Software de Administración de Riesgos para Procesos y Tecnología de Información.

Versión 7.5 - Año 2022

Agenda

- Estados Actual y deseable de la Gestión Integral de Riesgos de Empresariales.
- ControlRisk: Qué es y para Qué Sirve?.
- La Norma ISO 31000: 2018
- Menú Principal del Software
- Resumen funcionalidades de los Módulos de ControlRisk
- Especificaciones Técnicas del Software ControlRisk.
- Que recibe el Cliente por la Compra o Suscripción Anual /Arrendamiento del software?
- Características del Software CONTROLRISK que generan valor a las organizaciones -
- Beneficios de Utilizar ControlRisk.
- Empresas Usuarias del software ControlRisk.

El Software ControlRisk

Estados Actual y deseable de la Gestión de Riesgos en las Empresas

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 Deseable-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.

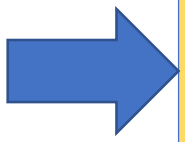
3) Utilizar ***Enfoque Proactivo y Preventivo de los Controles*** **–** Todos los controles deben actuar antes de la ocurrencia de los riesgos.

El Software ControlRisk

Estados Actual y deseable de la Gestión de Riesgos en las Empresas

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 mejoramiento y Acciones Correctivas.

El software CONTROLRISK

Qué es y para que sirve?

"CONTROLRISK es un software en tecnología Web que provee funcionalidades *para implantar, documentar y actualización continua de la Gestión de Riesgos de la Empresa*.

Asiste a la Gerencia de Riesgos y los Dueños de Procesos para:

1) **Implantar** la Gestión de Riesgos en los procesos de la cadena de valor, los procesos de la infraestructura de TIC, los Sistemas de Información automatizados (aplicaciones de computador ó módulos de ERPs) y el Sistema de Gestión de Seguridad de la Información (ISO 27001).
2) **Construir y actualizar el Perfil de Riesgos Consolidado de la Empresa.**
3) Crear y mantener actualizada ***la Base de Datos de Eventos de Riesgo Ocurridos en la organización.***
4) **Monitorear el funcionamiento del Plan de Continuidad del Negocio de la Organización.**
5) **Auditar** la Gestión de Riesgos.

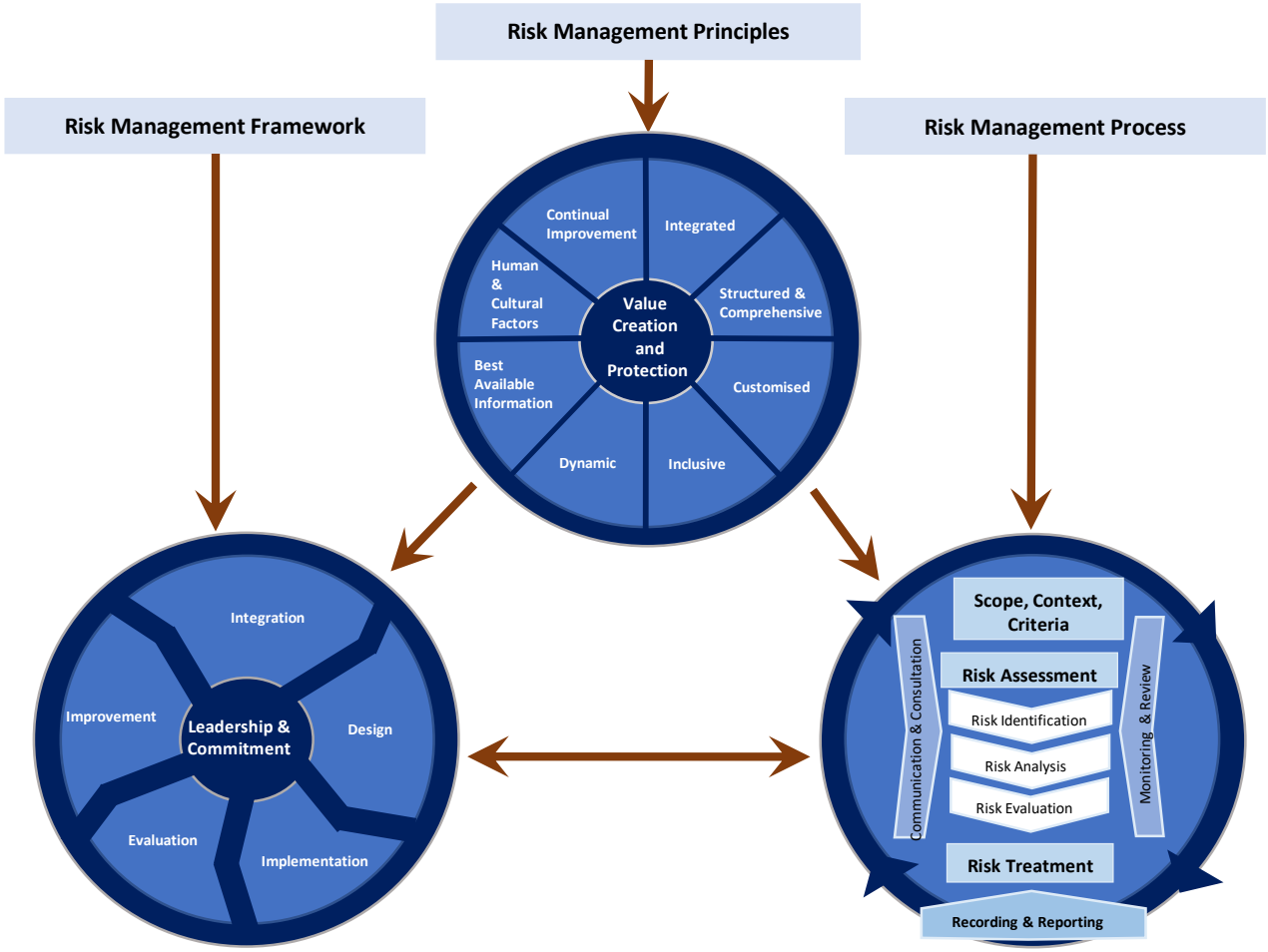
El software CONTROLRISK

Qué es y para que sirve?

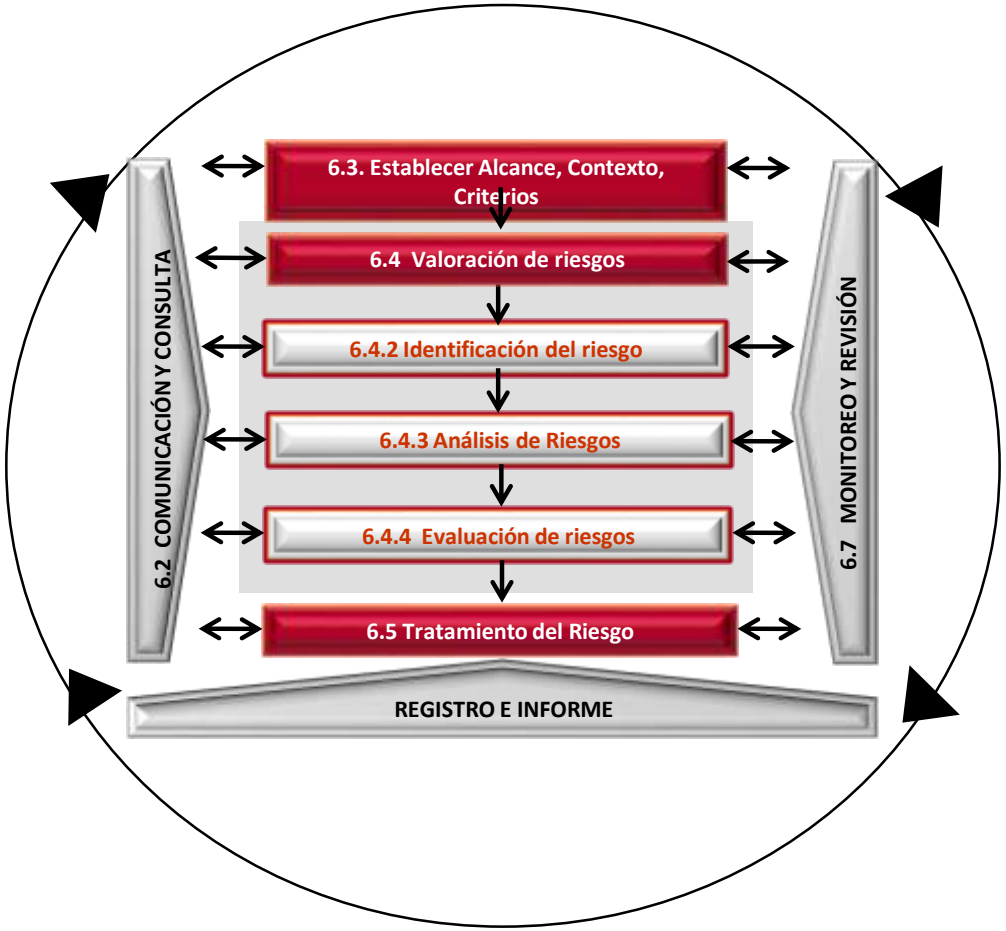
CONTRORISK WEB está alineado con estándares internacionales y nacionales vigentes de Gestión de Riesgos, Control Interno, Seguridad y Calidad

- **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: 2013 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 020 de 2020 SFC, CE025 de 2020 de Supersolidaria

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



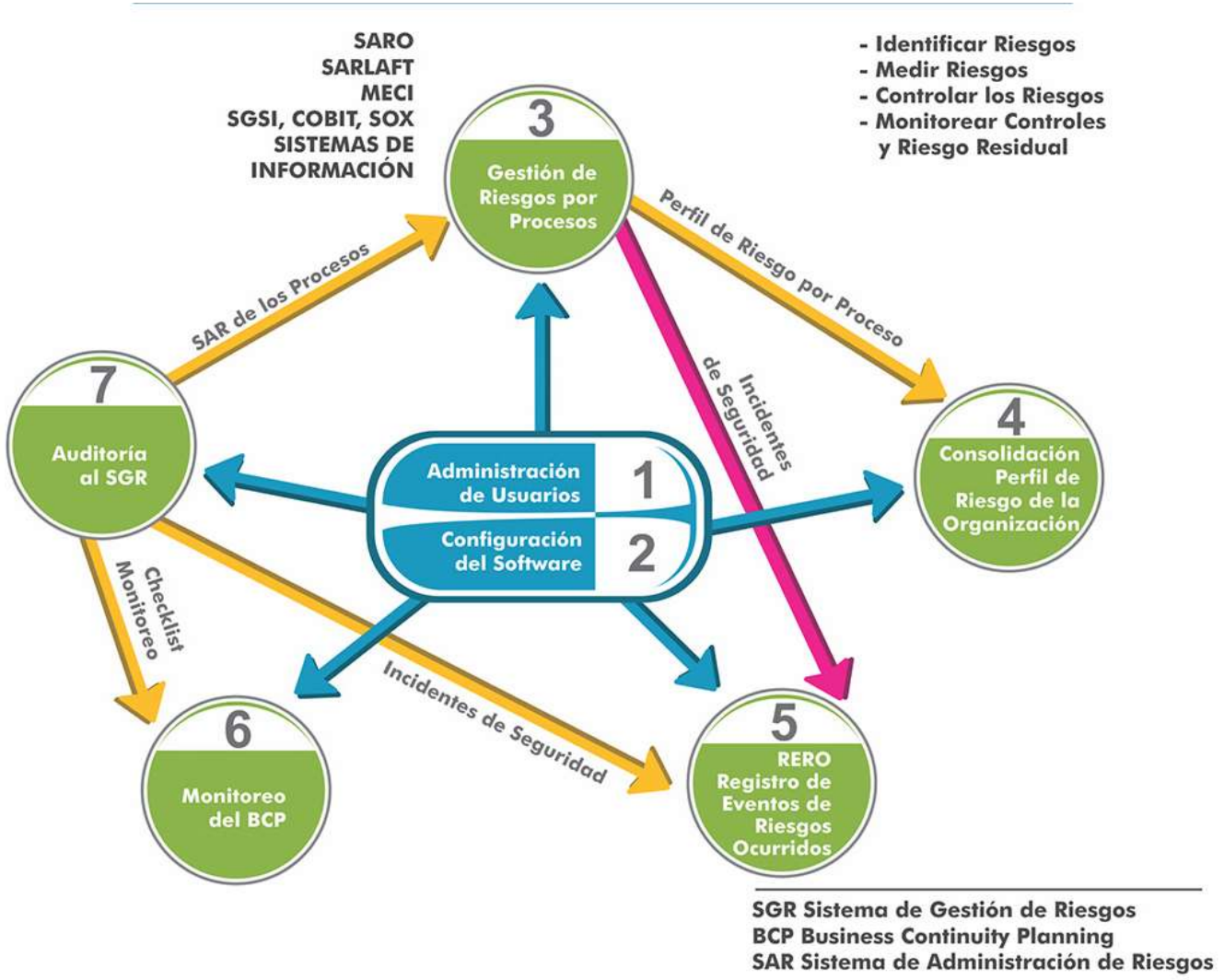
ISO 31000: 2018 - Elementos del Proceso de Gestión del Riesgo



El software CONTROLRISK

Menú Principal del Software ControlRisk Web

Módulos de CONTROLRISK



ControlRisk Web

Modulo 1: 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 por Subsistema:

a) **Administradores de Riesgos** de la Empresa con derechos de acceso a todas las funcionalidades de un Subsistema.

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.
- Analista de Riesgos.
- Auto-evaluador – Monitoreo de riesgos, CSA.
- Administrador RERO.
- Administrador BCP.
- Auto-evaluador del BCP.

Dueños de Procesos

- Administrador de EGR (Estudio de Gestión de Riesgos), Auxiliar RERO, Implantadores de Tratamientos, Mejoramientos y Acciones Correctivas.
- Auxiliar de RERO.

Auditores.

- Administrador de Auditoría.
- Auditor.

ControlRisk Web

Módulo 2: Configuración del Software

Módulo 2:

Configuración del Software.

CONTROLRISK provee funcionalidades para:

- Consultar / modificar tablas Base de Conocimientos de Gestión de Riesgos y Controles con información privada de la Empresa.
- Seleccionar Criterios de Evaluación Individual y colectiva de controles por riesgo.
- Cargar tablas de Frecuencia Anual de Ocurrencia y tipos de impacto de los riesgos, parámetros de monitoreo por riesgo.
- Configurar correo corporativo de la *Unidad de Riesgos y dueños de procesos para envío automático de mensajes de recordatorio por Correo electrónico sobre Acciones de Tratamiento y Acciones de Mejoramiento y Acciones Correctivas.*

El Software CONTROLRISK

MODULO 3: Implantar la Gestión de Riesgo por Proceso o Sistema (Cont.)

- Crear y comprender contexto EGR (Proceso o Sistema)
- Identificar y Analizar Eventos de Riesgo por Categoría de Riesgo
- Elaborar el Cubo de Riesgos del EGR
- Evaluar Riesgos – Diagnostico y Diseño Tratamientos

Tipos de Estudios de Gestión de Riesgos (EGRs) que puede realizar

- A procesos de la Cadena de Valor (Mapa de Riesgos Modelo de Operación de la Empresa)
- A procesos de la Infraestructura de TIC de la Empresa.
- A Aplicaciones de Computador o Módulo de ERPs
- Al Sistema de Gestión de Seguridad de la Informacion (ISO 27001).

El Software CONTROLRISK

MODULO 3: Implantar la Gestión de Riesgo por Proceso o Sistema (Cont.)

- Analizar Costo / Beneficio de los Controles
- Asignar Responsables de ejecutar y Supervisar los Controles
- Monitorear los riesgos y los controles
- Generar Manual de Gestión de Riesgos del EGR

Tipos de Estudios de Gestión de Riesgos (EGRs) que puede realizar

- A procesos de la Cadena de Valor (Mapa de Riesgos Modelo de Operación de la Empresa)
- A procesos de la Infraestructura de TIC de la Empresa.
- A Aplicaciones de Computador o Módulo de ERPs
- Al Sistema de Gestión de Seguridad de la Informacion (ISO 27001).

El Software CONTROLRISK

Módulo 3: Implantar la Gestión de Riesgos por EGR

Metodología para Implantar la Gestión de Riesgos (GR).

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

ETAPAS DE LA METODOLOGIA

- **Etapa 1:** Definir el Contexto de Riesgos del Proceso.
- **Etapa 2:** Identificar, analizar y documentar los riesgos que podrían presentarse.
- **Etapa 3:** Elaborar Cubo de Riesgos del Proceso.
- **Etapa 4: Evaluación de Riesgos /** Diagnóstico sobre 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

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

(1) En los procesos y sistemas de la organización

ControlRisk Web

Modulo 3: Implantar la Gestión de Riesgos por EGR

El ciclo PHVA del proceso de implantación de la gestión de Riesgos

Por cada EGR

- **P: Planear.** Aplicar procedimientos para Identificar, analizar, evaluar, diseñar tratamientos y monitorear los riesgos inherentes (framework de la Gestión de Riesgos).
- **H: Hacer.** Implementar los procedimientos de gestión de riesgos y el plan de tratamientos.
- **V: Verificar.** Poner en Operación y 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.

Modulo 3: Implantar la Gestión de Riesgos por EGR

Etapa 1:

Comprender el contexto del EGR

Caracterizar el EGR

Es necesario conocer contexto del EGR (proceso o sistema) como requisito para identificar, analizar, controlar y monitorear los riesgos que pueden presentarse.

- Objetivos que satisface
- Actividades del Proceso (ciclo PHVA)
- Entradas y proveedores de las entradas.
- Salidas y destinatario de las salidas.
- Requisitos que debe satisfacer: legales, reglamentarios, de la industria, internos, de calidad, de los clientes.
- Roles de las Areas Organizacionales y terceros que intervienen en el proceso o sistema.

Modulo 3: Implantar la Gestión de Riesgos por EGR

Etapa 1:

Comprender el contexto del EGR (Cont.)

Caracterizar el EGR (Cont)

Es necesario conocer el contexto del EGR (proceso o sistema) como requisito para identificar analizar, controlar y monitorear los riesgos que pueden presentarse.

- Activos / Recursos que se utilizan en el EGR
- Organización del proceso (líder, cargos, etc.
- Interfaces de Entrada con otros procesos.
- Interfaces de salida con otros procesos
- Rol de las Areas en las Actividades del Proceso.
- Indicadores de Gestión.
- Otros

ControlRisk Web

Modulo 3: Implantar la Gestión de Riesgos por EGR

Etapa 2:

Identificar y Analizar los Riesgos del EGR que pueden presentarse

Funcionalidades de CONTROLRISK

1. Identificar clases de riesgo que pueden presentarse en el EGR.
2. Identificar clases de Riesgo CRITICAS / Priorizar
3. Identificar Actividades del proceso en las que pueden presentarse las clases de riesgo criticas.
4. Identificar Eventos de Riesgo inherente que pueden presentarse por Clase de Riesgo Critica en las actividades del proceso.
5. Realizar Análisis Cuantitativo de los eventos de riesgo.

Modulo 3: Implantar la Gestión de Riesgos por EGR

Etapa 2 – Paso 1 :

Identificar Clases de Riesgo aplicables a la Empresa

IDENTIFICAR CLASES DE RIESGO APLICABLES

Del Sistema de Administración de Riesgo Operacional (SARO) - 7 clases de riesgos.

- Fraude Interno
- Fraude Externo.
- Daños a Activos Físicos
- Fallas en Atención a los Clientes.
- Fallas en Relaciones Laborales.
- Fallas Tecnológicas.
- Errores en Diseño y Ejecución del Proceso

Modulo 3: Implantar la Gestión de Riesgos por EGR

Etapa 2 – Paso 1 :

Identificar Clases de Riesgo aplicables a la Empresa

IDENTIFICAR CLASES DE RIESGO APLICABLES

Del Sistema de Administración de Riesgo de lavados de Activos y Financiación del Terrorismo (SARLAFT – SAGRILAFT) – 4 clases de riesgo

- Riesgo de Contagio
- Riesgo Reputacional.
- Riesgo Operativo (las 7 clases de SARO)
- Riesgo Legal

Modulo 3: Implantar la Gestión de Riesgos por EGR

Etapa 2 – Paso 1 :

Identificar Clases de Riesgo aplicables a la Empresa

IDENTIFICAR CLASES DE RIESGO APLICABLES (cont.)

Para Entidades del Sector Público (Modelo del Departamento Administrativo de la Función Publica) - 6 clases de riesgo

- Estratégico.
- Financiero.
- Operativo (las 7 del SARO)
- Fallas Tecnológicas.
- Incumplimiento Normas legales
- De Corrupción.

Modulo 3: Implantar la Gestión de Riesgos por EGR

Etapa 2 – Paso 1 :

Identificar Clases de Riesgo aplicables a la Empresa

IDENTIFICAR CLASES DE RIESGO APLICABLES (Cont.)

OTRAS:

- Pérdida de Ingresos.
- Gastos Excesivos
- Desventaja Competitiva
- Encubrimiento de Pasivos.
- Otras.

Modulo 3: Implantar la Gestión de Riesgos por EGR

Etapa 2 – Paso 4 :

Identificar Eventos de Riesgo inherente que pueden presentarse por Clase de Riesgo Critica en las actividades del proceso.

Identificar Eventos de Riesgo Inherente por Clases de Riesgo

- Apoyarse en la Base de Datos de ControlRisk - Amenazas (riesgos inherentes) por clases de riesgo
- El software genera Reporte de Amenazas / eventos de riesgo inherente elegibles, por clases de Riesgo. De estas, seleccione las que apliquen al EGR
- Adicionar Amenazas que no estén en Base de Datos. Antes realizar búsqueda de Amenazas por palabra clave o código de identificación.

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 y ambiente de operacion. Es intrínseco a los activos del que intervienen en el proceso. Este riesgo no puede ser evitado, pero si puede ser mitigado. Su SEVERIDAD se evalúa sin tener en cuenta los controles establecidos en la Entidad.

- **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 (Potencial): 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).

Modulo 3: Implantar la Gestión de Riesgos por EGR

Etapa 2 – Paso 5 :

Analizar riesgos inherentes identificados

Entregables del Análisis por Evento de Riesgo.

1. *Valuación de Activos impactados.*
2. *Vulnerabilidades.*
3. *Agentes Generadores.*
4. *Exposición del Evento de Riesgo.*
   - *Pérdida por ocurrencia (PS: Pérdida Simple)*
   - *Factor de Exposición por ocurrencia.*
   - *Frecuencia Anual de y Probabilidad de Ocurrencia*
   - *Pérdida Anual Estimada (PAE)*
   - *Calificación Impacto por Ocurrencia.*
5. *Consecuencias.*
6. *Controles Utilizados por evento de riesgo.-*

Modulo 3: Implantar la Gestión de Riesgos por EGR

Etapa 2 – Paso 5:

Analizar riesgos inherentes identificados

Entregables del Análisis de Riesgos consolidados por EGR

1. *Mapas de Riesgos / Matrices de Riesgos del EGR.*
   - *Por Clases de Riesgo.*
   - *Por Areas y Terceros que intervienen en el EGR.*
   - *Por actividades del EGR (Escenarios de Riesgo)*
   - *General del EGR.*
2. *Acciones de Respuesta a Riesgos / opciones manejo de riesgos*
3. *Vulnerabilidades del EGR por Evento de Riesgo.*
4. *Agentes Generadores del EGR por eventos de Riesgo*
5. *Consecuencias por evento de Riesgo.*
6. *Estadísticas de Eventos de Riesgo por clases de Riesgo, áreas organizacionales y Actividades del Proceso*

Modulo 3: Implantar la Gestión de Riesgos por EGR

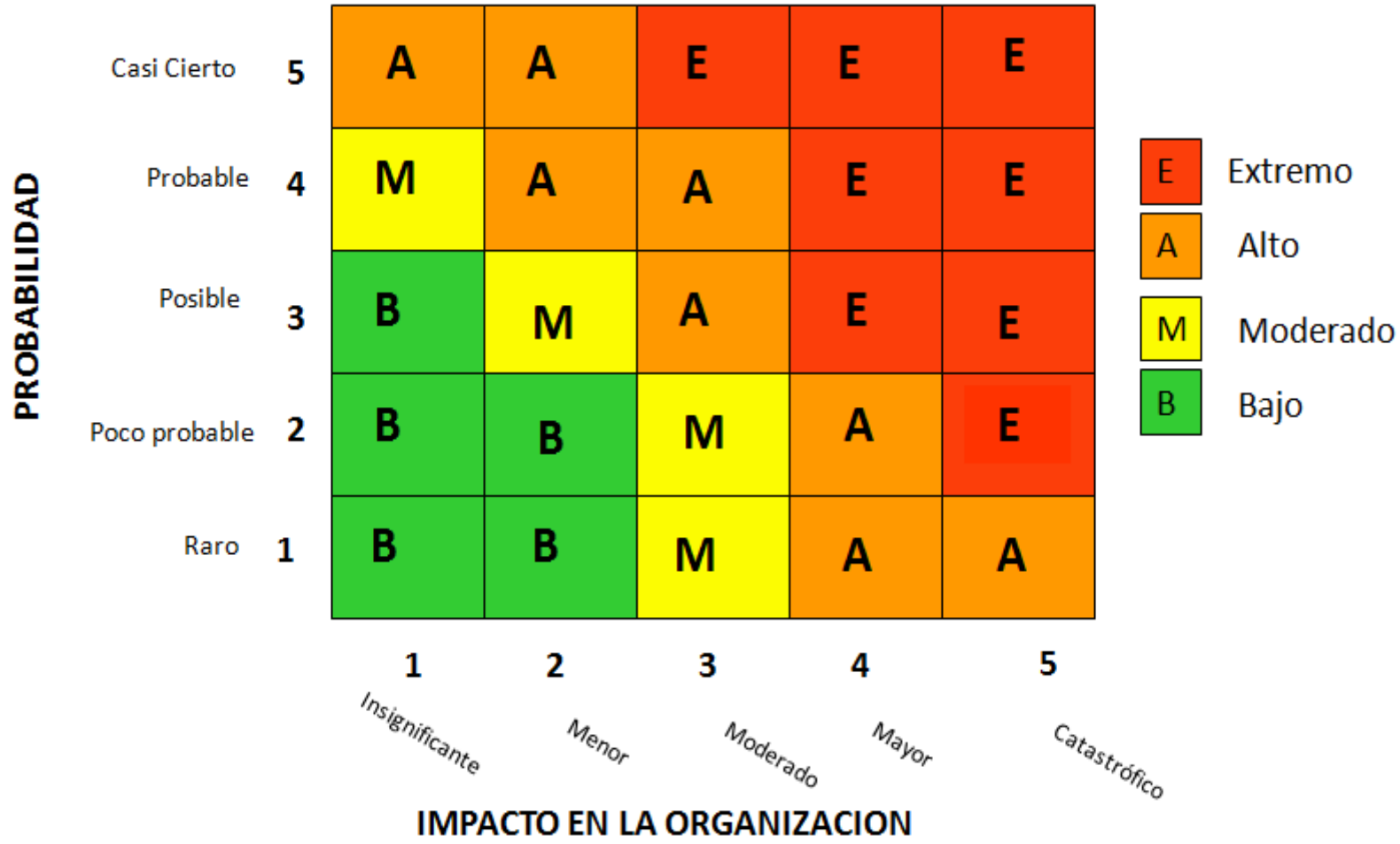
Etapa 2 – Paso 5:

Analizar riesgos inherentes identificados

Entregables del Análisis de Riesgos consolidados por EGR

1. *Mapas de Riesgos / Matrices de Riesgos del EGR.*
   - *Por Clases de Riesgo.*
   - *Por Areas y Terceros que intervienen en el EGR.*
   - *Por actividades del EGR (Escenarios de Riesgo)*
   - *General del EGR.*
2. *Vulnerabilidades del EGR por Evento de Riesgo.*
3. *Agentes Generadores del EGR por eventos de Riesgo*
4. *Consecuencias por evento de Riesgo.*

Mapa de Riesgos Inherentes -



Matriz de Acciones de Respuesta a Riesgos

PROBABILIDAD	1: Insignificante	2: Menor	3: Moderado	4: Severo	5: Catastrófico
5: Casi Cierto	**Zona de Riesgo Alta.** Reducir, transferir, Evitar	**Zona de Riesgo Alta.** Reducir, transferir, Evitar	**Zona de Riesgo Extremo** . Evitar, transferir, mitigar	**Zona de Riesgo Extremo** . Evitar, transferir, mitigar	**Zona de Riesgo Extremo.** Evitar, Mitigar, tranferir
4: Probable	**Zona de Riesgo Moderada.** Asumir, Reducir	**Zona de riesgo Alta.** Reducir, transferir, Evitar	**Zona de riesgo Alta.**, Reducir, transferir, Evitar	**Zona de Riesgo Extremo** . Evitar, transferir, mitigar	**Zona de Riesgo Extremo**. Evitar, Mitigar, tranferir
3: Posible	**Zona de Riesgo Baja**. Asumir,o aceptar el Riesgo	**Zona de Riesgo Moderada.** Reducir	**Zona de riesgo Alta.** Reducir, transferir, Evitar	**Zona de Riesgo Extremo** . Evitar, transferir, mitigar	**Zona de Riesgo Extremo**. Evitar, Mitigar, tranferir
2: Poco Probable	**Zona de Riesgo Baja**. Asumir o aceptar el Riesgo	**Zona de Riesgo Baja**. Aceptar, o aceptar el Riesgo	**Zona de Riesgo Moderada.** Reducir, Asumir	**Zona de riesgo Alta.** Reducir, transferir, evitar	**Zona de Riesgo Extremo**. Evitar, Mitigar, tranferir
1: Raro	**Zona de Riesgo Baja**. . Asumir ó Aceptar el Riesgo	**Zona de Riesgo Baja**. . Asumir ó Aceptar el Riesgo	**Zona de Riesgo Moderada.** Reducir, Asumir	**Zona de riesgo Alta**. Reducir, transferir, evitar	**Zona de riesgo Alta.** Reducir, transferir, evitar

IMPACTO

Modulo 3: Implantar la Gestión de Riesgos por EGR

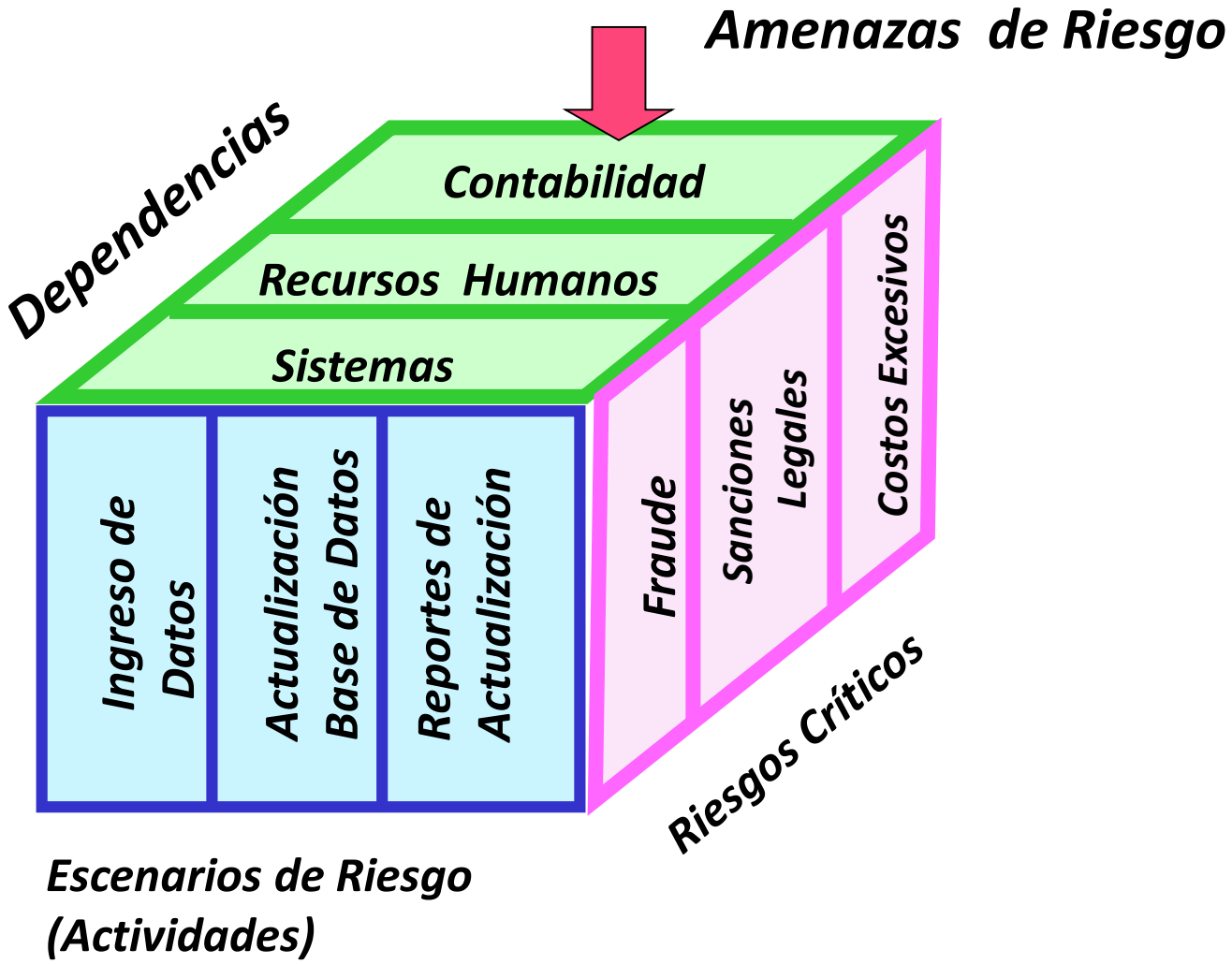
Etapa 3.

Elaborar Cubo de Riesgos del EGRs

Entregables de la Etapa

1. Dos Matrices con documentación ocurrencia de las Clases de Riesgo
   - Clases de Riesgo Vs. Escenarios de Riesgo (actividades) del EGR.
   - Clases de Riesgo Vs. Areas Organizacionales que intervienen en el EGR.
2. Una Matriz de Roles de las Areas organizacionales en las actividades del proceso.
3. Definición de objetivos de control por Escenario de riesgo y eventos de Riesgo.

Cubo de Riesgos del Proceso o Sistema de Información



ControlRisk Web

Modulo 3: Implantar la Gestión de Riesgos por EGR

Etapa 4:

Evaluación de Riesgos -

Diagnóstico y Tratamiento de Riesgos del EGR

Funcionalidades de CONTROLRISK

1. Generar Checklist de Controles que se necesitan por cada evento de riesgo y reporte para revisión dueños de proceso.
2. Identificar controles utilizados por evento de Riesgo sobre el checklist de controles que se necesitan.
3. Evaluar Efectividad de los controles por Evento de Riesgo – Individual y colectiva.
4. Identificar Eventos de Riesgo que requieren tratamientos.
5. Diseñar Planes de tratamiento por eventos de riesgo con debilidades de control.
6. Asignar responsables de implantar y notificarlos con mensajes automáticos del sistema..
7. Implantar Tratamientos y recalcular evaluación individual y colectiva de los eventos de riesgo.

Modulo 3: Implantar la Gestión de Riesgos por EGR

Etapa 4:

Evaluación de Riesgos -

Diagnóstico y Tratamiento de Riesgos del EGR

Entregables de la Etapa

1. Reporte de Protección Ofrecida / efectividad de los controles utilizados por Evento de Riesgo.
2. Mapas de Riesgo Residual por los siguientes conceptos:
   a. Por Escenarios de Riesgo.
   b. Por Clases de Riesgo.
   c. Por Areas Organizacionales
   d. General del EGR.
3. Diseño Plan de Tratamiento de Riesgos.
4. Asignación de Responsables y plazos para Implantar los tratamientos

Modulo 3: Implantar la Gestión de Riesgos por EGR

Etapa 4:

Evaluación de Riesgos -

Diagnóstico y Tratamiento de Riesgos del EGR

Entregables de la Etapa (Cont.)

5. Reporte de Controles Establecidos por Objetivo de Control.
6. Reporte de Controles Establecidos por vulnerabilidad y evento de riesgo.
7. Reporte de Controles establecidos para mitigar Consecuencias de ocurrencia por evento de riesgo.
8. Reporte de Controles Establecidos por Agentes de Riesgo.
9. Estadísticas de controles por tipo (preventivos, detectivos y correctivos).
10. Estadísticas de controles por clase (manuales y automáticos).
11. Estadísticas de controles por discrecionalidad (Discrecionales y No Discrecionales))

Modulo 3: Implantar la Gestión de Riesgos por EGR

Etapa 4:

Evaluación de Riesgos -

Diagnóstico y Tratamiento de Riesgos del EGR

Criterios para Evaluar Efectividad Colectiva de los Controles

Alternativa 1.

Criterios de Eficacia

- *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****?.*

Criterio de Eficiencia

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

Modulo 3: Implantar la Gestión de Riesgos por EGR

Etapa 4:

Evaluación de Riesgos -

Diagnóstico y Tratamiento de Riesgos del EGR

Criterios para Evaluar Efectividad Colectiva de los Controles

Alternativa 2.

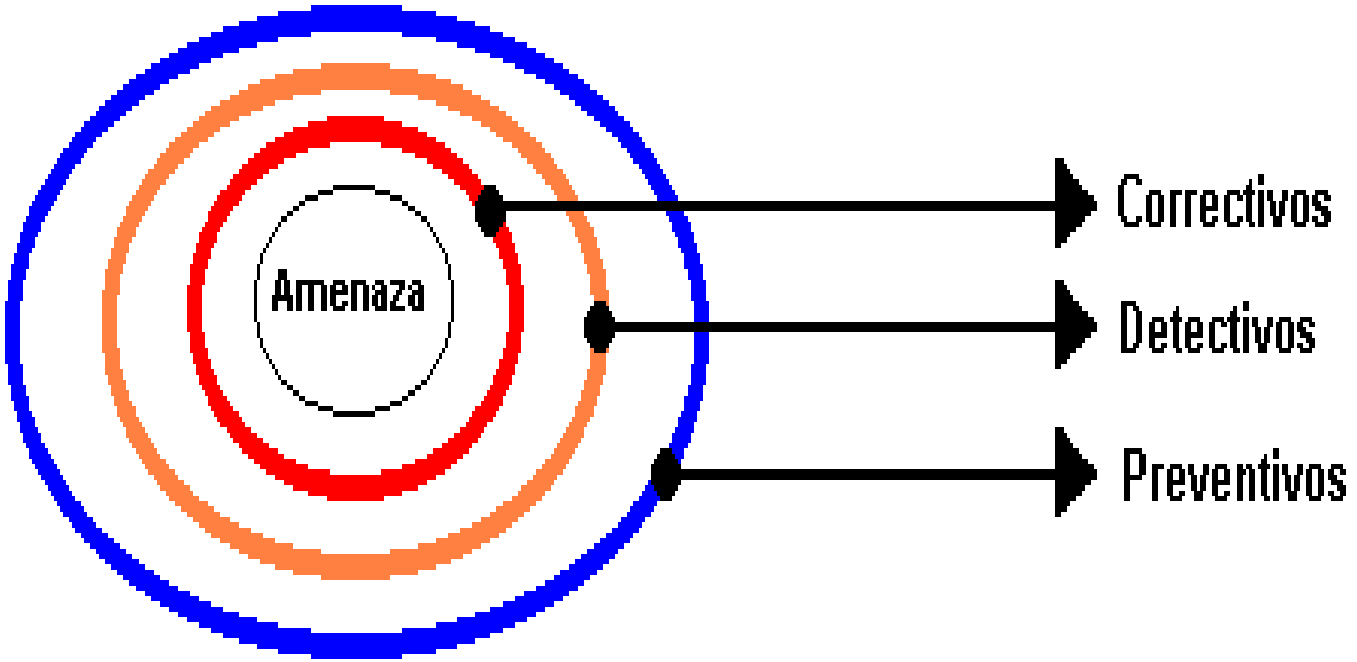
Criterios de Eficacia

- *La cantidad de controles es mayor que 1 (número plural de controles).*
- *El Promedio de Efectividad Individual de los Controles* ***es Aceptable****?.*

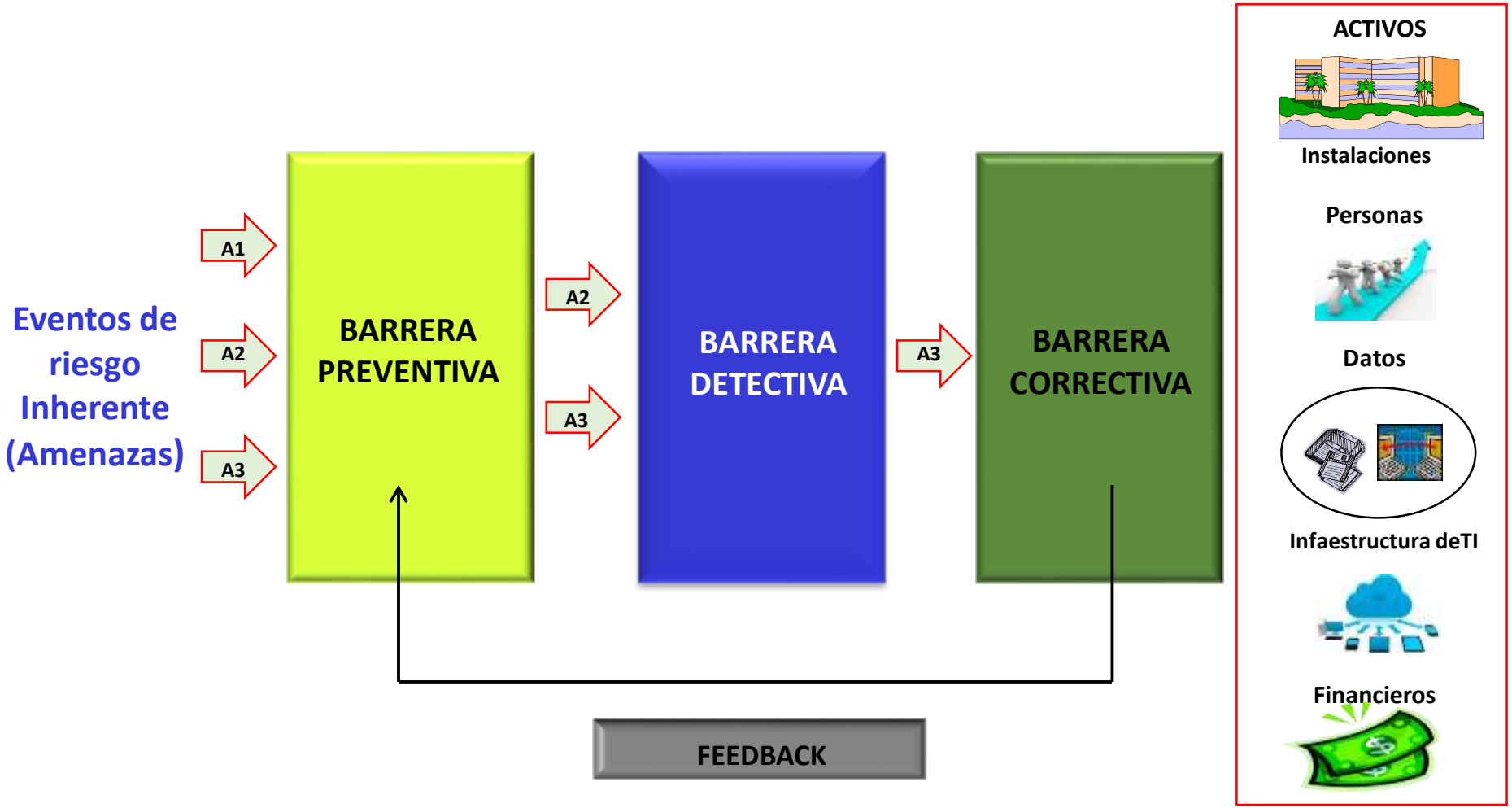
Criterio de Eficiencia

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

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



Evaluación de Riesgos Inherentes –

Calificaciones Efectividad de los Controles Establecidos por Evento de Riesgo

Efectividad de los Controles por Evento de Riesgo	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.

Evaluación de Riesgos Inherentes -

Después de Controles y Antes de Tratamientos

Mapa de Riesgos Residuales

Riesgo Inherente	1: Muy Deficiente	2: Deficiente	3: Insuficiente	4: Mejorable	5: Apropiada
4: Extremo (E)	Extremo	Extremo	Alto.	Moderado.	Bajo
3: Alto (A)	Alto	Alto	Alto.	Moderado.	Bajo
2: Moderado (M)	Moderado.	Moderado.	Moderado.	Moderado.	Bajo
1: Bajo (B)	Bajo	Bajo	Bajo	Bajo	Bajo

Efectividad Colectiva de Controles Establecidos / Protección Existente

ControlRisk Web

Módulo 5: BD de Eventos de Riesgo Ocurridos

Módulo 5.

Creación y Mantenimiento Base de Datos 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 y evaluar Eficacia de la Gestión de Riesgos Empresariales.
- **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.

Módulo 6: Monitorear el BCP

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.
- Mide el % de cumplimiento de los procedimientos del BCP.
- Generación Indicadores de Cumplimiento / preparación para trabajar en modo contingencia.
- Genera Reportes del Monitoreo.

ControlRisk Web

Módulo 7: Auditoría a la Gestión de Riesgos

Módulo 7.

Auditoría al Sistema de Gestión de Riesgos de la Organización.

Funcionalidades de ControRisk

- **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

Módulo 8: Seguimiento a Implantación de PM

Módulo 8.

Seguimiento a Implantación de Planes de Mejoramiento de la Gestión de Riesgos

- **Acciones de Tratamiento de Riesgos por Procesos:** 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

- ControlRisk: Qué es y para qué sirve?.
- **Especificaciones Técnicas del Software ControlRisk.**
- Descripción Resumida Módulos Componentes de ControlRisk.
- Características del Software ControlRisk que generan valor para las organizaciones.
- Beneficios de Utilizar ControlRisk.
- Usuarios del software ControlRisk.

Especificaciones Técnicas 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.

Elementos que recibe el Cliente de CONTROLRISK

Por Licencias del Software a Perpetuidad.

- ⇨ Licencia de uso a perpetuidad, multiempresa, por servidor y cantidad de usuarios concurrentes.
- ⇨ Software ejecutable
- ⇨ Manual del Usuario del Software (PDF).
- ⇨ 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.

Elementos que recibe el Cliente de CONTROLRISK

Por Licencias del Software por Suscripción 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.

Elementos que recibe el Cliente de CONTROLRISK

Servicios Complementarios por Subsistema - Opcionales.

- ⇨ 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.

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.

Beneficios Corporativos

ControlRisk:

- ⇨ Mejora y facilita el ejercicio del Gobierno Corporativo.
- ⇨ Ayuda a implantar la cultura de **Medición** de la Exposición a riesgos potenciales, 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 estudiados con 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**