



**ASOBANCARIA**

Construyendo  
la **Confianza** y **Solidez** del sector financiero

# Sistema de Administración de Riesgo Operacional – SARO

## Capacitación gremial a terceros

Vicepresidencia Técnica  
Dirección Financiera y de Riesgos

11 de abril de 2018



## Público asistente

- Representante Legal de la empresa o su delegado.
- Áreas gerenciales y administrativas encargadas de la administración de riesgos o de los procesos críticos (funcionarios del área de formación encargada de replicar la capacitación).
- Áreas de auditoría interna de cada tercero.

El ideal es que cada tercero replique esta presentación a todas las áreas de la organización involucradas en el cumplimiento del servicio





# Agenda

- 1 Objetivo
- 2 ¿Qué es riesgo operativo (RO)?
- 3 Riesgos asociados al RO
- 4 Antecedentes y gestión del RO en Colombia
- 5 Factores de riesgo
- 6 Sistema de Administración de Riesgo Operativo - SARO
- 7 Etapas del SARO
- 8 Seguridad de la información y continuidad del negocio



# Agenda

9

Clasificación eventos de riesgo RO

10

Servicio contratado con el tercero

11

Riesgos y eventos / ciclo de los eventos de riesgo operacional

12

¿Qué se espera de la gestión de los terceros?



# Agenda

- 1 Objetivo
- 2 ¿Qué es riesgo operativo (RO)?
- 3 Riesgos asociados al RO
- 4 Antecedentes y gestión del RO en Colombia
- 5 Factores de riesgo
- 6 Sistema de Administración de Riesgo Operativo - SARO
- 7 Etapas del SARO
- 8 Seguridad de la información y continuidad del negocio



## Objetivo

- a) Capacitar a los proveedores o terceros con los que nuestras entidades agremiadas tienen relaciones contractuales, y cuyo servicio involucra procesos y sistemas claves para la operación y cumplimiento de objetivos estratégicos de nuestras afiliadas.
  
- b) Concientizar a los proveedores y terceros sobre la importancia identificar, controlar y realizar seguimiento de los riesgos operacionales presentes en sus servicios y procesos.
  
- c) Identificar debilidades en el servicio contratado y oportunidades de mejora en los procesos.



# Agenda

- 1 Objetivo
- 2 ¿Qué es riesgo operativo (RO)?
- 3 Riesgos asociados al RO
- 4 Antecedentes y gestión del RO en Colombia
- 5 Factores de riesgo
- 6 Sistema de Administración de Riesgo Operativo - SARO
- 7 Etapas del SARO
- 8 Seguridad de la información y continuidad del negocio



# ¿Qué es riesgo operativo (RO)?

1.



**Personas**

2.



**Procesos**

3.



**Sistemas**

4.

**Eventos  
externos**



“ La posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos. Esta definición incluye el riesgo legal y reputacional, asociados a tales factores”





# Agenda

- 1 Objetivo
- 2 ¿Qué es riesgo operativo (RO)?
- 3 Riesgos asociados al RO**
- 4 Antecedentes y gestión del RO en Colombia
- 5 Factores de riesgo
- 6 Sistema de Administración de Riesgo Operativo - SARO
- 7 Etapas del SARO
- 8 Seguridad de la información y continuidad del negocio



## Riesgos asociados al RO

**RIESGO LEGAL:** :“Posibilidad de pérdida en que incurre una entidad al ser sancionada u obligada a indemnizar daños como resultado del incumplimiento de normas o regulaciones y obligaciones contractuales.”

**RIESGO REPUTACIONAL:** “Posibilidad de pérdida en que incurre una entidad por desprestigio, mala imagen, publicidad negativa cierta o no, respecto de la institución y sus prácticas de negocios, que cause pérdida de clientes, disminución de ingresos o procesos judiciales. “



# Agenda

- 1 Objetivo
- 2 ¿Qué es riesgo operativo (RO)?
- 3 Riesgos asociados al RO
- 4 Antecedentes y gestión del RO en Colombia**
- 5 Factores de riesgo
- 6 Sistema de Administración de Riesgo Operativo - SARO
- 7 Etapas del SARO
- 8 Seguridad de la información y continuidad del negocio



## Antecedentes y gestión del RO en Colombia

1975

- Comité de Basilea

1995

- Expedición Circular Básica Contable y Financiera que regula, entre otros, los riesgos asociados a la operación de cada entidad.

2006

- Expedición Circular Externa 48 que estableció instrucciones para la implementación del Sistema de Administración de Riesgo Operativo (SARO).

2007

- Expedición Circular Externa 41 estableció que en el marco del SARO las entidades deben diseñar, programar y coordinar **planes de capacitación anuales** para sus empleados y para los **terceros** con quienes existe una relación contractual y desempeñan funciones para la entidad.



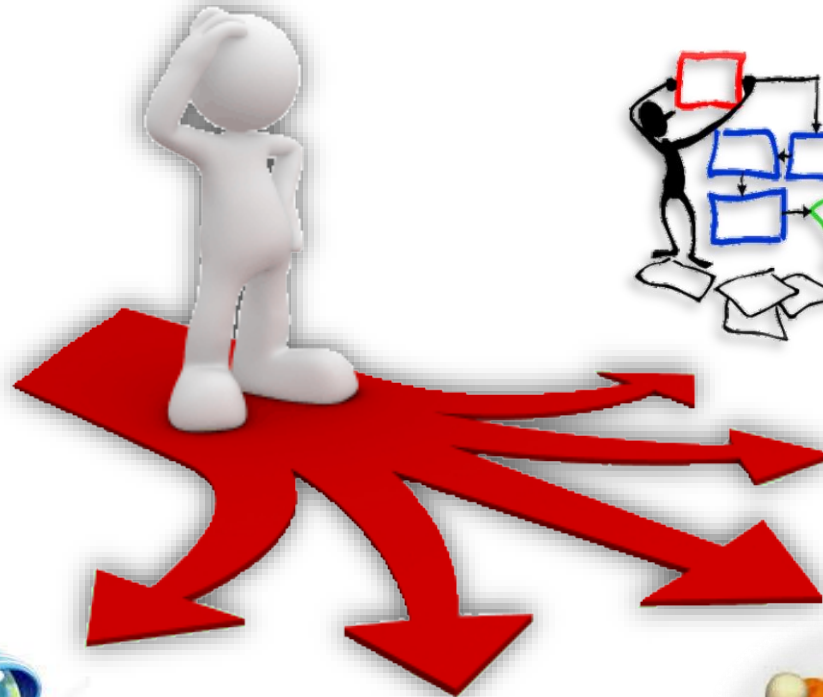
# Agenda

- 1 Objetivo
- 2 ¿Qué es riesgo operativo (RO)?
- 3 Riesgos asociados al RO
- 4 Antecedentes y gestión del RO en Colombia
- 5 Factores de riesgo**
- 6 Sistema de Administración de Riesgo Operativo - SARO
- 7 Etapas del SARO
- 8 Seguridad de la información y continuidad del negocio



# Factores de Riesgo:

“Fuentes generadoras de riesgos operativos que pueden generar pérdidas”



## Procesos



## Tecnología

- Hardware
- Software
- Telecomunicaciones



## Recurso humano

- Vinculación directa
- Vinculación indirecta (Outsourcing)



## Externos

- Fuerza la de naturaleza
- Ocasionado por terceros



## Infraestructura

- Edificios
- Espacios de trabajo
- Almacenamiento
- Transporte



# Ejemplos

## Procesos



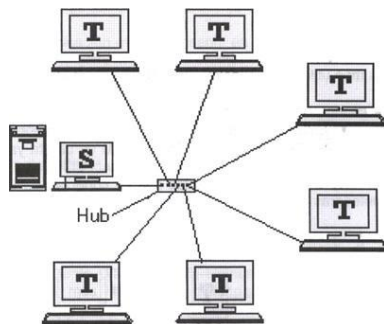
El pago de un cheque con  
limite de montos

## Recursos humanos



Errores, omisiones o inoportuna  
ejecución de los operaciones.

## Tecnología



Fallas o indisponibilidad de los  
sistemas.

## Eventos externos



Asalto en una sucursal de las  
Entidades.

## Infraestructura



Afectaciones en la  
infraestructura de oficinas o  
sucursales que puedan generar  
pérdidas.



# Agenda

- 1 Objetivo
- 2 ¿Qué es riesgo operativo (RO)?
- 3 Riesgos asociados al RO
- 4 Antecedentes y gestión del RO en Colombia
- 5 Factores de riesgo
- 6 Sistema de Administración de Riesgo Operativo - SARO**
- 7 Etapas del SARO
- 8 Seguridad de la información y continuidad del negocio





**ASOBANCARIA**

Construyendo  
la **Confianza** y **Solidez** del sector financiero

## ¿Qué es SARO?



“Conjunto de elementos tales como políticas, procedimientos, documentación, estructura organizacional, registro de eventos de riesgo operativo, órganos de control, plataforma tecnológica, divulgación de información y capacitación, mediante los cuales las entidades vigiladas identifican, miden, controlan y monitorean el riesgo operativo”.

**Fuente:** Circular Externa 041 de 2007



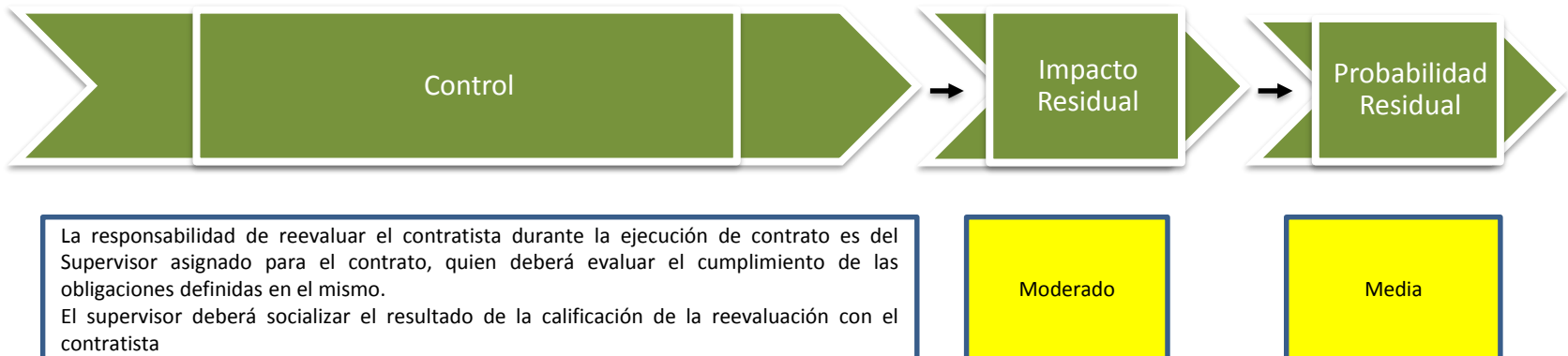
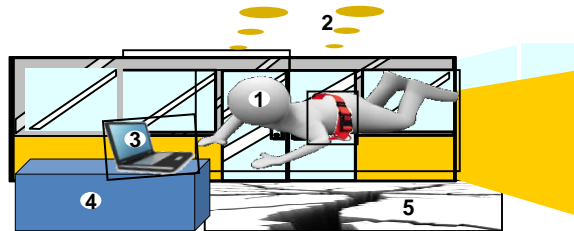
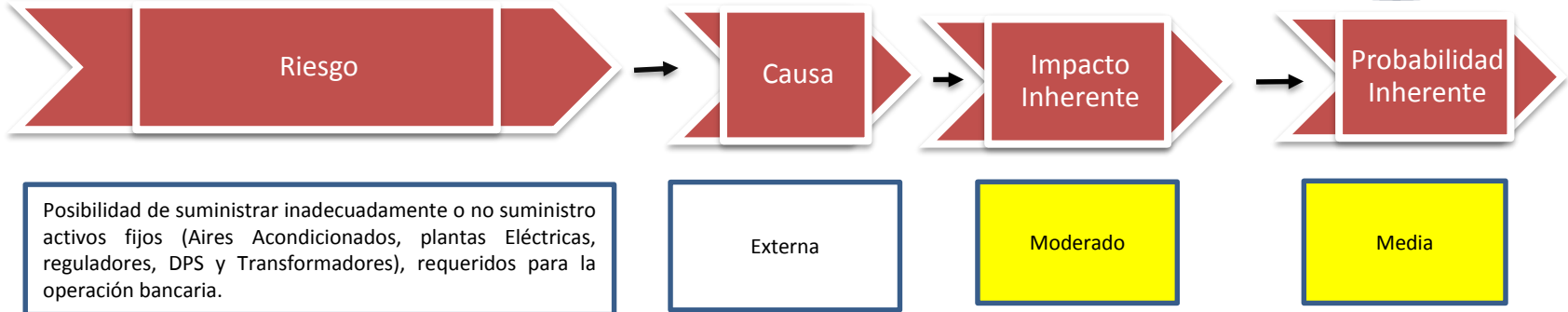
# Agenda

- 1 Objetivo
- 2 ¿Qué es riesgo operativo (RO)?
- 3 Riesgos asociados al RO
- 4 Antecedentes y gestión del RO en Colombia
- 5 Factores de riesgo
- 6 Sistema de Administración de Riesgo Operativo - SARO
- 7 Etapas del SARO**
- 8 Seguridad de la información y continuidad del negocio





# Ejemplos





# Agenda

- 1 Objetivo
- 2 ¿Qué es riesgo operativo (RO)?
- 3 Riesgos asociados al RO
- 4 Antecedentes y gestión del RO en Colombia
- 5 Factores de riesgo
- 6 Sistema de Administración de Riesgo Operativo - SARO
- 7 Etapas del SARO
- 8 Seguridad de la información y continuidad del negocio**



# Seguridad de la información

## Tercerización o Outsourcing

- Niveles de servicio y operación.
- Acuerdos de confidencialidad
- Restricciones sobre el software
- Normas de seguridad informática y física.
- Procedimientos y controles para la entrega y destrucción de la información.
- Planes de contingencia y continuidad.





# Plan de continuidad del negocio





# Agenda

9

Clasificación eventos de riesgo RO

10

Servicio contratado con el tercero

11

Riesgos y eventos / ciclo de los eventos de riesgo operacional

12

¿Qué se espera de la gestión de los terceros?





## Clasificación de los eventos de riesgo



**Fraude Externo:** Actos, realizados por una persona externa a la entidad, que buscan defraudar, apropiarse indebidamente de activos de la misma o incumplir normas o leyes.

Falsificación  
Robo  
Hackers



**Fraude interno:** Actos que de forma intencionada buscan defraudar o apropiarse indebidamente de activos de la entidad o incumplir normas o leyes, en los que está implicado, al menos, un empleado o administrador de la entidad.

Deslealtad de empleados  
Uso indebido de información



**Relaciones laborales:** Actos que son incompatibles con la legislación laboral, con los acuerdos internos de trabajo y, en general, la legislación vigente sobre la materia.

Demandas por  
discriminación  
Violación de normas  
laborales



## Clasificación de los eventos de riesgo



**Cientes:** Fallas negligentes o involuntarias de las obligaciones frente a los clientes y que impiden satisfacer una obligación profesional frente a éstos.

- Mal uso de la información confidencial de clientes.
- Actividades comerciales inadecuadas en cuentas propias.
- Venta de productos no autorizados.



**Daños a activos físicos:** Pérdidas derivadas de daños o perjuicios a activos físicos de la entidad.

- Terrorismo.
- Vandalismo.
- Terremotos
- Daños involuntarios causados por clientes o usuarios



## Clasificación de los eventos de riesgo



**Fallas tecnológicas:** Pérdidas derivadas de incidentes por fallas tecnológicas

- Caídas del software.
- Problemas de telecomunicaciones (Internet).
- Apagones públicos.



**Ejecución administración de procesos:** Pérdidas derivadas de errores en la ejecución y administración de los procesos.

- Errónea entradas de datos.
- Documentación legal incompleta.



# Agenda

9

Clasificación eventos de riesgo RO

10

Servicio contratado con el tercero

11

Riesgos y eventos / ciclo de los eventos de riesgo operacional

12

¿Qué se espera de la gestión de los terceros?



## Cajeros electrónicos - Eventos

Tipología de Riesgo	Eventos Presentados
<b>Ejecución y administración de procesos</b>	Entrega de dinero no acorde con lo solicitado por el cliente (excedentes / billetes falsos)
<b>Fallas tecnológicas</b>	Caída masiva de cajeros por fallas en el canal de comunicaciones.
<b>Clientes</b>	Debitados no dispensados.
<b>Relaciones laborales</b>	Demandas por Incumplimientos en los acuerdos contractuales con los empleados (salud ocupacional)
<b>Daños a activos físicos</b>	Daños a la infraestructura de los cajeros por asonadas / marchas públicas / atracos.
<b>Fraude Interno</b>	Instalación de dispositivos de clonación.
<b>Fraude Externo</b>	Instalación de Skimmer. Adulteración del cajero (cambio de teclado, intrusión de troyanos a través de USB)



# Agenda

9

Clasificación eventos de riesgo RO

10

Servicio contratado con el tercero

11

Riesgos y eventos / ciclo de los eventos de riesgo operacional

12

¿Qué se espera de la gestión de los terceros?



## Cajeros electrónicos - Riesgos

Factores de riesgo	
Factores Internos	Riesgos
Recurso humano	Ausencia del recurso humano o de personal crítico Desconocimiento en la ejecución de procesos Actividades para beneficio propio o de terceros Apropiación indebida de activos propios o de terceros
Procesos	Concentración de actividades críticas o falta de segregación. Inadecuado diseño del proceso Inexistencia de estándares. Inadecuada definición de perfiles de cargos
Tecnología	Suspensión parcial o temporal de servicios tecnológicos (fallos de programación en gestión de cambios y diferencias entre los ambientes de pruebas y producción) Fallas en hardware, software o comunicaciones
Infraestructura	Infraestructura física inadecuada (edificios, espacios de trabajo, almacenamiento y transporte).
Factores Externos	
Eventos de la naturaleza	Terremoto, vendaval, huracán, inundación, incendio y descargas eléctricas (rayos)
Ocasionados por terceros	Robo, terrorismo, sabotaje, ataques de denegación de servicio, virus, intrusiones y hacking, incendio, vandalismo.



# Agenda

9

Clasificación eventos de riesgo RO

10

Servicio contratado con el tercero

11

Riesgos y eventos / ciclo de los eventos de riesgo operacional

12

¿Qué se espera de la gestión de los terceros?





# ASOBANCARIA

---

Construyendo  
la **Confianza** y **Solidez** del sector financiero