# Gestión Integral de Riesgos
# Noviembre 2016

Econ. Alejandro Bazo Bertrán, MSc
bazo.alejandro@gmail.com
http://alejandrobazo.blogspot.pe/

# INTRODUCCIÓN

*"(…) el curso de la acción adecuada es calibrar al adversario para asegurar la victoria y **calcular los riesgos** y las distancias. Salen vencedores los que libran batallas conociendo estos elementos, salen derrotados los que luchan ignorándolos".*

Sun Tzu, *"El Arte de la Guerra"*, escrito entre el 476 y 221 a.C.

Liu Qibing
Págs. 1 a 2 de Separata

# BOLSA DE METALES DE LONDRES

# FRAUDE FINANCIERO

## BOLSA DE METALES DE LONDRES

En 2005, **Liu Qibing**, un operador en la Bolsa de Metales de Londres que **trabajaba supuestamente en representación del gobierno chino** (ligado a la Comisión nacional de Desarrollo y Reforma), apostó erróneamente a que el precio del cobre iba a caer, acumulando pérdidas por más de **USD.800'MM**. Liu vendió una posición corta de entre 100 y 200 mil toneladas de cobre, con la esperanza de comprarlo cuando su precio bajara (lo que no ocurrió).

Qibing apostó por que los precios, después de subir un 34% desde principios del año 2005, bajarían durante el verano (hemisferio norte), pero sucedió lo contrario.

El intermediario chino debía entregar la mercancía a un precio muy inferior, algo imposible de cumplir por plazo y porque en todo el mundo hay unas 140,M toneladas almacenadas oficialmente.

# FRAUDE FINANCIERO

**BOLSA DE METALES DE LONDRES**

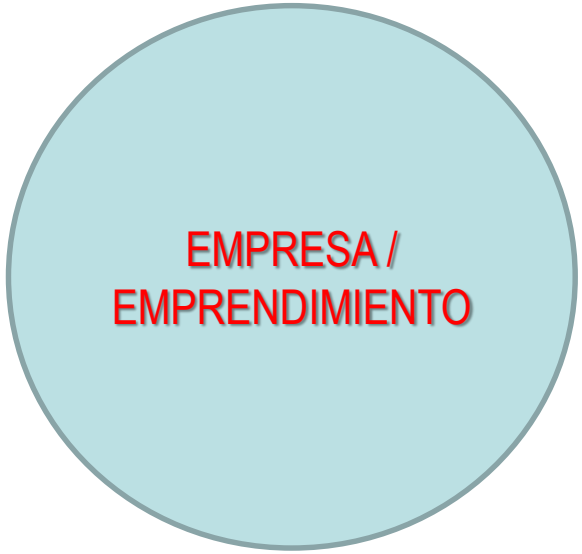
El buró de la Reserva Estatal de Shangai donde supuestamente trabaja Liu Qibing, negó conocerlo. El diario oficial *China Daily* aseguró que el intermediario actuó por iniciativa propia.

Inicialmente el gobierno chino negó su existencia, pero posteriormente reconoció haberlo detenido para interrogar. Finalmente informó que fue condenado a 7 años de prisión.

**Políticas:**

Conoce a tu empleado / Conoce a tu cliente / Conoce a tu proveedor.

Analicemos cada uno de los componente de esta ecuación

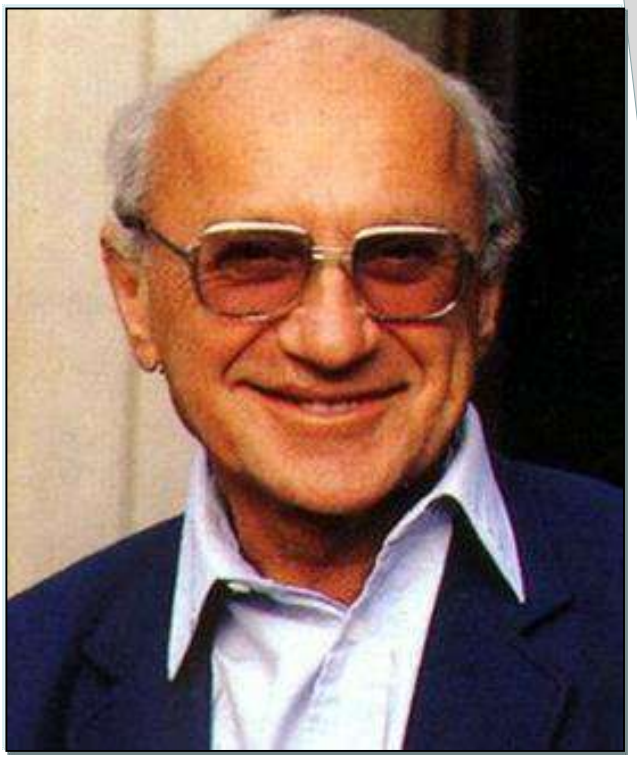



- ¿Qué es la economía?
- ¿Qué es la empresa?
- ¿Cuál es su relación?
- ¿Qué buscamos con ella?
- ¿Cuál es su verdadero valor?

"La fortuna favorece a los valientes"

Virgilio – Roma, Siglo I a.C.

"Solo hay **una y única responsabilidad social de las empresas**: usar sus recursos para participar en actividades diseñadas para **incrementar sus beneficios**, siempre y cuando se mantenga dentro de las **reglas de juego**, es decir, se dedica a la **competencia libre y abierta, sin engaño o fraude**."



Citando al premio Nobel de Economía, Milton Friedman, precursor de la Escuela de Chicago, que sostenía en la década de los setenta que la responsabilidad de las empresas es maximizar sus beneficios y no dedicarse a la filantropía ni a la acción social.

"Capitalism and freedom", Milton Friedman. América Economía, Feb./2013

“ ‘…el liberalismo económico **sin reglas y sin controles** es una de las causas de la actual crisis económica’ al crear ‘mercados financieros fundamentalmente especulativos, dañinos para la economía real, especialmente en los países debiles’ ”

Fuente: América Economía, abril de 2013

# CUESTIONANDO A FRIEDMAN

Los valores inciden en el modo en que la empresa es gestionada, la manera de tratar a sus colaboradores, las empresas a las que vende y los países donde opera.


Para desarrollar una empresa que sea admirada, es necesario que la empresa sea también buena en un sentido moral. Una empresa así, atraerá profesionales de alto nivel para un proyecto empresarial que trascienda.

# CUESTIONANDO A FRIEDMAN

**Una empresa bien gobernada, respeta:**

- Su Visión / Misión.
- Sus Valores.

Que la proyectan en el largo plazo

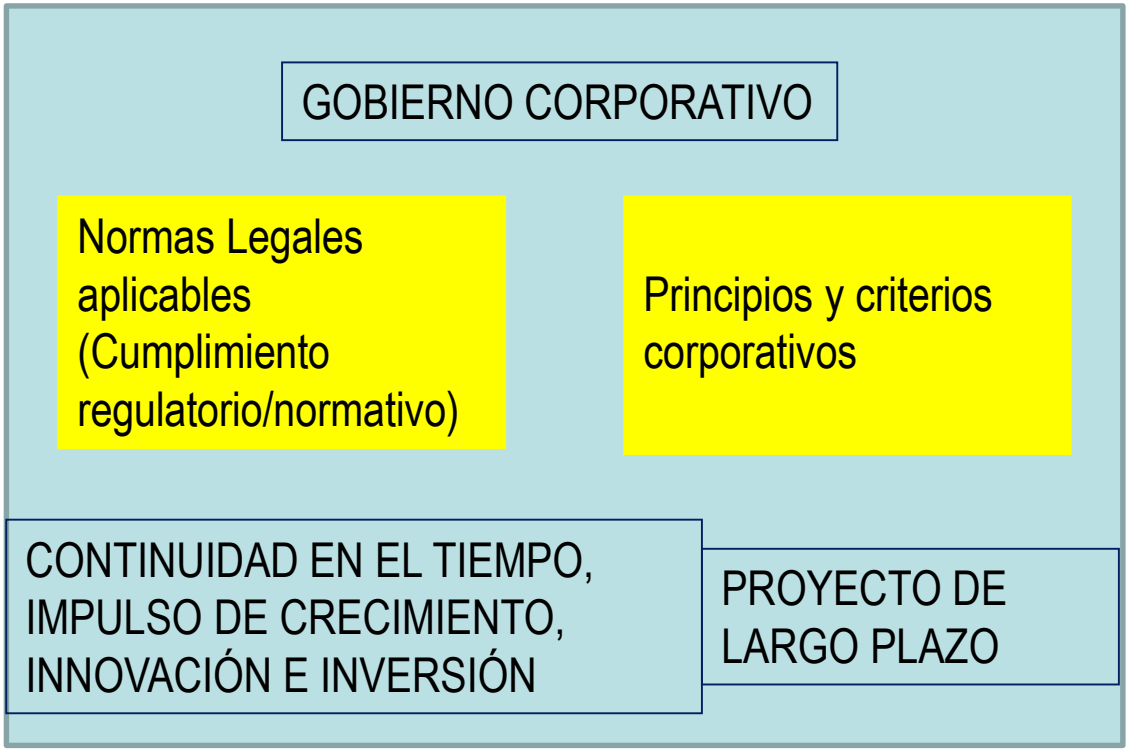
- Sus obligaciones legales.
- Los intereses de sus accionistas (incluidos los minoritarios).
- Define los conflictos de interés.
- Tiene implementado un eficiente sistema de control.

**Importante:**

**Las empresas que no tienen voluntad de permanecer en el largo plazo son sólo un negocio.**

**El control viene siempre de arriba hacia abaja.**

# CUESTIONANDO A FRIEDMAN



Ética individual y de negocios deben ir de la mano para poder asegurar buenos resultados.
Cuando no existe se desencadena el caos o un desequilibrio en el modo de proceder frente a dilemas empresariales.

Especialmente cuando la ética se va disolviendo en los altos mandos, se desencadenan hechos fraudulentos de mayores proporciones.

La falta de regulación de los mercados financieros y la debilidad de los organismos controladores constituyen una amenaza para la economía en general y refleja la volatilidad de los mismos.

La magnitud de muchos problemas pudo ser evitada si los organismos de control hubieran actuado a tiempo.
Es importante que cada organización cumpla de manera apropiada su rol.

INNOVACIÓN

- ¿Qué es la innovación?
- ¿Qué buscamos con ella?
- ¿Cuándo se presenta?
- ¿Cómo nos afecta?

## Innovaciones

Piense en alguna innovación que haga que debamos actualizar o revisar el marco normativo. Entonces, ¿es posible que la normativa vaya a la par de las innovaciones?

# NORMATIVA - ¿PARA QUÉ?

1769 – Primer vehículo a vapor "Fardier" (Nicolás Cugnot)

1889 – Primera fábrica de automóviles (Francia)

1908 – Henry Ford inicia la producción en cadena de montaje

1760 1770 1780 1790 1800 1810 1820 1830 1840 1850 1860 1870 1880 1890 1900 1910 1920 1930 1940 1950 1960

Se inicia la producción masiva de automóviles

1886 – Primer vehículo con motor de combustion interna (Karl Benz), modelo Benz Patent-Motorwagen.

1889 – Chicago pide a los conductores que pasen un examen. Nueva York requiere de un Ingeniero licenciado para conducir un coche a vapor.
1903 – Primer piloto de licencias (Massachusetts y Missouri)
1908 – Primer congreso de transito vial (Roma)
1909 – Covención Internacional de Ginebra
1959 – Dakota del Sur exige exámen a los conductores.
1968 - Convención de Viena

# NORMATIVA - ¿PARA QUÉ?

**Innovaciones**

Fuente: Diario “El Comercio”, 09/Sep/2015, A18

# Europa apoya extender el veto a la clonación animal

Parlamento europeo busca prohibir la importación de productos de crías de animales clonados.

**Estrasburgo** *[AFP]*. El Parlamento Europeo (PE) aprobó por mayoría un informe que sugiere que la prohibición de la clonación de animales en Europa debería extenderse a la importación de sus crías, así como a los alimentos producidos a partir de estos descendientes. Esta medida impondría a los socios comerciales de la Unión Europea (UE) rígidas condiciones para acceder esta clase de productos.

“La clonación es tortura animal”, resumió la relatora del texto, la conservadora alemana Renate Sommer. La experta explica que los animales concebidos por este método sufren malformaciones y tienen una elevada tasa de mortalidad.

Según la Autoridad Europea de Seguridad Alimentaria (EFSA), la “clonación pone en peligro el bienestar de los animales, dada la escasa eficacia de la técnica”.

En la UE no se procede en la actualidad al uso de esta técnica con fines de reproducción, pero los estados miembros pueden importar desde terceros países productos de animales clonados, como esperma y embriones, así como de los descendientes de animales clonados y sus productos.

Los productos de animales descendientes de especímenes clonados provienen principalmente de Estados Unidos, Argentina, Brasil y Uruguay.

La propuesta inicial alcanzaba a los animales de las especies bovina, porcina, ovina, caprina y equina, pero los eurodiputados modificaron esto y la ampliaron a todos los animales.

Un total de 529 diputados votaron a favor del texto, 120 en contra y 29 se abstuvieron.

La próxima etapa en el proceso legislativo será una negociación, que se anuncia complicada, entre el Parlamento, la Comisión y los estados miembros de la UE. Luego de esto se pasará a la etapa final de la aprobación de esta ley.

BLOOMBERG

**LEY.** La norma busca proteger a los animales de ser expuestos a malas prácticas bajo el amparo de necesidades comerciales.

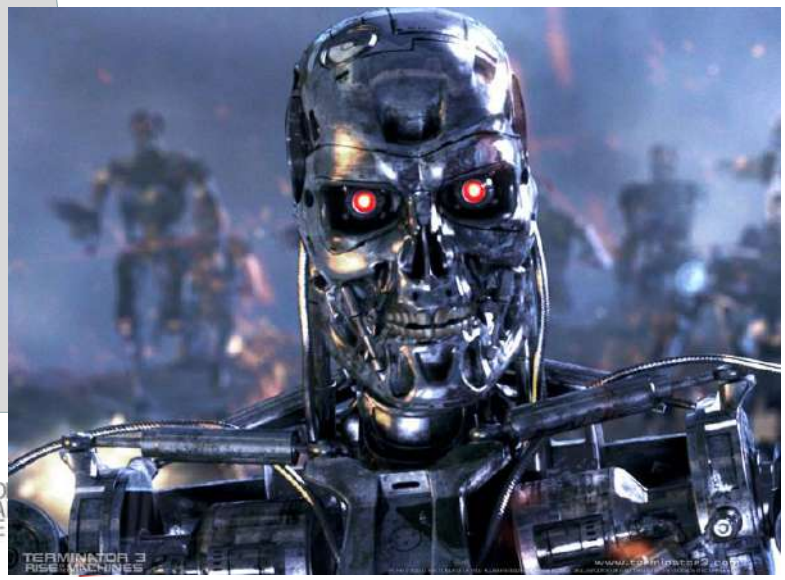
# NORMATIVA - ¿PARA QUÉ?

**Innovaciones**

El robot Atlas, creación de la empresa Boston Dynamics, que pertenece a Google, se encuentra aprendiendo a correr y saltar libremente por el bosque, según un video difundido por la compañía.

Aunque se trata de **un androide que supera los 182 centímetros y pesa prácticamente 150 kilogramos,** el correr por los desniveles de un bosque natural no parece resultarle una tarea complicada.

Fuente: http://pe.tuhistory.com/noticias/un-historico-paso-hacia-la-inteligencia-artificial (09/Sep/2015)



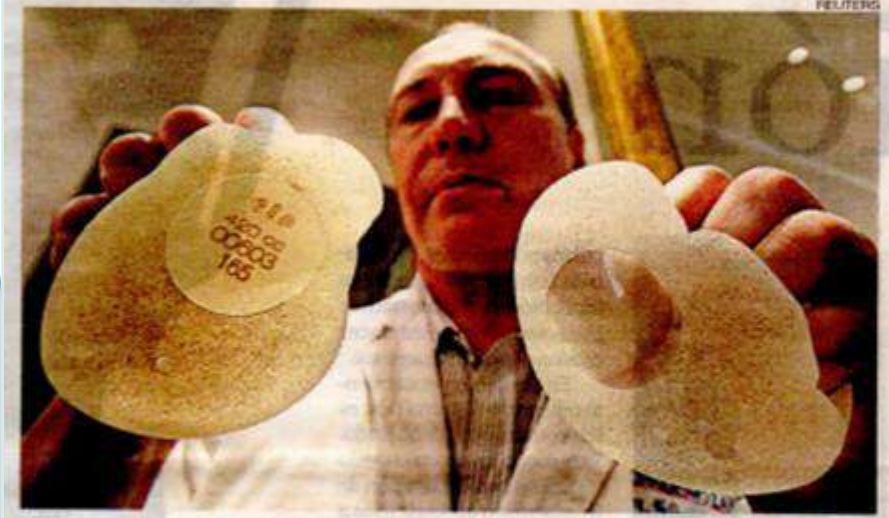
# NORMATIVA - ¿PARA QUÉ?

**Innovaciones**

El mes pasado, un hombre de Kentucky derribó un drone que sobrevolaba cerca de su patio trasero.
"Cuatro hombres llegaron a enfrentarme al respecto, y resultó que yo estaba armado, así que cambiaron de opinión", dijo Merideth. "Me preguntaron: '¿Eres el hijo de p** que le disparó a mi drone?, y yo les respondí: "Sí, yo soy'", dijo. "Tengo una Glock 40 mm y se me empezaron a acercar y les dije: 'Si cruzan mi acera, va a haber otro tiroteo'". La policía presentó cargos contra Merideth por conducta criminal y por poner en peligro a las personas.
La tecnología cambia todo. En concreto, cambia drásticamente el equilibrio social de hace mucho tiempo en torno a temas como la seguridad y la privacidad. Cuando una capacidad se hace posible, más barata o más común, los cambios pueden ser trascendentales. Reequilibrar la seguridad y privacidad después de las capacidades por los cambios tecnológicos podría ser muy difícil y toma años. Y no somos muy buenos en eso.
Fuente: http://cnnespanol.cnn.com/2015/09/09/esta-bien-derribar-un-drone-que-sobrevuela-sobre-tu-casa/
(09/Sep/2015)

- ¿Qué es el riesgo?
- ¿En qué circuntancias aparece?
- ¿Cómo nos afecta?

# Mil sudamericanas se suman a demandas por implantes



REUTERS

**FIN.** La industria PIP quebró en el 2010 ante reiteradas denuncias de roturas de sus prótesis.

**Nuevas denuncias se agregan a las cerca de 2.500 recibidas la semana pasada**

**PARÍS** [AFP]. Un millar de mujeres argentinas y venezolanas demandarán en Francia por homicidio y lesiones involuntarias a la empresa francesa PIP, que produjo prótesis mamarias defectuosas, informó el abogado de las demandantes, Ari Alimi.

**DEMANDANTES**

El representante legal informó que defiende a un grupo de 500 mujeres argentinas y una asociación venezolana de 500 mujeres.

Añadió que otras víctimas latinoamericanas, principalmente de Brasil y Colombia, podrían sumarse a la demanda que será presentada en Marsella, lugar donde la empresa PIP tenía su sede.

Según el abogado, el 80% de las prótesis PIP fue implantado en América Latina, incluso enfatizó que solo en Argentina la cifra se elevaría a 15.000 mujeres.

Las demandantes latinoamericanas contemplan además la posibilidad de pedir explicaciones a la Agencia Francesa de Productos de la Salud (Afssaps) y al laboratorio alemán TÜV Rheinland, organismo de certificación, advirtió Alimi.

**EL DATO**

El escándalo de los implantes Poly Implant Prothese (PIP) partió de Francia y tomó una dimensión internacional, ya que entre 400.000 y 500.000 mujeres en todo el mundo portarían estos implantes.

**CASOS PERUANOS**

En el Perú la marca francesa no tuvo mucho éxito, a pesar de ofrecer su producto a precios bajos. Según los reportes de Aduanas, entre el 2006 y el 2007 la representante de PIP en el país, Medsurgical Perú S.A.C., importó solo 341 unidades, pero hasta hoy las autoridades no saben dónde ni quiénes las adquirieron. ■

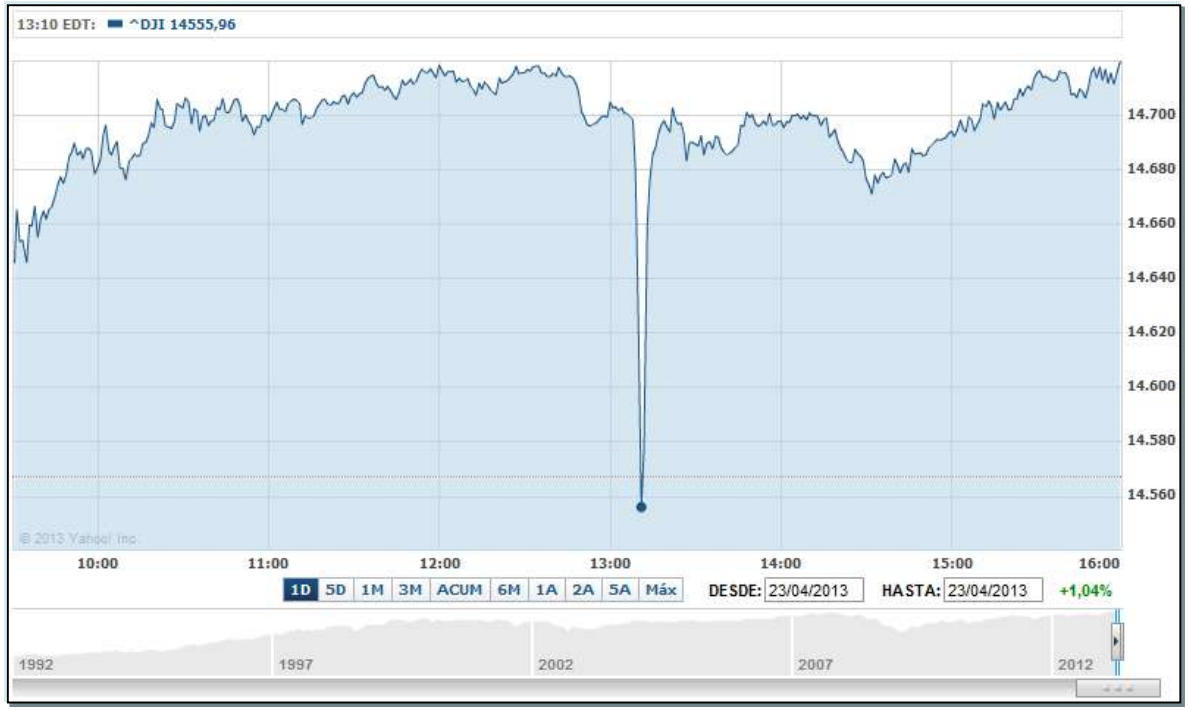
Fuente: El Comercio, 11/Ene/2012

Implantes de mama

Págs. 3 a 6 de Separata

**Responda las siguientes preguntas:**

- ¿Quién se ve afectado por este evento de manera primaria?
- ¿Quién se ve afectado por este evento de manera secundaria?
- ¿Qué implicancias puede tener para el mercado?
- ¿Se pudo prevenir? ¿Quién y cómo lo debió prevenir?
- ¿Cómo funcionaron los controles?




«Falso atentado contra Barack Obama ocasiona caída de hasta 150 puntos en el Dow Jones.
El falso atentado anunciado en la cuenta de Twitter de la agencia de noticias de Associated Press ha provocado un pequeño ataque de pánico en Wall Street».
Fuente: Alcierre, 23/Abr/2013

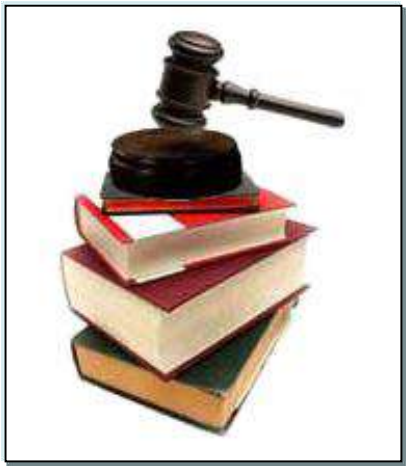
Falso atentado
Pág. 7 de Separata

**Responda las siguientes preguntas:**

- ¿A qué riesgos estamos expuestos en nuestra constante actividad?
- ¿Cómo definimos los controles?
- ¿Podemos estar preparados para todos los eventos que nos pueden ocurrir?

# CAMBIO DE TENDENCIAS EN EL MARCO REGULATORIO

# ¿Cómo marcamos las reglas claras en una sociedad?



A través del marco regulatorio y normativo

Y, ¿para qué nos sirve este marco normativo?
¿funciona?
¿Por qué no es efectivo en ocasiones?


Yo no necesito normativa que me proteja porque confío en mi asesor de inversiones!!!

No me compliquen la vida con normas aburridas que leer y peor aún … que tengo que cumplir!!!!!

- Los mercados se regulan para crear **condiciones homogeneas** que puedan ser **conocidas y seguidas por todos sus integrantes**, generando **igualdad de oportunidad** para sus integrantes.
- De esta manera se establecen **obligaciones** y se protegen los **derechos** de los participantes.

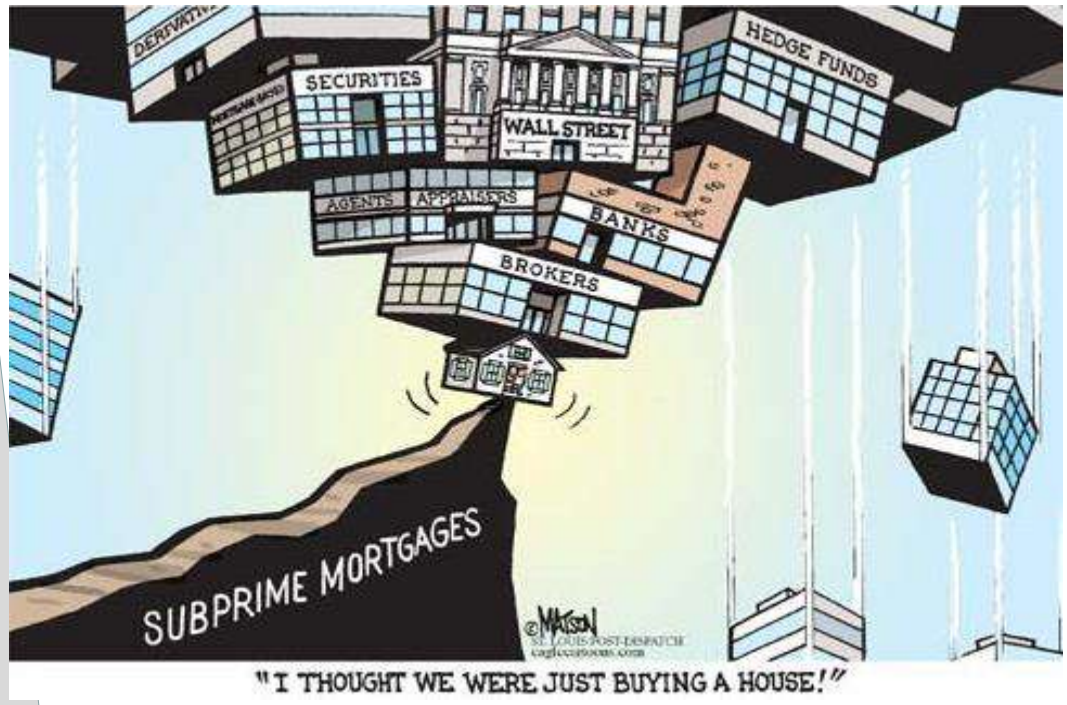
La legislación financiera se establece para alcanzar dos objetivos primarios:

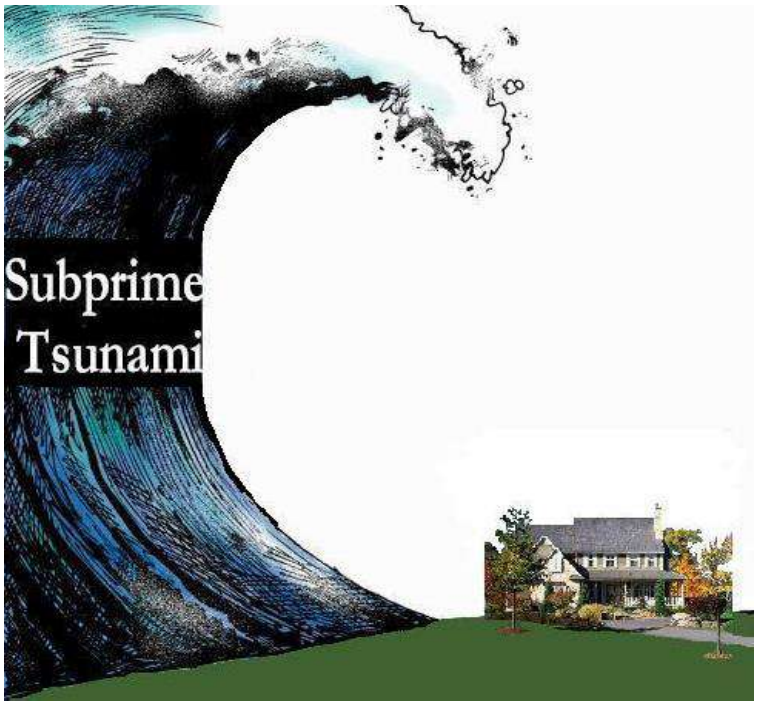
- Ofrecer **información a todos los inversionistas** potenciales de manera que puedan **tomar decisiones con conocimiento adecuado**; y,
- Asegurar la **adecuada solidez de todos los intermediarios financieros**, de modo que los ahorros y las inversiones estén protegidos.

**Pero, ¿en la práctica es así? ¿Esto se logra?**

- ✓ **Solidez de la industria en general y de cada uno de sus participantes en particular**.
- ✓ Entonces: abarca el **monitoreo continuo de la conducción de la industria** y de **sus componentes individuales**, con el fin de garantizar prudencia en las operaciones y la conformidad con leyes y reglamentos.
- ✓ El objetivo principal es **proteger al cliente, al inversionista y salvaguardar la economía contra el funcionamiento incorrecto del sistema**.

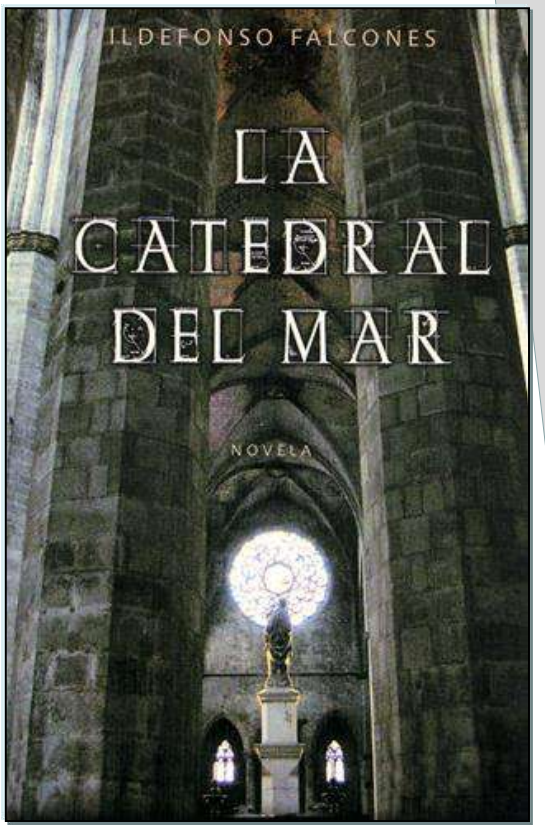
(La legislación debe ser constantemente **revisada y actualizada** y debe **ir a la par y misma velocidad** que las **innovaciones** en los mercados)



## Tema de discusión:

- ¿Se debería regular los precios en la economía?
- ¿Regular las tasas de interés?
- ¿Regular el cobro de comisiones?



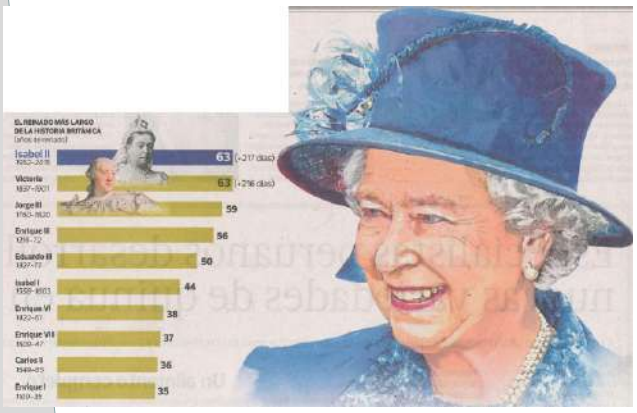
Problema:

¿Cuánto sería lo justo cobrar por el financiamiento?

Y la regulación debe garantizar la solidez del Sistema, el cumplimiento de las obligaciones … pero … ¿Cómo?

# INNOVACIÓN

# FORMAS DE GOBIERNO





**Lecturas**

“Repensando la Democracia”, La columna de FOZ. Semana Económica, 22 de junio de 2014, Pág. 13

Separata página 11

“Encrucinadas”, Opinión, Diario El Comercio, 12 de octubre de 2016, Pág. 26.

Separata páginas 12 y 13

BOLSA DE VALORES DE LIMA BVL

LUCHA CONTRA LA CORRUPCIÓN

Págs. 14 a 15 de Separata



*"Cuando pocos pagan impuestos, como en las economías informales, el saqueo del Estado es un robo a unos pocos contribuyentes, no a la mayoría de ciudadanos, y eso la hace mayoritariamente tolerable".*

Entrevista al Sr. Alfonso García Miró, Presidente de CONFIEP

Fuente: http://semanaeconomica.com/article/economia/144087-confiep-es-necesario-formalizar-relacion-entre-sector-privado-y-publico

PREVENCIÓN CONTRA EL L.A. Y F.T. (PLAFT)

Políticas, procedimientos y estándares que soporten las actividades de PLAFT dentro de las empresas

- Conoce a tu Cliente
- Conoce a tu Proveedor
- Conoce a tu Empleado

Operaciones en efectivo → Operaciones inusuales → Operaciones sospechosas

# INCLUSIÓN FINANCIERA

PERSONAS NATURALES

PEQUEÑAS Y MICRO EMPRESAS

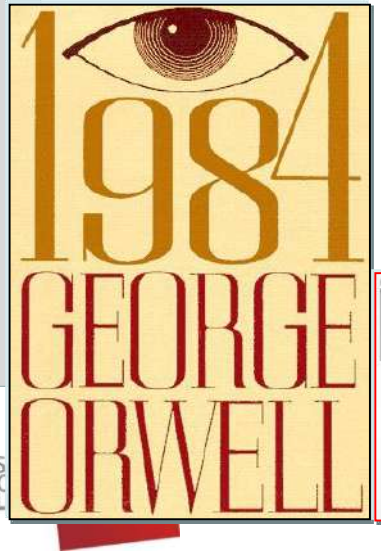
Págs. 16 a 17 de Separata

PROTECCIÓN DE USUARIOS / DATOS

La ampliación de seis meses a dos años del plazo en que los usuarios de las aseguradoras privadas puedan hacer sus reclamos, en la Defensoría del Asegurado, habla del esfuerzo de dichas compañías por autorregularse, en beneficio del sector.

**Eduardo Morón, Presidente de Apeseg**
**Diario El Comercio, 27 de junio de 2016, Día 1, Pág. 02.**

"1984" es una novela de George Orwell, publicada en 1949.

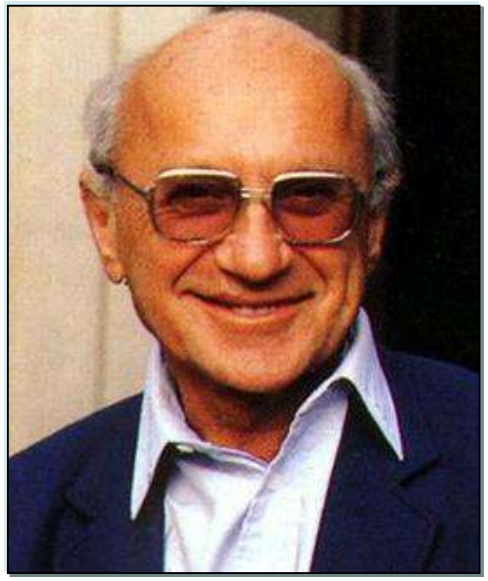




Fuente: América Economía, Ago/2013



# USO DE INFORMACIÓN PRIVILEGIADA



# PROTECCIÓN DEL MEDIO AMBIENTE Y RSE

INNOVACIÓN

INCLUSIÓN FINANCIERA

FORMAS DE GOBIERNO

PROTECCIÓN DE USUARIOS / DATOS

LUCHA CONTRA LA CORRUPCIÓN

USO DE INFORMACIÓN PRIVILEGIADA

PREVENCIÓN CONTRA EL L.A. Y F.T. (PLAFT)

PROTECCIÓN DEL MEDIO AMBIENTE Y RSE

# POLÍTICAS PARA LA GESTIÓN DE RIESGOS

Herramientas utilizadas para la Gestión de Riesgos

Orientadas a institucionalizar las tareas de identificar, monitorear, limitar, controlar, informar y revelar los distintos tipos de riesgo.

Cuerpo de políticas sólido y claro respecto a las medidas a tomar

- Claras
- Específicas
- Mensurable
- Aplicabilidad
- Incumplimiento

# POLÍTICAS PARA LA GESTIÓN DE RIESGOS

Políticas Generales

GIR adecuada al tamaño y complejidad de operaciones y servicios

GIR: rol del Directorio, Gerencia y personal. Aplicado a toda la organización

# POLÍTICAS PARA LA GESTIÓN DE RIESGOS

Políticas Específicas

**Prácticas cuestionables**
Sistemas internos apropiados que faciliten la oportuna denuncia e investigación de las actividades ilícitas

**GIR y CI**
La GIR incluye al CI del que es parte integral

**Declaración de Cumplimiento**
Directorio suscribe una Declaración de Cumplimiento, anual (120 días)

**Comités**
Auditoría / Riesgos / ALCO
Reglamentos: políticas y procedimientos
Libro de Actas

**Unidad de Riesgos**
Experiencia, conocimientos y formación académica
Plan de Capacitación
Reporta a Comité / Informe Anual SBS

**Subcontratación**

**Auditoría Interna**

**Transparencia**

**Auditoría Externa**

# POLÍTICAS PARA LA GESTIÓN DE RIESGOS

**Política de Aceptación**
Aprobación de propuestas de nuevas operaciones, servicios, líneas de negocio, estrategias e iniciativas de administración de riesgos.

**Política de Límites**
Establecimiento de límites aprobados para operaciones.
Adicionalmente se deben establecer límites de emergencia y preveer el actuar de la organización en situaciones de crisis.

**Política de Contingencia**
Casos en los cuales se exceden los límites de riesgo aprobados.
Las contingencias deben activar un Comité de Evaluación de contingencias a fin de determinar el plan de acción a seguir y efectuar el monitoreo de la situación de emergencia, hasta la normalización de la situación que generó la alerta.

# POLÍTICAS PARA LA GESTIÓN DE RIESGOS

***"No es tan cierto que los modelos complicados trabajen necesariamente mejor que las reglas simples … cuando estas están bien formuladas"***

***"Algunos –recordando la frase de Albert Einstein: 'Todo debe hacerse lo más simple posible, aunque sin exagerar'- sugieren mantener simples los procesos y no complicarlos innecesariamente"***

**"Reglas Simples". La columna de FOZ, Felipe Ortiz de Zevallos**
**Semana Económica, 18 de octubre de 2015, Pág. 11**

Criterios que deben cumplir las reglas simples:

i. Ahorro de recursos (tiempo y energía)
ii. Ajuste según las circunstancias
iii. Eliminar confusion
iv. Un marco dentro del cual se pueda improvisar
v. Deben permitir colaboración flexible, especialmente bajo tensión

## PRINCIPALES POLÍTICAS Y LINEAMIENTOS

| Políticas Generales | Políticas Especificas |
|---|---|
| 1. El Directorio es responsable de desarrollar una cultura organizacional relacionada a la GIR de la empresa.<br>2. El Directorio debe brindar las herramientas y recursos necesarios a la Unidad de Riesgos para desarrollar e implementar una adecuada GIR.<br>3. El Directorio debe establecer las políticas y procedimientos relativos a la GIR.<br>4. Para la adecuada GIR, la Unidad de Riesgos propondrá las metodologías y herramientas de gestión de riesgos necesarias.<br>5. Los procesos críticos deberán ser evaluados de forma anual.<br>6. Las actividades de la GIR deberán someterse a una evaluación anual por parte de la Unidad de Auditoría Interna.<br>7. La empresa debe contar con un Sistema de Gestión de Continuidad del Negocio y un Sistema de Gestión de Seguridad de la Información.<br>8. La identificación de riesgos es una responsabilidad de todo el personal de la empresa. | 1. La empresa debe contar con un Manual de GIR, aprobado por el Comité de Riesgos, así como por el Directorio.<br>2. La Unidad de Riesgos debe informar periódicamente al Comité de Riesgos los resultados de la GIR, así como del estatus de su implementación.<br>3. Las subcontrataciones significativas de servicios serán comunicadas a la Unidad de Riesgos.<br>4. La Unidad de Riesgos, debe realizar un informe de evaluación del producto o cambio importante en el ambiente de negocios, operativo o informático, previamente a su lanzamiento o ejecución<br>5. El importe mínimo de pérdida a partir del cual la empresa registrará un evento de pérdida por riesgo operacional en la Base de Datos de Eventos de Pérdida.<br>6. La Unidad de Auditoría Interna debe comunicar los resultados de su evaluación al Comité de Auditoría y al Directorio, así como del seguimiento de las observaciones de la Unidad de Auditoría Interna, Auditoría Externa y al regulador. |

# RIESGOS

# La mastectomía de Angelina Jolie

**PROBLEMA**

87% probabilidad de padecer cáncer de mama

Control

**RESULTADO**

Luego de la cirugía la probabilidad se redujo a 5%

Entre 1998 y 2005, el número anual de mujeres en los Estados Unidos que eligió someterse a una doble mastectomía preventiva se ha duplicado.
En 1997 el 6.7% de mujeres decidieron retirarse ambos senos cuando solo uno tenía cáncer, en el año 2004 ya era el 24%.

Nuevos riesgos asumidos:

- No podrá amamantar luego de la operación;
- Reducirá la sensibilidad en los senos;
- Riesgo de padecer depresión y ansiedad; y,
- No reduce en 100% el riesgo de padecer cáncer.

## Acuerdos de Basilea

En 1988 el Comité de Basilea establece criterios de capital mínimo en función de los riesgos.

El “capital regulatorio” debe ser suficiente para hacer frente a los riesgos de crédito y mercado.

Fines principales: (i) cubrir riesgos; y, (ii) proporcionar igualdad competitiva.

No vinculante / Incorporado en la legislación de más de 120 países

# Acuerdos de Basilea

**ACUERDO DE BASILEA II**

**1er. Pilar:**
**Cálculo de los requerimientos mínimos de capital**

- I. Riesgo de crédito: Método Estándar
- II .Riesgo de crédito: Método basado en calificaciones internas
- III. Riesgo de crédito: Marco de titulización
- IV. Riesgo operativo
- V. La cartera de negociación (incluido el riesgo de mercado)

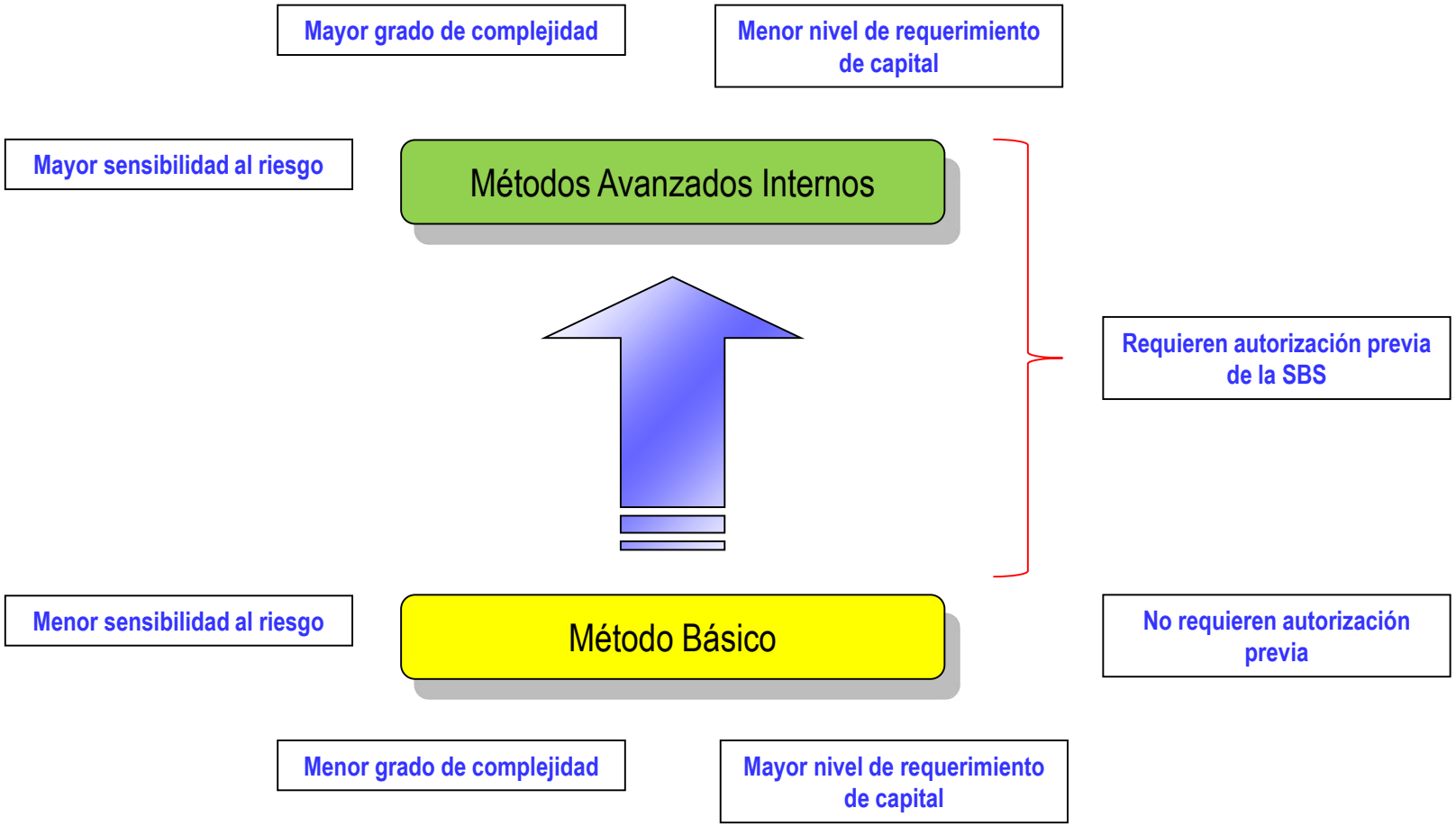
**2do. Pilar:**
**Revisión supervisora**

**3er. Pilar:**
**Disciplina de mercado**

Mayor estabilidad del sistema financiero y mayor protección de los ahorros del publico.

Págs. 19 a 23 de Separata

# MÉTODOS PARA CALCULAR EL REQUERIMIENTO



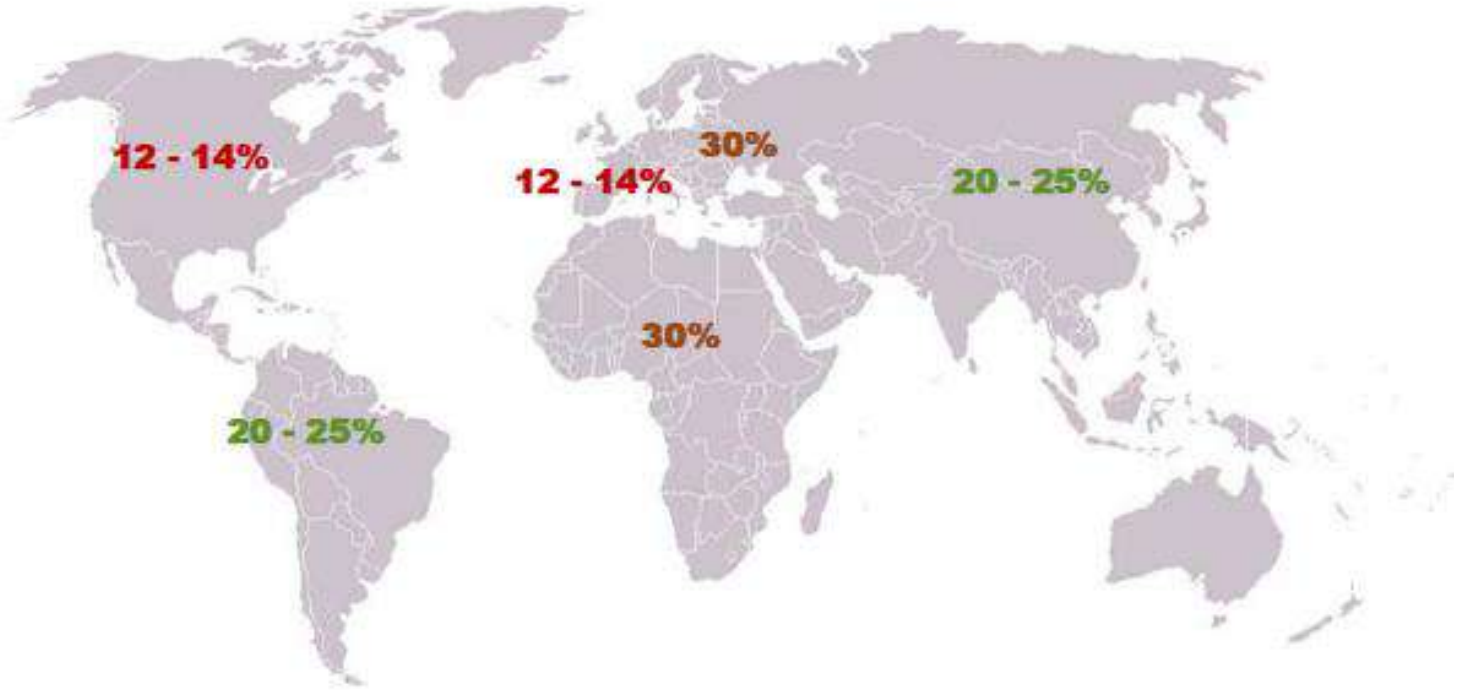
*"El **Gobierno Corporativo** es el sistema por el cual las sociedades son dirigidas y controladas. La estructura del gobierno corporativo especifica la distribución de los derechos y responsabilidades entre los diferentes participantes de la sociedad, tales como el directorio, los gerentes, los accionistas y otros agentes económicos que mantengan algún interés en la empresa. El Gobierno Corporativo también provee la estructura a través de la cual se establecen los objetivos de la empresa, los medios para alcanzar estos objetivos, así como la forma de hacer un seguimiento a su desempeño".*

*Organización para la Cooperación y el Desarrollo Económico - OCDE*


" Código de Buen Gobierno Corporativo para las Sociedades Peruanas" (2015)

Fuente: BVL

## Gobierno Corporativo: Prima de mercado




El valor adicional que estarían dispuestos a pagar los inversionistas, varía según la ubicación geográfica

Fuente: BVL

La **administración de riesgos** es uno de los pilares fundamentales del gobierno corporativo entendiendo este como “el sistema mediante el cual las compañías son dirigidas y controladas, para el beneficio de los dueños y de otros interesados claves, para sostener e incrementar el valor de la organización”.

Págs. 24 a 27 de Separata

# Misión de la Auditoría/Control Interno

Proporcionar garantía (assurance) objetiva e independiente sobre la calidad y efectividad de los controles y procesos operacionales de la organización así como ofrecer servicios de consultoría con valor agregado diseñados para mejorar las operaciones de la empresa.

Págs. 28 a 29 de Separata

**Metodología de Control Interno/Gestión de Riesgos:**

- De Arriba Abajo
- Basado en Riesgo
- Orientado a Procesos
- Utilizando el Marco Integral de Control Interno de COSO
- Aplicando Estándares Internos y Externos

**Problemas de Control Interno/Gestión de Riesgos:**

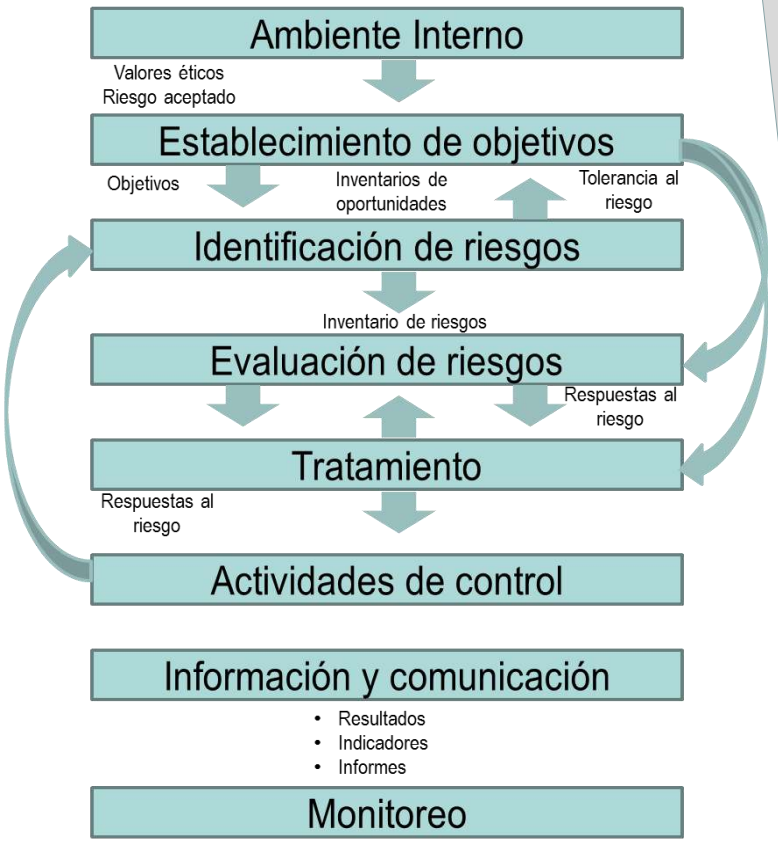
- Juicio
- Error humano
- Costo versus beneficio
- Fraude
- "Management override"

# Marco Integrado para la Gestión de Riesgos Corporativos (COSO ERM)

**La Gestión Integral de Riesgos considera las siguientes categorías de objetivos:**

a. Estrategia. Son objetivos de alto nivel, vinculados a la visión y misión empresarial.
b. Operaciones. Son objetivos vinculados al uso eficaz y eficiente de los recursos.
c. Información. Son objetivos vinculados a la confiabilidad de la información suministrada.
d. Cumplimiento. Son objetivos vinculados al cumplimiento de las leyes y regulaciones aplicables.

# Marco Integrado para la Gestión de Riesgos Corporativos (COSO ERM)

"Los inversionistas están asustados. No hay otra manera de explicar que alguien en EE.UU. quiera recibir 1,5% de tasa de interés a 10 años cuando el S&P 500 rinde 2,2% en dividendos anuales. El inversionista no quiere riesgos: está sobrepagando para no tenerlos".

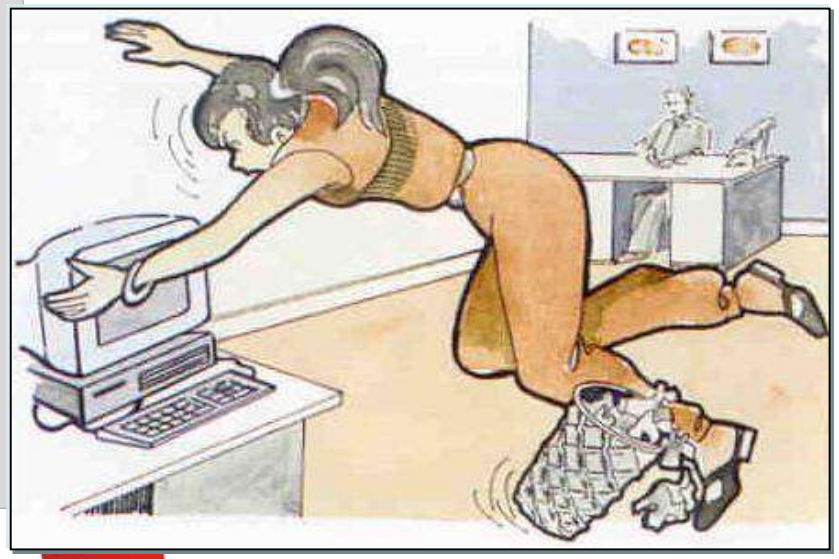
Artículo "En el Mercado"

Por Carlos Rojas, Revista G, junio de 2012, Pág. 19

# PRONOSTICANDO EL FUTURO

*"Paul Samuelson rehuía pronosticar por el mal recuerdo de un ensayo suyo escrito de estudiante en el MIT, en el que argumentó por qué Argentina sería el país al que mejor le iba a ir después de la Segunda Guerra. Philip Tetlock, profesor del Wharton School, analizó más de 80,000 predicciones efectuadas por casi 300 gurús, entre economistas, analistas políticos y periodistas. De las apuestas vistas como seguras, el 27% no sucedió y de los eventos considerados como imposibles, el 15% terminó ocurriendo. Concluyó con una frase harto citada:* ***'Los pronósticos de los expertos son ligeramente más acertados que los de un chimpancé que dispara dardos'*** *".*

*Fuente: La Columna de FOZ, Felipe Ortiz de Zevallos M., Semana Económica, 01/Nov/2015*



# ¿Qué es el Riesgo?

***La revolución tecnológica tiene 3 implicancias:***

***i. La automatización está reduciendo la demanda por trabajo***

***ii. Erosiona la capacidad del mercado para establecer algunos precios relacionados con la informática***

***iii. Surgimiento de bienes, servicios y organizaciones que no responden fácilmente a los dictados del mercado, ni a la jerarquía gerencial usual***

"El Poscapitalismo". La columna de FOZ, Felipe Ortiz de Zevallos
Semana Económica, 16 de agosto de 2015, Pág. 11

- Inevitable en los procesos de toma de decisiones en general y en los procesos de inversión en particular.
- En finanzas, el concepto de riesgo se relaciona con las pérdidas potenciales que se pueden sufrir en un portafolios de inversión.
- El beneficio debe asociarse con el riesgo asumido.
- La medición efectiva y cuantitativa del riesgo se asocia con la probabilidad de una pérdida en el futuro.

## *RIESGO*

*Posibilidad de un hecho adverso que puede afectar negativamente la habilidad de una organización para lograr sus objetivos.*

El objetivo de la gestión de riesgos puede expresarse en dos sentidos:

- No sufrir pérdidas económicas inaceptables (no tolerables); y,
- Tomar en cuenta el rendimiento ajustado por riesgo.

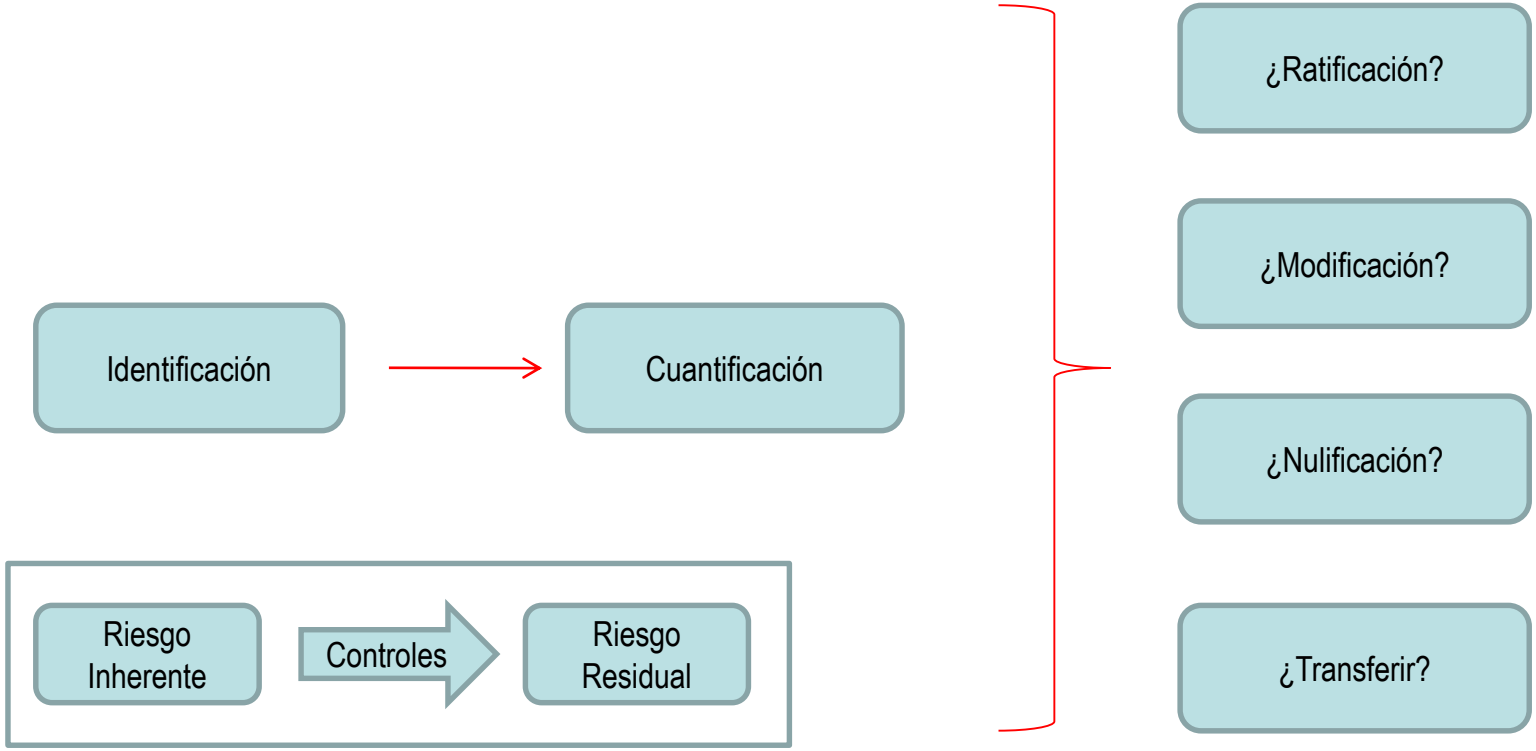
## ¿Se puede eliminar el riesgo?

## ¿Eliminar el riesgo?

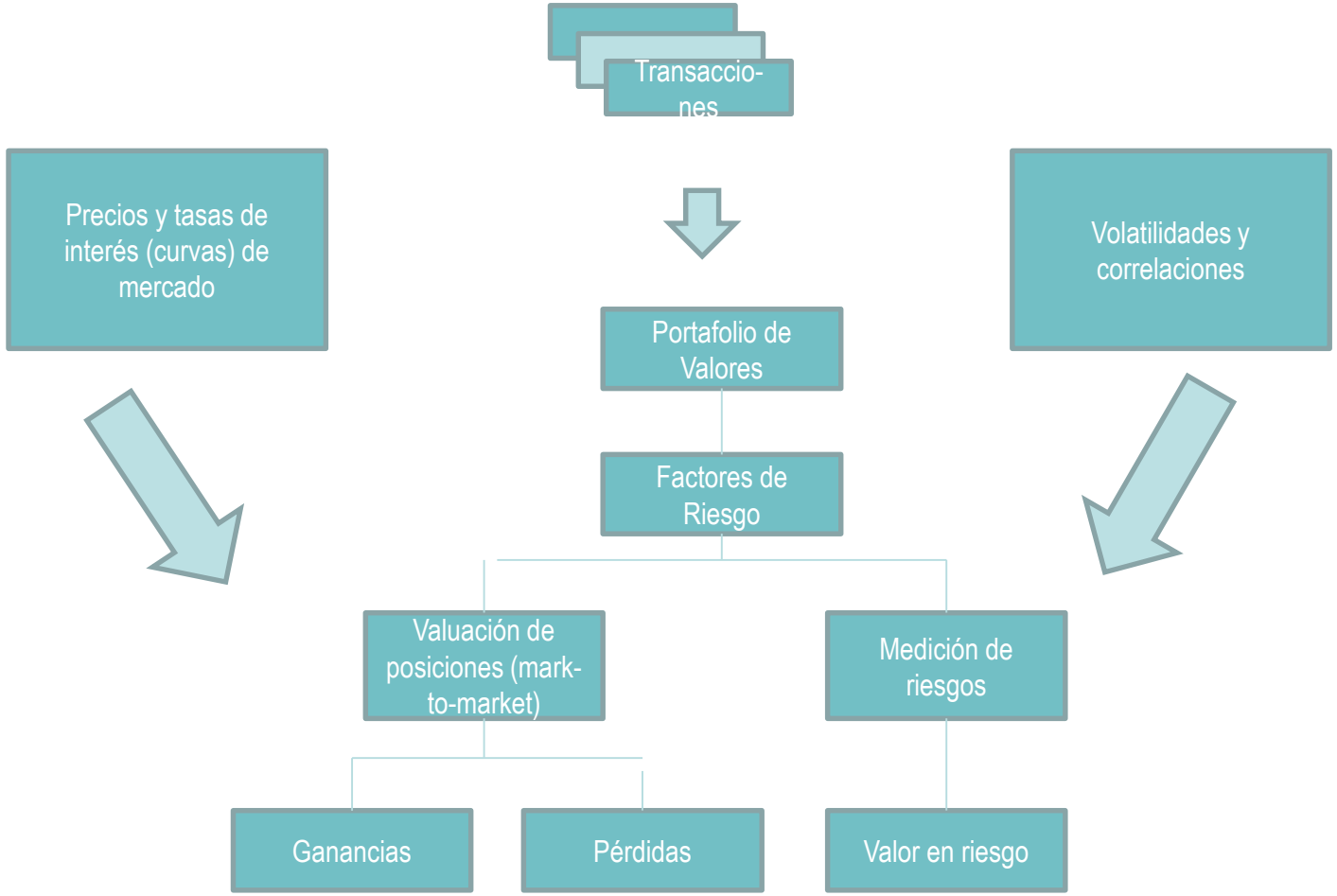
No, el riesgo se controla, reduce o minimiza, nunca se elimina …

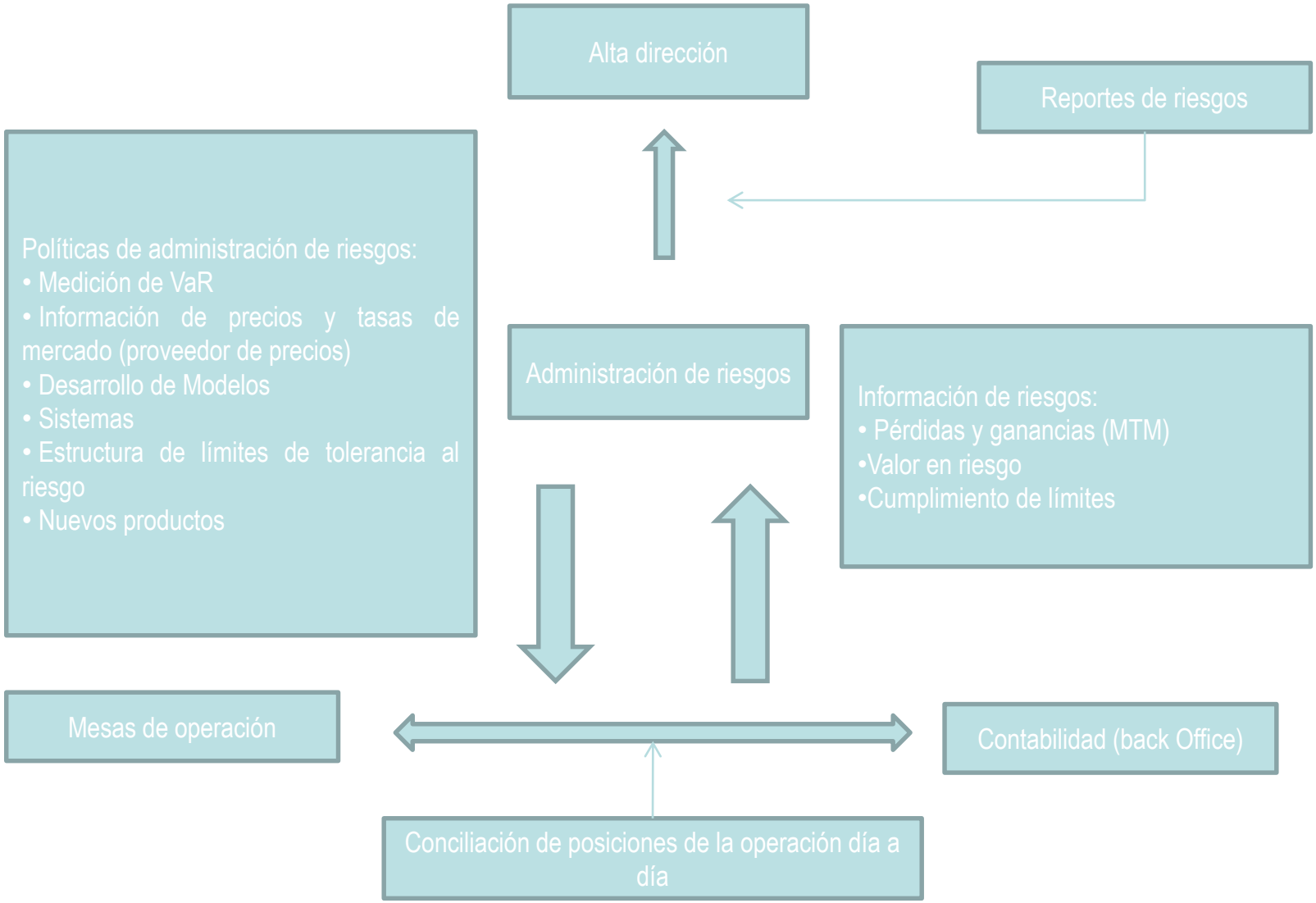
La función de un ejecutivo es decidir entre alternativas relativamente homogéneas, en ese sentido, la administración de riesgos es una herramienta que ayuda en este proceso de toma de decisiones, convirtiendo la incertidumbre en oportunidad y evitando catástrofes de graves consecuencias.

Para lograr una efectiva identificación de riesgos es necesario considerar las diferentes naturalezas de riesgo que se presentan en una transacción.



**Para lograr una efectiva identificación de riesgos es necesario considerar las diferentes naturalezas de riesgo que se presentan en una transacción.**



Transaccio-
nes
Precios y tasas de interés (curvas) de mercado
Volatilidades y correlaciones
Portafolio de Valores
Factores de Riesgo
Valuación de posiciones (mark-to-market)
Medición de riesgos
Ganancias
Pérdidas
Valor en riesgo


Alta dirección
Reportes de riesgos
Políticas de administración de riesgos:
• Medición de VaR
• Información de precios y tasas de mercado (proveedor de precios)
• Desarrollo de Modelos
• Sistemas
• Estructura de límites de tolerancia al riesgo
• Nuevos productos
Administración de riesgos
Información de riesgos:
• Pérdidas y ganancias (MTM)
•Valor en riesgo
•Cumplimiento de límites
Mesas de operación
Contabilidad (back Office)
Conciliación de posiciones de la operación día a día

Instituciones financieras: tomadoras de riesgo, por naturaleza.

Una cultura de riesgos crea una ventaja competitiva.

No tener una cultura de riesgo, puede generar ganancias en el corto plazo, pero en el largo plazo es probable que conviertan sus riesgos en pérdidas.

## Recomendaciones en la Administración de Riesgos:

- El papel de la alta dirección.
- Valuación a precio de mercado de las posiciones de riesgo.
- Medición cuantitativa de los riesgos.
- Simulaciones extremas o de stress.
- Independencia en la medición de riesgos.
- Medición de riesgos de crédito
- Experiencia y conocimiento de estadística y sistemas.

## Apetito por riesgo:

- Nivel de riesgo que la empresa está dispuesta a cambio de rentabilidad
- Filosofía de administración de riesgo que impacta en su cultura y estilo operativo

## Tolerancia al riesgo:

- Nivel de variación que la empresa está dispuesta a asumir
- Operar dentro de las tolerancias al riesgo proporciona a la administración una mayor confianza en que la entidad permanece dentro de su riesgo aceptado y mayor seguridad que la entidad alcanzará sus objetivos

**Controles:**

- Cualquier acción tomada por la organización para mejorar la probabilidad de alcanzar los objetivos establecidos.
- Las actividades de control tienen lugar a través de toda la organización, a todos los niveles y en todas las funciones.
- Los controles pueden clasificarse como:
  - Directivos: Provoca o fomenta la ocurrencia de un hecho deseable.
  - Preventivos: Evita la ocurrencia de eventos indeseables.
  - Detectivos: Descubren errores o irregularidades ya ocurridas
  - Correctivo: Rectifica un error o irregularidad.

**Crisis Relacionadas con Burbujas:**

- La tulipomanía (1636)
- La Compañía de los Mares del Sur (1720)
- El crac del '29 (1929)
- La crisis del petróleo (1973)
- La burbuja tecnológica (1999)

**Crisis Derivadas del Sobreendeudamiento:**

- Crisis latinoamericana (1980-1982)
- El Efecto Tequila mexicano (1995)
- Crisis asiática (1997)

**Crisis con rescate del Sector Financiero:**

- Crisis Overend & Gurney (1866-1890)
- Crisis savings & loans (1986-1995)
- Crisis de las hipotecas subprime (2007)

# GESTIÓN INTEGRAL DE RIESGOS

*"La **gestión eficaz de los riesgos** ha sido siempre un **punto clave en el desarrollo de las empresas más exitosas**. Los continuos **riesgos emergentes** en el entorno empresarial actual hace que sea cada vez más difícil para los ejecutivos **tener la confianza que los planes y estrategias definidos se concretarán según lo esperado**. Uno de los principales motivos, es que el impacto que pueden tener los riesgos actualmente se multiplica a consecuencia del **veloz movimiento de las tendencias de negocio e innovaciones tecnológicas**, como las redes sociales, tecnologías móviles y big data. La velocidad del riesgo es mucho mayor ahora que años atrás, motivando que las compañías busquen estar más y mejor preparadas para responder ante ello".*

*Fuente: Deloitte – Encuesta de Inteligencia en la Gestión del Riesgo Empresarial (Oct. 2014)*

## Definición:

La Gestión Integral de Riesgos (GIR) es un proceso, efectuado por el Directorio, la Gerencia y el personal aplicado en toda la empresa y en la definición de su estrategia, diseñado para identificar potenciales eventos que pueden afectarla, gestionarlos de acuerdo a su apetito por el riesgo y proveer una seguridad razonable en el logro de sus objetivos.

**Categoría de objetivos:**

- Estrategia.- Son objetivos de alto nivel, vinculados a la visión y misión empresarial.
- Operaciones.- Son objetivos vinculados al uso eficaz y eficiente de los recursos.
- Información.- Son objetivos vinculados a la confiabilidad de la información suministrada.
- Cumplimiento.- Son objetivos vinculados al cumplimiento de las leyes y regulaciones aplicables.

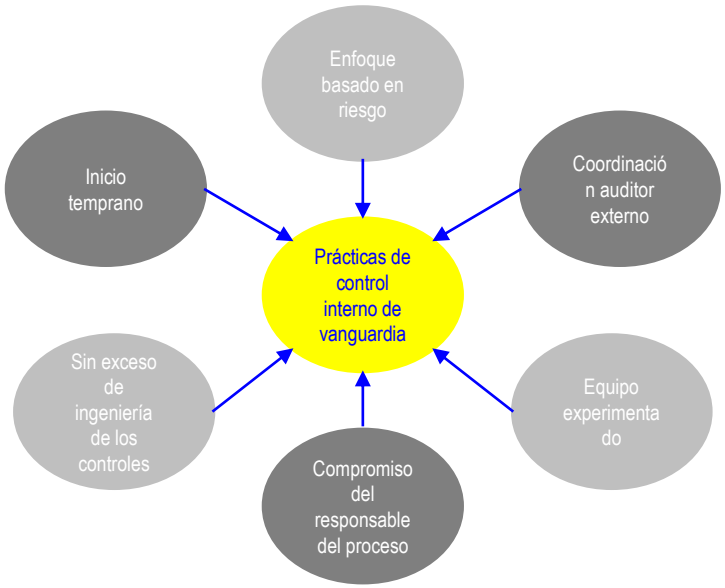
Las empresas deben efectuar una GIR adecuada a su tamaño y a la complejidad de sus operaciones y servicios.

- Un enfoque sólido de gestión de riesgos conduce a una forma de crecimiento sana, que atrae al inversionista, a través de un impacto positivo en el crecimiento de las utilidades a largo plazo.
- Nuevos y mayores riesgos surgen en un entorno empresarial que cambia constantemente. Para alcanzar el éxito son necesarios procesos y controles apropiados para afrontar estos riesgos que amenazan el poder alcanzar las estrategias y objetivos.
- Rápidos cambios en la economía global y teconología, requieren organizaciones que se adapten al cambio de forma rápida y eficaz, enfrentado altos niveles de riesgo por su expansion a nuevos mercados, requerimientos regulatorios, nuevas oportunidades y nuevos riesgos.

En 1958, una empresa podia esperar mantenerse en el índice Standard & Poor's 500 por 61 años. Hoy, solo pueden permanecer 18 años.

¿Tu empresa identifica y evalua riesgos continuamente, para optimizar el uso de los recursos disponibles?

Según EY, no es una tarea fácil, el diseño de procesos y controles apropiados es uno de los temas de gobierno corporativo más desafiante de enfrentar. Se asignan claramente los roles y responsabilidades sobre el riesgo y se definen claramente los canales y procesos de comunicación, Incluyendo un lenguaje de comunicación común sobre los riesgos y su nivel de importancia.



Trabajar para el corto y largo plazo simultáneamente require tiempo y esfuerzos considerable, pero fortalice el entorno de la gestión de riesgos.

| Riesgo, costo y valor | | |
|---|---|---|
| Riesgo | Costo | Valor |
| Una cultura de riesgos se patrocina desde el más alto nivel de la organización y es desplegado en cascada en toda la empresa. La evaluación de los riesgos es exhaustiva. Los reportes de riesgos son transparentes. | Las redundancias y superposiciones de controles para la mitigación de riesgos se racionalizan o eliminan y la cobertura se enfoca en los riesgos prioritarios. Para ello, la empresa emplea servicio de terceros o desarrolla equipos mixtos de distintas áreas. Se aprovecha la tecnología y técnicas de vanguardia en la gestión del conocimiento. | Una sólida gestión de riesgos brinda la confianza que se necesita para enfrentar un riesgo o evitarlo.<br>Como parte de su rol, la Auditoría Interna brinda sugerencias para mejorar los procesos, identificar riesgos y asiste en la determinación del apetito y tolerancia al riesgo.<br>Al contribuye con el monitoreo e las iniciativas más estratégicas. |

- Los procesos y controles apropiados son una necesidad para un crecimiento sostenible.
- Posibilitan el cumplimiento de metas y tranquilizan a los inversionistas y reguladores (piense en las certificaciones como una práctica de buen gobierno corporativo).
- Construye las bases para la mejora continua en la organización.
- La evaluación de riesgos debe ser profunda e identificar cambios internos y externos como nuevos contratos con terceros, nuevos requerimientos regulatorios y nuevas tecnologías que podrían afectar los procesos existentes.
- Sin embargo, hay que tener cuidado de no caer en la trampa … es más fácil hablar de desarrollar una gestión de riesgos apropiada que realmente desarrollarla y mantenerla.

1. Directorio: adecuadas estrategias de gestión del riesgo.
- Sólida cultura de gestión del riesgo
- Políticas y procesos definidos
- Niveles de apetito y tolerancia al riesgo definidos
- Alta Dirección comprometida y adopta las medidas necesarias.

2. Cuenta con políticas y procesos integrales para la gestión del riesgo.
- Visión integral del riesgo que incluya todo tipo de riesgos significativos.
- Perfil de riesgo (incluyendo relevancia sistémica).
- Evaluación de los riesgos procedentes del entorno de negocios y macroeconómico.

3. Estrategias, políticas, procedimientos y límites en materia de riesgo.
- Se documentan.
- Se revisan y actualizan periódicamente.
- Se comunican a la organización.
- Excepciones, políticas, procesos y límites establecidos se autorizan por niveles jerárquicos.

4. Directorio y Alta Dirección obtienen suficiente información.
- Comprende información sobre el nivel de riesgo asumido y los niveles adecuados de capital y liquidez.
- Se revisan periódicamente y entienden las implicancias, limitaciones e incertidumbres en la medición del riesgo.

5. Adecuados procesos internos de evaluación de suficiencia de capital y liquidez en relación con el perfil de riesgo de la compañía.

6. Modelos para cuantificar los componentes del riesgo.
- Resultados de modelos deben reflejar los riesgos asumidos.
- Cumplen normas de supervisión.
- Consideran limitaciones e incertidumbre.
- Se realizan validaciones y comprobaciones periódicas e independientes.

7. Se cuenta con sistemas de información adecuados.
- En circunstancias normales y en contingencia.
- Que permitan cuantificar, evaluar y notificar el volumen, composición y calidad de las exposiciones a todo tipo de riesgo, productos y contrapartes.

8. Políticas y procesos que garanticen que el Directorio y la Alta Dirección:
- Entienden los riesgos inherentes a nuevos productos, modificaciones significativas (cambios de sistemas, procesos, modelos de negocio y adquisiciones sustanciales).
- Vigilar y gestionar estos riesgos de forma continua.

9. Cuenta con funciones de gestión del riesgo.
- Abarcan todos los riesgos significativos y de suficientes recursos, independencia, autoridad y acceso al Directorio y Alta Dirección.
- Tareas claramente separadas de las unidades funcionales que asumen los riesgos en la entidad.

10. Adecúa e implementa las normas emitidas por los organismos supervisores (cumplimiento normativo).

11. Adecuados mecanismos de continuidad del negocio.
- Medidas en situaciones de contingencia (incluidas las que plantearían una grave amenaza para su viabilidad).
- Plan de pruebas.

## Responsabilidad del Directorio

- Establecer una GIR un ambiente interno que facilite su desarrollo adecuado.
- Aprobar las políticas generales que guíen las actividades de la empresa en la gestión de los diversos riesgos que enfrenta.
- Seleccionar una plana gerencial con idoneidad técnica y moral.
- Recursos necesarios para el desarrollo de la GIR, a fin de contar con la infraestructura, metodología y personal apropiado.
- Establecer incentivos para fomentar el funcionamiento de la GIR.
- Aprobar políticas y procedimientos.
- Conocer los principales riesgos afrontados estableciendo adecuados niveles de tolerancia y apetito por el riesgo.

## Objetivos para el Directorio

- Conocer los estándares previstos relacionados a GIR, así como sus responsabilidades.
- Una gestión apropiada de los riesgos para la complejidad y tamaño de la empresa.
- Conocimiento de la información de la Gerencia, de los informes del Comité de Auditoría, del Comité de Riesgos, de Auditoría Externa, y de otra información que el Directorio considere relevante, y que las medidas correctivas dispuestas consten en las actas correspondientes, con respecto al GIR.

## Responsabilidad de la Gerencia

- Implementar la GIR conforme a las disposiciones del Directorio.
- Comités para el cumplimiento de sus responsabilidades.
- Los gerentes de las unidades organizativas de negocios o de apoyo, en su ámbito de acción, tienen la responsabilidad de administrar los riesgos relacionados al logro de los objetivos de sus unidades.
- Consistencia entre operaciones y tolerancia al riesgo.
- Asumir los resultados de la GIR correspondiente a su unidad.

## Comités dentro de la GIR

- Constituir los comités necesarios para la apropiada GIR.
- Los comités constituidos deben contar con políticas y procedimientos para el cumplimiento de sus funciones.

## Comité de Riesgos

- Decisiones que atañen a los riesgos significativos.
- Sus integrantes deben tener los conocimientos y experiencia.
- Crear los comités de riesgos especializados necesarios.
- Aprobar las políticas y la organización para la GIR.
- Definir el nivel de tolerancia y el grado de exposición al riesgo que la empresa está dispuesta a asumir en el desarrollo del negocio.
- Implementación de las acciones correctivas necesarias.
- Aprobar variaciones significativas en el perfil de riesgo.
- Evaluar la suficiencia de capital de la empresa para enfrentar sus riesgos.
- Proponer mejoras en la GIR.

## Comité de Auditoría

- Vigilar que los procesos contables y de reporte financiero sean apropiados, así como evaluar las actividades realizadas por los auditores internos y externos.
- Adecuado funcionamiento del sistema de control interno.
- Informar de la existencia de limitaciones en la confiabilidad de los procesos contables y financieros;
- Cumplimiento de las políticas y procedimientos internos, así como de las medidas correctivas implementadas.
- Criterios para la selección de los auditores externos y evaluar su desempeño.
- Criterios para la selección del auditor interno y sus principales colaboradores.

## Unidad de Riesgos

- De acuerdo a su complejidad y líneas de negocio.
- Una unidad centralizada o unidades especializadas en la gestión de riesgos específicos.
- Experiencia y conocimientos apropiados.
- Plan de capacitación.
- Participar en el diseño y permanente adecuación de los manuales de GIR.
- Definir las responsabilidades de las unidades de negocios.
- Apoyar y asistir a las unidades de la empresa. Debe ser independiente de las unidades de negocios.

## Unidad de Riesgos

- Proponer las políticas, procedimientos y metodologías apropiadas para la GIR.
- Velar por una Gestión Integral de Riesgos competente.
- Guiar la integración entre la gestión de riesgos, los planes de negocio y las actividades de gestión empresarial.
- Estimar los requerimientos patrimoniales que permitan cubrir los riesgos.
- Informar los aspectos relevantes de la GIR.
- Informar los riesgos asociados a nuevos productos y a cambios importantes en el ambiente de negocios, el ambiente operativo o informático, de forma previa a su lanzamiento o ejecución; así como de las medidas de tratamiento propuestas o implementadas.

## Gerente de Riesgos

- Apropiada formación académica y experiencia relevante.
- Responsable de informar al Directorio, comités respectivos y a las áreas de decisión correspondientes, sobre los riesgos, el grado de exposición al riesgo aceptado y la gestión de éstos, de acuerdo a las políticas y procedimientos establecidos por la empresa.
- Emitir los informes de riesgos, incluyendo un plan de actividades.

## Subcontratación de la función de Riesgos

- Asumir plena responsabilidad sobre los resultados de los procesos subcontratados con terceros.
- Asegurarse de la reserva y confidencialidad sobre la información.
- Subcontratación significativa: análisis formal de los riesgos asociados.
- Se entiende por significativa aquella subcontratación que, en caso de falla o suspensión del servicio, puede poner en riesgo importante a la empresa, al afectar sus ingresos, solvencia, o continuidad operativa.
- La subcontratación de una o más funciones de la GIR es significativa.

# MENTE EN FOCO

"Una abundancia de información crea un déficit en la atención" (Goleman citando a Herbert Simon, considerado el creador de la "economía de la atención").

Daniel Goleman, señala que no solo debemos ser emocionalmente inteligentes, sino que dicha inteligencia emerge de la **capacidad de prestar atención a lo importante por encima de lo urgente**, tanto en el mundo exterior como interior de la persona.

Fuente: Revista G, Nr. 43, Junio 2014, Pág. 102.

*"¿Qué medidas piensa tomar ante el incremento de la moriosidad, especialmente en el segmento de banca minorista [pequeña y microempresa]?*

*Las medidas las tomamos hace 2 años, cuando empezamos un Proyecto para llevar nuestra gestión de riesgos de banca minorista a mejores practicas. Hemos aumentado la cantidad y la calidad de la gente que trabaja en ese equipo, y hemos mejorado la calidad de las herramientas con las que trabajamos y la gobernanza. Por eso hoy nos sentimos muy cómodos de que los nuevos créditos que estamos dando son de muy buena calidad. Probablemente el deterioro venga por los créditos que ya están adentro".*

Entrevista a Walter Bayly, CEO de Credicorp
Semana Económica, 16 de agosto de 2015, Pág. 28

"Tenemos ante nosotros dos oportunidades muy importantes, que son la eficiencia y la gestión de riesgos. Esas son dos palancas que todavía presentan oportunidades".

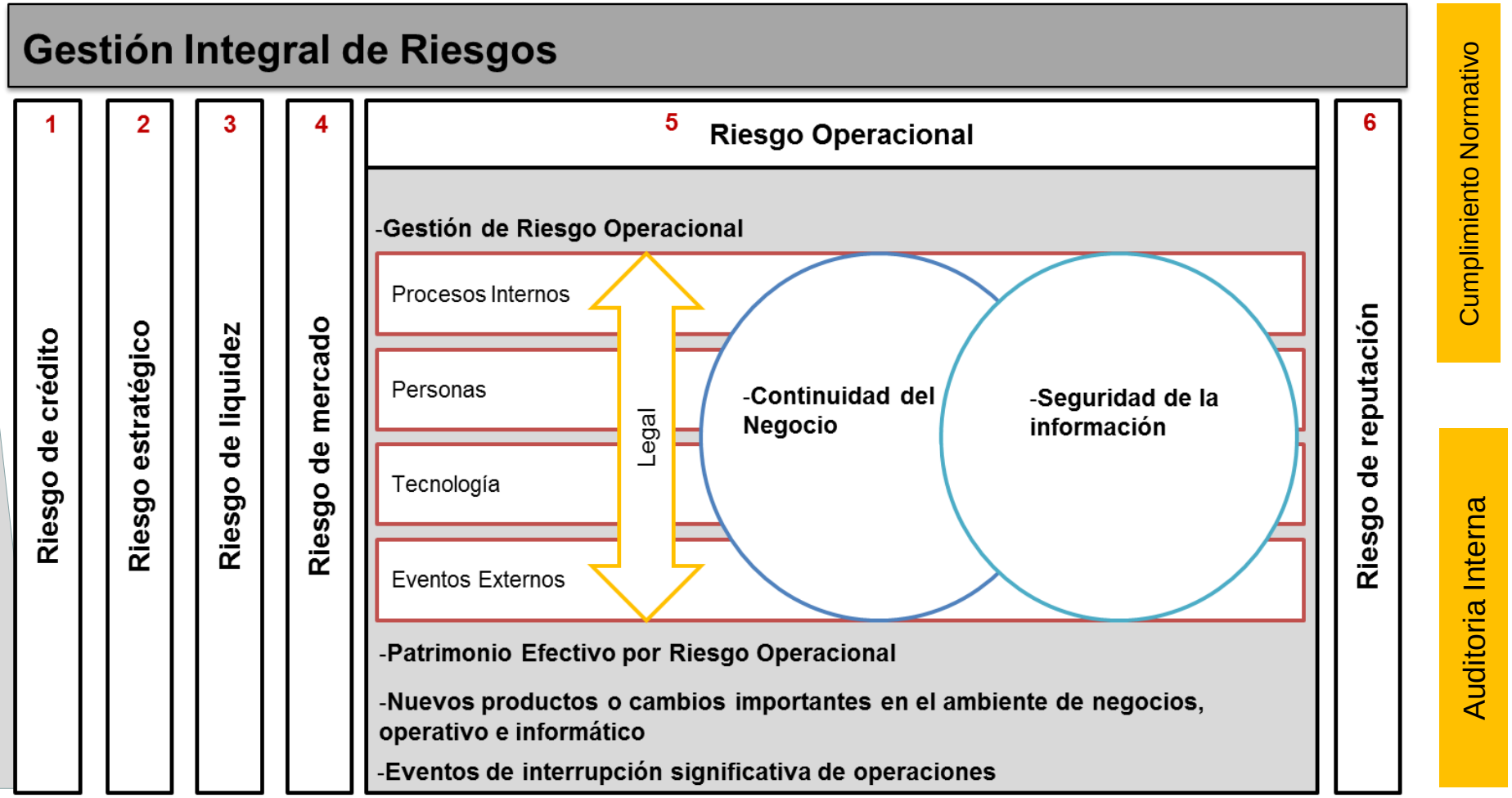
Otra decisión clave del BCP fue realizar avances significativos en el área de gestión de riesgos, precisamente, donde se introdujeron las mejores prácticas mediante la implementación de metodologías y procedimientos diseñados con la ayuda de consultores internacionales.

Esta práctica da origen a una gestión de riesgo completa y oportuna para garantizar una alta calidad de cartera y previsión de todo tipo de riesgo inherente a los negocios financieros, todo ello en un escenario internacional complicado, con mercados inestables.

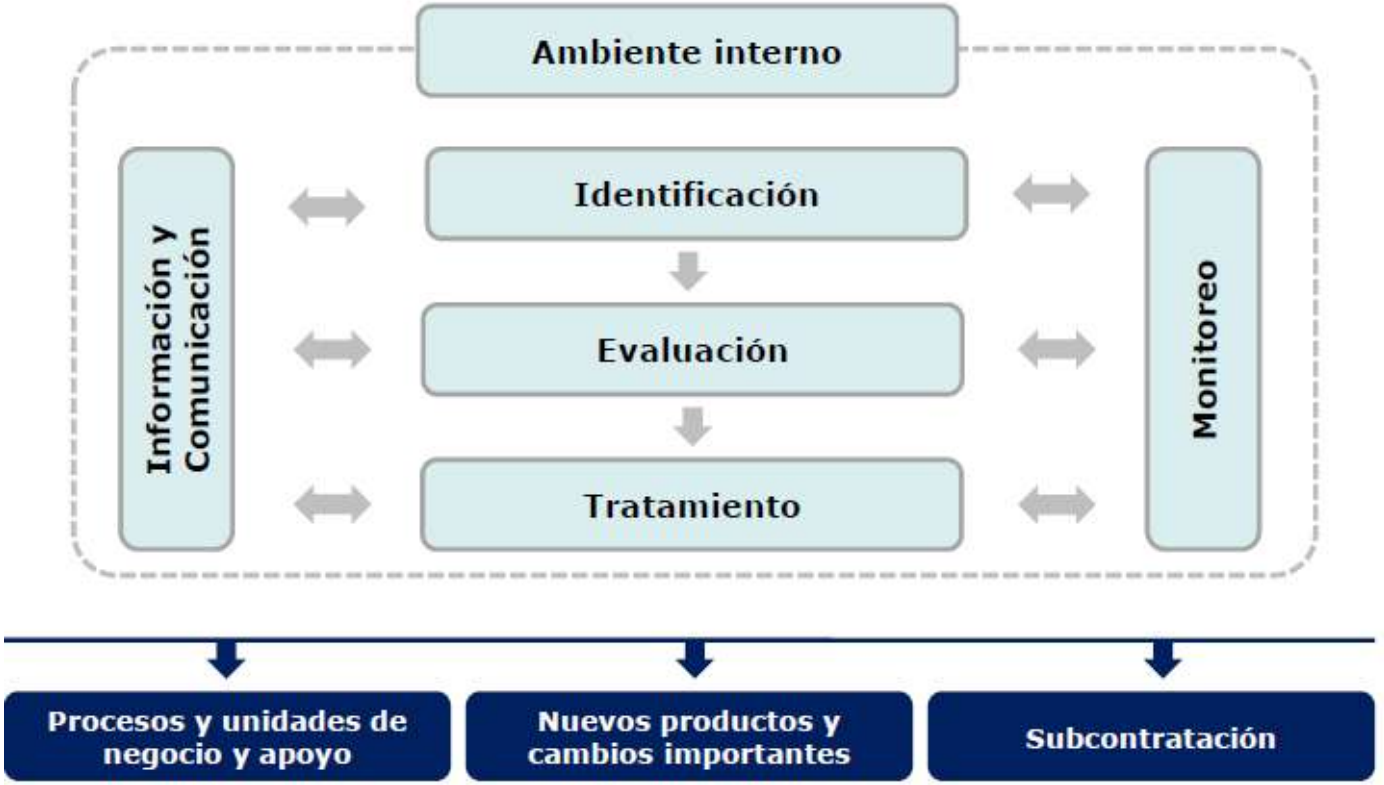

EFICACIA Y GESTIÓN DE RIESGOS

Fuente: Revista G, Octubre 2013

## Marco Normativo



# Componentes de la Gestión de Riesgo



# COMPONENTES DE LA GESTIÓN DE RIESGO

**Ambiente interno**

Comprende, entre otros, los valores éticos, la idoneidad técnica y moral de sus funcionarios; la estructura organizacional; y las condiciones para la asignación de autoridad y responsabilidades.

## Cultura de gestión de riesgos

- Políticas establecidas y aprobadas por el Directorio
- Implementación de políticas por la Gerencia

Apetito + Tolerancia

- Establecimiento de apetito y tolerancia al riesgo

- Capacitación continua (especializada y general)
- Sistema de incentivos asociados al desempeño.

## Estructura Organizativa

- Área especializada
- Independencia respecto a otras áreas
- Personal suficiente


- Coordinadores de RO en áreas de negocio/apoyo
- Comité de Gestión de Riesgos y/o específico (RO)

# COMPONENTES DE LA GESTIÓN DE RIESGO

Establecimiento de objetivos. Proceso por el que se determinan los objetivos empresariales, los cuales deben encontrarse alineados a la visión y misión de la empresa, y ser compatibles con la tolerancia al riesgo y el grado de exposición al riesgo aceptado.

# COMPONENTES DE LA GESTIÓN DE RIESGO

Identificación de riesgos. Proceso por el que se identifican los riesgos internos y externos que pueden tener un impacto negativo sobre los objetivos de la empresa. Entre otros aspectos, considera la posible interdependencia entre eventos, así como los factores influyentes que los determinan.

# COMPONENTES DE LA GESTIÓN DE RIESGO

Evaluación de riesgos. Proceso por el que se evalúa el riesgo de una empresa, actividad, conjunto de actividades, área, portafolio, producto o servicio; mediante técnicas cualitativas, cuantitativas o una combinación de ambas.

**Identificación y Evaluación de Riesgos**

## Principales Herramientas

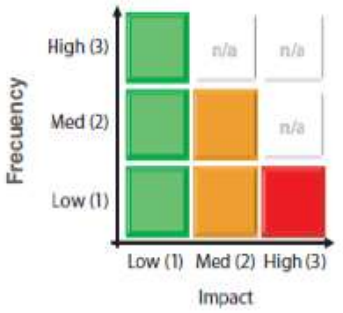
- Autoevaluaciones
- Base de datos de eventos de pérdida (BDEP)

## Evaluación de controles


- Evaluación de efectividad de controles

## Medición de la exposición

- Análisis cuali-cuantitativo de la **frecuencia e impacto** asociado a cada riesgo
- Variables con rangos numéricos asociados
- Estimaciones toman en cuenta información de la BDEP




- No se debe considerar "zona fantasma" de la matriz de riesgo
- Se deben evaluar los riesgos asociados a subcontratación

# COMPONENTES DE LA GESTIÓN DE RIESGO

Evaluación de riesgos. Proceso por el que se evalúa el riesgo de una empresa, actividad, conjunto de actividades, área, portafolio, producto o servicio; mediante técnicas cualitativas, cuantitativas o una combinación de ambas.

**Identificación y Evaluación de Riesgos**

## Recolección de Eventos de Pérdida

- Políticas y procedimientos de captura, validación, registro y reporte de esta información
- Entrenamiento de las personas que participan del proceso
- Criterios para la asignación de eventos multilínea
- Umbrales de captura de eventos (aprox. US$ 1000) y mantenimiento de expediente

- Información mínima
  - Código y descripción
  - Tipo de evento de pérdida
  - Líneas de negocio
  - Monto bruto
  - Moneda
  - Recuperación
  - Cuenta contable asociada
  - Fechas: descubrimiento, ocurrencia y registro contable

# COMPONENTES DE LA GESTIÓN DE RIESGO

**Tratamiento de Riesgos**

Proceso por el que se opta por aceptar el riesgo, disminuir la probabilidad de ocurrencia, disminuir el impacto, transferirlo total o parcialmente, evitarlo, o una combinación de las medidas anteriores, de acuerdo al nivel de tolerancia al riesgo definido.

## Estrategias

- Evitar
- Aceptar
- **Transferir**
- **Mitigar**


## Planes de acción y seguimiento
### Estrategias mitigar y transferir

- Aprobación de planes por parte de las Gerencias responsables
- Establecimiento de responsables y fechas propuestas de implementación
- Seguimiento periódico
- Reporte de excepciones en la implementación, cuando menos, al Comité de Riesgos y Gerencia General




# COMPONENTES DE LA GESTIÓN DE RIESGO

Control. Proceso que busca asegurar que las políticas, estándares, límites y procedimientos para el tratamiento de riesgos son apropiadamente tomados y/o ejecutados. Las actividades de control están preferentemente incorporadas en los procesos de negocio y las actividades de apoyo. Incluye los controles generales así como los de aplicación a los sistemas de información, además de la tecnología de información relacionada. Buscan la eficacia y efectividad de las operaciones de la empresa, la confiabilidad de la información financiera u operativa, interna y externa, así como el cumplimiento de las disposiciones legales que le sean aplicables.

# COMPONENTES DE LA GESTIÓN DE RIESGO

Reporte. Proceso por el que se genera y transmite información apropiada y oportuna a la dirección, la gerencia, el personal, así como a interesados externos tales como clientes, proveedores, accionistas y reguladores, entre ellos la SBS. Esta información es interna y externa, y puede incluir información de gestión, financiera y operativa.

**Información y Comunicación**

**Reporte al interior de la empresa**

Se deben definir niveles y frecuencia

- Directorio
- Comité de Riesgos
- Comité de RO (si hubiera)
- Gerencia General
- Áreas de Negocio/Apoyo

SUPERINTENDENCIA DE BANCA, SEGUROS Y AFP

**Reporte a la SBS**

Informe de Gestión de Riesgo Operacional (IGROp), una vez al año

# COMPONENTES DE LA GESTIÓN DE RIESGO

Monitoreo. Proceso que consiste en la evaluación del adecuado funcionamiento de la Gestión Integral de Riesgos y la implementación de las modificaciones que sean requeridas. El monitoreo debe realizarse en el curso normal de las actividades de la empresa, y complementarse por evaluaciones independientes o una combinación de ambas. Incluye el reporte de las deficiencias encontradas y su corrección.

**Monitoreo de los Riesgos:**

## Monitoreo del área especializada

- Autoevaluaciones periódicas
- Evaluación de nuevos productos y cambios importantes



- Seguimiento a la implementación de planes de acción
- Base de datos de eventos de pérdida
- KRI (si los hubiera)

## Auditoría Interna

Debe evaluar el cumplimiento del Reglamento

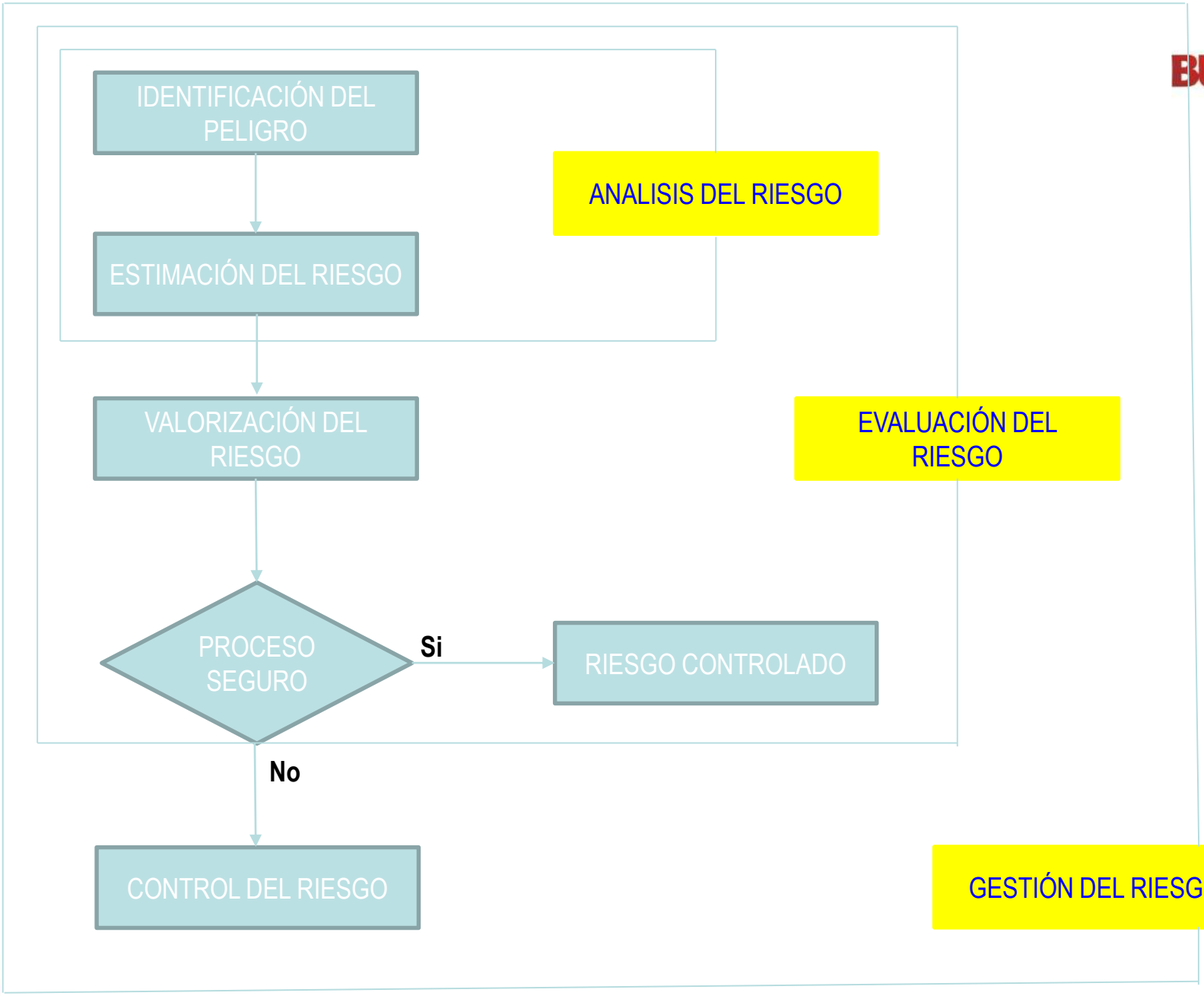

## Auditoría Externa

Debe indicar si se cuenta con políticas para la gestión del riesgo, en su informe sobre sistema de control interno

## Revisión de la SBS

Revisión periódica del cumplimiento de las normas referidas a la gestión del riesgo operacional

SUPERINTENDENCIA DE BANCA, SEGUROS Y AFP


IDENTIFICACIÓN DEL PELIGRO
ESTIMACIÓN DEL RIESGO
ANALISIS DEL RIESGO
VALORIZACIÓN DEL RIESGO
EVALUACIÓN DEL RIESGO
PROCESO SEGURO
Si
RIESGO CONTROLADO
No
CONTROL DEL RIESGO
GESTIÓN DEL RIESGO

## Prácticas cuestionables.

Las empresas deben establecer los sistemas internos apropiados que faciliten la oportuna denuncia e investigación de las actividades ilícitas, fraudulentas, identificadas por cualquier trabajador de la empresa o por alguna persona que interactúa con ésta.

Estas actividades deben ser reportadas a Auditoría Interna, para lo cual la empresa implementará procedimientos que permitan mantener la confidencialidad del denunciante.

En el caso de que los hechos sean significativos, Auditoría Interna debe informar al Comité de Auditoría y al Regulador.

## Relación de la Gestión Integral de Riesgos y el Control Interno

- La GIR es parte integrante del Control Interno, expandiendo y desarrollando los conceptos de CI de manera más amplia y sólida, con énfasis en los riesgos.
- El objetivo de confiabilidad en la información financiera del CI se encuentra principalmente referido a la confiabilidad de los EEFF. En la GIR, este objetivo es expandido para incluir todos los reportes e informes generados por las empresas, incorporando en su alcance la información no financiera.
- Eso incluye objetivos referidos a la estrategia; a las operaciones, información y cumplimiento que deben encontrarse alineados a la estrategia.

## Cumplimiento Normativo

- El CN tiene como objetivo velar por el adecuado cumplimiento de la normativa que le sea aplicable a la empresa.
- Determinar la forma más apropiada y eficiente de implementar el monitoreo y evaluación del CN.
- Los encargados de llevar a cabo la función de CN deben ser independientes respecto de las actividades de las unidades de negocios y contar con conocimientos sólidos de la normativa aplicable a la empresa así como de su impacto en las operaciones de ésta.

## Responsabilidades de cumplimiento normativo

- Asesorar al Directorio.
- Informar de manera continua y oportuna al Directorio y a la Gerencia General respecto a las acciones necesarias para un buen cumplimiento normativo y las posibles brechas existentes.
- Vigilar el cumplimiento normativo aplicable a la entidad.
- Informar sobre la implementación de la adecuación normativa.
- Orientar (capacitar) al personal de la empresa.
- Programa de cumplimiento anual.
- Medidas correctivas.
- Política y Procedimientos de Cumplimiento Normativo. Principios básicos a seguir por la Gerencia General y el personal.

## Responsabilidades de cumplimiento normativo

- Asesorar al Directorio.
- Informar de manera continua y oportuna al Directorio y a la Gerencia General respecto a las acciones necesarias para un buen cumplimiento normativo y las posibles brechas existentes.
- Vigilar el cumplimiento normativo aplicable a la entidad.
- Informar sobre la implementación de la adecuación normativa.
- Orientar (capacitar) al personal de la empresa.
- Programa de cumplimiento anual.
- Medidas correctivas.
- Política y Procedimientos de Cumplimiento Normativo. Principios básicos a seguir por la Gerencia General y el personal.

# LOS RIESGOS OCULTOS

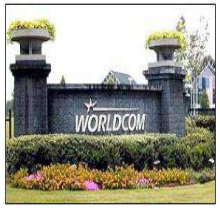
- **El riesgo operacional.**
- El propio inversionista y su ambición.
- Disfrutar de la adrenalina de la inversion.
- El nivel de endeudamiento.
- Llevarse por la intuición sin documentar las decisiones.
- Llevarse por opiniones sin documentarse.
- Pensar que el comportamiento histórico se repetirá necesariamente en el futuro.

*"(…) el curso de la acción adecuada es calibrar al adversario para asegurar la victoria y calcular los **riesgos** y las distancias. Salen vencedores los que libran batallas conociendo estos elementos, salen derrotados los que luchan ignorándolos".*

Sun Tzu, *"El Arte de la Guerra"*, escrito entre el 476 y 221 a.C.


| Principales acreedores financieros de Wolrdcom al momento de la quiebra (en millones de dólares) | | | |
|---|---|---|---|
| **Entidad Financiera** | **Deuda** | **Entidad Financiera** | **Deuda** |
| Boston Safe Dep. Trust | 867.5 | Citibank NA | 155.2 |
| ABN Amro | 753.1 | Brown Brothers Arriman | 152.8 |
| Wilmington Trust | 750.0 | BNP Paribas | 150.3 |
| Salomon Smith Barney | 747.9 | Fleet National Bank | 150.3 |
| Northern Trust | 649.9 | Intesabci SPA | 150.3 |
| UBS Warburg | 369.2 | Mizuho Holdings | 150.3 |
| Wells Fargo | 352.1 | BNY Clearing Services | 142.9 |
| Banc of America Securities | 333.7 | Bank of Tokyo-Mitsubishi | 140.2 |
| Firstar | 298.3 | Icahn & Co | 140.0 |
| Chase Securities | 273.4 | Verinzon Comm. | 121.2 |
| CS First Boston | 272.6 | Morgan Stanley | 118.4 |
| Lehman Bros. | 270.3 | UMB Bank | 112.3 |
| Deutsche Bank | 240.8 | Bank of Nova Scotia | 100.2 |
| ABN Amro Bank | 203.2 | Bank One | 100.2 |
| DB Alex. Brown | 188.8 | Bayerische Landesbank | 100.2 |
| FUNB-Phil Main | 186.5 | Credit Lyonnais | 100.2 |
| West LB | 171.6 | Lloyds TBS Bank | 100.2 |
| Custodial Trust | 163.7 | Mellon Bank | 100.2 |
| Merrill Lynch | 155.5 | Royal Bank of Scotland | 100.2 |

Fuente: Enrique Jiménez R., *"El Riesgo Operacional. Metodologías para su medición y control"*, 2011.

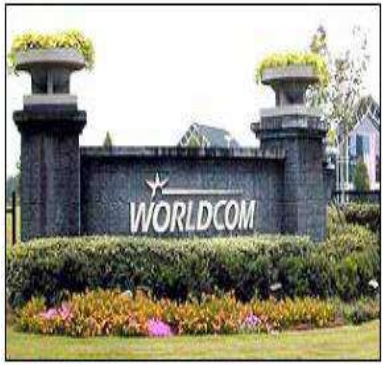



| Pérdida por Multas e Indemnizaciones (en millones de dólares) | | |
|---|---|---|
| **Entidad Financiera** | **Enron** | **Worldcom** |
| JP Morgan Chase | 2,200.00 | 2,000.00 |
| Citigroup | 2,000.00 | 2,650.00 |
| Leman Brothers | 223.00 | 61.71 |
| Bank Of America | 69.00 | 460.00 |
| Merrill Lynch | 190.50 | |
| Credit Suisse First Boston | | 12.54 |
| UBS | | 12.54 |
| Goldman Sachs | | 12.54 |
| Mitsubishi Securities Int. | | 75.00 |
| BNP Paribas | | 37.50 |
| Mizuho Int. | | 37.50 |
| Westlb AG | | 75.00 |
| Canadian Imperial | 2,650.00 | |
| Deutsche Bank | | 325.00 |
| Toronto Dominion Bank | 70.00 | |
| Caboto Holding Sim | | 37.50 |

Fuente: Enrique Jiménez R., *"El Riesgo Operacional. Metodologías para su medición y control"*, 2011.

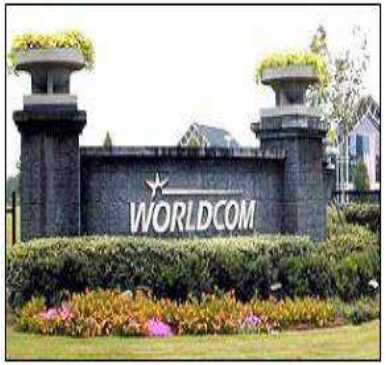
*"Según un informe publicado en 2002 por el Instituto de Análisis Económico Brookings de Washington, la corrupción empresarial tuvo un coste sólo para la economía estadounidense, de 35,000 millones de dólares en el año 2001".*

Enrique Jiménez R., *"El Riesgo Operacional. Metodologías para su medición y control"*, 2011.




Los bancos desempeñaron un papel importante en el fraude financiero de estas dos empresa, “colaborando” en enmascarar la situación financiera y económica en la que se encontraban.

Luego de las quiebras llegaron las demandas judiciales que resultaron en altas indemnizaciones por parte de estas entidades financieras, además de las multas de organismos reguladores.




ENRON

# IMPORTANCIA DE GESTIONAR EL RIESGO

**INTERNOS**

- Aumentar eficiencia operativa.
- Optimización de operaciones.
- Reducción de costos de operaciones.
- Aumento de Rentabilidad.
- Optimización de sistemas de controles.
- Mejor balance riesgo real.

**EXTERNOS**

- Marco regulatorio sobre requerimiento de capital.
- Conciencia creciente entre “stakeholder”
- Revelación externa de infraestructura de AR mejora imagen y se percibe como mayor calidad interna de gestión.

# CONSECUENCIAS DE NO GESTIONAR EL RIESGO

- Pérdidas financieras.
- Responsabilidades legales / Sanciones regulatorias.
- Interrupción temporal o definitiva del negocio.
- Pérdida de la reputación.
- Daño a personas y entorno.

## RIESGO

***Posibilidad de un hecho adverso que puede afectar negativamente la habilidad de una organización para lograr sus objetivos.***

## ADMINISTRACIÓN DE RIESGOS

***Proceso para incrementar la confianza en la habilidad de una organización de anticipar, dar prioridad y vencer obstáculos en el logro de sus objetivos.***


## GESTIÓN DE RIESGOS

*porcionar seguridad razonable en el logro de los objetivos de negocios.*

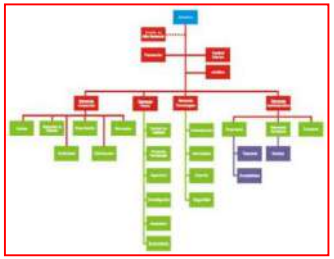
*Eficiencia y eficacia de las operaciones*

- *Informes financieros confiables*

*mplimiento con leyes y reglamentos aplicables*

Metodología del Control Interno:

- De Arriba Abajo
- Basado en Riesgo
- Orientado a Procesos
- Utilizando el Marco Integral de Control Interno de COSO
- Aplicando Estándares Internos y Externos



COSO
The Committee of Sponsoring Organizations of the Treadway Commission

*Control de Calidad*

LIMITANTES:

- Juicio
- Error humano, fallas de sistemas
- “Management override”
- Costo vs. Beneficio
- **FRAUDE**

**ENTORNO EMPRESARIAL CONTROLADO – SISTEMA/MERCADO SANO**

| | | |
|---|---|---|
| EFICIENTE Y NORMADO SISTEMA DE GESTIÓN DE RIESGOS / MARCO NORMATIVO | CONTROLES EFICIENTES Y FUNCIONANDO | ADECUADA SEGREGACIÓN DE FUNCIONES |

*GESTIÓN DE RIESGOS*

*Proporciona seguridad razonable en el logro de los objetivos de negocio:*

- *Eficiencia y eficacia de las operaciones*
- *Informes financieros confiables*
- *Cumplimiento con leyes y reglamentos aplicables*

# Gestión Integral de Riesgos
# Noviembre 2016

Econ. Alejandro Bazo Bertrán, MSc
bazo.alejandro@gmail.com
http://alejandrobazo.blogspot.pe/

# ¿Qué es el riesgo operacional?

# RIESGO OPERACIONAL - DEFINICIÓN

- Basilea II lo define con la mayor precisión posible y lo situa en relación a los otros tipos de riesgo.
- Implementa una metodología para identificarlo y medirlo.
- Establece capital regulatorio para hacer frente a sus efectos adversos.
- Los riesgos en Basilea II:
  - Mercado
  - Crédito
  - Liquidez
  - Reputaciones
  - Estratégico
  - Operativo

# RIESGO OPERACIONAL - DEFINICIÓN

Hasta antes de la definición de Basilea, se podría definer como de manera residual como:

**“el conjunto de todos aquellos riesgos no incluidos en los riesgos de mercado, de credito ni de liquidez”**

Este concepto tan general, convierte al riesgo operacional en una gran ***“bolsa de sastre”*** y no permite identificar las causas y fuentes de riesgo que lo afectan.

Aunque cabe indicar que siempre ha sido gestionado, aunque de manera reactiva y no proactiva.

# RIESGO OPERACIONAL - DEFINICIÓN

El riesgo operativo fue definido, una década antes de que apareciera el riesgo operacional como:

**“el riesgo de pérdidas inesperadas debidas a ineficiencias en los sistemas de informacióno en los controles internos”**

# RIESGO OPERACIONAL - DEFINICIÓN

En septiembre de 2001, el grupo de trabajo del Comité de Basilea, revisó la definición de riesgo operacional que había sido propuesta en 1999 en el "Nuevo Marco de Capitales de Basilea II" (publicado en junio de 2004), para quedar de la siguiente manera:

**"Riesgo operacional es el riesgo de sufrir pérdidas debido a la inadecuación o fallos en los procesos, personal y sistemas internos, o bien por causa de eventos externos".**

Es decir, se refiere a las pérdidas que pueden causa 4 factores: **personas**, **procesos**, **sistemas** y **factores externos**.

Incluye el riesgo legal, pero excluye los riesgos **reputacional**, **estratégico** y **sistémico**.

# RIESGO OPERACIONAL - DEFINICIÓN

- En 2006 ya se consideraba que era el riesgo operacional el que era una carga al capital económico de mayor importancia que la asociada al riesgo de mercado.
- Pero sin duda son los efectos adversos producidos por la ausencia o inadecuada gestión del riesgo operacional el principal factor del énfasis que hoy le dan las instituciones financieras y supervisoras y que motivan su estudio, medición, fiscalización y gestión.

# RIESGO OPERACIONAL - DEFINICIÓN

Basilea II incluye, específicamente para riesgo operacional:

- Primer pilar: **Requerimientos mínimos de capital** a las entidades bancarias; una categorización pormenorizada de los eventos de pérdida asociados; y, tres métodos de estimación para la carga de capital.
- Segundo pilar: **Supervisión**. Principios de supervision básicos, incluyendo recomendaciones específicas relacionadas con la estimación y gestión del riesgo operacional.
- Tercer pilar: **Disciplina de mercado**. Recomendaciones sobre la transparencia de mercado y divulgación de información relacionada a aspectos cualitativos y cuantitativos de riesgo operacional.

# RIESGO OPERACIONAL - DEFINICIÓN

Por tanto, es un concepto muy amplio, amplísimo, y está asociado con fallas en:

- Los sistemas;
- Los procedimientos y modelos;
- Las personas; y,
- Los eventos externos.

*"Una clara comprensión del significado del riesgo operacional en la organización es vital para su eficiente gestión"*.

Enrique Jiménez R. en *"El Riesgo Operacional. Metodologías para su medición y control"*, 2011, citando a Hoffman (2002).

# RIESGO OPERACIONAL - DEFINICIÓN

Es la posibilidad de pérdidas debido a procesos inadecuados, fallas del personal, de la tecnología de información, o eventos externos. Esta definición incluye el riesgo legal, pero excluye el riesgo estratégico y de reputación.

# RIESGO OPERACIONAL - DEFINICIÓN

- Entonces el riesgo operativo evalúa y se adelanta a la potencial pérdida económica (todavía no realizada), que se deriva de la realización de un evento adverso respecto a los resultados esperados.

- Un ejemplo para diferenciar riesgos: Considere que un cliente de alguna institución bancaria inclumple sus compromisos crediticios … ¿a qué clase de riesgo se refiere? ….

# RIESGO OPERACIONAL - DEFINICIÓN

Riesgo crediticio … por supuesto ……

Pero, ¿qué ocurre si el cliente incumple porque en el proceso de análisis de crédito no se debió haber aprobado la operación?

Supongamos que no se siguieron los lineamientos establecidos en el Manual de Créditos (uno o todos) de la institución … entonces se trata claramente de riesgo operativo y no de crédito.

# RIESGO OPERACIONAL - DEFINICIÓN

Aclaración:

Si bien al inicio los términos "**riesgo operacional**" y "**riesgo operativo**" eran utilizados como sinónimos, lo cierto es que tienen una diferencia conceptual:

**Riesgo Operativo** es contempla principalmente los fallos de operaciones internas de una entidad, mientras que, el concepto de riesgo operacional tiene un ambito bastante más amplio.

# RIESGO OPERACIONAL
# FACTORES QUE LO ORIGINAN

PERSONAS

PROCESOS

TECNOLOGIA

EVENTOS
EXTERNOS

# RIESGO OPERACIONAL
# FACTORES QUE LO ORIGINAN - PERSONAS

PERSONAS

- Errores: Concepto, razonamiento o acción equivocada de buena fe.
- Negligencia: Falta de cuidado u omisión de diligencia exigible.
- Dolo: Voluntad deliberada de engañar, incumplir una obligación o cometer un delito.

# RIESGO OPERACIONAL
# FACTORES QUE LO ORIGINAN – PERSONAS (FRAUDES)

Asociados generalmente a tres factores:

- Carácter
- Necesidad
- Oportunidad. Controles internos insuficientes:
  - ✓Falta de segregación de funciones
  - ✓Falta de supervisión adecuada
  - ✓Falta de rotación en el puesto
  - ✓Falta de limitación de acceso a los activos, cuentas o sistemas
  - ✓Ejecución ineficiente de controles debido a falta de recursos o falta de conocimiento del personal
  - ✓Colusión del personal

# RIESGO OPERACIONAL
# FACTORES QUE LO ORIGINAN – PERSONAS (FRAUDES)

## Operaciones bursátiles no autorizadas.

| Ejemplo de pérdidas operacionales por operaciones no autorizadas (en millones de dólares) | | |
|---|---|---|
| **AÑO** | **ENTIDAD** | **PÉRDIDAS** |
| 1995 | Barings Brothers & Co. Bank | USD.1,300'MM |
| 1995 | Daiwa Bank | USD.1,100'MM |
| 1996 | Sumitomo Bank | USD.2,600'MM |
| 2002 | Allied Irish Bank | USD. 750'MM |
| 2008 | Societe Generale | USD.7,000'MM |

**¡¡¡ La segregación de funciones es la clave !!!**

# RIESGO OPERACIONAL
# FACTORES QUE LO ORIGINAN – PERSONAS (FRAUDES)

Pero no siempre hay dolo … no siempre existe voluntad malisiosa de engañar a alguien o de incumplir una obligación contraída …

¡¡¡ Entonces, ¿Por qué? !!!

# RIESGO OPERACIONAL
# FACTORES QUE LO ORIGINAN – PERSONAS (FRAUDES)

En mayo de 2001, un 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 que debió ingresar.

La venta la ejecutó sobre un conjunto de valores del índice londinense FTSE 100, lo que provocó un descenso del índice de 120 puntos, equivalente a unos 40 mil millones de libras esterlinas en pérdidas.


Este es el *"Síndrome de los dedos gordos"*.

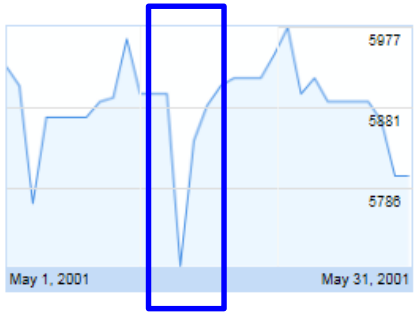
# RIESGO OPERACIONAL
# FACTORES QUE LO ORIGINAN – PERSONAS (FRAUDES)

Daily prices — May 1, 2001 - May 31, 2001 — Update

| Date | Open | High | Low | Close | Volume |
|---|---|---|---|---|---|
| May 31, 2001 | 0.00 | 5,796.15 | 5,796.15 | 5,796.15 | - |
| May 30, 2001 | 0.00 | 5,796.85 | 5,796.85 | 5,796.85 | - |
| May 29, 2001 | 0.00 | 5,863.87 | 5,863.87 | 5,863.87 | - |
| May 25, 2001 | 0.00 | 5,889.80 | 5,889.80 | 5,889.80 | - |
| May 24, 2001 | 0.00 | 5,915.91 | 5,915.91 | 5,915.91 | - |
| May 23, 2001 | 0.00 | 5,897.45 | 5,897.45 | 5,897.45 | - |
| May 22, 2001 | 0.00 | 5,976.62 | 5,976.62 | 5,976.62 | - |
| May 21, 2001 | 0.00 | 5,941.59 | 5,941.59 | 5,941.59 | - |
| May 18, 2001 | 0.00 | 5,914.98 | 5,914.98 | 5,914.98 | - |
| May 17, 2001 | 0.00 | 5,904.55 | 5,904.55 | 5,904.55 | - |
| May 16, 2001 | 0.00 | 5,884.03 | 5,884.03 | 5,884.03 | - |
| May 15, 2001 | 0.00 | 5,842.91 | 5,842.91 | 5,842.91 | - |
| May 14, 2001 | 0.00 | 5,690.47 | 5,690.47 | 5,690.47 | - |
| May 11, 2001 | 0.00 | 5,896.77 | 5,896.77 | 5,896.77 | - |
| May 10, 2001 | 0.00 | 5,963.99 | 5,963.99 | 5,963.99 | - |
| May 9, 2001 | 0.00 | 5,893.67 | 5,893.67 | 5,893.67 | - |
| May 8, 2001 | 0.00 | 5,886.40 | 5,886.40 | 5,886.40 | - |
| May 4, 2001 | 0.00 | 5,870.29 | 5,870.29 | 5,870.29 | - |
| May 3, 2001 | 0.00 | 5,765.81 | 5,765.81 | 5,765.81 | - |
| May 2, 2001 | 0.00 | 5,904.20 | 5,904.20 | 5,904.20 | - |
| May 1, 2001 | 0.00 | 5,928.02 | 5,928.02 | 5,928.02 | - |

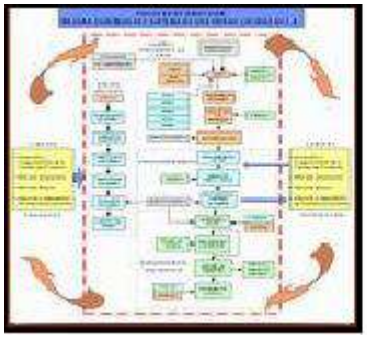
Show rows: 30 — 1 - 21 of 21 rows

Historical chart



# RIESGO OPERACIONAL
# FACTORES QUE LO ORIGINAN – PROCESOS

PROCESOS

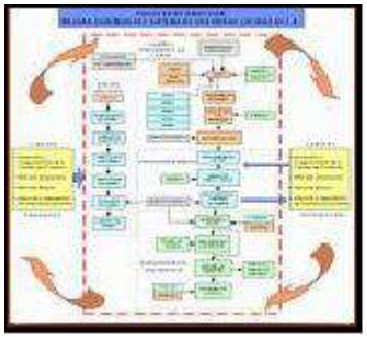


Políticas y procedimientos son:

- Inexistentes
- Inadecuados: Puede derivarse del incorrecto diseño de los mismos o de cambios en el ambiente externo o interno que los vuelve obsoletos/desfasados o inaplicables.

# RIESGO OPERACIONAL
# FACTORES QUE LO ORIGINAN – PROCESOS

PROCESOS



Pueden derivar en:

- Riesgo de modelos. debido a errores en las metodologías de gestión o en el modelo de mercado.
- Riesgo de transacciones. Errores en la ejecución de operaciones, complejidad de los productos, riesgo contractual, etc.
- Riesgo de control. Exceder límites (monetarios o de volumen) de operaciones, riesgos de seguridad, etc.

# RIESGO OPERACIONAL
# FACTORES QUE LO ORIGINAN – TECNOLOGÍA

TECNOLOGIA



Implementación de sistemas informáticos o tecnología que no son adecuados a las necesidades de la empresa, son incompatibles entre sí o presentan fallas debido a su inadecuado desarrollo o funcionamiento; pueden generar:

- Ejecución errada de las transacciones
- Inadecuada seguridad de los sistemas
- Falta de integridad y disponibilidad de la información
- Falta de continuidad de las operaciones

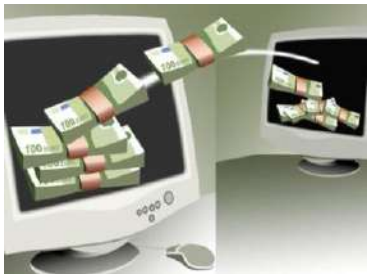
# RIESGO OPERACIONAL
# FACTORES QUE LO ORIGINAN – TECNOLOGÍA

*Crimeware.*

El fraude bancario en internet aprovechando la frágil seguridad de la banca *on line*, por lo general tiene como objetivo las transacciones financieras y las operaciones de pago con tarjetas de crédito.

Perjuicios:

- ✓ Pérdida de productividad. Parada productiva del sistema, proceso de detección de virus y reinstalación de programas.
- ✓ Pérdida de información. Cortes en los sistemas de información o daños a nivel de datos.
- ✓ Deterioro de la imagen corporativa. Publicidad negativa. La vulnerabilidad de los sistemas genera desconfianza.



# RIESGO OPERACIONAL
# FACTORES QUE LO ORIGINAN – EVENTOS EXTERNOS

EVENTOS
EXTERNOS

Factores humanos o físicos ajenos a la entidad y sobre los que ésta no tiene ningún tipo de control.

- Contingencias legales.
- Fallas en los servicios públicos.
- Fallas en servicios críticos provistos por terceros.
- Atentados y actos delictivos.
- Ocurrencia de desastres naturales.

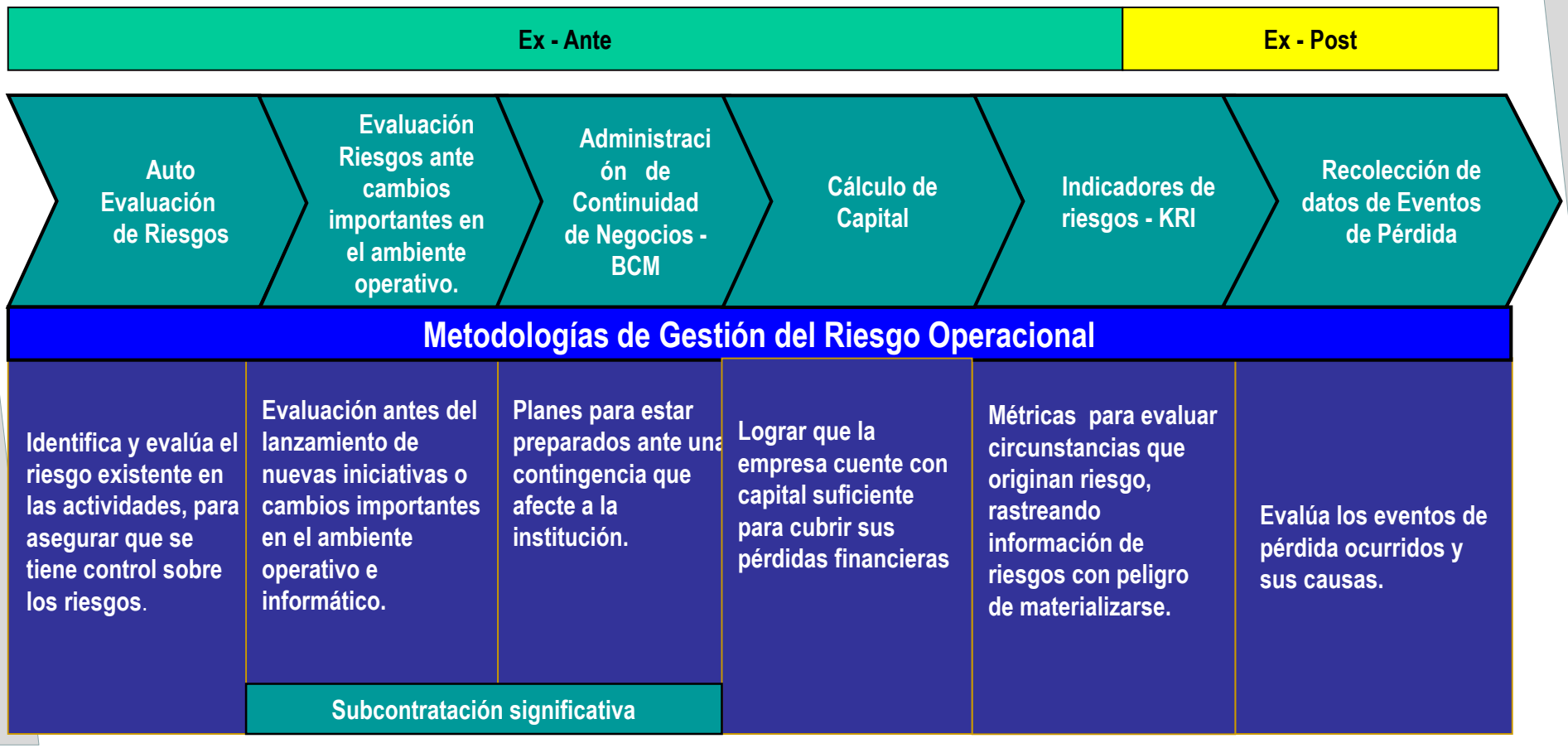
# ¿ CÓMO GESTIONAMOS EL RIESGO OPERACIONAL ?

# GESTIÓN DE RIESGO OPERACIONAL

Es el proceso interno desarrollado por la Compañía para identificar, medir, monitorear los riesgos operacionales a los que está afecta la Compañía.

Entiéndase por riesgo operacional a la posibilidad de ocurrencia de pérdidas debido a procesos inadecuados, fallas del personal, de la tecnología de información, o eventos externos. Esta definición incluye el riesgo legal, pero excluye el riesgo estratégico y de reputación.

# GESTIÓN DE RIESGO OPERACIONAL



# GESTIÓN DE RIESGO OPERACIONAL

El Comité de Basilea establece el marco conceptual para el control y la supervisión eficaz el riesgo operacional, a modo de referencia, en su documento *"Sound Practices for the Management and Supervision of Operational Risk"* (2003). En este documento se han relacionado 10 principios básicos que deben guiar el correcto tratamiento del riesgo operacional:

| SOUND PRACTICES FOR THE MANAGEMENT AND SUPERVISION OF OPERATIONAL RISK |
|---|
| **DESARROLLO DE UNA ADECUADA CULTURA DE RIESGOS** |
| Principio 1: El Directorio debe ser consciente de los principales aspectos de los riesgos operacionales de la institución financiera. |
| Principio 2: El Directorio debe asegurar que el esquema de gestión del riesgo operacional de la institución financiera esté sujeto a una auditoría interna efectiva e integral. |
| Principio 3: La Alta Gerencia es responsable de implementar el esquema de gestión del riesgo operacional aprobado por el Directorio. |

# GESTIÓN DE RIESGO OPERACIONAL

| SOUND PRACTICES FOR THE MANAGEMENT AND SUPERVISION OF OPERATIONAL RISK |
|---|
| **GESTIÓN DE RIESGOS: IDENTIFICACIÓN, EVALUACIÓN, SEGUIMIENTO, CONTROL Y MITIGACIÓN** |
| Principio 4: Las instituciones financiares deben identificar y evaluar el riesgo operacional inherente a todos los productos, actividades, procesos y sistemas relevantes. |
| Principio 5: Deben implementar un proceso para el seguimiento regular de los riesgos operacionales y de su exposición material a pérdidas. |
| Principio 6: Deben tener políticas, procesos y procedimientos para controlar o mitigar los riesgos operacionales más significativos. |
| Principio 7: Deben implementar planes de contingencia y de continuidad del negocio a fin de garantizar su capacidad para operar en forma continua y minimizar las pérdidas en caso de una interrupción severa del negocio. |
| **PAPEL DE LOS SUPERVISORES** |
| Principio 8: Los supervisores deben exigir a los bancos, independientemente de su tamaño, que implementen un sistema eficaz para identificar, evaluar, seguir y controlar o mitigar los riesgos operacionales materiales como parte de un enfoque integral para la gestión de riesgos. |
| Principio 9: Deben llevar a cabo, directa o indirectamente, una evaluación periódica independiente de las políticas, procedimientos y prácticas de un banco relacionadas con el riesgo operacional. |
| **PAPEL DE LA DIVULGACIÓN** |
| Principio 10: Las instituciones financieras deben realizar la suficiente divulgación pública para permitir que los participantes del mercado evalúen su enfoque para la gestión del riesgo operacional. |

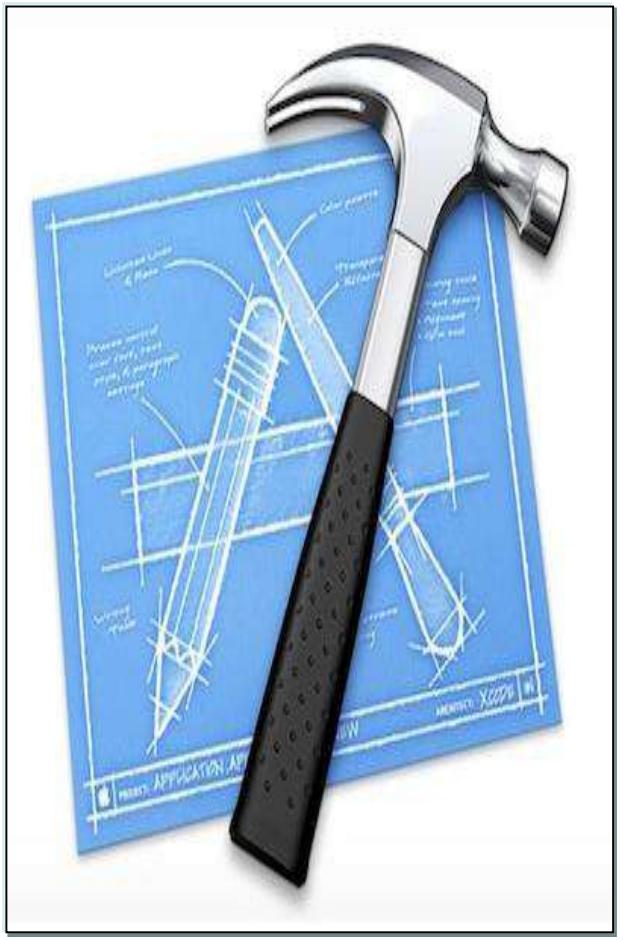
# CAMBIOS RELEVANTES
# Y
# SUBCONTRATACIÓN SIGNIFICATIVA

# GESTIÓN DE RIESGO OPERACIONAL
# CAMBIOS RELEVANTES
# AMBIENTE OPERATIVO O INFORMÁTICO

Informe de riesgos por nuevos productos o cambios importantes en el ambiente de negocios, operativo o informático que incluya las características.

La actividad consiste en identificar los riesgos operacionales y establecer medidas de tratamiento, en las siguientes actividades:

- Cambios en Procedimientos.
- Creación de Nuevos Productos o Servicios.
- Implementación de Nuevos Proyectos.
- Cambios en el entorno informático (hardware y software).



# GESTIÓN DE RIESGO OPERACIONAL
# CAMBIOS RELEVANTES - SUBCONTRATACIÓN

Modalidad de gestión mediante la cual una empresa contrata a un tercero para que éste desarrolle un proceso que podría ser realizada por la empresa contratante.

Se entiende por significativa aquella subcontratación que, en caso de falla o suspensión del servicio, puede poner en riesgo importante a la empresa, al afectar sus ingresos, solvencia, o continuidad operativa.

La subcontratación de una o más funciones de la gestión de riesgos se considera como significativa.

# GESTIÓN DE RIESGO OPERACIONAL
# CAMBIOS RELEVANTES - SUBCONTRATACIÓN

En toda subcontratación significativa debe incluirse:

- Un análisis formal de los riesgos asociados, el cual será aprobado por el Directorio.
- Cláusulas que faciliten una adecuada revisión de la prestación por parte de las empresas, de la Unidad de Auditoría Interna y de la Sociedad de Auditoría Externa.

# GESTIÓN DE RIESGO OPERACIONAL
# CAMBIOS RELEVANTES - SUBCONTRATACIÓN

Políticas y procedimientos asociados:

- Proceso de selección del proveedor.
- Elaboración del acuerdo de contratación:
  - Formalizados mediante contrato.
  - Deben incluir acuerdos de niveles de servicio (SLA).
  - Definir claramente las responsabilidades del proveedor y de la empresa.
- Gestión de riesgos asociada a la subcontratación.
- Implementación de entorno de control efectivo.
- Establecimiento de planes de continuidad.

# GESTIÓN DE RIESGO OPERACIONAL
# CAMBIOS RELEVANTES - SUBCONTRATACIÓN

Las empresas:

- Asumen plena responsabilidad sobre los resultados de los procesos subcontratados.
- Deben asegurarse que se mantenga reserva y confidencialidad sobre la información proporcionada.
- Deben establecer políticas y procedimientos para evaluar, administrar y monitorear los procesos subcontratados.
- Deben formalizar los acuerdos de subcontratación mediante contratos firmados, los cuales deben incluir acuerdos de niveles de servicio, y definir claramente las responsabilidades del proveedor y de la empresa.

# GESTIÓN DE RIESGO OPERACIONAL
# PROCESOS TERCERIZADOS

| | |
|---|---|
| **Programa general de gestión de riesgos de procesos tercerizados**<br>Evaluar el programa general implementado para manejar el riesgo de procesos ejecutados por terceros.<br>Cubrir los criterios y proceso de evaluación de riesgos, roles y responsabilidades de áreas, protocolos de comunicación, políticas y procedimientos y un programa de monitoreo continuo. | ¿Cuán consistente es el proceso de riesgo de proveedores de servicios de procesos tercerizados?<br>¿Cuán incorporado está el proceso en la organización?<br>¿La propiedad, roles y responsabilidades están claramente entendidos?<br>¿Se han implementado los procesos de gestión de riesgos tanto para proveedores directos como indirectos? |
| **Proceso de gestión de contratos**<br>Proceso y responsabilidades de control y fiscalización; proceso general para la firma de nuevos contratos y renovar los existentes.<br>Proceso de cumplimiento. | ¿Existe un proceso para mantener y administrar contratos?<br>¿Se han establecido métricas y criterios para las revisiones periódicas? |

# GESTIÓN DE RIESGO OPERACIONAL
# PROCESOS TERCERIZADOS

| | |
|---|---|
| **Programa de gestión de proveedores de servicios de procesos tercerizados**<br>Incluir revisiones del sitio del proveedor, en relación con la política de seguridad; privacidad y gestión de datos; seguridad del personal; control de accesos; seguridad física y medioambiental; desarrollo y mantenimiento de sistemas; evaluación de contratos; evaluación financiera; mapeo de procesos; cumplimiento y continuidad de negocio. | ¿Se han desarrollado criterios y métricas que identifiquen temprano problemas potenciales? ¿Cuenta con un proceso de presentación periódica de información clave por proveedores para su revisión y seguimiento? |

# CLASIFICACIÓN DE EVENTOS DE PÉRDIDA BASILEA

| Tipo de Pérdida | |
|---|---|
| **Nivel I** | **Nivel II** |
| Fraude Interno | Actividades No Autorizadas |
| | Robo y Fraude Interno |
| Fraude Externo | Robo y Fraude Externo |
| | Seguridad de los Sistemas |
| Relaciones laborales y seguridad en el puesto de trabajo | Relaciones laborales |
| | Higiene y seguridad en el trabajo |
| | Diversidad y discriminación |
| Clientes, productos y prácticas empresariales | Adecuación, divulgación de información y confianza |
| | Prácticas empresariales o de Mercado improcedentes |
| | Productos defectuosos |
| | Selección, patrocinio y riesgos |
| | Actividades de asesoramiento |
| Daños a activos físicos | Desastres y otros acontecimientos |
| Interrupción en los negocios y fallas en los sistemas | Sistemas |
| Ejecución, entrega y gestión de procesos | Recepción, ejecución y mantenimiento de operaciones |
| | Seguimiento y presentación de informes |
| | Aceptación de clientes y documentación |
| | Gestión de cuentas de clientes |
| | Contrapartes comerciales |
| | Distribuidores y proveedores |

# CLASIFICACIÓN DE EVENTOS DE PÉRDIDA BASILEA

| Tipo de Pérdida | | | |
|---|---|---|---|
| Nivel I | Definición | Nivel II | Ejemplos |
| Fraude Interno | Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o soslayar regulaciones, leyes o políticas empresariales (excluidos los eventos de diversidad y discriminación) en las que se encuentra implicado, al menos, un miembro de la empresa. | Actividades No Autorizadas | Operaciones no reveladas (intencionalmente), operaciones no autorizadas (con pérdidas pecunarias), valorización erronea de posiciones (intencional). |
| | | Robo y Fraude Interno | Robo, malversación, falsificación, soborno, apropiación de cuentas, contrabando, evasión de impuestos (intencional). |
| Fraude Externo | Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o soslayar la legislación, por parte de un tercero. | Robo y Fraude Externo | Robo, falsificación. |
| | | Seguridad de los Sistemas | Daños por ataques informáticos, robo de información. |
| Relaciones laborales y seguridad en el puesto de trabajo | Pérdidas derivadas de acutaciones incompatibles con la legislación o acuerdos laborales, sobre higiene o seguridad en el trabajo, sobre el pago de reclamaciones por daños personales, o sobre casos relacionados con la diversidad o discriminación. | Relaciones laborales | Cuestiones relativas a remuneración, prestaciones sociales, extinción de contratos. |
| | | Higiene y seguridad en el trabajo | Casos relacionados con las normas de higiene y seguridad en el trabajo; indemnización a los trabajadores. |
| | | Diversidad y discriminación | Todo tipo de discriminación. |

# CLASIFICACIÓN DE EVENTOS DE PÉRDIDA BASILEA

| Tipo de Pérdida | | | |
|---|---|---|---|
| **Nivel I** | **Definición** | **Nivel II** | **Ejemplos** |
| Clientes, productos y prácticas empresariales | Pérdidas derivadas del incumplimiento involuntario o negligente de una obligación empresarial frente a clientes concretos (incluidos requisitos fiduciarios y de adecuación), o de la naturaleza o diseño de un producto. | Adecuación, divulgación de información y confianza | Abusos de confianza / incumplimiento de pautas, aspectos de adecuación / divulgación de información (conocimiento del cliente, etc.), quebrantamiento de la privacidad de información sobre clientes minoristas, quebrantamiento de privacidad, ventas agresivas, abuso de información confidencial. |
| | | Prácticas empresariales o de Mercado improcedentes | Prácticas restrictivas de la competencia, prácticas comerciales / de mercado improcedentes, manipulación del mercado, abuso de información privilegiada (en favor de la empresa), lavado de dinero. |
| | | Productos defectuosos | Defectos del producto (no autorizado, etc.), error de los modelos. |
| | | Selección, patrocinio y riesgos | Ausencia de investigación a clientes conforme a las directrices, exceso de los límites de riesgo frente a clientes. |
| | | Actividades de asesoramiento | Litigios sobre resultados de las actividades de asesoramiento. |
| Daños a activos físicos | Pérdidas derivadas de daños o perjuicios a activos materiales como consecuencia de desastres naturales u otros acontecimientos. | Desastres y otros acontecimientos | Pérdidas por desastres naturales, pérdidas humanas por causas externas (terrorismo, vandalismo). |

# CLASIFICACIÓN DE EVENTOS DE PÉRDIDA BASILEA

| Tipo de Pérdida | | | |
|---|---|---|---|
| **Nivel I** | **Definición** | **Nivel II** | **Ejemplos** |
| Interrupción en los negocios y fallas en los sistemas | Pérdidas derivadas de interrupciones en el negocio y de fallos en los sistemas. | Sistemas | Pérdidas por fallas en equipos de hardware, software o telecomunicaciones, falla en energía eléctrica. |
| Ejecución, entrega y gestión de procesos | Pérdidas derivadas de errores en el procesamiento de operaciones o en la gestión de procesos, así como de relaciones con contrapartes comerciales y proveedores. | Recepción, ejecución y mantenimiento de operaciones | Errores de introducción de datos, mantenimiento o descarga, incumplimiento de plazos o de responsabilidades, ejecución errónea de modelos / sistemas, errores contables. Errores en el proceso de compensación de valores y liquidación de efectivo (por ejemplo en el delivery versus payment). |
| | | Seguimiento y presentación de informes | Incumplimiento de la obligación de informar, inexactitud de informes externos (con generación de pérdidas). |
| | | Aceptación de clientes y documentación | Inexistencia de autorizaciones / rechazos de clientes, documentos jurídicos inexistentes / incompletos. |
| | | Gestión de cuentas de clientes | Acceso no autorizado a cuentas, registros incorrectos de clientes (con generación de pérdidas), pérdida o daño de activos de clientes por negligencia. |
| | | Contrapartes comerciales | Fallos de contrapartes distintas de clientes, otros litigios con contrapartes distintas de clientes. |
| | | Distribuidores y proveedores | Subcontratación, litigios con proveedores. |


Riesgo Operacional
Seguridad de Información
Continuidad del Negocio

# GESTIÓN DE CONTINUIDAD DEL NEGOCIO

# GESTIÓN DE CONTINUIDAD DEL NEGOCIO

"A medida que las organizaciones crecen, tanto en tamaño como en complejidad, el impacto de la no disponibilidad decualquier recurso se ha multiplicado.

Los eventos de gran visibilidad causados por desastres naturales y fallas de infraestructura tecnológica han aumentado la toma de consciencia sobre la necesidad de desarrollar, mantener y sostener programas de continuidad del negocio (…)

Empresas que anteriormente habrían sobrevivido a un desastre o perturbación mayor, pueden encontrar ahora que el mismo evento empuje su existencia corporativa al borde del precipicio. Los ejecutivos están dándose cuenta que una BCM eficaz puede ser el único amortiguador entre una pequeña perturbación y la bancarrota".

"Perspectivas sobre Gobierno, Riesgo y Cumplimiento". EY. 2014.

# GESTIÓN DE CONTINUIDAD DEL NEGOCIO

Proceso interno implementado en una empresa a través de un conjunto de políticas y procedimientos utilizados para minimizar el impacto de los eventos de interrupción de negocio y lograr la operación normal del negocio, manteniéndose las pérdidas financieras y operacionales en un nivel aceptable, mediante una combinación de controles preventivos y acciones de respuesta.

Incendio

Desastres Naturales

Terrorismo

Sabotaje

# GESTIÓN DE CONTINUIDAD DEL NEGOCIO

La GCN consiste en:

- Identificar procesos, productos, servicios y proveedores, clasificándolos por su criticidad.
- Evaluar los riesgos que podrían causar la interrupción de actividades que puedan poner en riesgo la CN (fallas en el ambiente informático, desastres naturales, eventos delictivos, etc.).
- Evaluar el impacto que causaría la interrupción.
- Establecer el periodo máximo tolerable de interrupción.
- Definir qué procesos requieren contar con una estrategia de continuidad y asegurar la continuidad de los mismos.

# GESTIÓN DE CONTINUIDAD DEL NEGOCIO

**Objetivos:**

- Proteger al personal y los activos de la empresa.
- Implementar respuestas efectivas para que la operatividad del negocio continúe de una manera razonable y dentro de márgenes de tiempo tolerables, ante la ocurrencia de eventos que puedan crear una interrupción o inestabilidad en sus operaciones.
- Alcance: las líneas de negocio de la empresa, conformadas por productos y servicios, soportados por procesos.
- Administrar las crisis y emergencias que se presenten.
- Cumplir con la normativa vigente.

**Evaluación costo/beneficio**

# GESTIÓN DE CONTINUIDAD DEL NEGOCIO

**Importancia:**

- Salva vidas.
- Mantiene la continuidad de las operaciones y servicios.
- Confianza del cliente y de la organización (refuerza su cultura).
- Es una ventaja competitiva / reputación de la empresa.
- Mitiga los riesgos del negocio y las exposiciones financieras.
- Preservación de la información del negocio.
- Cumplimiento de la regulación (supervisadas).

**Evaluación costo/beneficio**

# GESTIÓN DE CONTINUIDAD DEL NEGOCIO

**Algunas estrategias de GCN:**

- Servidores alternos de respaldo de información y aplicaciones que dan soporte a los procesos críticos.
- Procedimientos de contingencia: Plan de Gestión de Crisis, Plan de Continuidad, Plan de Emergencia, Plan de Recuperación.
- Capacitación del personal.
- Pruebas periódicas de planes.
- Asegurar que los proveedores de servicios críticos administren su GCN.
- Dar mantenimiento periódico / actualizar Planes.

# GESTIÓN DE CONTINUIDAD DEL NEGOCIO

## Metodología:

| Fase | Nombre de la Fase | Descripción de la Actividad |
|---|---|---|
| Fase I | Planificación de la GCN | Consiste en conocer los objetivos y metas de la empresa a fin de definir el alcance del programa de GCN. Debe identificar los procesos críticos que se evaluarán en el Análisis de Impacto del negocio (BIA). |
| Fase II | Entender la organización | Evaluar los riesgos que podrían causar una interrupción de las actividades de la empresa y el impacto que podría tener dicha interrupción, así como definir los escenarios para los cuales se establecerán estrategias. |
| Fase III | Establecer la estrategia de continuidad | Seleccionar y establecer las diferentes estrategias disponibles para proteger y mantener la continuidad de los procesos críticos de la empresa y garantizar la entrega del servicio al cliente, dentro del RTO |
| Fase IV | Desarrollar e implementar la respuesta de continuidad | Desarrollar planes de respuesta ante los eventos analizados en las fases previas e implementar un modelo de respuesta flexible y escalable que permita cubrir los eventos inesperados y proveer los recursos necesarios, acorde con la estrategia seleccionada, para enfrentar con éxito un evento de interrupción de operaciones. |
| Fase V | Probar, mantener y revisar | Realizar ejercicios para validar los planes y procedimientos desarrollados, así como realizar su revisión y mantenimiento de forma periódica y a intervalos definidos. |

Integrar la GCN a la cultura de la organización: proceso para desarrollar e incorporar de forma sostenida la GCN en la cultura de la organización es consecuencia de los siguientes 3 pasos:

- Evaluación del grado de conocimiento sobre la GCN.
- Desarrollo y mejora de la cultura de continuidad.
- Monitoreo permanente.

# GESTIÓN DE CONTINUIDAD DEL NEGOCIO

## Roles y responsabilidades:

| Gerente General | |
|---|---|
| 1. | Implementar el Plan de Continuidad del Negocio, aprobando los recursos necesarios para una adecuada ejecución. |
| 2. | En un evento de interrupción de operaciones, emitir comunicados a la prensa y entidades externas. |

# GESTIÓN DE CONTINUIDAD DEL NEGOCIO

## Roles y responsabilidades:

| Líder del Plan de Recuperación de TI (Gerente de TI) | |
|---|---|
| 1. | Activar el Plan de Recuperación de TI y realizar seguimiento del cumplimiento del mismo y emitir el informe correspondiente luego de finalizado el evento. |
| 2. | Mantener acuerdos de nivel de servicio con los proveedores claves de TI y en caso de eventos de interrupción, monitorear el cumplimiento de los mismos. |
| 3. | Participar activamente en los talleres para el desarrollo de la GCN, tales como: entendimiento de procesos, análisis de impacto en el negocio, evaluación de riesgos, etc. |
| 4. | Participar en las charlas de concientización y capacitación relacionadas a la GCN y en las actividades de integración de la GCN a la cultura organizacional de la empresa. |
| 5. | Identificar el origen de la contingencia y tratar de solucionarla. De tratarse de un problema con un proveedor externo realizar las coordinaciones con el mismo para su regularización en los tiempos establecidos. |
| 6. | Informar a las personas encargadas dentro de la empresa de la existencia del evento de interrupción de operaciones, así como el tiempo estimado de solución (activar un **árbol de llamadas**). |
| 7. | Informar la regularización de las operaciones al personal responsable. |
| 8. | Después de solucionado el problema, deberá realizar un diagnóstico del evento de interrupción ocurrido y proponer mejoras para que no se repita o disminuir el impacto del evento. |
| 9. | Revisar periódicamente el Plan de Recuperación de TI y realizar las actualizaciones necesarias. |
| 10. | Ejecutar las pruebas y ejercicios del Plan de Recuperación de TI y emitir los informes respectivos. |

# GESTIÓN DE CONTINUIDAD DEL NEGOCIO

## Roles y responsabilidades:

| Líder del Plan de Continuidad del Negocio (Gerente de Operaciones) | |
|---|---|
| 1. | Durante el evento de interrupción, evaluar e informar el escenario presentado y el impacto de la interrupción en el proceso, coordinando con la Gerencia de TI el tiempo estimado para la solución de la contingencia. |
| 2. | Activar el Plan de Continuidad del Negocio. |
| 3. | Coordinar con el personal a su cargo la activación del Plan, así como la desactivación, una vez superada la contingencia. |
| 4. | Coordinar con la Gerencia de TI la habilitación del Sitio Alterno para procesar operaciones de las instalaciones que se encuentren en contingencia. |
| 5. | Verificar que todas las operaciones de clientes recibidas durante la contingencia hayan sido procesadas correctamente, ya sea en el sitio alterno o no, una vez solucionado el problema. |
| 6. | Informar al personal implicado la regularización de las operaciones y la desactivación del plan. |
| 7. | Realizar un diagnóstico del evento de interrupción de operaciones, presentar y proponer mejoras para que la misma no se vuelva a presentar o disminuir el impacto de la misma. |
| 8. | Elaborar y mantener actualizado el PCN en coordinación con el Oficial de Continuidad del Negocio. |
| 9. | Ejecutar y/o participar en las pruebas y ejercicios de GCN según corresponda. |
| 10. | Realizar semestralmente pruebas operativas en el sitio alterno, verificando la funcionalidad de los equipos, acceso a red de comunicaciones, impresora y anexo; luego debe completar la ficha de pruebas y hacerle llegar copia del mismo al Jefe de Riesgos. |

# GESTIÓN DE CONTINUIDAD DEL NEGOCIO

## Roles y responsabilidades:

| Líder del Plan de Continuidad del Negocio (Gerente de Operaciones) | |
|---|---|
| 11. | Difundir el PCN al personal bajo su cargo y guardar copia impresa del mismo en su domicilio. |
| 12. | Participar activamente en los talleres para el desarrollo de la GCN, tales como: talleres de entendimiento del proceso, talleres de análisis de impacto en el negocio, talleres de evaluación de riesgos, entre otros.. |
| 13. | Participar en las charlas de concientización y capacitación relacionadas a la GCN y en las actividades de integración de la GCN a la cultura organizacional de la empresa. |

# GESTIÓN DE CONTINUIDAD DEL NEGOCIO

## Roles y responsabilidades:

| Oficial de Continuidad del Negocio | |
|---|---|
| 1. | Llevar un registro de los eventos de interrupción de operaciones reportadas. |
| 2. | Participar de pruebas de continuidad del negocio programadas, ejecutar pruebas sorpresivas y hacer seguimiento de las observaciones e incidencias presentadas en la misma. |
| 3. | Informar periódicamente a la Gerencia General, Comité de Riesgos, Directorio y ente regulador los eventos de interrupción registrados de las operaciones. |
| 4. | Evaluar el evento de interrupción presentado y realizar recomendaciones para que la misma no se vuelva a presentar o disminuir el impacto de la misma. |
| 5. | Elaborar plan de capacitación anual y velar por integrar la GNC a la cultura organizacional. |
| 6. | Guardar copia del plan de continuidad en su domicilio. |

# GESTIÓN DE CONTINUIDAD DEL NEGOCIO

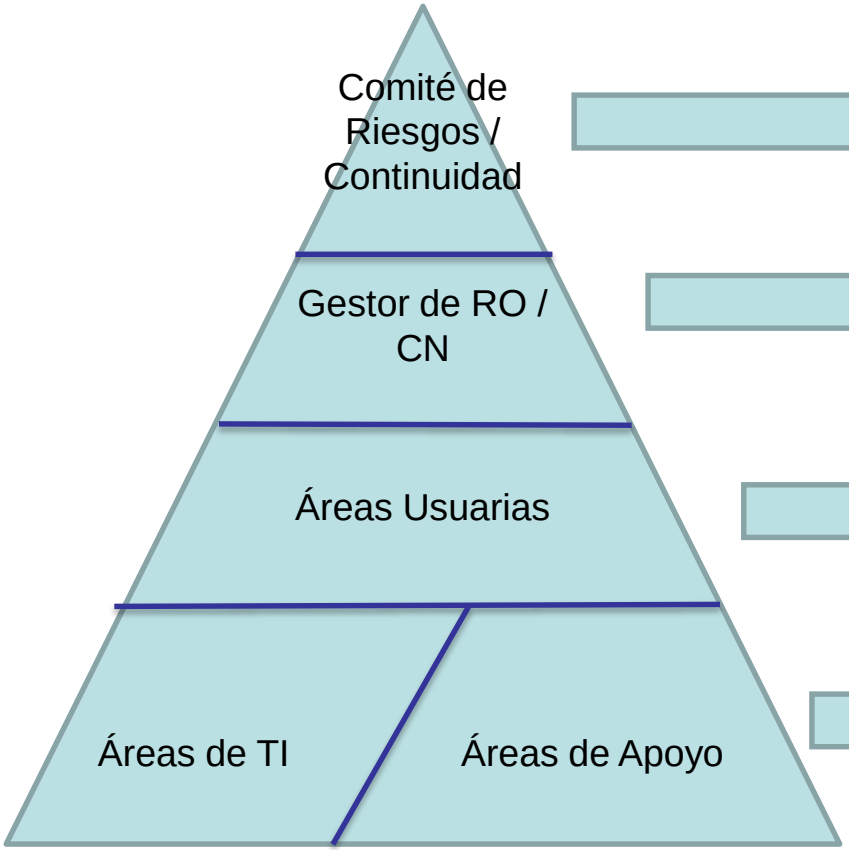
## Roles y responsabilidades:

| Colaboradores (todos): | |
|---|---|
| 1. | Ejecutar los procedimientos y actividades definidas en el Plan de Continuidad del Negocio. |

| Otros (importante): | |
|---|---|
| 1. | Mantener actualizado el listado de los contactos internos y externos de la empresa. |
| 2. | Mantener actualizado el listado de proveedores claves de la empresa. |
| 3. | Informar al responsable de Continuidad del Negocio los cambios que ocurran en los procesos de la empresa. |

# GESTIÓN DE CONTINUIDAD DEL NEGOCIO

## Estructura Organizacional




- Establece y soporta adecuadamente la GCN
- Administra la GCN asegurando que sea permanente y conducida metodológicamente
- Estar preparado para recuperar los procesos del negocio
- Estar preparado para recuperar los servicios de TI y procesos de soporte

# GESTIÓN DE CONTINUIDAD DEL NEGOCIO

**Respuestas de CN:**

- **Plan de CN por línea de negocio y proceso:** Describe las actividades a ejecutar para restablecer la **operatividad mínima aceptable** de los procesos críticos.
- **Plan de Emergencia** (por local/oficina/ubicación): Describe las actividades a realizar para salvaguardar la integridad de las personas.
- **Plan de Gestión de Crisis:** Describe las actividades a realizar para la comunicación con externos y toma de decisiones.
- **Plan de Recuperación de Desastres TIC:** Describe las actividades a realizar para restablecer el funcionamiento de los sistemas de información y comunicaciones que soportan los procesos críticos.

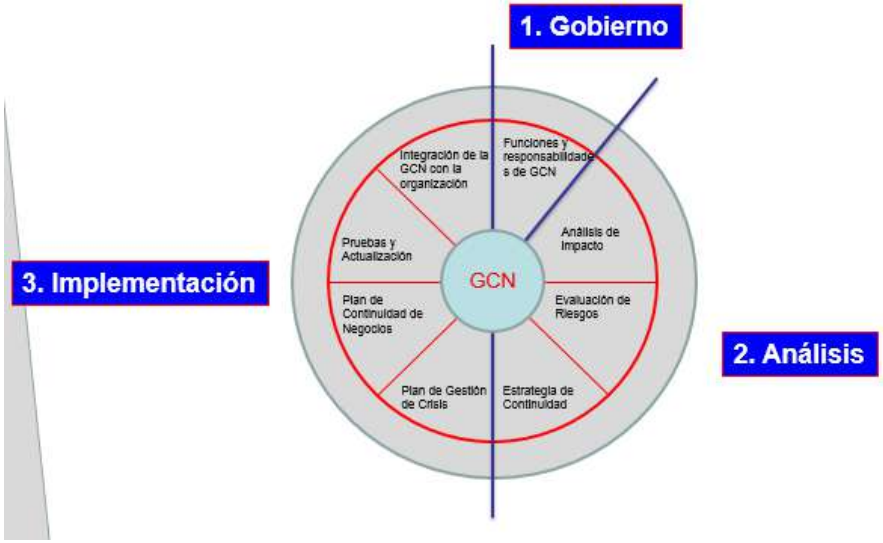

# GESTIÓN DE CONTINUIDAD DEL NEGOCIO

1. Gobierno

2. Análisis

3. Implementación

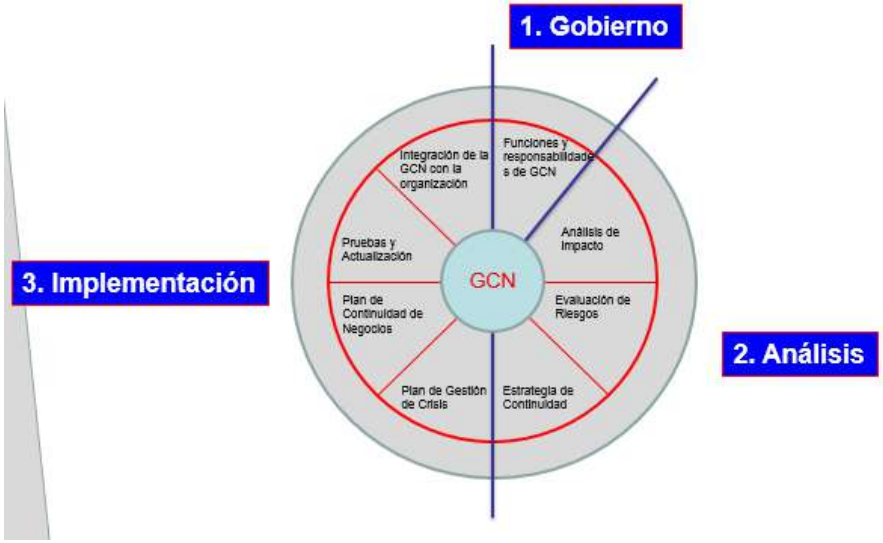
# GESTIÓN DE CONTINUIDAD DEL NEGOCIO
## 1. Gobierno




Funciones y Responsabilidades:

- La empresa deberá contar con una función de Continuidad del Negocio.
- El Directorio es el responsable de establecer una adecuada GCN.
- La Gerencia General es la responsable de implementar la GCN.
- La Unidad de Riesgo asegura el cumplimiento de las políticas y procedimientos.

# GESTIÓN DE CONTINUIDAD DEL NEGOCIO
## 2. Análisis

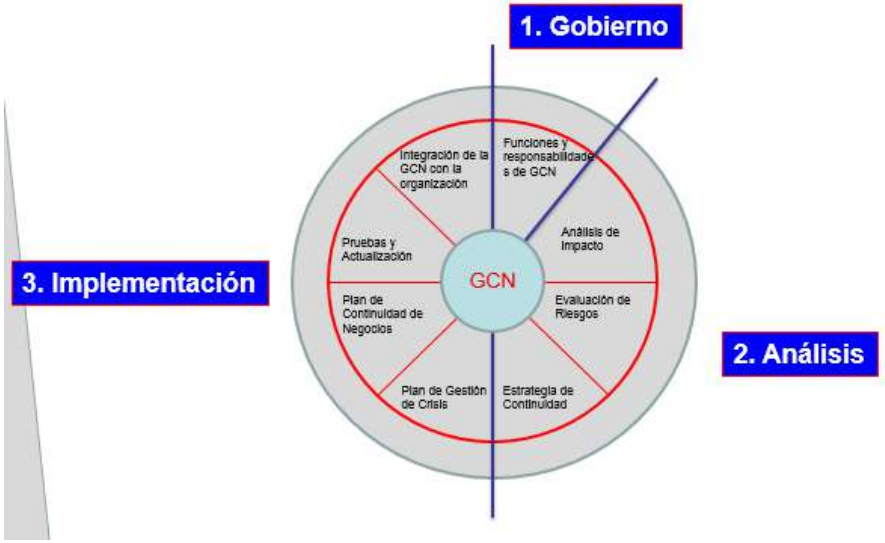



Análisis de Impacto en el Negocio (BIA):

- Relevamiento de información del proceso orientado a identificar puntos de falla, activos de información críticos y escenarios posibles de interrupción o no disponibilidad del proceso.
- Análisis de escenarios de interrupción en el cual se relaciona los procesos, los tiempos de interrupción y los posibles impactos.
- Definición de RTO, RPO y MTD de los procesos analizados.

RTO – Tiempo objetivo de recuperación – Recovery Time Objective
RPO – Punto objetivo de recuperación – Recovery Point Objective
MTD – Tiempo máximo de recuperación – Maximun Tolerable Downtime

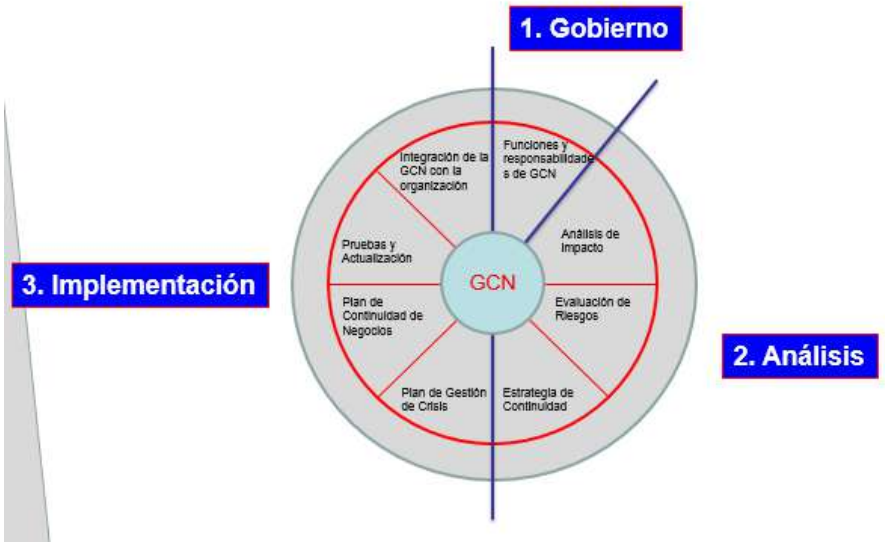
# GESTIÓN DE CONTINUIDAD DEL NEGOCIO
## 2. Análisis




Evaluación de Riesgos:

- Análisis de Riesgos asociados a la interrupción de las operaciones.
- Evaluación del impacto de materializarse cualquiera de los siguientes escenarios:
  - Caída total de los Sistemas.
  - Caída parcial de los Sistemas.
  - Caída de las telecomunicaciones.
  - Pérdida de datos de los Sistemas.
  - Corte de fluido eléctrico.
  - Desastres naturales.
  - Sabotaje o terrorismo.
  - Pandemia.

# GESTIÓN DE CONTINUIDAD DEL NEGOCIO
## 2. Análisis




Estrategia de Continuidad:

- A partir del resultado del análisis de impacto y evaluación de riesgos de una interrupción del negocio, se desarrollan diferentes estrategias de recuperación para poder hacer frente a los escenarios de riesgo propuestos.
- De acuerdo a los RTO y RPO definidos en los análisis de impacto y evaluación de riesgos, se define la estrategia más acorde a las necesidades de la compañía.
- Aquellos riesgos que no tienen un escenario definido, deben ser asumidos por la compañía.

# GESTIÓN DE CONTINUIDAD DEL NEGOCIO
## 3. Implementación

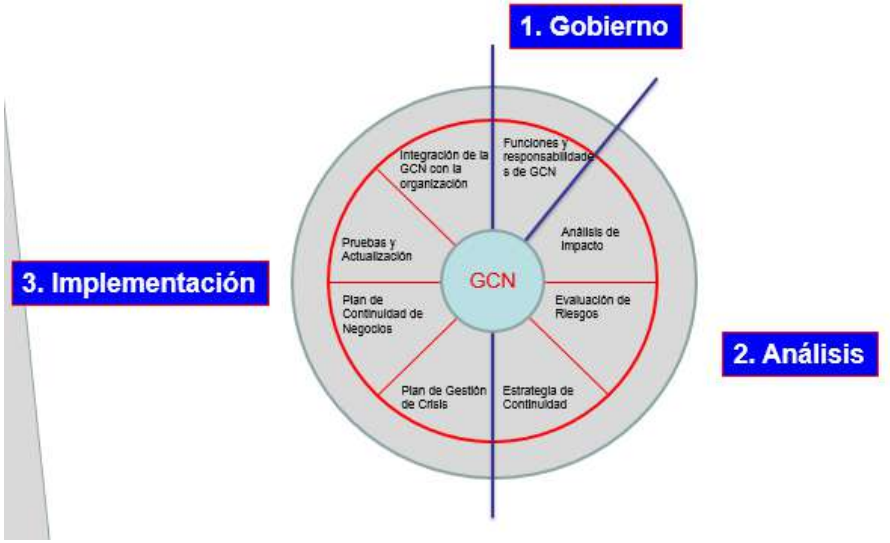
Plan de Gestión de Crisis:

- Consiste en preparar la empresa para enfrentarse a la fase aguda de un evento de interrupción de operaciones, incluso de aquellos no esperados.
- Contar con un Plan de Gestión de Crisis, el que dependiendo del nivel de interrupción y el tipo de crisis, activa los procedimientos establecidos para retornar a las actividades normales de atención.

# GESTIÓN DE CONTINUIDAD DEL NEGOCIO
# 3. Implementación

Plan de Continuidad del Negocio:

- Su objetivo es dotar la compañía de la capacidad de mantener, o de ser el caso recuperar, los principales procesos de negocio dentro de los parámetros previamente establecidos.
- Para recuperar los principales procesos la compañía debe contar con algunos planes:
  - Planes de tipo BCP (Business Continuity Plan) orientados a recuperar los procesos.

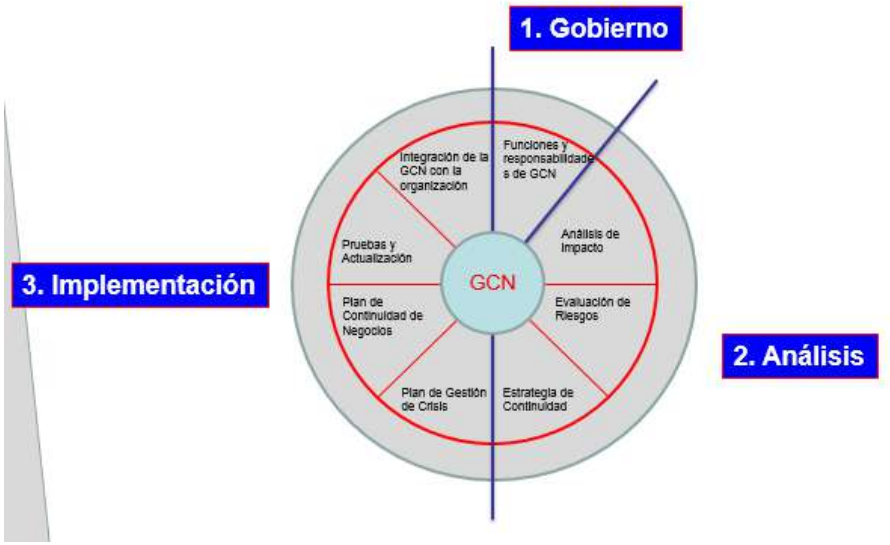



  - Planes de tipo DRP (Desaster Recovery Plan) orientados a recuperar los sistemas.
  - Planes de emergencia, orientados a salvaguardar al personal de la empresa.

# GESTIÓN DE CONTINUIDAD DEL NEGOCIO
## 3. Implementación

Pruebas y Actualización:

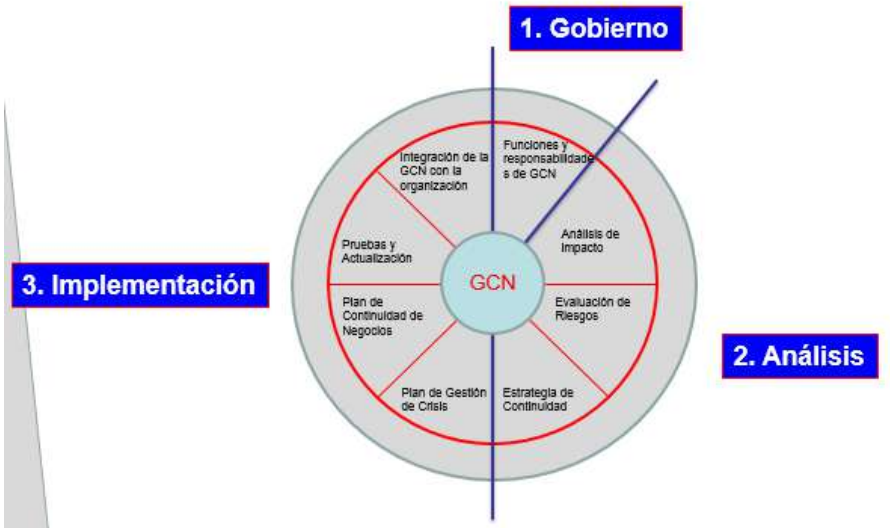
- Anualmente el área de Riesgo Operacional debe prepara un plan de pruebas de planes de continuidad.
- En estas pruebas se simulan escenarios de riesgo o crisis y se evalúan los tiempos de respuesta versus los RPO y se determina si se están cumpliendo los tiempos objetivo de recuperación.



# GESTIÓN DE CONTINUIDAD DEL NEGOCIO
## 3. Implementación

Integración de la GCN a la cultura organizacional:

- Cursos de inducción de Riesgo Operacional, que incluye la capacitación en gestión de continuidad del negocio.
- Las pruebas de los planes de continuidad del negocio son realizadas por el personal de la empresa en coordinación y conjunto con el área de Riesgo Operacional.
- Programas de capacitación y evaluación en los que se mide el grado de conocimiento sobre la GCN.



# GESTIÓN DE CONTINUIDAD DEL NEGOCIO

Tipos de pruebas de GCN:

| Complejidad | Tipo | Descripción |
|---|---|---|
| Baja | Prueba de Escritorio (Comprobación sobre el papel) | Revisar el contenido del Plan de Continuidad del Negocio (PCN). |
| Media | Ensayo | Validar el contenido del PCN a partir de entrevistas. |
| | Simulación | Usar situaciones artificiales para validar que el PCN contiene la información necesaria para una recuperación exitosa. |
| | Pruebas de las actividades críticas | Invocar los PCN en una situación que no haga peligrar el negocio. |
| Alta | Prueba completa, incluyendo la gestión de incidentes y pruebas con agentes externos. | Prueba real de abandono de edificios, caída del data center, etc. |

# GESTIÓN DE CONTINUIDAD DEL NEGOCIO

## Tipos de pruebas de GCN:

- **Prueba de escritorio:** Son un método efectivo (y poco costoso) de ejercitar los planes de continuidad, sin ocasionar una interrupción en la operativa del negocio, elevando aun así, el nivel de preparación de la empresa. Se reúne al equipo de gestión de crisis para discutir secuencialmente los pasos a seguir ante un escenario de desastre.
- **Ensayo:** El Oficial de CN realiza en forma sorpresiva entrevistas con la finalidad de validar el contenido del Plan de CN con los dueños de los procesos críticos y demás participantes.

# GESTIÓN DE CONTINUIDAD DEL NEGOCIO

## Tipos de pruebas de GCN:

- **Simulación:** Se simula un desastre. El funcionamiento normal de la empresa no debe ser interrumpido. Un escenario de desastre debería tomar en consideración el propósito de la prueba, los objetivos, el tipo de prueba, calendario, programación, duración, los participantes en la prueba, las tareas, las restricciones, las suposiciones, y los pasos de la prueba. Pueden incluir procedimientos de notificación, procedimientos operativos temporales, y operaciones de recuperación y de respaldo.
- Los dueños de los procesos y el Oficial de CN deben evaluar: hardware, software, personal, comunicaciones radiotelefónicas y de datos, procedimientos, suministros y formularios, documentación, transporte, servicios básicos (electricidad, aire acondicionado, calefacción, ventilación), y el procesamiento del sitio alterno.
- Puede que no sea práctico ni económicamente viable realizar ciertas tareas durante una prueba de simulación (por ejemplo, viajes largos, traslado del equipo, eliminación de comunicaciones radiotelefónicas o de datos).

# GESTIÓN DE CONTINUIDAD DEL NEGOCIO

## Tipos de pruebas de GCN:

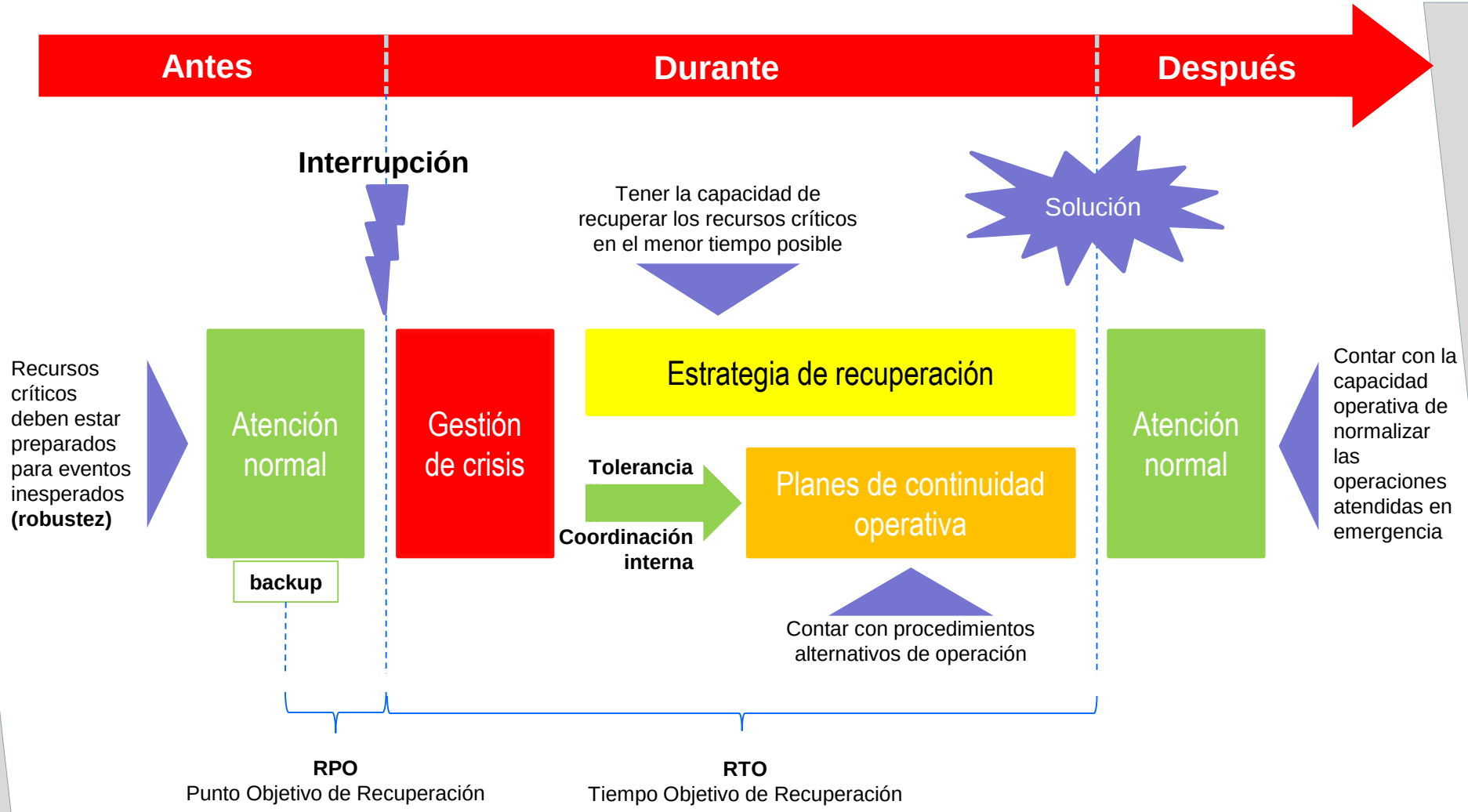
- **Prueba de actividades críticas:** Se define el alcance en la cual se realizará la prueba, a fin de invocar los planes en una situación que no haga peligrar el negocio.
- **Prueba completa (incluye pruebas con agentes externos):** Se realiza una prueba real que debe involucrar escenarios de terremoto, caída total del sistema, caída de data center principal, etc. Se planificará y acordará con los dueños de los procesos con el objetivo que el riesgo de provocar un incidente derivado de la prueba del plan sea minimizado.

# GESTIÓN DE CONTINUIDAD DEL NEGOCIO

**Consideraciones para la ejecución de pruebas:**

- Ejecutar las pruebas cuando las interrupciones afecten menos las operaciones del negocio.
- Involucrar la participación del personal clave del equipo y/o activación de los comités según corresponda.
- Simular condiciones reales de procesamiento de horas principales.
- Evaluar el desempeño del personal que participó.
- Evaluar el entrenamiento y conciencia de continuidad del personal externo.
- Evaluar la coordinación entre los equipos de continuidad y los proveedores.
- Planificar detalladamente cada prueba, independientemente del tipo, considerando las actividades que se tienen que realizar antes, durante y después de la prueba.

# GESTIÓN DE CONTINUIDAD DEL NEGOCIO



# GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

# GESTIÓN DE SEGURIDAD DE INFORMACIÓN

## ¿Qué es la Seguridad de la Información?

Todas aquellas medidas preventivas y correlativas aplicadas por las organizaciones que permitan resguardar y proteger la **información** buscando mantener la **confidencialidad**, la **disponibilidad** e **integridad** de la misma.

# GESTIÓN DE SEGURIDAD DE INFORMACIÓN

## ¿Qué es la Seguridad de la Información?

Todas aquellas medidas preventivas y correlativas aplicadas por las organizaciones que permitan resguardar y proteger la **información** buscando mantener la **confidencialidad**, la **disponibilidad** e **integridad** de la misma.

| | |
|---|---|
| CONFIDENCIALIDAD | Accesible a personal autorizado |
| DISPONIBILIDAD | Activos de información disponibles de forma organizada cuando sea requerida |
| INTEGRIDAD | Información completa, exacta y válida |

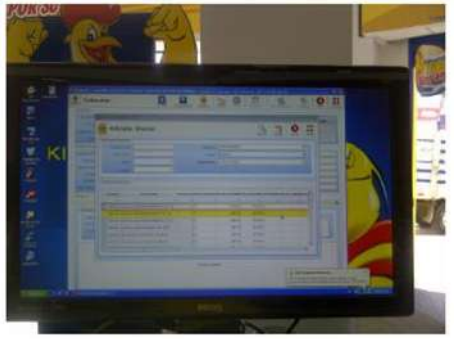
**Pilares de la Seguridad de Información**

# GESTIÓN DE SEGURIDAD DE INFORMACIÓN

CONFIDENCIALIDAD

Accesible a personal autorizado:

- Información de clientes.
- Contraseñas.
- Información impresa.



**Pilares de la Seguridad de Información**

# GESTIÓN DE SEGURIDAD DE INFORMACIÓN

DISPONIBILIDAD

Activos de información disponibles de forma organizada cuando sea requerida:

- Correos no deseados.
- Información en dispositivos externos.


Pilares de la Seguridad de Información

# GESTIÓN DE SEGURIDAD DE INFORMACIÓN

INTEGRIDAD

Información completa, exacta y válida:

- Correo electrónico.
- Expedientes de clientes.
- Información de cuentas, saldos.

Pilares de la Seguridad de Información

# GESTIÓN DE SEGURIDAD DE INFORMACIÓN

## Dominios de la Seguridad de la Información

### 1. Política y Organización de GSI

**Reglas aplicadas a las actividades relacionadas al manejo de información de una entidad.**

- Manual aprobado por el Directorio, incluyendo políticas de administración de sistemas, roles responsabilidades de la GSI, procedimientos y est[andares, etc.
- Revisión periódica.
- Conocimiento de todo el personal.
- Gestión de riesgos de SI alineada a RO.

**Organización de la Seguridad:**

- Asignación de la responsabilidad de GSI.
- Establecimiento de **acuerdos de confidencialidad.**
- Evaluación de riesgos de contratación y **acceso a la información por parte de terceros**, así como revisión de seguridad por terceros.

Ejemplos: Política de Administración de Sistemas, Roles y responsabilidades de GSI, etc.

# GESTIÓN DE SEGURIDAD DE INFORMACIÓN

## Dominios de la Seguridad de la Información


**2. Gestión de Activos y clasificación de información**

**Diseño, establecimiento e implementación de un proceso de mejora continua que permita la identificación, valoración, clasificación y tratamiento de los activos de información más importantes de la Compañía.**

- **Inventarios** de activos de información.
- Asignación de **responsabilidades** respecto a la protección de los activos de información.
- **Clasificación** de la información, **nivel de riesgo** existente para la empresa, y medidas apropiadas de **control** asociadas a las clasificaciones.

**3. Seguridad de Personal**

**Procedimientos relacionados al cumplimiento de las políticas de seguridad de acuerdo con la legislación laboral vigente.**

- Roles y responsabilidades sobre la SI. Concientización y entrenamiento.
- Procedimientos de **selección de personal** que incluyan la verificación de antecedentes.
- Procesos disciplinarios por incumplimiento de políticas de seguridad.
- Procedimientos por cese de personal (revocación de derechos de acceso, devolución de activos)

Ejemplo: Verificación de los antecedentes, perfiles y competencias del equipo de GSI.

# GESTIÓN DE SEGURIDAD DE INFORMACIÓN

## Dominios de la Seguridad de la Información

### 4. Seguridad Lógica


**Procedimientos y controles relacionados con la administración de derechos y perfiles de usuarios para el acceso a los sistemas de información.**

**Control de accesos:**

- Procedimientos para el alta, baja, suspensión o modificación de usuarios y perfiles.
- Revisiones periódicas sobre los derechos concedidos a los usuarios.
- Gestión de identificadores y contraseñas.
- Seguimiento sobre el acceso y uso de los sistemas.
- Controles especiales sobre usuarios remotos y computación móvil.

Ejemplo: Procedimientos de administración de accesos de usuarios a los sistemas.

# GESTIÓN DE SEGURIDAD DE INFORMACIÓN

## Dominios de la Seguridad de la Información


### 5. Seguridad Física y Ambiental

**Reglas relacionadas a los accesos físicos autorizados a los locales e información física.**

- Perímetro de seguridad física.
- Controles físicos de entrada e identificación.
- Seguridad de oficinas.
- Protección ante amenazas ambientales.
- Acceso al público, carga y descarga.
- Traslado de equipos.
- Seguridad del cableado.

Ejemplos: Procedimientos de acceso al centro de computo, medidas de seguridad de protección de la información, etc.

### 6. Seguridad de Operaciones y Comunicaciones

**Procedimientos relacionados al ambiente operativo de los sistemas de información y las instalaciones de procesamiento, así como los canales electrónicos entre los mismos.**

- Procedimientos documentados para la operación de los sistemas.
- Control sobre los cambios en el ambiente operativo.
- Separación de funciones para reducir el riesgo de error o fraude.
- Monitoreo del servicio dado por terceras partes.
- Protección contra código malicioso.
- Seguridad sobre el intercambio de la información.

Ejemplo: Procedimientos de control de cambios de la infraestructura tecnológica.

# GESTIÓN DE SEGURIDAD DE INFORMACIÓN

## Dominios de la Seguridad de la Información

**7. Seguridad en la Adquisición, Desarrollo y Mantenimiento de Sistemas**

**Procedimientos relacionados a la administración de la seguridad en la adquisición, desarrollo y mantenimiento de sistemas informáticos.**

- Controles sobre el ingreso de información, el procesamiento y la información de salida.
- Controles sobre la implementación de aplicaciones antes del ingreso a producción.
- Pruebas de usuarios.

Ejemplo: Aplicaciones de validación de integridad de data.

**8. Gestión de Incidentes**

**Procedimientos relacionados a los incidentes y vulnerabilidades de seguridad de información para que sean controlados de manera oportuna.**

- Procedimientos para el reporte de incidentes de SI y vulnerabilidades asociadas con los sistemas.
- Procedimientos para dar una respuesta adecuada a los incidentes y vulnerabilidades de seguridad reportadas.

Ejemplo: Procedimiento de reporte de incidentes de GSI.

# GESTIÓN DE SEGURIDAD DE INFORMACIÓN

## Dominios de la Seguridad de la Información


**9. Cumplimiento Normativo**

**Procedimientos relacionados a los requerimientos legales, contractuales o de regulación.**

- Asegurar que los requerimientos legales, contractuales o de regulación sean cumplidos, y cuando corresponda, incorporados en la lógica interna de las aplicaciones informáticas
- Derechos de propiedad intelectual
- Privacidad de datos

Ejemplo: Cumplimiento con las normas del regulador.

**10. Privacidad de la Información**

**Procedimientos relacionados a privacidad de la información que reciben de sus clientes y usuarios de servicios.**
Ejemplos: Protección de datos personales, sobre la confidencialidad de la información.

# GESTIÓN DE SEGURIDAD DE INFORMACIÓN

## Dominios de la Seguridad de la Información

**11. Gestión de Continuidad / Procedimiento de Respaldo**

**Procedimientos relacionados con la generación de copias de respaldo de información (backup), software base, aplicaciones, configuraciones, usuarios y bases de datos; administración de los medios magnéticos de respaldo, procedimiento de generación.**

- Procedimientos de respaldo regulares y periódicamente validados.
- Almacenamiento de la información de respaldo y los procedimientos de restauración en una ubicación a suficiente distancia.

Controles

# GESTIÓN DE SEGURIDAD DE INFORMACIÓN

**Cibercriminal ´hackea´ web del Banco Central de Europa y roba información.**

Un criminal cibernético, hackeó" la página web del Banco Central de Europa (BCE) y robó información de 20 mil direcciones electrónicas, exigiendo dinero a cambio de los datos.

Confirmando que la data sustraída no contenía información sensible sobre los mercados, el presidente del BCE, Mario Draghi, confirmó este jueves que su página web había sido pirateada.

El instituto emisor reveló que el robo salió a la luz después de recibir un e-mail anónimo que exigía una compensación económica por la información robada.

Como primera acción de prevención, el BCE se puso en contacto con las personas que pueden haberse visto afectadas por el robo y está cambiando todas las claves.

"La policía alemana fue informada y hemos dado los pasos necesarios para que una situación así no vuelva a repetirse", señala el banco en un correo electrónico.

Fuente: http://www.rpp.com.pe/2014-07-24-cibercriminal-hackea-web-del-banco-central-de-europa-y-roba-informacion-noticia_710620.html

# HERRAMIENTAS

# GESTIÓN DE RIESGO OPERACIONAL
# HERRAMIENTAS DE GESTIÓN

Para llevar a la práctica la gestión de riesgo operacional, las empresas deben apoyarse en un conjunto de herramientas que faciliten la identificación y recopilación de pérdidas operacionales, así como la evaluación, seguimiento, control y reporte de los riesgos a los que están expuestas:

# GESTIÓN DE RIESGO OPERACIONAL
# HERRAMIENTAS DE GESTIÓN

Enfoque cualitativo:

- Flujogramas de procesos.
- Mapas de riesgos.
- Auto evaluaciones.

Enfoque cuantitativo:

- Bases de datos.
- Modelos actuariales.
- Redes causales.

Enfoque mixto:

- Indicadores de riesgo.
- Alertas.
- Cuadros de mando (Balance scorecard).

# HERRAMIENTAS DE GESTIÓN
# FLUJOGRAMAS DE PROCESOS

Ilustra gráficamente, paso a paso, los procesos identificados en cada área de negocio junto con sus riesgos inherentes.

Se trata de graficar la secuencia de actividades recurrentes mediante las cuales se transforman un conjunto de entradas *(inputs)* en un conjunto de salidas *(outputs)*.

Representa las diferentes operaciones que componen un procedimiento en secuencia cronológica.

Respecto al riesgo operacional, su objetivo es identificar los puntos críticos de riesgo.

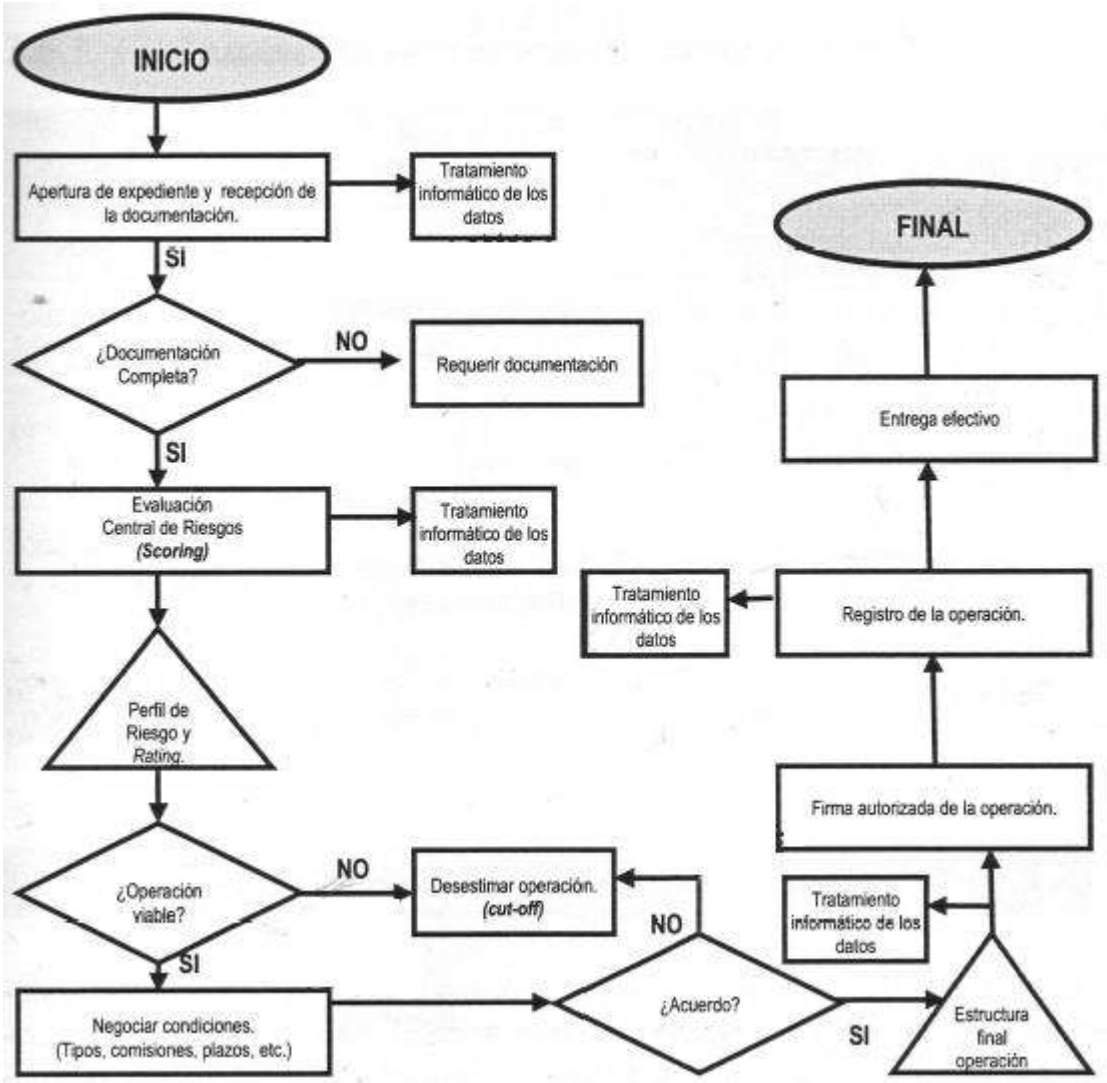
Deben ser:

- Sintéticos.
- Simbolizados.
- Esquemas visibles de un sistema o proceso.

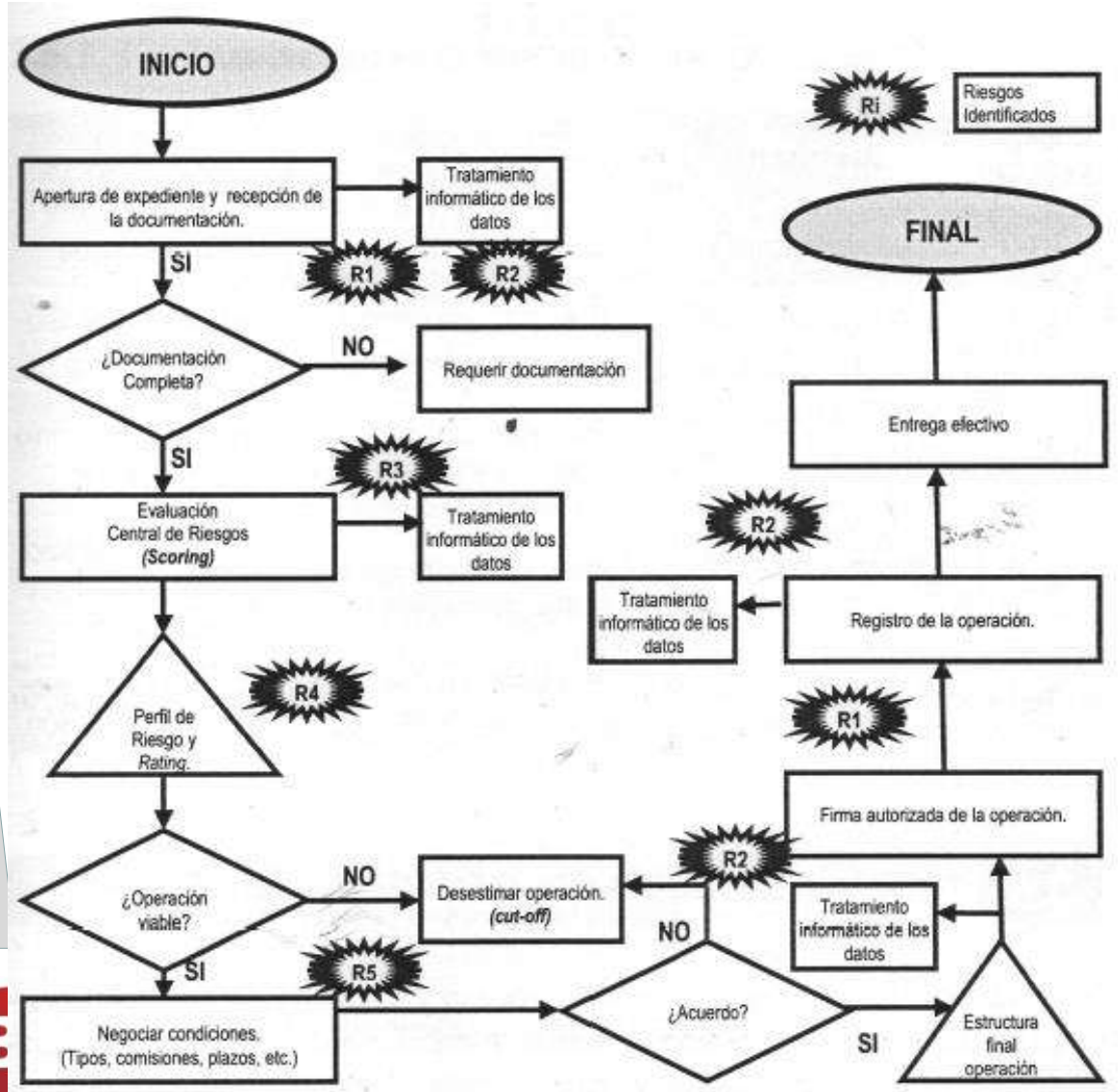
# HERRAMIENTAS DE GESTIÓN
# FLUJOGRAMAS DE PROCESOS

Ejercicio 1:

Revise el flujograma de procesos de estudio y concesión de un crédito bancario que se adjunta y determine que puntos de riesgo existen en el proceso.



# HERRAMIENTAS DE GESTIÓN
# FLUJOGRAMAS DE PROCESOS




| RIESGOS IDENTIFICADOS EN EL FLUJOGRAMA | |
|---|---|
| **EVENTO** | **DESCRIPCIÓN** |
| R1 | Falsificación. |
| R2 | Errores de introducción de datos. |
| R3 | Ausencia de investigación a cliente conforme a las políticas. |
| R4 | Comunicación defectuosa. |
| R5 | Prácticas inadecuadas de negociación. |

# HERRAMIENTAS DE GESTIÓN
# MAPEO DE RIESGO OPERACIONAL

Una vez identificados los puntos críticos del proceso y los factores potenciales de peligro, deben ser inventariados en el mapa de riesgos.
El mapa de riesgos nos permite de manera efectiva visualizar de manera rápida, global y comparativa, el grado de exposición al riesgo.
Los riesgos identificados son catalogados en base a su importancia relativa para el entidad, en términos de probabilidad de ocurrencia e importancia económica. Esto determinará el uso más eficiente de los recursos y la decisión respecto a su control.
Establecer criterios claros de valorización.

# HERRAMIENTAS DE GESTIÓN
# MAPEO DE RIESGO OPERACIONAL

Evaluando los riesgos:

- Estimar la amenaza o peligro. Cuantificar la frecuencia e impacto del riesgo.
- Evaluar la vulnerabilidad. Determinar la calidad de los controles establecidos.
- Estimar el riesgo asumido. Como resultado de relacionar la amenaza y el control.

| ESCALA DE PONDERACIÓN DE LA SEVERIDAD DE UN RIESGO – IMPACTO ECONÓMICO | | |
|---|---|---|
| **NIVEL** | **RANGOS** | **DESCRIPCIÓN – PÉRDIDA ECONÓMICA** |
| 5 | Catastrófico | Enorme |
| 4 | Alto | Mayor |
| 3 | Moderada | Media |
| 2 | Baja | Bajas |
| 1 | Insignificante | Mínimas |

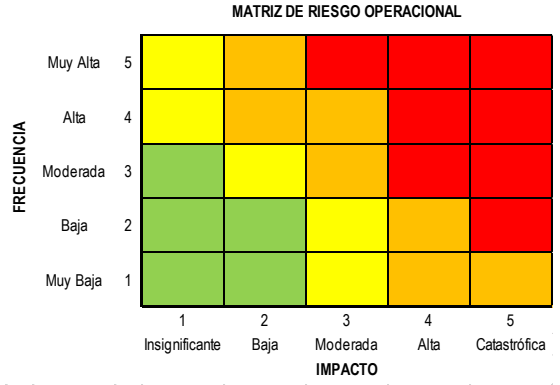
| ESCALA DE PONDERACIÓN DE LA FRECUENCIA DE UN RIESGO | | |
|---|---|---|
| **NIVEL** | **RANGOS** | **DESCRIPCIÓN** |
| 5 | Catastrófico | La expectativa de ocurrencia se da en todas las circunstancias |
| 4 | Alto | Probabilidad de ocurrencia en la mayoría de las circunstancias |
| 3 | Moderada | Puede ocurrir |
| 2 | Baja | Podría ocurrir algunas veces |
| 1 | Insignificante | Ocurre sólo bajo circunstancias excepcionales. |

# HERRAMIENTAS DE GESTIÓN
# MAPEO DE RIESGO OPERACIONAL

Riesgo inherente y riesgo residual.


Obtendremos una nueva clasificación de los riesgos a que resulta de la combinación de 3 factores: impacto económico, frecuencia y controles implantados.

| | |
|---|---|
| **Riesgo extremo** | **Requiere acción inmediata** |
| **Riesgo alto** | Requiere atención de la Alta Dirección |
| **Riesgo moderado** | Aceptable, debe ser controlado y monitoreado |
| **Riesgo bajo** | Gestionable con procedimientos de rutina |



# HERRAMIENTAS DE GESTIÓN
# MAPEO DE RIESGO OPERACIONAL

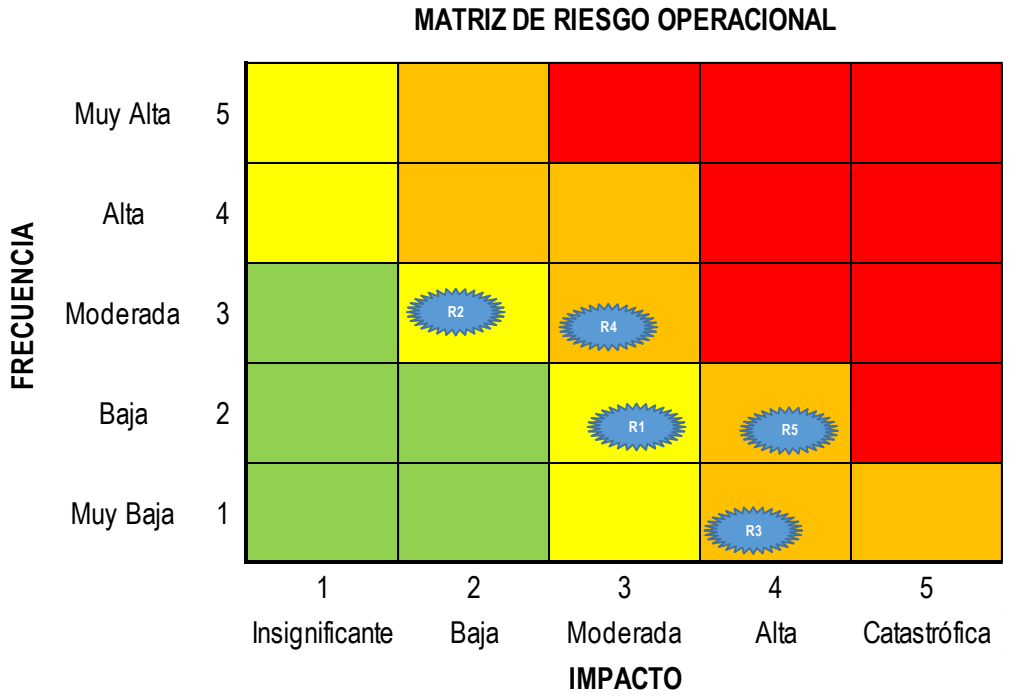
Ejercicio:

Asuma el impacto económico y la frecuencia que tendría en los riesgos que ha identificado en el ejercicio, luego grafique su matriz de riesgo.

| CLASIFICACIÓN DEL RIESGO RESIDUAL | | | | |
|---|---|---|---|---|
| **EVENTO** | **DESCRIPCIÓN** | **IMPACTO (1-5)** | **FRECUENCIA (1-5)** | **RIESGO** |
| R1 | Falsificación. | 3 | 2 | MODERADO |
| R2 | Errores de introducción de datos. | 2 | 3 | MODERADO |
| R3 | Ausencia de investigación a cliente conforme a las políticas. | 4 | 1 | ALTO |
| R4 | Comunicación defectuosa. | 3 | 3 | ALTO |
| R5 | Prácticas inadecuadas de negociación. | 4 | 2 | ALTO |

# HERRAMIENTAS DE GESTIÓN
# MAPEO DE RIESGO OPERACIONAL

| CLASIFICACIÓN DEL RIESGO RESIDUAL | | | | |
|---|---|---|---|---|
| **EVENTO** | **DESCRIPCIÓN** | **IMPACTO (1-5)** | **FRECUENCIA (1-5)** | **RIESGO** |
| R1 | Falsificación. | 3 | 2 | MODERADO |
| R2 | Errores de introducción de datos. | 2 | 3 | MODERADO |
| R3 | Ausencia de investigación a cliente conforme a las políticas. | 4 | 1 | ALTO |
| R4 | Comunicación defectuosa. | 3 | 3 | ALTO |
| R5 | Prácticas inadecuadas de negociación. | 4 | 2 | ALTO |



# HERRAMIENTAS DE GESTIÓN
# MAPEO DE RIESGO OPERACIONAL

Mapa de Riesgo Operacional.

Los factores identificados deben ser agregados por categoría de riesgo operacional.

Propuesta de clasificación del riesgo operacional agregado:

- Riesgo Alto. Más del 25% de factores de riesgo alto.
- Riesgo Medio-Alto. Más del 25% de factores clasificados entre riesgo alto y medio-alto.
- Riesgo Medio. Más del 50% de factores clasificados entre riesgo alto, medio-alto y medio.
- Riesgo Bajo. Cuando no se ha cumplido con ninguna de las condiciones anteriores.

# HERRAMIENTAS DE GESTIÓN
# MAPEO DE RIESGO OPERACIONAL

## Mapa de Riesgo Operacional.

| Área Organizativa | TIPO DE RIESGO | | | | | | |
|---|---|---|---|---|---|---|---|
| | Fraude Interno | Fraude Externo | Relaciones laborales y seguridad laboral | Cliente, productos y prácticas comerciales | Daños a Activos Materiales | Interrupción de operaciones y fallos de sistemas | Ejecución, entrega y gestión de procesos |
| Área 1 | | | | | | | |
| Área 2 | | | | | | | |
| … | | | | | | | |
| Área n | | | | | | | |

# HERRAMIENTAS DE GESTIÓN
# AUTO-EVALUACIONES (SELF ASSESSMENT)

Proceso por el cual las unidades de negocio y de soporte, de forma subjetiva, identifican los riesgos inherentes a sus actividades, evalúan el nivel de control existente y determinan los puntos de mejora que deben realizarse.

Entonces, la actividad consiste en:

- Identificar los riesgos asociados a la actividad: Riesgo Inherente.
- Identificar los controles existentes y el Riesgo Residual.
- Evaluar su probabilidad e impacto.
- Establecer Planes de Acción para la mitigación de los riesgos.

# HERRAMIENTAS DE GESTIÓN
# AUTO-EVALUACIONES (SELF ASSESSMENT)

TIPOS DE AUTOEVALUACIÓN:

- Cuestionarios (encuestas, entrevistas, check list).
- Descripción de objetivos.
- Talleres (Workshops).
- Análisis de la Gerencia.

# HERRAMIENTAS DE GESTIÓN
# AUTO-EVALUACIONES (SELF ASSESSMENT)

Proceso de evaluación de los puntos de control.

| RANGO DE PONDERACIÓN DE LOS PUNTOS DE CONTROL | | |
|---|---|---|
| **CALIFICACIÓN** | **CRITICIDAD** | **MEDIDAS DE CONTROL** |
| 1 | Muy Baja | Opcionales |
| 2 | Baja | Deseables |
| 3 | Moderada | Convenientes |
| 4 | Alta | Necesarias |
| 5 | Extrema | Imprescindibles |

| RANGO DE CALIFICACIONES CUALITATIVAS | | |
|---|---|---|
| **CALIFICACIÓN** | **INTERVALO (%)** | **ADECUACIÓN** |
| A | 81 – 100 | Óptima |
| B | 61 – 80 | Buena |
| C | 41 – 60 | Adecuada |
| D | 21 – 40 | Deficiente |
| E | 0 - 20 | Muy deficiente |

# HERRAMIENTAS DE GESTIÓN
# AUTO-EVALUACIONES (SELF ASSESSMENT)

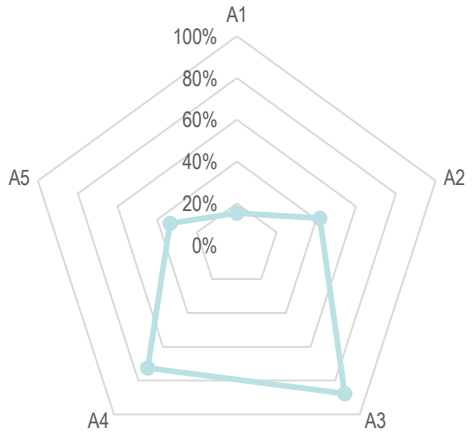
## Proceso de evaluación de los puntos de control.

| AUTO-EVALUACIÓN DEL ÁREA DE SERVICIO TÉCNICO | | | | |
|---|---|---|---|---|
| PUNTOS DE CONTROL | PONDERACIÓN (P) | ADECUACIÓN RATING | ADECUACIÓN % | (P) * % |
| PC-1 ¿Se dispone de sistemas informáticos que gestionen de manera centralizada todas las solicitudes de servicio? | 4 | 1 | 25.0% | 1.0000 |
| PC-2 ¿Se dispone de un teléfono de asistencia 24 horas? | 3 | 3 | 75.0% | 2.2500 |
| PC-3 ¿Hay establecido un control de calidad que evalúe el servicio de asistencia? | 4 | 4 | 100.0% | 4.0000 |
| PC-4 ¿Se realizan revisiones peródicas del estado de conservación y utilidad del inventario inmovilizado? | 3 | 1 | 25.0% | 0.7500 |
| PC-5 ¿Se tiene establecido un servicio de mantenimiento integral para edificios declarados como patrimonio histórico o artístico? | 1 | 4 | 100.0% | 1.0000 |
| PC-6 ¿Se ha realizado un análisis sobre la capacidad de respuesta o servicio de la entidad en una situación crítica? | 5 | 0 | 0.0% | 0.0000 |
| PC-7 ¿Hay implantado un sistema de control que alerte del vencimiento de las revisiones? | 5 | 1 | 25.0% | 1.2500 |
| PC-8 ¿Se responsabiliza esta área de la revisión periódica? | 2 | 2 | 50.0% | 1.0000 |
| Total Ponderación | 27 | | | 11.2500 |
| GRADO DE DECUACIÓN DEL ÁREA | 41.7% | | | |

# HERRAMIENTAS DE GESTIÓN
# AUTO-EVALUACIONES (SELF ASSESSMENT)

## Proceso de evaluación de los puntos de control.

| EJEMPLO DE CALIFICACIONES CUALITATIVAS | | | |
|---|---|---|---|
| **CÓDIGO ÁREA** | **ÁREA** | **ADECUACIÓN** | **CALIFICACIÓN** |
| A1 | Marketing | 15.34% | Muy Deficiente (E) |
| A2 | Servicio Técnico | 41.70% | Adecuada (C) |
| A3 | Legal | 87.80% | Óptima (A) |
| A4 | Medios de Pago | 72.67% | Buena (B) |
| A5 | Tesorería | 33.65% | Deficiente (D) |



# HERRAMIENTAS DE GESTIÓN
# AUTO-EVALUACIONES (SELF ASSESSMENT)

VENTAJAS DE LA AUTOEVALUACIÓN:

- Los propios empleados (expertos) evalúan sus procesos y controles.
- La unidad de riesgos trabaja como facilitador.
- Ayuda a identificar controles “suaves” o poco eficientes.
- Mejor aceptación por los usuarios (participativo).
- Mejora el ambiente de control de la organización.
- Estimula el trabajo en equipo.

DESVENTAJAS DE LA AUTOEVALUACIÓN:

# HERRAMIENTAS DE GESTIÓN
# INDICADORES DE RIESGO

- Los controles internos efectivos dan a los ejecutivos la confianza de que el negocio funciona apropiadamente sin su supervisión constante y que pueden firmar diversas certificaciones y declaraciones de cumplimiento regulatorio con un mayor nivel de confianza.
- Un entorno de control interno efectivo, incluyendo un proceso para identificar y remediar los problemas potenciales, fortalece la confianza de los ejecutivos clave de que la organización presentará informes financieros correctos y oportunos.

# HERRAMIENTAS DE GESTIÓN
# INDICADORES DE RIESGO

Alertan de situaciones delicadas cuando se alcanzan determinados umbrales preestablecidos.

Por tanto, su objetivo es contrastar, periódicamente, el perfil de riesgo de la entidad.

Son:

*"Variables cuantitativas o cualitativas, determinadas en base a información histórica, que reflejan de manera específica la criticidad de un determinado factor de riesgo y, en su conjunto, el perfil de riesgo de la entidad".*

# HERRAMIENTAS DE GESTIÓN
# INDICADORES DE RIESGO

CENTRO DE ESTUDIOS BURSÁTILES

Modelo de indicadores óptimo: claramente definidos los objetivos a ser alcanzados.

Requisitos que deben cumplir los Indicadores de Riesgo:

- Ser parte de un sistema integral de gestión de riesgos.
- Reflejar el riesgo de cada proceso.
- Mostrar flexibilidad y capacidad de adaptación a las necesidades de cada unidad de la organización.
- Estar enlazados a las diferentes herramientas que forman parte del sistema de gestión del RO (auto-evaluaciones o BD de eventos de pérdida), a fin de analizar incoherencias entre los resultados.
- Proporcionar información agregada a nivel de entidad o de cada área en particular.
- Tener capacidad predictiva de eventos.

BOLSA DE VALORES DE LIMA BVL

# HERRAMIENTAS DE GESTIÓN
# INDICADORES DE RIESGO



Requisitos que deben cumplir los Indicadores de Riesgo:

- Ser parte de un sistema de información dinámico, ágil e interactivo, de manera que al sobrepasar los umbrales o niveles de criticidad, requieran de una respuesta adecuada y aporten información sin necesidad de una acción inmediata.
- Interrelacionar los riesgos inherentes con las diferentes líneas de negocio.

# HERRAMIENTAS DE GESTIÓN
# INDICADORES DE RIESGO



Deben ser (características):

- Relevantes: deben proporcionar información oportuna y significativa.
- No redundantes: si dos indicadores presentan una alta correlación, solamente uno debe ser considerado.
- Objetivos: El valor del indicador no puede depender de interpretaciones subjetivas.
- Simples: El indicador no debe ser demasiado amplio y costoso, para que pueda reflejar los cambios y actualizarse con facilidad.
- Verificables: Debe fundamentarse en aspectos que puedan ser contrastados.

# HERRAMIENTAS DE GESTIÓN
# INDICADORES DE RIESGO

CENTRO DE ESTUDIOS BURSÁTILES

Tipos de indicadores de riesgo (Scandizzo, 2005).

- Indicadores descriptivos de riesgo (KRI, *key risk indicators*): Cuantifican el nivel de riesgo de la entidad. Se configuran en función del grado de relevancia y representatividad a partir de los indicadores de rendimiento y de control.
- Indicadores de volumen (KPI, *key performance indicators*): Controlan la eficacia operativa y activa; alertan si su valor se mueve fuera del ámbito establecido. Estas variables informan sobre aspectos clave de la dimensión de la actividad: tamaño, volumen, importes, etc., que de uno u otro modo, tienen una relación directa con eventos de pérdida de tipo operacional.
- Indicadores clave de control (KCI, *key control indicators*): Reflejan la efectividad de los controles: número de autorizaciones, de confirmaciones pendientes, etc.

BOLSA DE VALORES DE LIMA BVL

# HERRAMIENTAS DE GESTIÓN
# INDICADORES DE RIESGO

CENTRO DE ESTUDIOS BURSÁTILES

Otra clasificación de indicadores de riesgo (Hoffman, 2002).

- Indicadores por clase:
  i. De información o de exposición;
  ii. Indicadores de control;
  iii. Indicadores básicos, que forman parte de indicadores índice o cesta; y,
  iv. Indicadores específicos de un factor de riesgo.
- Indicadores por tipo de riesgo: hace referencia al mapa de indicadores desglosándolo para cada factor de riego operacional.
- Indicadores genéricos de la entidad y los específicos de cada línea de negocio: Los indicadores de negocio son medidas de riesgo específicas para cada área que, interrelacionados con los de otras áreas, conforman indicadores a nivel agregado para la entidad.

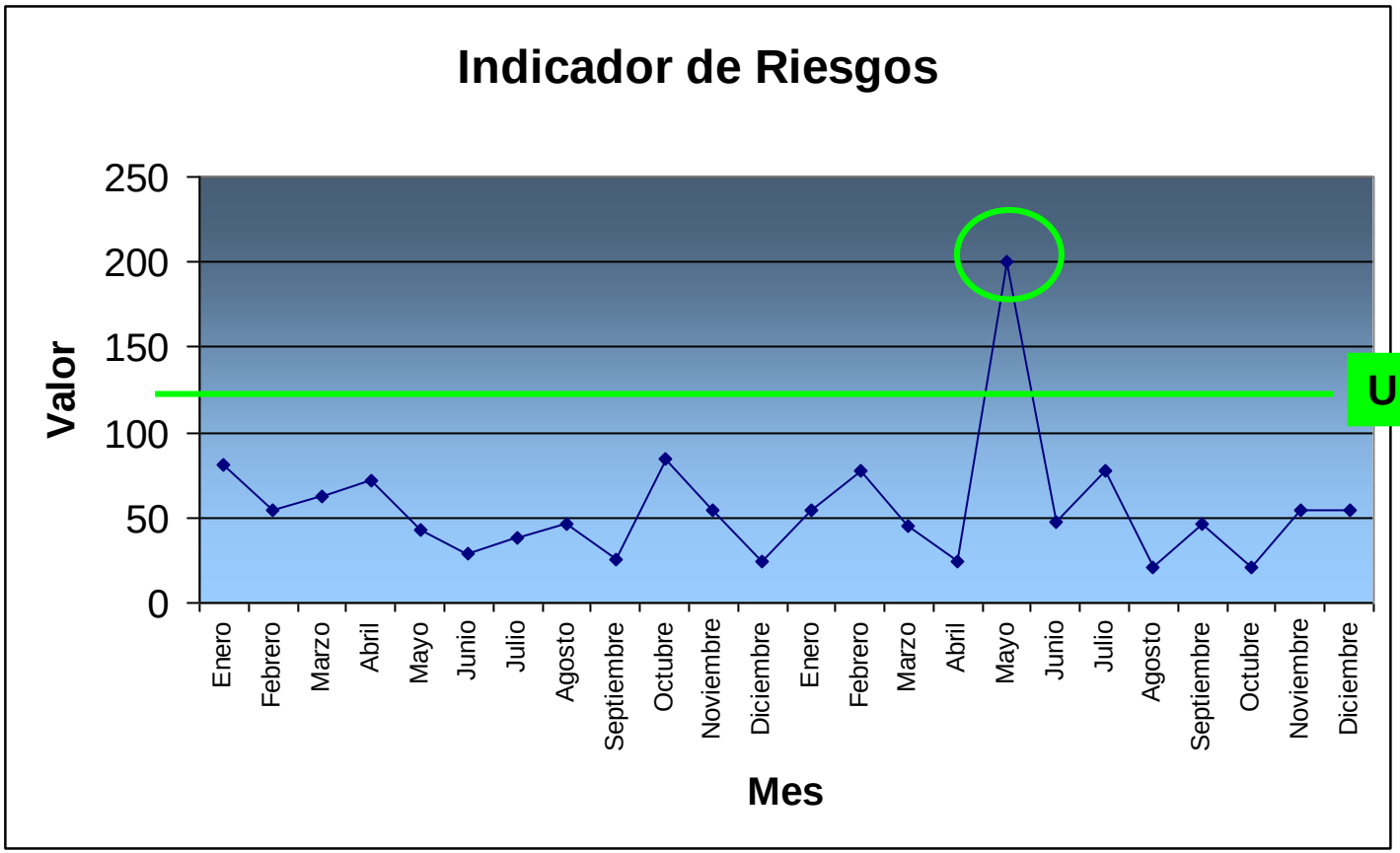
BOLSA DE VALORES DE LIMA BVL

# HERRAMIENTAS DE GESTIÓN
# INDICADORES DE RIESGO

| Área de Negocio o de Soporte | Causa del Riesgo | Tipo de Riesgo | Indicador |
|---|---|---|---|
| Banca Minorista | Acceso no autorizado a cuentas | Hurto y fraude | Número de bloqueos de operaciones de acceso al servicio de Banca On-line. |
| Banca Minorista | Acceso no autorizado a cuentas | Seguridad de los sistemas | Número de accesos al portal de Internet bloqueados. |
| Banca Minorista | Potenciales actividades fraudulentas | Actividades no autorizadas | Número de operaciones de activo donde se han detectado más de 3 modificaciones de los datos introducidos en los sistemas de calificación crediticia en un período. |
| Medios de Pago | Errores en la ejecución de tareas | Sistemas | Porcentaje de cajeros que presentan descuadres o incidencias en la realización de los arqueos, sobre el total de los cajeros. |
| Operaciones | Publicación errónea de datos | Gestión de cuentas de clientes | Número de reclamos originados por comunicaciones incorrectas de estatus de mora de clientes. |
| Tesorería | Incumplimiento de límites / Fallos de modelo | Actividades no autorizadas | Número de veces que se han superado los límites establecidos por el área para posiciones abiertas de divisas. |
| Recursos Humanos | Pérdidas de oportunidades por carecer de los recursos necesarios | Relaciones laborales | Tiempo medio de espera que tarda en cubrirse un puesto. |
| Internacional | Ineficiencia en la gestión del proceso | Recepción, ejecución y mantenimiento de operaciones | Porcentaje de envío de mensajes SWIFT manuales respecto al total de los envíos. |

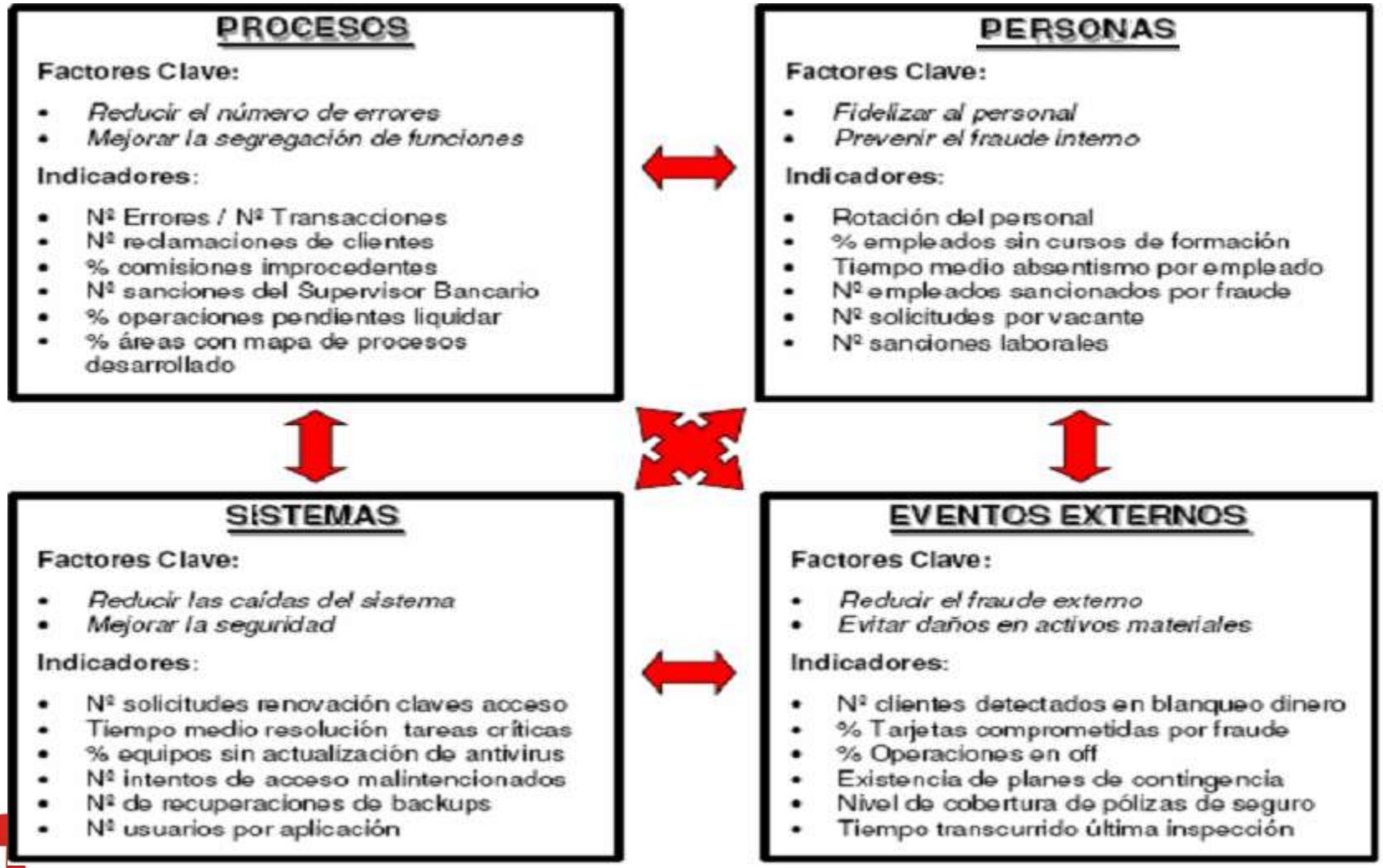
# HERRAMIENTAS DE GESTIÓN
# INDICADORES DE RIESGO

CENTRO DE ESTUDIOS BURSÁTILES




BOLSA DE VALORES DE LIMA BVL

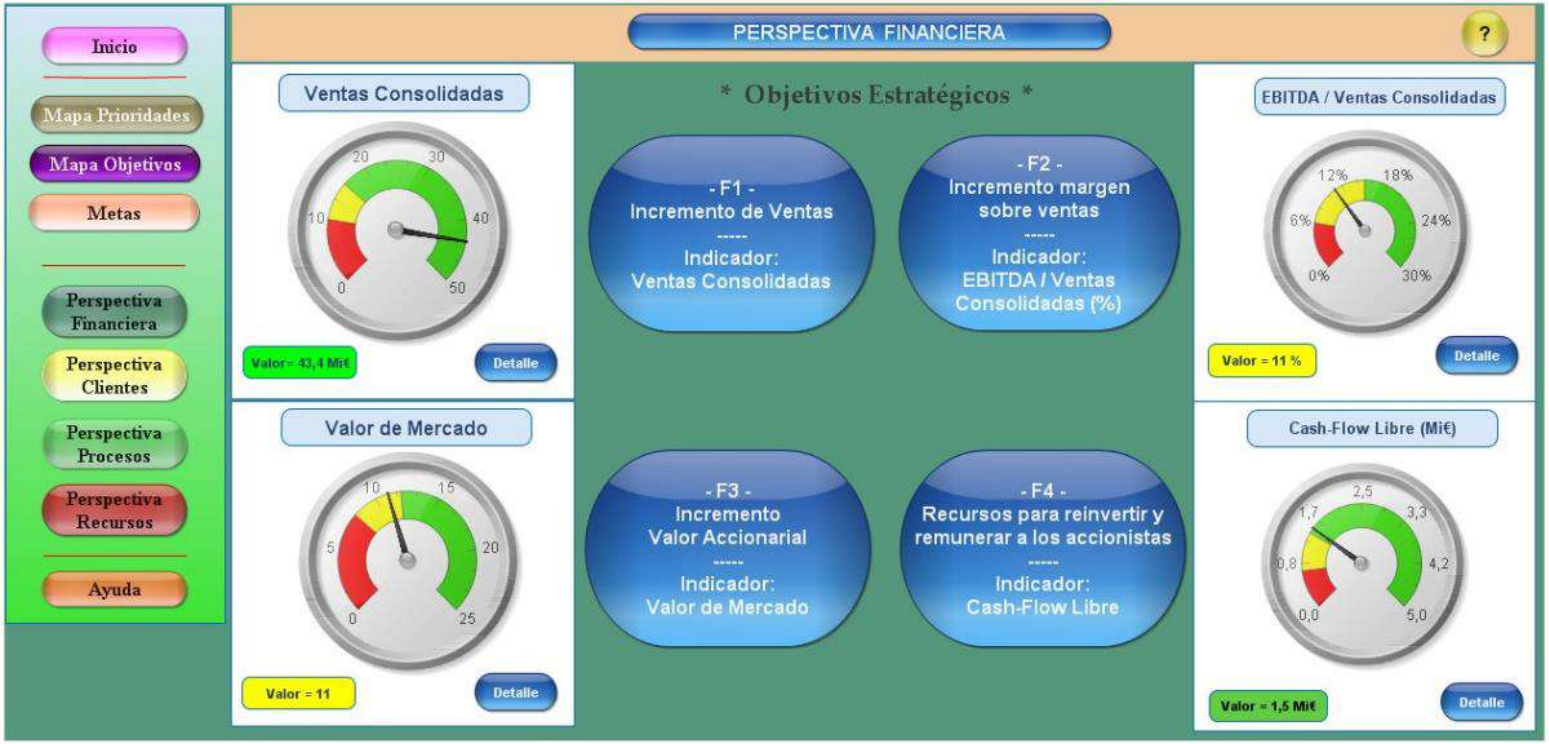
# HERRAMIENTAS DE GESTIÓN
# INDICADORES DE RIESGO



# HERRAMIENTAS DE GESTIÓN
# CUADROS DE MANDO (BALANCE SCORECARD)

Recoge el conjunto de indicadores establecidos por la entidad. Es el conjunto de indicadores cuyo seguimiento periódico permitirá delimitar con un mayor grado de conocimiento de la situación de la empresa.

El cuadro de mando debe presentar sólo la información que resulte ser imprescindible de una forma sinóptica y resumida.



# Gestión Integral de Riesgos
# Noviembre 2016

Econ. Alejandro Bazo Bertrán, MSc
bazo.alejandro@gmail.com
http://alejandrobazo.blogspot.pe/

# EVENTOS DE PÉRDIDA - CONCEPTOS

**Evento de riesgo operacional.**

Es un suceso o series de sucesos derivados de los factores de riesgo operacional originados por la(s) misma(s) causa(s), que ocurren durante un periodo de tiempo, afectando el curso normal de los procesos de la entidad.

**Evento de pérdida por riesgo operacional.**

Todo evento que genero un impacto negativo en el estado de resultados o en el patrimonio de la entidad cuyo origen se deriva de un evento de riesgo operacional.

# EVENTOS DE PÉRDIDA - CONCEPTOS

**Cuasi Pérdidas (near-misses).**

Evento de riesgo operacional que debiera materializarse como evento de pérdida, sin embargo, la pérdida no se produce debido a una situación fortuita distinta del control.

**Ingreso no percibido.**

Ingreso real que la entidad deja de percibir por la ocurrencia de un evento de riesgo operacional, cuando la transacción se ejecutó. Por ejemplo, comisiones no cobradas a los clientes por algún evento de riesgo operacional. En algunas entidades es denominado "costo de oportunidad financiero".

# EVENTOS DE PÉRDIDA - CONCEPTOS

**Lucro Cesante.**

Ingreso susceptible de estimación que la entidad deja de percibir por la ocurrencia de un evento de riesgo operacional, es decir, no se ejecuta la transacción. Por ejemplo, ventas no realizada por caídas de sistemas o fallas en el sistema eléctrico.

**Concesión Comercial.**

Salidas monetarias asumidas por estrategia comercial propia de la entidad en función a un análisis costo beneficio. Si bien la salida monetaria representa una pérdida, debido a que no existe un ingreso previo, esta no se deriva de un evento de riesgo operacional. Es una “decisión comercial”.

# CASO ALLIED IRISH BANK

# CASO ALLIED IRISH BANK

- ¿Cuál fue el problema en esta organización?
- ¿Qué clase de riesgos no fueron apropiadamente controlados?
- Describa y discuta cada uno de los riesgos que no fueron controlados y qué controles hubiera usted establecido

**Haga la lectura del caso y después responda estas preguntas**

# CASO ALLIED IRISH BANK

En 2002, el operador de divisas estadounidense John Rusnak, empleado del Allied Irish Bank (AIB), fue acusado de falsificar documentos para encubrir malas inversiones.
El banco dijo que, como resultado, perdió USD.750'MM.
La fiscalía dijo que Rusnak no se benefició personalmente de las pérdidas, que fueron en su mayoría en transacciones entre el dólar estadounidense y el yen japonés. El yen había bajado durante los últimos meses del año 2001 y aparentemente esperaba un cambio y que volviera a subir contra el euro pero no fue así, sino al contrario.
Él le confesó al FBI que sus deudas se acumularon mientras trataba de concebir una táctica para recuperar el dinero perdido sin tener que admitir a sus jefes el problema inicial.
El reporte Ludwig concluyó que sistemáticamente falsificó registros bancarios y documentos y había evadido débiles controles existentes en la tesorería de Allfirst y de la matriz. Opciones no existentes con ganancia ficticias (ocultar pérdidas de 1997). En 1999 pudo corregir parcialmente la pérdida
En 2003, fue sentenciado a 7.5 años.

# CASO ALLIED IRISH BANK

**Debilidades de control:**

- Las personas de la tesorería eran inexpertos y a Rusnak se le facilitó maniobrar el desvió de las pérdidas.
- La empresa no tenía una comunicación apropiada entre el front y el back office lo cual daba pie para que las transacciones que este efectuaba no llegaran con la misma información de un área a otra.
- En cuanto a las debilidades tecnológicas el FBI determinó que el programa que se utilizaba para la verificación de la validez de las transacciones era obsoleto (hasta físicamente podían autorizar los movimientos).

# CASO ALLIED IRISH BANK

**Responsables:**

- El FBI concluyó que nadie conspiró, a sabiendas, con Rusnak, sino que debido a la facilidad de poder perpetrar las transacciones no se pudo detectar que estas eran fraudulentas.
- Sin embargo, 6 personas de la administración fueron despedidas de Allfirst.
- El rol que desempeñaron los sistemas fue determinante para realizar un fraude.
- El conjunto de programas utilizado por Allied Irish permitía el control del front office y el back office permitiéndole a Rusnak tomar el control sobre el medio para unir las dos partes y así poder figurar y falsificar la aceptación de hacer una transacción.

**Los sistemas pudieron impedir el fraude:**

- Se confió en el trader, pero esto no era suficiente, si hubiera existido un programa que determinara la seguridad de las transacciones Rusnak no habría podido cometer el fraude y/o habría sido detectado a tiempo

# CASO ALLIED IRISH BANK

**Lecciones Aprendidas:**

- Falta de claridad en las líneas de reporte, inadecuada supervisión de los empleados y falta de controles por parte de la matriz.
- Es necesaria una estructura sólida de administracíón de riesgos.
- La relación entre la matriz y las subsidiarias debe ser clara.
- Enérgicos controles a las áreas de apoyo son esenciales para evitar omisiones o complacencias a saltarse procedimientos.

**¿Qué haría para diseñar los nuevos sistemas de control?**

# CASO ALLIED IRISH BANK

| Riesgo Operacional | | | | Riesgo de Mercado | |
|---|---|---|---|---|---|
| *Situación* | *Riesgo Identificado* | | | *Situación* | *Riesgo Identificado* |
| Falsificar registros bancarios y documentos | Fraude | Opciones a un día con amplios márgenes no eran ejercidas y nadie se dio cuenta | Falta de conocimiento / habilidades y fallas en los controles | Tomar posiciones de Tipo de Cambio | Tipo de Cambio |
| Evadir los controles existentes en la tesorería | Fallas en los procesos | Persuadir a las áreas de apoyo para evitar controles | Fraude, falta de conocimiento / habilidades y fallas en los procesos | | |
| No preparar reportes de opciones a un día | Fallas en los procesos | No seguir procedimientos para validar | Fallas en los procesos | **Otros Riesgos** | |
| Activos falsos fueron registrados en los libros | Fallas en los procesos | | | *Situación* | *Riesgo Identificado* |
| | | | | El caso se volvió de dominio público | Reputacional |

AIB Allied Irish Bank (GB)


# Medición del riesgo

# RIESGO ESTRATÉGICO

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.

## Etapas en la gestión del riesgo estratégico

- Entendimiento de los objetivos estratégicos: Cuáles; Indicadores de gestión; Apetito y tolerancia;
- Identificación del riesgo estratégico: riesgos asociados a los objetivos del plan:

| Factores Externos | Factores Internos |
|---|---|
| Financieros - Económico | Infraestructura |
| Producto-Mercado | Personal |
| Medioambientales | Procesos |
| Políticos | Operaciones |
| Sociales | Tecnología |
| Tecnológicos | |

Responsabilidad Social / Gobierno Corporativo

Alineación de cada riesgo identificado con el correspondiente objetivo estratégico

Alineación de cada riesgo estratégico identificado con productos, servicios, TI, proveedores, etc., y elaborar un mapa de riesgos estratégicos

## Etapas en la gestión del riesgo estratégico

- Cuantificación y evaluación del riesgo estratégico: evaluación de los riesgos estratégicos relacionando frecuencia con exposición.
- Tratamiento del riesgo estratégico: evitar, reducir, mitigar, aceptar, transferir.
- Monitoreo del riesgo estratégico.
- Reporte del riesgo estratégico.

# ¿Cuál es tu posesión más valiosa?

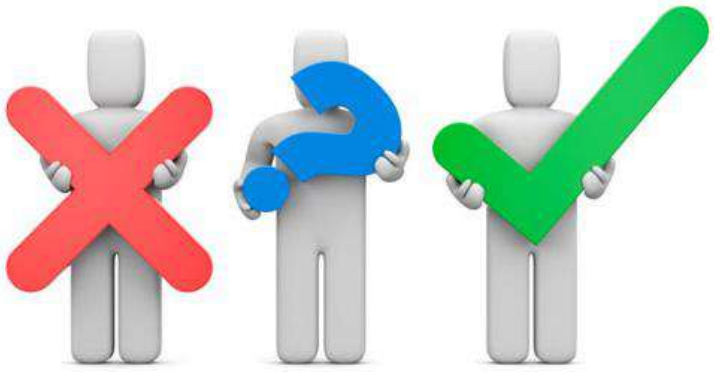
¿Tu casa?

¿Tu auto?

¿Tus inversiones?

Más cerca …
¿Tu familia?

¿Un recuerdo inolvidable?

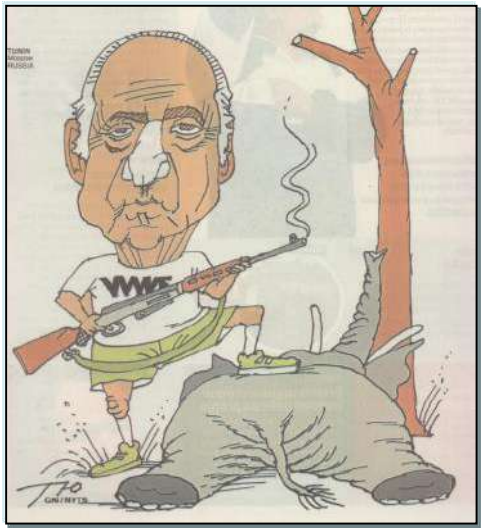


Tu reputación !!!

# RIESGO REPUTACIONAL

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.

- No debemos confundirlo con la imagen de la empresa, la cual se puede fabricar.
- En ocasiones, se puede ver afectado por acciones de terceros, a partir de debilidades existentes o inventadas.
- Es transversal a todos los otros riesgos.

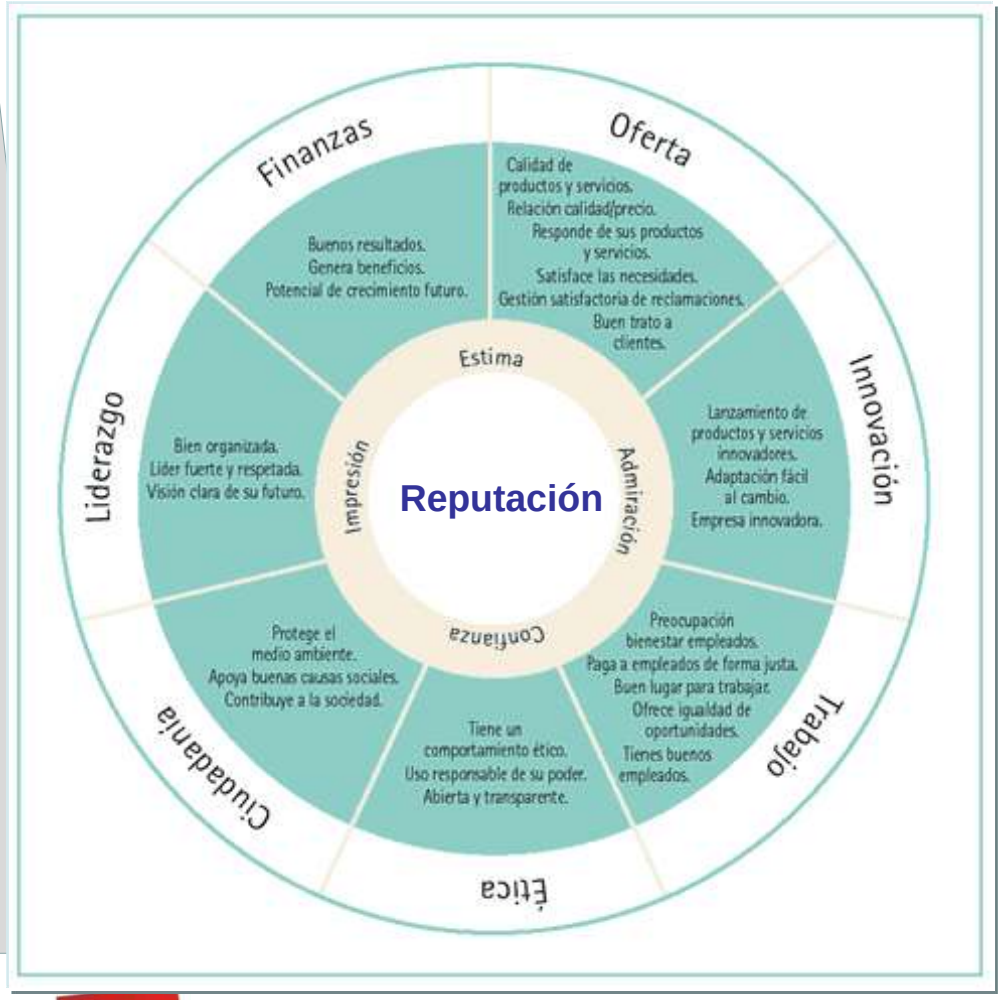



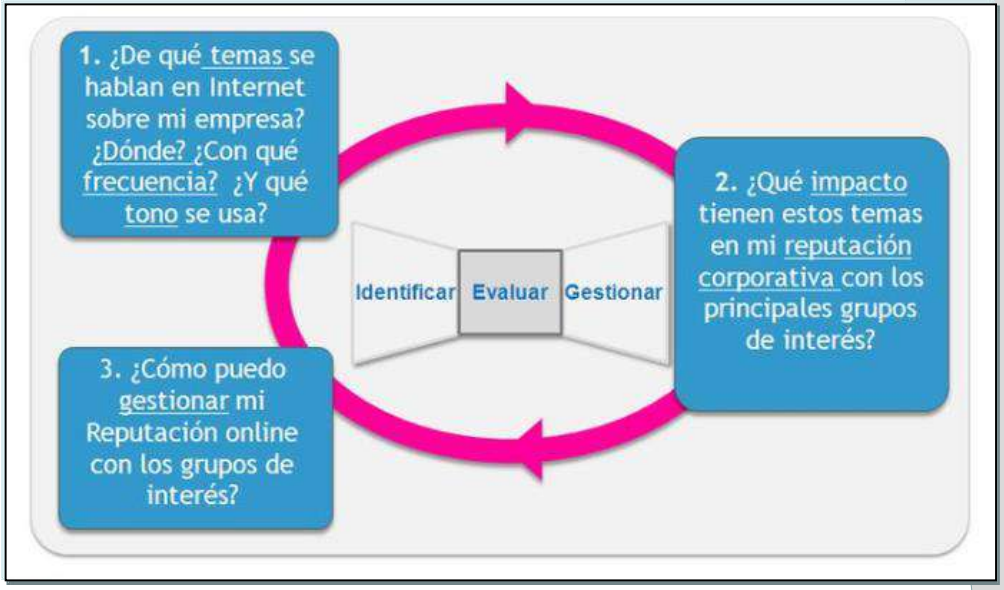

Fuente: El Comercio, Suplemento Internacional, 22/Abr/2012

# RIESGO REPUTACIONAL

- Identificar las potenciales fuentes de riesgo reputacional: identificar las fallas internas y débiles capacidades de respuesta escenarios externos adversos.
- La medición de riesgo reputacional puede ser la más complicada y subjetiva de todas ¿Cómo lo calculamos?
- Para gestionar este riesgo lo más eficaz es el tratamiento preventivo: reforzamiento de la GIR:
  - Integrar a la organización: capacitación y alertas.
  - Autoevaluciones de gobierno corporativo.
  - Evaluar la reputación de la compañía desde el punto de vista de los *stakeholders* – "percepción es realidad".
  - Gestión apropiada de escenarios de crisis.
  - Gestión apropiada de atención a ususarios y clientes.
  - Cumplimiento normativo: evitar sanciones regulatorias.

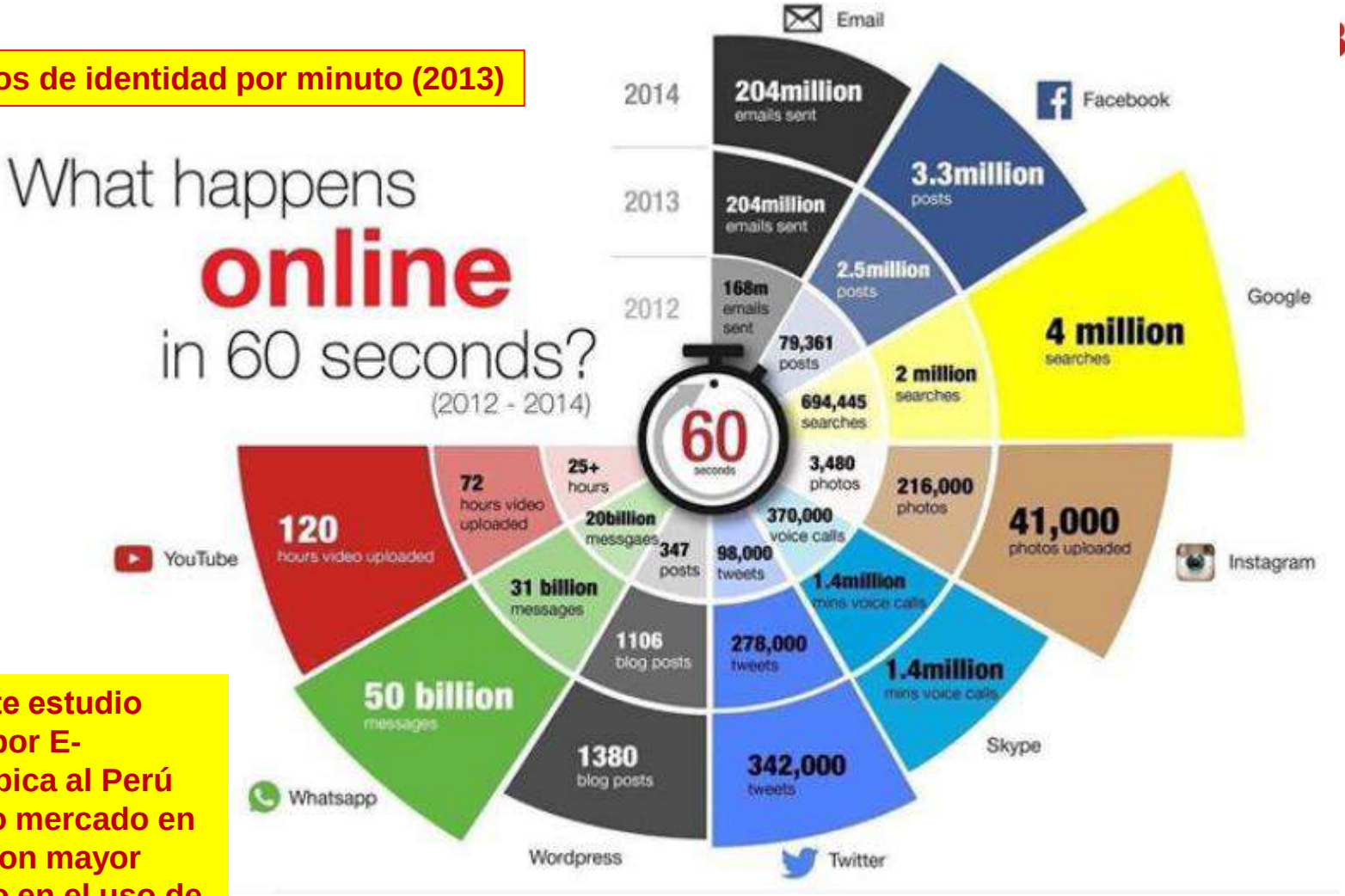
# RIESGO REPUTACIONAL




Pérdida de oportunidades de negocio atribuibles al desprestigio de una institución

**20 robos de identidad por minuto (2013)**




**"Un reciente estudio publicado por E-marketer ubica al Perú es el quinto mercado en el mundo con mayor crecimiento en el uso de Internet y con una penetración de Internet móvil de 61%".**
Fuente. Semana Económica, Pág. 26, 26/Feb/2016

RIESGO REPUTACIONAL

# RIESGO DE CRÉDITO

Es el más antiguo y probablement e el más importante

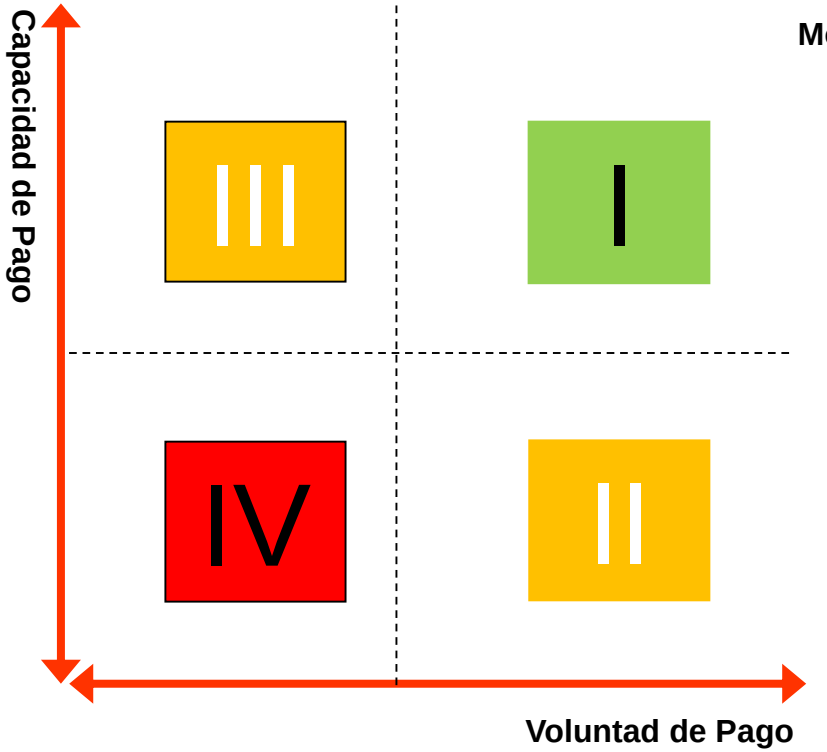
Pérdida potencial por incumplimient o de contraparte

Deterioro de la calidad crediticia de la contraparte

La posibilidad de pérdidas por la incapacidad o falta de voluntad de los deudores, contrapartes, o terceros obligados, para cumplir sus obligaciones contractuales registradas dentro o fuera del balance.

Riesgo de concentración. Parte del riesgo de crédito, se produce por la falta de diversificación de la cartera de créditos.
Puede producirse por número y exposición, sectorial, geográfico, etc.

# RIESGO DE CRÉDITO

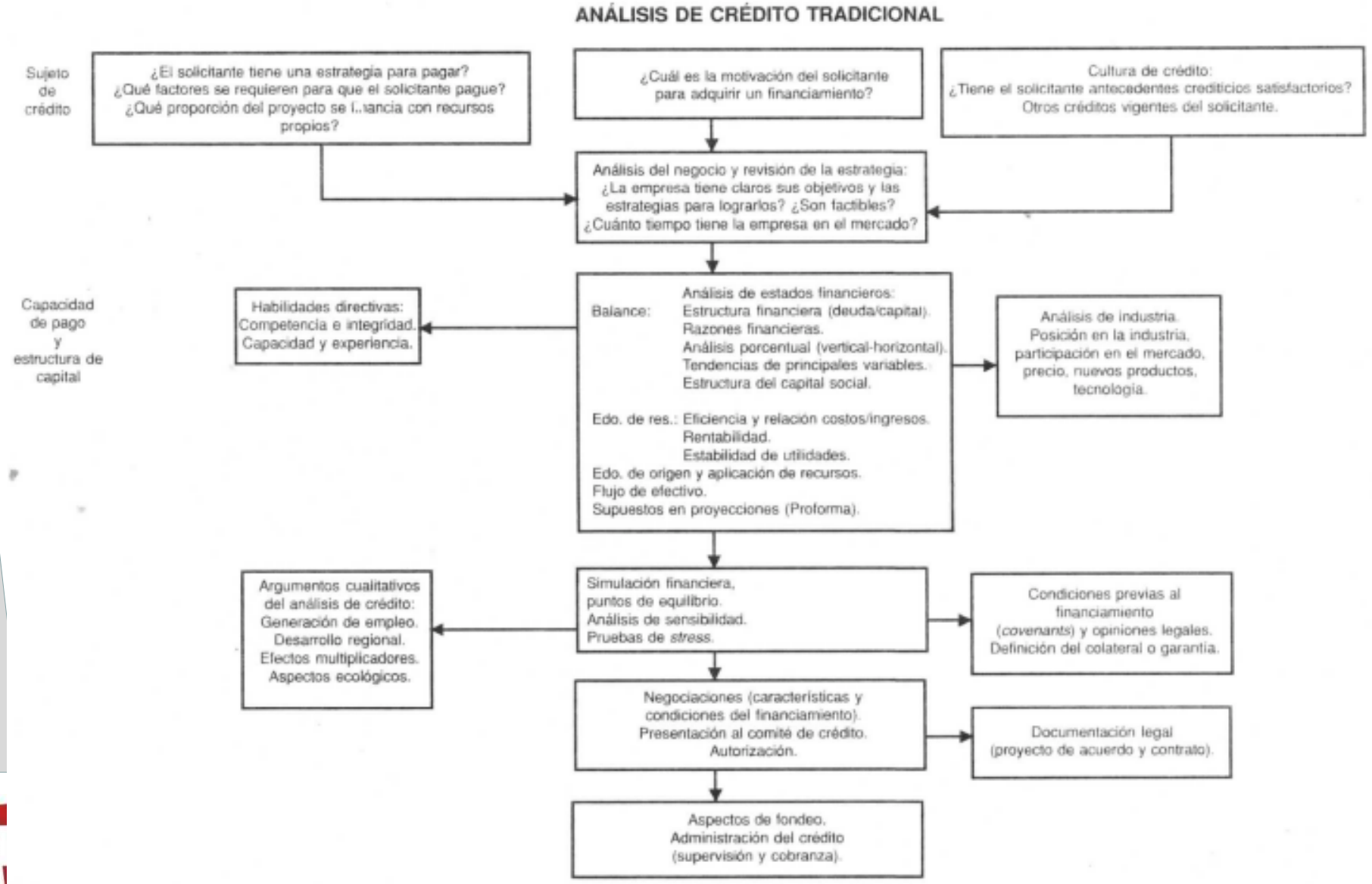



**Motivo del crédito**

Afecta las cuentas patrimoniales y al resultado de la empresa

- Conocer
- Capacidad de pago
- Condicion es cíclicas
- Capital
- Colateral

# RIESGO DE CRÉDITO



## Responsabilidad del Directorio

- Aprobar y revisar la estrategia, objetivos y lineamientos.
- Aprobar y revisar las políticas y procedimientos.
- Establecer y revisar la estructura organizacional.

## Responsabilidad de la Gerencia General

- La implementación de la GRC conforme a la aprobación del Directorio.
- Proponer un Plan Estratégico, el cual incluye apetito y tolerancia al riesgo
- Los gerentes de las unidades tienen la responsabilidad de asegurar la consistencia entre las operaciones y los niveles de tolerancia al riesgo aplicables a su ámbito de acción.

## Responsabilidad de Riesgos

- Proponer las políticas, límites, metodologías, modelos y parámetros para identificar, medir, tratar, controlar y reportar el riesgo de crédito, así como sus modificaciones.
- Monitorear el RC y su mantenimiento a nivel de apetito y tolerancia:
  - Exposición al RC, incidencia e impacto en resultados y solvencia. Análisis de sensibilidad y pruebas bajo diferentes escenarios.
  - Desviaciones que se presenten, incluyendo análisis de causas.
  - Excepciones.
  - Acciones correctivas necesarias.
  - Cumplimiento normativo.
- Cálculo de los requerimientos de capital por RC.
- Clasificación regulatoria de deudores y cálculo de provisiones.
- Gestión de operaciones refinanciadas.

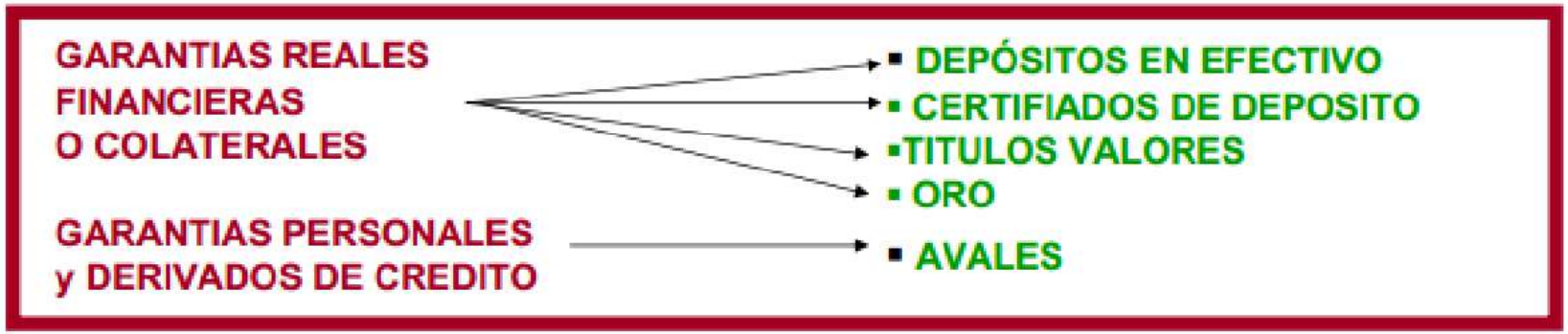
## Responsabilidad de Riesgos

- Seguimiento individual de los deudores.
- Seguimiento de portafolio.
- Señales de alerta temprana / Indicadores / Sobreendeudamiento.
  - ¿En cuántas entidades tiene el cliente créditos aprobados?
  - Ratio de endeudamiento/ingresos
  - Monto máximo de línea a partir de su nivel de ingresos
  - Monto máximo de pago mensual a partir de su nivel de ingresos
- Análisis de cosechas.
- Evolución de cartera / Pruebas de estrés.
- Gestión del Riesgo Cambiario Crediticio. Sistema de control para las colocaciones en moneda extranjera que identifique, mida, controle y reporte adecuadamente sus niveles de exposición. Variable adicional: fluctuación del tipo de cambio.

## Tipos de riesgo de crédito

- **Riesgo de impago**. Que la contraparte no realice los pagos en la fecha fijada. Indicador: FPD.
- **Riesgo de crédito individual**. También llamado Riesgo de Solvencia, muestra las exposiciones importantes con una sola contraparte.
- **Riesgo de cartera**. También llamado Riesgo de Portafolio, riesgo inherente a la composición global de la cartera: concentración en sectores económicos, geografía, grupos SE, etc.
- **Riesgo de calificación**. Derivado del hecho de que la contraparte varíe su calidad crediticia en el período de la obligación.

# Mecanismos de Cobertura del Riesgo de Crédito




- Políticas y procedimientos para la gestión de garantías.
- Gestión de plazos.
- Control de riesgos residuales.
- Gestión de garantías “sábana”.

# Líneas de Negocio – Basilea II

| Línea de negocio | Ejemplo de actividades |
|---|---|
| Finanzas Corporativas | Fusiones y adquisiciones, suscripción de emisiones, privatizaciones, titulizaciones, investigación, deuda (pública, alto rendimiento), acciones, sindicaciones, Ofertas Públicas Iniciales, colocaciones privadas en mercado secundario. |
| Negociación y ventas | Renta fija, renta variable, divisas, *commodities,* crédito, financiación, posiciones propias en valores, préstamo y operaciones con pacto de recompra, intermediación, deuda, intermediación unificada (*prime brokerage*) |
| Banca Minorista | Préstamos y depósitos de clientes minoristas y de banca priviada, servicios bancarios, fideicomisos, testamentarias, asesoramientos de inversiones, tarjetas de empresa / comerciales, créditos hipotecarios para vivienda. |
| Banca Comercial | Financiación de proyectos, bienes raíces, financiación de exportaciones, financiación comercial, factoring, arrendamiento financiero, préstamos, garantías, letras de cambio. |
| Liquidación y pagos | Pagos y recaudaciones, transferencia de fondos, compensación y liquidación |
| Servicios de agencia | Cajas de seguridad, certificados de valores, préstamos de valores (clientes), operaciones de sociedades, agentes de emisiones y pagos, fideicomisos de empresas. |
| Administración de activos | Administración discrecional y no discrecional de fondos (agrupados, segregados, minoristas, institucionales) |
| Intermediación minorista | Bancaseguros, Suscripción y rescate de fondos mutuos por cuenta de una administradora. |

## Tipos de créditos

- Créditos Comerciales
- Créditos a las Micro Empresas
- Créditos de Consumo
- Créditos Hipotecarios para Vivienda

- Niveles de provisión.
- Tratamiento de operaciones vencidas.
- Tratamiento de refinanciados.

- Créditos Corporativos
- Créditos a grandes empresas
- Créditos a medianas empresas
- Créditos a pequeñas empresas
- Créditos a microempresas
- Créditos de consumo revolvente
- Créditos de consumo no-revolvente
- Créditos hipotecarios para vivienda

## Score crediticio

- Modelo estadístico para estimar las probabilidades de que una cuenta resulte fallida.
- A partir de ciertas variables predice el comportamiento futuro comparando el comportamiento de grupos de características similares.

| **Propiedad vivienda** | | **# Consultas últimos 6 meses** | |
|---|---|---|---|
| Propietario | +27 | 0 | +17 |
| Alquiler | -15 | 1 | 0 |
| V.C.P. | 0 | 2 | -27 |
| | | 3+ | -51 |
| **Edad** | | **Teléfono dado** | |
| Hasta 20 | -19 | Sí | +15 |
| 21 - 25 | -10 | No | -15 |
| 26 - 40 | 0 | | |
| 41 -65 | +23 | | |
| 66+ | **Rechazar** | **Otras variables** | |

## Score crediticio - beneficios

- Predictores reales de riesgo.
- Precisión en la evaluación de riesgo.
- Incremento en tasa de aprobación.
- Reducción de morosidad.
- Automatización: velocidad, precisión, productividad.
- Decisiones consistentes.
- Mayor control.
- Información clave para la Dirección y gestión de riesgos.

# RIESGO DE MERCADO

Riesgo de tener pérdidas en posiciones dentro y fuera de la hoja de balance, derivadas de movimientos en los precios de mercado. Se incluye a los riesgos pertenecientes a los instrumentos relacionados con tasas de interés, riesgo cambiario, cotización de las acciones, commodities y otros.

# RIESGO DE MERCADO

**El valor en riesgo (VaR) es una medida estadística de riesgo de mercado que estima la pérdida máxima que podría registrar un portafolios en un intervalo de tiempo y con cierto nivel de probabilidad o confianza.**

Confianza

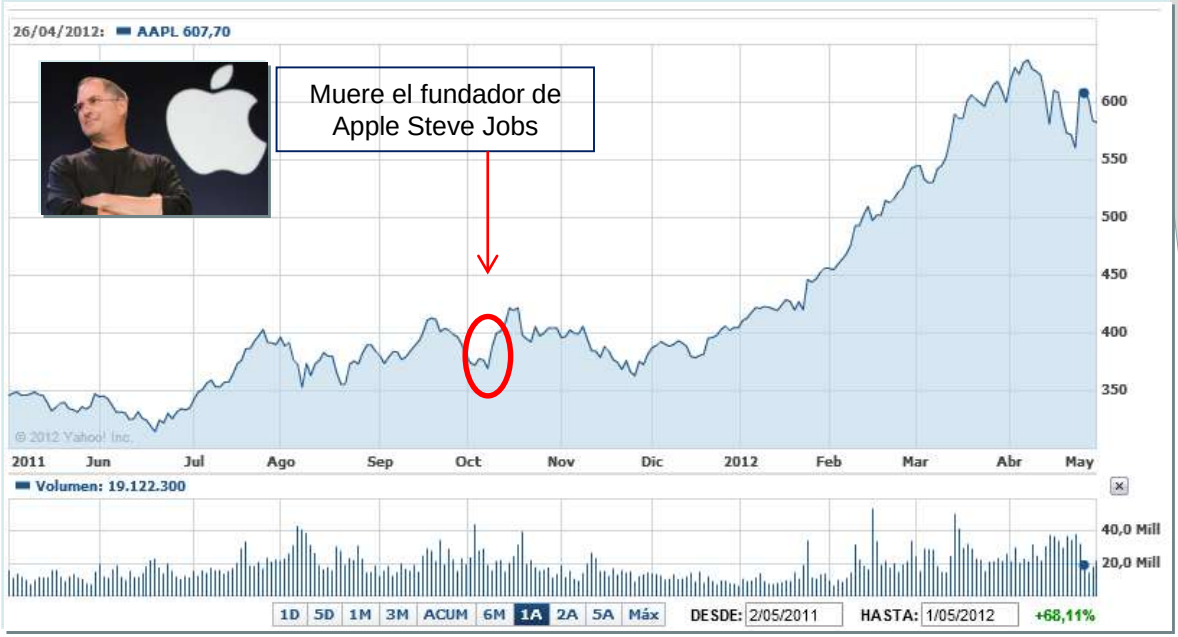
Horizonte de tiempo

**No otorga certidumbre respecto a las pérdidas, sino una expectativa de resultados basada en estadística y supuestos**

# RIESGO DE MERCADO

**El VaR es válido únicamente en condiciones normales de mercado.**

**En momentos de crisis y turbulencia la pérdida esperada se define por pruebas de stress o valores extremos.**



Ejemplo: Un inversionista tiene un portafolios de activos con un valor de $10 millones, cuyo VaR de un día es de $250,M con 95% de nivel de confianza (significa que la pérdida máxima esperada en un día será $250,M en 19 de cada 20 días), es decir, sólo un día de cada 20 de operación (1/20 = 5%), en condiciones normales, la pérdida que ocurrirá puede ser mayor a $250,M.

Ejemplo: Un inversionista compra 10,000 acciones cuyo precio es de $30 por acción y su volatilidad es de 20% anual (un año consta de 252 días de operación en el mercado, aproximadamente). Se desea conocer el VaR diario de esta posición considerando un 95% de confianza.

$$VaR = 1.65 \times \$300{,}000 \times 0.20 \times \sqrt{1/252} = \$6{,}236.41$$

# RIESGO DE MERCADO

## RIESGO CAMBIARIO


## RIESGO DE PRECIOS

## RIESGO DE COMMODITIES

## RIESGO DE TASA DE INTERÉS

a) **Riesgo Cambiario o de Divisas (RD).** Surge en las posiciones abiertas en divisas extranjeras, las cuales originan una exposición a pérdidas potenciales debido a la variación de los tipos de cambio correspondientes.

b) **Riesgo de Tasas de Interés (RTI).** Surge por el hecho de mantener activos y pasivos (reales o nominales) con diferentes fechas de vencimiento o repreciación. De este modo se crea exposición a los cambios en los niveles de las tasas de interés para los plazos correspondientes.

c) **Riesgo Accionario (RPC).** Surge al mantener posiciones abiertas (compra o venta) con acciones, índices o instrumentos basados en acciones. De este modo se crea una exposición al cambio en el precio de mercado de las acciones vinculadas a los índices o instrumentos basados en éstas.

d) **Riesgo de Volatilidad (TO).** Surge en los instrumentos financieros que contienen opcionalidad, de forma tal que su precio sea función, entre otros factores, de la volatilidad percibida en el subyacente de la opción (tasas de interés, acciones, tipo de cambio, etc.)

e) **Riesgo Base o de Margen (RMP).** Surge cuando un instrumento se utiliza como cobertura de otro y cada uno de ellos es valuado con distinta curva de tasas (por ejemplo, un bono gubernamental cubierto con un derivado de tasas interbancarias) de manera que su valor a mercado puede diferir, generando imperfecciones en la cobertura.

## Proceso para la gestión de riesgo de mercado

- Identificar operaciones afectas a RM.
- Cuantificar el riesgo asumido.
- Controlar el cumplimiento de políticas.
- Sistema de registro e información para medir y supervisar el RM.
- Informes de RM.

Stop loss

En este contexto, ¿cuál será el rol de las empresas clasificadoras de riesgo?

**Ninguna técnica analítica por más sofisticada que sea, podrá reemplazar a la experiencia y el buen juicio profesional en el manejo de riesgos.**

**JP Morgan**

# MODELO Z-SCORE DE ALTMAN

Las variables financieras se combinan linealmente con un peso específico para cada una a fin de obtener como resultado final una calificación (*Z-score*) que discrimina las empresas que incumplen en sus compromisos crediticios, de aquellas que no lo hacen.

En su primer modelo (1968) Altman escogió 22 razones financieras que formaban su lista original y finalmente escogió 5 de ellas:

# MODELO Z-SCORE DE ALTMAN

$$Z = 1.2x_1 + 1.4x_1 + 3.3x_3 + 0.6x_4 + 0.99x_5$$

Donde:

- $x_1$ - capital de trabajo/activos totales
- $x_2$ - utilidades retenidas/activos totales
- $x_3$ - utilidades netas antes de impuestos/activos totales
- $x_4$ - valor de mercado de la acción/valor en libros de la deuda
- $x_5$ - ventas/activos totales

# MODELO Z-SCORE DE ALTMAN

- $X_1$ – Pondera la contracción que puede existir en los activos corrientes con relación a los activos totales, producto de las pérdidas operativas de la empresa.
- $X_2$ – Pondera las utilidades reinvertidas o pérdidas de la empresa. Muestra la utilidad acumulada a largo plazo.
- $X_3$ – Mide la productividad real de los activos de la empresa, mostrando la capacidad real de la empresa de obtener ingresos a partir de la utilización de sus activos.
- $X_4$ – Evidencia la cantidad de activos que pueden perder valor antes de que los pasivos superen a los activos y la empresa se declare insolvente.
- $X_5$ – Habilidad de la empresa para generar ventas a partir del uso de sus activos. Mide la productividad del activo.

# MODELO Z-SCORE DE ALTMAN

De acuerdo con E. Altman, la situación dinanciera de la emisora depende del valor de Z:

- Si Z > 2.99 la empresa se considera saludable
- Si Z < 1.81 la empresa está en bancarrota
- Si 1.81 < Z < 2.99 no se puede determinar la condición financiera de la empresa (zona gris)

- Z > 2.99 - empresa saludable
- 2.69 < Z < 2.99 – cautela
- 1.81 < Z < 2.69 – posibilidad de quiebra
- Z < 1.81 - empresa en quiebra

# RIESGO DE LIQUIDEZ

Situación de crisis

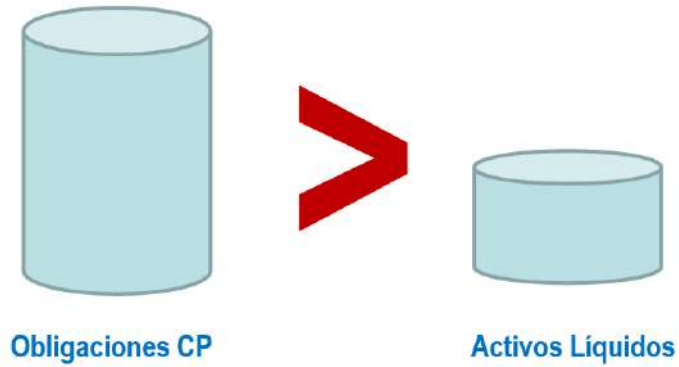
Imposibilidad de transformar en efectivo un activo

Potenciales pérdidas al requerir una mayor cantidad de recursos para financiar activos a un costo posiblemente inaceptable

# RIESGO DE LIQUIDEZ

La posibilidad de pérdidas por incumplir con los requerimientos de financiamiento y de aplicación de fondos que surgen de los descalces de flujos de efectivo, así como por no poder cerrar rápidamente posiciones abiertas, en la calidad suficiente y a un precio razonable.

- La liquidez mide la capacidad de una empresa de cubrir sus obligaciones de corto plazo y financiar su crecimiento de largo plazo.
- El RL es el riesgo de calce entre los fondos disponibles y los fondos necesarios.



# RIESGO DE LIQUIDEZ

## Utilidades

- Permite absorber pérdidas esperadas.
- Evaluación enfocada en el nivel (objetivos), sostenibilidad (recurrencia) y volatilidad (riesgo de las actividades), como fuente de generación interna de capital.

## Capital

- Permite absorber pérdidas no esperadas.
- Evaluación enfocada en el nivel (requerimientos mínimos) y calidad.

## Liquidez

- Una adecuada estructura de balance es fundamental para la solidez de la empresa.
- Evaluación enfocada en el nivel del riesgo (requerimientos mínimos) y la calidad de la gestión.

# CASO NORTHERN ROCK BANK

# CASO NORTHERN ROCK BANK

## Descripción

- Cooperativa de crédito orientada al sector construcción, constituida en el siglo XIX (1865).
- Lista en bolsa desde 1997.

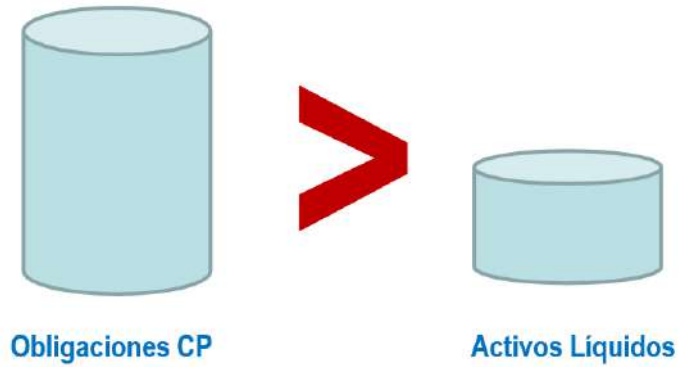
## Antecedentes a la quiebra

- Tasa anual de crecimiento de 23,2%.
- Fuerte dependencia (financiamiento) proveniente de fondos de la banca de inversión.
- Asset-backet commercial paper (ABCP) fue su principal recurso de financiación de activos hipotecarios a largo plazo y barómetro para medir apetito del mercado de activos hipotecarios.

# CASO NORTHERN ROCK BANK

## Asset-backet commercial paper (ABCP).

- Papel comercial con garantía de activos financieros, utilizado para diversificar activos y generar ganancias a corto plazo.
- Típicamente es un instrumento de corto plazo entre 1 y 270 días (promedio 30 días)



# CASO NORTHERN ROCK BANK

## La quiebra

- Segundo semestre de 2007.
- Coincidencia de una fuerte caída de ABCP y pérdida sustancial del financiamiento mayorista.
- Necesitaba apelar intensamente al mercado de capitales a corto plazo para cubrir su gap de financiación en un momento crítico para el mercado.
- Entre junio y diciembre de 2007 perdió el 57% del financiamiento mayorista y minorista.

# RIESGO DE LIQUIDEZ

## Atributos de un activo

- Liquidez: capacidad para ser transformado en efectivo en un tiempo y costo razonable.
- Rendimiento: Ingresos financieros que genera el activo a su tenedor.

Normalmente existe una relación inversa entre el grado de liquidez y el rendimiento de un activo: a mayor rendimiento menor liquidez

## Naturaleza del pasivo

- Volatilidad: Probabilidad de que el pasivo sea retirado de manera rápida e imprevista por el acreedor.
- Costo: Gastos financieros que genera el pasivo a su tenedor.

Normalmente existe una relación inversa entre el nivel de volatilidad y el costo de un pasivo: a mayor costo menor volatilidad

# RIESGO DE LIQUIDEZ

## Trade off rentabilidad y riesgo

- Mantener activos ilíquidos (largo plazo).
- Mantener pasivos volátiles (corto plazo).

Esta decisión incrementa de manera importante la exposición al riesgo de liquidez.

## Necesidades de liquidez

- Disminución del pasivo (retiros de depósitos).
- Incremento del activo (uso de líneas)

El RL se puede generar del lado del pasivo o del activo.

# RIESGO DE LIQUIDEZ

## Factores a tener en cuenta

- Entorno del mercado (precios).
- Nivel de apetito y tolerancia al riesgo.
- Posiciones de liquidez que se mantienen.
- Acceso a nuevas fuentes de fondeo.
- Diversificación de fuentes de fondeo.
- Requerimientos regulatorios (encaje y ratios mínimos de liquidez).

## Efectos

- Corridas de depósitos.
- Incremento de las tasas de interés interbancario. Incumplimiento de encaje.
- Costos de financiamiento más elevados.
- Problemas con acreedores, incapacidad de renovar depósitos.
- Desconfianza del mercado.

## Gestión de liquidez

| | |
|---|---|
| **Liquidez de corto plazo** | • Habilidad para cumplir con las obligaciones de corto plazo<br>• Gestión de los flujos de efectivo |
| **Liquidez de mediano y largo plazo** | • Balancear las colocaciones y el financiamiento de mediano y largo plazo<br>• Buscar un financiamiento de bajo costo |
| **Negociación** | • Liquidez de los activos<br>• Habilidad para liquidar posiciones en un tiempo y a un costo razonable |
| **Acceso al mercado** | • Financiamiento en el mercado<br>• Habilidad para financiarse en los mercados de capitales |

## Gestión de liquidez

**Roles:**

**Directorio**: Revisión y aprobación

**Gerencia**: Diseño e implementación

**Personal**: Aplicación y retro-alimentación

## Gestión de liquidez

- Grado de liquidez de los activos.
- Niveles de endeudamiento.
- Estructura del pasivo.
- Volatilidad de los pasivos.
- Volatilidad de los depósitos.
- Disponibilidad de líneas de financiamiento.
- Efectividad de la gestión de activos y pasivos.

## Indicadores de liquidez

- Posición en efectivo: activos líquidos a cp / activos totales
- Indicadores de liquidez: activos líquidos a cp / pasivos líquidos de cp
- Concentración de depósitos.

- Análisis de brechas
- Escenarios de estrés

# FRAUDE EN LOS NEGOCIOS

Muchos directivos tienden a limitar su campo de visión y se enfocan únicamente en los procedimientos y controles contables, en lugar de fijarse en los riesgos específicos (de fraude) que enfrenta el negocio.

Los defraudadores son oportunistas que sacan ventaja de las debilidades temporales o de las brechas desapercibidas entre la fortaleza aparente y la efectividad de los controles.

Indicadores de fraude:

- Del personal,
- Comerciales,
- Estructurales, y
- Culturales.

**Indicadores de fraude: del personal.**

- Estilo administrativo autocrático
- Incompatibilidad entre personalidad y posición
- Comportamientos inusuales
- Actos ilegales
- Estilos de vida costosos
- Vacaciones no tomadas
- Personal de baja calidad
- Moral baja
- Alta rotación
- Compensación vinculada al rendimiento

**Indicadores de fraude: comerciales.**

- Estrategia comercial pobremente definida
- Utilidades por encima del promedio de la industria
- Desajuste entre el crecimiento y el desarrollo de los sistemas
- Reputación pobre
- Problemas de liquidez

**Indicadores de fraude: estructurales.**

- Estructuras complejas
- Sitios remotos mal supervisados
- Varias firmas de auditores

**Indicadores de fraude: culturales.**

- Resultados a cualquier costo
- Bajo compromiso frente al control
- Ausencia de código de ética comercial
- Obediencia incuestionable del personal

**¿Cuándo ocurre el fraude?.**

- **Cuando el motivo coincide con la oportunidad**.
- Motivo: codicia, falta de dinero, venganza, sentido de propiedad de lo robado o de habérselo ganado
- Oportunidad: falta de un factor disuasivo real o a la baja probabilidad de ser descubierto debido a la existencia de áreas grises en las reglas.

# ¿QUÉ OCURRE CUANDO NO GESTIONAMOS EL RIESGO DE MANERA EFICIENTE?

# CRISIS FINANCIERAS

**CRISIS FINANCIERA (2007)**

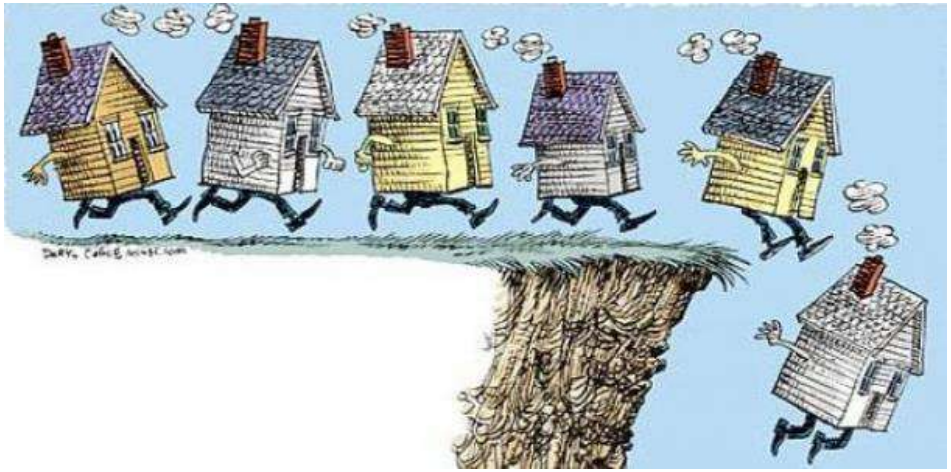
- Es uno de los casos más claros de los **efectos de la globalización**.
- Una crisis inmobiliaria, terminó convirtiéndose en una de las crisis financieras más graves de todos los tiempos.
- Pero, **¿qué es una hipoteca subprime?**

# CRISIS FINANCIERAS

## CRISIS FINANCIERA (2007)

- El término hace referencia a las **hipotecas de alto riesgo**.
- Se conceden a clientes que por su nivel de solvencia no tienen acceso a otro tipo de créditos (hipotecas prime).
- Al ser el riesgo de estos clientes más alto, se les exige a cambio un tipo de interés también más elevado, aunque durante los primeros años las condiciones son más ventajosas y se endurecen pasado un plazo (¿?).

# CRISIS FINANCIERAS



Video: La Crisis de los Tulipanes

# CRISIS FINANCIERAS

Titulización de activos: empaquetar los préstamos y colocarlos en forma de bonos en el mercado internacional

## CRISIS FINANCIERA (2007)

- **¿Cómo se extiende la crisis a otros sectores y países?**



Riesgo de Crédito bancario

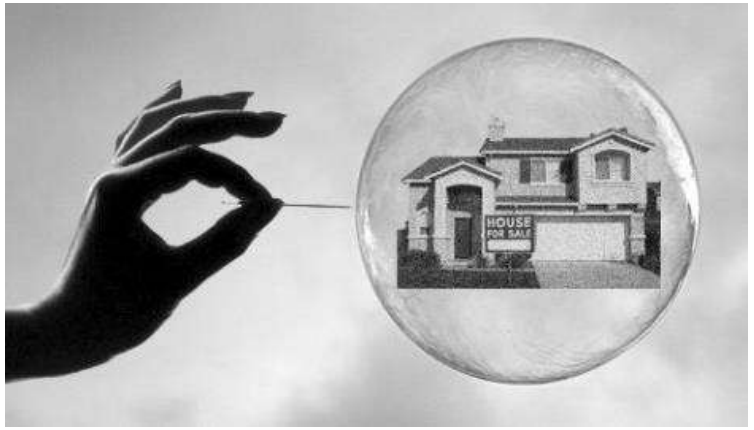
Riesgo de Mercado de inversionistas

# CRISIS FINANCIERAS

## CRISIS FINANCIERA (2007)

- Las hipotecas subprime estaban condenadas a implosionar una vez que reventara la burbuja inmobiliaria.
- También la tendencia de los consumidores estadounidenses a endeudarse por más dinero del que ganaban.
- Para muchos observadores no es claro que los reguladores gubernamentales tengan la voluntad, la influencia y la sabiduría necesarias para reescribir las reglas del juego financiero del siglo XXI.

Lectura recomendada:
"Cómo provoqué la crisis financiera"
Tetsuya Ishikawa



# CRISIS FINANCIERAS

- La prosperidad del país creó la **atmósfera optimista** dentro de las cuales tienden a aparecer las burbujas.
- Como los precios no pueden aumentar de manera indefinida, alcanzaron su nivel más alto el 04 de febrero de 1637 y en adelante la disminución determinó la fase de caída y crisis.
- **La reducción en el precio fue el equivalente de USD.75,000 dólares a USD.1 dólar**.

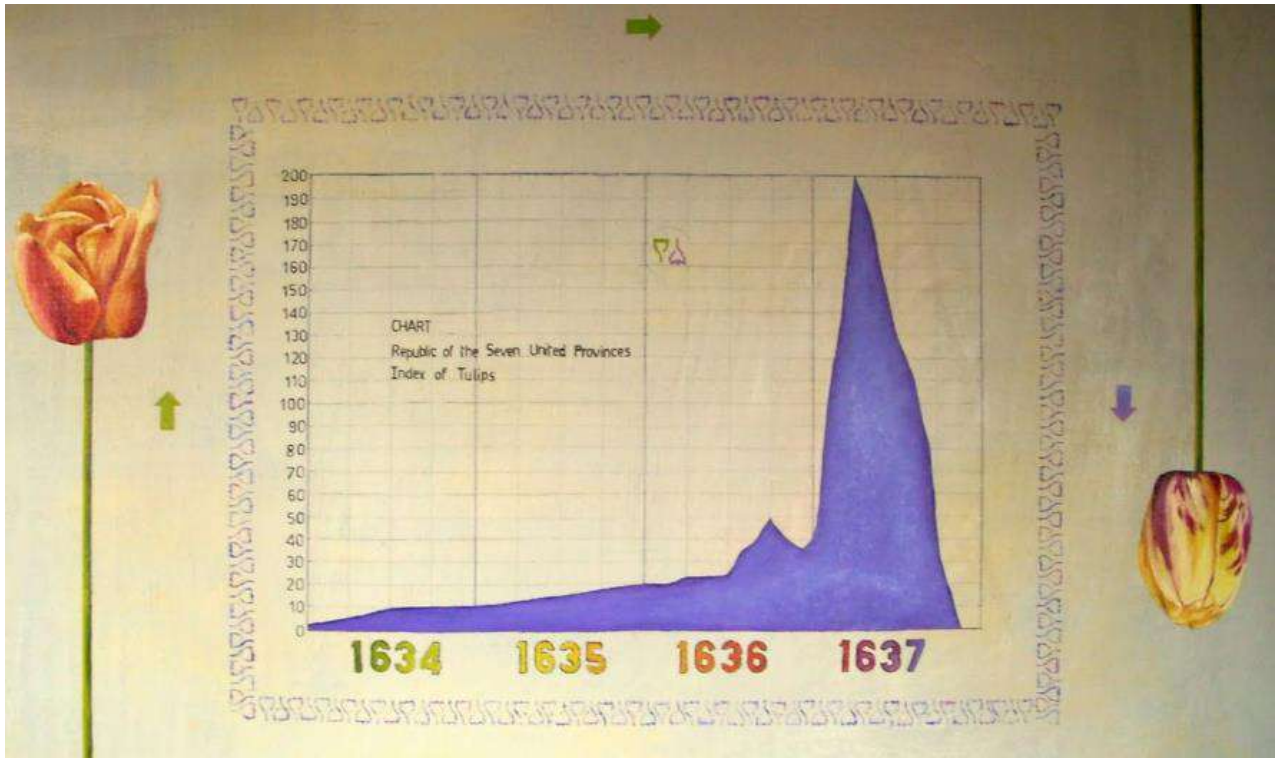
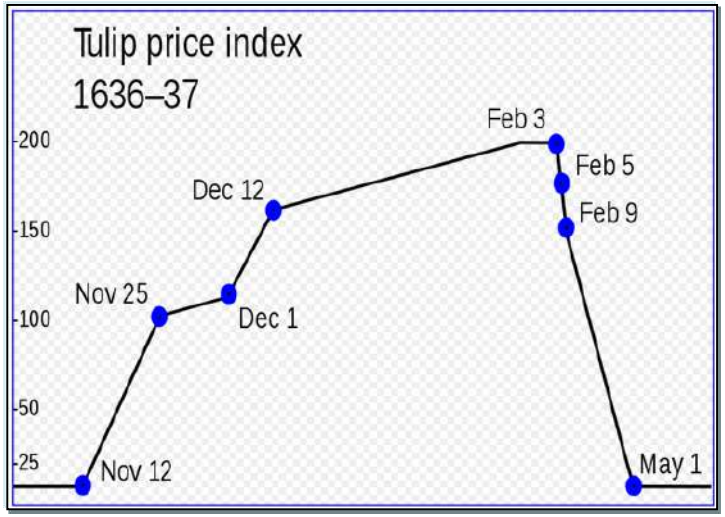
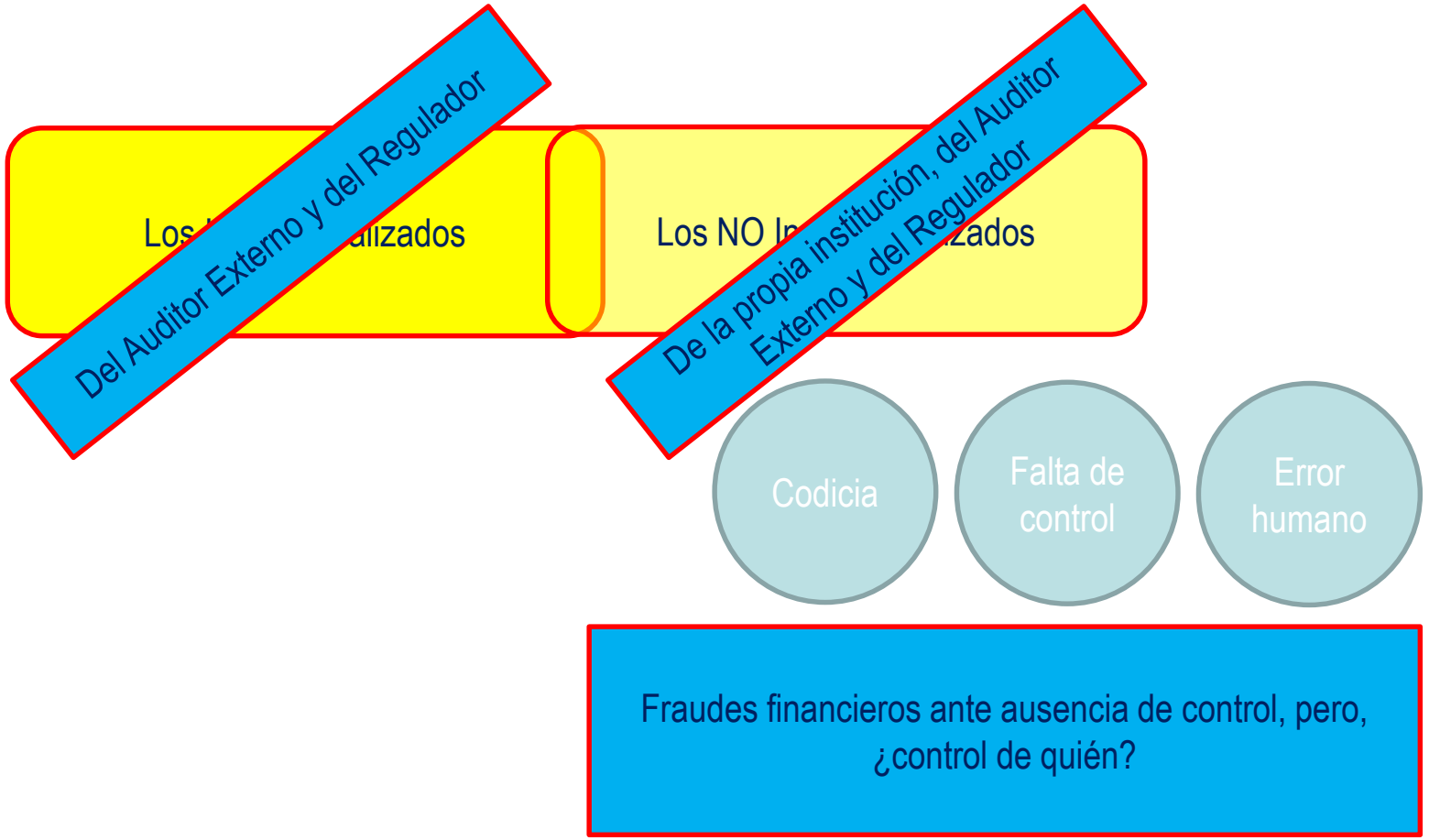


CHART
Republic of the Seven United Provinces
Index of Tulips
200
190
180
170
160
150
140
130
120
110
100
90
80
70
60
50
40
30
20
10
0
1634
1635
1636
1637


Tulip price index
1636–37
200
150
100
50
25
Nov 12
Nov 25
Dec 1
Dec 12
Feb 3
Feb 5
Feb 9
May 1

# FRAUDES FINANCIEROS ANTE AUSENCIA DE CONTROL



# FRAUDES FINANCIEROS ANTE AUSENCIA DE CONTROL

BARINGS

## BARINGS BANK (1995)

# BARINGS BANK

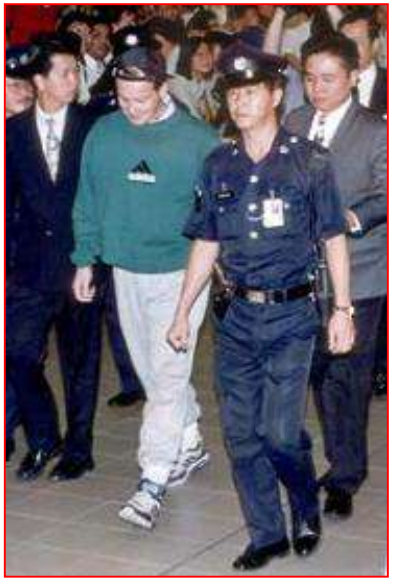
## HISTORIA DEL BANCO

- El banco más antiguo de Gran Bretaña y uno de los más antiguos del mundo, financió las Guerras Napoleónicas y gestionaba el patrimonio de la Reina Isabel de Inglaterra.
- El banco quedó en la bancarrota al no poder obtener la liquidez necesaria para salir de la crisis.
- La familia Barings tuvo el control de la institución hasta su quiebra en 1995 (233 años).
- Este es un caso emblemático ya que todo lo que podía salir mal en términos de gestión de riesgo, ocurrió.


# BARINGS BANK

## HISTORIA DEL TRADER

- Nicolas ´Nick' William Leeson, operador del mercado de derivados que trabajaba en la subsidiaria del Barings Bank en Singapur.
- Leeson dirigía desde la sede del banco en Singapur las operaciones de futuros en los mercados asiáticos y apostó a la caída del yen, entre 1992 y 1995. El banco perdió todas sus reservas lo que lo llevó a la quiebra.
- Sufrió pérdidas que rebasaban en exceso el capital del banco y llevó a la quiebra al banco en febrero de 1995 con pérdidas superiores a US$ 1,300 millones, invirtiendo en el índice Nikkei de Japón.
- Leeson fue condenado por fraude y sentenciado a 6 años de prisión.
- Escribió su autobiografía *Rogue Trader* (Trader granuja).



# BARINGS BANK

## ¿Qué falló en un banco tan antiguo?

| | | |
|---|---|---|
| Nick Leeson era una persona ambiciosa | ¿Está mal ser ambicioso?<br>¿Es el perfil correcto? | "Trabaja duro, juego duro" |
| Personal sin experiencia y novato, con ambición | Búsqueda de un nuevo perfil "hambriento" | ¿Y la definición de apetito y tolerancia al riesgo? |
| Personal sin experiencia y novato, con ambición | Recibe instrucciones y las ejecuta | ¿Esto ocurre hoy en nuestras organizaciones? |
| Manejo de todos los aspectos del negocio | ¿es esto correcto? ¿por qué es tan importante la segregación de funciones? | "Al menos hasta que suban los volúmenes" |
| Falta de estrategia clara / pérdida de visión de los objetivos corporativos | ¿Grandes ganancias a bajo riesgo? | "No es extremadamente difícil hacer ganancias en el negocio de derivados financieros"<br>Incremento de ganancias pero, ¿reduciendo los niveles de riesgo? (expectativa de bonificaciones) |

# BARINGS BANK

## ¿Qué falló en un banco tan antiguo?

| | | |
|---|---|---|
| Fallar no es una opción / Utilización de la información | Presión por metas poco realistas e improvisadas | ¿Replicar la operación en Singapur? ¿Cómo? |
| Personal a la defensiva | Los controles no deben tomarse como algo personal, sino como parte de los procesos | Tácticas evasivas, ocultarse. |
| Gestión de riesgos deficiente | Manejo ineficiente (inexistente) de errores operacionales | Una oportunidad/ventana de fraude<br>Gestión de cuentas contables |
| Búsqueda de nuevos mercados / clientes (más vulnerables) | Plan de Negocios | ¿Es congruente con la estrategia de la organización? ¿Tiene conformidad del área de Riesgos? |
| "Empleados estrella" … ¿modelos a seguir o sospechosos por evaluar? | Debemos desconfiar de los resultados "extraordinarios" | Auditorías estrictas<br>Señales de alerta son obviadas<br>Falta de seguimiento de indicadores |
| Falta de normas, políticas y procedimientos | ¿Son suficientes las auditorías externas?<br>¿Funcionan las auditorías internas? | ¿Cómo nos protegemos de la falsificación de documentos? |

# BARINGS BANK

**¿Qué falló en un banco tan antiguo?**

*"Mis superiores no entendían el funcionamiento básico de futuros y opciones, pero no estaban dispuestos a hacer preguntas"*

Nick Leeson
Entrevista BBC de Londres, 2001.

*"Muchos analistas se muestran escépticos respecto a la capacidad de estos rogué traders de acumular pérdidas tan enormes sin que nadie se entere. Sospechan que éstos son chivos expiatorios que se sacrifican para salvar a los responsables de una supervisión y fallos de gestión"*

Wall Street Journal, 27 de septiembre de 1997.

# BARINGS BANK

**¿Qué clase de riesgos no fueron apropiadamente controlados?**

**¿El riesgo moral?**

**¿Cuáles otros riesgos?**

**¿Y los reguladores?**

Describa y discuta los riesgos que no fueron controlados y qué controles hubiera establecido usted?

**Revisemos los errores críticos que ocurren en todos los niveles de la organización y en la aplicación de las medidas de control.**

# FRAUDES FINANCIEROS ANTE AUSENCIA DE CONTROL


## BANAMEX - CITIGROUP MÉXICO (2014)

# BANAMEX – CITIGROUP MÉXICO

**Citigroup reporta fraude en unidad de México**

*"Puedo asegurarles que los responsables de perpetrar estos delitos pagarán por ello, lo mismo que cualquier empleado del Banco que haya participado directa o indirectamente; que haya permitido, supervisado con laxitud o mostrado falta de control, en abierta violación a nuestro Código de Conducta. Todos serán igualmente responsables por sus actos y nos aseguraremos que su castigo sirva como un claro ejemplo respecto de las consecuencias de los mismos".*


Michael Corbat – CEO Citigroup

# FRAUDES FINANCIEROS ANTE AUSENCIA DE CONTROL


## LONDON INTERBANK OFFERED RATE (LIBOR)

# LONDON INTERBANK OFFERED RATE (LIBOR)

BARCLAYS

HSBC

JPMorganChase

Deutsche Bank


Morgan Stanley

Bank of America

SOCIETE GENERALE

citi

CRÉDIT AGRICOLE

UBS

Rabobank

LLOYDS BANK

CREDIT SUISSE

# LONDON INTERBANK OFFERED RATE (LIBOR)

Año 2007
*Financial Times* devela que el banco británico Barclays Bank había estado publicando tasas interbancarias más bajas que las reales.

La Libor se calcula a partir del promedio de las tasas que se cobran entre sí 18 bancos británicos cuando se prestan fondos no asegurados.

Una manipulación en su cálculo genera una repercusión a nivel global, dado que es el *benchmark* en múltiples productos financieros.

¿Cuál es el proceso?
¿Qué controles tiene?
¿Cuál es el rol del regulador?

# LONDON INTERBANK OFFERED RATE (LIBOR)

16 bancos bajo investigación

Colusión de un grupo de operadores para manipular el indicador financiero clave del mundo.

Multas:
Barclays US$ 450'MM
UBS US$1,500'MM
RBS US$ 627'MM

US$ 9,000'MM para evitar procesos judiciales

21 imputados

Estos montos no consideran las pérdidas que los bancos han debido asumir para compensar a sus clientes o por pérdidas de negocios.

# LONDON INTERBANK OFFERED RATE (LIBOR)

| Operador | Banco | Acusación | Condena | Comentarios |
|---|---|---|---|---|
| Tom Hayes (35) | UBS<br>Citigroup | Culpable de 8 acusaciones de conspiración para cometer fraude | 10 años | Diagnosticado con Síndrome de Asperger, dijo durante el juicio que fue transparente sobre sus intentos de influir en las tasas y que sus jefes conocían y aprobaban unos métodos que eran comunes en el sector.<br>Dijo además que no recibió formación para estas prácticas, que la Libor no estaba regulada en ese entonces y que dejó un rastro de correos electrónicos y conversaciones en chats porque no pensaba que estuviera cometiendo ningún delito. (1) |
| | | | | |

(1) http://semanaeconomica.com/article/economia/economia-internacional/166321-escandalo-libor-justicia-britanica-condeno-a-14-anos-de-carcel-a-operador-bursatil/ (04/Ago/2015).

# ENRON


Transmisión y distribución de electricidad y gas y al desarrollo, construcción y operación de plantas de energía y oleoductos

Nuevos mercados en el área de comunicaciones, administración de riesgos y seguros

21,000 empleados

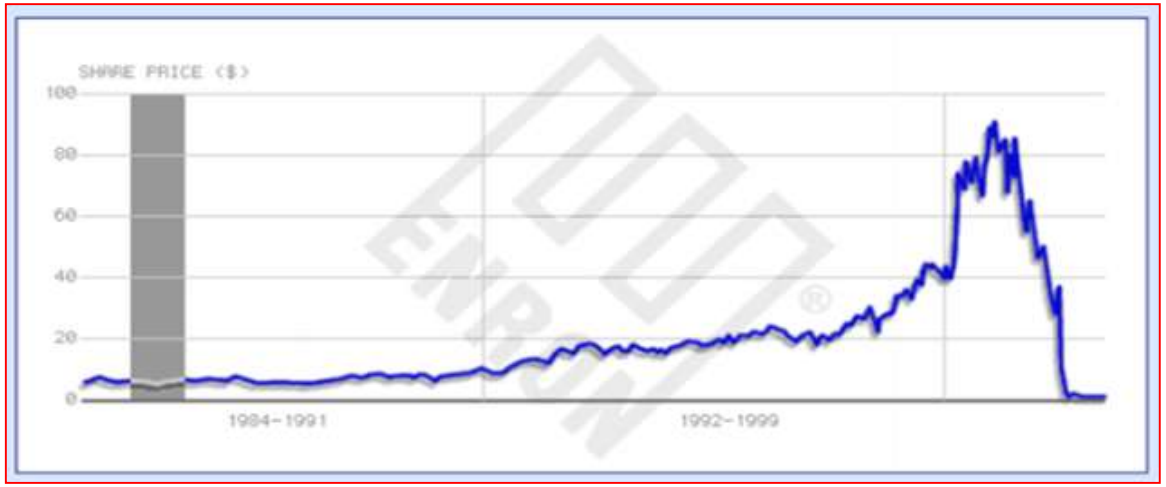
En la lista de los 100 mejores empleadores (1996-2000)

Ganancias US$ 1,000 millones en 2001

Pérdidas de US$ 30,000 millones a fines de año

Prácticas contables / Reputación / destrucción documentos

# ENRON





Kenneth Lay y Jeffrey Skilling, presidente y director ejecutivo, son condenados por 6 cargos de conspiración para cometer fraude y 28 cargos de conspiración, fraude y maniobras financieras para ocultar las pérdidas y exagerar los beneficios de Enron, con el fin de atraer el dinero de los inversionistas.

# WOLDCOM


Sector telecomunicaciones

En 1999: US$ 64.50 por acción

"Maquillaje" de cuentas contables

Ingresos fraudulentos de US$ 3,800 millones

Deuda de intereses impagable de US$ 75 millones


Bernard Ebbers, director ejecutivo, condenado a 25 años de prisión por 9 cargos de conspiración, fraude de valores y presentación de documentos falsos.

# ARTHUR ANDERSEN LLP

¿¿¿ Y el auditor ????

# ARTHUR ANDERSEN LLP

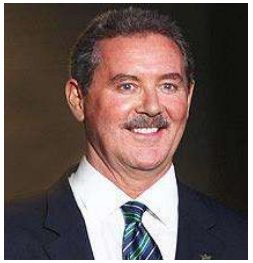

Fundada en 1913, fue hasta 2002 una de las cinco grandes empresas auditoras del mundo, con sede en Chicago. Ofrecía servicios de auditoría, consultoría tributaria y asesoría jurídica.
En 2001 facturó USD.9,300'MM.
En el año 2002 se vio involucrada en los escándalos de Enron (empresa que auditó por 16 años) y Worldcom. Inicialmente estimó haber perdido 650 de sus 2,300 clientes del sector público en Estados unidos y otros más en el extranjero.

**Desenlace:**

En 2002, fue sentenciada por delitos de obstrucción a la justicia y de destrucción y alteración de documentos relacionados a la quiebra de Enron. Se le impuso una multa de USD.500,M y la prohibición de ofrecer servicios de auditoría y asesoría a empresas que cotizan en la Bolsa norteamericana.
En 2005 la Corte Suprema absolvió a la compañía, pero esta no pudo recuperarse.

ARTHUR ANDERSEN

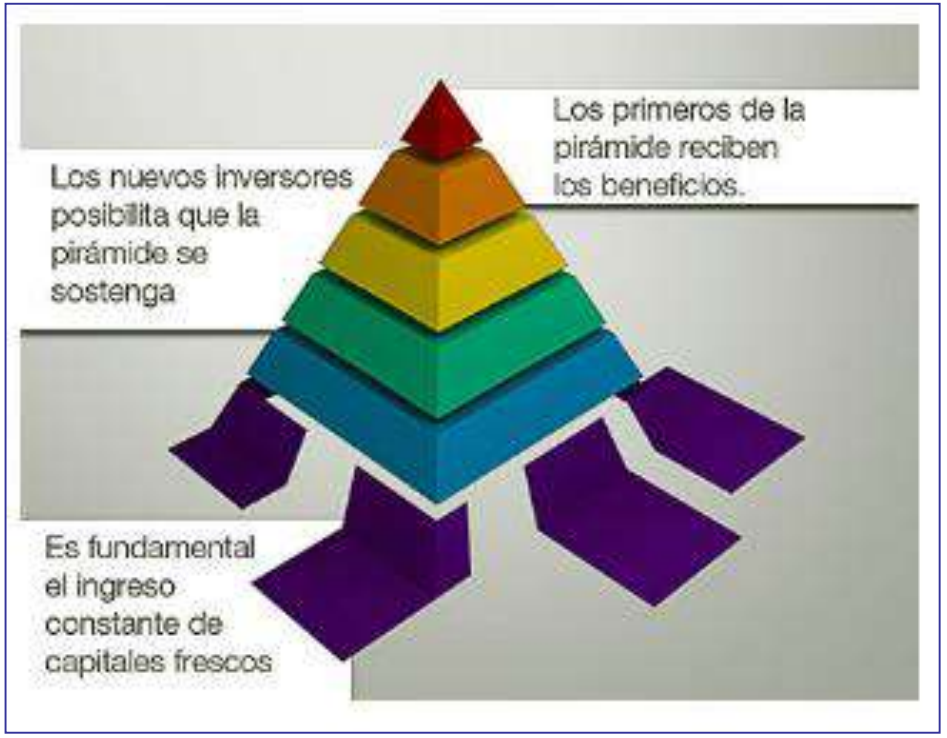
# VEAMOS OTROS CASOS



# VEAMOS OTROS CASOS


Un negocio legítimo se puede ir convirtiendo gradualmente en un esquema Ponzi
Cuando un empresario pide un préstamo ofreciendo interesas más altos a los usuales porque espera conseguir beneficios espectaculares de un negocio.




Al fracasar en el negocio u obtener beneficios menores al esperado, puede ser que acepte retomar la inversión con el fin de volver a intentar el negocio.
Pueden acabar de cualquiera de las siguientes formas:

- Los estafadores huyen con el dinero
- El sistema se hunde por si mismo
- La estafa es expuesta

# VEAMOS OTROS CASOS


**Bernard Madoff**

Bernard Lawrence “Bernie” Madoff. Nacido en 1938, Presidente de una firma de inversiones con su nombre desde 1960, una de las más importantes de Wall Street.

En diciembre de 2008 fue detenido por el FBI acusado de fraude por **USD.50,000 MM**.

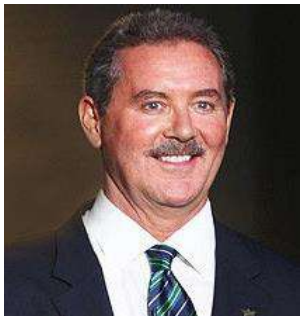
Es el mayor fraude perpetrado por una persona en la historia, que se prolong por más de dos décadas.

El 29 de junio de 2009 fue condenado a 150 años de prisión y el decomiso de USD.17,179 millones.

**Cargos:**

Fraude de valores, asesor de inversiones fraudulentas, fraude postal, fraude electrónico, lavado de dinero, falso testimonio, perjurio, fraude a la Seguridad Social, robo de un plan de beneficios para empleados.

# VEAMOS OTROS CASOS




**Robert Allen Stanford**

Nacido en 1950, Presidente del Stanford Financial Group.

A principios de 2009 se inició una investigación por fraude y el 17 de febrero de 2009 la SEC lo acusa de frade y multiples violaciones a las leyes de inversión americanas por “fraude masivo continuo” por **USD.8,000 MM**. Este cargo fue posteriormente cambiado por el de “Conspiración masiva Ponzi”.

Fue arrestado por el FBI el 18 de junio de 2009. ha sido condenado a 110 años de prisión y al pago de USD.5,900 millones.

También es investigado por lavado de dinero, evasión tributaria y violaciones a la ley de patentes.

**Cargos:**

Fraude electrónico, fraude postal, lavado de dinero, conspiración, obstrucción de la justicia.

# FRAUDE FINANCIERO

**SOCIETE GENERALE**

Fundada en 1864.

Segundo banco de Francia.

Global, más de 33 millones de clientes en el mundo.

Negocio:

- Banca Corporativa y de Inversión
- Banca minorista
- Servicios de inversion global

Más de 160,M empleados.

# FRAUDE FINANCIERO

**SOCIETE GENERALE**

Broker Jerome Kerviel de 31 años, con Maestría en Finanzas en la Universidad de Lyon.

Posiciones previas: administración de riesgos, sistemas de back office y seguridad de sistemas.

Opiniones relativas a él: “tranquilo y sin pretensiones”, “educación mediocre”, “trataba de impresionar a sus superiores”

**Función como trader de bajo riesgo:** compra de índices europeos de futuros de acciones con el objetivo de obtener pequeñas ganancias de bajo riesgo basadas en alto volume.

Hizo operaciones por USD.87,000’MM.

**Conocía al detalle el funcionamiento de los controles.**

**Borraba transacciones ficticias antes del cierre.**

**Utilizaba contraseñas de otros empleados.**

**No salía de vacaciones.**

# FRAUDE FINANCIERO

## SOCIETE GENERALE

En 2008, el broker **Jerome Kerviel** produjo pérdidas de **USD.7,000'MM**. Ha sido condenado a 5 años de cárcel.

Kerviel siempre ha defendido su inocencia durante el proceso judicial y ha asegurado que sus jefes y los altos cargos del banco francés conocían "en todo momento" sus operaciones que le reportaron miles de millones de euros en su cuenta corriente por beneficiarse de las transacciones que ordenaba con sus clientes y que se desviaba en una cuenta personal. **Abuso de confianza, falsificación de documentos e introducción fraudulenta de datos en el sistema informático del banco.**

Se lo acusa de haber realizado operaciones especulativas enormes en mercados de riesgo sin autorización de sus superiores y de haber burlado los controles de su banco con operaciones ficticias, documentos falsos y mentiras.

# FRAUDE FINANCIERO

**SOCIETE GENERALE**

¿Qué motivó a Jerome Kerviel?

¿Complejo de inferioridad? ¿Ego? ¿Arrogancia? ¿jugador compulsivo? ¿psicópata?

¿Fué consciente de sus actos?
¿Sus compañeros de trabajo estaban al tanto?
¿Puede ser buena la ambición? ¿la codicia?
¿La administración no supo que estaba pasando? ¿cuál sería su responsabilidad? ¿Riesgos?
¿Existe una cultura de riesgo?
¿Cómo estar seguros que no hay casos similares aún no descubiertos?

# FRAUDE FINANCIERO

**SOCIETE GENERALE**

Recomendaciones:

- Línea anónima para denuncias.
- Entrenamiento en el código de ética.
- ¿Pruebas psicológicas?
- Revisión de posiciones dentro de día y mes. Conciliaciones.
- Política de vacaciones.
- Controles más rigurosos.
- Sanciones estrictas para quienes no acatan los procedimientos, políticas o normas.
- Controles sistemáticos, indicadores de gestión eficientes.
- Marco normativo apropiado.

# FRAUDE FINANCIERO

**UBS**

**Kweku Adoboli**, broker de UBS en Londres, de 32 años de edad, hijo de un diplomático ghanés, trabajaba en UBS desde el año 2006.

En 2011, produjo pérdidas de **USD.2,000'MM** por operaciones financieras no autorizadas, en lo que es considerado el mayor y más sofisticado fraude financiero en el Reino Unido. Las operaciones fraudulentas se realizaron entre los años 2008 y 2011.

Según el banco, el fraude fue posible ya que el operador de mercados creaba presuntamente datos ficticios para camuflar los riesgos que asumía.

Adoboli argumentó que todas sus acciones estaban destinadas a "beneficiar" a la entidad, a la que consideraba su "familia", pero admitió que "perdió el control en el torbellino de la crisis financiera".

Adoboli ha alegado en todo momento que sufría presiones por parte de sus superiores para asumir riesgos.

En 2012 Adoboli fue condenado a 7 años de cárcel.

# FRAUDE FINANCIERO

**SUMITOMO CORPORATION**

En 1996, Sumitomo Corporation reportó pérdidas por **USD.2,600'MM** debido a operaciones no autorizadas en la Bolsa de Metales de Londres.

**Yasuo Hamanaka**, era el principal inversionista en cobre de la corporación japonesa Sumitomo Corporation. Era conocido como "Sr. 5%" porque controlaba anualmente cerca del 5% del suministro mundial de cobre. También fue acusado de falsificar las firmas de dos de sus superiores en cartas a inversionistas extranjeros.

Fue sentenciado a 8 años de prisión.

Sumitomo Corporation

# FRAUDE FINANCIERO

## MORGAN GRENFELL

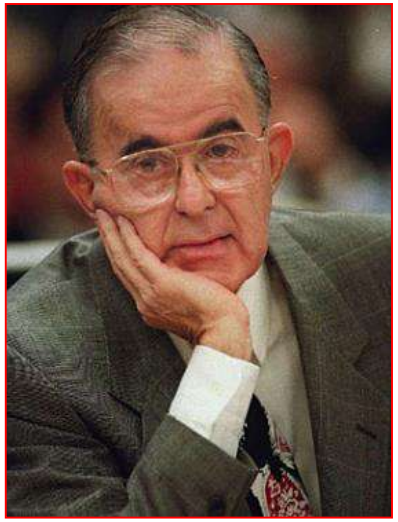
En 1998, **Peter Young**, un gestor de fondos del banco británico Morgan Grenfell (fundado en 1838), luego adquirido por Deutsche Bank, fue acusado de haber causado pérdidas por más de **£ 220'MM**, en inversiones no autorizadas.

Según Morgan Grenfell, Young empleó dinero invertido en tres grandes fondos europeos de la compañía para comprar acciones muy especulativas.

En diciembre de 2000, un jurado determinó que no estaba mentalmente capacitado para ir a juicio, luego de que se presentara ante un tribunal de Londres vestido de mujer. Fue recluido en una institución mental.

Morgan Grenfell

# FRAUDE FINANCIERO



## ORANGE COUNTY

En 1994, **Bob Citron**, tesorero del condado de Orange en el estado de California, Estados Unidos, invirtió en posiciones altamente riesgosas que se tradujeron en pérdidas por más de **USD.1,700 MM** debido al alza de las tasas de interés en 1994.

Su política de inversiones generó la quiebra del condado de Orange.

Fue condenado a 14 años de prisión.

# FRAUDE FINANCIERO


## DAIWA BANK

**Toshihide Iguchi**, un operador que manejaba posiciones en mercado de dinero en Daiwa Bank, entró al Banco en 1976, después de haber trabajado como vendedor de autos en Estados Unidos; siete años después pasó a desempeñarse como Vicepresidente adjunto. Se dice que en ese mismo momento comenzaron sus actividades ilegales en Bonos del Tesoro de Estados Unidos, negocio en el cual perdió unos USD.200,M en 1983.

A pesar de eso, la reputación de Iguchi creció, en tanto la filial del Daiwa en Nueva York registró utilidades de más de USD.100'MM al año.

Iguchi escondió los registros y fraguó documentos para ocultar la cantidad de títulos vendidos.

En 1995, tuvo pérdidas acumuladas por **operaciones no autorizadas** por **USD.1,100'MM,** en un período de 12 años que comenzó en 1983.

# FRAUDE FINANCIERO


## DAIWA BANK

Iguchi custodiaba los bonos del Tesoro del banco y los de sus clientes por medio de una cuenta, en la que se acumulaban los intereses de los bonos y los resultados de las operaciones de compraventa de los mismos. Cuando Iguchi empezó a perder dinero, decidió vender bonos de la cuenta para cubrir sus pérdidas y falsificar los balances de la cuenta para que la venta efectuada no quedase reflejada. Luego estaba el problema de cuando un cliente quería vender los valores que Iguchi custodiaba y que, a lo mejor, hacía tiempo que había vendido, o cuando había que pagar a los clientes intereses de unos bonos que hacía años que no existían.

En total se calcula que Iguchi **debió de falsificar más de 30.000 documentos de toda índole**. Fue sentenciado a 4 años de prisión.

**Dato curioso:** Medió una diferencia de dos meses entre que Iguchi informó a sus superiores acerca de las pérdidas y que el Daiwa las comunicó a los agentes fiscalizadores, constituyéndose una violación de las leyes estatales bancarias de Estados Unidos y Nueva York.

# FRAUDE FINANCIERO


## DAIWA BANK

***"Estamos profundamente contrariados porque nuestros controles y procedimientos internos no fueron suficientes para impedir esta acción fraudulenta".*** Masuhiro Tsudo, Gerente General de la filial en Nueva York del Daiwa Bank.

***"En realidad creímos en él (Iguchi). Creó un sistema en el cual estaba a cargo de todo".*** Akira Fujita, Presidente del Banco Daiwa.

***"Lo que sucede es que los gerentes no preguntan nada cuando las cosas parecen andar bien" "Si los negocios caminan, ellos no vigilan nada"***. Dough Henwood, editor de Left Business Observer.

Como consecuencia de este caso, Fujita dijo que él y otro alto jerarca del Banco han renunciado al 30% de los ingresos que percibirían en los siguientes seis meses, y que varios directores del banco tendrían reducciones salariales de entre un 10% y un 30%.

# FRAUDE FINANCIERO

¿Se puede perder tanto dinero sin que nadie se percate?