

ISO 31000:2009. **Herramienta para evaluar la gestión de riesgos**

Cr Carlos Serra CISA CGEIT

Datasec Uruguay

Agenda



- ¿Qué es el riesgo?
- ¿Qué riesgo asume al no pensar en sus riesgos organizacionales?
- ¿Cómo lo ayuda la ISO 31000:2009 para evaluar su gestión de riesgos?
- Algunos temas del día a día

4.2 Mandato y compromiso

“La introducción de la gestión del riesgo y el aseguramiento de su eficacia continua requieren un compromiso fuerte y sostenido de la dirección de la organización, así como el establecimiento de una planificación estratégica y rigurosa para conseguir el compromiso a todos los niveles ...”

ISO 31000:2009

CiGRAS



- “Sorprendentemente ese caso **no parece haber figurado como un riesgo** de que las líneas aéreas y muchas otras compañías para garantizar la gestión. Aparte de las compañías aéreas, el cierre del espacio aéreo europeo **ha dejado huella en todo**, desde el turismo a la flor y los productores de verduras frescas en África, los fabricantes de prendas de vestir en Bangladesh y los fabricantes de componentes electrónicos en el Lejano Oriente” Kevin W. Knight

CiGRAS

Objetivo: Vender, producir, hacer



CiGRAS

A veces los eventos ocurren...



ISACA®

Confianza y valor en sistemas informáticos

Montevideo Chapter

- Riesgo crediticio
- Riesgo operacional
- Riesgo tecnológico
- Riesgo estratégico
- Riesgo legal
- Riesgo de mercado
- Riesgo de liquidez
- Riesgo de cumplimiento
- No satisfacer los requisitos del cliente
- Peligros Ambientales
- Riesgo de Seguridad Alimenticia
- Peligro para el ser humano
- Riesgo reputacional
- ...



¿Por qué no analizar sus riesgos?

- No aporta valor...
- Si pensamos en todo lo malo, no hacemos nada
- Hay suficientes controles.
- Acá pensamos en metas, no en riesgos.
- Aceptamos que es común que fallen los sistemas tecnológicos.
- ¡No hay tiempo para evaluar los riesgos, necesito vender!
- Acá nunca pasó nada.
- No tenemos los procesos definidos.
- Gestionar los riesgos no me va a ayudar a vender más.
- Si ocurre algo ,ya lo arreglaremos.

Conceptos de la Norma ISO 31000:2009

(Y de la ISO GUIA 73 y la ISO
31010:2009)

- “Mientras **todas las organizaciones gestionan el riesgo** a diferentes niveles, esta norma internacional establece un conjunto de principios que se deben satisfacer para que la gestión del riesgo **sea eficaz**. ... recomienda que las organizaciones desarrollen, implementen y mejoren de manera continuada **un marco de trabajo** cuyo objetivo sea integrar el proceso de gestión del riesgo **en los procesos de gobierno, de estrategia y de planificación, de gestión, y de elaboración de informes, así como en las políticas, los valores y en la cultura de toda la organización.**”

1. OBJETO Y CAMPO DE APLICACIÓN

- “Esta norma internacional proporciona los principios y las directrices genéricas sobre la gestión del riesgo.
- Puede utilizarse por cualquier empresa pública, privada o social, asociación, grupo o individuo. Por tanto, no es específica de una industria o sector concreto.”

Interesados:

- “a) Responsables de desarrollar la política de gestión del riesgo dentro de su organización;
- b) Encargados de asegurar que el riesgo se gestiona de manera eficaz dentro de la organización, considerada en su totalidad o en un área, un proyecto o una actividad específicos;
- c) Los que necesitan evaluar la eficacia de una organización en materia de gestión del riesgo; y
- d) Los que desarrollan normas, guías, procedimientos y códigos de buenas prácticas que, en su totalidad o en parte, establecen cómo se debe tratar el riesgo dentro del contexto específico de estos documentos.”

¿Qué es riesgo?

- Es “el efecto de la incertidumbre en la consecución de los objetivos” ISO 31000:2009
- 1. *Incertidumbre* (puede que nunca ocurra).
- 2. El riesgo importa y debe gestionarse porque tiene un *efecto (positivo y negativo)*.
- 3. Ese efecto es sobre los *objetivos fijados*.

1. Crea valor.
2. Está integrada en los procesos de una organización.
3. Forma parte de la toma de decisiones.
4. Trata explícitamente la incertidumbre.
5. Es sistemática, estructurada y adecuada.
6. Está basada en la mejor información disponible.
7. Está hecha a medida.
8. Tiene en cuenta factores humanos y culturales.
9. Es transparente e inclusiva.
10. Es dinámica, iterativa y sensible al cambio.
11. Facilita la mejora continua de la organización.

**Principios de gestión del riesgo
(cláusula 4)**

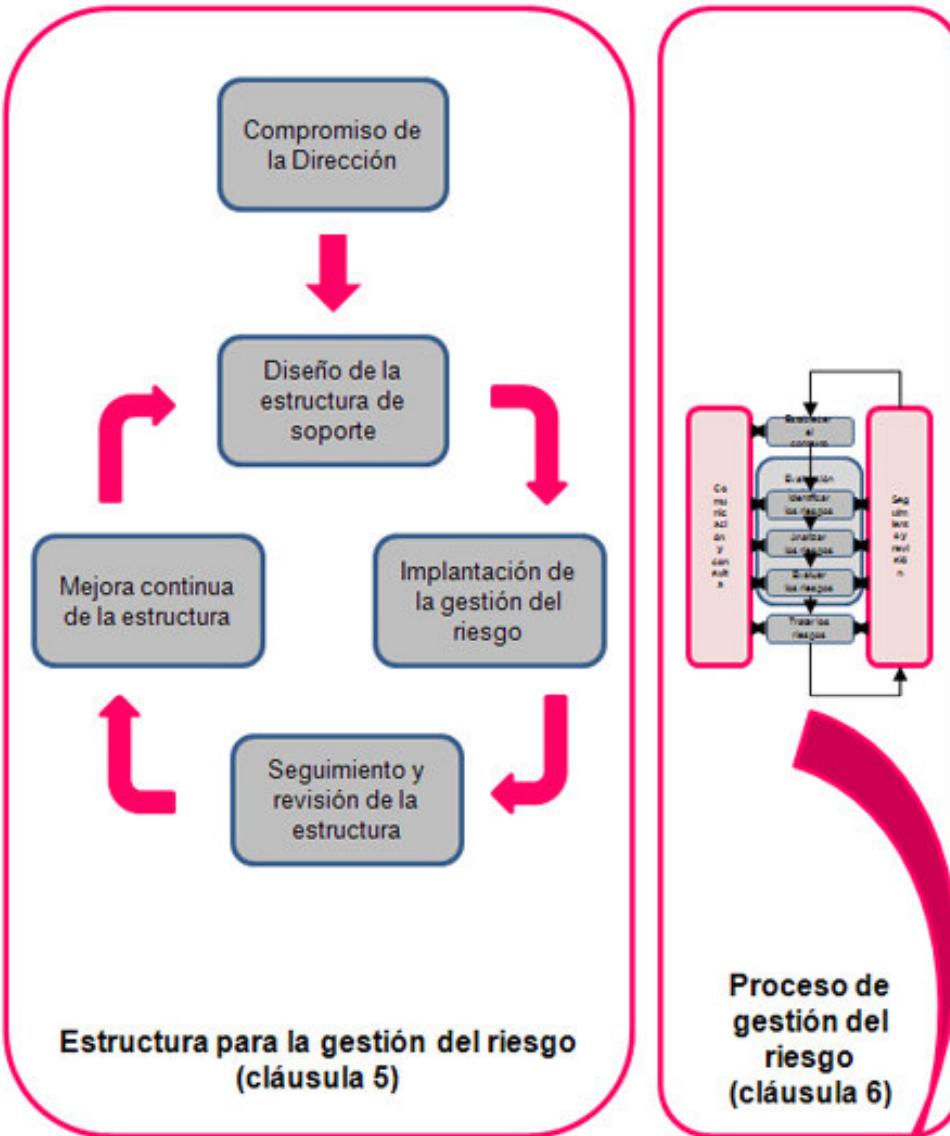
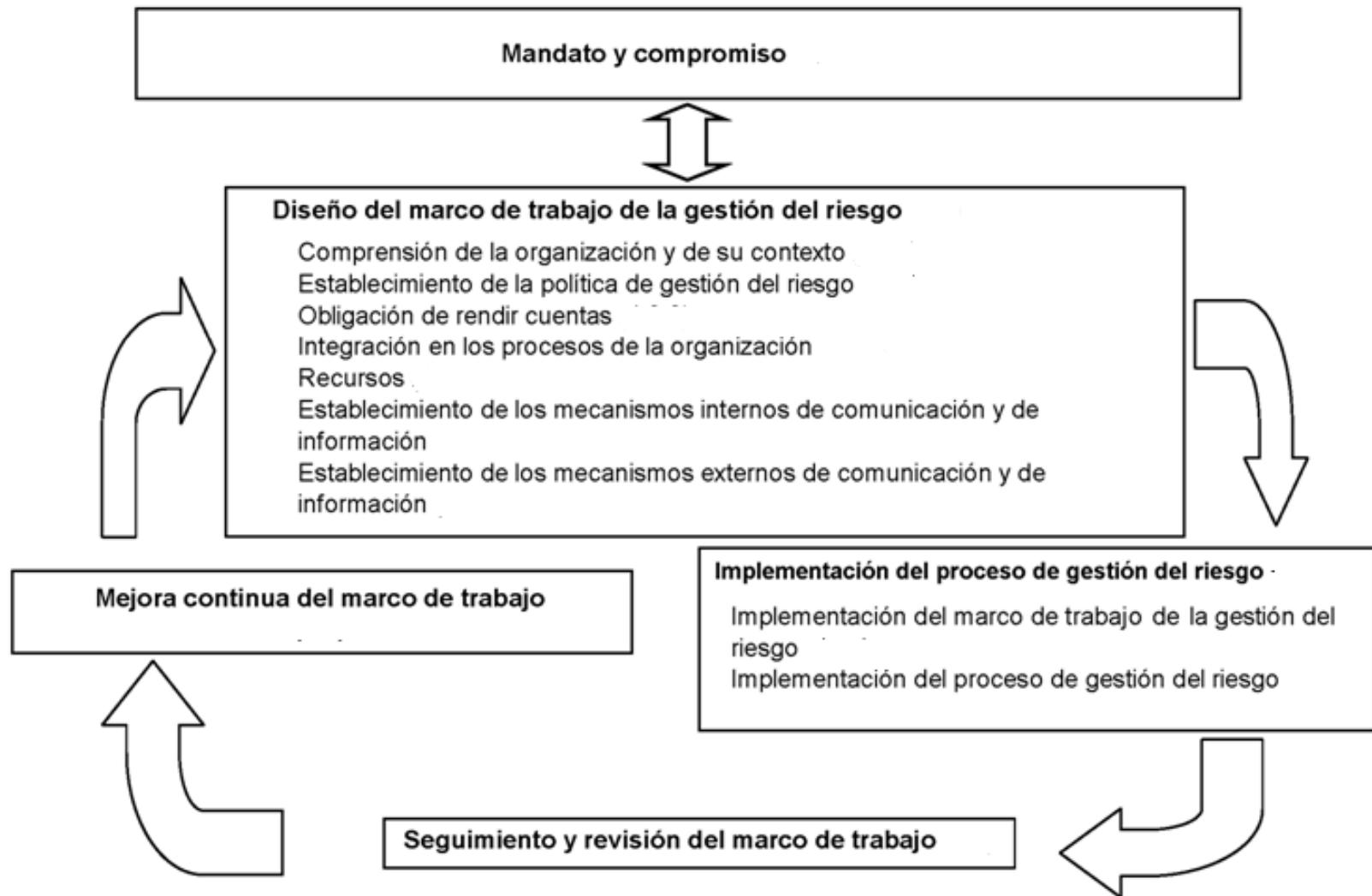


Figura 1. Relación entre los Principios, estructura de soporte y proceso de gestión del riesgo.

Estructura para la gestión de riesgos



ISO 31000 ANEXO A (INFORMATIVO) ATRIBUTOS DE UNA GESTIÓN DEL RIESGO OPTIMIZADA

- A.3.1 Mejora continua
- A.3.2 Responsabilidad completa de los riesgos
- A.3.3 Aplicación de la gestión del riesgo en todas las tomas de decisiones
- A.3.4 Comunicación continua
- A.3.5 Integración completa en la estructura de gobierno de la organización

Normas complementarias

ISO Guía 73:2009

ISO 31010 :2009

“...proporciona el vocabulario básico para desarrollar una comprensión de los conceptos y términos que se utilizan en la gestión del riesgo que son comunes a diferentes organizaciones y funciones, ...”

3.6.1.7 matriz de riesgo:

Herramienta que permite clasificar y visualizar los **riesgos** (1.1), mediante la definición de categorías de **consecuencias** (3.6.1.3) y de su **probabilidad** (3.6.1.1).

- Tormenta de ideas
- Entrevistas estructuradas o semiestructuradas
- Delphi
- Listas de ejemplo
- Análisis de riesgos preliminar (PHA)
- Estudio de Peligros y Operabilidad - HAZOP
- Análisis de peligros y puntos críticos de control (HACCP)
- Evaluación del riesgo ambiental
- Análisis Qué pasa si
- Análisis de escenarios
- Análisis de Impacto de negocio (BIA)
- Análisis de Causa Raíz (RCA)
- Análisis de modo y efecto de la falla (FMEA)
- Análisis de árbol de fallos
- Análisis de árbol de eventos

- Análisis de causas y consecuencias
- Análisis de causa y efecto
- Análisis de Capas de Protección (LOPA)
- Árboles de decisión
- Análisis de la fiabilidad humana
- Árbol de fallos y sucesos iniciadores (bow tie)
- Mantenimiento Centrado en la Fiabilidad (RCM)
- Análisis de circuitos de fugas
- Análisis de cadenas de Markov
- Simulación de Monte Carlo
- Análisis Bayesiano
- Curvas FN
- Índices de riesgo
- Matrices de probabilidad y consecuencia
- Análisis costo beneficio
- Análisis de decisión multicriterio (MCDA)

¿Qué pasa cuando coexisten
diversas evaluaciones de riesgo?

- “La gestión del riesgo contribuye de manera tangible al logro de los objetivos y a la mejora del desempeño, por ejemplo, en lo referente **a la salud y seguridad de las personas, a la conformidad con los requisitos legales y reglamentos, a la aceptación por el público, a la protección ambiental, a la calidad del producto, a la gestión del proyecto, a la eficacia en las operaciones, y a su gobierno y reputación.**”
- REFERENCIA EN LA ISO 31000

CiGRAS La ISO 9000 y el riesgo

- **Acción preventiva** : “acción tomada para eliminar la causa de una no conformidad potencial u otra situación potencialmente inestable”
- **No conformidad** es el incumplimiento de un requisito.

Entonces...

- Recuerde que esta Norma ISO 31000 no es certificable...
- Ignorar sus riesgos no es una opción

La Alta Gerencia

- Tiene responsabilidad dentro del Buen Gobierno de buscar el logro de los objetivos
- Le permite demostrar debida diligencia
- Le ayuda a invertir los recursos en forma ordenada
- Le permite conocer los riesgos a que está expuesto (incluso hoy)

Esto se traduce en : mensajes claros , coherentes y continuos a toda la organización

¿Cuánto se habla del tema riesgos en las reuniones gerenciales?

- Saber: Conocer en profundidad el proceso que lidera, sus objetivos y riesgos.
- Poder: Debe tener capacidad para la toma de decisiones y mejorar el proceso, en función del grado de responsabilidad delegada a cada uno.
- Querer: Debe entender el valor de gestionar los riesgos y asumir voluntariamente su responsabilidad contribuyendo así al logro de los objetivos estratégicos de la organización.

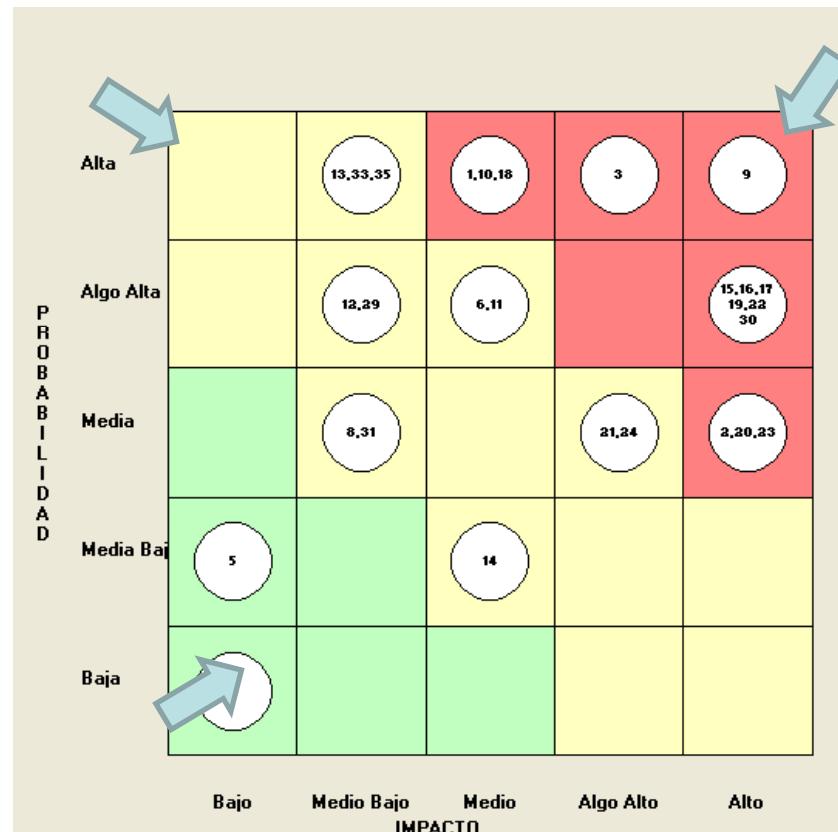
¿La descripción de puesto gerencial incluye la tarea de gestionar sus riesgos? ¿Cuántas veces se trata el tema en las reuniones gerenciales?

ACTIVIDADES DE ANÁLISIS Y GESTIÓN DE RIESGO



Definiendo las prioridades

*Riesgos a tener en cuenta y monitorear. Costo-Beneficio.
Oportunidades-Consecuencias*

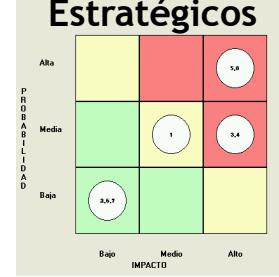


Riesgos a estar alerta a cambios en su severidad u Ocurrencia. No asumir costos
www.isaca.org.uy

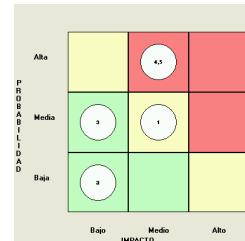
Riesgos intolerables requieren acciones urgentes

Propiedad de los Riesgos en cada área

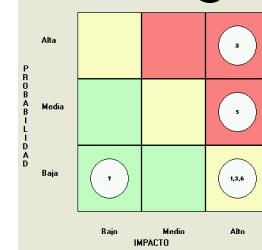
Directorio, Gcia Grl
Estratégicos



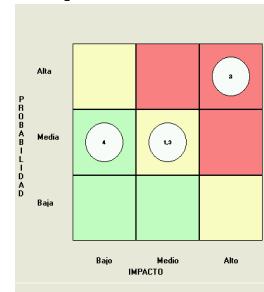
Gerencia de Créditos



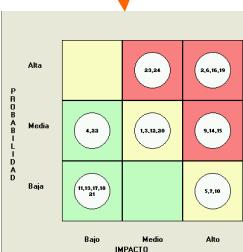
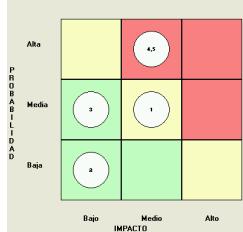
Tecnología



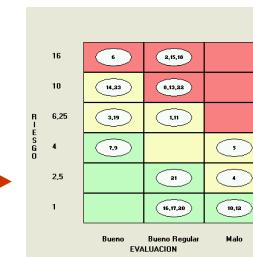
Operaciones



Contaduría



Mapa Gral



C/Controles

¿Cómo podemos evaluar los riesgos tecnológicos?

Meycor COSO AG - Eval v.5.2 - Usuario: ADMIN - Base: eval130 - [Evaluación de Riesgos y Actividades de Control Genéricos]

Archivo Edición Proyectos Codificación Entidades Grupos y Revisores Evaluaciones Tratamientos Períodos Ventana ?

Proyectos Reportes

- + PO10-Gestión de proyectos
- COBIT: Adquisición e Implementación
 - + AI1-Identificación de soluciones automatizadas
 - + AI2-Adquisición y mantenimiento de software de aplicación
 - + AI3-Adquisición y mantenimiento de infraestructura tecnológica
 - + AI4-Habilitación de la operación y el uso
 - + AI5-Abastecimiento de recursos de TI
 - + AI6-Gestión de cambios
 - + AI7-Instalación y acreditación de soluciones y cambios
- COBIT: Entrega y Soporte
 - + DS1-Definición de los niveles de servicio
 - DS2-Administración de servicios prestados por terceros
 - + 1 - KGI
 - + 2 - KPI
 - 3 - DS2.1 Identificación de las relaciones con todos los proveedores
 - No se identifica a los proveedores críticos o importantes.
 - Los recursos para la administración de proveedores se usan de forma ineficaz e ineficiente.
 - La falta de claridad respecto a los roles y responsabilidades ocasiona problemas de comunicación, malos servicios y costos elevados.**
 - 4 - DS2.2 Administración de las relaciones con los proveedores
 - Los proveedores no son receptivos y no están comprometidos con la relación.
 - No se resuelven los problemas y las dificultades.
 - La calidad del servicio no es la adecuada.

Proceso	COBIT: Entrega y Soporte
Sub Proceso	DS2-Administración de servicios prestados por terceros
Objetivo de Proceso	3 - DS2.1 Identificación de las relaciones con todos los proveedores
Factor de Riesgo	La falta de claridad respecto a los roles y responsabilidades ocasiona problemas de comunicación, malos servicios y costos elevados.
Actividades de Control	0 / 0

Meycor Knowledge Provider > Inicio > Riesgos

Proyectos Riesgos Eventos Autoevaluación Reportes Novedades



Procesos

Activos

Valoración de activos

Grupos de activos

Amenazas

Evaluación del riesgo

Tratamiento del riesgo

Resultado de evaluación

Cierre de evaluaciones

Valoración de activos

Activos @Office Firewall

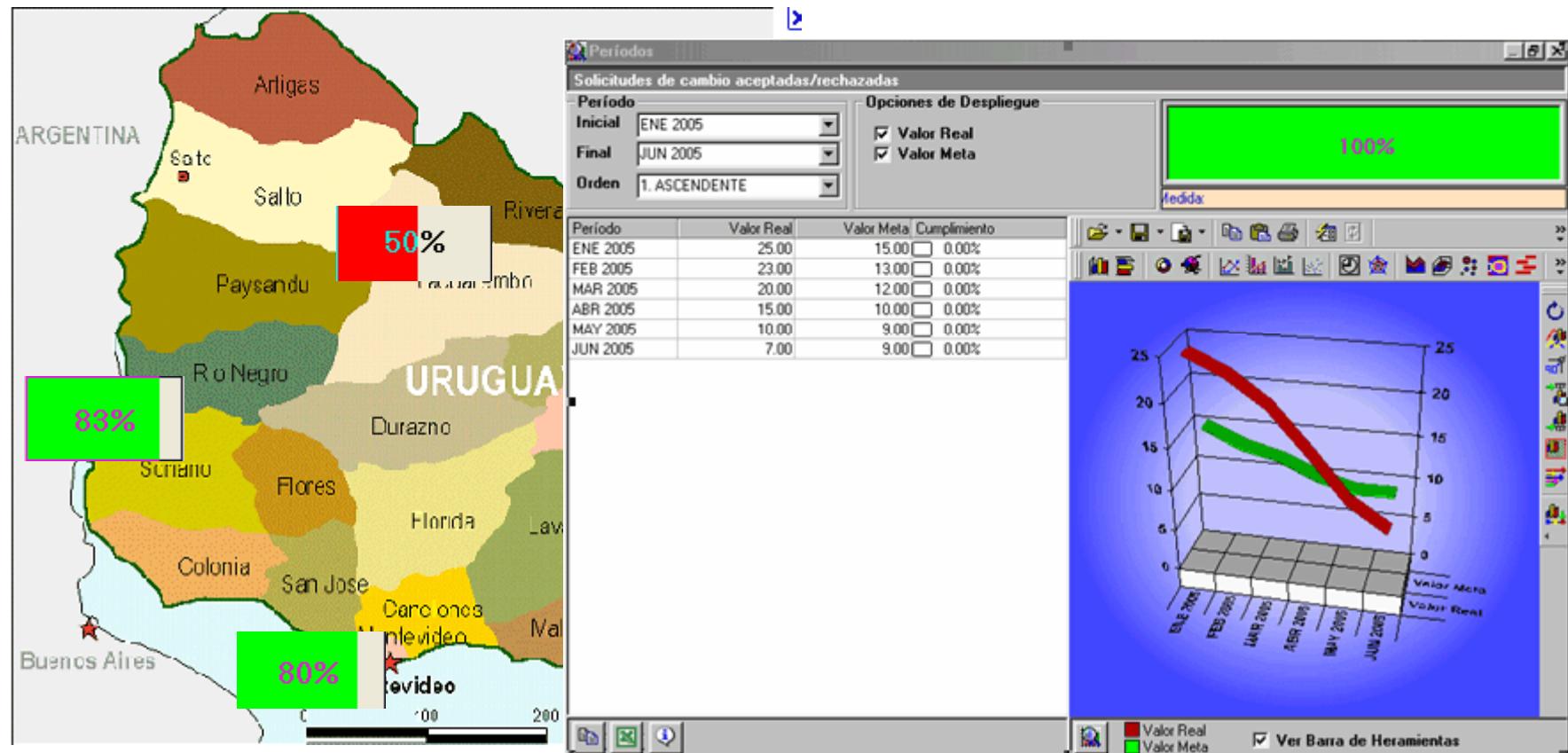


Justificación

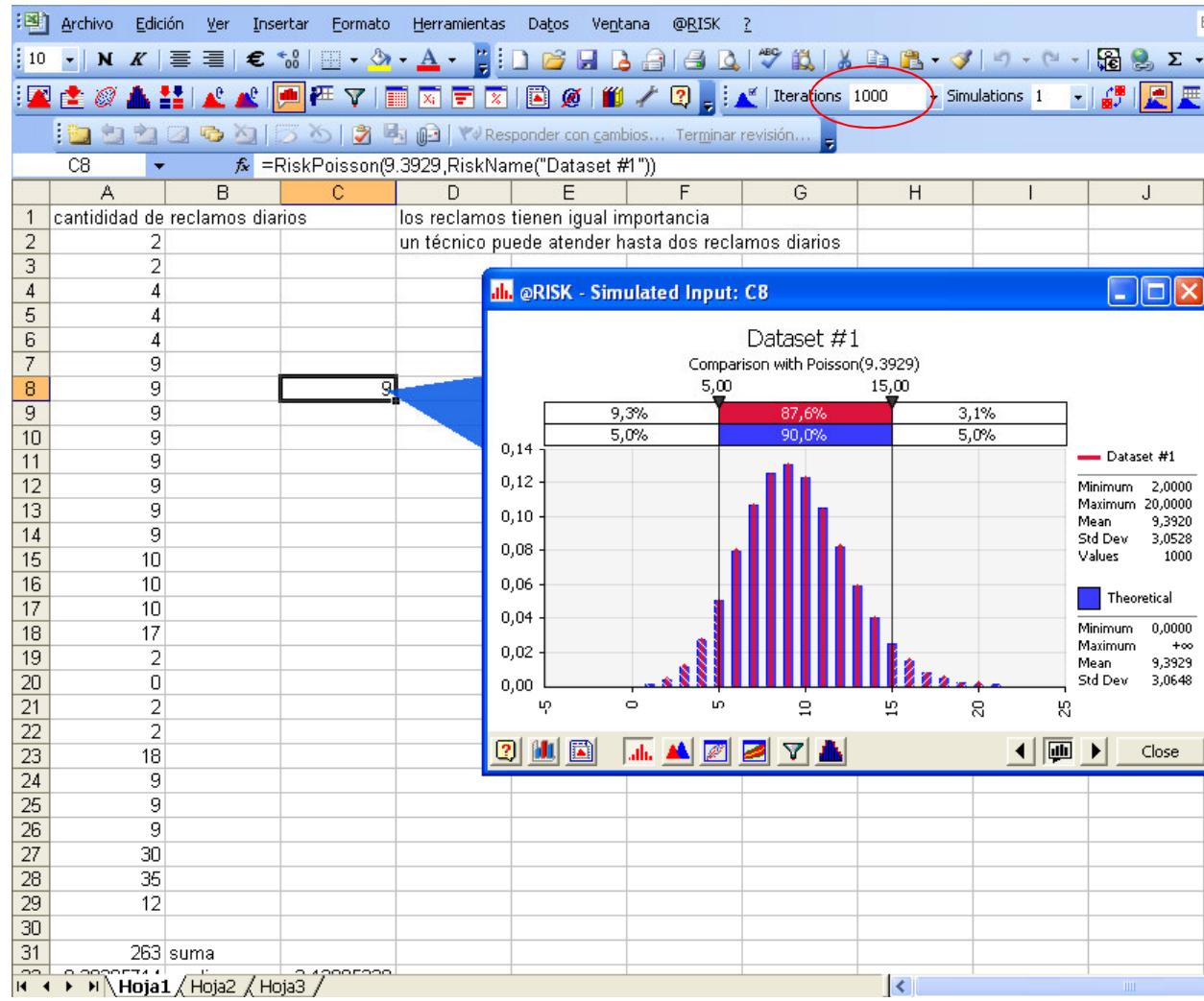
Confidencialidad	Medio-Alto	Solo el personal autorizado conoce la configuración y reglas del firewall.
Disponibilidad	Medio-Alto	Debe de estar disponible casi en todo momento.
Integridad	Alto	Debe estar bien configurado y funcionar correctamente.

ACTUALIZAR

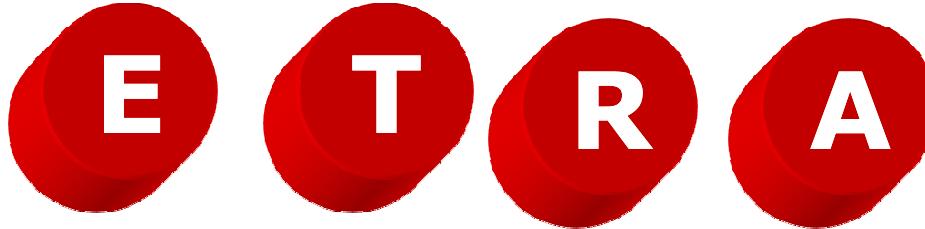
¿Qué dicen nuestros Indicadores clave de riesgo (KRI)?



Algo cuantitativo: Modelo Monte Carlo



¿Y ahora que medimos los riesgos qué podemos hacer?



- ✓ **ELUDIR** no proseguir con la actividad riesgosa (!No siempre es posible !)
- ✓ **TRANSFERIR** que otra parte soporte parte del riesgo (Pensar en que nuevos riesgos ocasiona este cambio)
- ✓ **REDUCIR** tomar medidas tendientes a reducir la probabilidad de ocurrencia y/o impacto, (No siempre implica costos financieros adicionales, incluso puede ahorrar dinero)
- ✓ **ASUMIR** aceptar el riesgo inherente (!Pero **conociéndolo!**)

El análisis de riesgos del análisis de riesgos

- La Dirección entiende que

Conocer los Riesgos Operacionales es importante () Es problema de la Unidad de Riesgos() No ha entendido que son los RO ()

- Al Valuar los riesgos, la gente “experta”:

Es muy optimista o pesimista () Es realista () No tiene tiempo para hacerlo ()

- Mapas de riesgo por proceso

No tiene () Tiene para mostrar a la auditoria () Tiene y se usa para decidir ()

- En el registro de eventos, piensa que se registraran:

Menos del 25 % de los eventos () entre un 25 y un 50 () entre 50 y un 75% () entre el 75 y el 100% ()

- Sobre los Indicadores

Hay tantos que no son manejables () Se empieza con unos pocos pero adecuados () Elige los que sabe que dan bien ()

Ejemplo de puntos a evaluar

Punto de Atención	Evaluación	Comentarios	Referencia	Evidencia
¿Se entiende por parte de la Dirección que la incertidumbre del futuro implica amenazas y oportunidades que deben ser identificadas?		Normalmente, este atributo se podría verificar a través de las entrevistas con la dirección y a través de la evidencia de sus acciones y declaraciones. Si no hay apoyo de la Dirección no habrán recursos para este proceso	A.3.5 Integración completa en la estructura de gobierno de la organización	

Ejemplo de puntos a evaluar

Punto de Atención	eval.	Comentarios	Referencia	Evidencia
¿Tiene un marco de trabajo que atiende los aspectos estructurales y organizativos de la gestión de riesgos?		Esta etapa es básica para un adecuado trabajo práctico posterior. El marco de trabajo facilita una gestión eficaz del riesgo mediante la aplicación del proceso de gestión del riesgo a diferentes niveles y dentro de contextos específicos de la organización.	4 Marco de Trabajo ISO 31000	

Ejemplo de puntos a evaluar

Punto de Atención	eval.	Comentarios	Referencia	Evidencia
¿Se cuenta con un plan de tratamientos razonable, acorde a la severidad de los riesgos asociados?		El plan debe identificar con claridad el orden de prioridad en que se deberían implementar los tratamientos de riesgo individuales	5.5.3 Preparación e implementación de los planes de tratamiento del riesgo	

Anexo (para después...)

¿Cuál es el nivel de madurez de su organización en gestión de riesgos ?

(origen del modelo :opinión del autor)

¿Usted cómo está gestionando sus riesgos?

- 0- No se piensa en ello.
- 1- Se habla de los riesgos a veces y para algunos proyectos en forma inconsistente . Hay un responsable del monitoreo de riesgos con autoridad limitada.
- 2- La administración de riesgos se da por lo general a alto nivel y típicamente se aplica solo a proyectos grandes o como respuesta a problemas. Se han identificado riesgos de algunos procesos en forma inicial, medidos en forma cualitativa.
- 3- Hay una política de administración del riesgo que define cuándo y cómo llevar a cabo las evaluaciones de riesgo. Todos los riesgos identificados tienen un propietario asignado, si bien el mismo aún actúa en forma reactiva. Se comienzan a registrar los eventos ocurridos pero no se analizan. Hay capacitación en la materia.
- 4- La alta gerencia ha determinado los niveles de riesgo tolerables para la organización. Hay mediciones cuantitativas cuando aplica. Hay indicadores clave definidos y se presentan a un comité que los usa para toma de decisiones.
- 5- La administración del riesgo está efectivamente integrada en todas las operaciones , es bien aceptada e involucra extensamente a los empleados. Los propietarios de procesos gestionan sus propios riesgos. La gerencia evalúa en forma permanente las estrategias de mitigación de riesgos. Hay paneles que muestran la medición del nivel de riesgo organizacional y por área.

CiGRAS La norma ISO 31000 :

- Si su nivel de madurez es 0,1,2
lo ayudará a ordenarse, a mejorar los logros y demostrar debida diligencia (piense que este esfuerzo NO CREA RIESGOS NUEVOS),
- Si su nivel de madurez es 3,4,5
lo ayudará a examinar críticamente si las prácticas y procesos que está aplicando son las más adecuadas a su caso.

¿Preguntas? Muchas Gracias

Carlos R. Serra

serra@datasec-soft-com