



GESTION Y REGULACION DEL RIESGO OPERACIONAL



OSCAR BASSO WINFFEL
Ciudad de Guatemala, GUATEMALA
Julio del 2017

Stakeholders del Area de Riesgos

La soledad... (?)



Stakeholders del Area de Riesgos

La soledad... (?)

Yo los entiendo...!



Stakeholders del Area de Riesgos

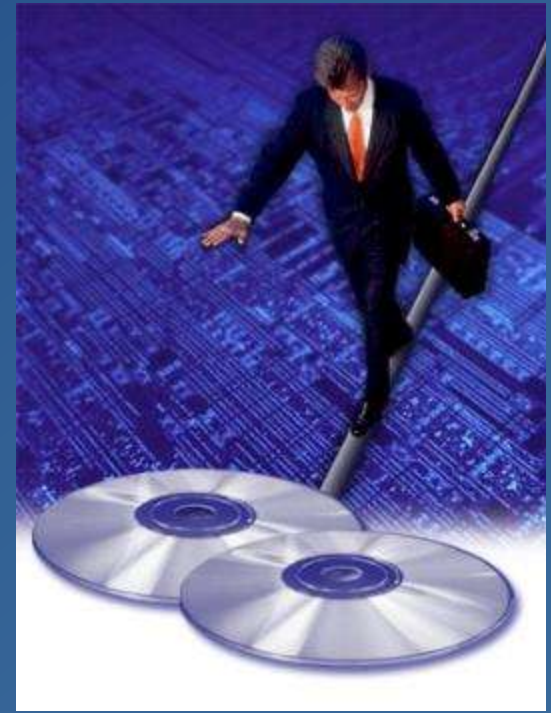
La soledad... (?)

Supuesto de Supervisor:

“El Área de Riesgos quiere hacer su trabajo...”

Elementos Básicos del Riesgo

La inherencia



A lo largo de la historia y el desarrollo

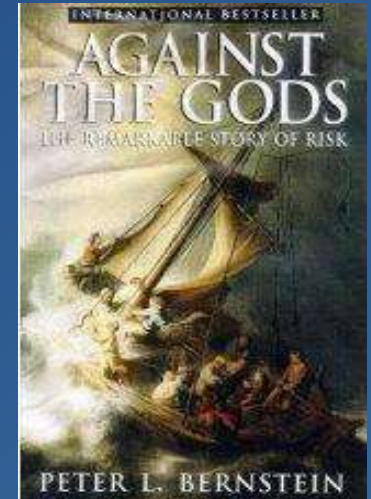


Elementos Básicos del Riesgo

La conciencia

“Against the Gods: the remarkable story of risk”

Peter Bernstein



“La idea revolucionaria que define la línea divisoria entre los tiempos modernos y el pasado es el manejo del riesgo: la noción de que el futuro es más que un improntus de los dioses y que hombres y mujeres no son pasivos frente a la naturaleza. Hasta que la humanidad descubrió el camino para cruzar esa línea divisoria, el futuro era un espejo del pasado o el oscuro dominio de oráculos o pitonisos que tenían el monopolio del conocimiento de los eventos futuros.”

Elementos Básicos del Riesgo

La continuidad

Bloomberg



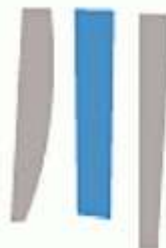
REUTERS

**Goldman
Sachs**



JPMorganChase

LEHMAN BROTHERS



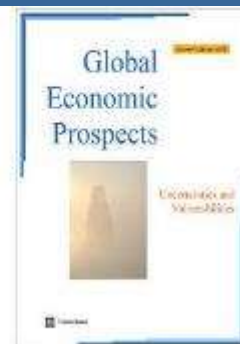
**European
Investment
Bank**



**Banco Central
de Reserva
del Perú**



Banco Mundial



Elementos Básicos del Riesgo

La amplitud y variabilidad



La reflexión de ROP fue motivada por casos especiales a mediados de los 90s

- ❑ 1995: Barings Bank (UK, 1762)
 - Quiebra por pérdida de US\$ 1.4 billones



- ❑ 1995: Daiwa Bank (Japón)
 - Pérdidas de US\$ 1.1 billones



- ❑ 1996: Sumitomo Corporation (Japón)
 - Pérdidas por US\$ 2.6 billones



- ❑ Fallas se dieron en trading y administración de portafolio:
 - Falta de segregación de funciones y supervisión
 - Ciclos largos sin revisión por terceros

Y reforzada por casos de principios de los 2000....



- ❑ Se evidencia que los Controles Internos no son suficientes:
 - Las prioridades del Directorio son distintas,
 - Puede haber mal uso de los recursos por parte de la Gerencia

Y reforzada por casos de principios de los 2000....

- Estos casos, por lo tanto, mostraban también una ausencia de “buen Gobierno Corporativo”



Y reforzada por casos de principios de los 2000....

□ En términos de Gobierno Corporativo se hace prioritario evaluar:

- Políticas de gobierno y gestión de RIESGOS
- Controles Internos – Disciplina de gestión
- Código de Conducta Ética
- **Cultura de riesgos – Comité**
- Transparencia de información
- *Accountability*
- Dirección: independencia, cualificaciones, presupuesto
- Comité de Auditoría de EEFF – SOX,
- Remuneraciones y bonos

Más allá de los casos legendarios...

❑ Diversos Tipos de fallas:

- Fraude interno: Allied Irish Bank, US\$ 691 millones por trading fraudulento
- Fraude externo: Republic New York Corp., US\$ 611 millones por estafa de cliente
- Prácticas inadecuadas: Providian Financial Corp., US\$ 405 millones por ventas y facturación inapropiada
- Fallas en sistemas y procesos: Solomon Brothers, US\$ 303 millones por migración fallida de sistemas informáticos

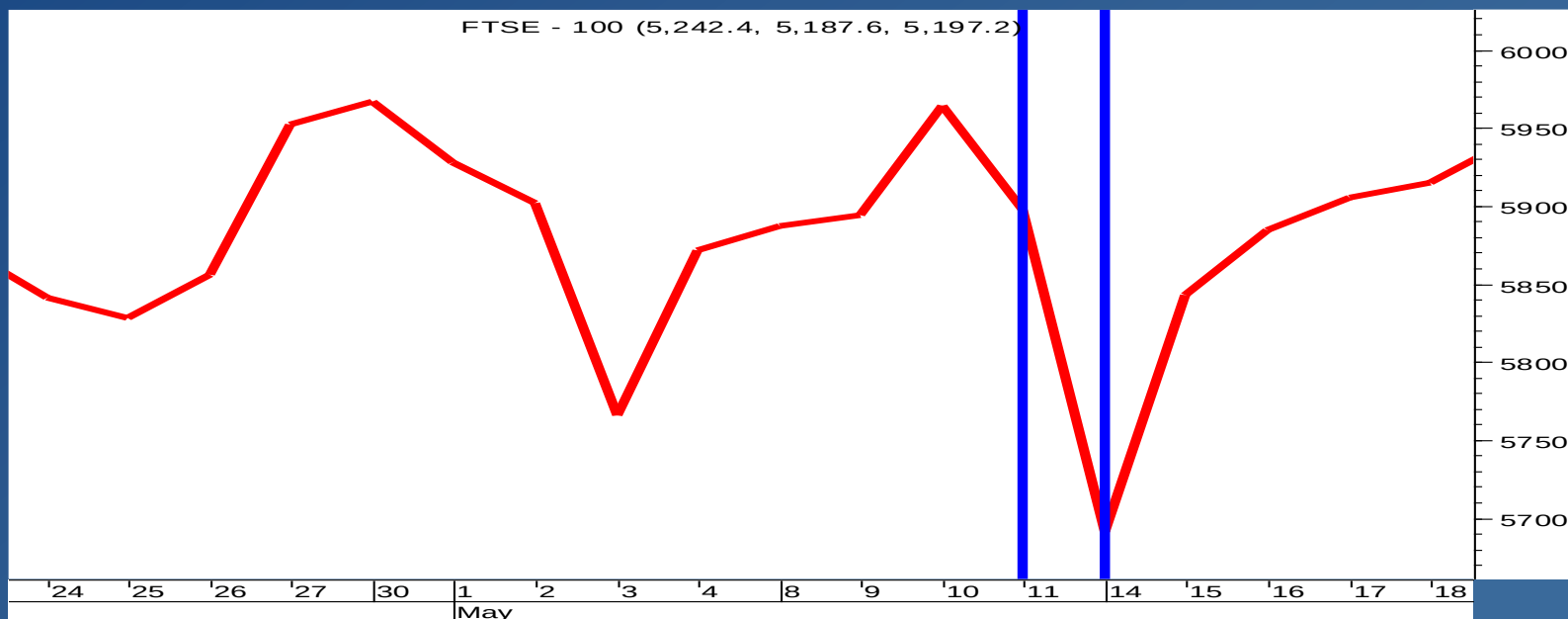
❑ En la década (98-08) más de 100 casos mayores a US\$ 100 Mill.

- ❑ Encuesta Basilea 2002: 89 bancos, reportaron más de 47,000 pérdidas mayores a US\$ 10,000. 700 casos excedieron US\$ 1 Mill.
- ❑ Encuesta Basilea 2008: 119 bancos, reportaron pérdidas de más de 65 billones y mas de 10 millones de eventos de pérdida registrados.

Más allá de los casos legendarios...

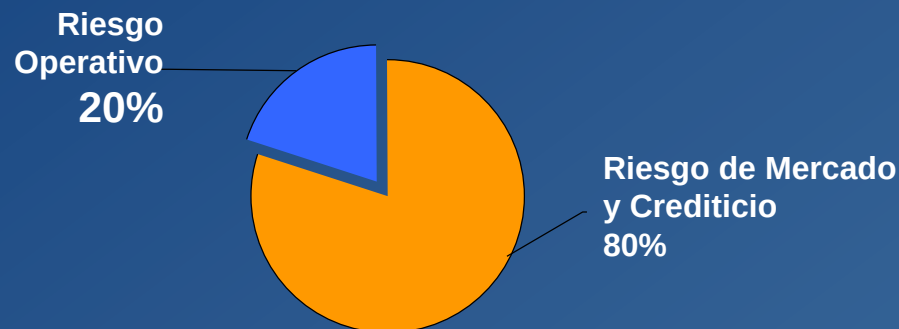
❑ Caso Lehman Brothers:

Mayo de 2001. Un broker, empleado de Lehman Brothers, al ejecutar una orden de venta, añadió un cero más a la derecha y realizó una operación de 300 millones de libras esterlinas, en lugar de los 30 millones perseguidos. La venta la ejecutó sobre un conjunto de valores del índice londinense FTSE 100, lo que provocó un descenso del índice de 120 puntos, equivalentes a unos 40 millardos de libras en pérdidas.

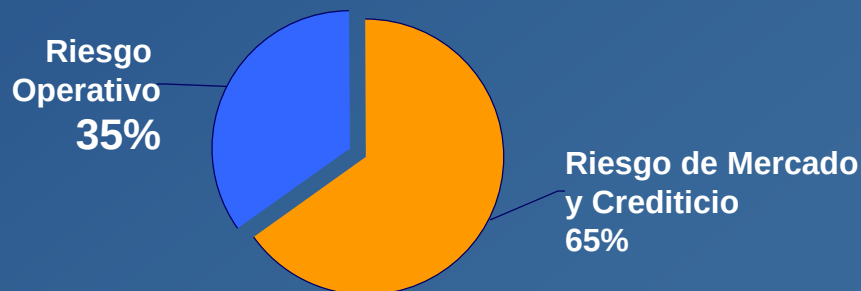


Los análisis sugieren que los ROP son mayores que lo estimado en el pasado...

Percepción años 2000



Percepción Reciente



Los análisis sugieren que los ROP son mayores que lo estimado en el pasado...

- ❑ Mayores riesgos ante mayor complejidad y magnitud de operaciones.
- ❑ Mejor identificación de riesgos
- ❑ Mejor clasificación del tipo de riesgo:
 - *Por ejemplo Barings*: riesgo de mercado (movimiento del índice Nikkei) vs riesgo de operación (falta de control en primer lugar)
 - Default de un crédito y dificultad de probar el derecho de cobro por firma no validada
- ❑ Mayor conciencia sobre costos:
 - En sólo 5 años de registro, 36 bancos internacionales registraron pérdidas acumuladas por 21 800 millones de euros*.
 - Se estima que entre 12 y 15% del capital bancario puede requerirse para cubrir este riesgo

Y hoy las cifras se exponencian... (Sanciones a Bancos por manipulación)

MAYORES SANCIONES AL SECTOR FINANCIERO

En millones de dólares

Multa	Firma	Motivo	Año
25.000	Citi, JPMorgan, BofA, Wells Fargo, Ally Financial	Hipotecas	2012
16.500	Bank of America	Hipotecas	2014
13.000	JPMorgan	Hipotecas	2013
9.300	Bank of America	Hipotecas Fannie Mae	2013
8.500	Bank of America	Hipotecas	2011
8.830	BNP Paribas	Violar sanciones económicas	2014
7.000	Citi	Hipotecas	2014
5.100	JPMorgan	Hipotecas	2013
4.300	Citi, JPMorgan, BofA, HSBC, RBS y UBS	Manipular divisas	2014
2.600	Morgan Stanley	Hipotecas	2015
2.500	Credit Suisse	Evasión fiscal	2014
2.120	Citi, JPMorgan, RBS, Societe Generale, Deutsche Bank y RP Martin	Manipular Libor y Euribor	2013
2.042	Barclays, HSBC, RBS y otros 7 bancos	Mala asesoria	2013

Multa	Firma	Motivo	Año
1.920	HSBC	Blanqueo capitales	2012
1.700	JPMorgan	Madoff	2014
1.500	UBS	Manipular Libor	2012
1.375	Standard & Poor's	Hipotecas	2015
1.196	Commerzbank	Blanqueo	2015
920	JPMorgan	Barrera de Londres	2013
800*	Citigroup y Barclays	Divisas	2015
780	UBS	Evasión fiscal	2011
772	Bank of America	Servicios tarjetas	2014
619	ING	Violar sanciones económicas	2012
553	Deutsche Bank	Evasión fiscal	2010
550	BOCI	Fraude bancario	1991
500	RBS (ABN Amro)	Violación de sanciones	2010
410	JPMorgan	Manipular mercado eléctrico	2013
350	Lloyds	Violación de sanciones	2009
300	Standard Chartered	Violación de sanciones	2012
298	Barclays	Violación de sanciones	2010

(*) Acuerdo que previsiblemente se cerrará en los próximos días.

REGULATORS HIT 6 BANKS WITH BIG PENALTIES

TOTAL FINES (B=billions, M=millions)



Financial regulators fining banks

- Britain's Financial Conduct Authority
- U.S. Commodities Futures Trading Comm.
- U.S. Office of the Comptroller of the Currency
- Swiss financial regulator FINMA

The 16 Banks of LIBOR



Importancia y Naturaleza del ROP

Importancia



Naturaleza



Importancia y Naturaleza del ROP



Importancia

Crisis Subprime...



Importancia y Naturaleza del ROP

Importancia

Lo establecen los estándares internacionales como Basilea...

Principios básicos para una supervisión bancaria eficaz:

Principio 15 – *Riesgo operacional: los supervisores deben tener constancia de que los bancos cuentan con políticas y procesos de gestión de riesgos para identificar, evaluar, vigilar y controlar/mitigar el riesgo operacional. Estas políticas y procesos han de ser proporcionales a las dimensiones y complejidad del banco en cuestión.*

V. Consulta dic. 2011 Principio 25 – *el supervisor verifica que los bancos cuentan con un marco adecuado de gestión del riesgo operacional que tiene en cuenta su apetito por el riesgo, su perfil de riesgo y la situación macroeconómica y de los mercados. Esto incluye políticas y procesos prudentes para identificar, cuantificar, evaluar, vigilar, informar y controlar o mitigar el riesgo operacional en el momento oportuno.*

**Norma:
criterios
mínimos**

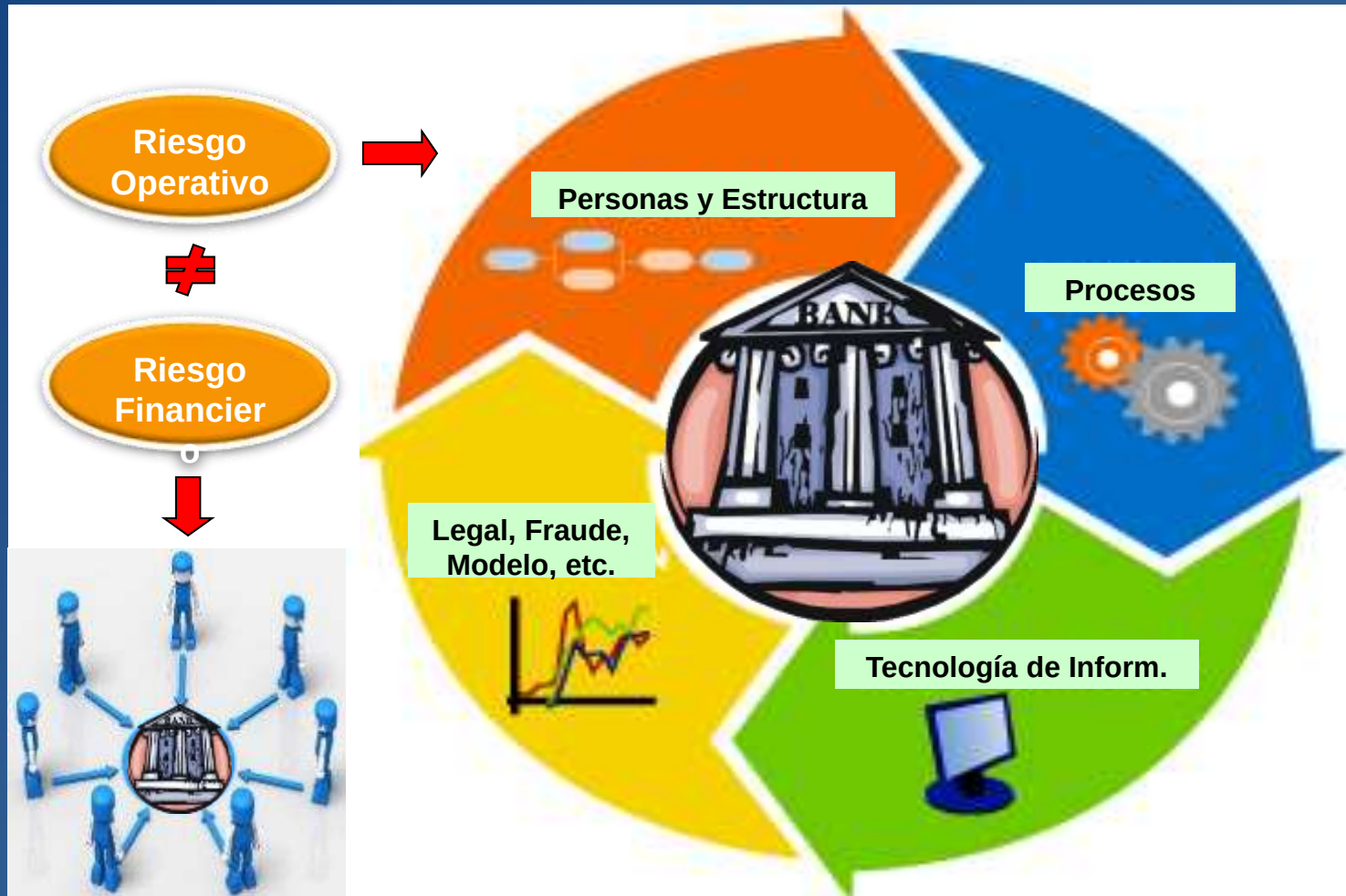


**Req. de
capital a
MP**

Importancia y Naturaleza del ROP

Naturaleza

El ROP mira al interior de la Organización.



Importancia y Naturaleza del ROP

Naturaleza

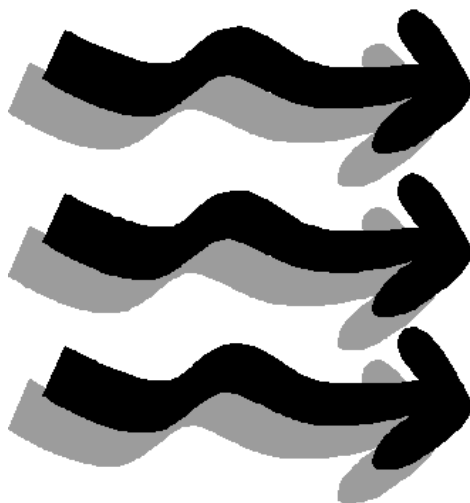
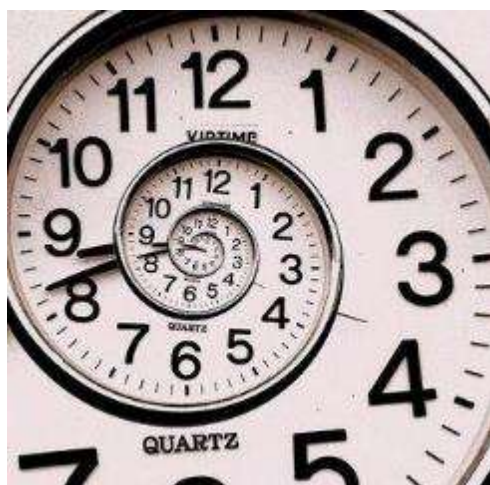
La gestión del riesgo operativo tiene una **dinámica distinta**. Implementar una gestión adecuada requiere del concurso de toda la organización y de un cambio de “cultura organizacional”



Importancia y Naturaleza del ROP

Naturaleza

La gestión del riesgo operativo tiene una **temporalidad distinta**. Implementar una gestión adecuada puede tomar de 4 a 5 años.



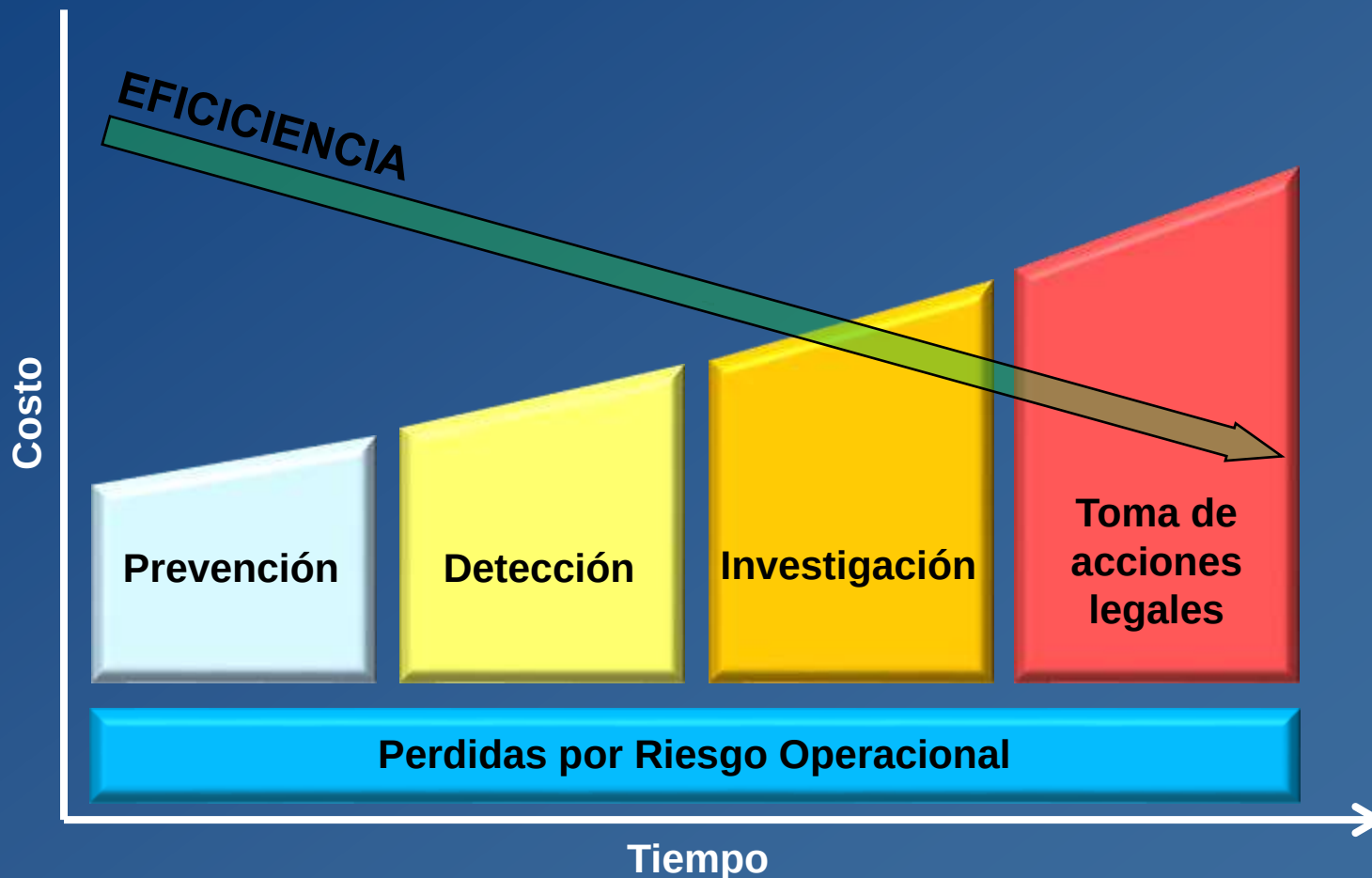
Importancia y Naturaleza del ROP

Naturaleza

Existe una **lógica inversa** en el Riesgo Operativo que no opera como en los Riesgos Financieros.



Naturaleza distinta del ROP... pero similar lógica preventiva



Evolución de la Administración del Riesgo



¿Qué es el Riesgo Operacional?



¿Qué es el Riesgo Operacional?

Tipos de enfoque

Amplia



Cualquier cosa que pueda evitar que la organización cumpla con sus objetivos

Todos los riesgos, que no son riesgos de crédito o de mercado.

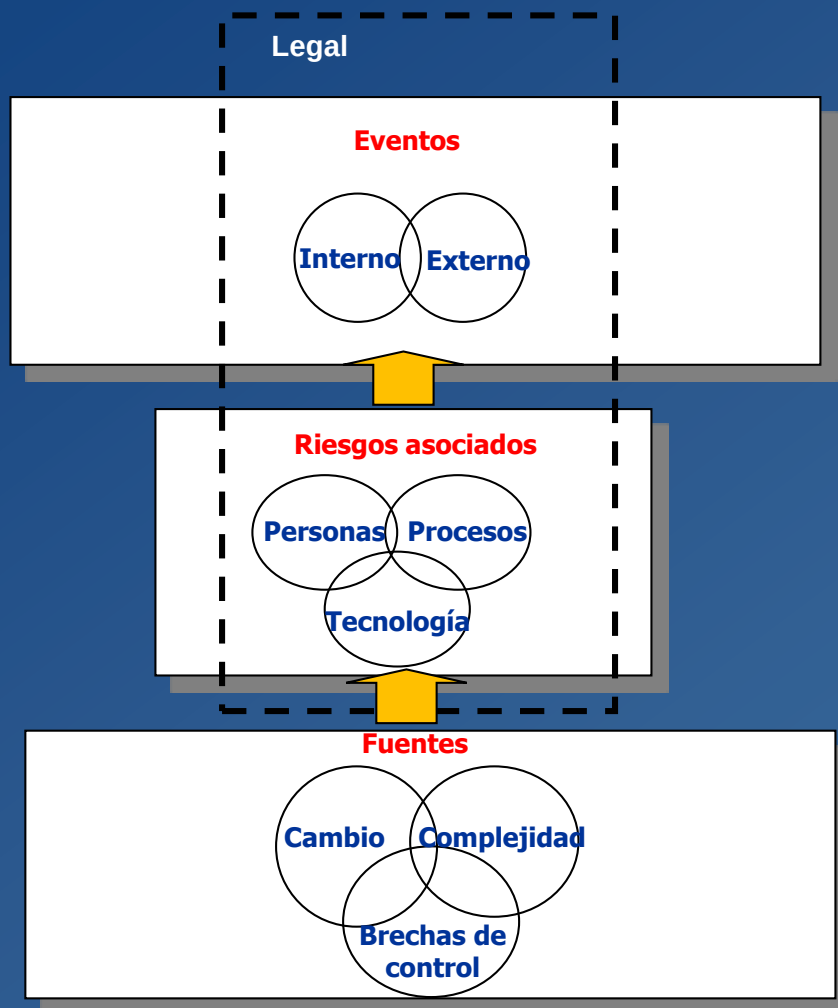
El riesgo de pérdidas por un inadecuado o fallido proceso interno, personal y fallas de sistemas o de eventos externos.

El riesgo de pérdidas originadas por un procesamiento transaccional.

Específica

¿Qué es el Riesgo Operacional?

El Comité de Basilea propuso la siguiente definición:



“ El riesgo de pérdida causado por la falla o insuficiencia de los procesos, personas y sistemas internos, o por eventos externos. Esta definición incluye el riesgo legal, pero excluye los riesgos estratégico, de reputación y sistémico”

Fuente: Prácticas Adecuadas para la Gestión y Supervisión de los Riesgos de Operación, Comité de Supervisión Bancaria de Basilea, Julio de 2002.
BANK FOR INTERNATIONAL SETTLEMENTS



¿Qué tópicos abarca el ROP?

❑ ¿Qué es Riesgo Legal? (SI)

Posibilidad de ocurrencia de pérdidas financieras debido a la falla en la ejecución de contratos o acuerdos, al incumplimiento no intencional de las normas, así como a factores externos, tales como cambios regulatorios, procesos judiciales, etc.

❑ ¿Qué es Riesgo Estratégico? (NO)

La posibilidad de pérdidas por decisiones de alto nivel asociadas a la creación de ventajas competitivas sostenibles. Se encuentra relacionado a fallas o debilidades en el análisis del mercado, tendencias e incertidumbre del entorno, competencias claves de la empresa y en el proceso de generación e innovación de valor.

¿Qué tópicos abarca el ROP?

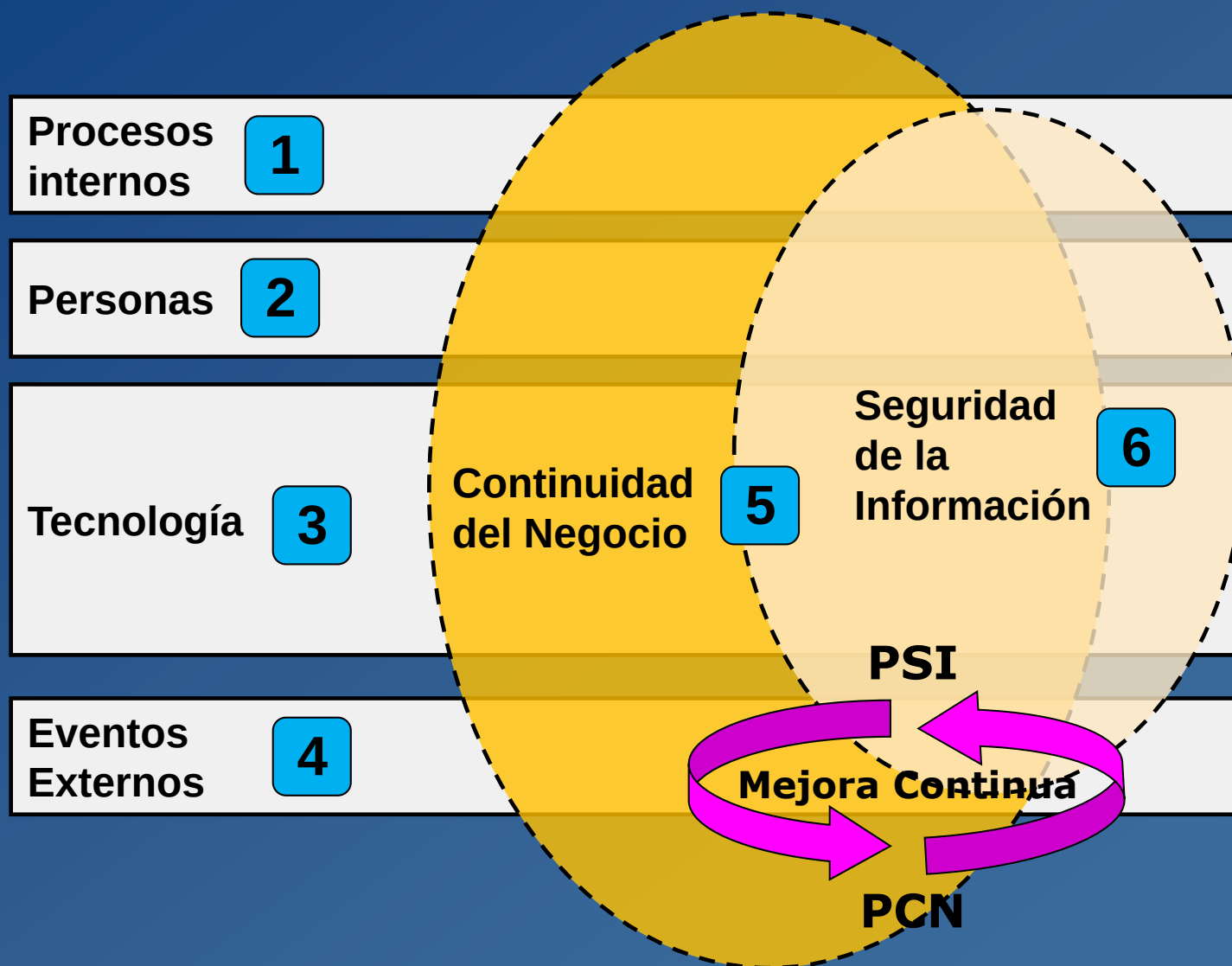
❑ ¿Qué es Riesgo Reputacional? (NO)

La posibilidad de pérdidas por la disminución en la confianza en la integridad de la institución que surge cuando el buen nombre de la empresa es afectado. El riesgo de reputación puede presentarse a partir de otros riesgos inherentes en las actividades de una organización.

❑ ¿Qué es Riesgo Sistémico? (NO)

Aquella reacción en cadena que conduce a que el riesgo de una entidad financiera de incumplir con sus obligaciones cause que otras entidades incumplan con las suyas cual si fuesen piezas de dominó interconectadas. O Alternativamente, shock macro-económico que produce efectos adversos para la mayor parte del sistema financiero.

¿Qué tópicos abarca el ROP?



¿Qué tópicos abarca el ROP?

Factores que originan el Riesgo Operacional

Personal interno

Conjunto de personas vinculadas directa o indirectamente con la ejecución de los procesos de la compañía.

- Robo
- Negligencia
- Error humano
- Fraude

- Falta de cláusulas claras en los términos de contratación

Procesos internos

Conjunto interrelacionado de actividades para la transformación de elementos de entrada en productos o servicios, para satisfacer una necesidad.

- Diseño inapropiado de procesos
- Políticas inexistentes
- Desarrollo ineficiente de operaciones

Tecnología de información

Conjunto de herramientas empleadas para soportar los procesos de la compañía (Hardware, software y telecomunicaciones)

- Uso inadecuado de sistemas y/o tecnología
- Fallas o interrupción en los sistemas

Eventos externos

Eventos asociados a la fuerza de la naturaleza u ocasionados por terceros, que escapan en cuanto a su causa y origen al control.

- Desastres
- Robo
- Contingencias legales
- Fallas en servicios críticos provistos por externos

Supervisión Basada en Riesgos y ROP



Supervisión Basada en Riesgos y ROP

- ❑ Es una metodología de supervisión que implica un cambio organizacional en la institución y cultural en todos sus miembros: radica fundamentalmente en pasar de un esquema de cumplimiento a un esquema entendimiento de la industria financiera.
- ❑ Se fundamenta en el análisis y entendimiento de los riesgos que enfrentan las EF y en los mecanismos de gestión, control y mitigación que usan para asegurar la continuidad del negocio y generar utilidades.
- ❑ La supervisión bancaria ha sido la primera en buscar adoptar el enfoque dados los lineamientos claros del Comité de Basilea. Esto se ha evidenciado tanto en supervisores integrados (que agrupan Bancos, Seguros, Pensiones y/o Valores) como especializados.



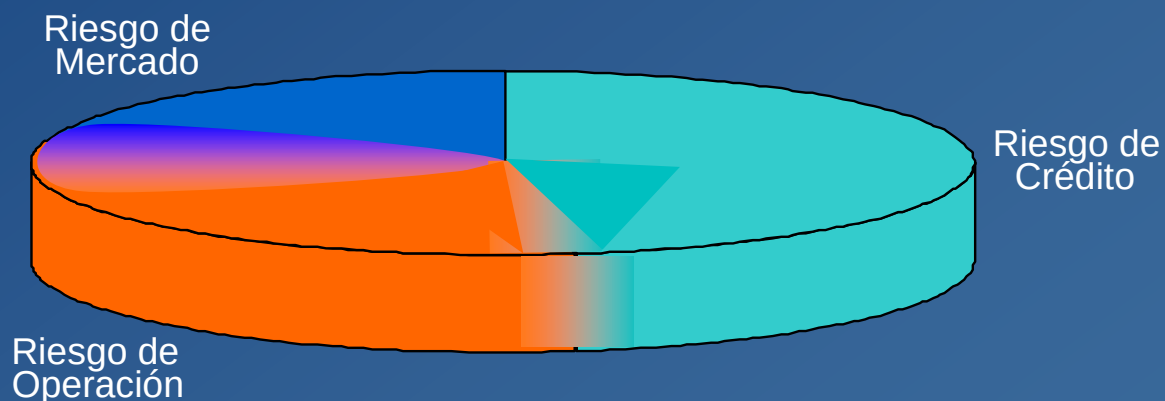
Costos de no gestionar el ROP

- Responsabilidades legales.
- Interrupción del negocio.
- Pérdidas financieras.
- Costos financieros.
- Pérdida de la reputación.
- Daño a las personas, y al entorno.
- Sanciones regulatorias.
- Suspensión del servicio al cliente.
- Salir del negocio.
- NO GESTIONAR ADECUADAMENTE LOS OTROS RIESGOS.



Costos de no gestionar ROP

- NO GESTIONAR ADECUADAMENTE LOS OTROS RIESGOS: MERCADO Y CREDITO



¡Las fronteras no son claras!

Costos de no gestionar ROP

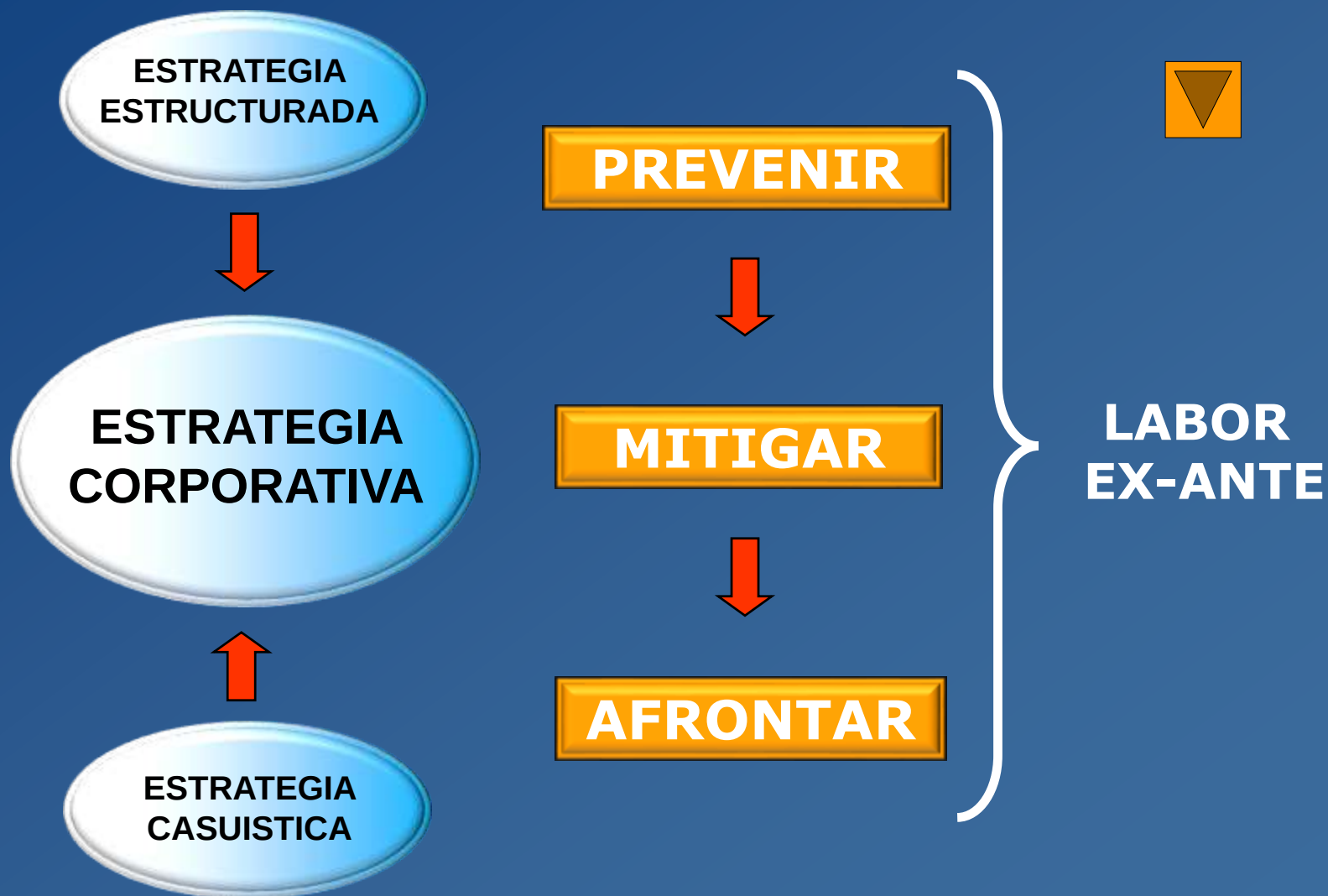
- NO GESTIONAR ADECUADAMENTE **TODOS** LOS OTROS RIESGOS



Elementos Claves para impulsar una adecuada gestión del ROP

1. Conciencia de la importancia de la gestión del ROP y de su naturaleza distinta al Riesgo Financiero.
2. Establecimiento de un Marco Normativo que incentive la Gestión.
3. Determinación del rol:
 - a. Del Supervisor.
 - b. Del Supervisado (Alta Dirección, U. de Riesgo, Institución).
4. Establecimiento de la Estrategia e Implementación de la Metodología de Gestión.

Para gestionar los ROP se debe definir la estrategia y estar preparado para:



Gestión de Riesgo Operativo



Metodología para la Gestión

Metodología de Gestión del Riesgo Operacional



Gestión de Riesgo Operativo

❑ Tipos de Gestión



Autoevaluación de Riesgos

Indicadores de Riesgo Clave (KRIs)

Procesos de Asignación del Riesgo

Tarjetas de Puntaje (Scorecards)

Análisis de Escenarios

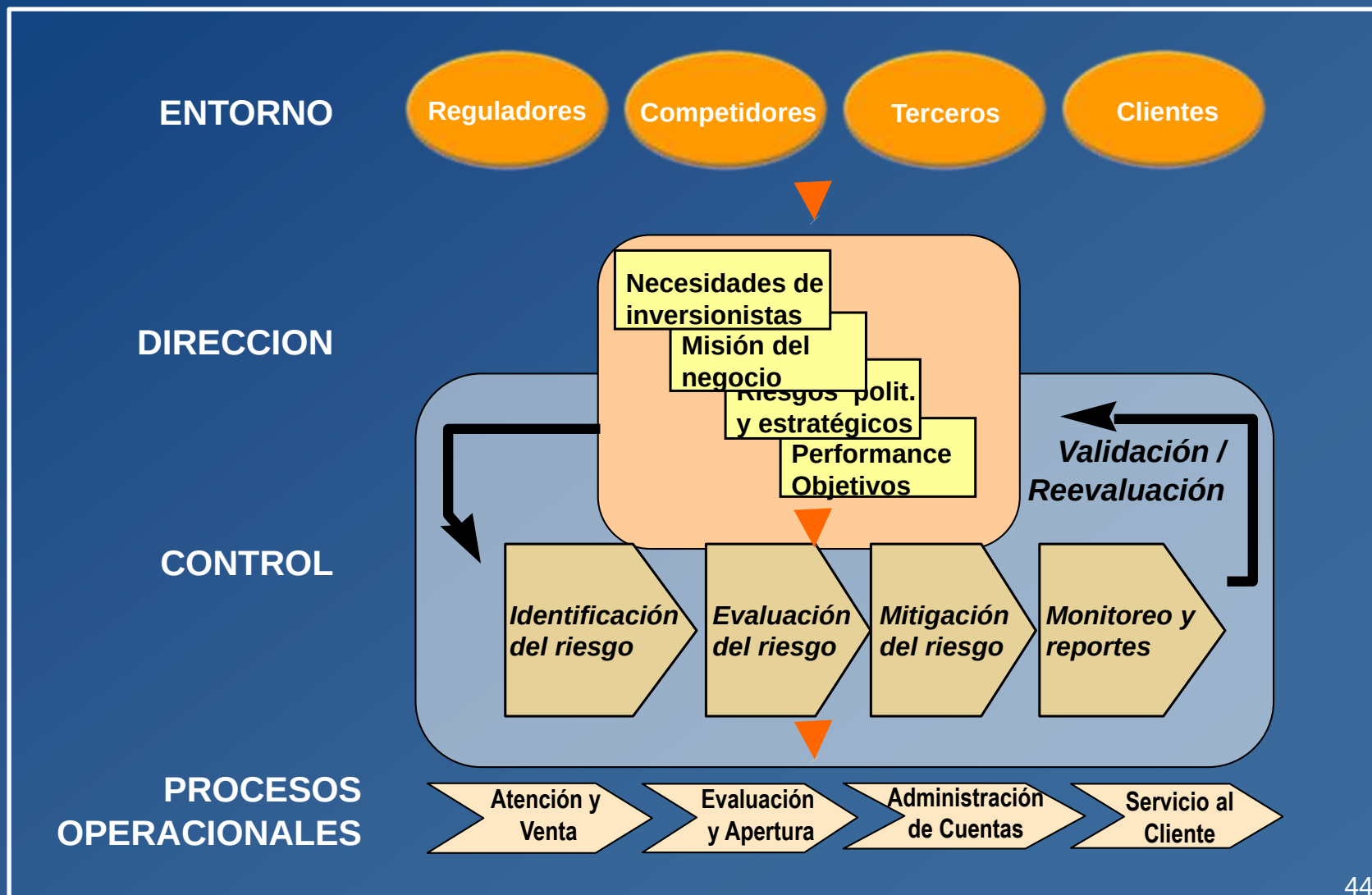
Generación de Bases de datos

Modelo de Medición Interna

Modelo de Distribución de Perdidas (LDA)

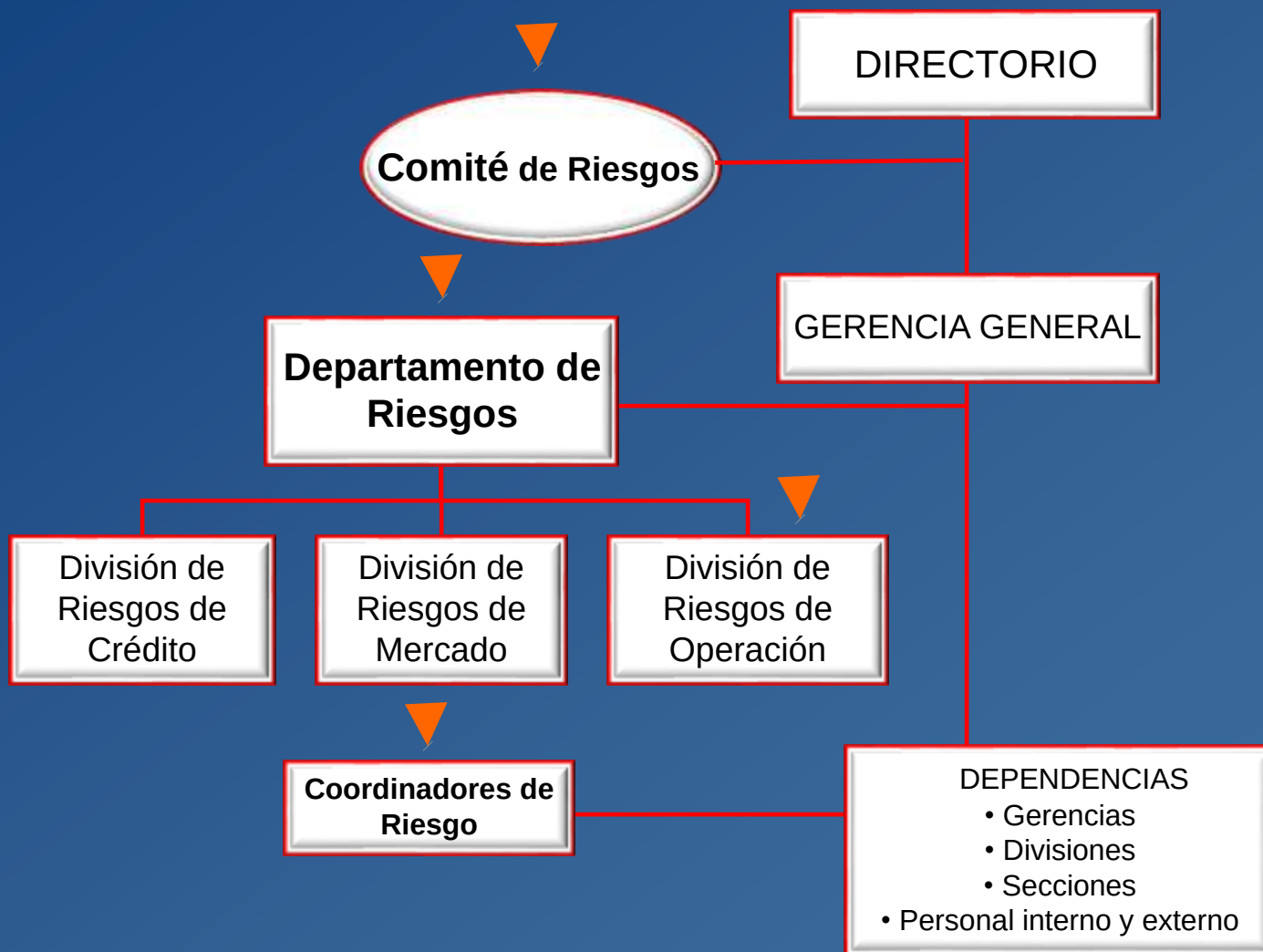
Metodología para la Gestión: GENERICO

Estructura de la Gestión



Conceptos Clave para la Gestión

□ Estructura Organizacional



Conceptos Clave para la Gestión

Pirámide del Fraude: valido para gestión de ROP?



Conceptos Clave para la Gestión

❑ Pérdidas Directas – Pérdidas Indirectas

Pérdidas Directas

Impactan directamente en los resultados. Ejemplo: El pago por multa a la Superintendencia una irregularidad.

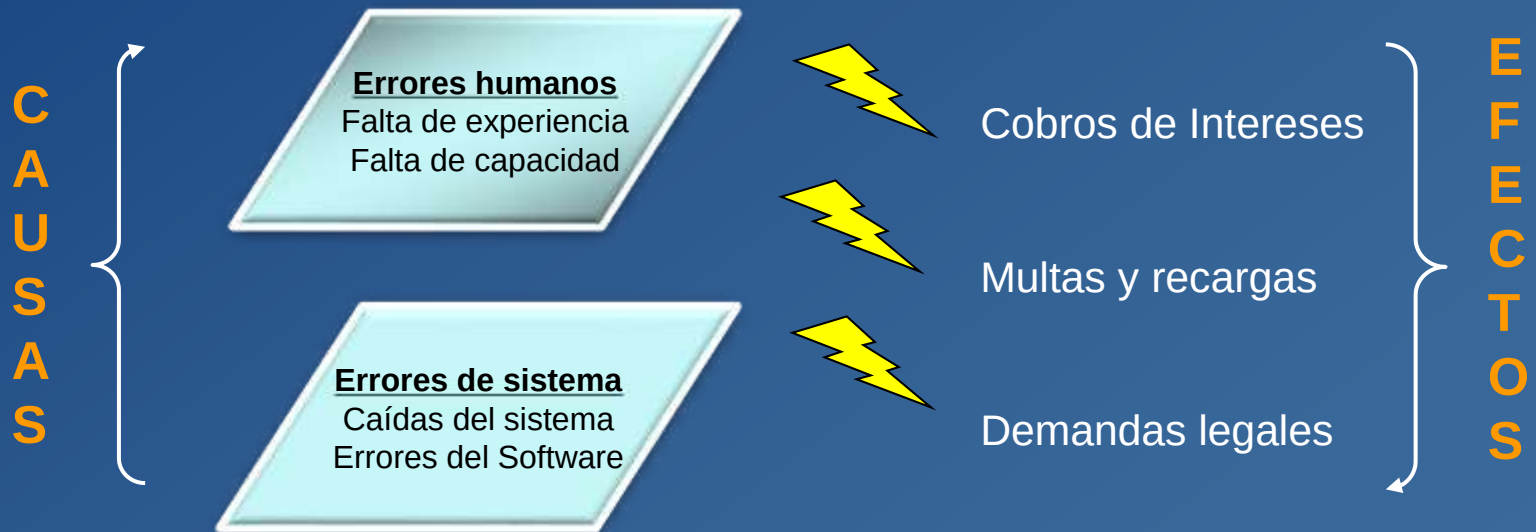
Pérdidas Indirectas

Surgen por cualquier otra causa. Ejemplo, caída de línea por lo que varias transacciones no se realizan, resultando en cobro de intereses etc.

Conceptos Clave para la Gestión

❑ Clasificación de pérdidas: Causas vs. Efectos

Las causas y efectos de los eventos operacionales son frecuentemente confundidos.



Conceptos Clave para la Gestión

□ Diferencia entre causa, evento y pérdida



Conceptos Clave para la Gestión

❑ Frecuencia y Severidad

Frecuencia (Probabilidad)

Es una medida del coeficiente de ocurrencia de un evento. Se toma como la cantidad de ocurrencias de un evento en un periodo dado.

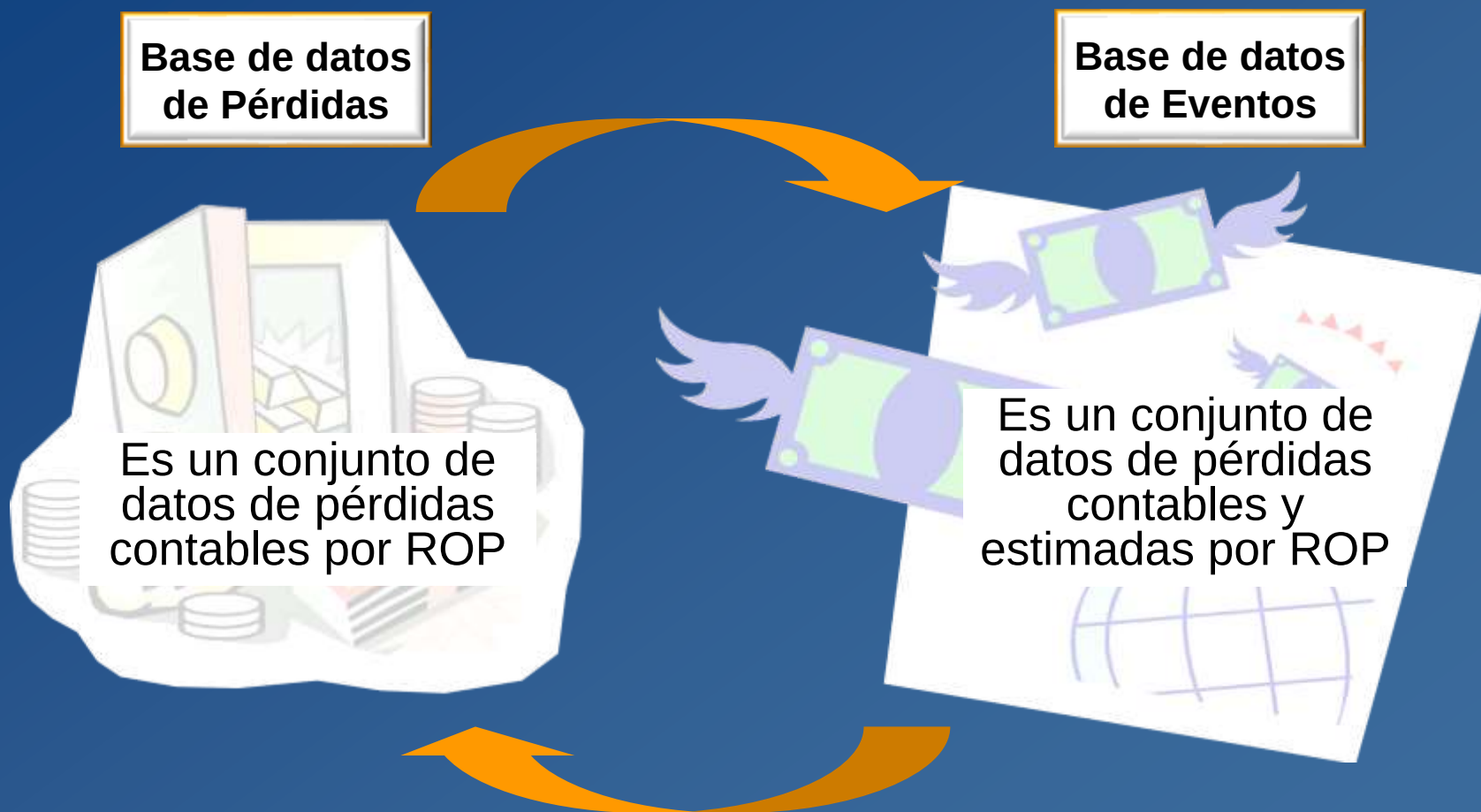


Severidad (Impacto)

Se expresa como la pérdida monetaria (calculable o estimable) como consecuencia de la ocurrencia de un evento.

Conceptos Clave para la Gestión

❑ Base de datos de pérdidas



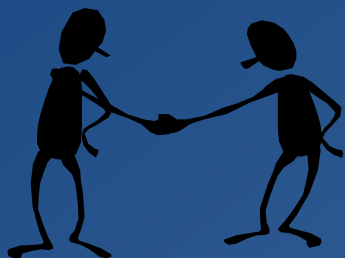
Metodología para la Gestión: GENERICO



1. Identificación de Riesgos

Dependencia de los procesos

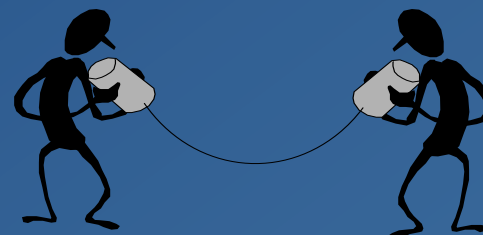
- Las estrategias establecidas por la Alta Dirección son aplicadas a través de uno o más procesos, los cuales son dependientes de uno o más recursos:



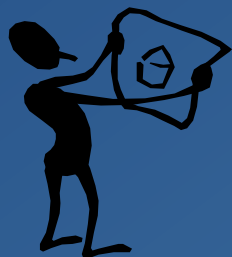
Terceros



Personas



Información



Procedimientos



Activos

1. Identificación de Riesgos

Dependencia de los procesos

- Problemas con los recursos requeridos para asegurar la integridad y confiabilidad de los procesos pueden ser eventos generadores de pérdidas



1. Identificación de Riesgos

Dependencia de los procesos

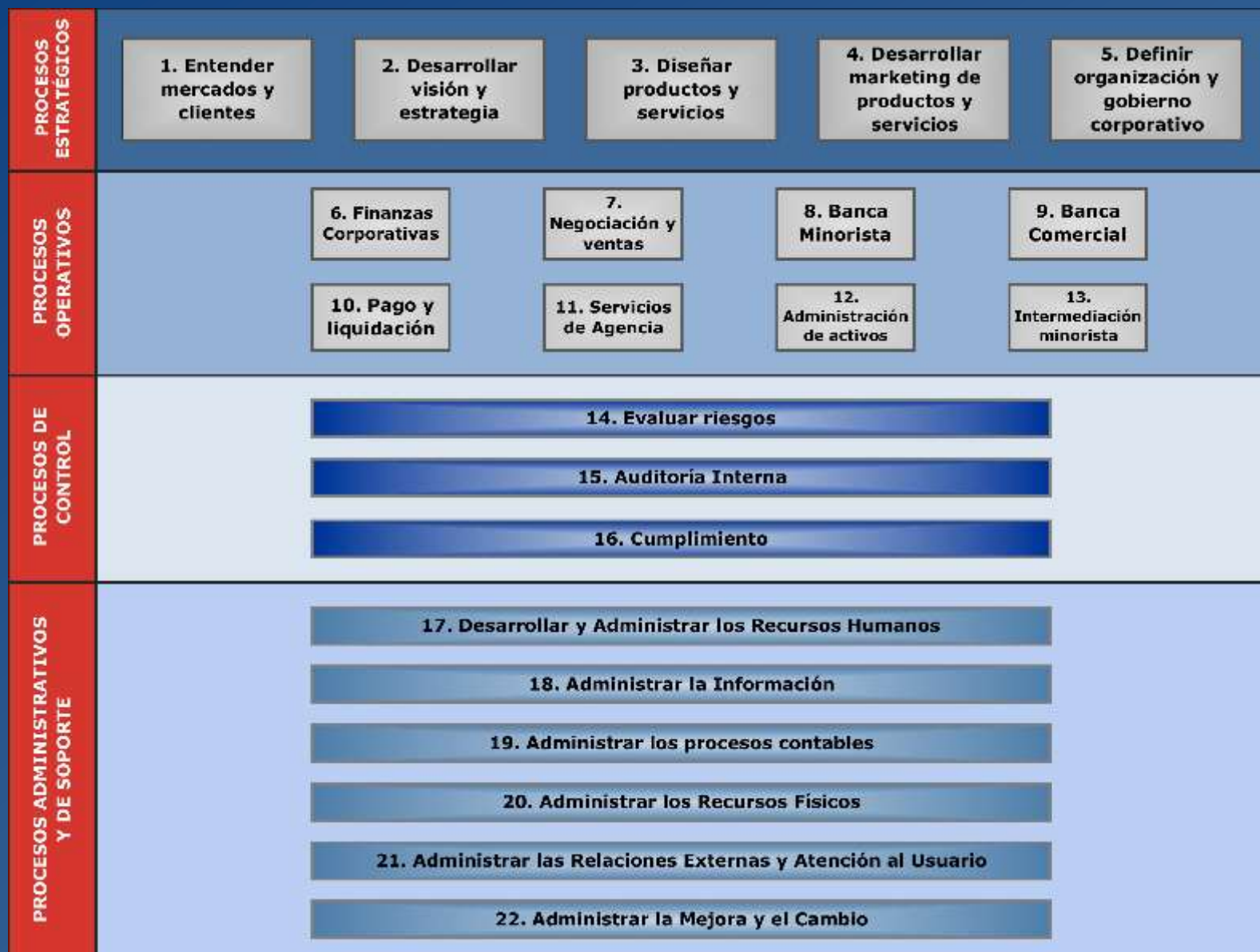
- Podría llevar a que “cosas malas sucedan o que las buenas cosas no sucedan”
- Un evento que daña y desestabiliza los recursos que soportan el proceso.

<u>Tipo de riesgo :</u>	<u>Ejemplos :</u>
• Procesos →	• Fallas de software
• Eventos Externos →	• Fuego, inundación, vandalismo
• Honestidad →	• Fraude



1. Identificación de Riesgos

Modelo de Procesos Bancarios



1. Identificación de Riesgos

Dependencia de los procesos



Las buenas prácticas establecen que para levantar eventos de riesgos es ideal a partir del análisis de los PROCESOS.

Para que esto resulte adecuado la Institución debe contar con procesos FORMALES, ACTUALIZADOS y FORMALIZADOS.

Cuando lo anterior no se produce, un segundo óptimo es utilizar las UNIDADES DE NEGOCIO o Áreas.



1. Identificación de Riesgos

Utilizando Basilea: Tipologías

TIPOLOGIAS DEL RIESGO OPERACIONAL		
Factor Potencial	Eventos	Ejemplos
<i>Fraude Interno</i>	Actos destinados a defraudar, usurpar la propiedad o evadir la regulación, la Ley o las políticas de la empresa que involucren al menos una parte interna	Reportes de posiciones intencionalmente errados
		Defraudación de empleados
<i>Fraude Externo</i>	Actos por parte de terceros destinados a defraudar, usurpar la propiedad o evadir la Ley	Negociación con Información privilegiada por parte de un empleado
		Robo y Falsificación
		Emisión de cheques sin fondos
<i>Prácticas de empleo y seguridad del ambiente de trabajo</i>	Actos ilegales frente a las normas laborales que resulten en pagos por perjuicios al personal o reclamos por seguridad o por salud.	Intrusión en los sistemas de comunicación e información
		Reclamos por compensación de trabajadores
		Pagos por violación a normas de salud o seguridad de empleados
<i>Prácticas Relacionadas con los clientes, los productos y el negocio</i>	Fallas negligentes o no intencionadas que impidan cumplir con las obligaciones profesionales con clientes específicos o derivadas de la naturaleza del diseño de un producto	Obligaciones derivadas de reclamos de terceros por razones de seguridad
		Brechas fiduciarias
		Mal manejo de información confidencial de clientes
		Actividades de negocio inapropiadas o cuenta del banco
		Lavado de activos
<i>Daño a los Activos Físicos</i>	Pérdida o daño a los activos físicos debido a desastres naturales u otros eventos	Venta de productos no autorizados
		Vandalismo, terrorismo
		Terremotos
<i>Interrupción del Negocio y Fallas en los Sistemas</i>	Interrupción en las actividades del negocio o fallas en los sistemas de información	Incendios e inundaciones
		Fallas en el hardware o software
		Problemas en las telecomunicaciones
<i>Administración de la Ejecución, la Entrega y el Proceso</i>	Fallas en el procesamiento de transacciones o en la administración del proceso y en las relaciones con las contrapartes y los proveedores.	Corte en el suministro de servicios públicos
		Errores en la grabación de datos
		Fallas en la administración de colaterales
		Documentación legal incompleta
		Acceso no aprobado a las cuentas de los clientes
		Desempeño inadecuado de las contrapartes no clientes
		Disputa con los proveedores

Fuente: *Prácticas Adecuadas para la Gestión y Supervisión de los Riesgos de Operación*. Comité de Supervisión Bancaria de Basilea, Julio de 2002. BANK FOR INTERNATIONAL SETTLEMENTS

1. Identificación de Riesgos

Utilizando Basilea: Tipologías y Factores

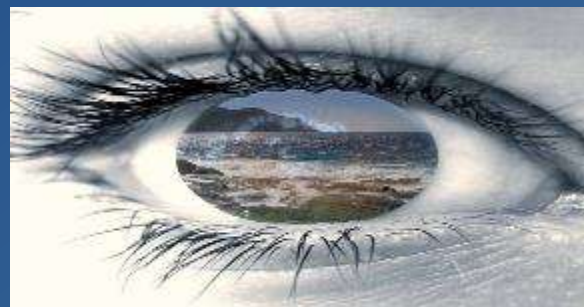
TIPOLOGIAS DE RIESGO	CATEGORIAS	FACTORES DE RIESGO ASOCIADOS
Fraude Interno	Actividades no Autorizadas	Personas , Procesos, Tecnología
	Hurto y Fraude	
Fraude Externo	Hurto y Fraude	Tecnología , Eventos externos, Procesos
	Seguridad de los Sistemas	
Relaciones laborales y seguridad en el puesto de trabajo	Relaciones Laborales	Personas
	Higiene y seguridad en el trabajo	
	Discriminación	
Clientes, productos y prácticas empresariales	Adecuación, divulgación de información y confianza	Personas , Procesos, Tecnología
	Prácticas empresariales o de mercado improcedentes	
	Productos Defectuosos	
	Selección, patrocinio y riesgos	
	Actividades de Asesoramiento	
Daños a activos materiales	Desastres y otros acontecimientos	Eventos externos
Fallas tecnológicas	Sistemas	Tecnología
Ejecución, entrega y gestión de de procesos	Recepción, ejecución y mantenimiento de operaciones	Procesos , Personas , Eventos externos
	Seguimiento y presentación de informes	
	Aceptación de clientes y documentación	
	Gestión de cuentas de Clientes	
	Contrapartes comerciales	
	Distribuidores y Proveedores	

1. Identificación de Riesgo

Tipos de Eventos

**EVENTOS
POTENCIALES**

Lo que NO ha ocurrido pero puede ocurrir.



**INCIDENCIAS
DE RIESGO**

Lo que ha ocurrido y puede VOLVER a ocurrir.



1. Identificación de Riesgos

Registro de Incidencias de Riesgo

RIR - Sistema de Registro de Incidencias de Riesgo
MÓDULO DE VALIDACION DE USUARIO

Bienvenidos al Sistema de Registro de Incidencias de Riesgo

Para acceder al sistema RIR, regístrese con su Usuario y Contraseña.

Usuario:
Contraseña:

¿Sabes de algún riesgo en el Banco? [Regístrate](#)

Si no puede acceder al sistema sírvase comunicarse con el Señor César Condori al número de red 12382 o al correo riesgo@bcr.com.pe

REGISTRO DE INCIDENCIAS DE RIESGO (RIR)									
								FECHA :	
DEPARTAMENTO									
DIVISION/SECCION									
AGENCIA/DEPENDENCIA									
RESPONSABLE DEL REPORTE									
PRIORIDAD DEL REPORTE		Alta		Media		Baja		PERIODO	
CARACTERISTICAS DE LAS INCIDENCIAS									
Descripción de la Incidencia o incidente (acciones conducentes, causas)	Detalle del daño/perjuicio (Estimar pérdida actual en Soles)	Detalle de Circunstancias tiempo/lugar/fecha, identificado por		Acciones inmediatas de respuesta por parte del administrador		Observaciones (prevención, frecuencia, afectados, resultado crítico)			

1. Identificación de Riesgos

Registro de Eventos Potenciales

Auto
evaluación
(AERO)

UNIDAD # 1						ALTO
Evaluación de Riesgo DEPARTAMENTO DE CONTABILIDAD <i>Perfil Total</i>		Coordinadores de Riesgo - Debrief 1				
COSTO ASIGNADO:		GERENTE:				NIVEL
COORDINADOR DE RIESGO:		# PERSONAL:				DE RIESGO
ACTIVIDADES		CONDUCTORES DE RIESGO CLAVE				
CATEGORIA	FREQ	RIESGO NETO	CONTROLES	EVENTO DE PERDIDA?		
PERSONAS	ALTO	ALTO	BAJO	SI		
PROCESOS	ALTO	ALTO	BAJO	SI		
TECNOLOGIA	MEDIO	MEDIO	BAJO	SI		
EXTERNOS	BAJO	BAJO	BAJO	SI		
FACTORES PROMOTORES DE RIESGO						
INFORMACION IMPORTANTE ENCONTRADA						
SCORE DE RIESGO DENTRO DEL BANCO		IMPACTO VS. PROBABILIDAD				
	BAJO	MEDIO	ALTO			
Fraude						
Violación						
Personal Clave						
Operatividad						
Software						
Red						
Hacking						
Corrupción						
Procesos						
Calas Infe						
CONDUCTOR	RIESGO CRITICO					
PERSONAS						
PROCESOS						
TECNOLOGIA						
EXTERNOS						

1. Identificación de Riesgos

Mapa de Riesgos

Modelo de Administración de Riesgos Operacionales

Inventario de riesgos por proceso

Proce

Solicitud de Chequeras

Objetivos

Objetivo 1

Objetivo 2

Objetivo 3

Objetivo 4

N°	Ref. objetivo	Descripción del Riesgo	Tipo de Riesgo	I	P	Riesgo Potenc.	Control 1	Efect. 1	Riesgo Resid.	Responsable
1	1, 2, 3	Documentación presentada es falsa dando lugar a que el cliente no reconozca la transacción	Honestidad	A	B	M	Verificación de firmas en el sistema	M	M	
4	2, 3	Extravío de la solicitud de chequera / talonario de chequeras en la misma agencia.	Errores	A	B	M	Cuadre documentario a final del día	M	M	
6	3	Las características de las chequeras recibidas no concuerdan con el reporte de la imprenta.	Cumplimiento	A	B	M	Verificación visual de chequeras recibidas con el reporte de la imprenta.	A	B	
8	1,3	Chequeras recibidas con errores en la impresión de los talonarios, cantidad de cheques, numeración, etc.	Cumplimiento	A	B	M	Verificación visual de las chequeras recibidas.	A	B	

Legenda:

I - Impacto en la organización / P - Probabilidad de ocurrencia / E- Efectividad

Criterio de Evaluación: A - Alto / M - Medio / B - Bajo

1. Identificación de Riesgos

Mapa de Riesgos (detalle)

DEPARTAMENTO/OFICINA: []											
DIVISION/SECCION: []	PROCESO: []	PERIODO: []									
IMPACTO (Ejm.) Bajo= < "\$X" Medio= > "\$X" y < "\$Y" Alto= > "\$Y" PROBABILIDAD (Ejm.) Bajo = Remoto Medio = Posible Alto = Muy probable											
DEPENDENCIA OPERAC.: _____											
CATEGORIA DEL RIESGO: _____											
AMENAZA / RIESGO											
DESCRIPCION: RESPONSABLE(S): []		<table border="1" style="margin: auto;"> <tr> <td style="font-size: small;">Ind. Stress (Si/No)</td> <td style="font-size: small;">Imp.</td> <td style="font-size: small;">Obj.</td> </tr> <tr> <td style="height: 40px;"></td> <td style="height: 40px;"></td> <td style="height: 40px;"></td> </tr> </table>	Ind. Stress (Si/No)	Imp.	Obj.						
Ind. Stress (Si/No)	Imp.	Obj.									
_____ _____ _____		OBJET. NEGOCIO: [] DEPT. IMPACTADO: []									
IMPACTO: _____ _____ _____		<table border="1" style="width: 100%; text-align: center;"> <tr><th colspan="3">IMPACTO</th></tr> <tr> <td style="width: 33%;">B</td> <td style="width: 33%;">M</td> <td style="width: 33%;">A</td> </tr> <tr> <td style="height: 40px;"></td> <td style="height: 40px;"></td> <td style="height: 40px;"></td> </tr> </table>	IMPACTO			B	M	A			
IMPACTO											
B	M	A									
PROBABILIDAD DE OCURRENCIA: _____ _____ _____		<table border="1" style="width: 100%; text-align: center;"> <tr><th colspan="3">PROBABILIDAD</th></tr> <tr> <td style="width: 33%;">B</td> <td style="width: 33%;">M</td> <td style="width: 33%;">A</td> </tr> <tr> <td style="height: 40px;"></td> <td style="height: 40px;"></td> <td style="height: 40px;"></td> </tr> </table>	PROBABILIDAD			B	M	A			
PROBABILIDAD											
B	M	A									

Metodología para la Gestión: GENERICO



2. Medición de Riesgos

Probabilidad de Ocurrencia e Impacto

PROBABILIDAD (Frecuencia)

“Nunca suceden”

“Posible?”

“Casi destinado a
que sucedan /
ya suceden”

RANGO

Bajo

Medio

Alto



IMPACTO (Severidad)

“Podría no tener impacto /
impacto insignificante en el
servicio / reputación / posición
financiera / regulaciones”

“Significantes *pero* contenible”

“Extremadamente perjudicial /
casi un impacto catastrófico en
el servicio / reputación /
posición financiera/
regulaciones.”

2. Medición de Riesgos

Evaluación de Impacto

	Impacto
Alto	- Impacto financiero en el Banco que probablemente exceda \$xx millones, o - Impacto significativo en el Banco para alcanzar sus objetivos estratégicos / Operacionales, o - Alta sensibilidad política o de la comunidad
Medio	- Impacto financiero en el Banco entre \$xx y \$yy millones, o - Impacto moderado en el Banco para alcanzar sus objetivos estratégicos / operacionales, o - Sensibilidad política o de la comunidad moderada
Bajo	- Impacto financiero en el Banco entre \$xx y \$yy millones, o - Impacto mínimo en el Banco para alcanzar sus objetivos estratégicos / operacionales, o - Sensibilidad política o de la comunidad mínima

2. Medición de Riesgos

Evaluación de Probabilidad

Evaluación	Descripción	Indicadores
Alta	Probable - Probabilidad de que ocurra dentro de un periodo de un año. - Mas del 25% de probabilidad de ocurrencia	- Ocurrencia potencial varias veces en los próximos 10 años. - Ha ocurrido en los últimos dos años. - Típico de operaciones de este tipo debido a influencias externas.
Media	Posible - Probable que ocurra en los próximos 10 años. - Menos del 25% de probabilidad de ocurrencia (pero más del 2%)	- Puede ocurrir más de una vez en los próximos 10 años. - Puede ser difícil de controlar debido a influencias externas. - Historia de ocurrencias en la organización
Baja	Remota - No es probable que ocurra en los próximos 10 años. - Menos del 2% de probabilidad de que ocurra.	- No ha ocurrido en este país. - Sería sorprendente si llegara a ocurrir.

2. Medición de Riesgos

Controles Existentes

RANGO

DESCRIPCIÓN

Bajo

Los riesgos son completamente controlados y existe un pequeño riesgo o no hay riesgo de que la amenaza se materialice

Medio

La administración del riesgo puede ser mejorada y existe algún riesgo que la amenaza se materialice

Alto

Existe un riesgo significativo que la amenaza se materialice (o ya está materializada)



2. Medición de Riesgos

Criterio Cualitativo (arbitrario) Existentes

$$P + I - C = \text{Calificación}$$

Solo para
establecer
RANKING

ESCALAS RELATIVAS CUALITATIVAS PARA LA CUANTIFICACIÓN DE RIESGOS DE OPERACIÓN

Impacto								
1	2	3	4	5	6	7	8	9
Bajo			Medio			Alto		
Impacto financiero no significativo en la organización. Impacto no significativo en el servicio o la reputación. No dificulta el cumplimiento de los objetivos organizacionales			Impacto financiero moderado en la organización. Impacto significativo pero contenible. Dificulta el cumplimiento de los objetivos organizacionales			Impacto financiero en la organización extremadamente perjudicial. Impacto catastrófico en el servicio. Pone en peligro el cumplimiento de los objetivos organizacionales		

Frecuencia								
1	2	3	4	5	6	7	8	9
Baja			Media			Alta		
No ha ocurrido. Sería sorprendente si llegara a ocurrir. Su ocurrencia es remota.			Historia de ocurrencias en la organización.			Ocurrencia potencial varias veces.		

Efectividad en el Control								
1	2	3	4	5	6	7	8	9
Baja			Media			Alta		
Existe un riesgo significativo que la amenaza se materialice (o ya esta materializada) por la ineficacia o inexistencia de las medidas de mitigación implantadas.			La administración del riesgo puede ser mejorada y existe algún riesgo de que la amenaza se materialice.			Los riesgos están adecuadamente mitigados y existe una pequeña posibilidad o no hay posibilidad de que la amenaza se materialice.		

2. Medición de Riesgos

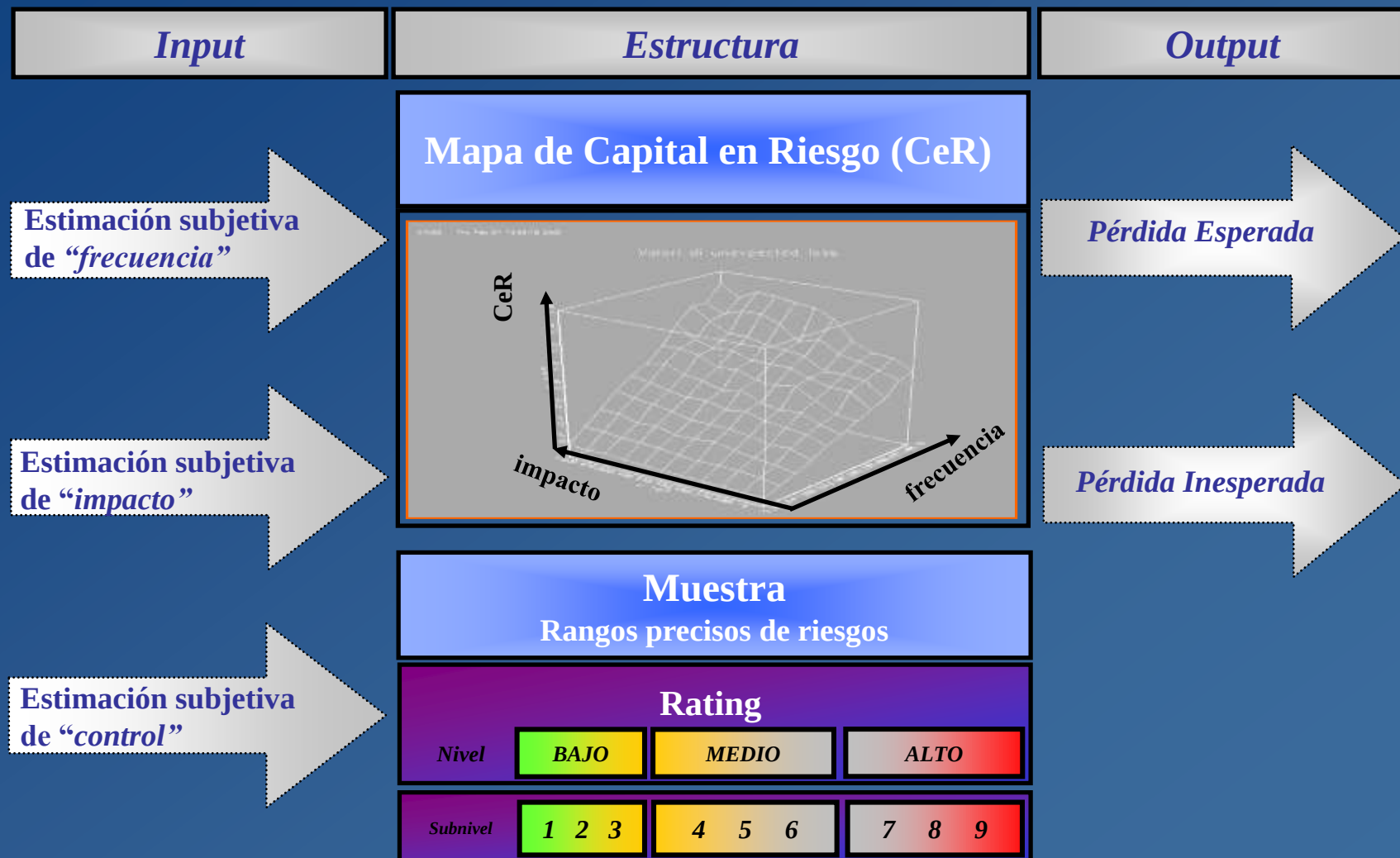
Matriz subjetiva para iniciar mitigación

Likelihood	Consequences				
	Insignificant	Minor	Moderate	Major	Severe
Almost certain	M	H	H	E	E
Likely	M	M	H	H	E
Possible	L	M	M	H	E
Unlikely	L	M	M	M	H
Rare	L	L	M	M	H

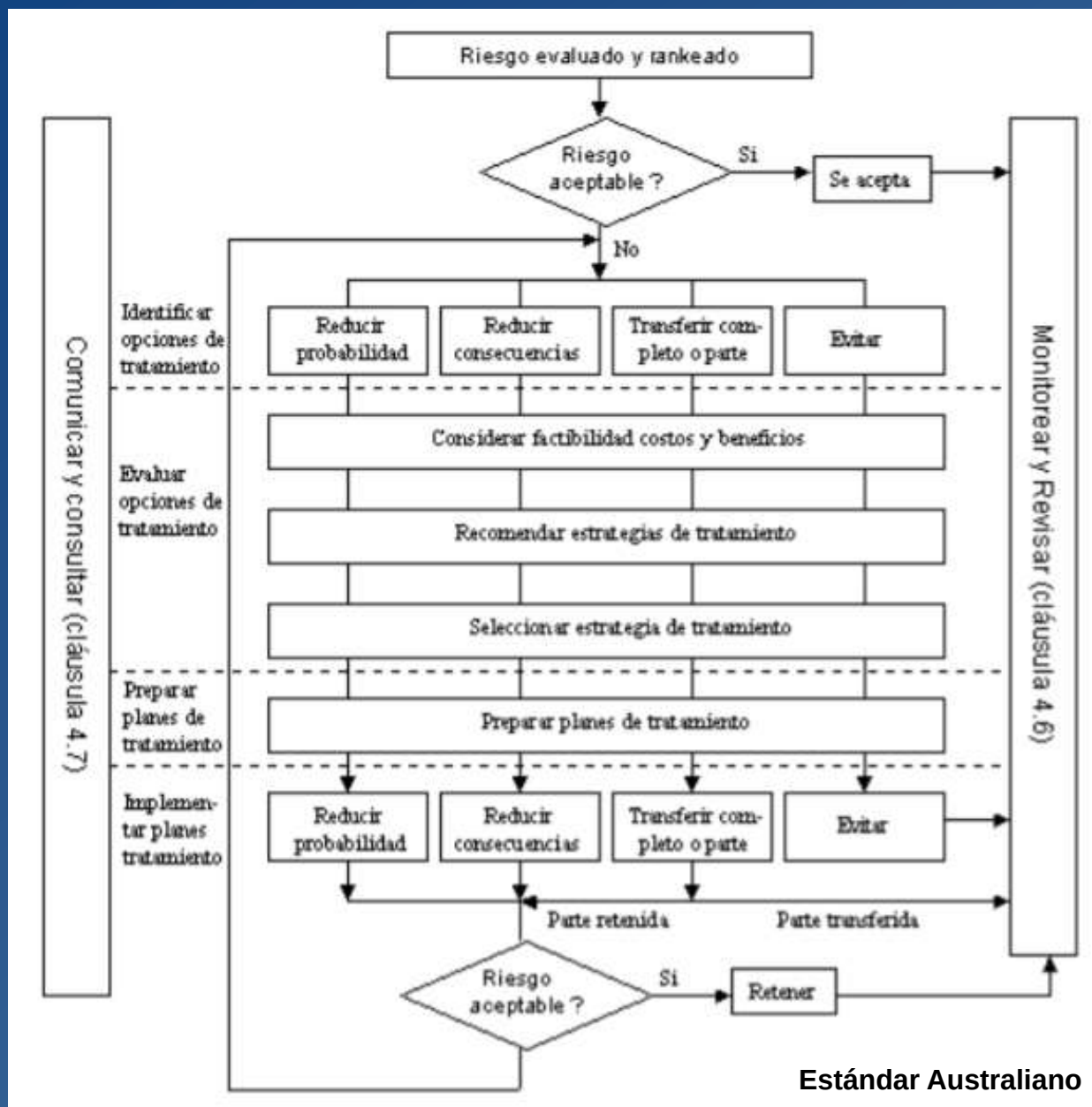
	Code	Explanation
Rating risk level	(E) (H) (M) (L)	Extreme risk - detailed action plan required High risk - needs senior management attention Moderate risk - specify management responsibility Low risk - managed by routine procedures
Likelihood	A B C D E	Almost certain - expected in most circumstances Likely - will probably occur in most circumstances Possible - could occur at some time Unlikely - not expected to occur Rare - exceptional circumstances only
Consequences	5 4 3 2 1	Severe - would stop achievement of functional goals / objectives Major - would threaten functional goals / objectives Moderate - necessitating significant adjustment to overall function Minor - would threaten an element of the function Negligible - lower consequence

2. Medición de Riesgos

Evolucion hacia el modelo

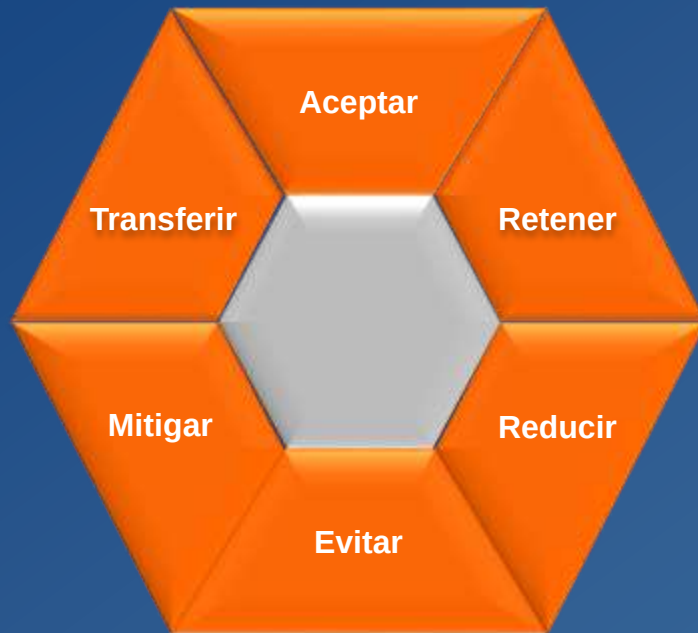


Proceso de tratamiento de los eventos



Proceso de tratamiento de los eventos

Proceso por el que se opta por una medida o combinación de medidas teniendo en cuenta el nivel de tolerancia al riesgo definido.



- **Aceptar:** aceptar niveles de riesgo altos para aprovechar oportunidades
- **Transferir:** transferir a un tercero la administración del riesgo (ej. tomar un seguro)
- **Retener:** conservar el riesgo sin tomar ninguna acción adicional más que su adecuado monitoreo
- **Mitigar:** establecer controles para disminuir el impacto del riesgo
- **Reducir:** establecer controles para disminuir la probabilidad de ocurrencia del riesgo
- **Evitar:** dejar de realizar la actividad que genera el riesgo (Subcontratar el servicio)

Metodología para la Gestión: GENERICO



3. Medidas de Mitigación

Tipos

Los mecanismos para mitigar amenazas pueden incluir:

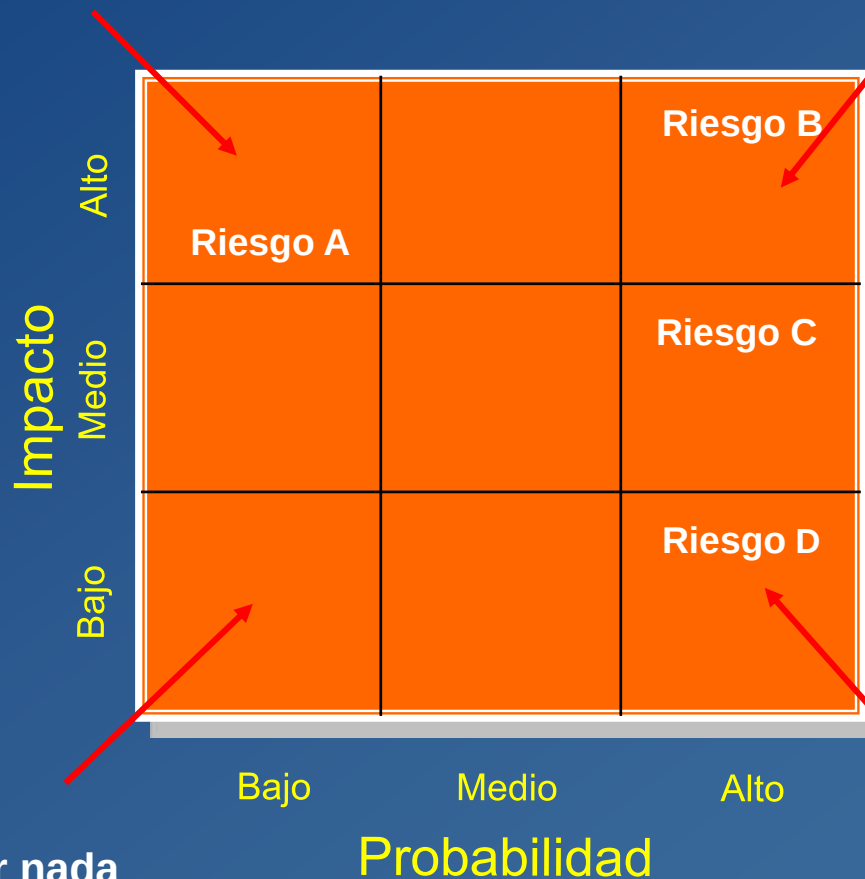
- Transferencia vía contrato (fuentes externas)
- Medidas preventivas
- Transferencia vía seguros
- Alertas tempranas y medidas de detección
- Medidas de contingencia



3. Medidas de Mitigación

Matriz de Impacto y Probabilidad

Planes de Contingencia



Estratégicos:

- Transferir el impacto vía una reponsabilidad contractual
- Transferir el impacto vía un “seguro”

?

No hacer nada
(aceptar el impacto)

Mejorar Controles

3. Medidas de Mitigación

Matriz de Impacto y Probabilidad

Riesgos a gestionar a través del **mapa de riesgos** de la entidad, al considerarse riesgos críticos, a definir en la gestión de escenarios.

Impacto	Alto	Riesgo A		Riesgo B
	Medio			Riesgo C
	Bajo			Riesgo D
		Bajo	Medio	Alto

Probabilidad

Riesgos «no gestionados», en los que la inversión para su mitigación y gestión de los mismos es superior a la pérdida que ocasionan.

Riesgos de **acción inmediata** y que en principio no se deberían identificar, ya que supondrían la no supervivencia de la entidad

Riesgos a gestionar mediante la **base de datos** de eventos de pérdidas, componiendo la pérdida esperada de la entidad en ROP

3. Medidas de Mitigación

Matriz de Impacto y Probabilidad

Entonces, el marco de gestión del ROP permite realizar una gestión activa del riesgo mediante la identificación de cuatro clases de riesgos:

- Riesgos «no gestionados», en los que la inversión para su mitigación y gestión de los mismos es superior a la pérdida que ocasionan.
- Riesgos a gestionar mediante la base de datos de eventos de pérdidas, ya que se producen de forma recurrente (alta frecuencia) pero con escaso impacto en pérdidas, componiendo la pérdida esperada de la entidad en riesgo operacional.
- Riesgos a gestionar a través del mapa de riesgos de la entidad, al considerarse riesgos críticos (de alta severidad y baja frecuencia) a definir en la gestión de escenarios.
- Riesgos de acción inmediata debido a su alto impacto en pérdida y alta frecuencia, y que en principio no se deberían identificar, ya que supondrían la no supervivencia de la entidad.

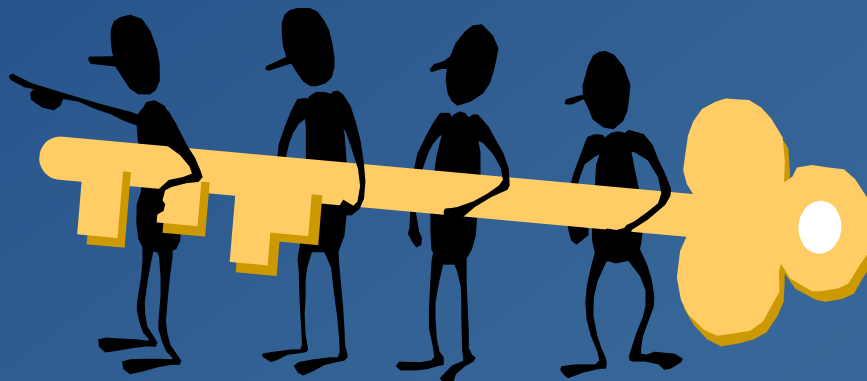
3. Medidas de Mitigación Seguros

- Medida de tratamiento: transferencia de riesgo a través del cual se intercambia un impacto financiero desconocido de eventos específicos a una tercera parte a cambio de costos financieros conocidos. Ejm: seguros, fideicomisos o titulización.
- Basilea II reconoce un máximo del 20% de la severidad para seguros. Para eventos de baja frecuencia y alta severidad.

3. Medidas de Mitigación

Plan de Acción

- Extraer riesgos que están siendo mitigados en forma inadecuada
- Considerar posibles caminos o acciones
- Asignar responsabilidades para las acciones a seguir y definir plazos para su implantación



DEPARTAMENTO/OFICINA: []

DIVISION/SECCION: []

PROCESO: []

PERIODO: []

IMPACTO (Ejm.) Bajo= < "\$X" Medio= > "\$X" y < "\$Y" Alto= > "\$Y"
PROBABILIDAD (Ejm.)Bajo = RemotoMedio = Posible Alto = Muy probable

DEPENDENCIA OPERAC.: _____

CATEGORIA DEL RIESGO: _____

AMENAZA / RIESGO

DESCRIPCION:RESPONSABLE(S): []

OBJET. NEGOCIO: []

DEPT. IMPACTADO: []

Ind. Stress
(Si/No)

Imp.

Obj.

IMPACTO:

IMPACTO

B

M

A

PROBABILIDAD DE OCURRENCIA:

PROBABILIDAD

B

M

A

MEDIDAS DE MITIGACION

EFECTIVIDAD

DESCRIPCION

RIESGO
POTENCIAL

EFECTIVIDAD

RIESGO
RESIDUAL

PLAN DE ACCION

Estado (Pendiente, en
proceso, completado)

Plazo

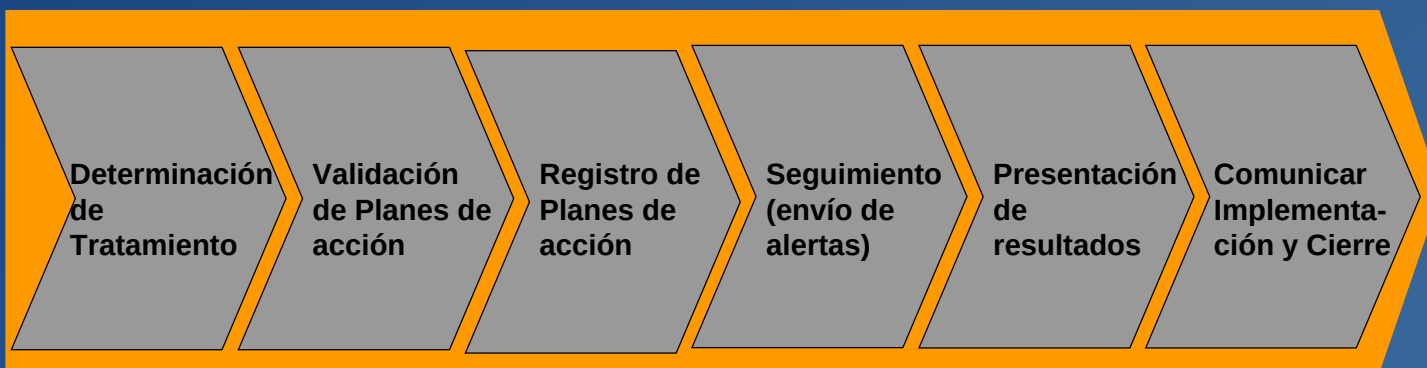
RESPONSABLE

*

Planes de Acción: mitigación o monitoreo?

Planes de Acción generados por:

- Eventos de pérdida
- Superación de umbrales en KRIs
- Nuevos Productos / Cambios Significativos



Matriz de Tratamiento



Comité de RO



Coordinador RO /Unidad de RO



Sistema



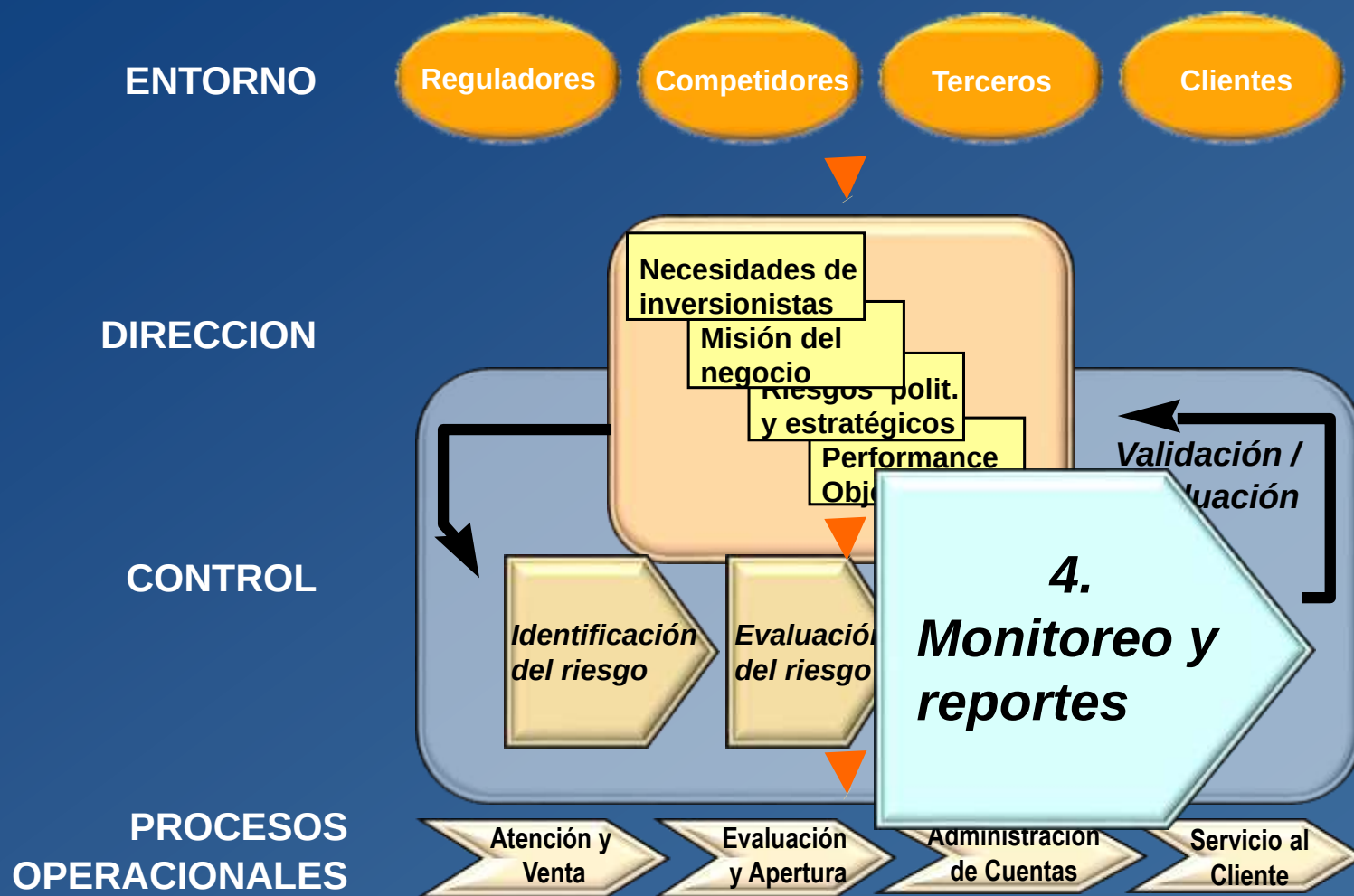
Comité de RO / Directorio



Coordinador de RO / Dueño del Proc.

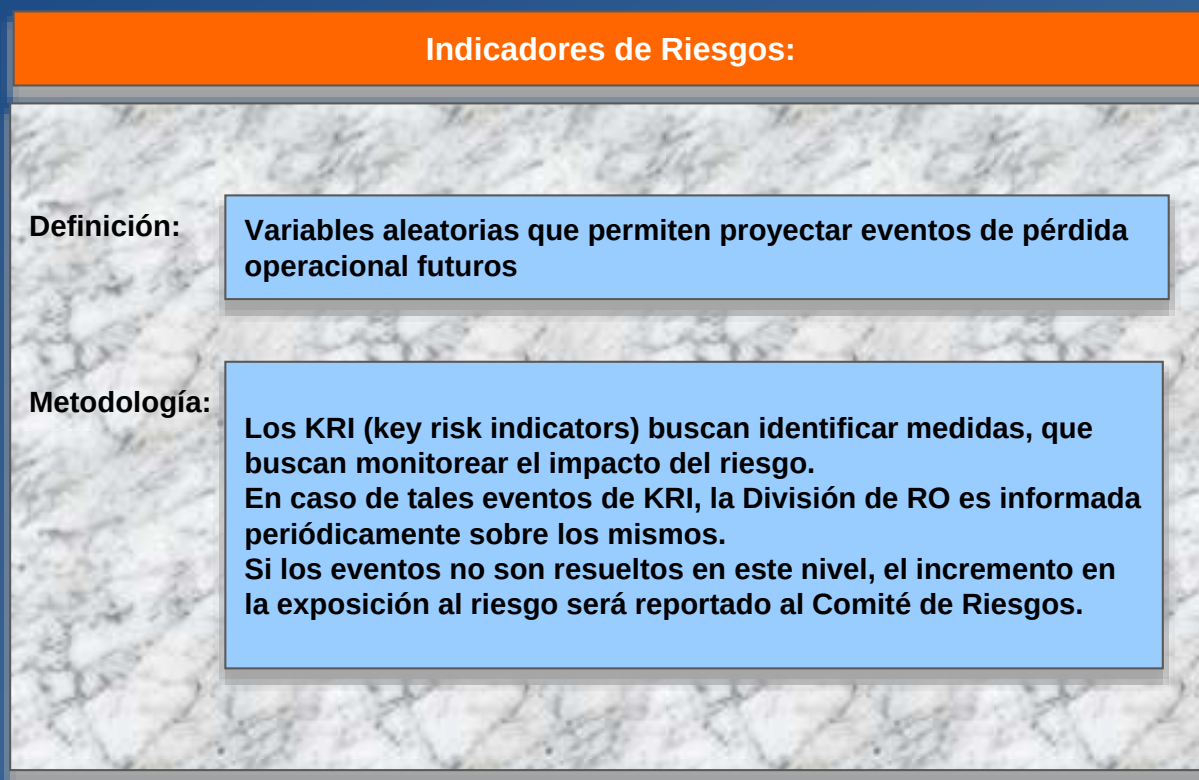
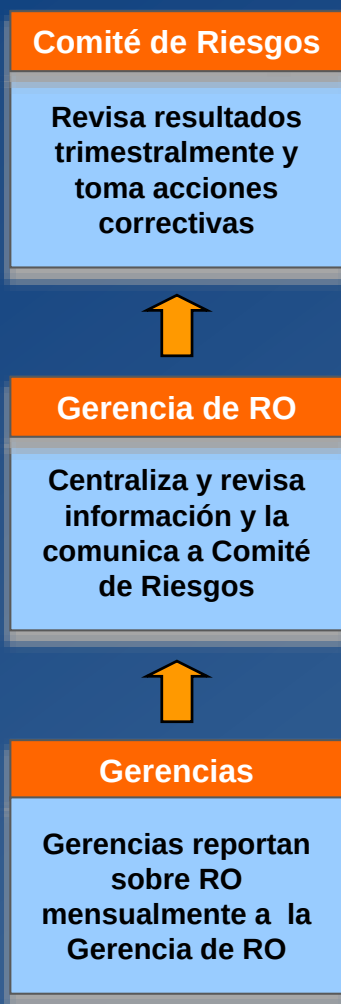
Registro de Controles

Metodología para la Gestión: GENERICO



4. Monitoreo

Mecanismos de Monitoreo



4. Monitoreo

Los Indicadores Claves de Riesgo (KRIs)

PERSONAS

- ✓ Tasa de rotación del personal
- ✓ % de nuevos empleados que dejan el puesto dentro de los primeros 6 meses
- ✓ Costos reales de entrenamiento vs. los proyectados
- ✓ Cantidad de horas extras pagadas.
- ✓ Ausentismo de personal / tasa de enfermedades.
- ✓ % de evaluación de personal por debajo de “satisfactorio”.
- ✓ % de personal permanente / temporario.
- ✓ Ratio de número días de personal enfermo sobre número total de días

PROCESOS

- ✓ Número y naturaleza de superación de límites establecidos.
- ✓ Cambio porcentual en el número de transacciones.
- ✓ Número de observaciones / cargos debidos a incumplimientos regulatorios.
- ✓ Volumen de transacciones a procesar proyectadas sobre capacidad disponible.
- ✓ Número de cuentas no conciliadas.

SISTEMAS

- ✓ Tasa Número y tipo de violaciones a seguridad.
- ✓ Número de incidentes con virus informáticos.
- ✓ Tiempo de sistema caído.
- ✓ Porcentaje de disponibilidad de servidores.
- ✓ Número de cambios de sistema.
- ✓ Número y severidad de incidentes con sistemas.

FRAUDES EXTERNOS E INTERNOS

- ✓ Número de fraudes de origen externo exitosos.
- ✓ Número de ataques informáticos.
- ✓ Cambio Cantidad de eventos de alarma de robo detectados por seguridad.
- ✓ Cantidad de violaciones a la confidencialidad de los clientes.

PRACTICAS DE NEGOCIOS, PRODUCTOS Y CLIENTES

- ✓ Número Discrepancias en el número de confirmaciones de operaciones
- ✓ Número de quejas de los clientes.
- ✓ Variabilidad de ingresos por producto.
- ✓ Cuota de mercado por producto.
- ✓ Número / porcentaje de cuentas de clientes con documentación incompleta.
- ✓ Número de nuevos productos.

4. Reporte

Reporte Consolidado de Riesgos por Area

DEPARTAMENTO: []

GERENTE: []

TRIMESTRE: []

IMPACTO:(Ejm.) Bajo= < "\$X" Medio= > "\$X" y < "\$Y" Alto= > "\$Y"
PROBABILIDAD:(Ejm.)Bajo =RemotoMedio = Posible Alto = Muy probable

[DIVISION: A]									
[Dependencia Operacional]									
[Objetivo del Negocio 1]									
	RIESGO POTENCIAL			RIESGO RESIDUAL			Objetivo	Importanc	Esi. Sit
	B	M	A	B	M	A			
Riesgo 1									
Riesgo 2									
[Objetivo del Negocio 2]									
Riesgo 1									
Riesgo 2									
[Dependencia Operacional 2]									
[Objetivo del Negocio 1]									
	B	M	A	B	M	A	Objetivo	Importanc	Esi. Sit
Riesgo 1									
Riesgo 2									
[Objetivo del Negocio 2]									
Riesgo 1									
Riesgo 2									

4. Reporte

Informe al Directorio

Informe Mapa de Riesgos de Operación
Segundo Trimestre 2007



MAPA DE RIESGOS DE OPERACIÓN DEL BANCO DE LA NACIÓN

Segundo Trimestre 2007

San Isidro, septiembre de 2007

DEPARTAMENTO DE RIESGOS
DIVISION RIESGOS DE OPERACION

Informe Mapa de Riesgos de Operación
Segundo Trimestre 2007



Índice

1. OBJETIVO	8
2. ALCANCE Y METODOLOGÍA	8
3. EVALUACIÓN GLOBAL DE LOS EVENTOS DE RIESGO DE OPERACIÓN DEL BANCO	10
3.1 Principales indicadores	10
3.2 Nivel de criticidad (riesgo residual)	11
3.3 Nivel de riesgo	12
3.4 Clasificación de Riesgo	13
3.5 Situación de solución	13
3.6 Número de eventos	15
3.7 Ranking de eventos	16
4. REGISTRO CONSOLIDADO DE INCIDENCIAS DE RIESGO	20
Departamento de Asesoría Jurídica	24
Departamento de Comunicación Corporativa	29
Departamento de Contabilidad	33
Departamento de Créditos	37
División de Fideicomisos	41
Departamento de Finanzas	45
Departamento de Informática	49
Departamento de Logística	54
Departamento de Oficialía de Cumplimiento	58
Departamento de Operaciones	62
Departamento de Personal	66
Departamento de Planeamiento y Desarrollo	70
Departamento de Red de Agencias	74
Departamento de Secretaría General	78
División Seguridad de Información	82
Departamento de Servicios Bancarios	88
División Seguridad	93
6. PRINCIPALES CONCLUSIONES Y RECOMENDACIONES	97

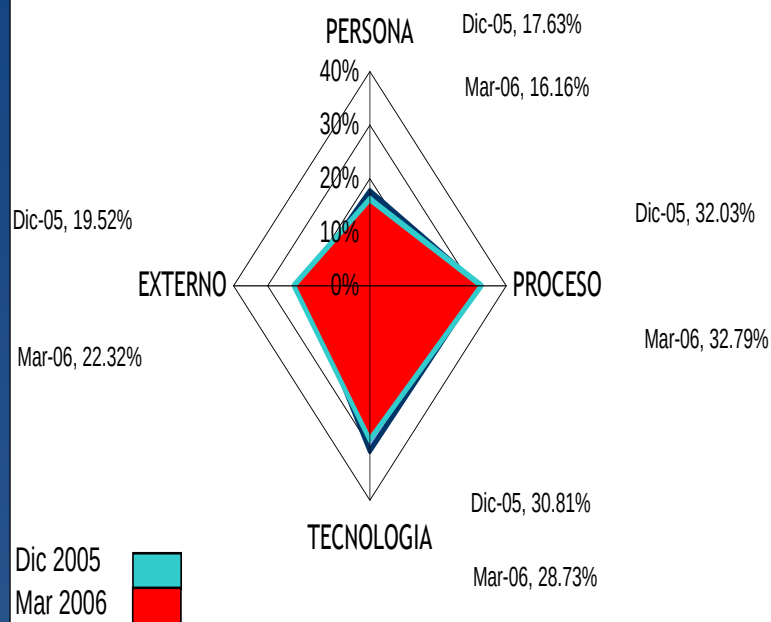
RESUMEN EJECUTIVO

DEPARTAMENTO DE RIESGOS
DIVISION RIESGOS DE OPERACION

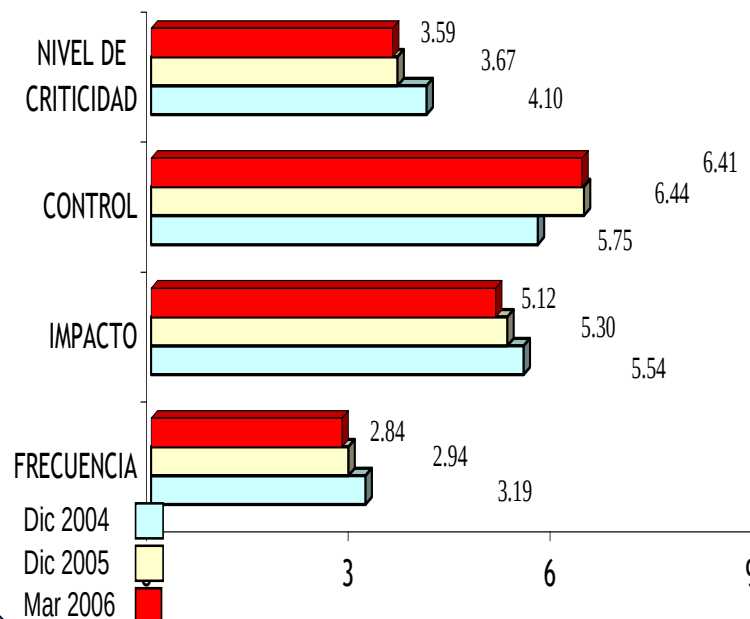
2

4. Reporte Análisis

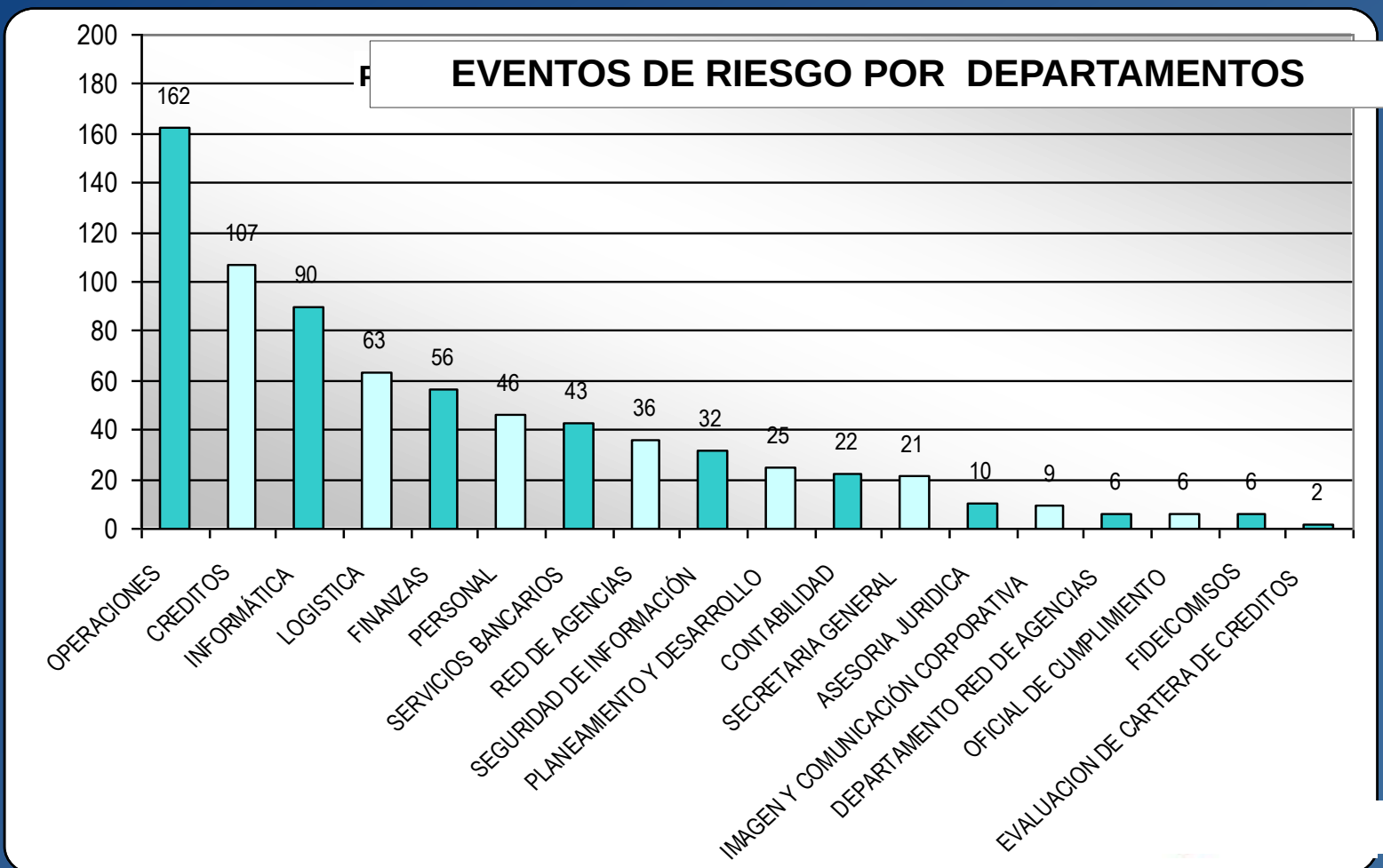
COMPARATIVO POR PERFIL DE RIESGO



INDICADORES PROMEDIO
BANCO DE LA NACION



4. Reporte Análisis



4. Reporte Análisis

**Situación de Solución
Junio 2007**

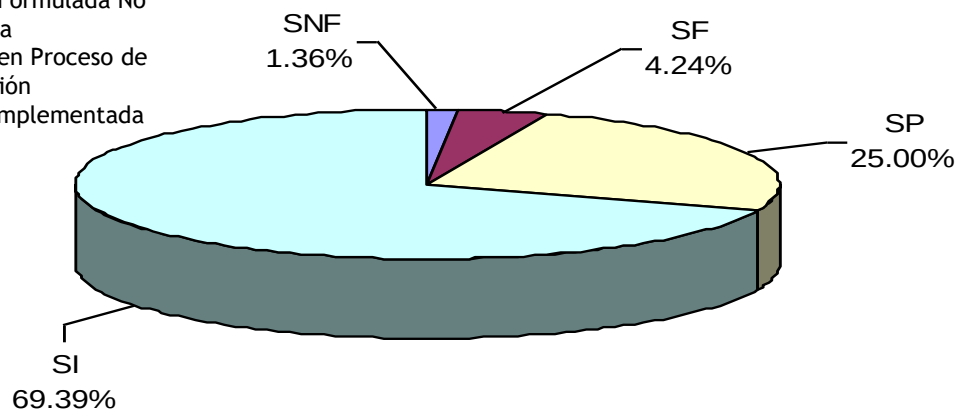
Leyenda

SNF: Solución No Formulada

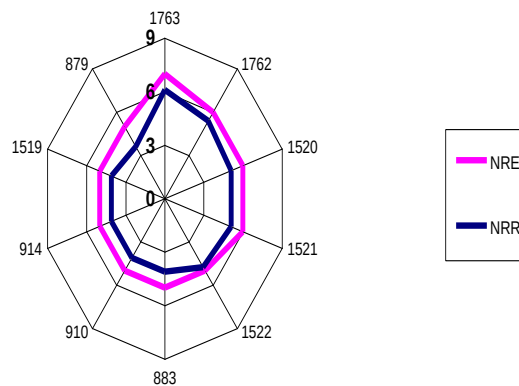
SF: Solución Formulada No
implementada

SP: Solución en Proceso de
implementación

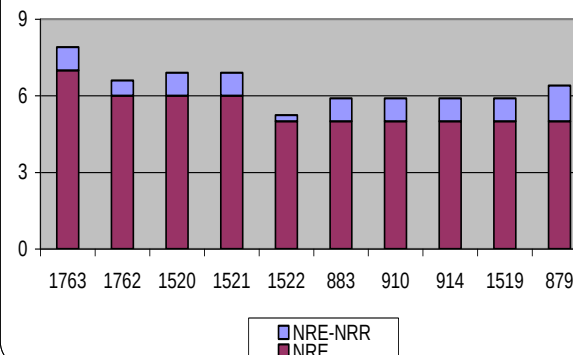
SI: Solución Implementada



NIVEL DE RIESGO EXISTENTE Vs RESIDUAL



GRADO DE AVANCE DE LA EFECTIVIDAD DE CONTROL



4. Reporte Análisis

TOP 10

REPORTE DE RIESGOS TOP10				TOP10			
PERIODO:							
FECHA:							
RANKING AL DD/MM/AA POR RIESGO				RANKING AL DD/MM/AA POR DEPARTAMENTO			
RANKING	RIESGO	CLASIFICACION	NIVEL	RANKING	DEPARTAMENTO	NIVEL	EVENTO DE PERDIDA?
1				1			
2				2			
3				3			
4				4			
5				5			
6				6			
7				7			
8				8			
9				9			
10				10			

MAPA TOP10

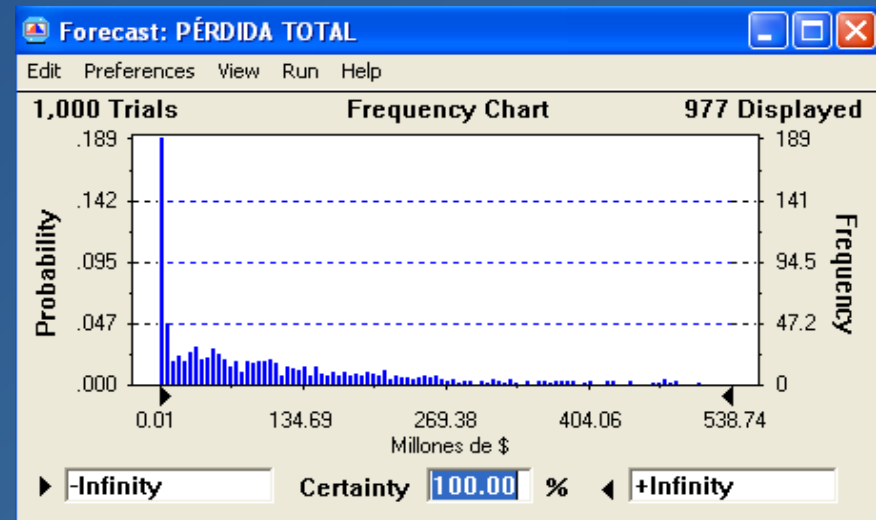
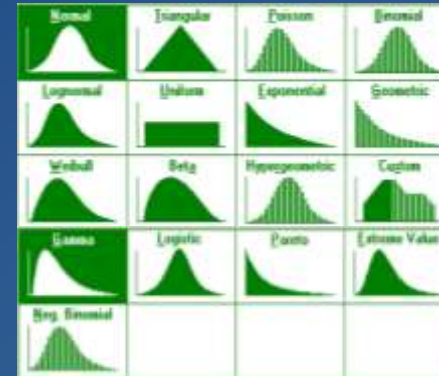
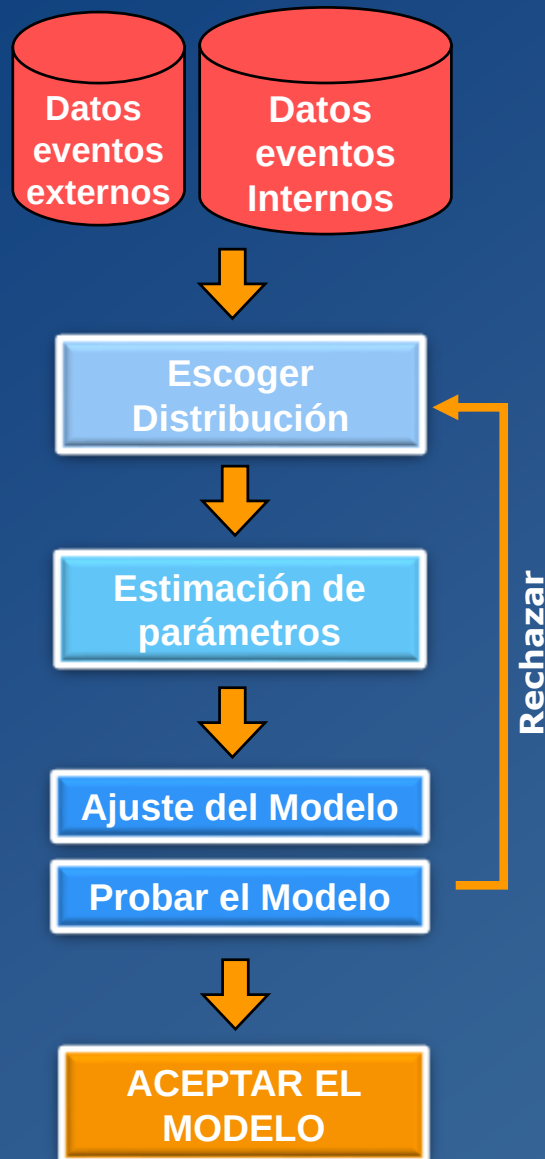
FACTORES PROMOTORES DE RIESGO

EVALUACION DE CONTROLES EXISTENTES

Mapa de riesgos Mitigación



Gestión de Riesgo Operativo





Gracias!

obassow@gmail.com



OSCAR BASSO WINFFEL

Ciudad de Guatemala
Julio de 2017

La reflexión del ROP fue motivada por casos muy especiales a mediados de los 90s

❑ 1995: Barings Bank (UK), fundado en 1762



ä Quiebra por pérdida de US\$ 1.4 billones

❑ Reseña

- ä Nick Leeson, Jefe de la Unidad de Futuros de Singapur apostó en derivados del índice Nikkei-225
- ä Valor de los contratos fue afectado negativamente por terremoto de Kobe
- ä Leeson amplió continuamente su posición en los mismos instrumentos en espera de mejores condiciones
- ä El Banco no pudo cubrir obligaciones en los mercados de Japón y Singapur por \$1,400 millones y se declaró en quiebra a pesar de los intentos del Bank of England por rescatarlo

❑ ¿Cómo y por qué sucedió?

- ä Escasa supervisión y control para el trader estrella
- ä Leeson era a la vez supervisor y ejecutor de operaciones y contratos
- ä Las pérdidas eran registradas en una cuenta oculta para reportar únicamente ganancias
- ä El Banco carecía de una unidad independiente de administración de riesgo en sus oficinas descentralizadas

La reflexión del ROP fue motivada por casos muy especiales a mediados de los 90s

□ 1995: Daiwa Bank (Japón)

ä Pérdidas de US\$ 1.1 billones



□ Reseña

- ä En septiembre, Daiwa reportó una pérdida de \$1,100 millones debido a transacciones no autorizadas de compra/venta de bonos en su oficina de New York entre 1983 y 1995
- ä Las pérdidas habían sido ocultadas por el trader Iguchi Toshihide y nunca reportadas en los estados financieros
- ä Cuando la empresa descubrió la falta, la dirección ordenó realizar cuantiosas transacciones para tratar de recuperar la pérdida sin necesidad de reportarla a las autoridades regulatorias.
- ä Los reguladores en US expulsaron a Daiwa del país al conocerse el encubrimiento

□ ¿Cómo y por qué sucedió?

- ä Falta de segregación de tareas
- ä Toshihide era a la vez trader y portador de libros contables

La reflexión del ROP fue motivada por casos muy especiales a mediados de los 90s

❑ 1996: Sumitomo Corporation (Japón)



à Pérdidas por US\$ 2.6 billones

❑ Reseña

- à Yasuo Hamanaka, cabeza de la Unidad de trading de Cobre cubrió pérdidas de \$1,800 millones
- à Hamanaka tomó posiciones a nombre de la institución llegando a controlar 5% de la producción mundial de cobre y haciendo que los precios aumentaran artificialmente.
- à Al no poder seguir financiando sus posiciones en contratos, el precio del cobre se desplomó y con aquel la empresa acumuló pérdidas en contratos y préstamos por \$2,600 millones

❑ ¿Cómo y por qué sucedió?

- à Autonomía ilimitada de manejo de fondos en el área estrella de la oficina central en Tokyo
- à Avisos previos de reguladores sobre las prácticas sospechosas de Hamanaka no fueron escuchados por la Alta Gerencia
- à Se incumplió política interna de la empresa de rotación de puestos de alto riesgo
- à Jefatura de la unidad desconocía el detalle del negocio
- à La institución falló en separar el front office del back office

TIPOLOGIAS DEL RIESGO OPERACIONAL



Factor Potencial	Eventos	Ejemplos
<i>Fraude Interno</i>	Actos destinados a defraudar, usurpar la propiedad o evadir la regulación, la Ley o las políticas de la empresa que involucren al menos una parte interna	Reportes de posiciones intencionalmente errados Defraudación de empleados Negociación con Información privilegiada por parte de un empleado
<i>Fraude Externo</i>	Actos por parte de terceros destinados a defraudar, usurpar la propiedad o evadir la Ley	Robo y Falsificación Emisión de cheques sin fondos Intromisión en los sistemas de comunicación e información
<i>Prácticas de empleo y seguridad del ambiente de trabajo</i>	Actos ilegales frente a las normas laborales que resulten en pagos por perjuicios al personal o reclamos por seguridad o por salud.	Reclamos por compensación de trabajadores Pagos por violación a normas de salud o seguridad de empleados Obligaciones derivadas de reclamos de terceros por razones de seguridad
<i>Prácticas Relacionadas con los clientes, los productos y el negocio</i>	Fallas negligentes o no intencionadas que impidan cumplir con las obligaciones profesionales con clientes específicos o derivadas de la naturaleza del diseño de un producto	Brechas fiduciarias Mal manejo de información confidencial de clientes Actividades de negocio inapropiadas o cuenta del banco Lavado de activos Venta de productos no autorizados
<i>Daño a los Activos Físicos</i>	Pérdida o daño a los activos físicos debido a desastres naturales u otros eventos	Vandalismo, terrorismo Terremotos Incendios e inundaciones
<i>Interrupción del Negocio y Fallas en los Sistemas</i>	Interrupción en las actividades del negocio o fallas en los sistemas de información	Fallas en el hardware o software Problemas en las telecomunicaciones Corte en el suministro de servicios públicos
<i>Administración de la Ejecución, la Entrega y el Proceso</i>	Fallas en el procesamiento de transacciones o en la administración del proceso y en las relaciones con las contrapartes y los proveedores.	Errores en la grabación de datos Fallas en la administración de colaterales Documentación legal incompleta Acceso no aprobado a las cuentas de los clientes Desempeño inadecuado de las contrapartes no clientes Disputa con los proveedores

Fuente: *Prácticas Adecuadas para la Gestión y Supervisión de los Riesgos de Operación*. Comité de Supervisión Bancaria de Basilea, Julio de 2002. BANK FOR INTERNATIONAL SETTLEMENTS

1. Procesos

Categoría	Nivel 1	Nivel 2
Procesos	Control Interno	Falta de controles duales
		Deficiente labor de Auditoría Interna
	Contratación y designación del personal de confianza	Falta de Idoneidad del personal de confianza
	Cumplimiento	No observancia de los procedimientos de cumplimiento internos
		Confiabilidad de la información
		Deficiencias o incumplimientos en el manejo de información reservada
	Seguridad de información	Deficiencias en procedimientos para proteger la información
	Supervisión de empresas	Ingreso en el mercado de participantes no adecuados

2. Personas

Categoría	Nivel 1	Nivel 2
Personas	Fraude cometido por empleados / Doloso (criminal)	Colusión
		Malversación de fondos
		Hurto – físico
	Actividad no autorizada /Operaciones fraudulentas/ Delitos cometidos por empleados	Uso indebido de información confidencial
		Manipulación del mercado
		Ignorar o pasar por alto deliberadamente los procedimientos
	Pérdida o Falta de Personal Clave	Falta de empleados idóneos

3. Tecnología de Información

Categoría	Nivel 1	Nivel 2
Sistemas	Capacidad de los Sistemas	Falta de la adecuada capacidad de planeamiento / Software inadecuado
	Violación de los Sistemas de Seguridad	Violaciones de la seguridad externa
		Fallas en los controles de seguridad interna



4. Eventos Externos

Categoría	Nivel 1	Nivel 2
Eventos Externos	Riesgo sistémico en el mercado de valores	Desconfianza del público
		Problemas con otras empresas del sector
	Inadecuado manejo de la crisis por las autoridades	Medidas o acciones por parte de las autoridades
		Daños a la credibilidad de los organismos supervisores

5. Plan de Continuidad de Negocios

¿Qué es el PCN?

Un *plan* que mantiene la *continuidad* de los *procesos críticos* del negocio requeridos a un *nivel aceptable* de operación desde el momento de ocurrencia de *un evento de interrupción* de los mismos y/o de los recursos que los soportan hasta la *recuperación* de la normalidad.



5. Plan de Continuidad de Negocios

¿Cuáles son los objetivos del PCN?

- ❑ *Minimizar* el número de *decisiones* que deben ser tomadas durante la duración de un desastre o suceso de emergencia, garantizando la correcta recuperación de los sistemas y procesos
- ❑ *Reanudar* tan rápidamente como sea posible las *funciones* más *críticas* de la actividad de la empresa minimizando el *impacto* en el negocio (incluyendo los sistemas).
- ❑ *Minimizar* las *pérdidas* económicas y de información y, en general, preservar los objetivos estratégicos de la empresa.
- ❑ *Evitar* en la medida de lo posible *la dependencia* de la organización en la participación de *personas* específicas en el proceso de recuperación.

5. Plan de Continuidad de Negocios



6. Plan de Seguridad de Información

¿Qué es Seguridad de Información?

La adecuada interrelación de normas, procedimientos, mecanismos y recursos informáticos en una ADECUADA estructura de la ORGANIZACIÓN que permita garantizar los principios de confidencialidad, disponibilidad e integridad de la información.

¿Qué es el PSI?

Es un Plan que direcciona el sistema de administración de la seguridad de la información. Debe incluir los activos de tecnología que deben ser protegidos, la metodología usada, los objetivos de control y controles, así como el grado de seguridad requerido.



6. Plan de Seguridad de Información

Implantación del PSI

El diseño e implementación del PSI, se ejecuta aplicando como mínimo cinco etapas denominadas “Desarrollo de procesos”:

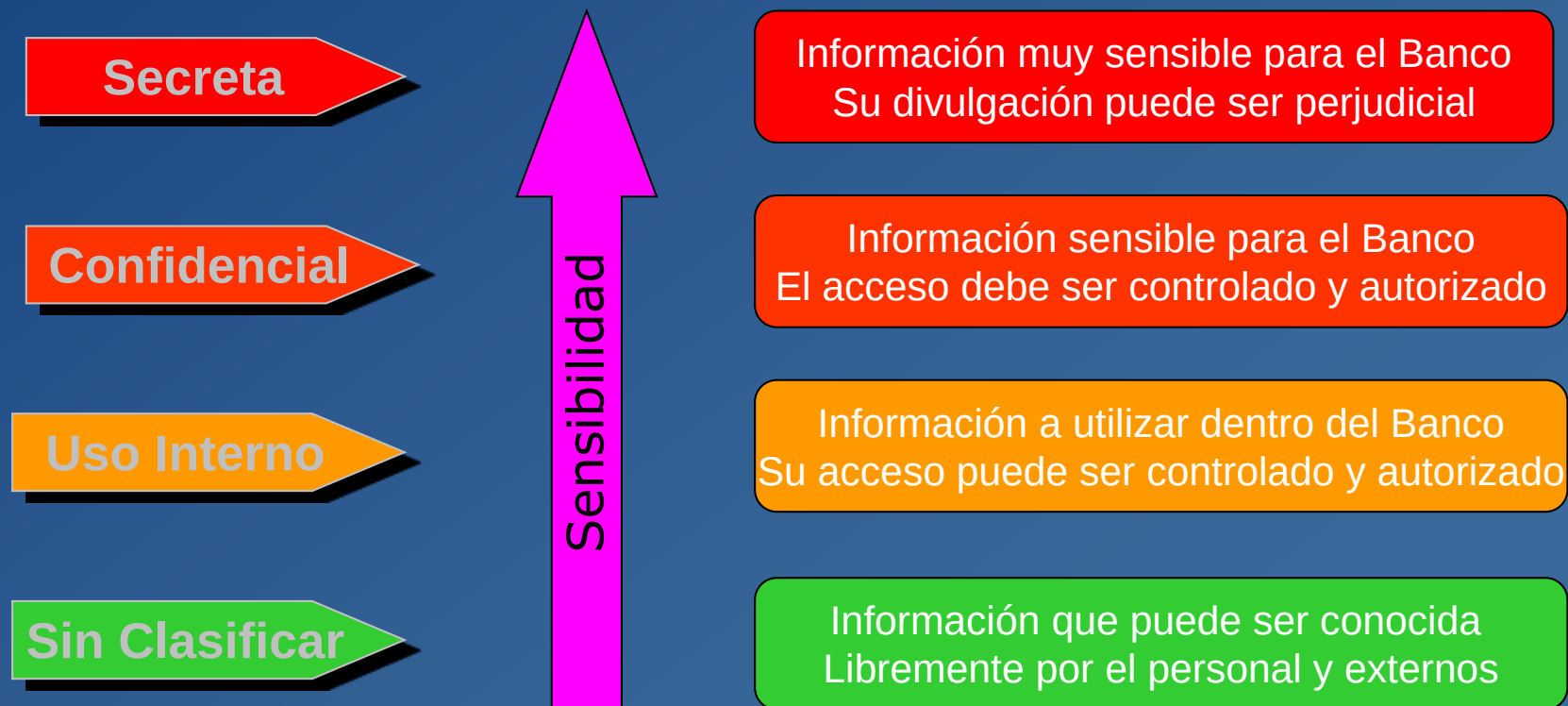
- I.- Definición de la Organización de Seguridad
- II.- Identificar Activos, Riesgos, Controles asociados a F. Estratégicos
- III.- Desarrollo de Políticas y Arquitectura de Seguridad
- IV.- Entrenamiento y Concientización
- V.- Implementación y Validación de Políticas y Arquitectura de Seguridad

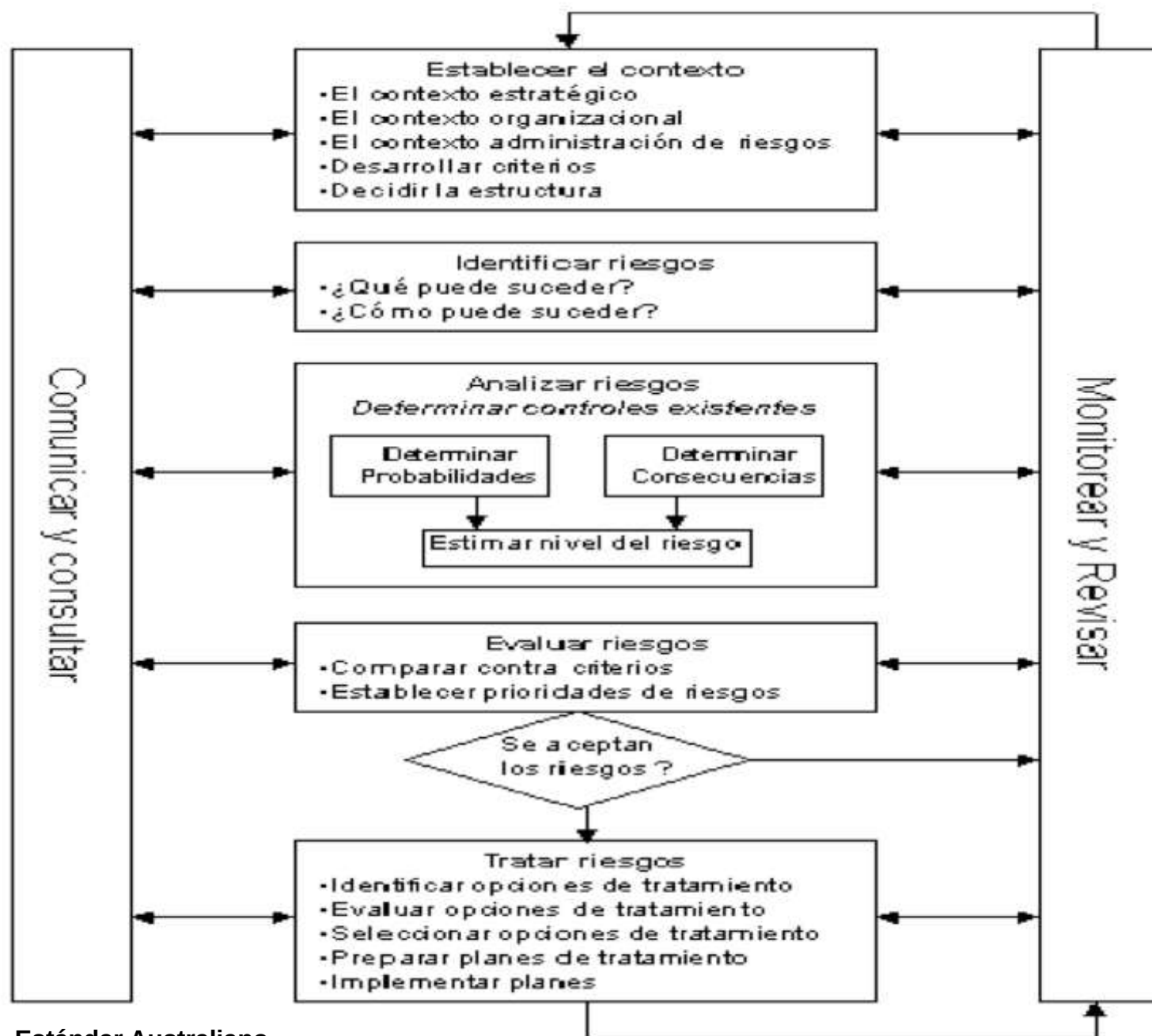
6. Plan de Seguridad de Información



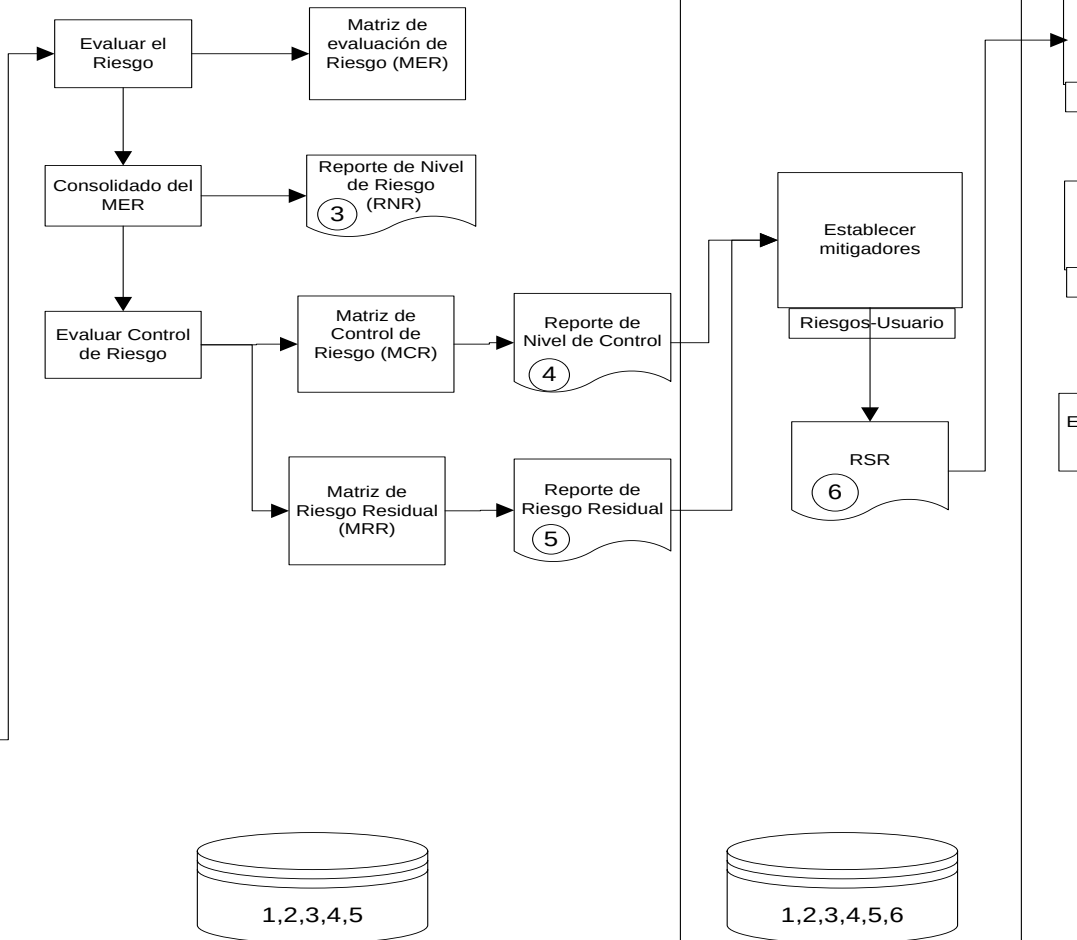
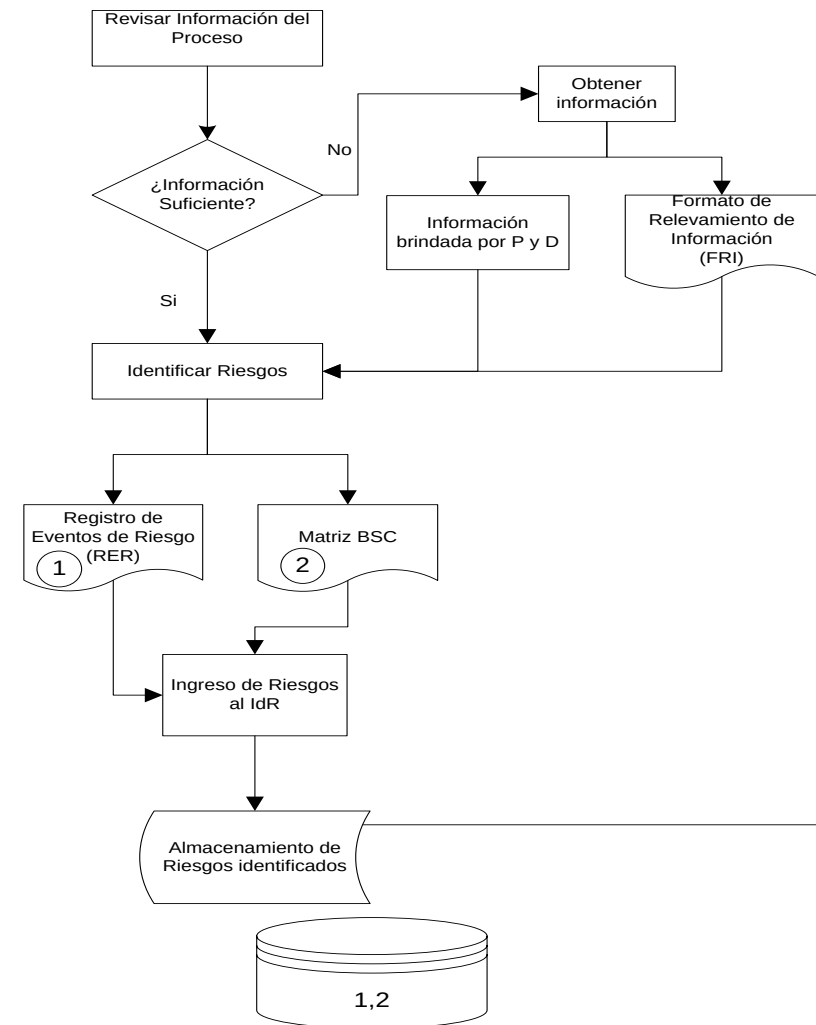
Clasificación y confidencialidad de la Información

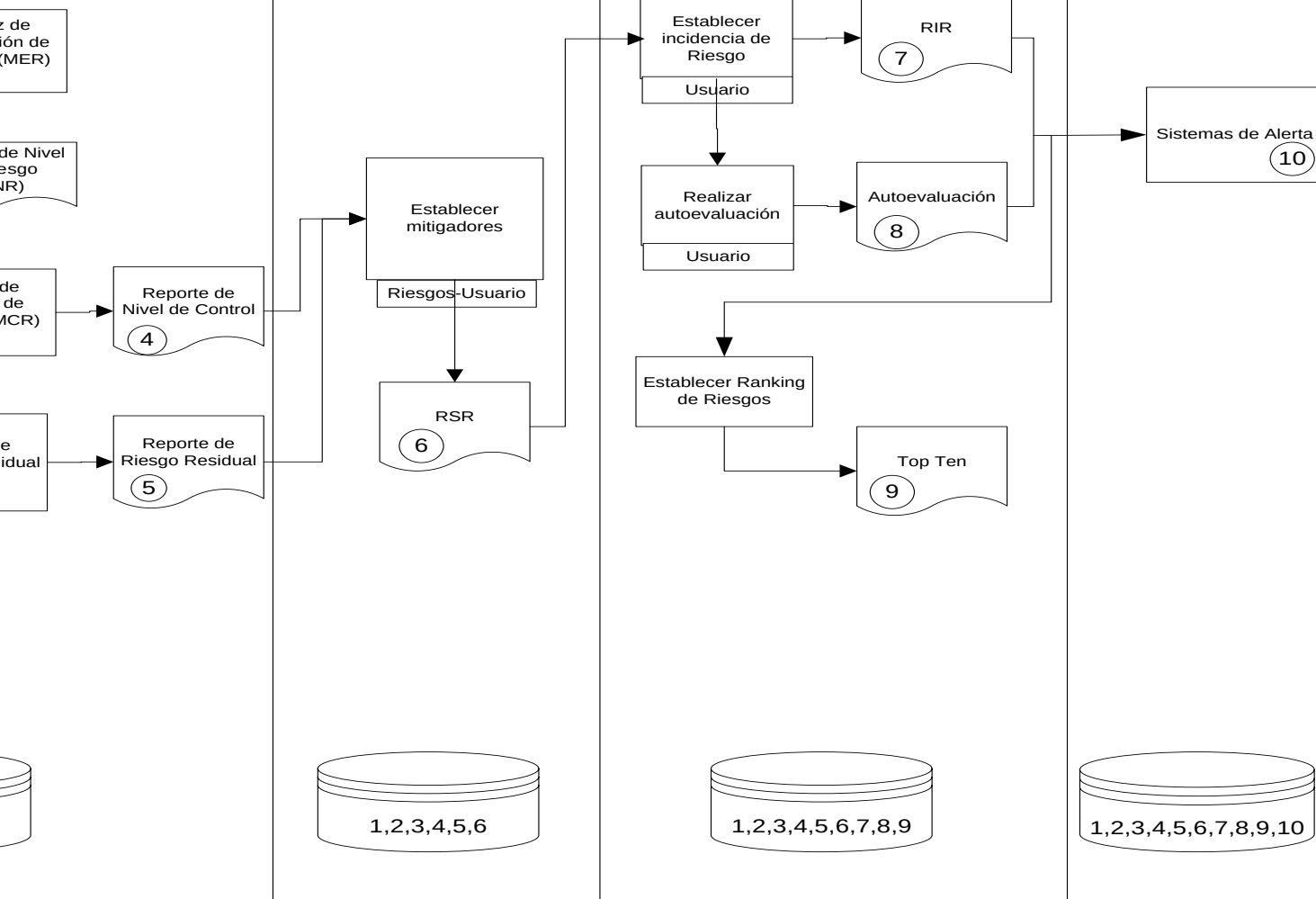
Es necesario asegurar una adecuada protección de la información frente a riesgos de pérdida, divulgación no autorizada o cualquier uso indebido de ella en forma intencional o accidental”



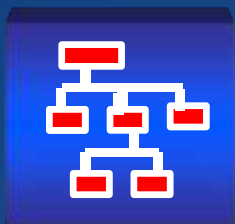


Estándar Australiano





Gestión de Riesgos Operativos

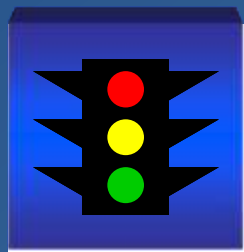


1. IDENTIFICACIÓN



4. REPORTE

2. CUANTIFICACIÓN



3. MITIGACIÓN

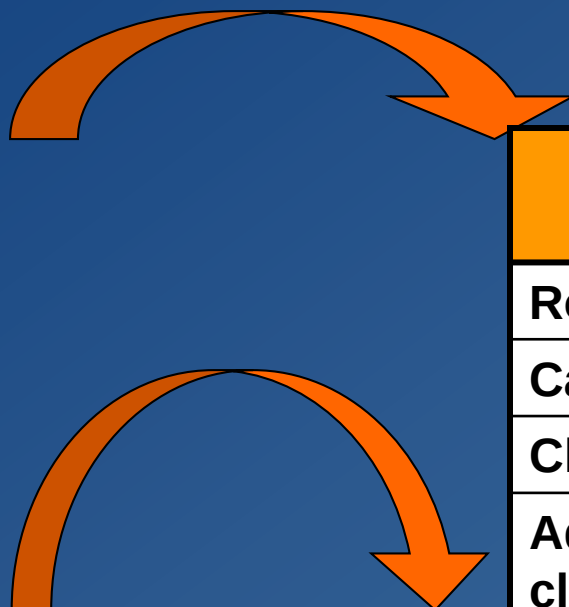


4. MONITOREO

Operaciones en ATMs

Algunos riesgos identificados

ORIGEN DEL RIESGO
Personas
Procesos
Tecnología
Relaciones con terceros
Eventos Externos



RIESGO/CONDICION OBSERVADA
Robo al paso
Cambio de tarjeta
Clonación de tarjeta
Adquisición clandestina de clave de tarjeta



TRATAMIENTO RECOMENDADO
Monitoreo: Transacciones sospechosas
Seguridad electrónica: Tarjeta con chip
Educación del cliente: Uso y cuidado de la clave personal
Autorizaciones: Límite diario de operaciones

Operaciones por Internet

Algunos riesgos identificados

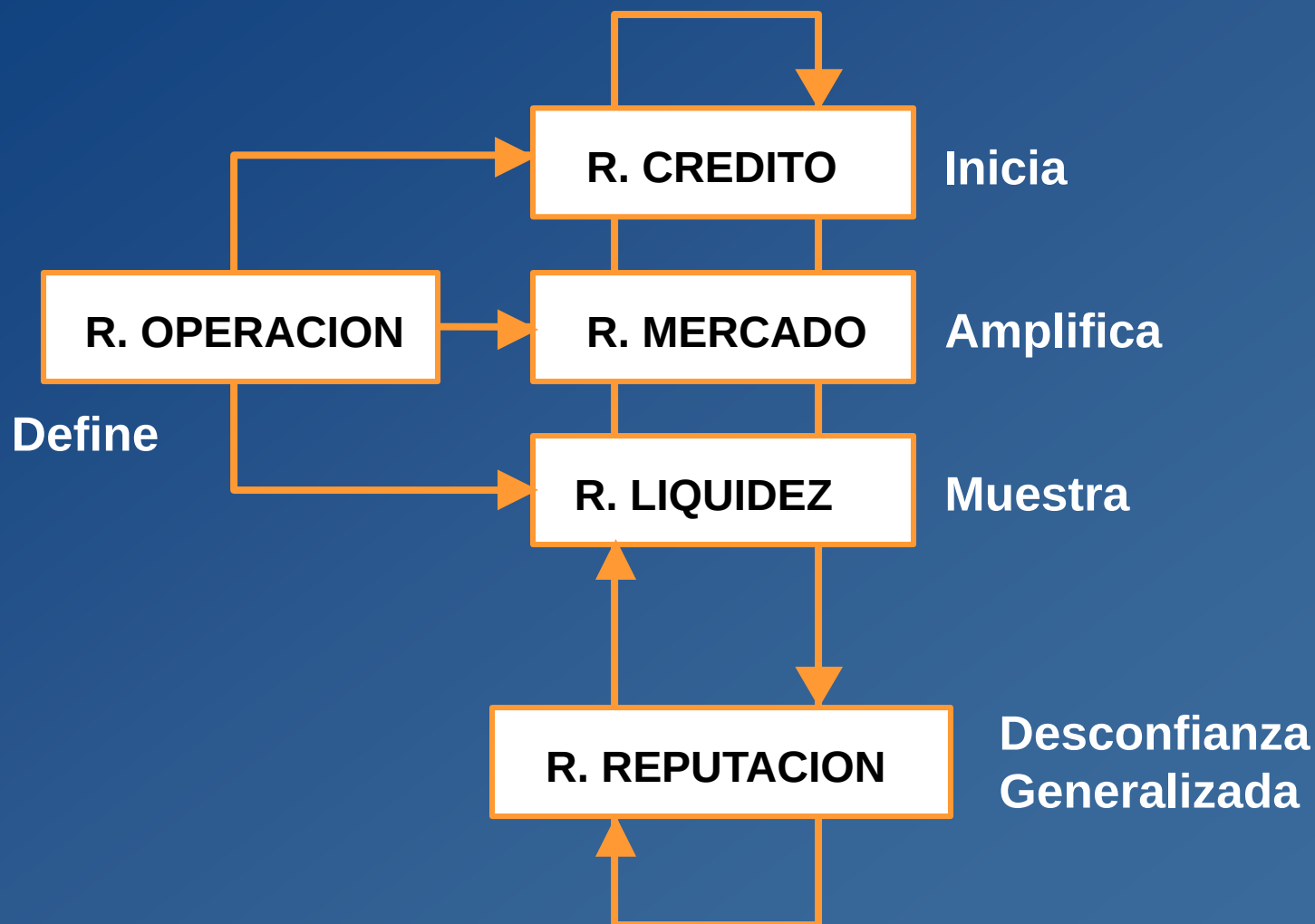
ORIGEN DEL RIESGO
Personas
Procesos
Tecnología
Relaciones con terceros
Eventos Externos

RIESGO/CONDICION OBSERVADA
Transacciones no autorizadas
Adquisición clandestina de clave personal
Correo electrónico falsificado
Intercepción de transmisiones

TRATAMIENTO RECOMENDADO
Monitoreo: Transacciones sospechosas
Seguridad electrónica: Encriptación, tarjetas token
Educación del cliente: Uso y cuidado de la clave personal
Estrategia de comunicación: Alerta oportuna a clientes



Crisis Subprime...



Crisis Subprime...

Liquidez

ESTADO
Prestamos
interbancarios

A	P
Activos Líquidos	
	Depósitos
	K

Solvencia

ESTADO
Aporte de
Capital

A	P
Créditos	Depósitos

Crisis Subprime...

- Se vivió cuatro crisis simultáneas que convergen y se amplifican mutuamente:
 - ä la del sistema financiero mundial,
 - ä la del sistema productivo globalizado,
 - ä la de ideas e ideologías, y
 - ä la crisis generalizada de confianza.



Crisis Subprime...



- ❑ La Crisis generalizada de confianza se refiere al factor clave en el funcionamiento de cualquier tipo de mercado: la confianza en que las transacciones acordadas serán respetadas y que todos los agentes, personas e instituciones, cumplirán su palabra y honrarán sus compromisos.
- ❑ Los **bancos** desconfían los unos de los otros y desconfían de sus clientes, y exigen garantías superseguras para prestarles. Las **personas** evitan tomar préstamos porque no saben si tendrán trabajo, y las **empresas** prefieren reducir inversiones porque no saben si tendrán mercados. El resultado es una **parálisis financiera** y una sobredosis de pesimismo.