XV CONGRESO LATINOAMERICANO DE AUDITORIA INTERNA Y EVALUACION DE RIESGOS

ISO 31.000- Nuevo Standard para la administración de riesgos
Una valiosa guía para la Auditoria Interna

Expositor : Sr. Carlos Valdivieso Valenzuela
carvalva@entelchile.net

Cartagena de Indias, Colombia, 31 de mayo del 2011

ALCANCE DE ESTA EXPOSICIÓN

- El expositor la hace a título personal y sin ningún beneficio económico; sólo como apoyo a CLAIN a objeto de instalar el tema para conversación y análisis entre nosotros en este Congreso.
- Los cuadros referentes de ISO tienen esa fuente en inglés con traducción libre al español del expositor.
- ISO 31.000 es de tipo general; cada cual debe estudiar cómo la desarrolla y aplica en su organización. Esta ISO es para cualquier tipo de empresa, no sólo Bancos.
- El expositor entrega algunas orientaciones basado en su experiencia; cada cual debe desarrollar sus propios modelos; por tanto estas orientaciones, son sólo guías para esta exposición.
- Se solicita tener en cuenta durante la presentación, que en la realidad, este es un tema de la empresa como un todo; la responsabilidad del auditor interno, según la definición de IIA es doble, tanto en assurance como consulting, formando equipos con otras áreas.
- Cada indicación de la ISO es todo un tema por si mismo , pero todos integrados. Es un tema de largo desarrollo e implementación, pero que llegó para quedarse.

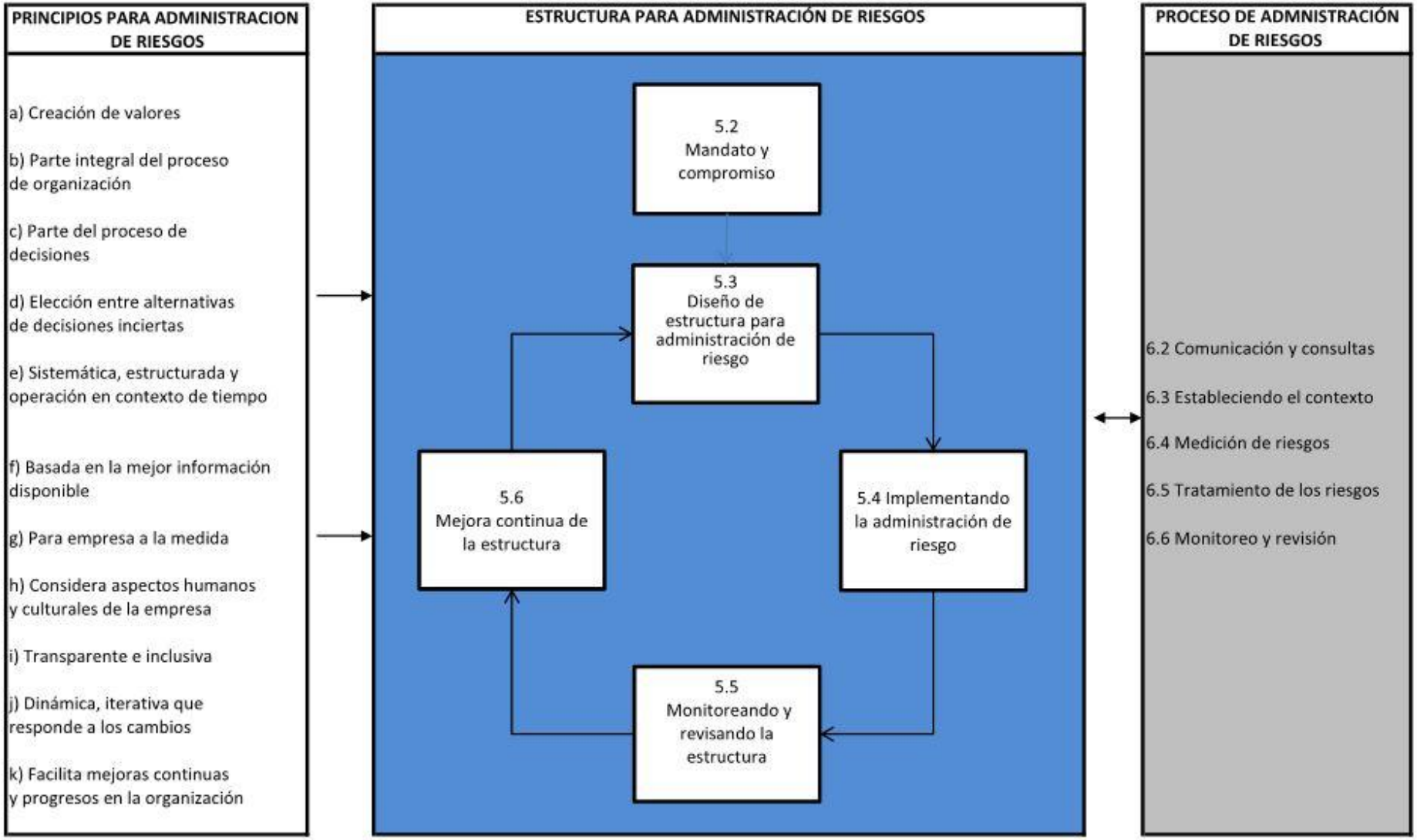
ALCANCE DE ESTA EXPOSICIÓN

- Si se analiza la evolución desde 1993, varias estructuras de control interno se han hecho famosas en los últimos años, entre otras: COSO y después COSO ERM- COCO (Canadá) – COBIT (para IT) y AS /NZS 4360-2004 conocida también por su origen australiano y nuevo zelandés; pues bien, la nueva ISO 31.000 ha tenido mucha influencia a partir de esta última. Tangencialmente, Basilea II también debe considerarse.
- Se aprecia que ya van unos 17 años caminando por riesgos , gobiernos corporativos y otros ; aquí hay un claro camino el que debe abordarse con el conocimiento, desarrollo y aplicación.
- Es tan claro y fuerte el mensaje de ISO 31.000 que hoy se está estudiando como reformular COSO y COSO ERM, el estándar australiano nuevo zelandés y otros.
- Esta exposición por limitación de tiempo, cubre sólo parte del material el que queda a vuestra disposición , incluido especialmente el archivo anexo con ejemplos.
- Espero pueda iniciarse luego una conversación profesional entre nosotros, que es lo más importante.

ORGANIZACIÓN INTERNACIONAL PARA LA ESTANDARIZACIÓN

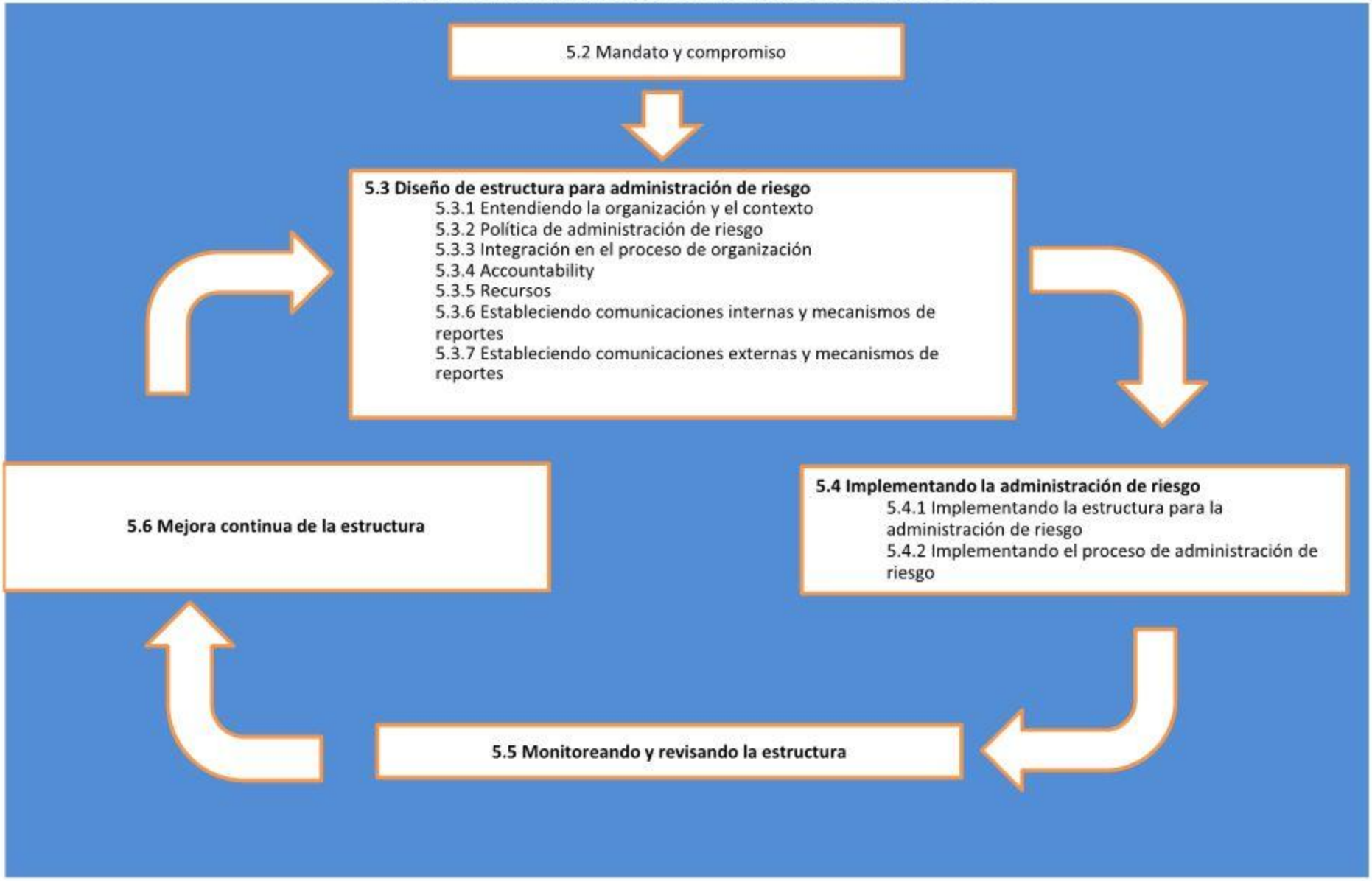
- 165 países miembros. La sede de ISO está en Ginebra.
- ISO es el organismo encargado de desarrollar normas internacionales en distintos ámbitos.
- Las normas ISO son voluntarias, pero son un referente, deben comprarse y están en francés e inglés.
- ISO 31.000 fue aprobada en noviembre del 2009 estableciendo un nuevo estándar para la administración de riesgos. Su revisión se hará el año 2013.

VISIÓN GENERAL ISO 31000

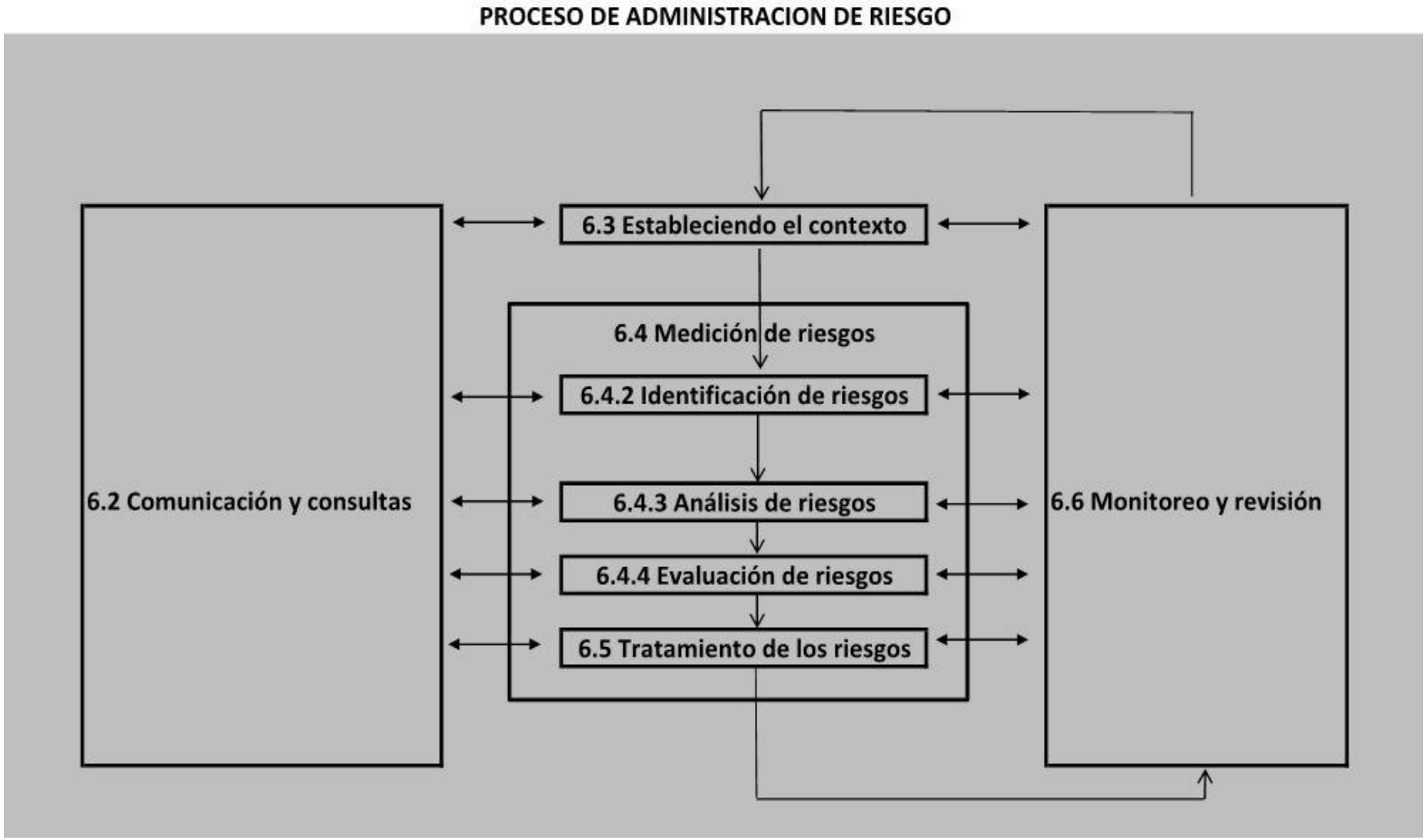


Fuente: ISO 31000 – Traducción libre al español del señor Carlos Valdivieso Valenzuela

ESTRUCTURA PARA LA ADMINISTRACION DE RIESGOS



Fuente: ISO 31000 – Traducción libre al español del señor Carlos Valdivieso Valenzuela

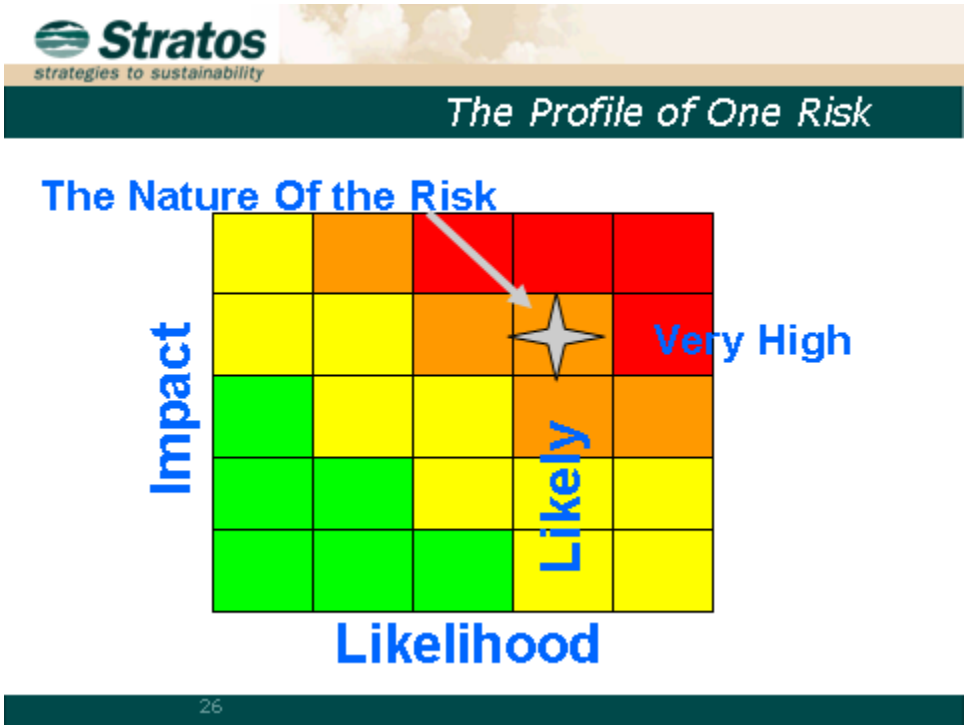


Fuente: ISO 31000 – Traducción libre al español del señor Carlos Valdivieso Valenzuela

CONSULTAR EN LA WEB GUIA ISO / CEI / 73

- Contiene terminología; uno podría haber esperado más, pero ahí está.
- Riesgo se define ahí como combinación de : probabilidad, un suceso y su consecuencia.
- Consecuencia; que pase algo y su impacto medible.
- Probabilidad , entre 0 y 1, lo mismo entre 0 y 100 %.
- Este expositor previene que se han hecho profusas presentaciones con el resultado en escalas de 1 a 5 para impacto y probabilidad , luego multiplicando en que el resultado peor es 25, esto es, 5x5 y luego con un gráfico de colores; les recomiendo, si no lo hubieren hecho, conocerlas, pero, tener cuidado , construir su propia escala con cinco años hacia atrás ; para construir las escalas y los tramos, recomiendo trabajar con los Estados de Resultados de los Estados Financieros y consulten con vuestros auditores externos; hay guías internaciones; no se encandilen fácilmente con ejercicios teóricos y gráficos de colores.

UN EJEMPLO GRAFICO (fuente Stratos)



COMPARAR LO QUE CADA EMPRESA TIENE CON EXPUESTO EN LA ISO 31.000

- Ya sabemos que las ISO son voluntarias y por ahora esta ISO no es certificable, pero también hemos conocido que el mercado valora cuando alguien cumple con alguna ISO.
- Por lo demás, espero que a esta altura de la exposición, la ISO 31.000 les parezca conveniente y ciertamente es una valiosa ayuda para Auditoría Interna.
- La ISO 31.000 expresa claramente que cada empresa debe comparar lo que tiene en estas materias con lo contenido en esta ISO 31.000 que es la norma recomendable.
- Es importante tener normas y modelo de Gobierno Corporativo (hay muchas) ; tengan como mera referencia general las normas de OECD " Principles of Corporate Governance " escrito el 2004 .
- Desde la mirada del Supervisor, el Comité de Basilea tiene 25 principios que pueden consultarse en los documentos de dicho Comité
- De todo esto,resulta algo evidente, las diferencias, establecer los planes de acción y …….a trabajar.

LA DEFINICIÓN DE AUDITORÍA INTERNA NOS INVOLUCRA BAJO UN DOBLE ROL: ASSURANCE Y CONSULTING

Definition of Internal Auditing

*Internal auditing is an independent, objective **assurance** and **consulting** activity designed to **add value** and **improve an organization's operations**. It **helps** an organization accomplish its objectives by bringing a **systematic**, disciplined approach to evaluate and improve the effectiveness of **risk management, control, and governance processes.***

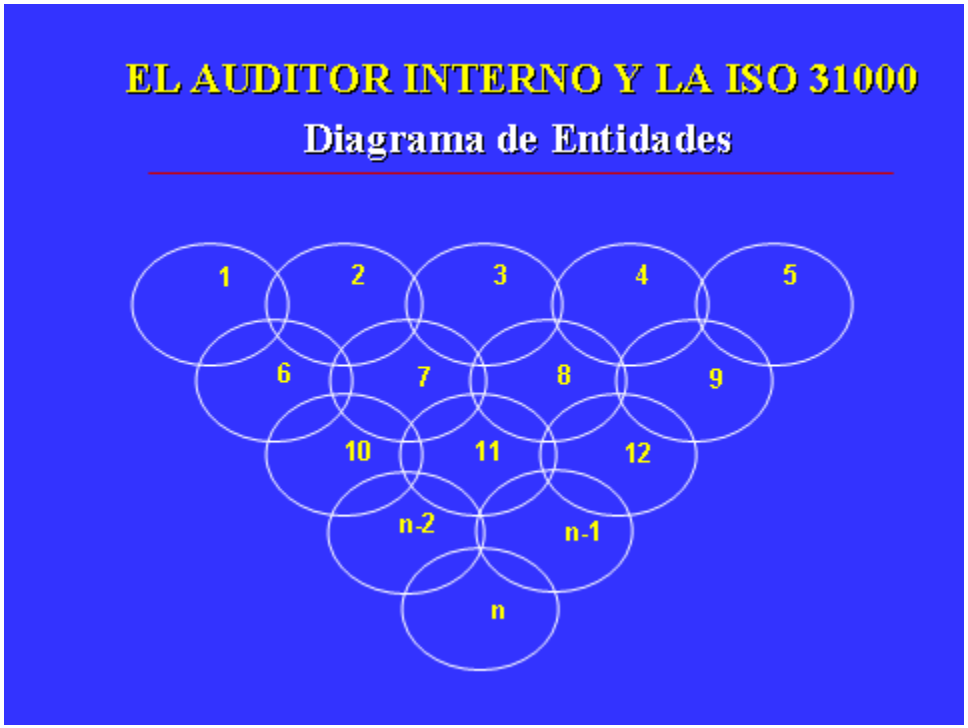
Fuente: The Institute of Internal Auditors

(TRADUCCIÓN OFICIAL) ESPAÑOL
Definición de la auditoría interna

La Auditoría Interna es una actividad independiente y objetiva de aseguramiento y consulta, concebida para agregar valor y mejorar las operaciones de una organización. Ayuda a una organización a cumplir sus objetivos aportando un enfoque sistemático y disciplinado para evaluar y mejorar la eficacia de los procesos de gestión de riesgos, control y gobierno.

Fuente: **IIA**

EL AUDITOR INTERNO Y LA ISO 31000 SER PARTE DE UN EQUIPO CON PERSONAS DE OTRAS ÁREAS



Fuente: Sr. Carlos Valdivieso Valenzuela

RESPECTO A LOS PRINCIPIOS DE ADMINISTRACIÓN DE RIESGOS

- Yo he leído muchas páginas y no sé cuantas miles, no habré leído; uno busca algo como un check list universal y no lo encuentra ; algunos consejos prácticos para no desesperarse:
- Traten de obtener el excelente libro escrito en 1996 por Coopers & Lybrands (hoy con Price) llamado Generally Accepted Risk Principles (GARP). Hay un muy buen listado con sus definiciones.
- Vean si en vuestras empresas tienen algo ya definido; si tuvieren sistemas de check & balanced, si estuviere definido lo que se acepta, lo que se evita, lo que se transfiere como riesgos.
- Consulten lo que tiene vuestro supervisor.
- Pregunten a vuestros auditores externos, lo que tienen a nivel internacional.
- Es ya un tema instalado internacionalmente que la administración de riesgos, está directamente relacionado con el Patrimonio (Ej. Basilea II) y proximante Basilea III.

RESPECTO A LOS PRINCIPIOS DE ADMINISTRACIÓN DE RIESGOS

- Aprecien si tuvieren principios de Gobierno Corporativo.
- En especial, vean los principios de los siguientes Riesgos : crédito, financiero, operacional, gestión de capital, prevención de lavado de activos, calidad, TI, RRHH, ético , cumplimiento, auditoria. Basilea II les puede ayudar algo.
- Consulten por los principios de toma de decisiones y de excepciones y de Comités.
- Aprecien si los procesos y procedimientos están levantados y enumerados los riesgos, los elementos de riesgos, los factores de riesgos , las actividades de control y quienes son los responsables.
- Consulten si hay matriz de riesgos sus definiciones y aplicación.
- Tengan siempre a mano lo que explicita genéricamente la ISO 31.000 y la Guía ISO / CEI 73 que pueden encontrar en la Web ; ánimo , no es fácil.

RESPECTO A LA ESTRUCTURA DE ADMINISTRACIÓN DE RIESGOS

- Hay un mandato explícito del Directorio sobre el tema ??? (ISO llama mandato y compromiso).
- La estructura, tiene un control de riesgo descentralizado ??es parcialmente centralizado ???.
- Hay Gerencia de Riesgos ??? Qué incluye ??? crédito, finanzas, operacional, incluido TI ???.
- Hay una matriz de riesgos??? Va en anexos, un ejemplo del expositor.

RESPECTO AL MONITOREO

- Existe algún sistema ???
- Es automático, semiautomático, manual ???
- Es ex ante, es durante, es expost???
- Trabaja inserto en las aplicaciones ???
- Es preventivo ???
- Hay monitoreo automático de logs sensibles (hay herramientas)
- En un Banco puede haber unas tres millones de transacciones computacionales diarias; cómo se automatiza un monitoreo de las cosas sensibles y por excepción ???
- Comentarios del expositor.

ANEXOS DE APOYO

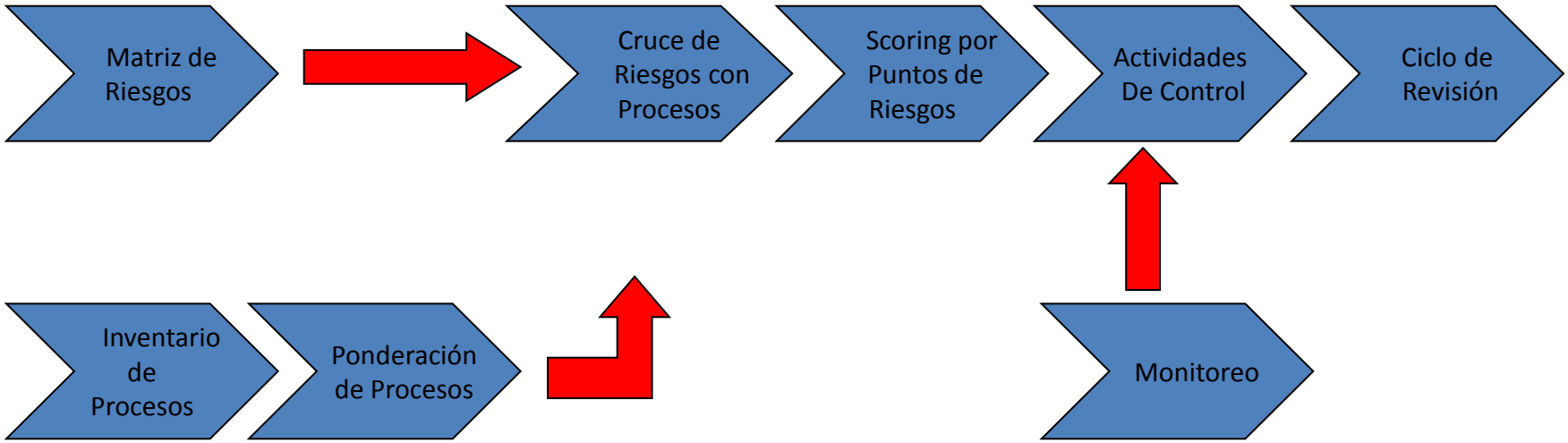
- Van en documento anexo.
- Se incluyen sólo a objeto de facilitar la exposición. **SOLO EN PARTE DE LA MISMA**
- Fueron hechos por el expositor y contienen sus experiencias reales de varios años de trabajo y continuos ajustes.
- Lo que quiero destacar hoy es que en temas generales como ISO 31.000, COSO, COSO ERM y tantos otros, surge la reflexión ; **BUENO, ENTENDÍ Y AHORA COMO SIGO ???** Yo creo, ésta es una pesada herencia de auditoría interna que hemos estado acostumbrados a check list, que siguen siendo necesarios, pero como partes de un todo mucho más amplio.
- Tenemos que saber coexistir con la vida diaria, los arqueos, la investigación de los fraudes y tantos otros que nadie discute son de Auditoría Interna y estos DESAFIOS GRANDES Y MOTIVADORES. Como decía el Presidente Obama en su campaña como candidato.

“ Yes, we can “.

ANEXOS DE APOYO

- Los ejemplos del expositor avanzan y como meros ejemplos en **parte de** la ISO 31000 Estos ejemplos, son sólo en lo referente a Matriz de riesgos y ponderación de procesos y riesgos: la idea es demostrar que para desarrollar e implementar la ISO 31.000 hay que hacer numerosas cosas y concretas; los auditores internos si bien deben revisar después que lo establecido se cumpla, que haya manuales, etc, etc, tienen un rol mucho más rico desde el levantamiento inicial de las diferencias y luego como consultores; los ejemplos referidos a una parte de la ISO muestran y motivan a que ello es posible.
- No son por tanto, ni verdades absolutas, ni métodos únicos; cada cual debe ver como lo hace**;** espero les sirvan.

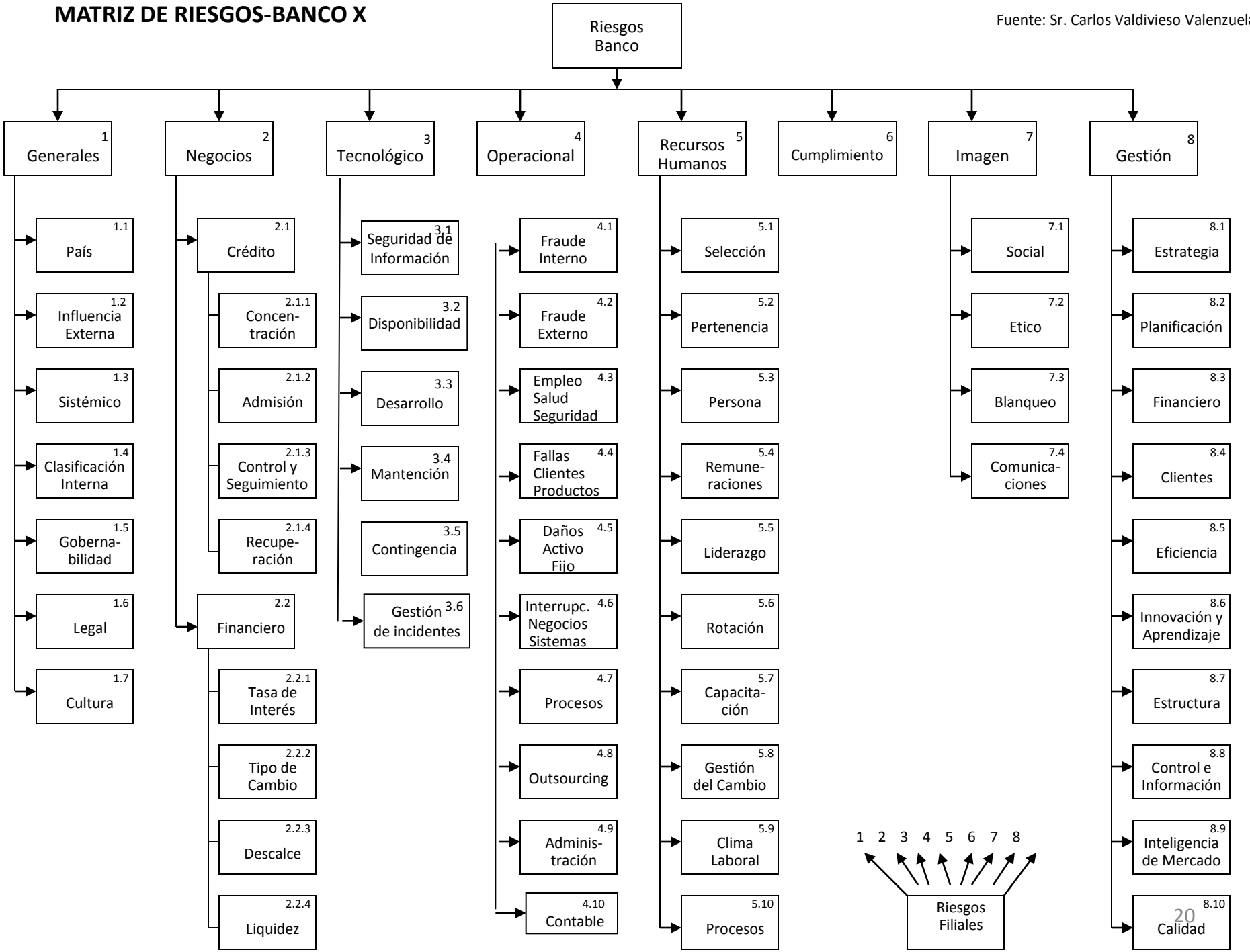
Etapas de desarrollo en la Metodología



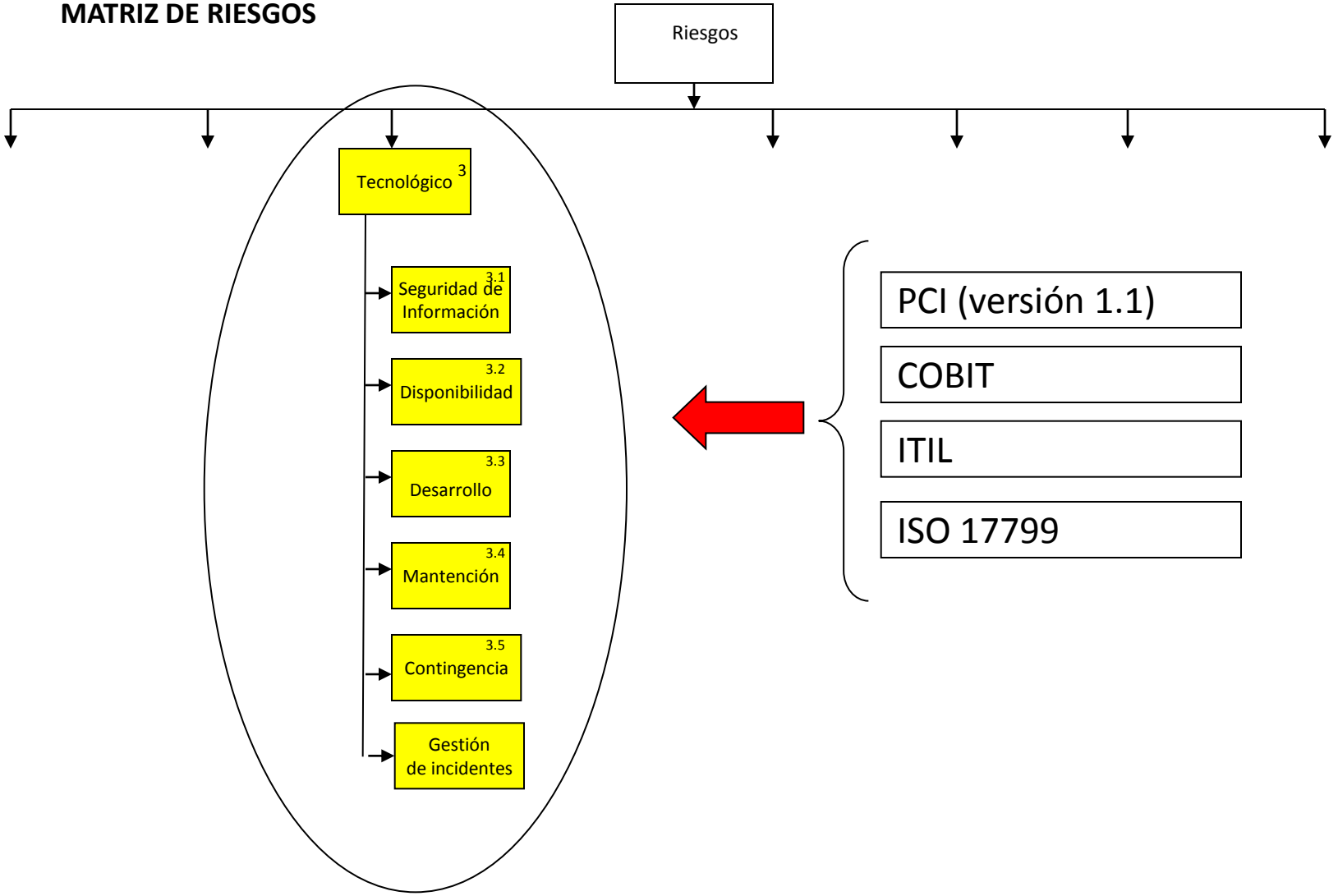
Fuente : Sr. Carlos Valdivieso Valenzuela

MATRIZ DE RIESGOS-BANCO X

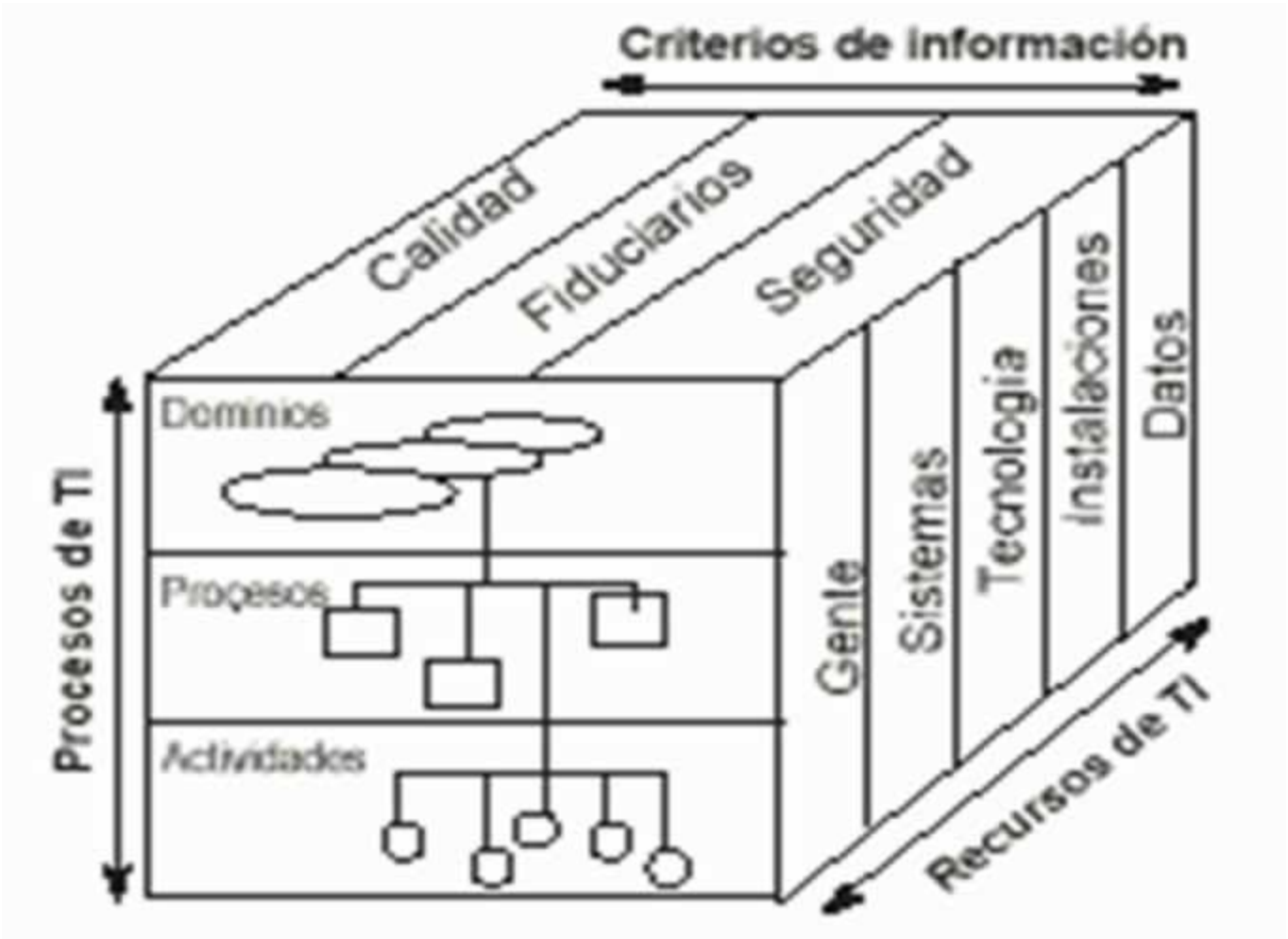
Fuente: Sr. Carlos Valdivieso Valenzuela



MATRIZ DE RIESGOS



Fuente : Sr. Carlos Valdivieso Valenzuela



Fuente : COBIT

Listar los Procesos

- Los procesos se dividen en monetarios y no monetarios.
- Es necesario tener flujogramas de los procesos (esto debe ser detallado,hay metodologías) los elementos de riesgos, los factores de riesgos y sus actividades de control y especificación de lo que puede fallar (metodología especial).
- Los monetarios son los que derivan de saldos en los estados financieros.
- Los no monetarios, no tienen asociados saldos.
- Un proceso incluye todo su flujo, incluido lo informático.
- Luego deben asignarse puntajes.

UN EJEMPLO DE FACTORES PARA PUNTUAR PROCESOS

- Riesgo inherente (dato duro para los monetarios y encuesta para no monetarios).
- Pérdida histórica (dato duro y encuesta para no monetarios).
- Riesgo de imagen (estimación).
- Impacto estratégico.
- Control Interno.

Puntuación de los Procesos

PROCESOS \ FACTORES DE PUNTAJE	Factor 1	Factor 2	Factor 3	Factor 4	Factor 5	Puntaje Total	Origen
04 Préstamos Comerciales	X1	Y1	Z1	W1	H1	X1*Y1*Z1*W1*H1	MB1
36 Gastos del Personal	X2	Y2	Z2	W2	H2	X2*Y2*Z2*W2*H2	MR1
50 Reclamos de Clientes	X3	Y3	Z3	W3	H3	X3*Y3*Z3*W3*H3	NM
etc.							

Fuente : Sr. Carlos Valdivieso Valenzuela

Cruce Estratégico

Proceso	Subproceso	Perspectiva Financiera	Aumentar Ingresos	Disminuir Costos y Gastos	Planes de Acción	Perspectiva de Clientes	Nuevos Clientes	Rentabilizar y mantener clientes	Gestionar la relación con clientes	Perspectiva de Eficiencia	Desarrollar Prod. Y servicios en base a clientes	Controlar el desarrollo de prod. y servicios	Incrementar la eficiencia	Perspectiva de crecimiento y desarrollo	Recursos Humanos (alineamiento, productividad, clima, etc.)	Tecnología para crecer	Inteligencia de mercado	Puntaje

Instrucciones para la Tabla:
1.- Marcar Intersecciones
2.- Cada intersección puede ser :

- Importancia Alta = 3 puntos
- Importancia Media = 2 puntos
- Importancia Baja = 1 punto

Resultado del Puntaje al sumar horizontalmente :

- De 0 a 7 = 1 punto
- De 8 a 15 = 2 puntos
- De 16 a 23 = 3 puntos
- De 24 a 30 = 4 puntos
- De 31 a 36 = 5 puntos

Fuente : Sr. Carlos Valdivieso Valenzuela

Fuente : Sr. Carlos Valdivieso Valenzuela

Procesos

Proceso :
Encargado(a):

Calidad del Ambiente de Control Interno

Item	Puntaje Total	NO	SI	N/A	Ajuste Auditoría	Respuesta Final	Observaciones
1 Descripción y conocimiento del proceso	**3**						
1.1 Está descrito y definido el proceso ?		0,6	0	0			
1.2 Hay una matriz de recorrido?		0,6	0	0			
1.3 Es conocida por el personal que interviene en el proceso?		0,6	0	0			
1.4 Está establecido lo que puede fallar?		0,8	0	0			
1.5 Están definidas las verificaciones para lo que puede fallar?		0,4	0	0			
2 Existencia y aplicación de políticas	**1**						
2.1 Existen políticas escritas y formalmente establecidas aplicables a ese proceso?		0,5	0	0			
2.2 Dichas políticas, están disponibles para el personal de ese proceso?		0,5	0	0			
3 Segregación de Funciones	**1**						
3.1 Hay segregación de funciones ?		1	0	0			
4 Existencia y uso de Normativa	**1**						
4.1 Los procedimientos relativos al proceso como un todo, incluyendo las distintas unidades que intervienen, existen?		0,4	0	0			
4.2 Estos procedimientos, se difunden de una manera que permita sean conocidos por el personal?		0,3	0	0			
4.3 Los procedimientos están actualizados?		0,3	0	0			
5 Niveles de autorización	**1**						
5.1 Existen formalmente establecidos los niveles de autorización?		1	0	0			
6 Existencia y ejecución de acividades de control	**2**						
6.1 Existen formalmente establecidas?		2	0	0			
7 Monitoreo	**1**						

Fuente : Sr. Carlos Valdivieso Valenzuela

Procesos

Proceso :
Encargado(a):

Calidad del Ambiente de Control Interno

Item	Puntaje Total	NO	SI	N/A	Ajuste Auditoría	Respuesta Final	Observaciones
7.1 Existen los indicadores para medir el proceso?		0,5	0	0			
7.2 Existen indicadores que detecten cuando los controles se omiten?		0,5	0	0			
8 Cantidad y calidad del personal	**1**						
8.1 La impresión general es: buena, regular, mala?		1	0	0			
9 Conciliaciones y cuadraturas	**1**						
9.1 Verificar y evaluar la integridad y exactitud de la información de los sistemas operativos con los registros contables		1	0	0			
10 Control de datos	**1**						
10.1 Validar los controles establecidos para que aseguren la integridad y validez de la información que procesan las aplicaciones que usa el proceso.		1	0	0			
11 Control de cambios	**1**						
11.1 Verificar los controles establecidos para asegurarse que sólo los cambios aprobados fueron incorporados en las aplicaciones		1	0	0			
12 Seguridad TI	**1**						
12.1 Verificar los procedimientos para garantizar los accesos y uso de la información		1	0	0			
13 Control de Informes emitidos (cualquier output)	**1**						
13.1 Hay evidencias de revisión?		1	0	0			
14 Observaciones de Auditorias	**2**						
14.1 Se resuelven oportunamente las observaciones de auditoria (hasta 6 meses)?		2	0	0			
Suma	**18**						

Suma de Puntajes		
Puntaje 1 en scoring	0-3 puntos	1
Puntaje 2 en scoring	4-6	2
Puntaje 3 en scoring	7-9	3
Puntaje 4 en scoring	10-12	4
Puntaje 5 en scoring	13-18	5

Cruce de un Proceso con el Riesgo “Cumplimiento de normas y procedimientos”

Riesgo	Proceso	Puntaje del Proceso	Puntaje del Riesgo	Puntos de Riesgo del cruce
5.01 Cumplimiento de normas y proced	04 Cuenta Corriente	122,40	1,50	183,60

Actividades de Control	Puntos Act. de Control	Cat 1 Fact 0	Cat 2 Fact 0,25	Cat 3 Fact 0,5	Cat 4 Fact 0,75	Cat 5 Fact 1	Puntos de Riesgos no mitigados
Act. De Control 1	62,2		X				15,55
Act. De Control 2	89,1			X			44,55
Act. De Control 3	32,3	X					0
	183,6						**60,1**

Categoría 1 : Cumple con toda la actividad y en todos los casos; FM=0
Categoría 2 : Cumple con la gran mayoría de las actividades y de los casos; FM=0,25
Categoría 3 : Cumple cerca del 50% del control y de los casos a los que se aplica; FM=0,5
Categoría 4 : Cumple sólo una parte de la actividad de control y se aplica en pocos casos; FM=0,75
Categoría 5 : No cumple con la actividad de control; FM=1

Fuente : Sr. Carlos Valdivieso Valenzuela

EJEMPLO DIDACTICO

Puntos de riesgos potenciales

Procesos	Riesgo 1	Riesgo 2	Riesgo 3	Riesgo 4	Otros (detallar)	Total	%
Colocaciones	900	800	1400	1000	900	5000	33,33
Inv Financieras	800	700	800	600	1100	4000	26,67
Cuenta Corriente	700	600	300	200	200	2000	13,33
Captaciones	1200	300	500	800	200	3000	20,00
Otros (detallar)	400	200	100	200	100	1000	6,67
SUMA	**4.000**	**2.600**	**3.100**	**2.800**	**2.500**	**15.000**	**100,00**
% Potencial	26,67	17,33	20,67	18,67	16,67		100,00

Puntos de riesgos residuales

Procesos	Riesgo 1	Riesgo 2	Riesgo 3	Riesgo 4	Otros (detallar)	Total	%
Colocaciones	200			100		300	6,00
Inv Financieras	100		200		200	500	12,50
Cuenta Corriente		100		200		300	15,00
Captaciones		100		100		200	6,66
Otros (detallar)		200		200		400	40,00
SUMA	**300**	**400**	**200**	**600**	**200**	**1700**	
%	17,65	23,53	11,76	35,29	11,76	100,00	
Puntos potenciales	4.000	2.600	3.100	2.800	2.500	15.000	
% Residual	**2,00**	**2,67**	**1,33**	**4,00**	**1,33**	**11,33**	

Fuente : Sr. Carlos Valdivieso Valenzuela

TENER UN INDICADOR UNICO Y CUANTITATIVO DE RIESGO POTENCIAL Y DE RIESGO RESIDUAL

- Recomiendo tener un modelo e ir perfeccionándolo en el tiempo.
- Cuando Uds. lleguen a puntos y un porcentaje, el modelo debe indicar los procesos y actividades de control donde están esos puntos y establecer planes de acción.
- Deben hacerse evaluaciones cada cierto tiempo; es indispensable definido el modelo, tener un software para su aplicación.
- Una vez más, este no es un trabajo que lidere Auditoria Interna, pero Ustedes deben verificar que exista, esté documentado y las evidencias de control.
- Mi experiencia por años, es que es un tema motivador.

FIN DE LA PRESENTACION

- Gracias por vuestra atención.
- Recordemos que la ISO 31.000 dice que cada empresa debe hacer su propio ejercicio de cómo desarrollarla e implementarla.
- Esta ISO aporta un marco de referencia y es una valiosa guía para Auditoría Interna tanto en su rol de assurance como de consulting.
- Ahora dejemos el tema instalado en CLAIN e iniciemos brevemente, por las limitaciones de tiempo una conversación, que espero pueda seguir en meses siguientes en CLAIN.