



# Gestión de Operaciones en Empresas de Servicios Financieros

## Sesión 3

### Julio 2019

Econ. Alejandro Bazo Bertrán, MSc  
[bazo.alejandro@gmail.com](mailto:bazo.alejandro@gmail.com)  
<http://alejandrobazo.blogspot.pe/>

# 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



## **Citigroup reporta fraude en unidad en México.**

- Involucra alrededor de US\$ 585 millones en créditos a corto plazo extendido por Banamex a Oceanografía SA de CV, una compañía mexicana de servicios petroleros que ha sido proveedor de Pemex.
- Citigroup extendió crédito a la compañía petrolera mexicana Oceanografía SA de CV a través de Banamex, que era un proveedor clave de la estatal Petróleos Mexicanos.
- A principios de febrero de 2014 el gobierno mexicano suspendió a Oceanografía de la posibilidad de recibir nuevos contratos. Entonces Citigroup y Pemex revisaron su exposición financiera ante Oceanografía.
- Pemex dijo que encontró fraudes en las cuentas por cobrar registradas por Banamex.

## Citigroup reporta fraude en unidad en México.

### Motivos:

- Errores críticos en el otorgamiento de préstamos, en contratos y gestión de riesgos, así como deficiencias en auditorías hicieron posible el fraude contra Banamex por parte de la empresa Oceanografía.

## **Citigroup reporta fraude en unidad en México.**

### **Consecuencias:**

- Baja en la cotización de sus acciones
- Coordinaciones con clientes (PEMEX y otros)
- Citaciones de reguladores locales (Senado, Fiscalía General, Comisión Nacional Bancaria y de Valores, Procuraduría General de la República –PGR- y el Servicio de Administración y Enajenación de Bienes –SAE-)
- Citaciones de reguladores norteamericanos (Departamento de Justicia, FBI, Comisión del mercado de Valores –SEC-, Corporación Federal de Seguro de Depósitos –FDIC- y de la Fiscalía Federal de Massachusetts)

## Citigroup reporta fraude en unidad en México.

### Consecuencias:

- Sanciones contra el banco debido a su carencia de controles internos eficientes.
- La CNBV entrevistó a empleados, revisó sus manuales de crédito y los contratos realizados con Pemex, entidad que dio a conocer que Oceanografía operaba con irregularidades desde el 2006, esto luego de detectar inconsistencias en 43 de los 85 convenios entre las dos entidades.
- Se ha dado a conocer la falsificación de documentos realizada por la proveedora de Pemex, originada en el centro de negocios e hipotecario de Banamex en Villahermosa, Tabasco, donde también se autorizó la salida de los USD.400'MM (el funcionario responsable está prófugo).
- Una investigación interna determinó que hubo un control laxo y créditos fraudulentos en su filial mexicana Banamex, de acuerdo con un comunicado interno enviado a sus empleados.
- El caso ha costado el puesto a 12 empleados en la filial mexicana de Citigroup, así como a Salvador Villar y Francisco Moreno, quienes se encargaban de manejar las operaciones de Banamex en Estados Unidos, aunque no se fijaron cargos judiciales en su contra.

## ¿Qué es riesgo?

- Es el potencial de impacto adverso que eventos esperados o inesperados pueden tener sobre el capital y las ganancias.
- Incertidumbre acerca de los eventos y/o de sus efectos que pudiesen tener un impacto material en las metas de la organización
- Inquietud de la gerencia sobre los efectos probables de un ambiente incierto
- Típicamente lo llamamos:
  - ¿Qué puede ir mal?
  - ¿Qué puede fallar?



## Determinación del riesgo

- Análisis e identificación por parte de la gerencia de los riesgos pertinentes para alcanzar o lograr las metas y objetivos fijados  
Interno / externo  
Los riesgos están en cambio constante
- Determinar la magnitud del riesgo
- Determinar la probabilidad o frecuencia en que el riesgo puede ocurrir
- Determinar qué acciones se deben llevar a cabo para manejar el riesgo (costo versus beneficio)





**PROBLEMA**

87%  
probabilidad  
de padecer  
cáncer de  
mama



**RESULTADO**

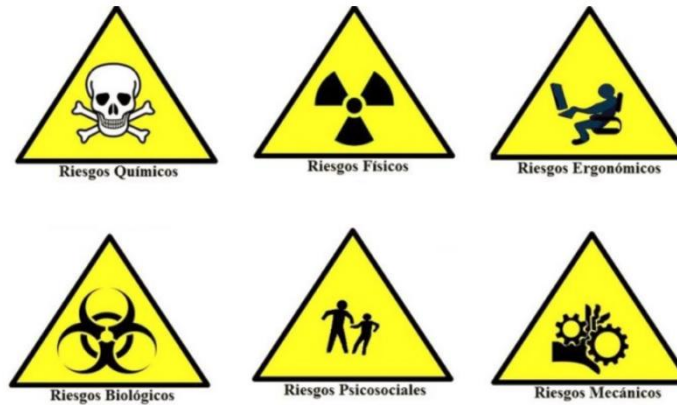
Luego de la  
cirugia la  
probabilidad  
se redujo a  
5%

## La mastectomía de Angelina Jolie

Nuevos riesgos asumidos:

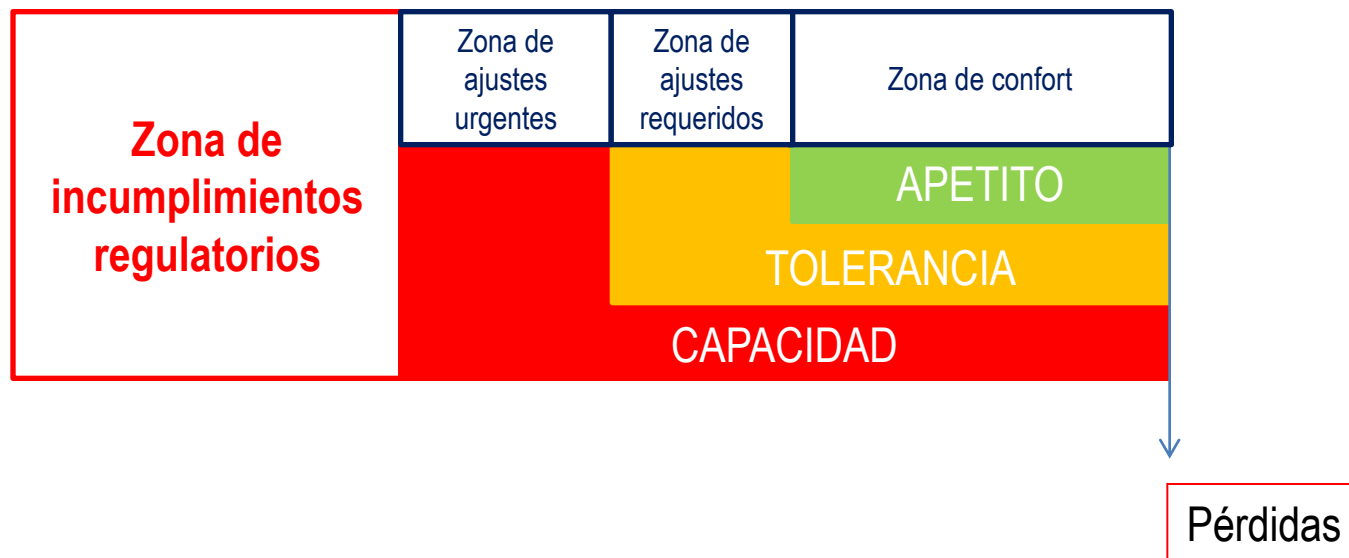
- No podrá amamantar luego de la operación;
- Reducirá la sensibilidad en los senos;
- Riesgo de padecer depresión y ansiedad; y,
- No reduce en 100% el riesgo de padecer cáncer.

¿Riesgo? ¿de qué? ¿dónde está?



## Riesgo inherente

- Es el potencial de ocurrencia que tiene un evento adverso de suceder si el factor de riesgo no es propiamente controlado
- Se fundamenta en los factores principales de riesgo que son manejados por la empresa o negocio
- Dependiendo de la probabilidad de ocurrencia se pueden clasificar en alto, medio o bajo.
- La clasificación debe hacerse basado en la premisa que el riesgo existe, sin importar cuan efectivo sea el ambiente de control





¿Los tenemos identificados?

## **GESTIÓN INTEGRAL DE RIESGOS**

Es el proceso efectuado por el Directorio, los Comités, Gerencia General y el resto del personal, aplicable al establecimiento de estrategias en toda la empresa, diseñado para identificar los eventos potenciales que pueden afectar a la organización, gestionar sus riesgos de acuerdo con su apetito por el riesgo y proporcionar una seguridad razonable para el logro de sus objetivos.



RIESGO ESTRATÉGICO



DIRECCIÓN DE LA  
EMPRESA



RIESGO ESTRATÉGICO

DIRECCIÓN DE LA EMPRESA

RIESGOS FINANCIEROS

RIESGO DE MERCADO:  
RIESGO DE PRECIOS  
RIESGO CAMBIARIO  
RIESGO DE TASA DE INTERÉS  
RIESGO DE COMMODITIES

RIESGO DE LIQUIDEZ

RIESGO DE CRÉDITO

ÁREAS DE RIESGO

RIESGO ESTRATÉGICO

DIRECCIÓN DE LA EMPRESA

RIESGO REPUTACIONAL

ÁREAS DE RIESGO

RIESGOS FINANCIEROS

RIESGO DE MERCADO:  
RIESGO DE PRECIOS  
RIESGO CAMBIARIO  
RIESGO DE TASA DE INTERÉS  
RIESGO DE COMMODITIES

RIESGO DE LIQUIDEZ

RIESGO DE CRÉDITO

RIESGOS OPERACIONALES

RIESGO OPERACIONAL  
RIESGO LEGAL  
SEGURIDAD DE LA INFORMACIÓN  
CYBERSECURITY  
CONTINUIDAD DEL NEGOCIO  
CORRUPCIÓN  
SPLAFT  
CUMPLIMIENTO NORMATIVO

TODA LA EMPRESA

## 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.



## RIESGO ESTRATÉGICO

### 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

# ¿Cuál es tu posesión más valiosa?



¿Tu casa?



¿Tu auto?



¿Tus inversiones?



Más cerca ...  
¿Tu familia?



¿Un recuerdo inolvidable?

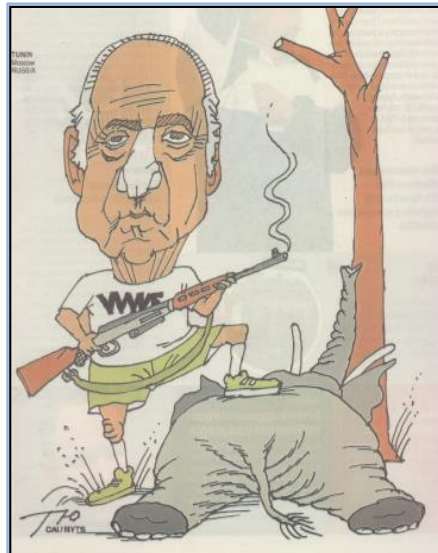


Tu reputación !!!

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.



## RIESGO REPUTACIONAL





## 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 información o en los controles internos”**

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 - 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”.**

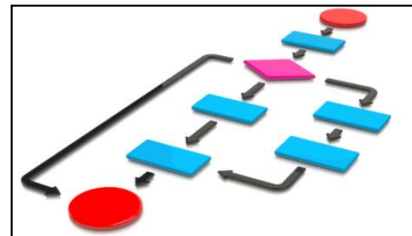
Es decir, se refiere a las pérdidas que pueden causar 4 factores: **personas, procesos, sistemas y factores externos.**

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

# RIESGO OPERACIONAL



Personas



Procesos



Tecnologías de la Información y Comunicaciones (TIC)



Eventos Externos

## FACTORES QUE ORIGINAN EL RIESGO OPERACIONAL

Personas



- La entidad debe gestionar los riesgos asociados a su personal como: la inadecuada capacitación, negligencia, error humano, sabotaje, fraude, robo, paralizaciones, apropiación de información sensible, alta rotación, concentración de funciones, entre otros.
- 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.

## FACTORES QUE ORIGINAN EL RIESGO OPERACIONAL

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

Personas

**FACTORES QUE ORIGINAN EL RIESGO OPERACIONAL**

**Operaciones bursátiles no autorizadas.**

**Ejemplo de pérdidas operacionales por operaciones no autorizadas (en millones de dólares)**

<b>AÑO</b>	<b>ENTIDAD</b>	<b>PÉRDIDAS</b>
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

- 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

- 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

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



La Entidad debe gestionar apropiadamente los riesgos asociados a los procesos internos implementados para la realización de sus operaciones y servicios. Estos riesgos están relacionados con el diseño inapropiado de los procesos, políticas y procedimientos inadecuados o inexistentes que puedan tener como consecuencia el desarrollo deficiente de las operaciones y servicios o la suspensión de los mismos.

## RIESGO OPERACIONAL – FACTORES QUE LO ORIGINAN

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



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

TECNOLOGIA



**Las entidades deben contar con la tecnología de información que garantice la captura, procesamiento, almacenamiento y transmisión de la información de manera oportuna y confiable; evitar interrupciones del negocio (errores en el diseño e implementación de los sistemas, problemas de calidad de la información) y lograr que la información sea íntegra, confidencial y esté disponible para una apropiada toma de decisiones.**

## RIESGO OPERACIONAL – FACTORES QUE LO ORIGINAN

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

EVENTOS  
EXTERNOS



Las entidades deben gestionar los riesgos de pérdidas derivadas de la ocurrencia de eventos ajenos al control de la entidad que pueden alterar el desarrollo de sus actividades. Se deben tomar en consideración los riesgos que implican las contingencias legales, las fallas en los servicios públicos, la ocurrencia de desastres naturales, atentados y actos delictivos, (así como las fallas en servicios críticos provistos por terceros\*).



## RIESGO OPERACIONAL – FACTORES QUE LO ORIGINAN

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.

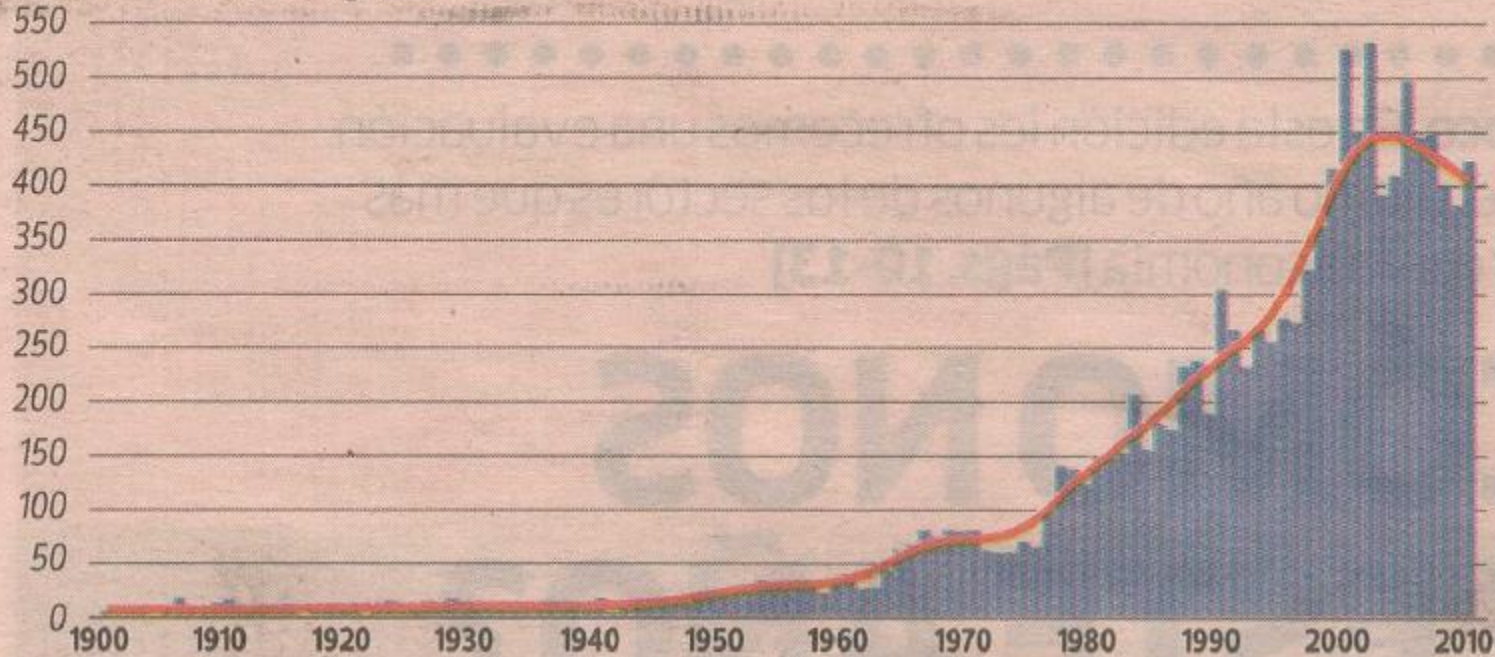
## RIESGO OPERACIONAL – FACTORES QUE LO ORIGINAN

Fuente: El Comercio, Portafolio, 28/Jul/2013

Los desastres naturales en el mundo se multiplicaron en 8 veces en las últimas 5 décadas.

### Desastres naturales registrados en el mundo, 1900–2010

Número de desastres registrados





**LONDON INTERBANK OFFERED RATE  
(LIBOR)**

## LONDON INTERBANK OFFERED RATE (LIBOR)



## LONDON INTERBANK OFFERED RATE (LIBOR)

Año 2007  
*Financial Times* revela  
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 Citigroup	Culpable de 8 acusaciones de conspiración para cometer fraude	10 años	<p>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.</p> <p>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)</p>

(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).

# GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (GSI)

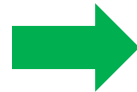


# GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

## ¿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 LA SEGURIDAD DE LA INFORMACIÓN



## Dominios de la Seguridad de la Información

1. Políticas y Organización de la GSI
2. Gestión de Activos y clasificación de información
3. Seguridad del Personal
4. Seguridad Lógica
5. Seguridad Física y Ambiental
6. Seguridad de Operaciones y Comunicaciones
7. Seguridad en la Adquisición, Desarrollo y Mantenimiento de Sistemas
8. Gestión de Incidentes de SI
9. Cumplimiento Normativo
10. Privacidad de la Información
11. Procedimiento de Respaldo

# GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

## Dominios de la Seguridad de la Información

### 1. Política y Organización de GSI



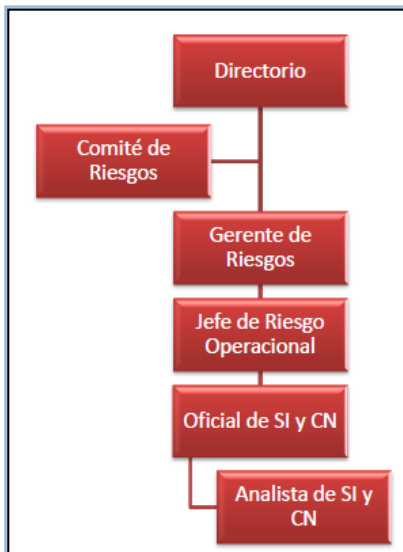
**Reglas aplicadas a las actividades relacionadas al manejo de información de una entidad.**

- Manual aprobado por el Directorio, incluyendo políticas de administración de sistemas, roles responsabilidades de la GSI, procedimientos y estándares, 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.



## Dominios de la Seguridad de la Información

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



### 3. Seguridad de Personal



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.

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.

#### 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.

## 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.

## 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.





## 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: Aplicación de la Protección de datos personales, sobre la confidencialidad 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 LA CIBERSEGURIDAD

¿Qué es la Ciberseguridad?



# GESTIÓN DE LA CIBERSEGURIDAD

## ¿Qué es la Ciberseguridad?

Algunos la llaman Seguridad Informática. Se refiere a la protección de la infraestructura computacional y lo relacionado con ella.

Es un tema de cada vez mayor importancia en la tecnología, para las grandes, medianas, y pequeñas empresas, así como también para los usuarios.

ISACA (Information Systems Audit and Control Association) define la ciberseguridad como una capa de protección para los archivos de información, a partir de la que se trabaja para evitar todo tipo de amenazas, las cuales ponen en riesgo la información que es procesada, transportada y almacenada en cualquier dispositivo.

La ciberseguridad trata de trabajar en robustos sistemas que sean capaces de actuar antes, durante y después, no sirve solo para prevenir, sino también dar confianza a los clientes y al mercado, pudiendo así reducir el riesgo de exposición del usuario y de los sistemas.

## GESTIÓN DE LA CIBERSEGURIDAD

- **Protección contra código malicioso malware:** Antivirus imprescindible para cualquier organización, sin importar su actividad o tamaño, además es importante ir mas allá de sistemas informáticos, puesto de trabajos o servidores, y reunir todos los aspectos que se relacionan con la movilidad. La gran cantidad de distintos tipos de malware y su evolución, se transforman en una de las amenazas más difíciles de lidiar.
- **Protección antifraude o phishing:** El engaño, se ha convertido en una de las prácticas más usadas en internet, tanto para infectar dispositivos, como para conseguir datos de los usuarios. Es necesario contar con el sentido común y desconfiar de lugares sospechosos (capacitación).

## GESTIÓN DE LA CIBERSEGURIDAD

- **Prevenir:** Conseguir la supervivencia de la organización después de un inconveniente de seguridad. Por ejemplo, copias de seguridad en la nube o en otros dispositivos, que mantengan a salvo la información de la empresa, la cual es indispensable para poder desempeñar sus funciones. También existen otras soluciones como las herramientas de recuperación de sistemas, la cual permiten restaurar un sistema desde un punto desde antes del ataque para perder el menor número posible de datos.
- **Protección de comunicaciones:** Estas soluciones se encargan de proteger a la organización de un grupo de amenazas, como los ataques de denegación de servicio, accesos no autorizados o la interceptación de las comunicaciones. Hay que tener en cuenta que las amenazas no solo pueden partir de Internet, sino también del interior de las empresas.



SEGÚN ENCUESTA REALIZADA POR EY

# La mitad de ejecutivos cree que ciberataques a firmas son originados por los empleados

La fuente de los ciberataques a empresas, para el 49% de gerentes de sistemas y de seguridad de la información, son los propios trabajadores, que lo hacen adrede o por descuido.

**FIORELLA MENDOZA HIDALGO**  
fiorella.mendoza@dianogestion.com.pe

La mitad de los ejecutivos peruanos que participaron en una encuesta global de seguridad de la información coincidieron en que sus propios empleados originan los ciberataques que afectan a las empresas.

Así, de acuerdo con el sondeo, el 26% de los ejecutivos considera que los ciberataques son originados por empleados maliciosos, y el 23% cree que la fuente son los empleados descuidados.

Como empleados maliciosos se define a aquellos que, adrede, realizan ataques informáticos en la empresa en la que trabajan, detalló Elder Cama, socio de Consultoría en EY Perú.

En tanto, los empleados descuidados, pese a recibir

capacitación preventiva, resultan víctimas de ciberataques.

## Evaluaciones

Un 25% de encuestados asegura que sus socios, proveedores y contratistas protegen la información de su empresa mediante evaluaciones efectuadas por seguridad de información, dijo Cama.

Añadió que estas evaluaciones se realizan, en muchas ocasiones, contratando a hackers "éticos", que ponen a prueba la seguridad de la empresa al intentar acceder a su información más valiosa.

**22%**

**DE EJECUTIVOS** encuestados a nivel global considera que quienes originan ciberataques son empleados descuidados.

**52%**

**DE ENCUESTADOS** cree que se debe priorizar la inversión en asegurar datos en la nube.

Además, el 58% consideró que el directorio de las empresas no entiende de modo integral los alcances de la seguridad de información, aunque afirma que existen planes de mejora.

## Madurez incipiente

Asu vez, el 46% de encuestados afirmó que el estado de madurez digital en el Perú se encuentra "encaminado", es decir, que su organización está en ruta hacia ese objetivo pero aún tiene claras oportunidades de mejora.

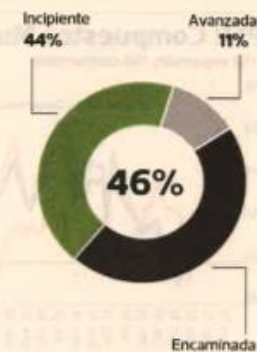
Sin embargo, el 44% consideró que ese grado de digitalización se encuentra en fase incipiente.

Además, el reporte indicó que para el 21% de los encuestados la información más valiosa que buscan obtener los cibercriminales son los planes estratégicos de la empresa, el 19% considera que buscan información personal de sus clientes y el 17% que pretenderían acceder a información de investigación y desarrollo.



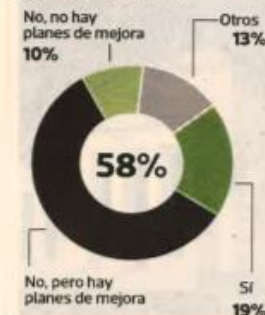
**Avance.** Para el 44% de los ejecutivos, el grado de madurez digital de su empresa es incipiente.

## Estado de madurez digital en el Perú



FUENTE: EY Perú

## ¿El directorio entiende la seguridad de la información?



FUENTE: EY Perú

SEGÚN OPTICAL NETWORKS

## Empresas dedican 20% de su presupuesto de TI en ciberseguridad

Sectores financiero, consumo masivo y educación son los más afectados por ataques cibernéticos.

El año pasado se registraron 21,800 ataques cibernéticos en el país. Esto equivale a 60 ataques por día.

Según una encuesta de Optical Networks realizada a medianas y grandes empresas, solo el 30% de ellas ha realizado un diagnóstico sobre vulnerabilidad de sus sistemas informáticos.

“Lo primero que debe hacer una empresa es priorizar

sus activos más valiosos y direccionar su presupuesto dependiendo de cuánto quiere mitigar el riesgo”, explica Víctor Jáuregui, director comercial de Optical Networks.

En esa línea, comentó que los sectores más afectados durante el 2018 fueron el fi-



Hubo 21,800 ataques en el 2018.

nanciero, consumo masivo y educación.

Asimismo, el 30% de las empresas encuestadas dedican entre 10% y 20% del presupuesto de Tecnologías de la Información (TI) en soluciones de ciberseguridad. Sin embargo, el 95% afirma

que aumentaría ese presupuesto si es que sufre un ataque cibernético.

“Ahora no se habla solo de Internet, sino de un Internet seguro. Por ello, las empresas deben capacitar a sus trabajadores sobre los riesgos que pueden sufrir en la nube”, afirma.

Fuente: Diario Gestión, 27/Feb/2019, Pág. 9



## FUGA INFORMÁTICA

# Hacker que robó 620 millones de datos, volvió por 127 millones más

El mismo pirata informático que usurpó 620 millones de registros de usuarios de 16 diferentes sitios web, a lo largo del año pasado, robó recientemente otros 127 millones de datos de más de ocho plataformas, señala el portal web de Techcrunch.

Anteriormente, divulgó información por US\$ 20 mil en bitcoin de la Deep Web. Ahora, tiene data de diversos sitios importantes como de MyFitnessPal y YouNow. De esta plataforma cuenta más de 151 millones de datos y 25 millones de Animoto.



Sin embargo, otros sitios web como 500px y Coffe Meets Bagel, aún no confirman la fuga de información.

El Registro, página especializada en tecnología del Reino Unido, afirma que por primera vez se filtraron los datos, incluidos nombres completos, correo electrónico, dirección exacta, contraseñas y, en algunos casos, información de inicio de sesión. En total, el pirata informático está vendiendo el contenido por unos US\$ 14,500 en bitcoins.

Fuente: Diario Gestión, 15/Feb/2019, Pág. 30



## Encuesta Global de Seguridad de la Información

¿La ciberseguridad es algo más que protección?

La Encuesta Global de Seguridad de la Información (GISS) de EY del 2019 muestra que la ciberseguridad continúa aumentando la agenda del Directorio. Las organizaciones están gastando más en ciberseguridad, dedicando cada vez más recursos a mejorar sus defensas y trabajando más arduamente para integrar la seguridad mediante el diseño.

Fuente: <https://www.ey.com/pe/es/issues/ey-encuesta-global-seguridad-informacion>

Febrero 2019

## 1. Proteger la empresa

Un número significativo de organizaciones (77%) todavía están operando con solo ciberseguridad y resiliencia limitadas. Es posible que ni siquiera tengan una idea clara de qué y dónde se encuentran sus activos y la información más importante, ni tienen las garantías adecuadas para proteger estos activos.

## 2. Optimizar la ciberseguridad

Menos de 1 de cada 10 organizaciones dicen que su función de seguridad de la información actualmente satisface plenamente sus necesidades, y muchas están preocupadas de que aún no se estén realizando mejoras vitales. Las empresas más pequeñas tienen más probabilidades de quedarse atrás. Mientras que el 78% de las organizaciones más grandes dicen que su función de seguridad de la información está satisfaciendo al menos parcialmente sus necesidades, eso se reduce a solo el 65% entre sus contrapartes más pequeñas.

Fuente: <https://www.ey.com/pe/es/issues/ey-encuesta-global-seguridad-informacion>

Febrero 2019

### 3. Habilitar el crecimiento

Las organizaciones ahora están convencidas de que cuidar el riesgo cibernético y desarrollar la ciberseguridad desde el principio son imperativos para el éxito en la era digital. El enfoque ahora también debe estar en cómo la ciberseguridad apoyará y permitirá el crecimiento empresarial. Para integrar la seguridad en los procesos de negocios desde el inicio y crear un entorno de trabajo más seguro para todos. La seguridad por diseño debe ser un principio clave a medida que las tecnologías emergentes se mueven en el centro de la escena.

Fuente: <https://www.ey.com/pe/es/issues/ey-encuesta-global-seguridad-informacion>

Febrero 2019



**39%**

indica que menos del 2% de sus equipos de TI trabaja únicamente en ciberseguridad

Latam | Perú  
**27%** | **16%**

de las organizaciones considera regularmente la seguridad de la información en sus estrategias y planes de negocio

Global | Latam | Perú  
**53%** | **29%** | **3%**

han observado un incremento en el presupuesto este año

Global | Latam | Perú  
**65%** | **42%** | **7%**

prevén un aumento en su presupuesto el próximo año

Fuente: <https://www.ey.com/pe/es/issues/ey-encuesta-global-seguridad-informacion>

Febrero 2019



## CASO PRÁCTICO: BARINGS BANK (1995)

### 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.

Enero de 1995

DO	LU	MA	MI	JU	VI	SA
25	26	27	28	29	30	31
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31	1	2	3	4

Febrero de 1995

DO	LU	MA	MI	JU	VI	SA
29	30	31	1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	1	2	3	4
5	6	7	8	9	10	11

## CASO PRÁCTICO: BARINGS BANK (1995)

### 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 6.5 años de prisión.
- Escribió su autobiografía *Rogue Trader* (Trader granuja).





## CASO PRÁCTICO: BARINGS BANK (1995)

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

¿Qué clase de riesgos no fueron apropiadamente controlados? ¿Cuáles son riesgos operacionales? ¿Hubo un apropiado manejo de las señales de alerta?

¿Qué es el riesgo moral?

¿Cuál debe ser el rol de los reguladores?

Describa y discuta los riesgos que no fueron controlados y qué controles hubiera establecido usted. Respecto del riesgo operacional aplique los factores de riesgo.

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

Utilice los 4 factores de Riesgo Operacional

## CASO PRÁCTICO: BARINGS BANK (1995)

### 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).



Video: Barings Bank

¿Qué falló en un banco tan antiguo?

## CASO PRÁCTICO: BARINGS BANK (1995)

**¿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.

## CASO PRÁCTICO: BARINGS BANK (1995)

*¿Qué lecciones nos deja este caso?*





# Gestión de Operaciones en Empresas de Servicios Financieros

## Sesión 3

### Julio 2019

Econ. Alejandro Bazo Bertrán, MSc  
[bazo.alejandro@gmail.com](mailto:bazo.alejandro@gmail.com)  
<http://alejandrobazo.blogspot.pe/>



# Gestión de Operaciones en Empresas de Servicios Financieros Julio 2019

Econ. Alejandro Bazo Bertrán, MSc  
[bazo.alejandro@gmail.com](mailto:bazo.alejandro@gmail.com)  
<http://alejandrobazo.blogspot.pe/>



## **ECONOMISTA ALEJANDRO BAZO BERTRÁN, MSc**

Economista de la USMP

Egresado del MBA de la UPC

Magíster en Dirección de Tecnologías de la Información de ESAN

Magíster en Dirección de Tecnologías de la Información de la Universidad Ramón Llull – La Salle, Barcelona

Consultor empresarial independiente (actualidad)

Coordinador General de BURSEN – Centro de Estudios Financieros de la BVL (actualidad)

Gerente General de EDPYME GMG Servicios Perú (2012-2016)

Gerente General de NCF Consultores (actual Grupo Diviso) (2012)

Director de CAVALI ICLV(2010 – 2012)

Gerente de Operaciones, Control Interno y Administración de Scotia Bolsa (2007 – 2012)

Vicepresidente Residente de Operaciones en Citibank Perú (1997 – 2007)





## Objetivo general del curso

**Proveer herramientas para cumplir adecuadamente con estándares operacionales en las empresas de servicios financieros que permitan el desarrollo de sus operaciones de manera eficaz, eficiente y controlada.**

Quiere decir, que sabemos qué está pasando y que podemos vivir tranquilos

## Objetivos al finalizar el curso

- Conocer e implementar estándares (reglas, políticas, recomendaciones mínimas a seguir para asegurar un entorno controlado)
- Documentar apropiadamente los procesos
- Identificar los riesgos de los procesos
- Identificar los controles asociados a los procesos
- Tener una guía para el desarrollo/mejora de los procesos de innovación
- Analizar el costo/beneficio en el diseño apropiado de los procesos

«En la actualidad, la experiencia del cliente y la del empleado son dos fuerzas motoras de las empresas. De manera independiente, cada función conduce a tener vínculos valiosos –con los clientes y los empleados-, pero cuando la experiencia del cliente y la del empleado se manejan juntas, generan una ventaja competitiva excepcional y sustentable»

Fuente: Lee Yohn, Denise, Diario Gestión, 24/06/2019, 28.



**Existen muchos riesgos a los que nos exponemos al momento de desarrollar los procesos de la empresa y en base a nuestras decisiones de innovación**

Temas relevantes en la gestión de operaciones en el sistema financiero:

- Planificación / Gobernanza
  - Capacitación
- Análisis Costo/Beneficio (BIA)
- Matrices y mapas de riesgo
  - Indicadores de gestión
- Información y transparencia

Conceptos que nos acompañan a lo largo de todo lo que hacemos

## CASO PRÁCTICO: BARINGS BANK (1995)

### 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.

Enero de 1995

DO	LU	MA	MI	JU	VI	SA
25	26	27	28	29	30	31
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31	1	2	3	4

Febrero de 1995

DO	LU	MA	MI	JU	VI	SA
29	30	31	1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	1	2	3	4
5	6	7	8	9	10	11

## CASO PRÁCTICO: BARINGS BANK (1995)

### 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 6.5 años de prisión.
- Escribió su autobiografía *Rogue Trader* (Trader granuja).





## CASO PRÁCTICO: BARINGS BANK (1995)

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

¿Qué clase de riesgos no fueron apropiadamente controlados? ¿Cuáles son riesgos operacionales? ¿Hubo un apropiado manejo de las señales de alerta?

¿Qué es el riesgo moral?

¿Cuál debe ser el rol de los reguladores?

Describa y discuta los riesgos que no fueron controlados y qué controles hubiera establecido usted. Respecto del riesgo operacional aplique los factores de riesgo.

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

Utilice los 4 factores de Riesgo Operacional

## CASO PRÁCTICO: BARINGS BANK (1995)

### 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).



Video: Barings Bank

¿Qué falló en un banco tan antiguo?

## CASO PRÁCTICO: BARINGS BANK (1995)

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

Nick Leeson era una persona ambiciosa	¿Está mal ser ambicioso? ¿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” Incremento de ganancias pero, ¿reduciendo los niveles de riesgo? (expectativa de bonificaciones)

**CASO PRÁCTICO: BARINGS BANK (1995)**

**¿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 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 Señales de alerta son obviadas Falta de seguimiento de indicadores
Falta de normas, políticas y procedimientos	¿Son suficientes las auditorías externas? ¿Funcionan las auditorías internas?	¿Cómo nos protegemos de la falsificación de documentos?

## CASO PRÁCTICO: BARINGS BANK (1995)

**¿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.

## CASO PRÁCTICO: BARINGS BANK (1995)

*¿Qué lecciones nos deja este caso?*



## **Objetivos de la gestión de operaciones en empresas de servicios financieros**

- Generar mayores ingresos para la empresa
- Generar menores gastos para la empresa
- Reducir la exposición a riesgos para la empresa

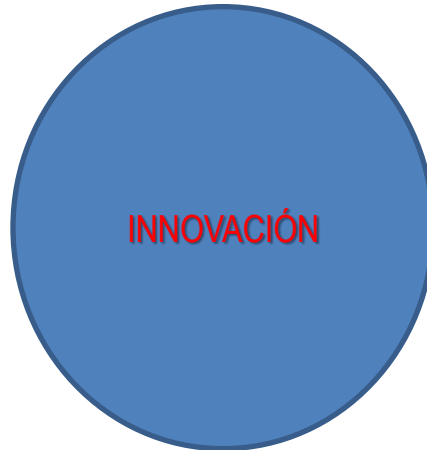
### **Para ello buscamos generar mejoras en la:**

- Satisfacción al cliente
- Satisfacción del colaborador
- Satisfacción del accionista
- Imagen y reputación de la empresa



## ¿Quiénes son los responsables de la gestión de operaciones en empresas de servicios financieros?

Todos somos los responsables en el campo de acción que nos compete



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

La innovación en las  
empresas debe generar  
rentabilidad

*“Aún sigue válida, contra muchos pronósticos, la Ley Moore (que establece una duplicación del desempeño relativo de las computadoras cada 18 meses). De ahora al 2025, hay para no menos de seis duplicaciones sucesivas de potencia. Ello resulta en un múltiplo de 64, difícil de visualizar en la práctica. Ello implicaría, por ejemplo, que las computadoras en el 2025 podrían ser, a la vez cuatro veces más potentes, cuatro veces más baratas y cuatro veces más pequeñas (requerirán, por tanto, cuatro veces menos energía) que las actuales. Para no referirnos a las mejoras que se lograrían en big data, robótica, biología sintética, sistemas de renovación energética, impresión 3D, inteligencia artificial y demás. Todo ello transformará de manera muy significativa el aprendizaje, el trabajo y el entretenimiento.*

*Hay pronósticos que constituyen un desafío a nuestro entendimiento del mundo. Por ejemplo, respecto de la salud. Vinod Khosla, fundador de Sun Microsystems, pronostica que para el 2025 el 80% de lo que los médicos hacen ahora podrá hacerse mejor y más barato con máquinas”.*

La columna de FOZ. “Anticipando el 2025” por Felipe Ortiz de Zevallos.

Semana Económica, 23/Ago/2015, Pág. 13

## ¿Qué influye en la gestión de operaciones en empresas de servicios financieros?

El mercado / la competencia

El mercado / los sustitutos

La estrategia de la propia empresa

El regulador

**Innovación**

- Creación
- Seguimiento

Los clientes

La tecnología

Los empleados

# Tendencias

INNOVACIÓN - FINTECH



Fuente: Diario Gestión, 21/Feb/2019, Pg. 1

SERÁN REGULADAS POR SMV

## Se exigiría un capital mínimo a las fintech para que puedan operar

Norma regularía las obligaciones, responsabilidades y prohibiciones de las fintech dedicadas al financiamiento colectivo (crowdfunding). Tendrían plazo máximo para recabar financiamiento de proyectos.

OMAR MANRIQUE P.  
omar.manrique@diariogestion.com.pe

Ya existe un proyecto de ley para regular a las fintech de financiamiento participativo o crowdfunding, reveló la gerente central de Operaciones del Banco Central de Reserva (BCR).

Marylin Choy precisó que el proyecto de ley tiene como finalidad regular a las fintech dedicadas a esquemas de financiamiento colectivo de préstamos de préstamos o de inversión a través de plataformas electrónicas, poniéndolas bajo el ámbito de regulación y supervisión de la Superintendencia del Mercado de Valores (SMV).

El crowdfunding es un mecanismo a través del cual un proyecto puede ser financiado con la participación de varias personas, ya sea como inversionistas o como prestamistas, refirió la funcionaria a Procapitales.



Otras fintech. También serán reguladas conforme crezcan en volumen, adelantó Choy.

De acuerdo con fuentes privadas, actualmente en el país hay aproximadamente 79 fintech operando, que se dedican principalmente a la gestión financiera (27%), pagos y transferencias (25%) y financiamiento (20%). El resto desarrolla actividades vinculadas a cambio de divisas, seguros, calificación de clientes financieros, comercio y financiamiento colectivo, entre otras.

**Plazo máximo**  
La norma en mención regularía las obligaciones, responsabilidades y prohibiciones de las plataformas crowdfunding.

“Además, la norma establecería un capital mínimo para los administradores de la plataforma, el ámbito y las prohibiciones para las operaciones de crowdfunding y la obligación de un plazo máximo para la obtención del financiamiento de un proyecto”, dijo Choy.

La ley establecería la obligación de obtener autorización de la SMV para funcionar, y sería este organismo el encargado de regular, supervisar y sancionar a las fintech que se dediquen a ese rubro de negocio.

### Fintech que operan en el Perú

Clasificación fintech	Empresas que operan	Participación
Medios de pago y transferencias	22	27.2%
Financiamiento	19	23.5%
Cambio de divisas	18	22.2%
Soluciones financieras para empresas	5	6.2%
Finanzas personales y asesoría financiera	5	6.2%
Infraestructura para servicios financieros	4	4.9%
Seguros	3	3.7%
Crowdfunding	2	2.5%
Mercado de capitales	2	2.5%
Criptodivisas	1	1.2%
<b>Total</b>	<b>81</b>	<b>100.0%</b>

Fuente: Fintech Perú

**81**  
**FINTECH** operan en el mercado local, según estadísticas de Fintech Perú.

**17**  
**MINUTOS** toma, en promedio, hacer una conversión de divisas en una casa de cambio digital.



TECNOLOGÍA EN PRÁCTICAS FINANCIERAS

## Panorama del mercado de fintech en la región

### Países con más fintech

		# de entidades
1	Brasil	380
2	México	273
3	Colombia	148
4	Argentina	116
5	Chile	84
6	Perú	57
7	Ecuador	34
8	Uruguay	28
9	Venezuela	11

### Distribución de segmentos fintech

# de entidades	% del total
Pagos y remesas	285 / 24.4%
Préstamos	208 / 17.8%
Gestión de finanzas empresariales	181 / 15.5%
Gestión de finanzas personales	90 / 7.7%
Financiamiento colectivo	89 / 7.6%
Tecnologías empresariales para bancos	71 / 6.1%

### Subsegmentación de pagos y remesa

- **37.2%** Pasarelas y agregadores de pago
- **36.8%** Pagos móviles y billeteras electrónicas
- **9.1%** Soluciones de pago móvil en puntos de venta
- **7%** Soluciones de criptomoneda
- **5.3%** Otros
- **4.6%** Transferencias internacionales y remesas

### Crecimiento por país encima de 100%





# El 63% elevó transacciones por uso de la banca móvil

El 50% incrementó adquisición de productos bancarios por uso de este canal tecnológico. El 41% usa con más frecuencia la banca móvil para sus transacciones bancarias.

**MIRTHA TRIGOSO LÓPEZ**  
mtrigoso@diariogestion.com.pe

Los canales tecnológicos que vienen ofreciendo los diferentes bancos para realizar transacciones financieras, haciendo ahorrar a los usuarios tiempo y dinero en desplazamiento, están dinamizando el negocio.

Así, el 63% de los limeños bancarizados señala que ya ha incrementado su número de operaciones o transacciones debido al uso de la banca móvil (de acceso por celular o tableta); mientras que el 54% refiere que ha hecho lo mismo gracias a que puede acceder a la banca por Internet u online (de acceso por una PC), según estudio de ISIL.

“Y es que con estas plataformas pueden acceder varias veces para ver sus saldos y movimientos, así como realizar desde cualquier lugar

## Motivos por los que no usa la banca móvil

(Limeños bancarizados)



FUENTE: ISIL

## LAS CLAVES

■ **Banca móvil.** 54% de los jóvenes entre 18 y 24 años usa este canal. El 47% tiene entre 25 y 35 años.

■ **Estudio.** Muestra de 600 limeños bancarizados entre 18 y 60 años de todos los NSE. El estudio se hizo por encuestas, entre setiembre y octubre del 2018.

transferencias, entre otros servicios”, señaló el gerente de Innovación y Desarrollo de la casa de estudios, José Miguel Marchena.

Pero no solo los canales tecnológicos han incrementado el número de transacciones, sino también la adquisición de productos bancarios.

Según el estudio, el 50% de limeños bancarizados afirma que ha incrementado sus productos financieros (cuentas de ahorro, débito, CTS, entre

otros) debido a la banca móvil, y el 45% lo hizo gracias a la banca por Internet.

## Tarea pendiente

Pese a los beneficios que ofrece la banca móvil, y la online, aún los limeños bancarizados prefieren en un mayor porcentaje acceder a los medios tradicionales de banca para hacer sus transacciones, señaló José Miguel Marchena.

Así, el 87% usa aún con mayor frecuencia los cajeros, el 76% los agentes, el 64% las ventanillas y el 42% la plataforma de los bancos, versus un 41% que opta por la banca móvil y un 29% por la banca online.

“Y los principales motivos para no usar la banca móvil, y la online son no considerarlos seguros y el no saber cómo utilizarlos. Es por ello que los bancos deben capacitar a sus clientes para que aprovechen estos canales tecnológicos”, refirió.

La principal operación que realizan los usuarios en la banca móvil es la consulta de saldos y movimientos (96%), seguida de transferencias (57%).

## II CEO INNOVATION DAY

# “Se debe usar la tecnología para personalizar la oferta”

**PALOMA VERANO**

paloma.verano@diariogestion.com.pe

La mentalidad digital en las grandes corporaciones no debe enfocarse solo en automatizar los procesos. Así lo manifestó Javier Zamora, profesor del IESE Business School y senior lecturer de sistemas de información, quien expuso en el II CEO Innovation Day.

Tradicionalmente, lo que han hecho las empresas cuando acceden al mundo digital es automatizar, de manera que se logre hacer más cosas con menos recursos, sostuvo.

“Pero si solo utilizamos la tecnología para la automatización, ¿cuál es el futuro? Si esa tecnología es cada vez más accesible para mis competidores, ¿cuál va a ser mi ventaja competitiva?”, preguntó en el evento organizado por el PAD de la Universidad de Piura y el IESE Business School.

## Personalizar la oferta

En esa línea, el expositor agregó que la tecnología y la transformación digital se



Javier Zamora.

deben usar de distinta forma a como se viene haciendo, inclusive para ingresar a otro tipo de industrias.

“Debemos utilizar la tecnología para anticiparnos a los cambios, coordinar con otras industrias que antes no estaban abiertas a nosotros, y para personalizar nuestra oferta”, afirmó.

En esa línea, agregó que ahora, con lo digital, las empresas pueden ofrecer un producto masivo altamente personalizado.

“Las compañías pueden utilizar grandes cantidades de datos para satisfacer mejor las demandas del cliente”, puntualizó.

## Tendencias

LUCHA CONTRA LA CORRUPCIÓN

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 Empleado

Conoce a tu Proveedor

Operaciones en efectivo

Operaciones inusuales

Operaciones sospechosas

## ¿Cómo hacemos la gestión de operaciones en empresas de servicios financieros?

- A través de la revisión de la calidad de nuestros procesos
- A través de la revisión de la satisfacción de nuestros clientes (externos/internos)
- A través de la revisión de las fallas de procesos y su corrección
- A través de un sistema de capacitación eficiente
- A través de una apropiada gestión de la imagen/reputación de la organización

## ¿Cómo hacemos la gestión de operaciones en empresas de servicios financieros?

- Identificar los riesgos inherentes de nuestro negocio
- Identificar las actividades de control para cada riesgo
- Probar las actividades de control y asegurar que están trabajando y detectan deficiencias
- Monitoreo continuo de los controles y resoluciones que identifican debilidades
- Reportar nuestros progresos

## 7 preguntas para cuestionar un proceso

- Qué                   What?
- Quién               Who?
- Cuándo           When?
- Dónde             Where?
- Por qué           Why? – 5W
- Cuál               Which?
- Cómo             How?



## Visión de operaciones

- Las operaciones son la piedra angular de un servicio al cliente satisfactorio
- Los estándares operacionales dictan y definen la manera de operar de un negocio
- Se verifica a través de transacciones procesadas en tiempo y sin errores, bajo un ambiente de control adecuado

## Políticas de control

- Identificación de riesgos de control de manera continua
- Establecer controles efectivos
- Practicar controles efectivos
- Verificación periódica de la efectividad de los controles
- Reporte de resultados de las pruebas y los procesos identificados
- Generación de las medidas correctivas correspondientes



## Políticas de control

- Deben ser transversales a los negocios de la empresa, participativas
- Deben establecer indicadores de gestión para monitorear el cumplimiento y/o las desviaciones
- Deben concretar las actividades del negocio de manera ordenada y eficiente
- Deben asegurar el seguimiento de las políticas establecidas
- Deben proteger a las personas, los bienes y los valores del negocio
- Deben asegurar la integridad de la información física y del sistema

## **Políticas de control (riesgos)**

- Error humano, descuido, negligencia
- Aprobaciones no autorizadas
- Fraude o abuso de poder por parte de funcionarios de confianza, responsabilidad y autoridad

## Políticas de control (preguntas)

Para cada tipo de operación, preguntarse:

- ¿Qué cosas pueden ir mal?
- ¿Qué procesos hay vigentes para asegurar que nada va mal?
- ¿Cómo se que los controles aún funcionan?
- ¿Cómo pruebo que estos aún trabajan?
- ¿Cómo administro el cambio y mejoro los procesos?



## ¿Cómo identifico puntos de riesgo?

- Comience con las áreas con el más alto nivel de riesgo
- Determine la función principal de la unidad
- Practique el proceso de transacciones y revise su flujo
- Dialogue sobre los riesgos potenciales que pueden haber
- Para cada riesgo identificado, determine los controles que aseguran que el mismo ha sido tomado en cuenta
- Evalúe si los controles resuelven los riesgos adecuadamente
- Determine las pruebas a realizar periódicamente para verificar que los controles aún funcionan

## ¿Cómo identifico puntos de riesgo?

### Evaluación de proceso y prueba

- Lista de *check-list* de operaciones
- Simulacros, prácticas y pruebas periódicas
- Reportes de excepciones
- Revisiones diarias de reportes de transacciones
- Observaciones regulares de asuntos de auditoría y de negocio

## Reflexión:

**¿Los procesos me avisan oportunamente si algo anda bien o no?**

- Sí
- No
- A veces





## ¿Cómo se obtiene información de los procesos?

A través de revisiones periódicas de los riesgos y de los controles para asegurar que:

- Los controles están funcionando
- Los controles están produciendo resultados

## Categorías de control

- Segregación de funciones
- Independencia de funciones
- Supervisión
- Revisión, autorización y aprobación
- Seguridad de los activos
- Verificación aritmética (conciliaciones y reconciliaciones)
- Política de personal
- Supervisión organizacional y gerencial

## **Para lograr una gestión de operaciones eficiente en empresas de servicios financieros**

- Existe un compromiso gerencial firme («el pescado comienza a apestar por la cabeza»)
- Existen procesos adecuados de evaluación de controles
- Se logra la responsabilidad por los riesgos inherentes
- Los estándares de control son aplicados a todos los negocios
- Los estándares de control se logran con el esfuerzo coordinado de todos en la organización (cada uno en su nivel de responsabilidad)
- Se promueve el trabajo en equipo

## **Para lograr una gestión de operaciones eficiente en empresas de servicios financieros**

- Gerencia (de todos los niveles) proactiva y alentadora  
Los gerentes de negocio son responsables de mantener, revisar y alentar periódicamente un entorno de control
- La gestión de riesgos es un elemento fundamental en la hoja de ruta del negocio
- Identificación y corrección de problemas
- Facilitar las iniciativas de control (no el controlismo)
- Conocimiento amplio de estándares operacionales, riesgo y controles (capacitación constante, reuniones de trabajo, comités)

## **Para lograr una gestión de operaciones eficiente en empresas de servicios financieros**

- Los negocios deben mantener un sistema de control interno (no control independiente o auditoría) que le permita identificar oportunamente los riesgos existentes y los emergentes
- Esto les permitirá establecer controles cuyos costos sean justificados para contener los riesgos (análisis de impacto)

## **Para lograr una gestión de operaciones eficiente en empresas de servicios financieros**

En un escenario ideal, cada negocio implementa y mantiene un programa de revisiones para:

- Probar que los controles internos se cumplen
- Probar que la regulación se cumple
- Asegurar la acción correctiva para contener el riesgo (a tiempo)
- Velar la acción correctiva dirigida a detectar cualquier situación en la que tales acciones no se ejecuten



## Identificación y dimensión del riesgo

- Es responsabilidad de todos, bajo el liderazgo de la gerencia, identificar y cuantificar los riesgos según ocurran los cambios antes y durante la implementación de un producto/sistema nuevo o de un cambio a un producto/sistema
- La identificación de los riesgos debe generar controles (¿siempre?)
- Los riesgos deben ser documentados y sometidos a una inmediata acción correctiva (¿siempre?, ¿quién decide?, ¿cómo?)
- Indicadores de gestión
- Reportes

## Caso - Reestructuración del proceso de envío de estados de cuenta en un agente de intermediación





## Situación:

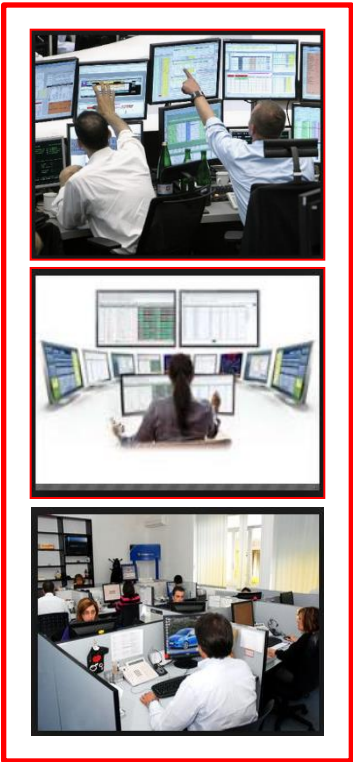
Se requiere de su aprobación para que proceda el siguiente cambio de proceso propuesto por un equipo de mejora de procesos.

Se trata de una empresa agente de intermediación con operaciones en todo el país y recibe la propuesta para el cambio de un proceso para el despacho de los estados de cuenta a los clientes de su institución.

Se pide que evalúe si el cambio es conveniente y emita su informe a fin de implementarlo.

## Consideraciones regulatorias:

- Los estados de cuenta deben ser enviados impresos a los clientes, de manera mensual para clientes que han tenido movimientos y de manera trimestral para clientes que no han tenido movimientos en la cuenta.
- La empresa tiene 30 días calendario para el envío de los estados de cuenta contados a partir del cierre del mes anterior.



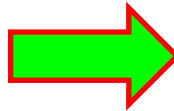
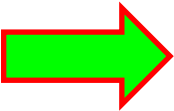
Agente de Intermediación  
Oficina Principal  
Lima

El Área de Operaciones del agente de intermediación entrega a la empresa de Mensajería los estados de cuenta. La empresa de Mensajería los recoge de la Oficina Principal en Lima del agente de intermediación.

Empresa de Mensajería



Distribución de los estados de cuenta en todas las ciudades del Perú a cargo de una empresa de Mensajería. Clientes en Lima y 12 ciudades del interior del país.



Situación actual:  
Los Estados de Cuenta a clientes son remitidos mensualmente a los clientes desde el área de Operaciones en Lima a todo el país.

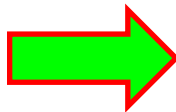
El área de Operaciones envía por vía electrónica los estados de cuenta a cada uno de los Brokers en las oficinas del interior del país. Sólo entrega los que deben ser distribuidos en Lima y Callao a una empresa de Courier local.



Cada Oficina del interior del país, a cargo de un Broker, contrata una empresa de Mensajería local y entrega los estados de cuenta para su distribución en la ciudad correspondiente.



Agente de Intermediación  
Oficina Principal  
Lima



Situación propuesta:  
Los EECC son enviados por correo a los Brokers en cada oficina del interior del país para que estos lo impriman y entreguen a la empresa de Mensajería local que se encargará de su distribución.

**Objetivo del proyecto:**

Reducción de costo de mensajería de USD.50,M mensuales.

**Información Adicional:**

Este AI tiene su oficina principal en Lima: áreas de trading, brokers, control y operaciones.

En el interior del país sus oficinas son de representación y están a cargo de uno o dos brokers.

**Se requiere:**

Usted es el Gerente de Operaciones y tiene que revisar el proceso y aprobarlo.

Evalúe si se trata de un cambio relevante para el proceso, si se está cambiando el perfil de riesgo del proceso y si hay controles complementarios que tomar antes de aprobarlo.

Adicionalmente podrá señalar indicadores o procesos de control adicionales.

Para resolver el caso, podrá hacer los supuestos que considere necesario.



## Caso - Reestructuración del proceso de envío de estados de cuenta en un agente de intermediación



## Controles

- Política de continuidad de negocio
- Política de seguridad de información
- Cumplimiento de requerimientos regulatorios
- Proceso de validación de documentación e información
- Proceso de validación de fondos (AML)
- Proceso anticorrupción
- Separación de funciones
- Doble validación (custodia de bienes y valores)
- Delegación de poderes y nombramiento de funcionarios

## Controles

- Gestión de archivos
- Tercerización de servicios del negocio
- Contratación significativa
- Políticas de gestión de personal (vacaciones)
- Aprobación de desviaciones a las políticas (aceptación del riesgo)

Ejercicio con un proceso que conozco, que me es familiar. Pero también apporto en aquellos que no lo son dando una visión fresca

Cada uno contribuye con su especialización e ideas para luego compartir en la mesa

## **Herramientas para la gestión de operaciones eficiente en empresas de servicios financieros:**

- Ofrecen ayuda al usuario al aplicar las guías de procedimientos
- Ayuda a la gerencia a determinar si se están siguiendo los procedimientos
- Ofrecen información y datos para el análisis al determinar el nivel de cumplimiento de los procedimientos
- Ofrecen información para mejoras, comunicación y estrategias de adiestramiento sobre procedimientos

## Herramientas: Check list

- Crear una lista de preguntas que se respondan con «Si» o «No» a fin de recoger datos y confirmar el desarrollo de determinadas tareas
- La respuesta «Si» indica que las tareas se han desarrollado dentro del procedimiento
- La respuesta «No» indica que las tareas se han desarrollado fuera del procedimiento
- Permiten calcular el nivel de cumplimiento y el progreso
- Permiten establecer planes de acción correctiva

## Herramientas: Check list

- Por cada proceso identificado debe haber entre 5 y 15 preguntas
- Se debe efectuar un análisis de las respuestas «No» a fin de elaborar la explicación y el plan de acción correspondiente
- Son herramientas que pueden ser agregadas con las de otras áreas o unidades de negocio

## Herramientas: Autoevaluación

- Administración proactiva del riesgo
- Identificación y corrección del problema
- Facilitar las iniciativas de control
- Establecer las medidas de seguimiento e indicadores de gestión más apropiados
- Revisión periódica de los procesos
- Reducción de los comentarios de auditorías
- Fortalecimiento del ambiente de control
- Fortalecimiento del equipo de trabajo



## Herramientas: Autoevaluación

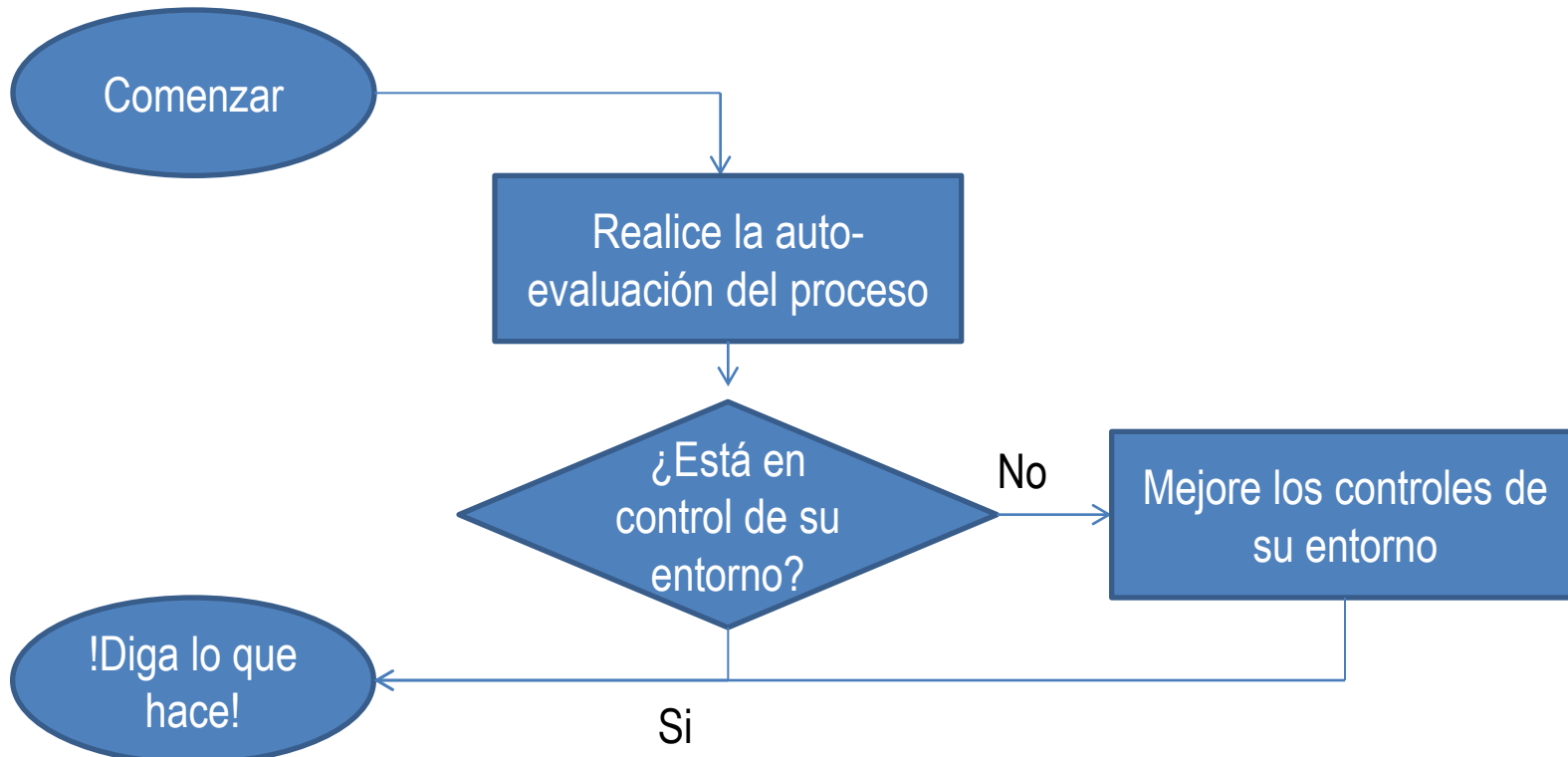
- Busca mantener un sistema de control efectivo
- Identifica riesgos actuales
- Identifica riesgos potenciales
- Establece controles económicamente viables
- Es un proceso continuo

## Herramientas: Autoevaluación (pasos)

1. Identifique los riesgos existentes y/o las áreas de mejora (¿qué puede salir mal?)
2. Dimensione el riesgo (¿qué pasaría si se realiza?)
3. Establezca costo de los controles justificados ante tal exposición (¿cómo lo controlamos?)
4. Identifique errores, deficiencias e irregularidades en los procesos (¿qué está mal?)
5. Plan de acción correctiva (¿cómo lo solucionamos?)
6. Monitoree la acción correctiva (¿dio resultado?)
7. Comunique oportunamente

## Herramientas: Autoevaluación (pasos)

1. Identifique los riesgos existentes y/o las áreas de mejora (¿qué puede salir mal?)



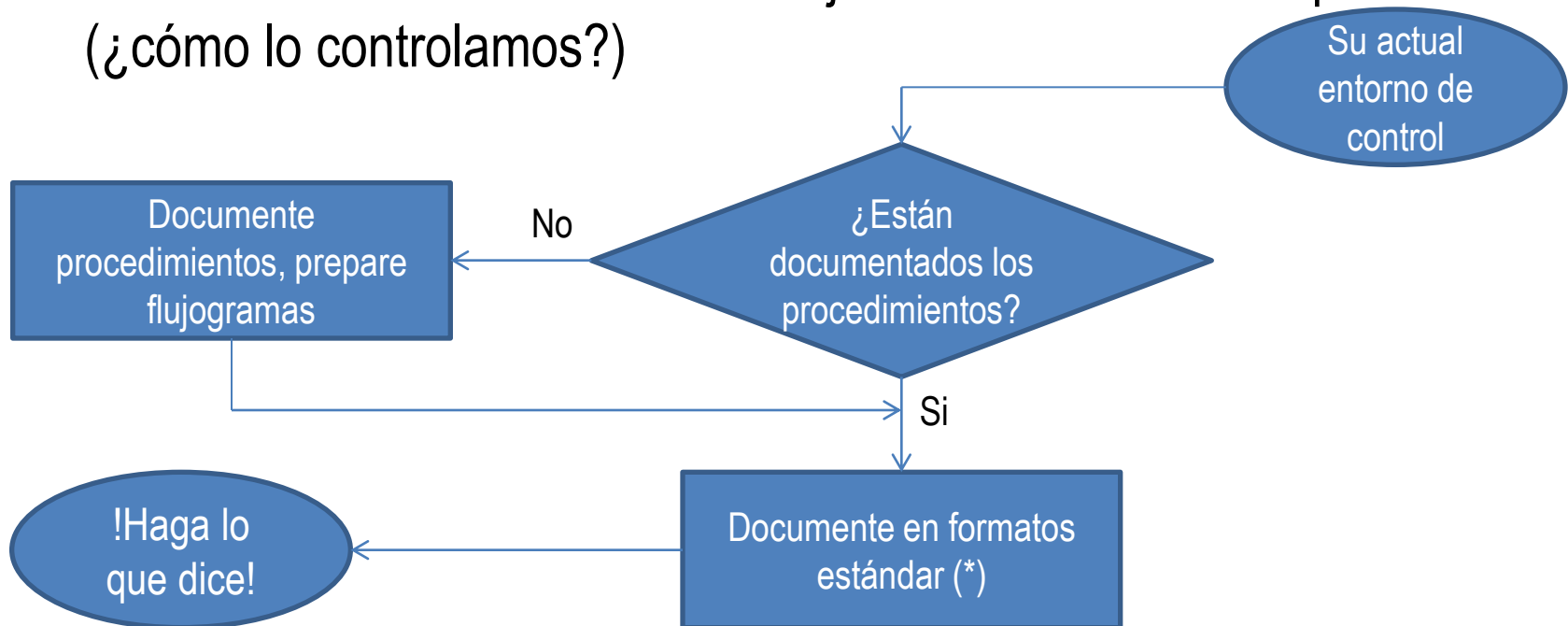
## Herramientas: Autoevaluación (pasos)

Una autoevaluación efectiva le permite satisfacer a sus clientes internos y externos:

- Identifique a sus clientes
- Identifique los estándares que le aplican
- Defina su proceso
- Observe y supervise su desempeño
- Mejore su proceso
- Mida los resultados de la mejora

## Herramientas: Autoevaluación (pasos)

2. Dimensione el riesgo (¿qué pasaría si se realiza?)
3. Establezca costo de los controles justificados ante tal exposición (¿cómo lo controlamos?)



(\*) Si necesita ayuda, ¡ pídale ! Use recursos internos/externos

## Herramientas: Autoevaluación (pasos)

En algún momento puede tener la necesidad de mejorar su trabajo y sus procesos. Esto puede ocurrir si:

- No está cumpliendo con las necesidades y requisitos del clientes
- No ha satisfecho los requisitos internos, de auditoría o de los reguladores
- Simplemente, desea hacerlo mejor

## Herramientas: Autoevaluación

Management by walking around (MBWA)

Similar al *gemba walk* japonés

Práctica en los años '70 implementada por los Ejecutivos de Hewlett-Packard

En 1982 Tom Peters y Robert H. Waterman desarrollan el concepto que también será tratado posteriormente por Peter Draker

Gerentes caminando **sin una estructura** por la operación para consultar con el equipo de trabajadores el estado actual de las operaciones

Le versión **estructurada** será la autoevaluación o self-assessment



## Herramientas: Autoevaluación

- Confirma el cumplimiento de las actividades detectivas y correctivas
- Asegura el cumplimiento de los planes de acción trazados
- Monitorea el cumplimiento y la calidad de las pruebas

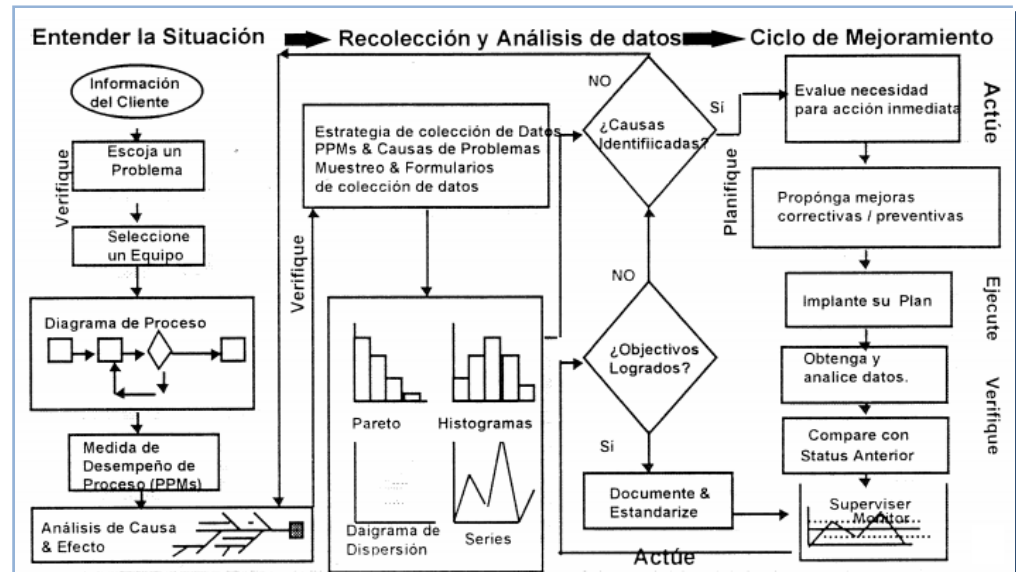
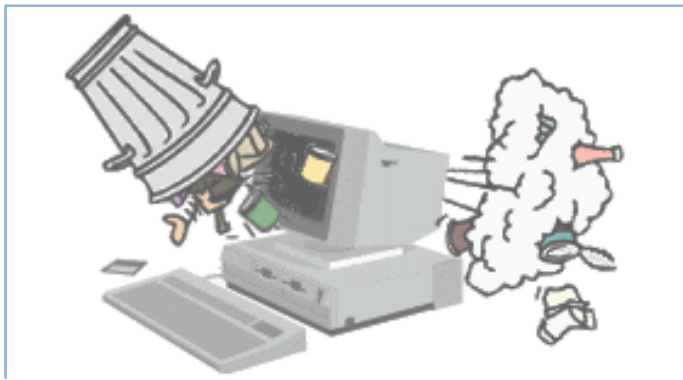
## Herramientas: Autoevaluación

### Responsabilidad:

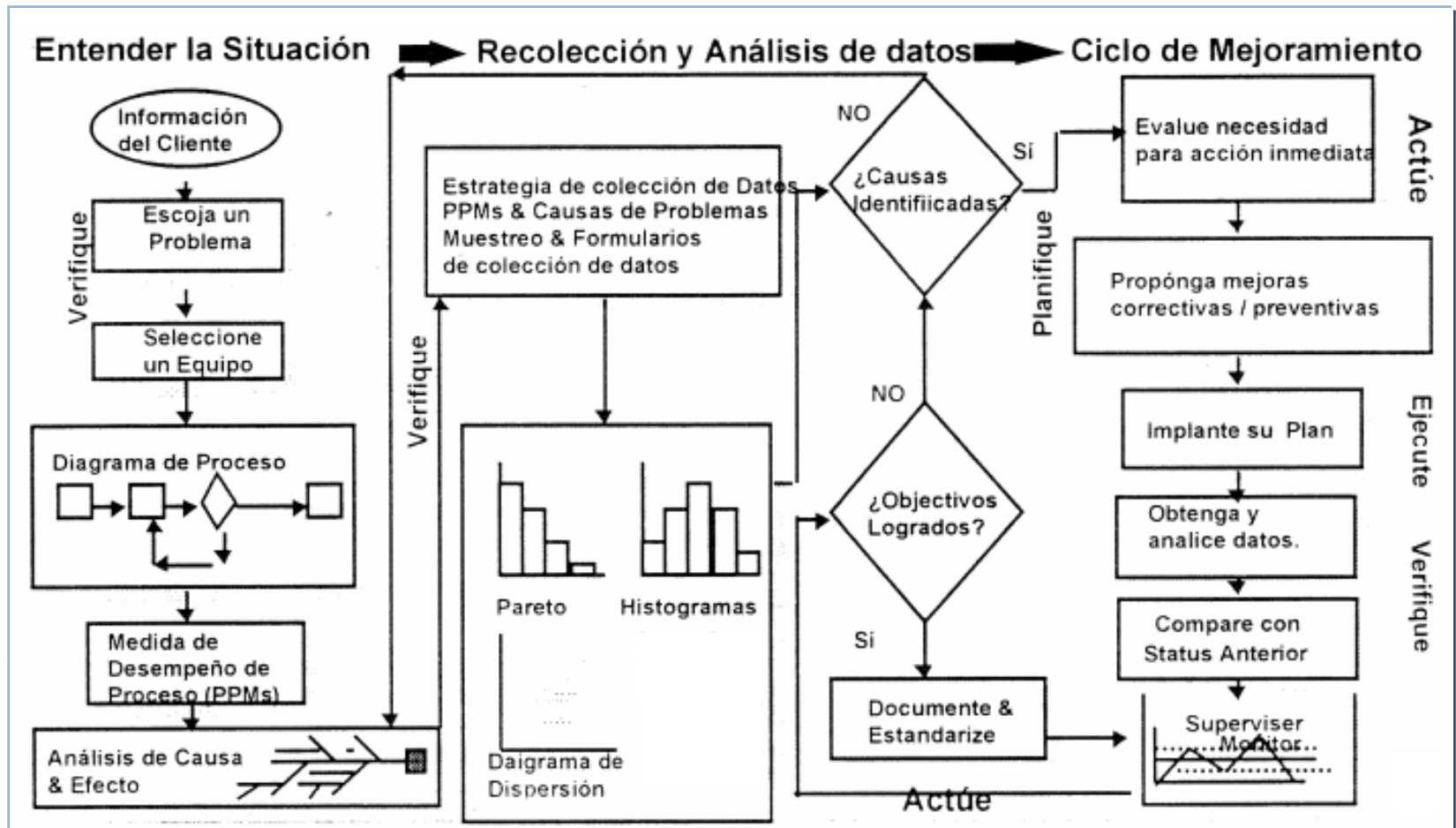
- Monitorear el cumplimiento y la calidad del proceso
- Revisar los procesos y evaluar los riesgos
- Reportar los resultados (no ocultar los problemas potenciales)
- Establecer controles alternativos para mitigar los riesgos
- Hacer el seguimiento de las excepciones
- Hacer una validación periódica
- Entrenar al personal nuevo

## Herramientas: Modelo de mejoramiento de proceso TQM

- Proceso de tres etapas
- Proceso de transformación activa
- Cuando lo que entra es igual a lo que sale, el proceso está de más
- “Garbage in, garbage out”

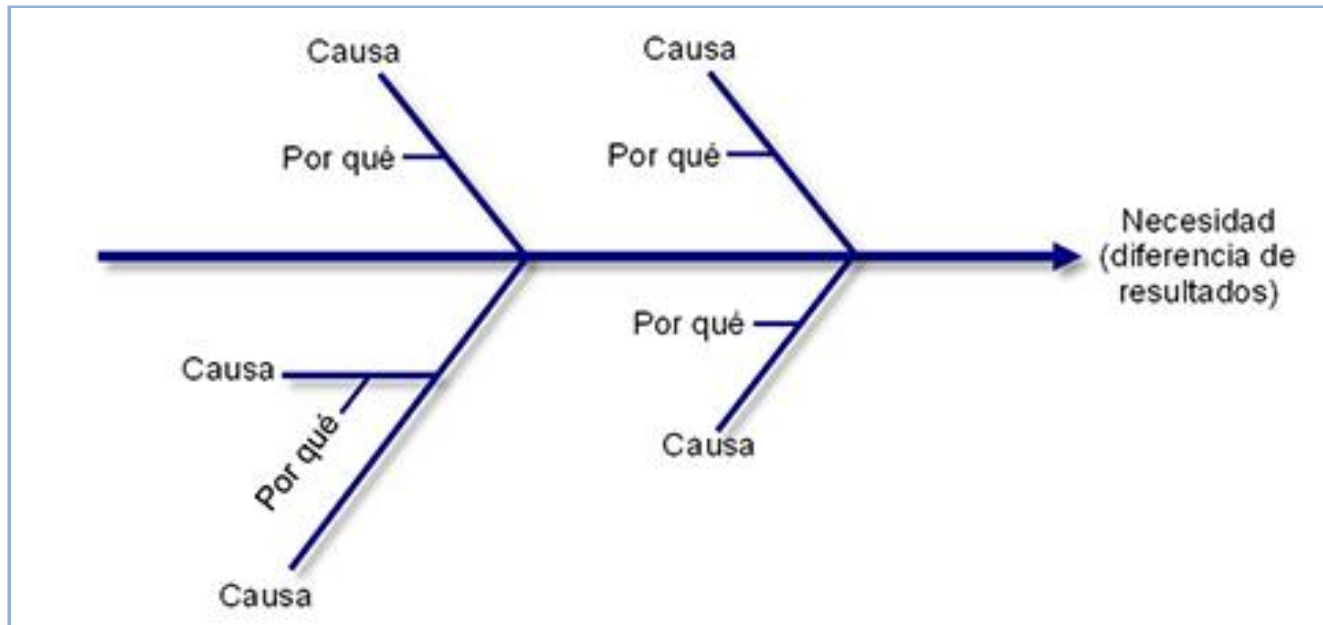


# Herramientas: Modelo de mejoramiento de proceso TQM



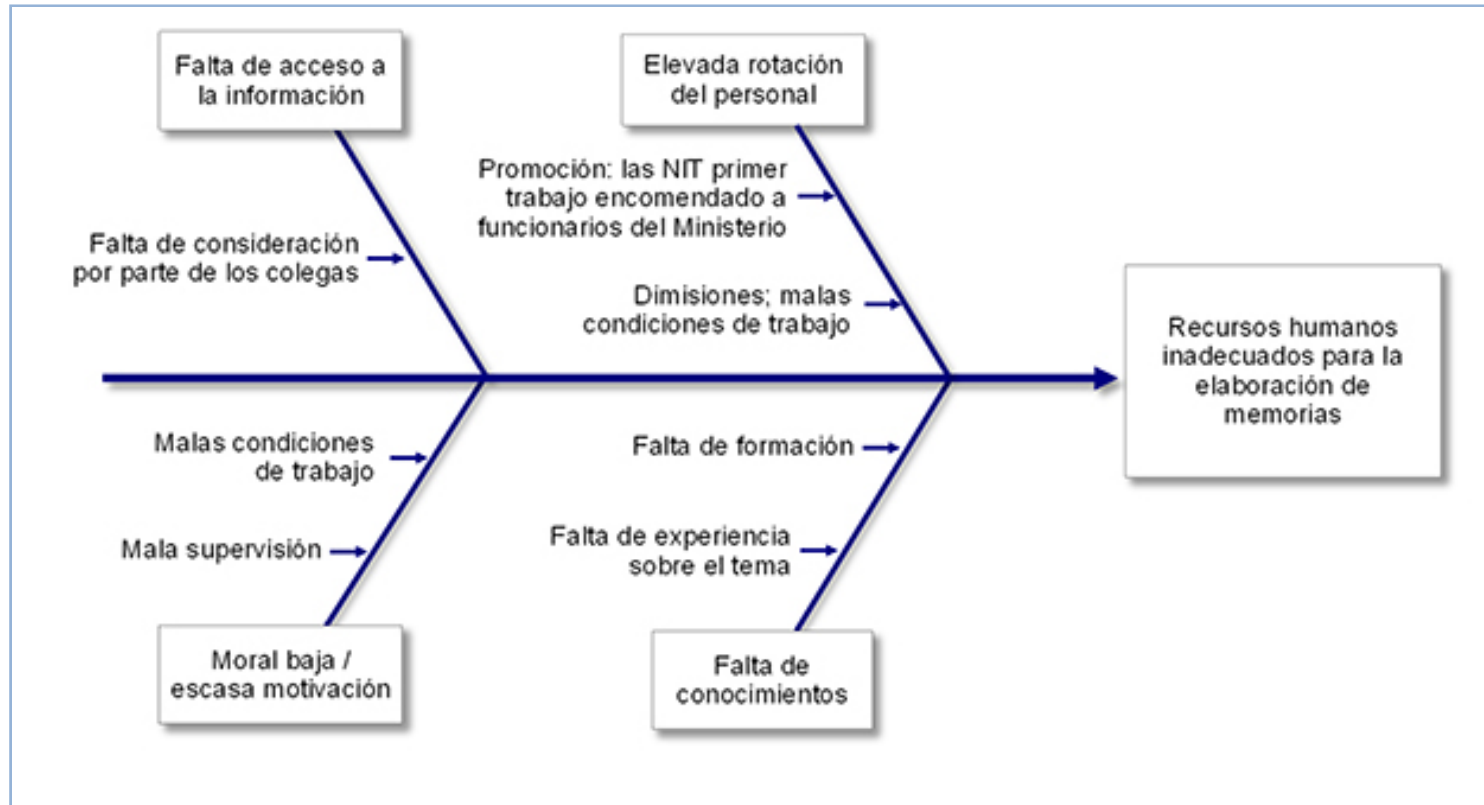
## Herramientas: Modelo de mejoramiento de proceso TQM

### Diagrama de Ishikawa o Análisis de causa y efecto



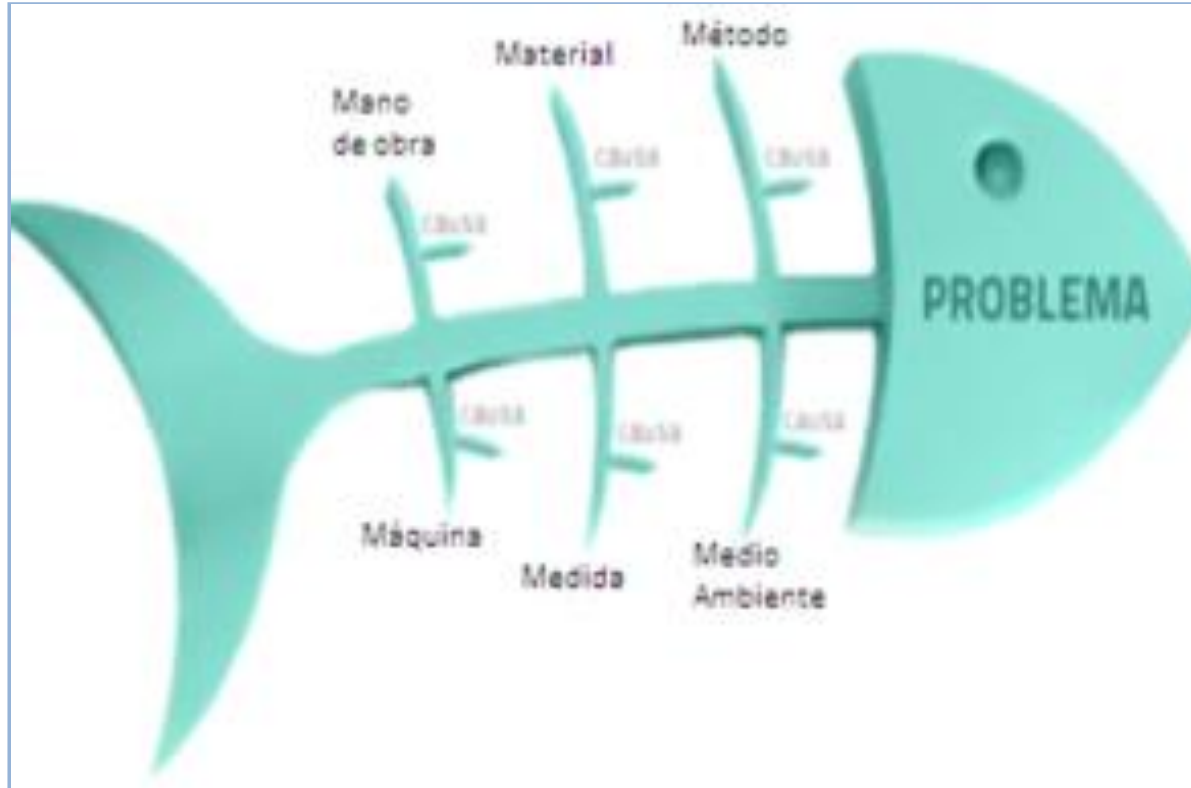
## Herramientas: Modelo de mejoramiento de proceso TQM

### Diagrama de Ishikawa o Análisis de causa y efecto



## Herramientas: Modelo de mejoramiento de proceso TQM

### Diagrama de Ishikawa o Análisis de causa y efecto

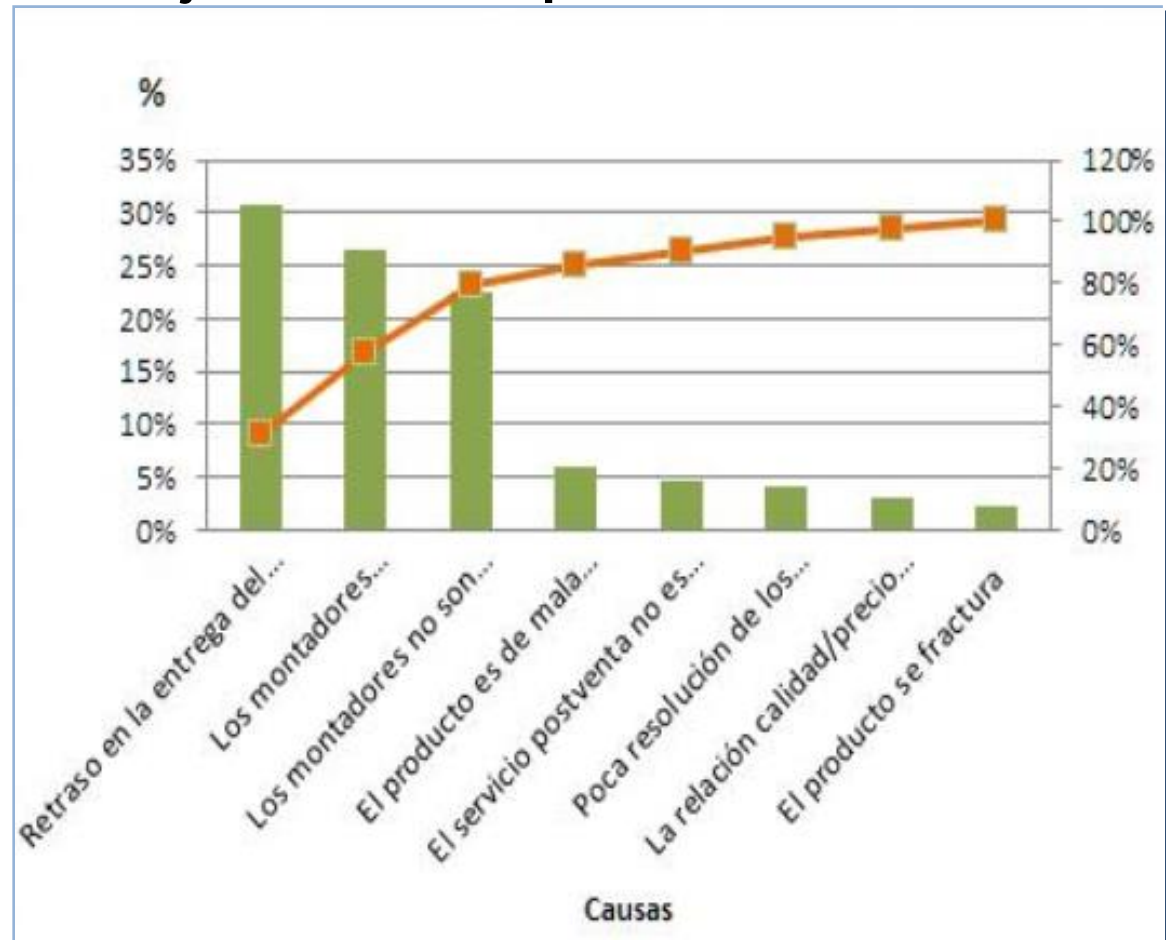




## Herramientas: Modelo de mejoramiento de proceso TQM

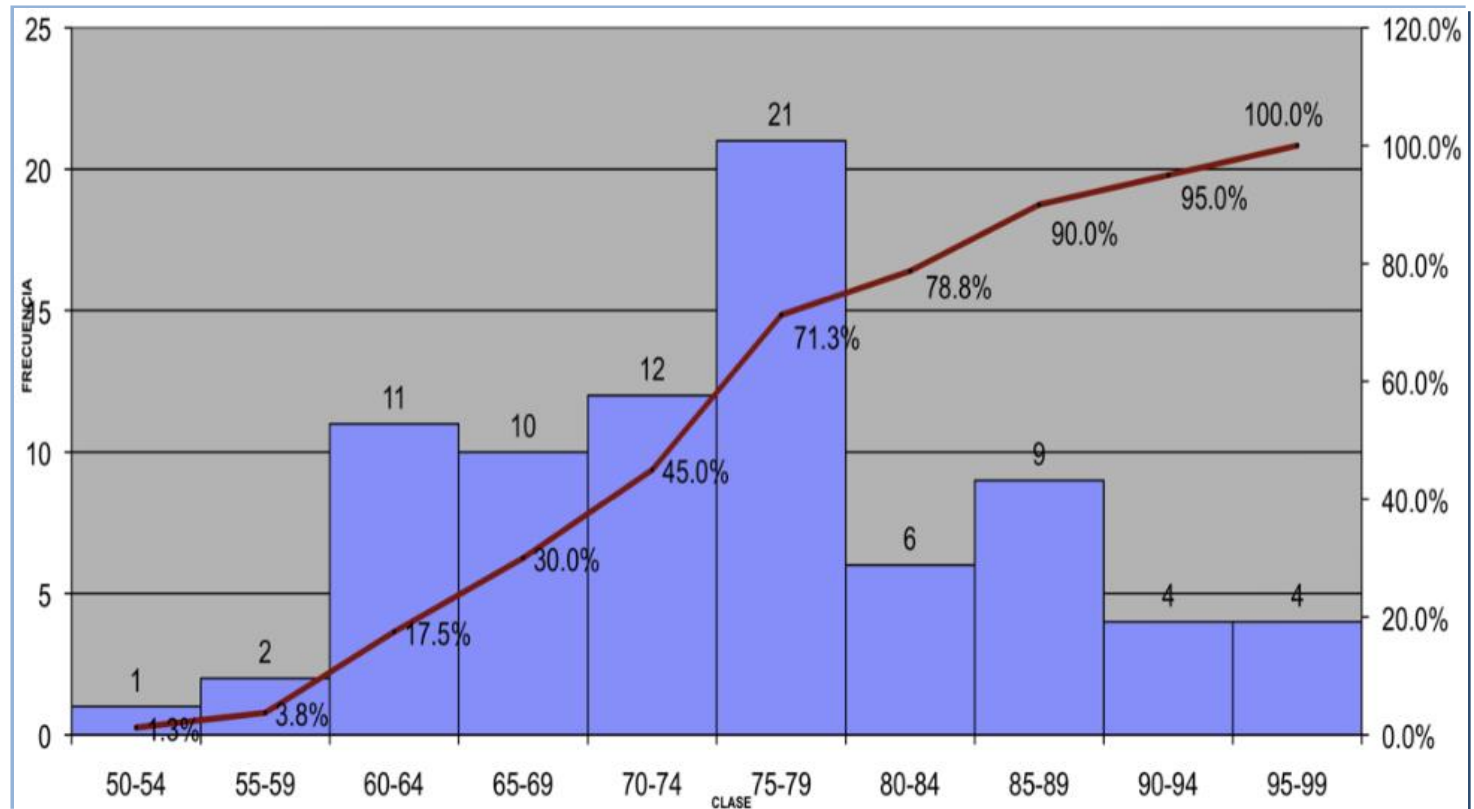
### Diagrama de Pareto

- Pocos vitales
- Muchos triviales
- Regla 80 / 20



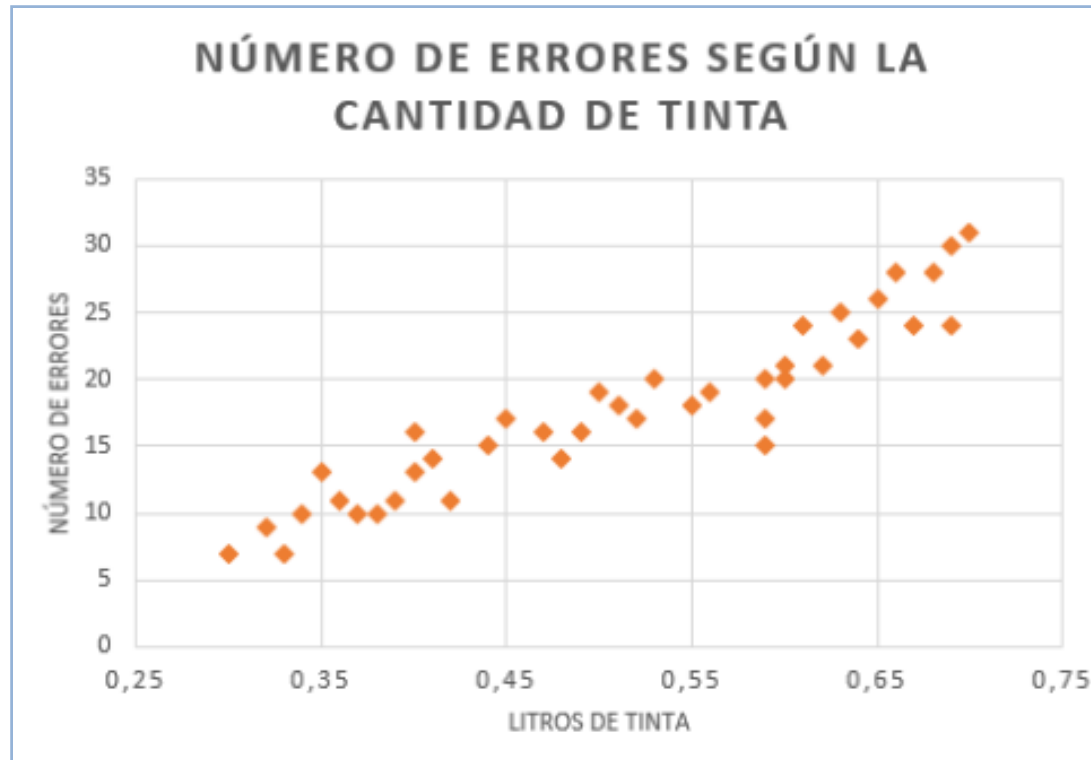
# Herramientas: Modelo de mejoramiento de proceso TQM

## Histogramas de frecuencia



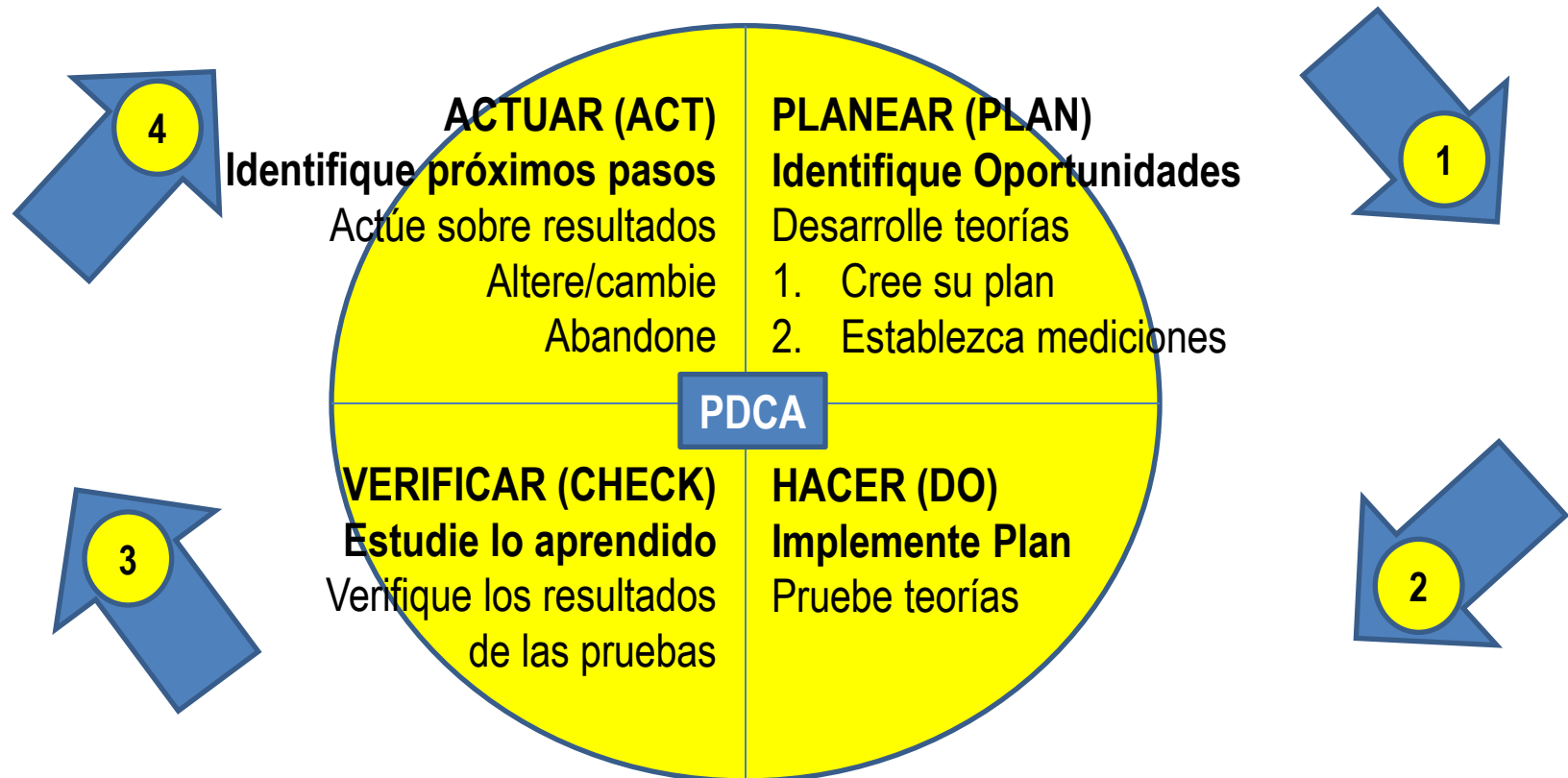
## Herramientas: Modelo de mejoramiento de proceso TQM

### Diagrama de dispersión



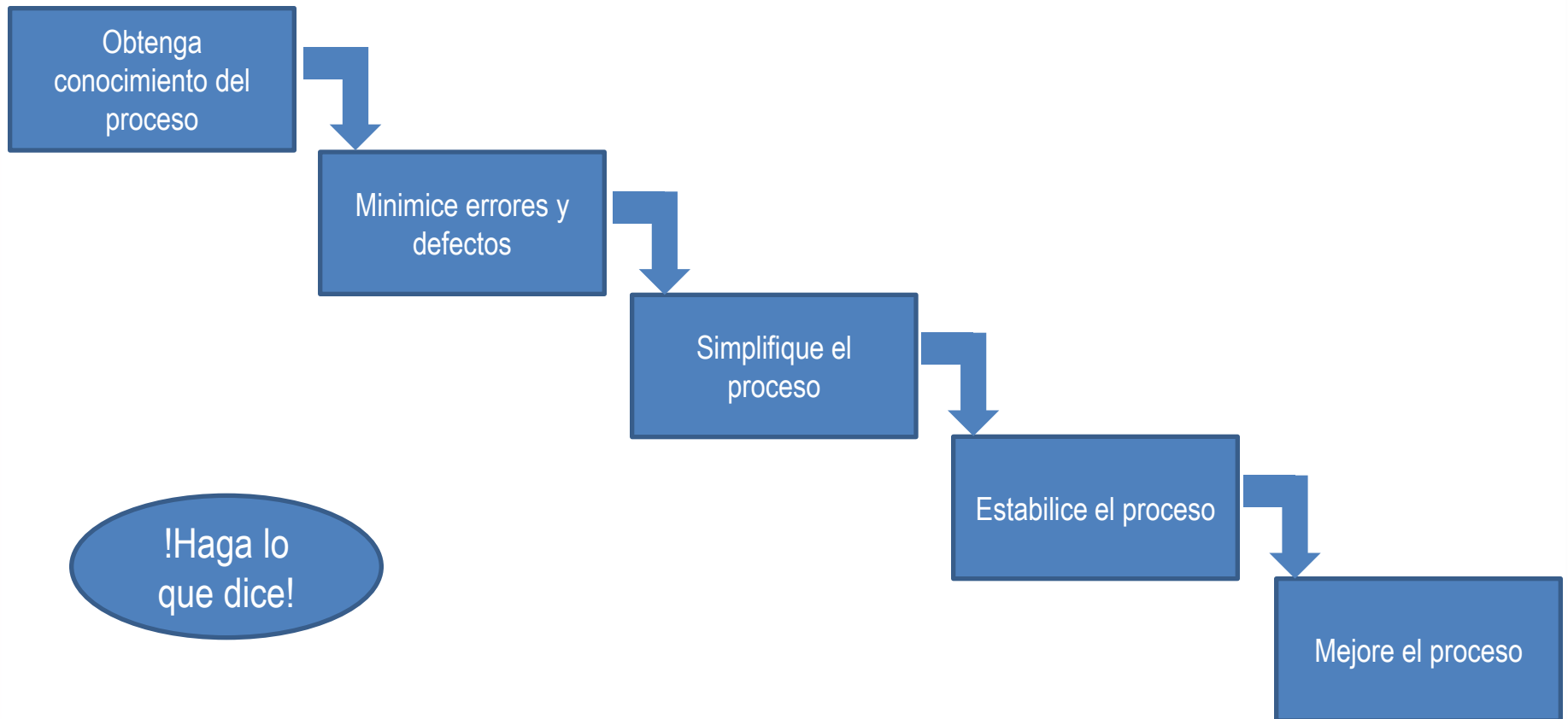
## Herramientas: Modelo de mejoramiento de proceso TQM

PDCA (plan-do-check-act) – Ciclo de Edward Deming



## Herramientas: Modelo de mejoramiento de proceso TQM

PDCA (plan-do-check-act) – Ciclo de Edward Deming



## Herramientas: Modelo de mejoramiento de proceso TQM

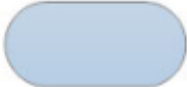

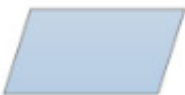


### Diagrama del proceso

- Defina el alcance del proceso
- Identifique las funciones que interactúan
- Establezca los supuestos
- Determine las etapas del proceso
- Establezca las secuencias de los pasos
- Diagrame el proceso
- Verifique que el diagrama esté completo
- Finalice el diagrama

!Diga lo que  
hace!

## Herramientas: Modelo de mejoramiento de proceso TQM

### Diagrama del proceso – Símbolos comúnmente utilizados

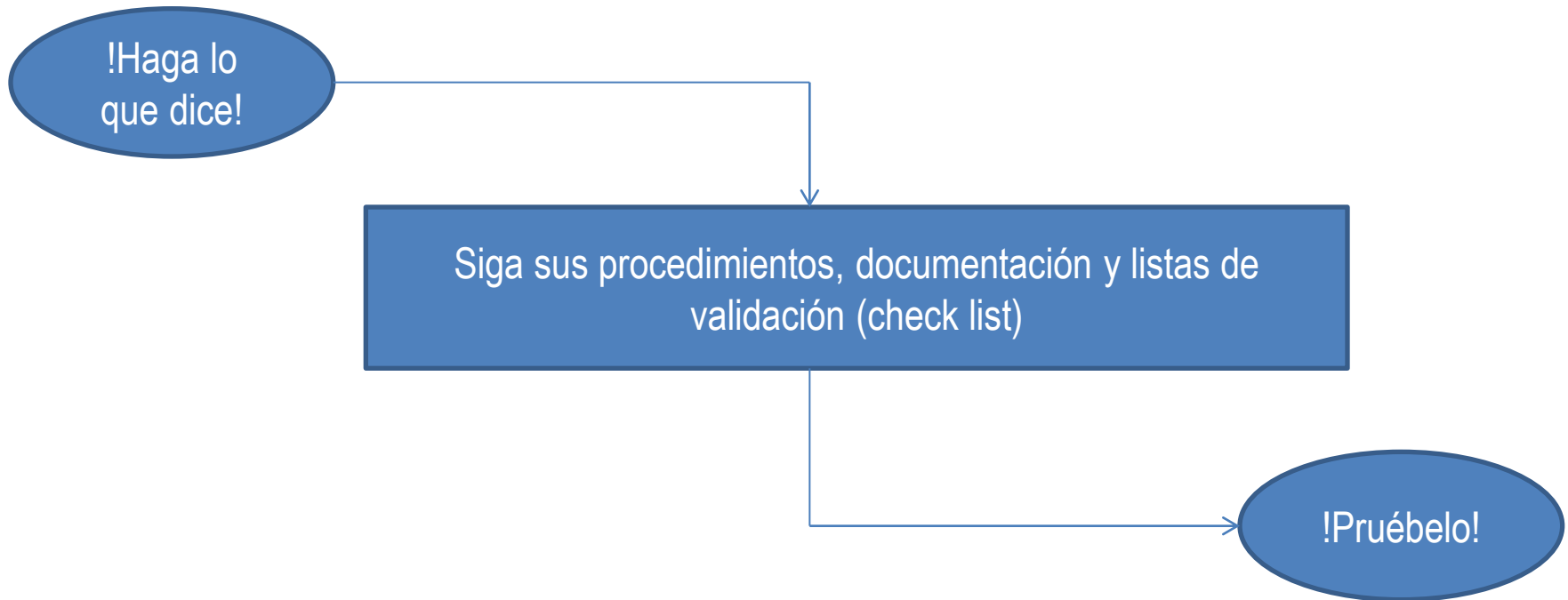
Símbolo	Nombre	Función
	Inicio / Final	Representa el inicio y el final de un proceso
	Línea de Flujo	Indica el orden de la ejecución de las operaciones. La flecha indica la siguiente instrucción.
	Entrada / Salida	Representa la lectura de datos en la entrada y la impresión de datos en la salida
	Proceso	Representa cualquier tipo de operación
	Decisión	Nos permite analizar una situación, con base en los valores verdadero y falso

!Diga lo que hace!



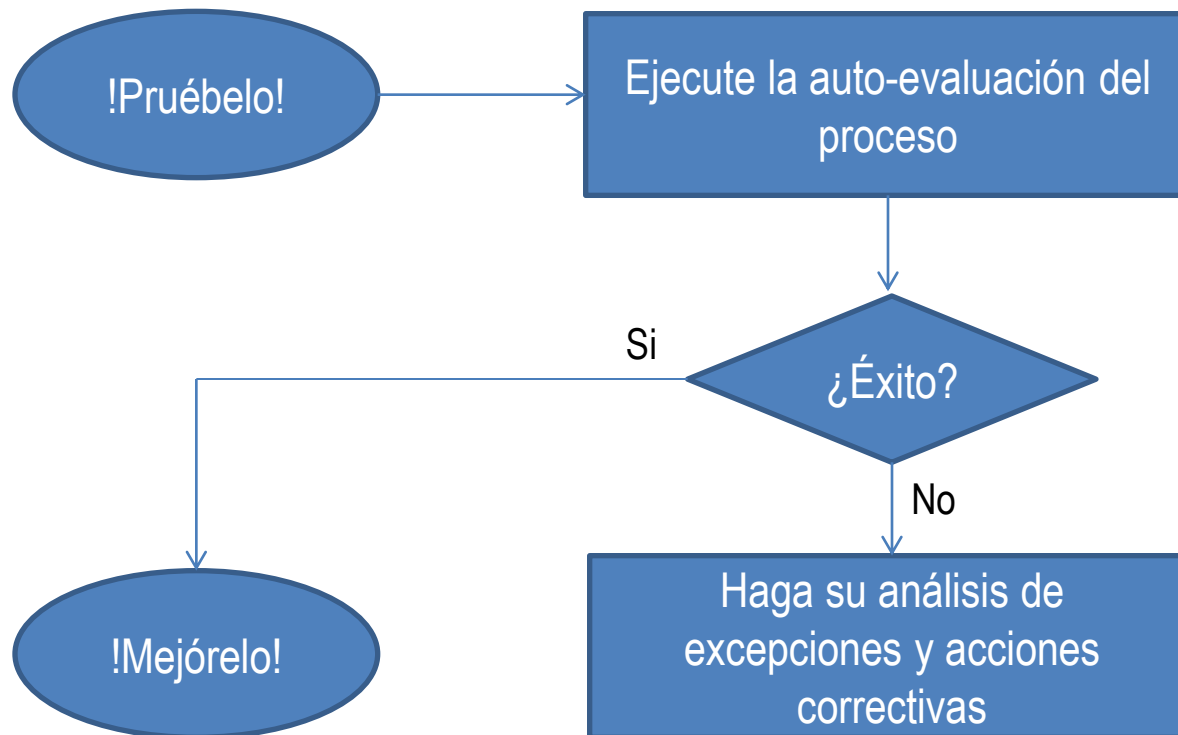
## Herramientas: Autoevaluación (pasos)

4. Identifique errores, deficiencias e irregularidades en los procesos (¿qué está mal?)



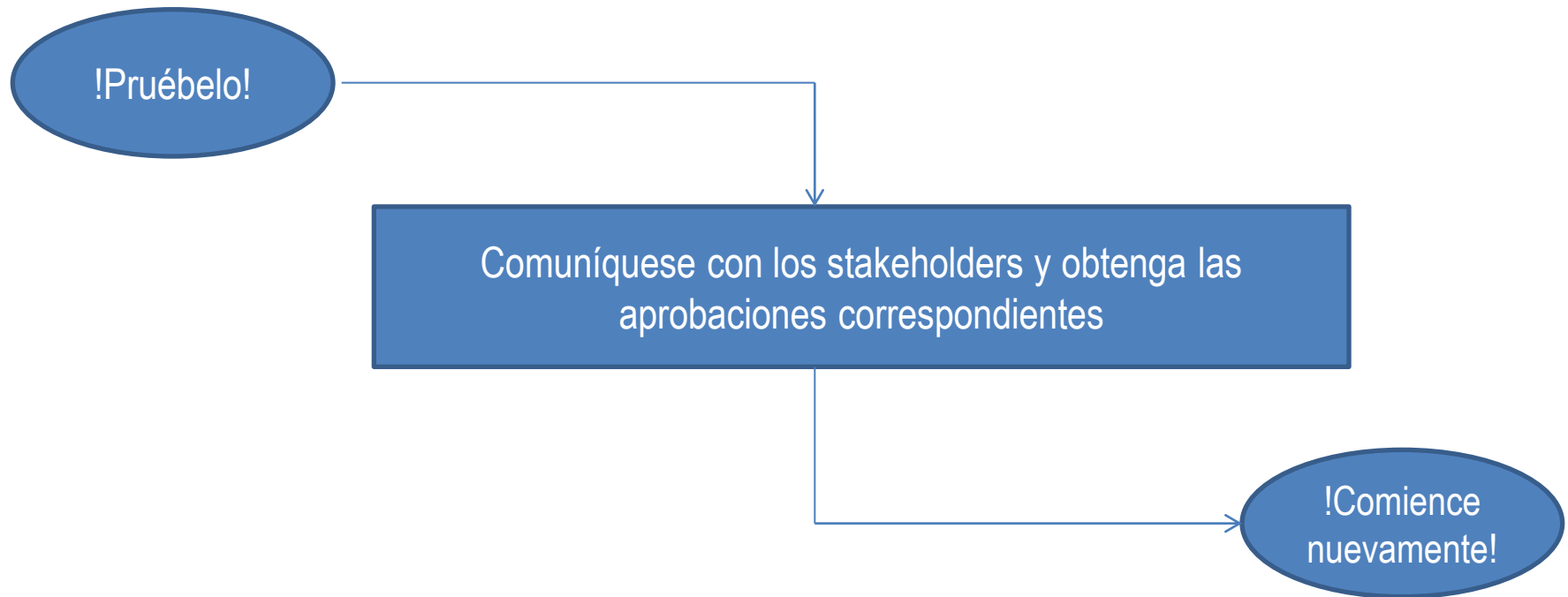
## Herramientas: Autoevaluación (pasos)

5. Plan de acción correctiva (¿cómo lo solucionamos?)
6. Monitoree la acción correctiva (¿dio resultado?)



## Herramientas: Autoevaluación (pasos)

### 7. Comuníquese oportunamente



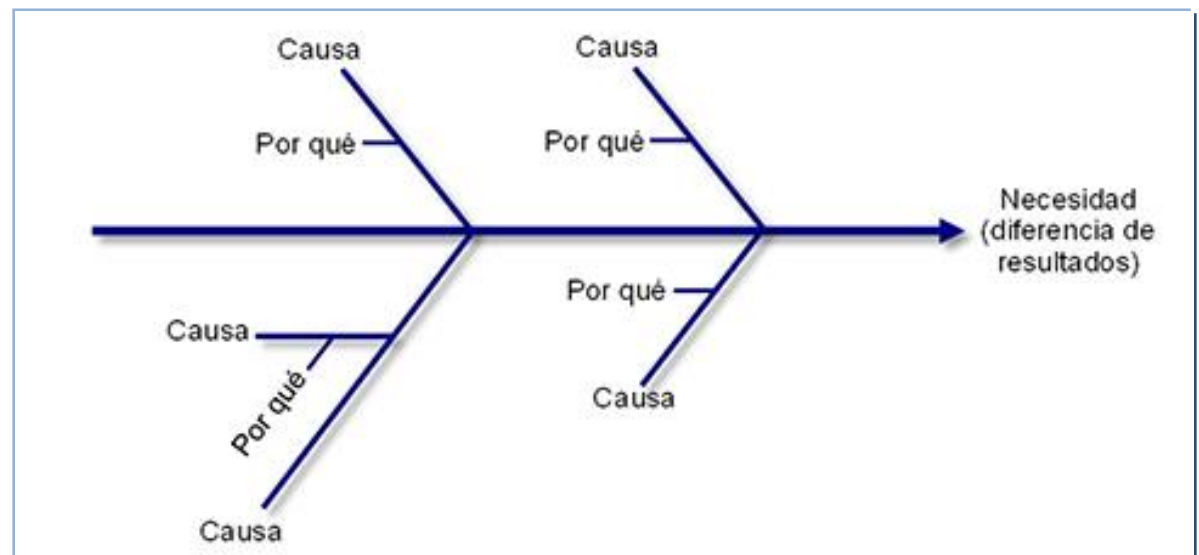
## Herramientas: Pruébalo y mejórela

Sistemas de procesos de control

Es el ciclo continuo de utilizar información de datos sobre el desempeño de un proceso para identificar las fuentes de variación y luego trabajar para reducir o eliminar dicha variación

Fuentes de variación:

- Causas comunes
- Causas especiales



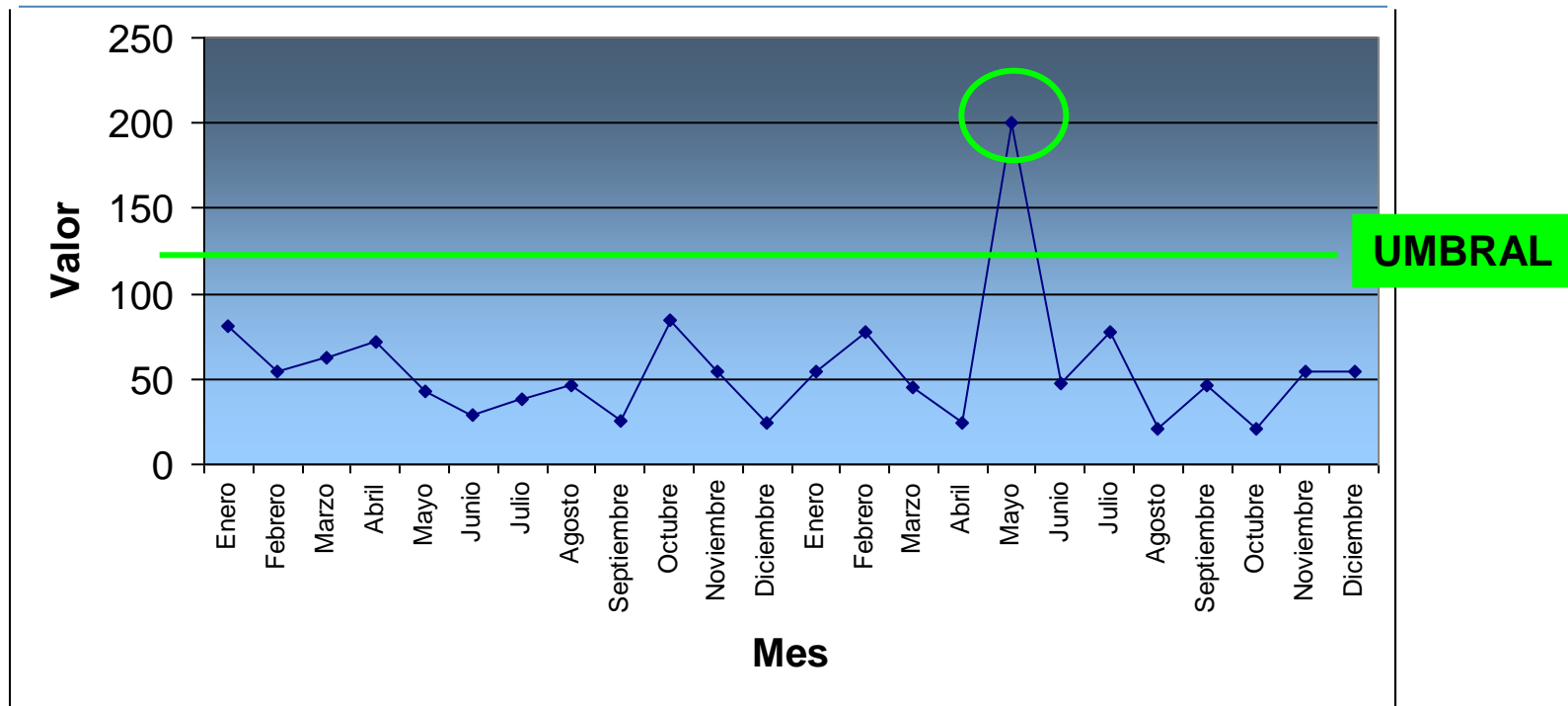
## Herramientas: Pruébalo y mejórello

### Gráfico de control

El gráfico de control es una herramienta gráfica que permite ver el trazo de variación de un proceso según pasa el tiempo

# Herramientas: Pruébalo y mejórello

## Gráfico de control



## Herramientas: Pruébelo y mejórelo

### Capacidad del proceso

Se utiliza para determinar si un proceso es capaz de cumplir con los requisitos, especificaciones y estándares establecidos

- ¿Es capaz de cumplir con los requisitos?
- ¿Ha habido algún cambio en el proceso?
- ¿Qué porcentaje del producto o servicio no cumple con los requisitos?

Lo que esperan los clientes: Servicio competente, a tiempo y sin problemas



## **Herramientas: Pruébalo y mejórello**

Data e información

Uso de indicadores de gestión, de riesgo y de control

Se obtienen para documentar la situación actual y entender cómo se desempeñan los procesos y qué acciones son necesarias para controlarlos, corregirlos y/o mejorarlos

## Herramientas: Pruébalo y mejórela

Uso de indicadores de gestión, de riesgo y de control

- 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: Pruébelo y mejórela

Uso de indicadores de gestión, de riesgo y de control

- Alertan de situaciones delicadas cuando se alcanzan determinados umbrales preestablecidos.
- Por tanto, su objetivo es contrastar, periódicamente, el perfil de riesgo de la entidad.
- Los indicadores 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: Pruébelo y mejórela

Uso de indicadores de gestión, de riesgo y de control

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

Requisitos que deben cumplir:

- Mostrar flexibilidad y capacidad de adaptación a las necesidades de cada unidad de la organización
- Proporcionar información agregada a nivel de entidad o de cada área en particular
- Tener capacidad predictiva de eventos
- Ser parte de un sistema de información dinámico, ágil e interactivo

## Herramientas: Pruébelo y mejórela

Uso de indicadores de gestión, de riesgo y de control

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: Pruébelo y mejórelo

Uso de indicadores de gestión, de riesgo y de control

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.

## Herramientas: Pruébelo y mejórello

Uso de indicadores de gestión, de riesgo y de control

Tipos de indicadores de riesgo (Scandizzo, 2005).

- 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.

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.



### PROCESOS

#### Factores Clave:

- Reducir el número de errores
- Mejorar la segregación de funciones

#### Indicadores:

- N<sup>2</sup> Errores / N<sup>2</sup> Transacciones
- N<sup>2</sup> reclamaciones de clientes
- % comisiones improcedentes
- N<sup>2</sup> sanciones del Supervisor Bancario
- % operaciones pendientes liquidar
- % áreas con mapa de procesos desarrollado

### PERSONAS

#### Factores Clave:

- Fidelizar al personal
- Prevenir el fraude interno

#### Indicadores:

- Rotación del personal
- % empleados sin cursos de formación
- Tiempo medio absentismo por empleado
- N<sup>2</sup> empleados sancionados por fraude
- N<sup>2</sup> solicitudes por vacante
- N<sup>2</sup> sanciones laborales

### SISTEMAS

#### Factores Clave:

- Reducir las caídas del sistema
- Mejorar la seguridad

#### Indicadores:

- N<sup>2</sup> solicitudes renovación claves acceso
- Tiempo medio resolución tareas críticas
- % equipos sin actualización de antivirus
- N<sup>2</sup> intentos de acceso malintencionados
- N<sup>2</sup> de recuperaciones de backups
- N<sup>2</sup> usuarios por aplicación

### EVENTOS EXTERNOS

#### Factores Clave:

- Reducir el fraude externo
- Evitar daños en activos materiales

#### Indicadores:

- N<sup>2</sup> clientes detectados en blanqueo dinero
- % Tarjetas comprometidas por fraude
- % Operaciones en off
- Existencia de planes de contingencia
- Nivel de cobertura de pólizas de seguro
- Tiempo transcurrido última inspección

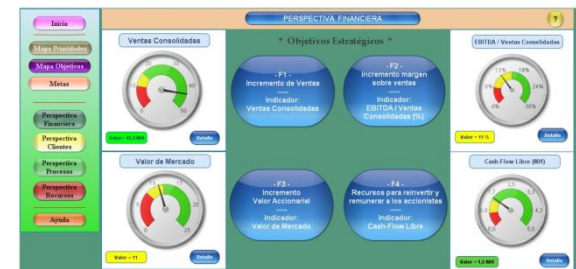


## Herramientas: Pruébalo y mejórello

Uso de indicadores de gestión, de riesgo y de control

Cuadro 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.



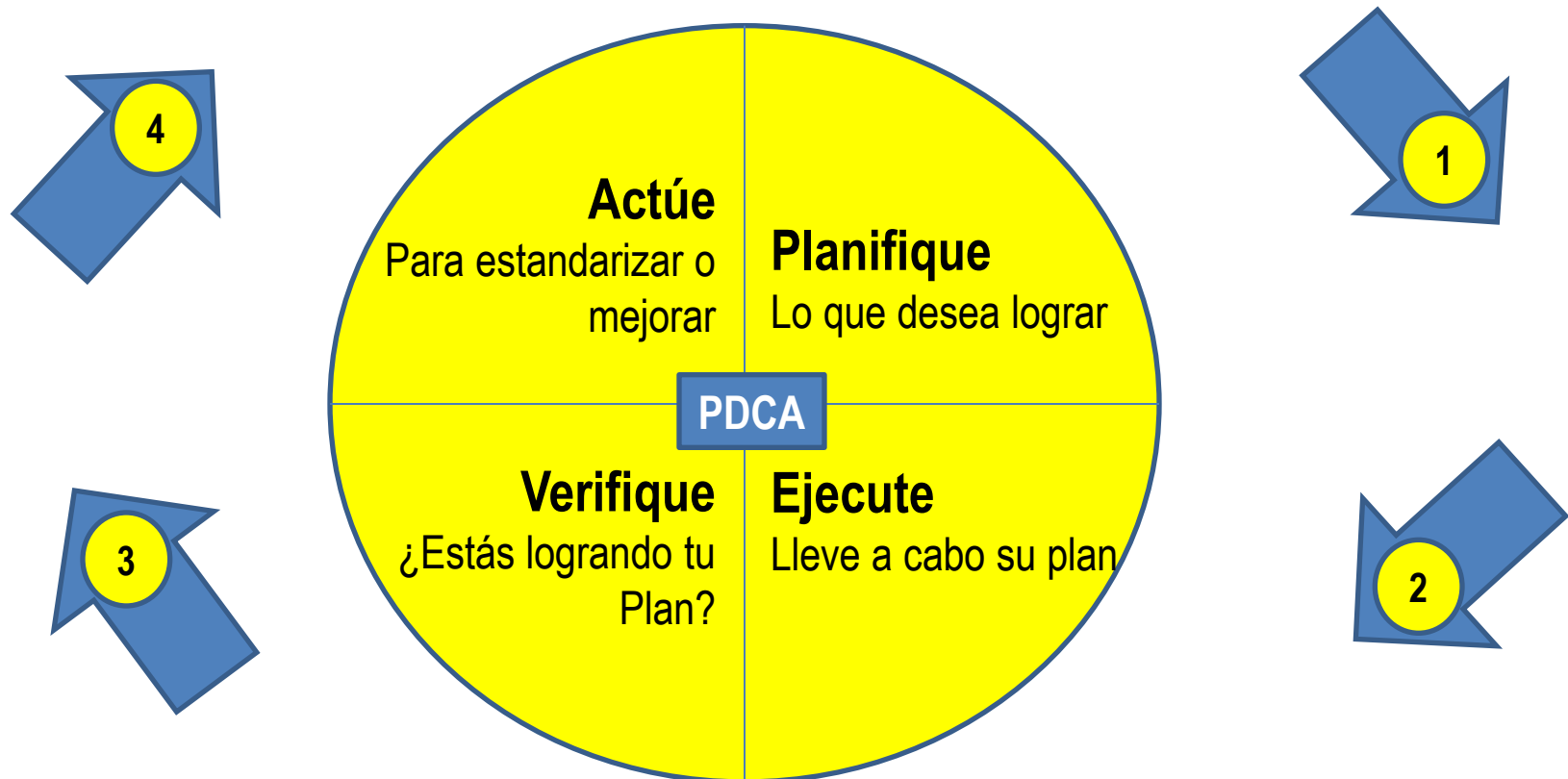
## **Herramientas: Pruébalo y mejórela**

Análisis de excepciones: “Gap Analysis”

Proceso para identificar elementos del proceso que faltan o que no han sido documentados

## Herramientas: Modelo de mejoramiento de proceso TQM

PDCA (plan-do-check-act) – Ciclo de Edward Deming



## Documentación

### 3. Verifique

Para entender el contenido del estándar

### 4. Actúe

Determine la necesidad de mejorar antes de preparar la documentación

### 2. Ejecute

Documente con calidad y control para que sea capaz de demostrar su operación

### 1. Planifique

Establezca un itinerario de entrenamiento y desarrollo de documentación

## Niveles de Documentación

### Nivel 1

Define: Propuesta y responsabilidad

### Nivel 2

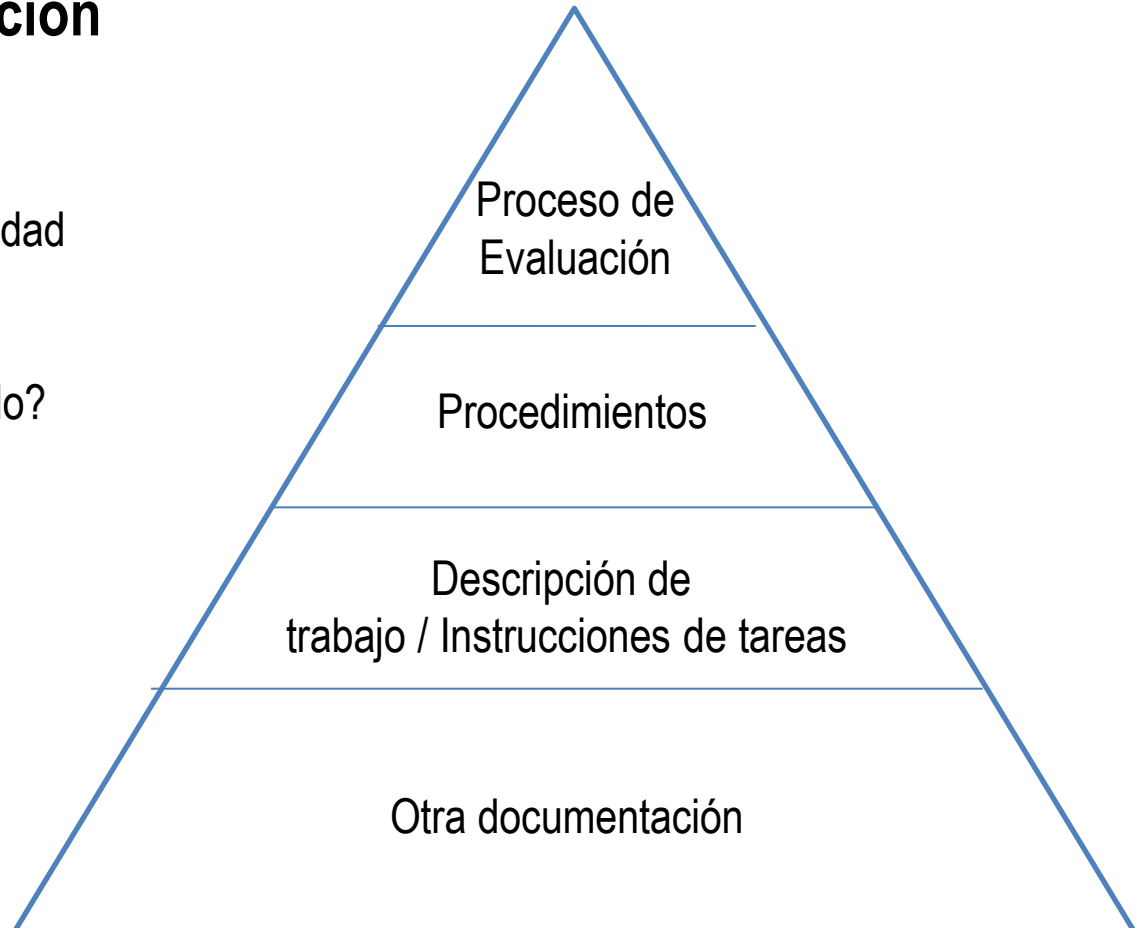
Define: ¿Quién? ¿Qué? ¿Cuándo?

### Nivel 3

Responde a: ¿Cómo?

### Nivel 4

Resultador: Demuestra que el sistema está operando



## Niveles de Documentación

### 1. Proceso de Evaluación

- Política
- Propósito y Objetivos
- Procesos
- Indicadores de gestión
- Plantilla de reporte
- Lista de revisiones
- Formato de reporte de excepciones

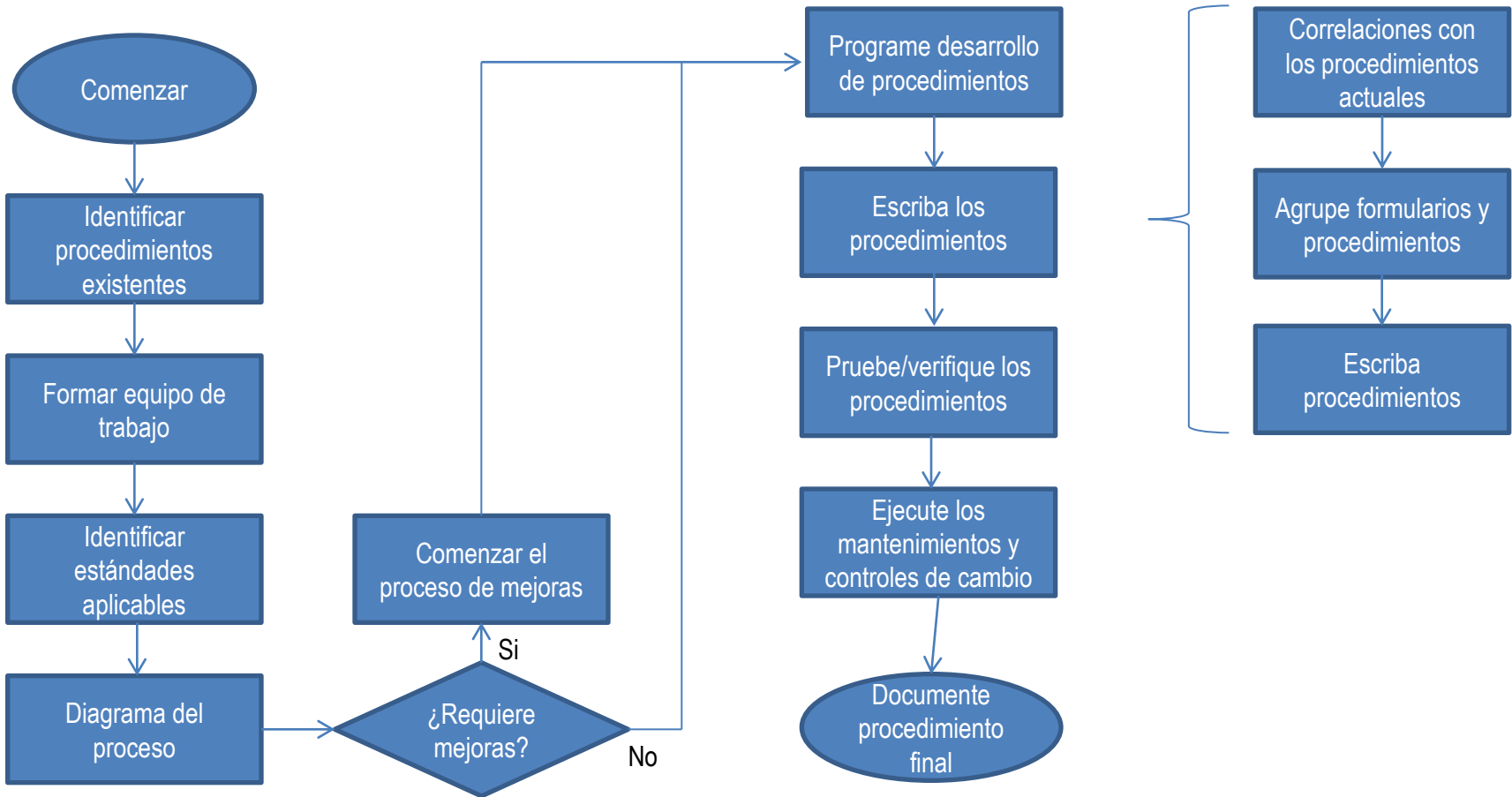
## Niveles de Documentación

### 2. Bosquejo de procedimientos del área

- Propósito y objetivos
- Alcance
- Responsabilidades
- Referencias
- Definiciones
- Procedimientos
- Documentación sustentatoria



## Diagrama para escribir procedimientos



## Niveles de Documentación

### 2. Bosquejo de procedimientos del área

Sugerencias para escribir documentación:

- Mantengalo corto y sencillo
- Diagrame el proceso
- Use un formato estándar
- Mantenga al usuario en mente
- Para cada tarea identifique “Por qué y cómo”
- Ejecute una prueba piloto (marcha blanca)
- Obtenga endosos y confirmación

## Niveles de Documentación

### 3. Instrucciones y descripciones de trabajo

- Comience con los que ya tiene
- Utilice la técnica de equipo para la preparación
- Verifique instrucciones disponibles y describa la actividad actual
- Determine si la práctica actual es satisfactoria o requiere mejorar
- Adopte prácticas mejoradas si es necesario
- Diagrame operaciones complejas
- Comience a mejorar/re-evaluar instrucciones de trabajo
- Verifique para seguimiento y cabalidad
- Use instrucciones de trabajo como base para capacitación

## Niveles de Documentación

### 3. Instrucciones y descripciones de trabajo

Contenido de una descripción de trabajo

- Título
- Número de documento
- Indicador de revisión
- Número de página
- Fecha de emisión
- Aprobaciones
- Autor/emisor/preparador
- Detalles

## Niveles de Documentación

### 4. Otros documentos

- Políticas de control interno asociadas
- Reportes a gerencia
- Organigramas
- Reportes a auditoría
- Reportes a finanzas/contabilidad
- Capacitación

## ¿Qué es riesgo?

- Es el potencial de impacto adverso que eventos esperados o inesperados pueden tener sobre el capital y las ganancias.
- Incertidumbre acerca de los eventos y/o de sus efectos que pudiesen tener un impacto material en las metas de la organización
- Inquietud de la gerencia sobre los efectos probables de un ambiente incierto
- Típicamente lo llamamos:
  - ¿Qué puede ir mal?
  - ¿Qué puede fallar?

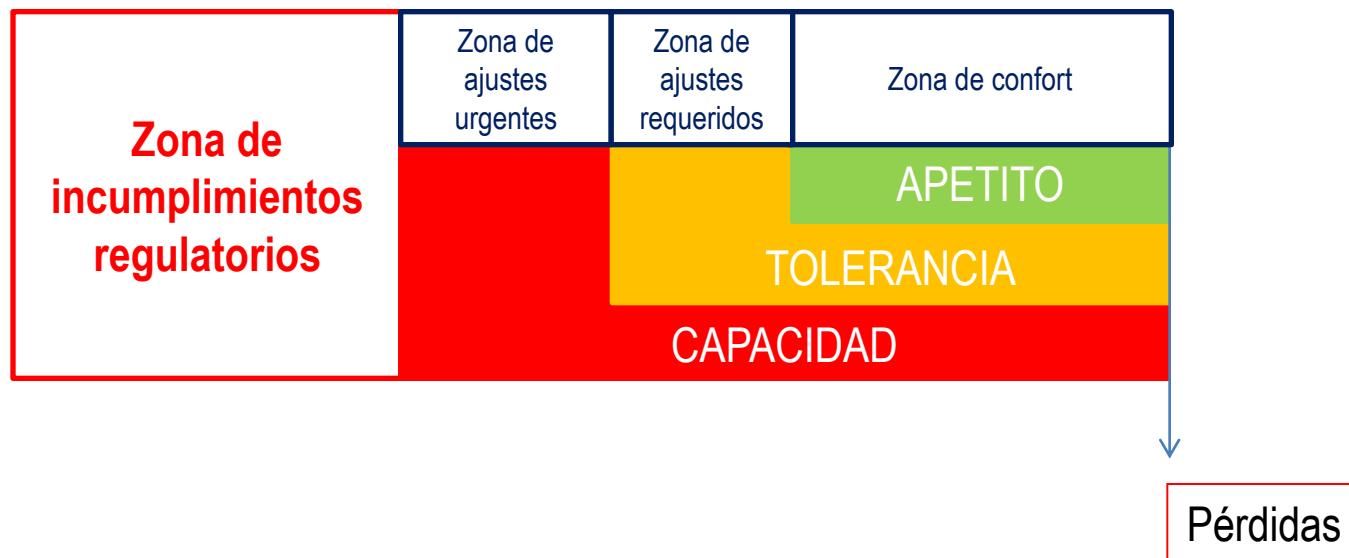
## Determinación del riesgo

- Análisis e identificación por parte de la gerencia de los riesgos pertinentes para alcanzar o lograr las metas y objetivos fijados  
Interno / externo  
Los riesgos están en cambio constante
- Determinar la magnitud del riesgo
- Determinar la probabilidad o frecuencia en que el riesgo puede ocurrir
- Determinar qué acciones se deben llevar a cabo para manejar el riesgo (costo versus beneficio)

## Riesgo inherente

- Es el potencial de ocurrencia que tiene un evento adverso de suceder si el factor de riesgo no es propiamente controlado
- Se fundamenta en los factores principales de riesgo que son manejados por la empresa o negocio
- Dependiendo de la probabilidad de ocurrencia se pueden clasificar en alto, medio o bajo.
- La clasificación debe hacerse basado en la premisa que el riesgo existe, sin importar cuan efectivo sea el ambiente de control







¿Los tenemos identificados?

## **GESTIÓN INTEGRAL DE RIESGOS**

Es el proceso efectuado por el Directorio, los Comités, Gerencia General y el resto del personal, aplicable al establecimiento de estrategias en toda la empresa, diseñado para identificar los eventos potenciales que pueden afectar a la organización, gestionar sus riesgos de acuerdo con su apetito por el riesgo y proporcionar una seguridad razonable para el logro de sus objetivos.

RIESGO ESTRATÉGICO

DIRECCIÓN DE LA EMPRESA

RIESGO REPUTACIONAL

ÁREAS DE RIESGO

RIESGOS FINANCIEROS

RIESGO DE MERCADO:  
RIESGO DE PRECIOS  
RIESGO CAMBIARIO  
RIESGO DE TASA DE INTERÉS  
RIESGO DE COMMODITIES

RIESGO DE LIQUIDEZ

RIESGO DE CRÉDITO

RIESGOS OPERACIONALES

RIESGO OPERACIONAL  
RIESGO LEGAL  
SEGURIDAD DE LA INFORMACIÓN  
CYBERSECURITY  
CONTINUIDAD DEL NEGOCIO  
CORRUPCIÓN  
SPLAFT  
CUMPLIMIENTO NORMATIVO

TODA LA EMPRESA

## 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.



**RIESGO ESTRATÉGICO**

**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

# ¿Cuál es tu posesión más valiosa?



¿Tu casa?



¿Tu auto?



¿Tus inversiones?



Más cerca ...  
¿Tu familia?



¿Un recuerdo inolvidable?



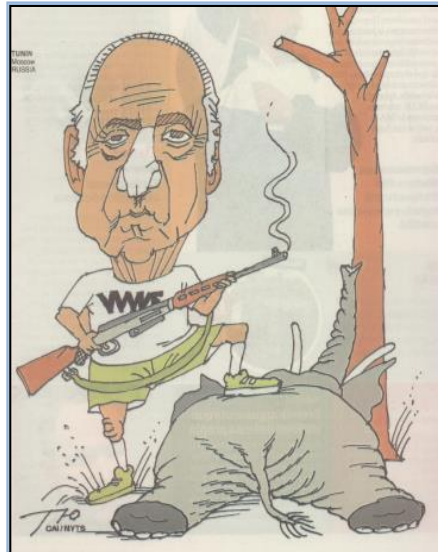
Tu reputación !!!



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.



## RIESGO REPUTACIONAL

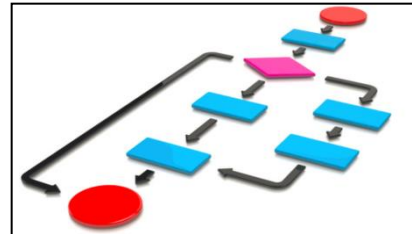




# RIESGO OPERACIONAL



Personas



Procesos



Tecnologías de la Información y Comunicaciones (TIC)



Eventos Externos

## Reflexión:

¿Qué es mejor?

- No tener un control para un proceso crítico
- Tener un control mal implementado en tanto implementamos uno robusto

## **Ambiente de control**

Es la base para los demás componentes de los controles internos que proveen disciplina y estructura.

Se compone de los siguientes elementos:

- Integridad y valores éticos de la empresa
- Filosofía gerencial y modo de operar
- Estructura organizacional
- Normas y actividades de control
- Manejo del riesgo
- Información y comunicación
- Seguimiento

## Ambiente de control

- Controles robustos (adecuados, oportunos, fuertes y efectivos)
- Preparados para los procesos de auditoría
- Aseguramiento de acción oportuna frente a la detección de problemas facilitando una mayor efectividad
- Evitar las sorpresas (conejos del sombrero)



## **Beneficios de un ambiente de control adecuado**

Aumenta el valor para el accionista

- Pérdidas financieras por errores o fraude
- Pérdida de clientes y/o incapacidad de atraer nuevos clientes
- Desconcierto/confusión corporativa, pérdida de imagen, mala publicidad
- Mal uso y divulgación de información confidencial
- Costos relacionados con la corrección de errores
- Multas y penalidades
- Costo de fondeo
- Costo por la corrección de errores y multas

## Aplicación del Control Interno en los procesos

- Métodos y plan de acción, así como medidas que implementa el área para salvaguardar sus activos, verificar su veracidad y confiabilidad, promoviendo la eficiencia y eficacia y fomentando el cumplimiento de las políticas
- Ofrece una seguridad razonable (no absoluta) en cuanto a la realización de los objetivos del área o empresa

## Aplicación del Control Interno en los procesos

### Limitaciones

- Proceso de toma de decisiones imperfecto
- Colapso de los controles debido a errores simples
- Confabulación de dos o más individuos
- Invalidación de controles internos por parte de la gerencia
- Relación costo/beneficio: el costo de implementar un control no deberá exceder el beneficio que se deriva de su implementación

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**

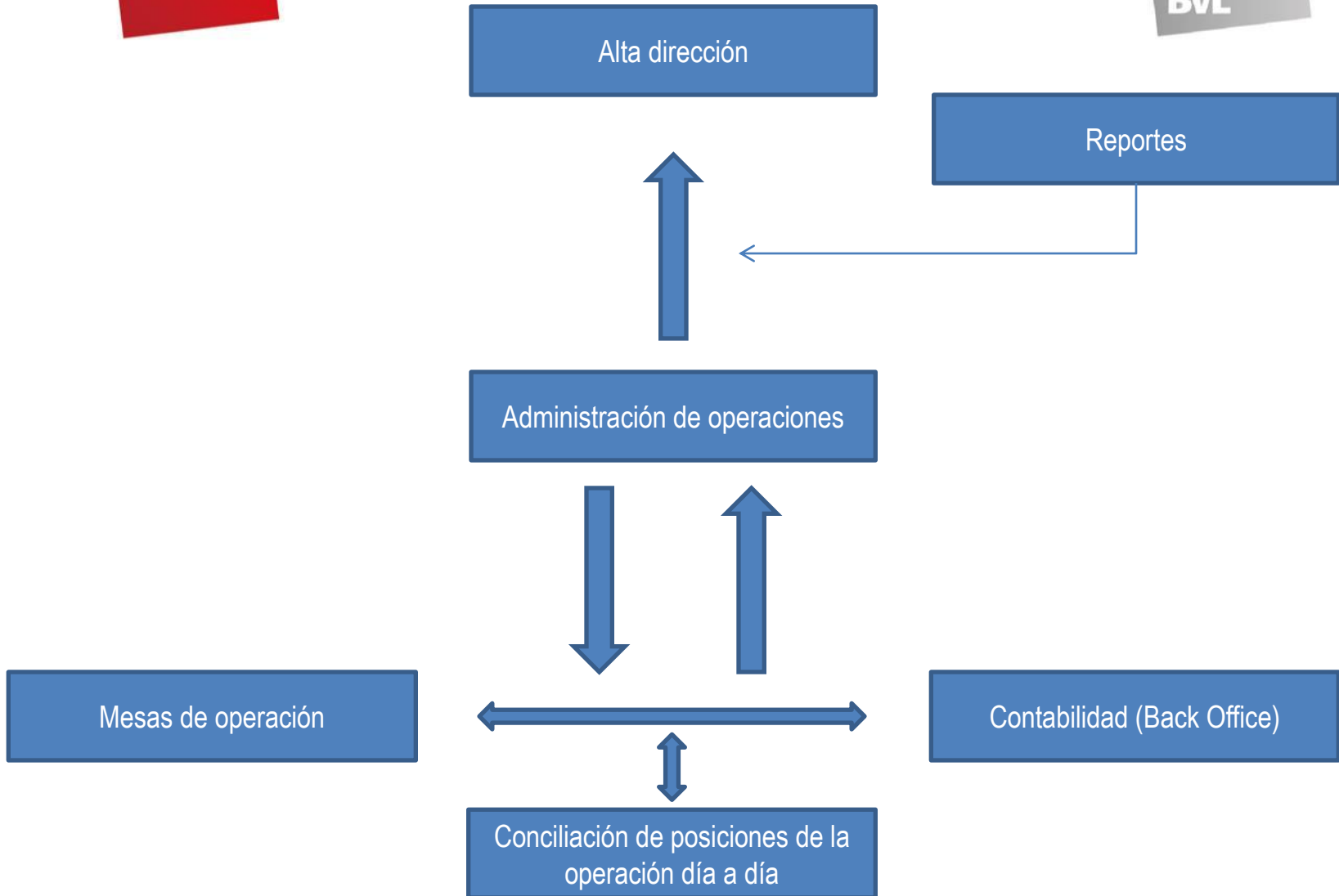
*Proporciona seguridad razonable en el logro de los objetivos de negocio:*

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



## ¿A quién le debe interesar un ambiente de control adecuado?

- Todos los empleados
- Accionistas
- Gerencia
- Auditores
- Reguladores
- Clientes
- Directorio
- Acreedores
- Clientes
- Competencia



## Actividades de control

Permite que se tomen acciones y decisiones para el cumplimiento de los objetivos de la empresa

- Autorizaciones
- Aprobaciones
- Verificaciones
- Reconciliaciones
- Revisiones de desempeño
- Seguridad de activos
- Segregación de funciones

## Proceso versus control

- Proceso: método o tarea realizada para lograr un objetivo. Es la forma en que completamos las transacciones. Por ejemplo, la información es ingresada en un sistema y se genera un informe
- Control: mecanismo que asegura que los objetivos o procesos definidos se realicen en forma adecuada. Por ejemplo, la revisión de la información ingresada por una persona independiente
- La presencia de una persona o sistema no es un control en si misma. Los controles siempre están orientados a acción/reacción

## **Control independiente versus control de proceso**

### Control independiente

- Los ejecutan personas ajenas al proceso y en fechas distintas
- No influyen en el resultado del proceso
- Pueden definirse a nivel muestral
- Verifican la calidad de los controles de proceso
- Validan la documentación sustentatoria

## Control independiente versus control de proceso

### Control de proceso

- Los ejecutan personas insertas en el proceso y en el momento que este se realiza
- Cubre la totalidad de las transacciones
- Si no se realizan, pueden afectar el resultado del proceso
- Son más riesgosos porque los realizan las personas que están en el proceso (¿siempre?)
- Pueden ser manuales o automáticos

## Prevención versus detección

- Depende de la oportunidad del control dentro del proceso
- Control de prevención: verificación de entrada de datos, claves de acceso, accesos restringidos
- Control de detección: detectan errores o excepciones después que los mismos han ocurrido. Por ejemplo, reconciliaciones.

## Características de los controles

- Eficientes
- Reales
- Documentados
- Correctos
- Concretos
- Tienen un responsable
- Se reportan (indicadores)



## **Etapas de un Plan de acción correctiva**

- Identificar el problema y su fuente
- Cuantificar el impacto de riesgo
- Determinar los pasos de acción requeridos (corrección)
- Establecer fechas de corrección
- Mitigar el riesgo con controles alternativos
- Obtener la aprobación al nuevo proceso (costo/beneficio)
- Cerrar la observación
- Hacer seguimiento (indicador)

## **Etapas de un Plan de acción correctiva**

### Identificar el problema y su fuente

- Describa el proceso que falló y los detalles que clarifiquen el problemas más adelante
- Determine si los controles establecidos son suficientes (síntoma-enfermedad)
- Ejecute su análisis de tendencias
- Determine si los errores están limitados a ciertos aspectos de proceso, períodos de tiempo, empleados, etc.

## **Etapas de un Plan de acción correctiva**

### Cuantificar el impacto de riesgo

- Identifique el riesgo asociado con la falla en el proceso
- ¿Este proceso impactará en otros procesos?
- Cuantifique pérdidas potenciales

## **Etapas de un Plan de acción correctiva**

Determinar los pasos de acción requeridos (corrección)

- Identifique los pasos para reestablecer el proceso a un estado de cumplimiento
- Asegure que las áreas afectadas por la falla, están involucradas en el desarrollo del plan de acción correctiva
- Comprometa a las unidades involucradas en las etapas de corrección del plan
- Defina y entienda claramente las responsabilidades de cada área en el plan de corrección
- Informe al área a cargo del seguimiento (Riesgos/Auditoría)

## **Etapas de un Plan de acción correctiva**

Establecer fechas de corrección

- Nivel de urgencia
- Fechas oportunas y razonables
- Fechas reales
- Control de reprogramaciones

## **Etapas de un Plan de acción correctiva**

### Mitigar el riesgo con controles alternativos

- Controles alternativos a ser implementados en caso el plan de acción definitivo tenga un tiempo de ejecución largo que exponga al área a un nuevo incidente

## **Etapas de un Plan de acción correctiva**

Obtener la aprobación al nuevo proceso (costo/beneficio)

- Aprobación de las personas responsables del proceso
- Para ello es necesario el sustento con el análisis de costo/beneficio

## **Etapas de un Plan de acción correctiva**

### Cerrar la observación

- Todos los afectados acuerdan el cierre de la observación debido a que a sido resuelta a satisfacción de los involucrados
- Se mantiene la evidencia de lo implementado y el análisis efectuado

### Hacer seguimiento (indicador)

- Indicadores de gestión
- Revisión periódica de la eficacia del control



## **Factores de riesgo a considerar en la elaboración de procesos operacionales en instituciones financieras**

- Contabilidad
  - Totalmente integrada
  - Batch/interface
  - Semi-integrada
  - Manual

## Factores de riesgo a considerar en la elaboración de procesos operacionales en instituciones financieras

- Cuentas sensitivas
  - Gastos anticipados
  - Cuentas por cobrar
  - Partidas pendientes
  - Cuentas inter-departamentales
  - Cuentas corrientes con otras instituciones (bancos)
  - Cuentas inactivas
  - Ítems no reclamados
  - Intereses por cobrar/ganar
  - Cuentas de ingresos
  - Cuentas de gastos

## Factores de riesgo a considerar en la elaboración de procesos operacionales en instituciones financieras

- Valores
  - Efectivo
  - Bonos/instrumentos de inversión
  - Cheques
  - Certificados de depósito
  - Formularios valorados/numerados
  - Sellos de caja
  - Llaves de Bóveda
  - Llaves de Cajas de Seguridad
  - Sobres con combinaciones

## **Factores de riesgo a considerar en la elaboración de procesos operacionales en instituciones financieras**

- Documentos
  - Pagarés
  - Garantías
  - Contratos
  - Tarjetas de firma
  - Documentación sensitiva de clientes
  - Recursos Humanos

## ¿Cómo documentar procedimientos?

### Compromiso gerencial

- Es la clave del éxito o del fracaso
- Sin el compromiso de la gerencia la infraestructura para las políticas y procedimientos eventualmente fracasará

## ¿Cómo documentar procedimientos?

### Efectividad

- Efecto decidido, decisivo y deseado
- Bien coordinado
- Competente
- Impresionante
- Poderoso
- Convincente
- Capaz/efectivo

**... todos se pueden medir !**

## ¿Cómo documentar procedimientos?

Bien coordinado

- Implica que el asunto se ha compartido y hablado/coordinado con los dueños del proceso
- La participación facilita la aceptación del cambio
- Los flujogramas son excelentes herramientas de diálogo

## ¿Cómo documentar procedimientos?

### Convincentes

- Sugiere que las políticas y procedimientos contienen:
  - Beneficios al lector
  - Son fáciles para entrenar, entender y aplicar al ambiente de trabajo
- Implica que un formato estructurado fue utilizado



## ¿Cómo documentar procedimientos?

### Capaces y competentes

- Sugiere que:
  - Se escogió la mejor solución posible
  - Se utilizaron herramientas apropiadas en el proceso de evaluación
- El endoso gerencial es evidente

## ¿Cómo documentar procedimientos?

### Plan de acción

- Instrucciones detalladas paso a paso y de principio a fin para asegurar un claro entendimiento de lo que se quiere lograr

Ciclo de mejoramiento	Pasos
Análisis e investigación	Planificar
Publicación y comunicación	Hacer
Verificación y auditoría	Verificar/controlar
Reporte y mejora	Actuar

## ¿Cómo documentar procedimientos?

### Representación gráfica

- **Un gráfico vale más que mil palabras**
- Los gráficos describen el proceso como es o como debe ser
- Utilizan símbolos, líneas y palabras que muestran gráficamente las actividades y secuencias del proceso
- El flujograma demuestra el tiempo, espacio, puntos de riesgo, desconexiones y puntos de control requeridos en un proceso
- El flujograma demuestra las funciones que interactúan con el proceso

## ¿Cómo documentar procedimientos?

### Formato estructurado básico

- Propósito
- Historial de revisiones
- Interacción de funciones
- Política
- Definiciones
- Responsabilidades
- Procedimientos

## ¿Cómo documentar procedimientos?

### Propósito

- Explique los objetivos para escribir el procedimiento
- Dos o tres oraciones son suficientes para un párrafo introductorio

### Ejemplo:

El presente procedimiento establece las guías para solicitar la compra de suministros con valor de \$500,000 o menos.

El proceso comienza con la preparación de la orden de compra y concluye con el pago de la factura al proveedor.

## ¿Cómo documentar procedimientos?

### Historial de revisiones

- Es un control de cambios del documento
- Provee el historial de cambios en el documento tales como mejoras al proceso, correcciones, actualizaciones, etc.
- Debe indicarse el número de versión del procedimiento
- Se recomienda su codificación
- Deben archivarse las diferentes versiones del documento

### Ejemplo:

## ¿Cómo documentar procedimientos?

### Historial de revisiones - Ejemplo:

Fecha	Descripción	Autor / Revisor / Aprobación
31 de mayo de 2018	Documento original	J. Sánchez (Analista del área XX) E. Aguirre (Gerente del área XX) E. Loayza (Gerente General) Acta de Directorio
15 de mayo de 2019	Actualización anual. Principales cambios: Cambio del límite de autorización del funcionario a cargo	L. Figueroa (Analista del área XX) E. Aguirre (Gerente del área XX) E. Loayza (Gerente General) Acta de Directorio

## ¿Cómo documentar procedimientos?

### Interacción de funciones

- Provee un listado de las funciones y funcionarios que interactúan con las políticas y procedimientos, interna o externamente

### Ejemplo:

Empleados, proveedores (internos y externos), clientes, áreas, funciones, sistemas, etc.



## ¿Cómo documentar procedimientos?

### Política

- Provee la estrategia organizacional de la institución o unidad, reflejando sus objetivos fundamentales, metas, visión y valores.
- Es una oportunidad para demostrar el enlace con las metas estratégicas del negocio

## ¿Cómo documentar procedimientos?

### Política - Ejemplo:

La política de esta compañía es asegurar:

1. Que todos los gastos por bienes y servicios son debidamente revisados y aprobados antes de su ejecución
2. La unidad de compras es la única autorizada para tranzar con proveedores por medio de órdenes de compra y comprometes fondos
3. ...

## ¿Cómo documentar procedimientos?

### Responsabilidades

- Ofrece un breve resumen de las responsabilidades de los funcionarios y unidades de negocio involucrados en el proceso
- Puede incluir el título funcional de la entidad: comprador, gerente, empleado, etc.

### Ejemplo:

1. El **agente de compras** es responsable de asegurar ...
2. Se espera que **los empleados** utilicen el formulario de compras más reciente publicado ...

## ¿Cómo documentar procedimientos?

### Procedimientos

- Define las guías, reglamentación, métodos, tiempo, lugar y personal responsable para lograr la política
- Debe ser consistente con el flujograma (en algunos casos puede ser reemplazado por el flujograma)
- El proceso se describe de principio a fin incluyendo todo insumo/producto y actividad que agrega valor

## ¿Cómo documentar procedimientos?

### Procedimientos

- Deben preferentemente mostrar los riesgos y controles definidos
- Pueden incluir los indicadores de gestión, así como los umbrales de logro a obtener, así como las medidas a tomar en caso que no se cumplan
- Las medidas en caso de contingencia



# Gestión de Operaciones en Empresas de Servicios Financieros Julio 2019

Econ. Alejandro Bazo Bertrán, MSc  
[bazo.alejandro@gmail.com](mailto:bazo.alejandro@gmail.com)  
<http://alejandrobazo.blogspot.pe/>

# RIESGO OPERACIONAL

## EJERCICIO 1: HERRAMIENTAS DE GESTIÓN – FLUJOGRAMAS DE PROCESOS

Revise el flujoograma de procesos de estudio y concesión de un crédito bancario que se muestra a continuación e identifique que puntos de riesgo existen en el proceso.

