



Riesgo Operacional

Programa de Capacitación sobre Gestión de Riesgos Financieros
Abril de 2018



Superintendencia de Bancos
Guatemala, C.A.



Presentación elaborada con fines informativos, en el marco del Programa de Educación Financiera. La Superintendencia de Bancos no es responsable por los usos que se dé o las decisiones que se tomen, basadas en la información contenida, ya que ésta no podrá considerarse como asesoría u opinión técnica vinculante. El uso, reproducción, edición, copia, publicación o distribución parcial o total, por cualquier medio, por parte de terceros, deberá contar con autorización de la Superintendencia de Bancos.



Superintendencia de Bancos
Guatemala, C.A.

Algunas de sus funciones



Cumplir y hacer cumplir las leyes,
reglamentos, disposiciones y
resoluciones aplicables

Evaluar las políticas, procedimientos,
normas y sistemas de las entidades y, en
general, asegurarse que cuenten con
procesos integrales de administración
de riesgo

Supervisarlas a fin de que mantengan la
liquidez y solvencia adecuadas que les
permita atender oportuna y totalmente
sus obligaciones, y evalúen y manejen
adecuadamente la cobertura,
distribución y nivel de riesgo de sus
inversiones y operaciones contingentes



Contenido



Introducción

- Definición
- Determinación del riesgo inherente
- Fuentes de riesgo

Estándares Internacionales

- Principios de riesgo Operacional

Administración del Riesgo

- Identificación
- Medición
- Mitigación
- Control

Monitoreo e Informes

- KRI
- Indicadores cualitativos
- Mapeo de procesos



Superintendencia de Bancos
Guatemala, C.A.

Introducción



Superintendencia de Bancos
Guatemala, C.A.

Riesgo Operacional



**Alta competitividad en el
sector financiero**



**Incursión en nuevos
mercados**



**Trabajar con nuevos
productos**

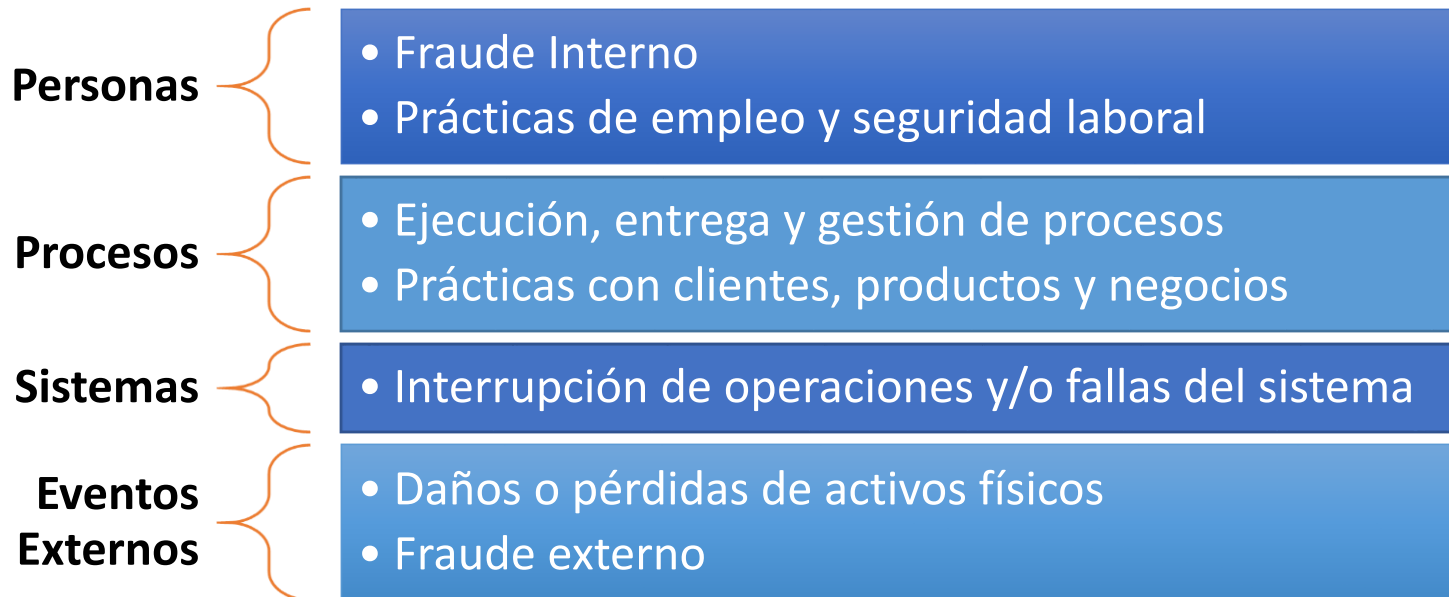


**Complejidad de
operaciones**



Definición

El Comité de Basilea de Supervisión Bancaria lo define como el riesgo de pérdida resultante de una **falta de adecuación o de un fallo de los procesos**, el personal o los sistemas internos, o bien como consecuencia de acontecimientos externos. **Incluye riesgo legal pero excluye al riesgo estratégico y al de reputación.**





Administración del RO

Conceptos básicos (1/2)





Superintendencia de Bancos
Guatemala, C.A.

Administración del RO

Conceptos básicos (2/2)

Frecuencia (Probabilidad)

Es una medida 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 (1) evento.



Superintendencia de Bancos
Guatemala, C.A.

Ventaja de la administración del RO





Eventos de Riesgo

Eventos	Causa
Fraude Interno	a) Error intencionados en el reporte de posiciones b) Robos por parte de empleados c) Utilización de información confidencial
Fraude externo	a) Robo b) Falsificación c) Circulación de cheques en descubierto
Prácticas de empleo y seguridad en el puesto de trabajo	a) Solicitud de indemnización b) Discriminación c) Infracción a normas laborales de seguridad e higiene
Prácticas con los clientes, productos y negocios	a) Abuso de información confidencial sobre el cliente b) Negociación fraudulenta en las cuentas del Banco c) Venta de productos no autorizados
Daños a activos materiales	a) Terrorismo b) Vandalismo c) Terremoto
Alteraciones en la actividad y fallos en los sistemas	a) Fallos en hardware y software b) Problemas de telecomunicaciones c) Interrupción en la prestación de servicios
Ejecución, entrega y manejo de procesos	a) Errores en la introducción de datos b) Documentación jurídica incompleta c) Acceso a cuentas de los clientes sin autorización



Superintendencia de Bancos
Guatemala, C.A.

Fuentes del Riesgo

Proceso

Error captura de operaciones
Error liquidación de operaciones
Falta de separación funcional

Personas

Espionaje industrial
Uso de información privilegiada
Fraude de empleados

Sistemas

Fallos hardware / software
Interrupción de sistemas
Virus informáticos

Eventos externos

Error de proveedores
Fallos outsourcing
Desastres naturales

Efectos

Pérdida de recurso
Restitución
Contingencias legales
Infracciones regulatorias

Eventos

- a) Fraude Interno
- b) Fraude Externo
- c) Relaciones Laborales y Seguridad en puesto de trabajo
- d) Clientes, Productos y Prácticas Empresariales
- e) Daños a activos materiales
- f) Fallos en los Sistemas
- g) Ejecución, entrega y manejo de procesos





Superintendencia de Bancos
Guatemala, C.A.

Buenas prácticas para la Gestión del Riesgo Operacional





Superintendencia de Bancos
Guatemala, C.A.

Estándares Internacionales



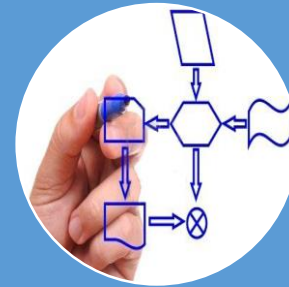
Superintendencia de Bancos
Guatemala, C.A.

Principios para la Gestión del Riesgo Operacional

Principio 1: Cultura de Gestión de Riesgos



La Junta Directiva debe establecer una cultura de gestión de riesgo fuerte a través de toda la organización.

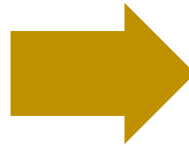


La Junta Directiva y la Alta Gerencia deben establecer una cultura de gestión de riesgo fuerte y que dé sustento y proporcione normas adecuadas para una conducta responsable y profesional.



Principios para la Gestión del Riesgo Operacional

Principio 2: Marco de Riesgo Operacional



Los bancos deben desarrollar, implementar y mantener un Marco que esté totalmente integrado dentro de los procesos generales de gestión del riesgo del banco.

El Marco de Riesgo Operacional seleccionado por un banco individual dependerá de una variedad de factores, incluyendo su naturaleza, tamaño, complejidad y perfil de riesgo.



Superintendencia de Bancos
Guatemala, C.A.

Principios para la Gestión del Riesgo Operacional

Principio 3: La Junta Directiva



Debe establecer, aprobar y revisar el Marco de forma periódica.

Vigilar a la Alta Gerencia para cerciorarse de que las políticas, procesos y sistemas estén implementados de forma efectiva.

Principio 4: Apetito y Tolerancia al Riesgo

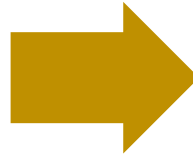


Debe aprobar y revisar el apetito por el riesgo y la declaración de tolerancia para el riesgo operacional que establezca la naturaleza, tipos y niveles del riesgo operacional que el banco esta dispuesto a asumir.



Principios para la Gestión del Riesgo Operacional

Principio 5: Alta Gerencia



Debe desarrollar una estructura de gobierno que sea clara, eficaz y robusta, y que contenga líneas de responsabilidad congruentes, transparentes y bien definidas para que sea aprobada por la Junta Directiva.

Implementar y mantener de forma continua a través de la organización, las políticas, procesos y sistemas para manejar el riesgo operacional en todos los productos, actividades, procesos y sistemas del banco que vayan de acuerdo con el apetito por el riesgo y la tolerancia.



Superintendencia de Bancos
Guatemala, C.A.

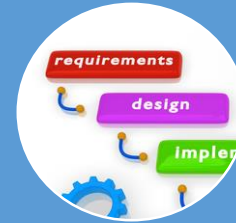
Principios para la Gestión del Riesgo Operacional

Principio 6: Identificación y Evaluación



La Alta Gerencia debe identificar y evaluar el riesgo operacional inherente en todos los productos, actividades, procesos y sistemas.

Autoevaluación de riesgo y control: a nivel de unidades de negocio.



Mapeo de procesos de negocio: análisis de procesos y de riesgo y controles asociados.

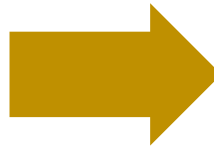
Indicadores de Riesgos y desempeño: estadísticas métricas como indicadores de riesgo clave o desempeño.

Medición: recopilación de datos de pérdida.



Principios para la Gestión del Riesgo Operacional

Principio 7: Administración por Nuevos Productos



La Alta Gerencia debe de cerciorarse de que exista un proceso de aprobación para todos los nuevos productos, actividades y sistemas que evalúen totalmente el riesgo operacional.

Principio 8: Monitoreo e Informes



La Alta Gerencia debe implementar procesos para monitorear periódicamente los perfiles de RO y las exposiciones importantes de pérdidas. Debe existir mecanismos adecuados de generación de informes a nivel de consejo, alta gerencia y líneas de negocio que sustenten la gestión proactiva del RO.



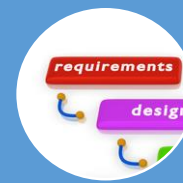
Principios para la Gestión del Riesgo Operacional

Principio 9: Control y Mitigación



Los bancos deben contar con un ambiente fuerte de control que utilice políticas, procesos y sistemas; controles internos adecuados; y estrategias adecuadas de mitigación de riesgo y/o de transferencia.

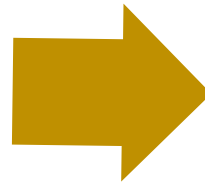
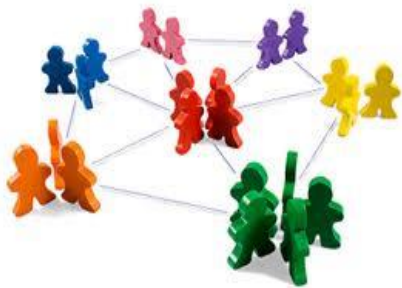
Como mitigar el riesgo?



- A) Evitando el riesgo: eliminar actividades.
- B) Controlando el riesgo: controles nuevos.
- C) Transfiriendo el riesgo: sub contratando actividades o asegurando actividades.
- D) Aceptando el riesgo.

Principios para la Gestión del Riesgo Operacional

Principio 10: Resistencia y Continuidad del Negocio



Los bancos deben contar con planes de resistencia y continuidad del negocio para asegurar la capacidad para seguir operando de forma continua y limitar las pérdidas en caso de ocurran casos severos en el negocio.

- Consideraciones importantes:
- A) Planes para funciones críticas del negocio.
 - B) Prioridades y objetivos de recuperación.
 - C) Sitios alternos.
 - D) Pruebas y capacitación.



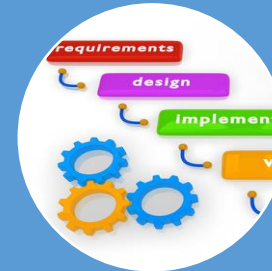
Superintendencia de Bancos
Guatemala, C.A.

Principios para la Gestión del Riesgo Operacional

Principio 11: Rol de Divulgación



Las divulgaciones al público del banco deben permitir que los actores evalúen su enfoque de gestión de riesgo operacional. Transparencia y el desarrollo de mejores prácticas en la industria mediante la disciplina de mercado.



Debe divulgarse de manera tal que permita que los actores determinen si el banco identifica, evalúa, monitorea y controla/mitiga el riesgo operacional con eficacia.





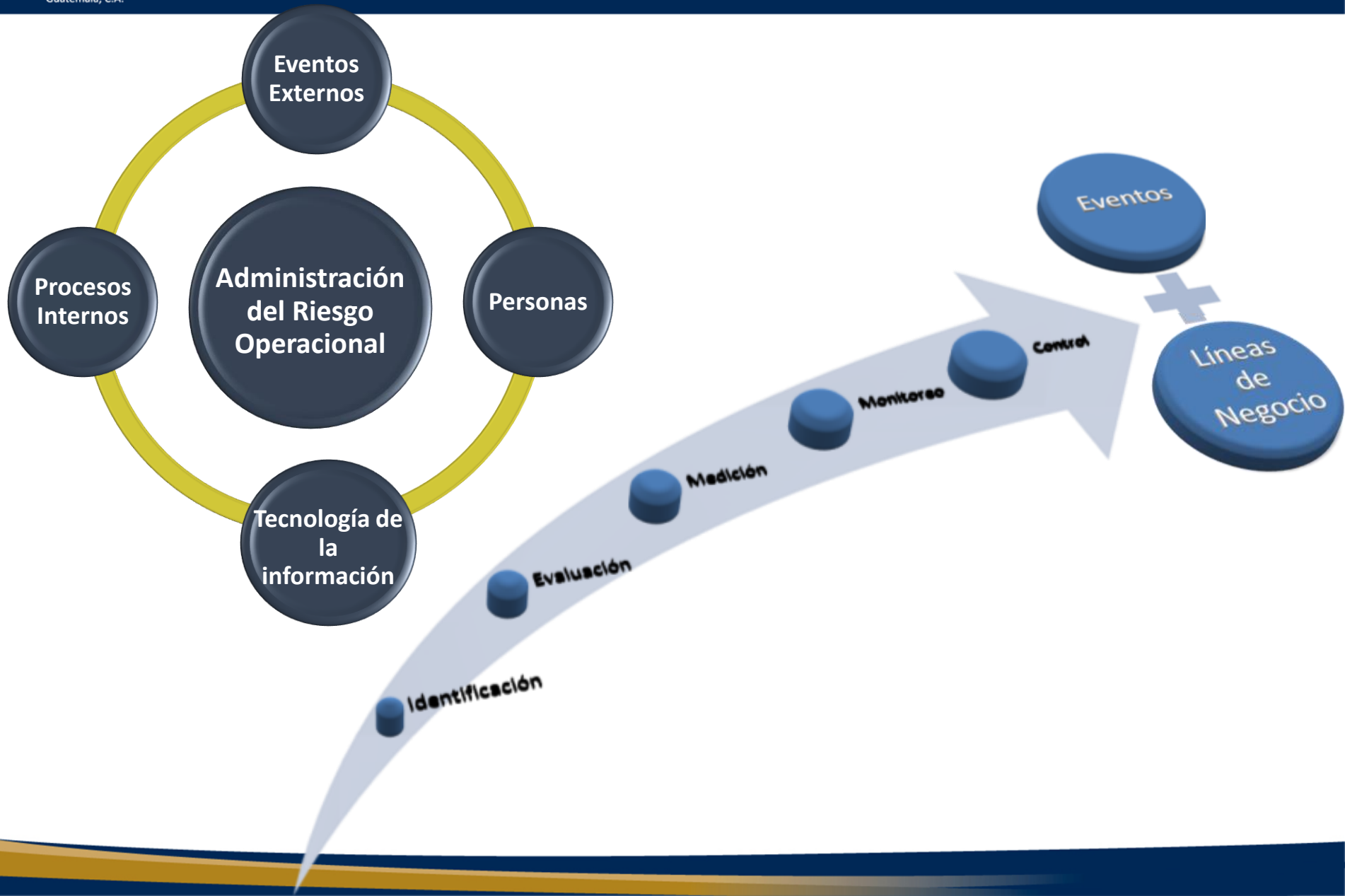
Superintendencia de Bancos
Guatemala, C.A.

Administración del Riesgo



Superintendencia de Bancos
Guatemala, C.A.

Administración del riesgo operacional





Superintendencia de Bancos
Guatemala, C.A.

Administración del riesgo operacional

Marco de gestión



**Gestión del
Riesgo
Operacional**

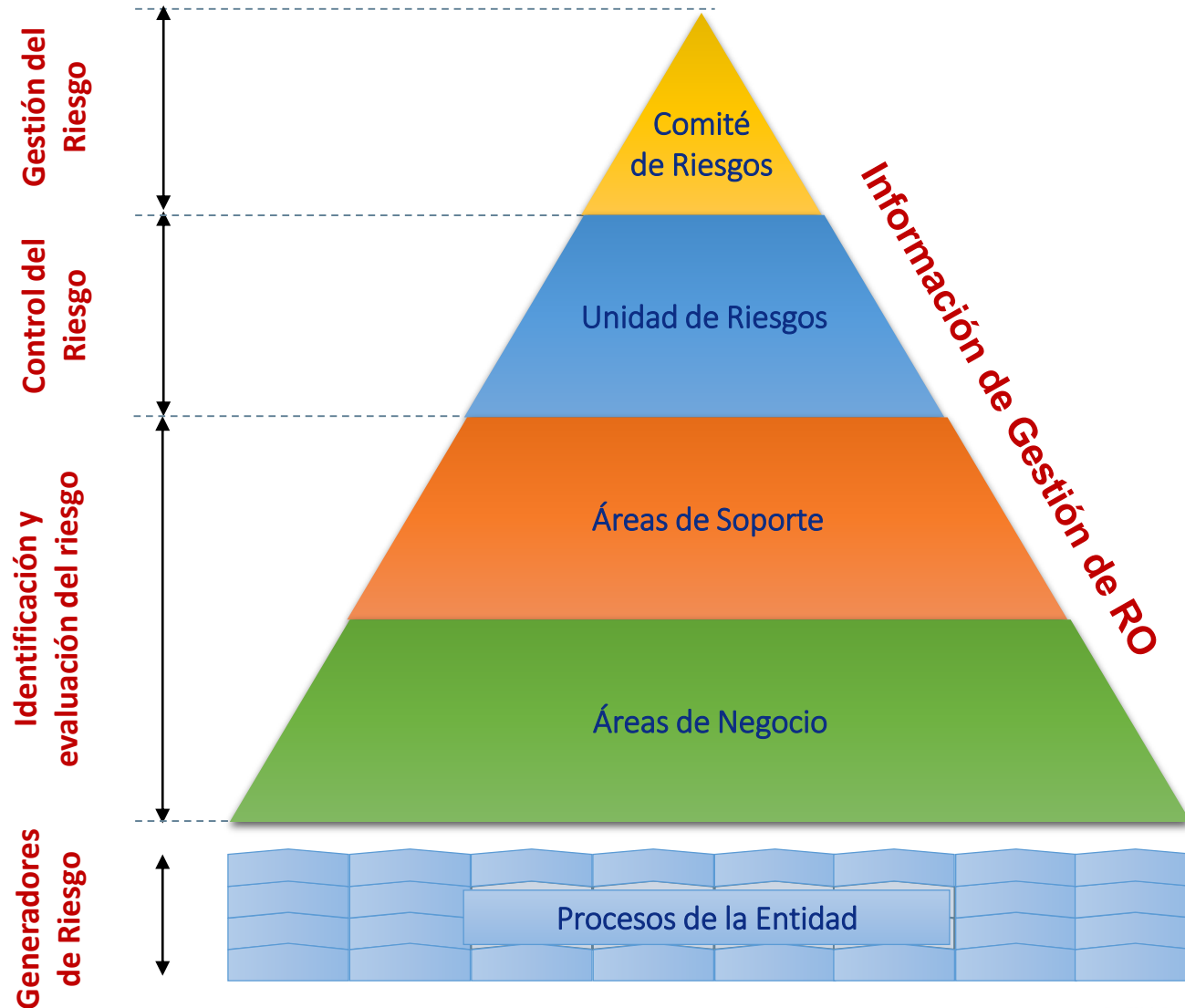


Proceso de gestión



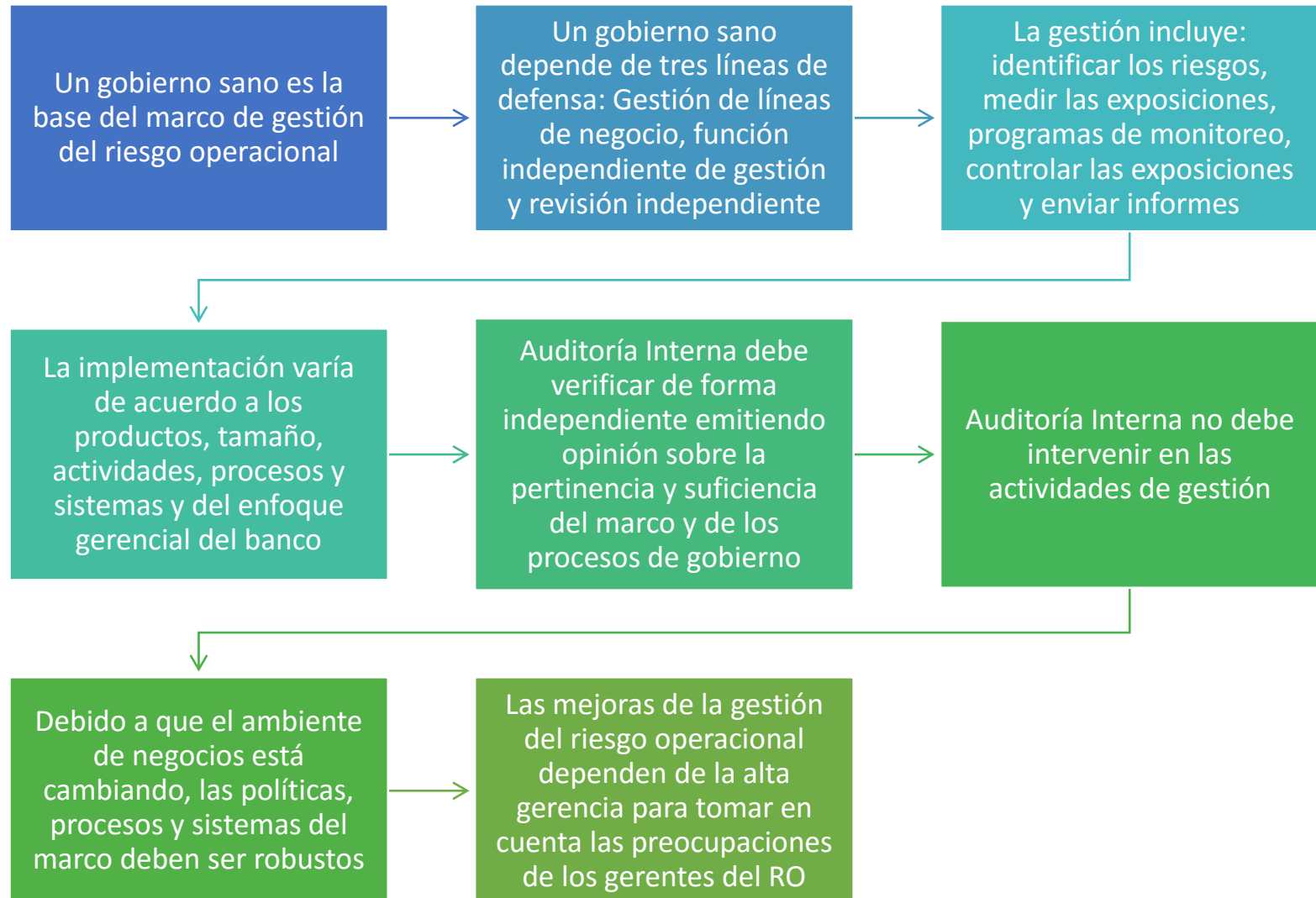


Estructura organizacional





Consideraciones para la Gestión





Superintendencia de Bancos
Guatemala, C.A.

Tres líneas de defensa



Los bancos tienen establecido los roles y responsabilidades de las tres líneas de defensa:

1. Gestión de la línea de negocio
2. Función independiente de la administración del riesgo operativo.
3. Revisión Independiente

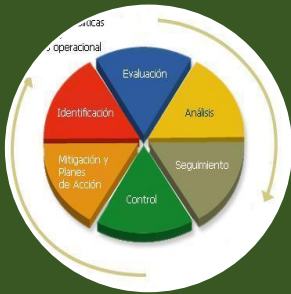


Hay una fuerte cultura del riesgo y una buena comunicación entre las tres líneas de defensa para asegurar un buen gobierno del riesgo operacional.



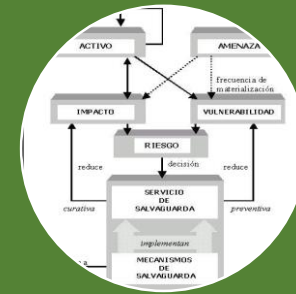
Etapa 1: Identificación

Qué tipo de eventos de pérdida son posibles?



Identificar la exposición al riesgo de pérdida como resultado de:

- a) Actividades fraudulentas/delictivas
- b) Error Humano
- c) Procesos faltantes o mal diseñados
- d) Sistemas fallidos

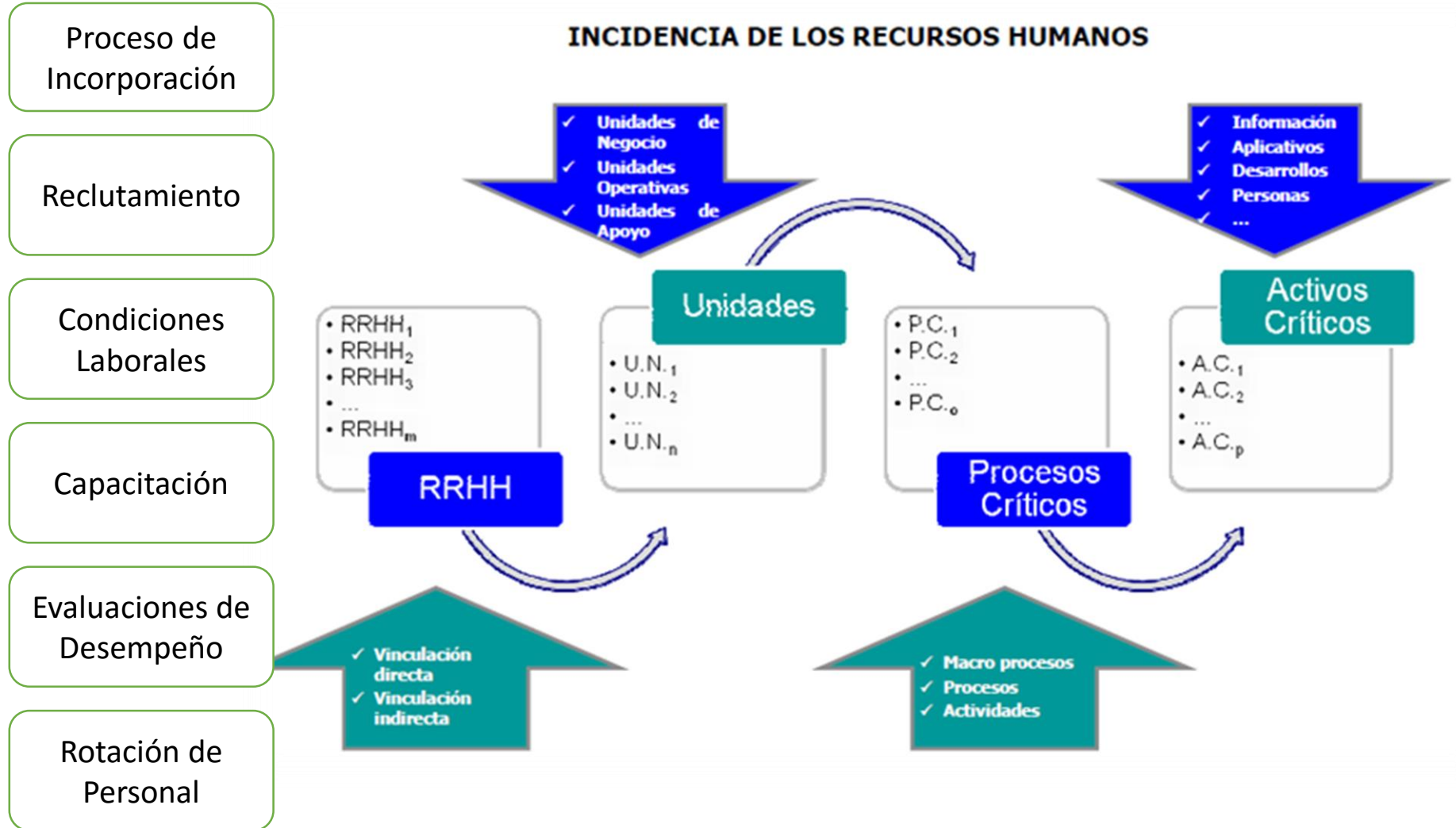


Técnicas para identificar los RO:

- a) Auto Evaluaciones
- b) Gerentes de Riesgo de línea de negocio
- c) Programas de Revisión de Productos Nuevos y Cambiados



Recurso Humano





Recurso Humano

Negligencia

Error Humano

Sabotaje

Fraude

Robo

Paralizaciones

Apropiación de
Información
Sensible

Lavado de
Dinero

Inapropiadas
relaciones
laborales

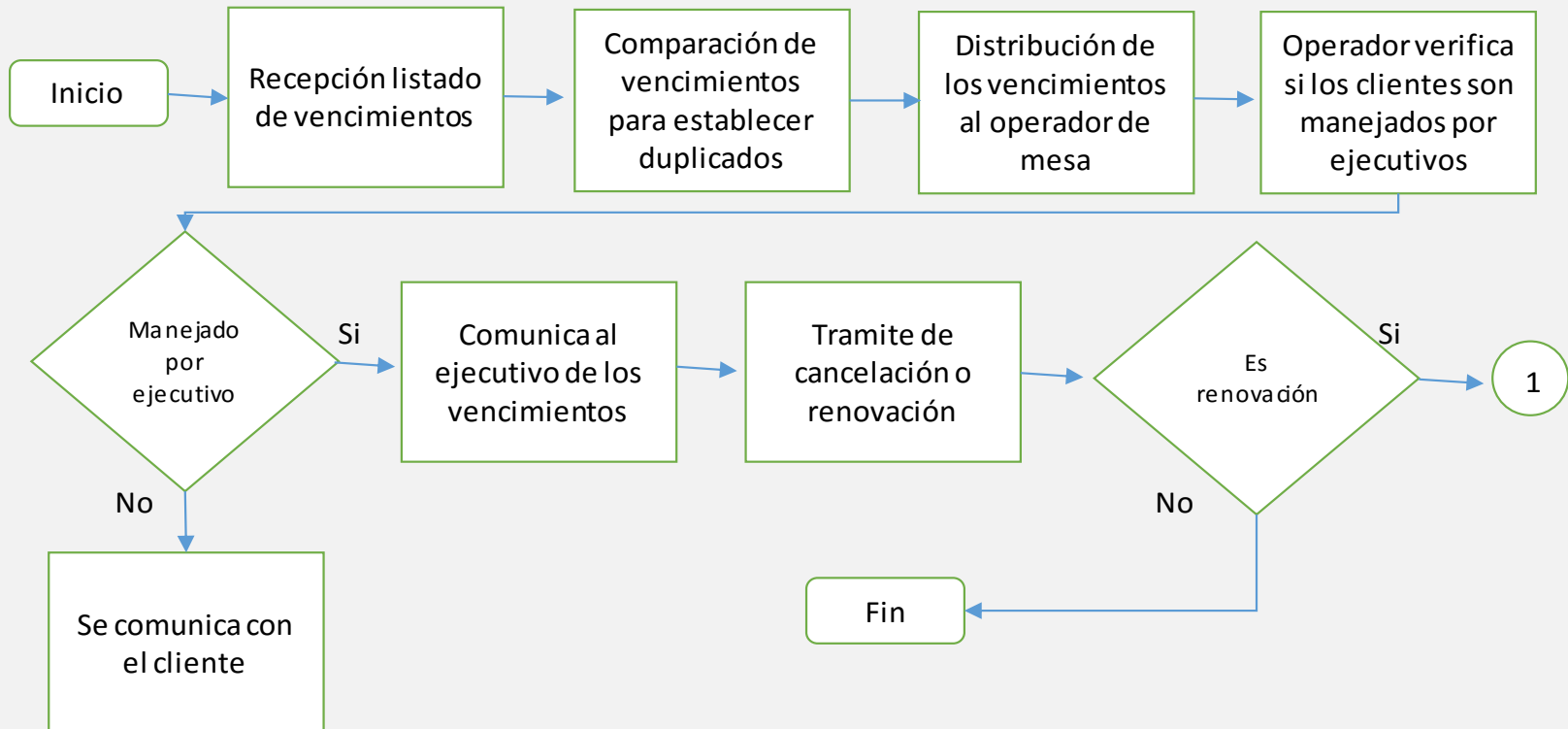
Ambiente
laboral
desfavorable

Insuficiencia
de personal

Entrenamiento
y capacitación
inadecuado

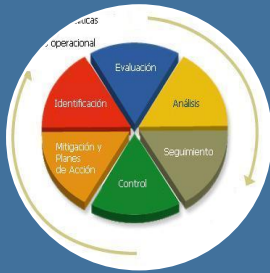


Revisión de Procesos Vencimiento de Depósitos a Plazo



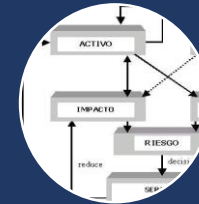
Etapa 2: Evaluación

Cuál es la exposición actual o potencial?



La exposición al riesgo es la combinación de la frecuencia y severidad de los eventos de pérdida.

Técnicas para evaluar el RO



- a) Niveles de Tolerancia
- b) Umbrales de Riesgo de la Línea de Negocio
- c) Datos de Pérdida Interna / Externa
- d) Gerentes de Riesgo de Líneas de Negocio.



Evaluación -matriz de frecuencia-

CLASIFICACION		PROBABILIDAD	DESCRIPCION	FRECUENCIA
RARA	1	Insignificante (muy improbable)	Eventos que son extremadamente raros	6 años o menos
POCO PROBABLE	2	Podría ocurrir en algún momento (poco probable pero posible)	Eventos que ocurren en circunstancias excepcionales	Una vez cada 3 años
FRECUENTE	3	Debería ocurrir en algún momento (moderada)	Evento que ocurre algunas veces	Anualmente
PROBABLE	4	Muy probablemente ocurrirá en algún momento (muy probable)	Evento que probablemente ocurrirá en la mayoría de circunstancias	Semestralmente
ESPERADA	5	Ocurrirá en la mayoría de los casos (alta incertidumbre)	Evento que ocurrirá en la mayoría de circunstancias	Al menos mensualmente

OBJETIVO: establecer la probabilidad de ocurrencia de cada evento sin considerar los controles.



Evaluación -matriz de severidad-

CLASIFICACION		PERDIDA DIRECTA	DESCRIPCION	FACTORES QUE INFLUENCIAN EL VALOR	
				Regulatorio	Servicio al Cliente
INSIGNIFICANTE	1	Por definir *	Pérdidas financieras pequeñas, no hay pérdidas para los clientes	Sin impacto	Sin cuidado
MENOR	2	Por definir	Pérdidas financieras promedio, pocos clientes sufren pérdidas	Intento infructuoso de acceso a los sistemas operacionales	Impacto pequeño
MODERADA	3	Por definir	Pérdidas financieras moderadas, sin pérdida reputacional total	Penetración lógica en los sistemas operacionales del banco	Número significativo de clientes afectados
MAYOR	4	Por definir	Pérdidas financieras mayores, pérdida de reputación general	Investigación policial o regulatoria	Pérdida prolongada de servicios en las últimas 24 horas
MASIVA (CATASTROFICA)	5	Por definir	Pérdidas financieras inmensas, seria pérdida reputacional	Fallo significativo del sistema total	Inconveniente para todos los clientes



Superintendencia de Bancos
Guatemala, C.A.

Evaluación – riesgo bruto

- Cuando ya se tiene la probabilidad y el impacto de cada evento, estos se multiplican para obtener el nivel de riesgo bruto.





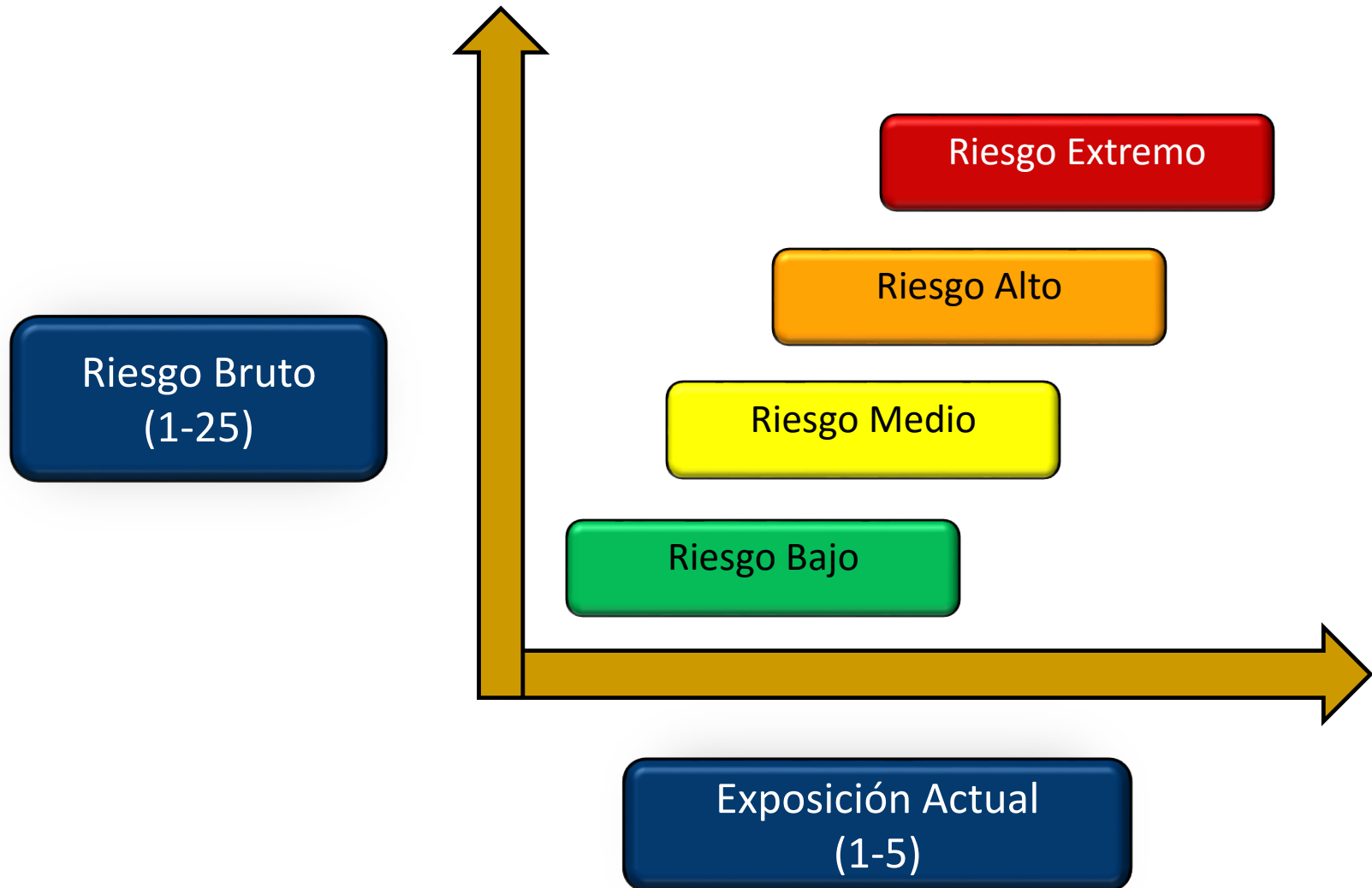
Evaluación - matriz de exposición actual -

EXPOSICION		EXISTENCIA DE PROCEDIMIENTOS	ULTIMOS CAMBIOS	CONTROL	CONTINGENCIA
MENOR	1	Se evalúa con los actuales procedimientos	Estable por 3 años	Definición detallada para todos los roles. Los controles son adecuados	Existe planes de contingencia completos
LIMITADA	2	Los procedimientos cubren todas los puntos clave del proceso	Cambios limitados en un año	Roles claros para la mayoría de actividades. Los controles son adecuados; sin embargo existen debilidades que no representan un riesgo significativo	Recuperación en 24 horas
MEDIA	3	Los procedimientos cubren la mayorías de los puntos clave del proceso	Existen nuevos proyectos que afectarán la operación	Roles definidos de manera general con problemas menores. Controles con debilidades que representan un	Recuperación en pocas horas
SIGNIFICANTE	4	Los procedimientos no cubren la mayorías de puntos clave	Grandes cambios en los métodos de trabajo en los siguientes 6 meses	Falta de implementación de acciones correctivas de largo plazo. Los controles no son de nivel aceptable.	Contingencia menor
MAYOR	5	No existen procedimientos	Actualmente en cambio y con alta incertidumbre	Falta de definición de responsabilidades y niveles de control	Sin planes de contingencia



Superintendencia de Bancos
Guatemala, C.A.

Evaluación





Evaluación

Como resultado de la valoración de los riesgos en cuanto a probabilidad e impacto, así como de los controles, se obtiene la clasificación global o riesgo residual. El resultado permite determinar las prioridades y planes de acción específicos para contrarrestar las vulnerabilidades encontradas.

MATRIZ DE RIESGO OPERACIONAL
CLASIFICACIÓN GLOBAL

RIESGO 2/	EXPOSICIÓN ACTUAL 1/				
	1	2	3	4	5
>10	C	B	A	A	A
	C	B	A	A	A
8 - 10	C	B	B	A	A
	C	B	B	A	A
5 - 7	C	C	B	B	A
	C	C	B	B	A
3 - 4	D	C	C	B	B
	D	C	C	B	B
0 - 2	D	D	C	C	C
	D	D	C	C	C

 Riesgo Extremo
 Riesgo Alto
 Riesgo Moderado
 Riesgo Bajo

1/ Derivado de la matriz de exposición

2/ Derivado de la matriz de frecuencia y severidad.

OBJETIVO: Priorizar los planes de mitigación de acuerdo al nivel de riesgo y la exposición actual

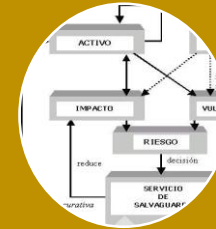
Etapa 3: Mitigación

Cómo se debería abordar cada riesgo?



Mitigando los Riesgos Operacionales mediante una de cuatro estrategias:

1. Evitando el Riesgo (eliminando productos o servicios, salirse del negocio)
2. Controlando el Riesgo (Implementando controles nuevos, mejorados, capacitación, revisando, responsabilidades, etc.)



3. Transfiriendo el riesgo (subcontratación de actividades/controles de terceros, seguros)
4. Aceptando el riesgo (precios más altos para compensar los riesgos, estableciendo reservas)





Mitigación

- Se elabora un resumen de todos los riesgos el cual contiene:
 - Clasificación del riesgo
 - Factor de riesgo
 - Nombre del riesgo
 - Valoración del riesgo bruto (probabilidad x impacto)
 - Valoración del control (exposición actual)
 - Valoración del Riesgo Residual
- La clasificación global es evaluada por el Comité de Riesgos con la finalidad de determinar cómo será administrado el riesgo y en qué casos se deberán establecer tratamientos. Los posibles tratamientos o respuestas al riesgo detectado son las siguientes:



Mitigación





Superintendencia de Bancos
Guatemala, C.A.

Mitigación

R
i
e
s
g
o
s

Evitar

Retiro de actividades causantes de riesgos en las cuales su tratamiento adicional no es efectivo en costo y el retorno no es atractivo en relación al riesgo involucrado (por ejemplo revocación de proyectos).

Reducir

Actividades y medidas tendientes a reducir la **probabilidad de ocurrencia y/o minimizar la severidad** de su impacto (por ejemplo planes de continuidad, cambio de políticas).

Transferir

Actividades y medidas tendientes transferir **a un tercero la responsabilidad por el manejo de riesgos y/o obligación por las consecuencias financieras del riesgo**, en caso de ocurrencia (por ejemplo seguros, sub-contratación).

Aceptar

Aceptación de **riesgo** donde el tratamiento adicional del mismo **no es costoso**, pero los retornos potenciales son atractivos en relación con los riesgos involucrados.

Etapa 4: Monitoreo e Informes

Cómo se debería informar sobre los datos y métrica de RO?



Informar y monitorear los riesgos operacionales residuales.

Técnicas para informar y monitorear:

1. Datos de pérdida interna.
2. Indicadores (Métricas de los indicadores de riesgos claves).



3. Informes sobre exposición al Riesgo Residual

4. Informes de Gerentes de Riesgo.

5. Auditoría Interna.





Superintendencia de Bancos
Guatemala, C.A.

Registro de eventos de pérdida

Evento	Factor de Riesgo	Línea de negocio	Descripción del Evento
Proceso afectado	Fecha de Ocurrencia	Fecha de Descubrimiento	Registro Contable
	Monto de la Pérdida	Monto Recuperado	



Monitoreo

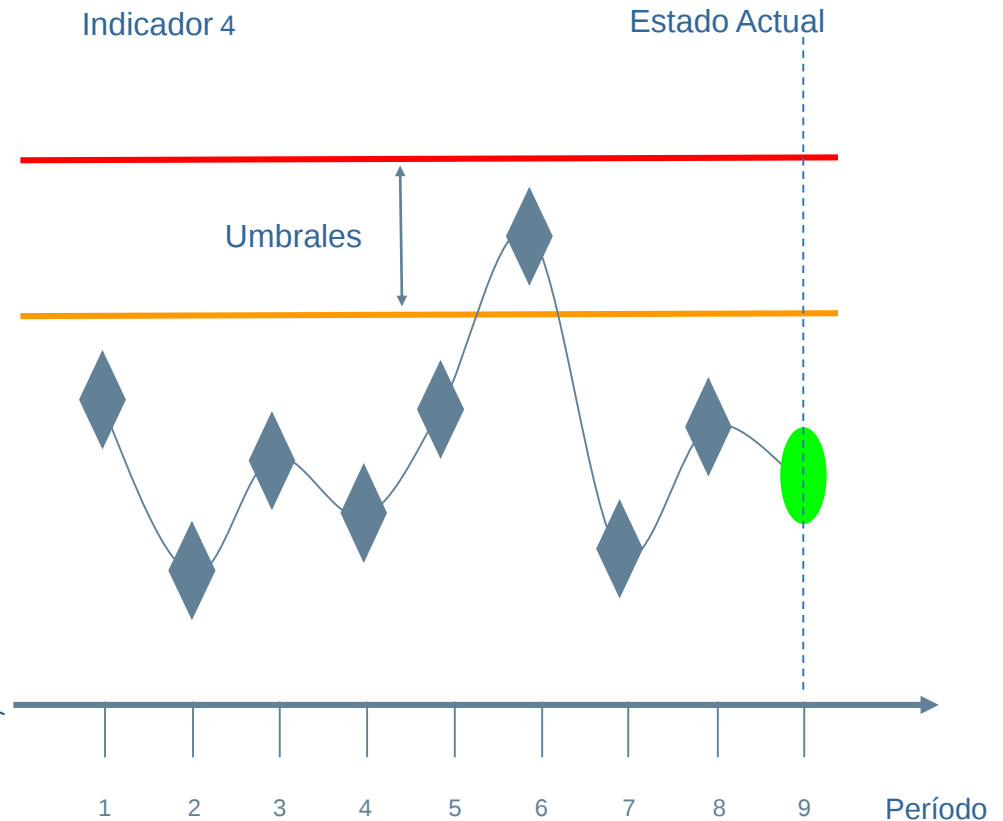
- Una vez identificados y cuantificados los riesgos, es importante disponer de indicadores (conocidos como KRI, Key Risk Indicator) que nos permitan realizar una gestión preventiva de los mismos.
- Las principales características que deben tener los indicadores:
 - La elección del indicador debe ayudar a explicar el riesgo asumido y reflejar el criterio experto del responsable del proceso o de la línea de negocio.
 - De ser posible (no siempre es el caso) los indicadores deberían poder ser traducidos en medidas cuantitativas.
 - Tener sensibilidad al riesgo: un incremento en el valor del indicador debe corresponder a un incremento en el riesgo monitoreado.
 - Los indicadores deben estar bien documentados y sujetos a revisiones independientes.
 - La validez y pertinencia de los indicadores deberá ser validada comparándolos con la historia de pérdidas registradas.



Monitoreo

Establecer un valor óptimo o valor objetivo para cada indicador, y a partir de este valor, fijar unos umbrales de fluctuación en donde el valor se considere como aceptable o crítico.

Indicadores	Estado
Indicador 1	
Indicador 2	
Indicador 3	
Indicador 4	





Monitoreo

INDICADORES DE RIESGO OPERACIONAL

FACTORES DE RIESGO	INDICADOR
PERSONAS	Tasa de rotación de personal
	Costos reales de capacitación
	Ratio de número de días de personal ausente sobre número total de días
	Cantidad de horas extras pagadas
	Ausentismo de personal/ tasa de enfermedades
PROCESOS	Número de superación de límites establecidos
	Número de observaciones/cargos debidos a incumplimientos regulatorios
	Volumen de transacciones
PRODUCTOS	Discrepancias en el número de confirmaciones de operaciones
Y	Número de quejas de clientes
CLIENTES	Número/porcentaje de cuentas de clientes con documentación incompleta
SISTEMAS	Número y tipo de violaciones de seguridad
	Número de incidentes con virus informáticos
	Tiempo de sistema caído
	Porcentaje de disponibilidad de servidores
	Número de cambios de sistema
	Número de incidentes con sistemas
EXTERNOS	Cantidad de eventos de alarma de robo detectados por el personal de seguridad
	Número de robos en agencias
	Número de ataques informáticos
	Número de fraudes de origen externo exitosos



Monitoreo

- De acuerdo con los datos históricos de pérdidas operacionales recogidas en la base de datos durante un determinado tiempo se debe realizar la modelización para cada factor de riesgo y línea de negocio, lo cual conlleva las siguientes etapas:
 - Modelización de la función de distribución de la frecuencia de ocurrencia de los eventos operacionales.
 - Modelización de la función de distribución de los impactos o pérdidas por evento (severidades).
 - Obtención de la distribución agregada de pérdidas operacional para dicho evento/línea de negocio. Cálculo del Valor en Riesgo Operacional, pérdidas esperadas e inesperadas.



Superintendencia de Bancos
Guatemala, C.A.

Gracias.

 SIB Guatemala  @sib_guatemala  SuperBancosGuatemala