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**

**9 de mayo 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 auditoria 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

ASOBANCARIA
Construyendo la Confianza y Solidez del sector financiero

# 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

# Agenda

ASOBANCARIA
Construyendo la Confianza y Solidez del sector financiero

# 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.

ASOBANCARIA
Construyendo la Confianza y Solidez del sector financiero

# 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”

**Fuente:** Circular Externa 041 de 2007

ASOBANCARIA
Construyendo la Confianza y Solidez del sector financiero

# 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. “

**Fuente:** Circular Externa 041 de 2007

ASOBANCARIA
Construyendo la Confianza y Solidez del sector financiero

# 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.

**Fuente:** Circular Externa 041 de 2007

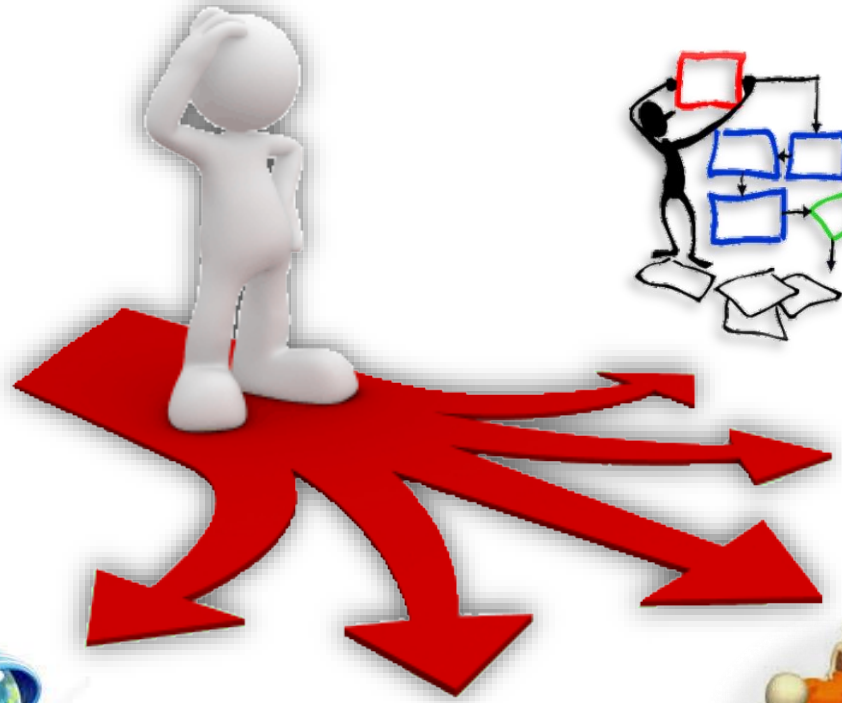
ASOBANCARIA
Construyendo la Confianza y Solidez del sector financiero

# 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

**Fuente:** Circular Externa 041 de 2007

# Ejemplos

## Procesos

**El pago de un cheque con limite de montos**

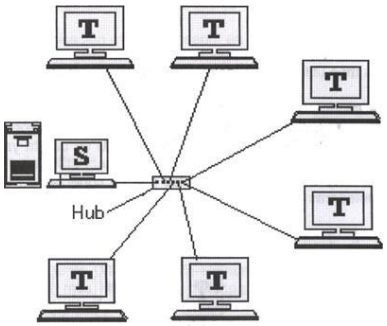
## Recursos humanos

**Errores, omisiones o inoportuna ejecución de los operaciones.**

## Infraestructura


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

## Tecnología




**Fallas o indisponibilidad de los sistemas.**

## Eventos externos

**Asalto en una sucursal de las Entidades.**

**Fuente:** Circular Externa 041 de 2007

ASOBANCARIA
Construyendo la Confianza y Solidez del sector financiero

# 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 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

ASOBANCARIA
Construyendo la Confianza y Solidez del sector financiero

# 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

# Etapas del SARO

**Identificación**

- Identificar y documentar el 100% los Procesos
- Metodologías de Identificación
- Identificación de riesgos

**Medición**

- Determinar y medir probabilidad e impacto

**Riesgo Inherente**

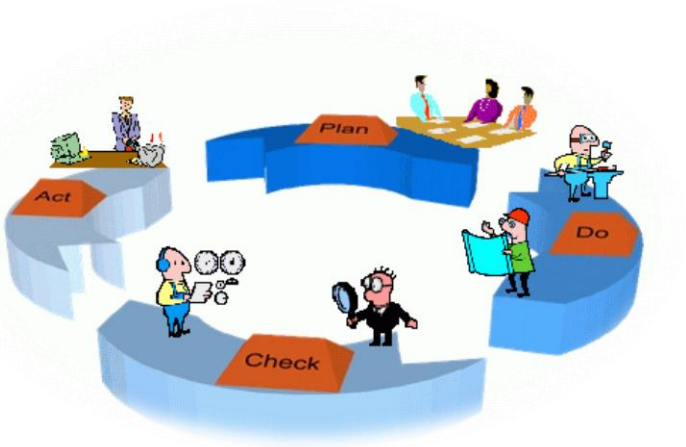
**Control**

- Medidas de control
- Administrar continuidad del negocio y seguridad de la información

**Riesgo Residual**

**Monitoreo**

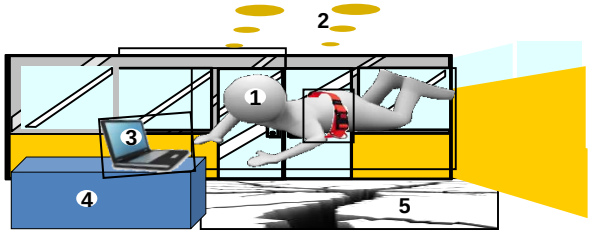
- Seguimiento del Perfil del Riesgo
- Exposición a pérdidas
- Indicadores SARO




**Fuente:** Circular Externa 041 de 2007

# Ejemplos

| Riesgo | Causa | Impacto Inherente | Probabilidad Inherente |
|---|---|---|---|
| Posibilidad de suministrar inadecuadamente o no suministro activos fijos (Aires Acondicionados, plantas Eléctricas, reguladores, DPS y Transformadores), requeridos para la operación bancaria. | Externa | Moderado | Media |




| Control | Impacto Residual | Probabilidad Residual |
|---|---|---|
| La responsabilidad de reevaluar el contratista durante la ejecución de contrato es del Supervisor asignado para el contrato, quien deberá evaluar el cumplimiento de las obligaciones definidas en el mismo.<br>El supervisor deberá socializar el resultado de la calificación de la reevaluación con el contratista | Moderado | Media |

ASOBANCARIA
Construyendo la Confianza y Solidez del sector financiero

# 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.


**Fuente:** Circular Externa 041 de 2007

# Plan de continuidad del negocio


**Fuente:** Circular Externa 041 de 2007

ASOBANCARIA
Construyendo la Confianza y Solidez del sector financiero

# Agenda

# 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 impliccado, 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

**Fuente:** Circular Externa 041 de 2007

# Clasificación de los eventos de riesgo

**Clientes:** 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

**Fuente:** Circular Externa 041 de 2007

# 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.

**Fuente:** Circular Externa 041 de 2007

ASOBANCARIA
Construyendo la Confianza y Solidez del sector financiero

# Agenda

# Agenda

# Desarrolladores de Software - Riesgos

| Factores de riesgo<br>Factores Internos | Riesgos |
|---|---|
| Recurso humano | Ausencia del recurso humano o de personal crítico<br>Desconocimiento en la ejecución de procesos<br>Actividades para beneficio propio o de terceros<br>Apropiación indebida de activos propios o de terceros |
| Procesos | Concentración de actividades críticas o falta de segregación.<br>Inadecuado diseño del proceso<br>Inexistencia de estándares.<br>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)<br>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. |

**Fuente:** información interna

# Desarrolladores de software – Riesgos - Eventos

Factores Internos

| Factores de riesgo | Riesgos | Eventos |
|---|---|---|
| Recurso humano | • Actividades para beneficio propio o de terceros<br>• Desconocimiento en ejecución de procesos<br>• Falta de comunicación efectiva o con demoras importantes | • Fraude Interno por uso de información confidencial o código fuente.<br>• Incapacidad para juzgar el alcance del software solicitado, error en la identificación de la funcionalidad requerida<br>• Incompatibilidades técnicas, demoras en actividades ya planeadas, costos excesivos |
| Procesos | • Demoras en la instalación de software y aplicaciones<br>• Concentración de actividades críticas o falta de segregación<br>• Inexistencia de estándares en los procedimientos<br>• Inadecuada definición de perfiles de cargos | • Incumplimiento de acuerdos de servicio<br>• Pérdida económica por fallas técnicas en el software solicitado<br>• Diseño inadecuado del software.<br>• Inexistencia de control de versiones de aplicativos |
| Tecnología | • Suspensión parcial o temporal de servicios tecnológicos (fallos de programación en gestión de cambios y diferencias entre los ambientes de pruebas y producción) | • Entrega de aplicativo que no cumple con la especificaciones de los usuarios<br>• Fallas en comunicaciones entre Banco – Proveedor<br>• Fallas en resguardo de línea base de aplicaciones. |
| Infraestructura | • Infraestructura física inadecuada (edificios, espacios de trabajo, almacenamiento y transporte).<br>• No contar con los equipos de soporte requeridos (USO, servidores, racks, etc) | • Cancelación e incumplimiento del proyecto por parte del Proveedor.<br>• Falta de capacidad para cumplir con los requerimientos del cliente. |

# Desarrolladores de software – Riesgos - Eventos

Factores Externos

| Factores de riesgo | Riesgos | Eventos |
|---|---|---|
| Eventos de la naturaleza | • Terremoto, vendaval, huracán, inundación, incendio y descargas eléctricas (rayos) | • Interrupción de los procedimientos durante el desarrollo del software |
| Ocasionados por terceros | • Robo, terrorismo, sabotaje, ataques de denegación de servicio, virus, intrusiones y hacking, incendio, vandalismo. | • Fraude por fuga de información de clientes o códigos fuente. |

**Fuente:** información interna

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

# 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