectividad de los Controles Establecidos

Niveles de Efectividad de los Controles	Criterios de Evaluación / Significado de la Efectividad de los Controles Establecidos por cada Evento de Riesgo Inherente (Amenaza)
5: Apropiada	Los controles establecidos son efectivos (eficaces y eficientes) para reducir los riesgos potenciales a nivel aceptable o tolerable de riesgo residual. Satisfacen los 3 anillos de seguridad y el nivel de automatización es aceptable o el costo beneficio es razonable.
4: Mejorable	Los controles satisfacen los 3 anillos de seguridad (preventivo, detectivo y correctivo), pero no son eficientes o tienen bajo nivel de automatización
3: Insuficiente	Los controles utilizados no satisfacen los tres anillos de seguridad. Se necesitan controles adicionales.
2: Deficiente	Los controles utilizados no satisfacen los tres anillos de seguridad y no son eficientes o tienen bajo nivel de automatización. Se necesitan controles adicionales
1: Muy Deficiente	No existen controles o los que se utilizan no sirven para controlar los riesgos potenciales.

El proceso de Evaluación del Riesgo – Eventos de Riesgos Inherentes

Paso 3.2: Alternativa 2 para Evaluar Efectividad Colectiva de los Controles Existentes, por Evento de Riesgo Inherente

Alternativa 2:

Criterios para evaluar "Efectividad Colectiva de los Controles" por cada Evento de Riesgo Inherente –

- ***Eficacia de los Controles.***
  - *Se utiliza un número plural de controles (más de un control)*
  - *El Promedio de Efectividad Individual de los Controles* ***es Aceptable****?.*

- ***Eficiencia de los Controles:*** *La relación Costo / Beneficio* ***es Razonable.*** Reduce la Pérdida Anual Estimada (PAE) mínimo en un 70% y el costo total de los controles no excede del 7.5% del valor total de los activos impactados por el riesgo. .

Evaluación de Eficiencia de los controles por Riesgo

Según el costo / beneficio del conjunto de controles que actúan sobre cada riesgo. **Ejemplos:**

Items	Conceptos	Caso 1	Caso 2
1	Valor total de los Activos Impactados	100	100
2	Pérdida Anual Estimada (PAE) antes de controles	90	90
3	Severidad del Riesgo Inherente antes de controles	Extremo	Extremo
4	Costo de los Controles	6	20
5	% costo de los Controles, respecto al valor total de los activos impactados	6%	20%
6	Pérdida Anual Estimada (PAE) después de controles	10	30
7	Reducción de la PAE por efecto de los controles	80	60
8	Riesgo Residual después de Controles	Bajo	Alto
9	Reducción PAE - Costo de los Controles	74	40
10	% Reducción de la PAE	89%	67%
11	Ganancia o Utilidad de la inversión en controles, Costo / Beneficio	1333%	300%
		80 / 6 = 1333%. Por cada peso invertido en controles se ahorran $1333	60 /20 = 300% . Por cada peso invertido en controles se ahorran $300
12	**EFICIENCIA DE LOS CONTROLES**	**ALTA**	**BAJA**

Valor Percibido que genera el Software para las Empresas.

El Software ControlRisk:

- ⇨ Mantiene actualizada la Base de Conocimientos con los elementos del SGR de todos los procesos y sistemas de la Organización – Repositorio Unico.

- ⇨ Habilita a los **dueños de los procesos,** para asumir el papel de responsables de "diseñar, mantener, monitorear y mejorar continuamente el SAIR".

- ⇨ Provee funcionalidades para que la **Gerencia de Riesgos de la Organización,** monitoree el funcionamiento del sistema de Administración de riesgos y ejecute seguimiento a los planes de tratamiento y las acciones de mejora.

Valor Agregado que genera el Software para las Empresas.

El Software ControlRisk:

- ⇨ Habilita a los **Auditores** para evaluar y verificar la Gestión de Riesgos de la Organización en su ambiente de operación normal.
- ⇨ Genera reportes exportables a varios formatos.
- ⇨ Utiliza métodos cualitativos y cuantitativos de evaluación de riesgos.
- ⇨ Deja Rastros de las actividades y cambios efectuados a la Base de Conocimientos de la Empresa.
- ⇨ Produce Manuales de Administración de riesgos en papel y formato electrónico.
- ⇨ Software Multicompañías.

Agenda

- Estados Actual y deseado de la Gestión de Riesgos Operacionales.
- ControlRisk Web: Qué es y para Qué Sirve?.
- Módulos Componentes del software CONTROLRISK Web.
- Características del Software CONTROLRISK que generan valor a las organizaciones.
- **Perfiles y Privilegios de Acceso al Software ControlRisk Web**
- Especificaciones Técnicas y Modalidades de Licenciamiento del Software ControlRisk.
- Que recibe el usuario por la Compra o Arrendamiento del software?
- Beneficios de Utilizar ControlRisk.
- Empresas Usuarias del software ControlRisk.

El software ControlRisk

Perfiles de Acceso establecidos para el SARO

Administradores de Riesgos

- ❑ Gerente de Riesgos .
- ❑ Gestor de Riesgos.
- ❑ Administrador RERO.
- ❑ Administrador BCP.
- ❑ Comité de Riesgos

Auditores.

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

Dueños de Proceso.

- ❑ Implantador Plan Acciones de Tratamiento
- ❑ Implantador Plan de Acciones de Mejora
- ❑ Implantador Acciones Correctivas (RERO).
- ❑ Administrador EGRs
- ❑ Auxiliar de RERO.
- ❑ Auto-Asegurador de Controles .
- ❑ Autoe-evaluador BCP.

¿A Quienes sirve el Software ControlRisk?

- ⇨ Gerentes de Riesgos / Directores de Planeación.
- ⇨ Jefes de Unidades de Riesgo Operativo (SARO).
- ⇨ Administradores del Sistema de Gestión de Seguridad de la Información (SGSI. ISO 27001).
- ⇨ Administradores de Seguridad en los Servicios de Tecnología de Información.
- ⇨ Auditores Internos / Revisores Fiscales / Auditores de Sistemas.
- ⇨ Departamentos de Control Interno.
- ⇨ Coordinadores de Gestión de Calidad y de otros sistemas de Gestión.

Agenda

- Estados Actual y deseado de la Gestión de Riesgos Operacionales.
- ControlRisk Web: Qué es y para Qué Sirve?.
- Módulos Componentes del software CONTROLRISK Web.
- Características del Software CONTROLRISK que generan valor a las organizaciones usuarias. .
- Perfiles de Acceso al Software ControlRisk
- **Especificaciones Técnicas y Modalidades de licenciamiento del Software ControlRisk.**
- Que recibe el usuario por la Compra o Arrendamiento del software?
- Beneficios de Utilizar ControlRisk.
- Empresas Usuarias del software ControlRisk.

Especificaciones del Software CONTROLRISK

- Herramienta de Desarrollo: .NET, Visual Studio.
- Sistema Operacional: Windows Server 2008 a 2012. Windows Vista, 7, 8 Y 10. Excepto las versiones Home.
- Motor de Base de datos: SQL Server.
- Memoria RAM: 4GB en servidor.
- Disco Duro: 16 GB.
- Navegadores: Internet Explorer 8.0 o superiores, Google Chrome, Firefox y Opera.

Modalidades de Licenciamiento del Software

Licencias del Software a Perpetuidad.

- Licencia de uso a perpetuidad, Multiempresa: Por equipo (servidor) y cantidad de usuarios concurrentes para tres perfiles: Administradores de Riesgos, Dueños de Procesos y Auditores.

Licencias por Suscripción Anual.

- Licencia de uso por suscripción anual, Multiempresa: Por equipo (servidor) y cantidad de usuarios concurrentes para tres perfiles: Administradores de Riesgos, Dueños de Procesos y Auditores.

Agenda

- Estados Actual y deseado de la Gestión de Riesgos Operacionales.
- ControlRisk Web: Qué es y para Qué Sirve?.
- Módulos Componentes del software CONTROLRISK Web.
- Características del Software CONTROLRISK que generan valor a las organizaciones.
- Perfiles y Privilegios de Acceso al Software.
- Especificaciones Técnicas y Modalidades de Licenciamiento del Software ControlRisk.
- **Productos / Entregables que recibe el usuario de ControlRisk Web**
- Beneficios de Utilizar ControlRisk.
- Empresas Usuarias del software ControlRisk.

Productos que recibe el Usuario de CONTROLRISK

Por Licencias del Software a Perpetuidad.

- ⇨ Licencia de uso a perpetuidad, multiempresa, por servidor y cantidad de usuarios concurrentes.
- ⇨ Software ejecutable (DVD).
- ⇨ Manual del Usuario del Software (E-book).
- ⇨ Bases de datos de conocimientos estándar.
- ⇨ Acceso a la Empresa ITF “Morraos de Colombia”, para consultar dos (2) Ejemplos de Gestión de Riesgos por proceso y realizar pruebas con fines de capacitación y entrenamiento .
- ⇨ Derecho a recibir soporte técnico y actualizaciones del software durante un año.

Productos que recibe el Usuario de CONTROLRISK

Por Licencias del Software por Suscripcion Anual.

- ⇨ Licencia de uso por suscripción anual, multiempresa, por equipo servidor y cantidad pactada de usuarios concurrentes.
- ⇨ Manual del Usuario del Software (E-book).
- ⇨ Acceso utilizar el Software ejecutable (DVD) como empresa licenciataria por arrendamiento.
- ⇨ Acceso a Bases de datos de conocimientos estándar.
- ⇨ Acceso a la Empresa ITF “Morraos de Colombia”, para consultar dos (2) Ejemplos de Gestión de Riesgos por proceso y realizar pruebas con fines de capacitación y entrenamiento .
- ⇨ Derecho a recibir soporte técnico y actualizaciones del software durante el año de suscripcion.

Productos que recibe el Usuario de CONTROLRISK

Servicios Complementarios ofertados por AUDISIS.

- Capacitación para la Operación y uso del Software.
- Consultoría - Acompañamiento para Integrar el Software al proceso de Gestión de Riesgos Empresariales. Por cada tema principal del software, consta de 3 sesiones:
  - **Sesión 1:** Capacitación para el uso de la metodología de GR y el software por parte del Consultor.
  - **Sesión 2:** Trabajo de Campo por parte de los Auditores, para aplicar conceptos impartidos en Sesión 1.
  - **Sesión 3:** Retroalimentación por el Consultor sobre trabajo de campo realizado por los auditores.
- Servicio Anual de Actualización y Soporte Técnico – Solo para licencias a Perpetuidad.

Agenda

- Estados Actual y deseado de la Gestión de Riesgos Operacionales.
- ControlRisk Web: Qué es y para Qué Sirve?.
- Módulos Componentes del software CONTROLRISK Web.
- Características del Software CONTROLRISK que generan valor a las organizaciones.
- Perfiles y Privilegios de Acceso al Software.
- Especificaciones Técnicas y Modalidades de Licenciamiento del Software ControlRisk.
- Productos / Entregables que recibe el usuario de ControlRisk Web
- **Beneficios de Utilizar ControlRisk.**
- Empresas Usuarias del software ControlRisk.

Beneficios de Utilizar CONTROLRISK

Beneficios Corporativos

ControlRisk establece un "Marco de trabajo" (Framework) para la Administración Integral de Riesgos Empresariales y el diseño de los controles internos de la organización, alineado con estándares y "Best Practices" universales de seguridad y control interno:

- COSO ERM.
- ISO 31000.
- ISO 27002, ISO 27001.
- ISO 20000.
- ISO 9001.
- COBIT.
- ITIL.
- DAFP -Guía Administración de
- Riesgos para Sector Publico

Beneficios Corporativos

ControlRisk:

- ⇨ Mejora y facilita el ejercicio del Gobierno Corporativo.
- ⇨ Ayuda a implantar la cultura de **Medición** de la Exposición a riesgos, de la protección existente y del riesgo residual.
- ⇨ Automatiza y estandariza el diseño, implementación y documentación de controles y procedimientos de administración de riesgos.

Beneficios para Propietarios de los Procesos (las áreas que manejan las Operaciones)

ControlRisk:

- Es una fuente permanente de aprendizaje organizacional sobre prevención de riesgos, controles y seguridad, en todas las áreas de la empresa que intervienen en el manejo de los procesos de negocio y de tecnología de información.
- Incrementa las características de seguridad, calidad y confiabilidad de los procesos de negocio y de sistemas de información.

Beneficios para el Departamento de Auditoría

ControlRisk:

- Facilita y hace más eficiente el trabajo de la auditoría: Se apoya en los resultados de la implantación de Sistemas de Gestión de Riesgos.
- Incrementa la productividad, eficiencia y valor agregado del trabajo de la auditoría.
- Reduce los costos de la auditoría a procesos y sistemas gestionados con ControlRisk.

Agenda

- Estados Actual y deseado de la Gestión de Riesgos Operacionales.
- ControlRisk Web: Qué es y para Qué Sirve?.
- Módulos Componentes del software CONTROLRISK Web.
- Características del Software CONTROLRISK que generan valor a las organizaciones.
- Perfiles y Privilegios de Acceso al Software
- Especificaciones Técnicas y Modalidades de Licenciamiento del Software ControlRisk.
- Productos / Entregables que recibe el usuario de ControlRisk Web
- Beneficios de Utilizar ControlRisk.
- **Empresas Usuarias del software ControlRisk**.

Usuarios de ControlRisk en Colombia y el Exterior

En Colombia.

Sector Industrial.

- Lafayette.
- Oleoducto Central de Colombia - OCENSA.
- AVESCO (Grupo Kokorico).

Cajas de Compensación Familiar.

- Comfenalco Tolima.
- COMFIAR: Caja de Compensación Familiar de Arauca.
- COMFAGUAJIRA: Caja de Compensación Familiar de la Guajira.
- Compensar.

Usuarios de CONTROLRISK en Colombia y el Exterior

En Colombia.

Sector Financiero.

- Cooperativa de Ahorro y Crédito – Progresa.
- Banco Popular.

Entidades de Sector Público.

- Terminal de Transporte de Bogotá.
- Contraloría General de la Republica de Colombia.
- Empresa Electrificadora de Santander – ESSA.
- Centrales Eléctricas de Nariño.
- Comisión Nacional de TV.
- Oleoducto Central de Colombia.

Usuarios de CONTROLRISK en Colombia y el Exterior

En Colombia.

Sector Educativo.

- Universidad Central de Bogotá.
- Universidad Militar Nueva Granada.
- Universidad la Gran Colombia.
- Universidad Autónoma de Colombia.
- Universidad Pedagógica y Tecnológica de Colombia.
- Universidad Santo Tomás - Bucaramanga.
- Universidad Católica de Colombia.
- Universidad Santo Tomás – Bucaramanga.

Usuarios de CONTROLRISK en Colombia y el Exterior

En el Exterior.

- Universidad UPEU Perú.
- Contraloría General del Perú.
- Banco Central del Ecuador.

Gracias por su atención.

Hasta Pronto !

Para conocer el software ingrese a www.softwareaudisis.com