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

26 de septiembre 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

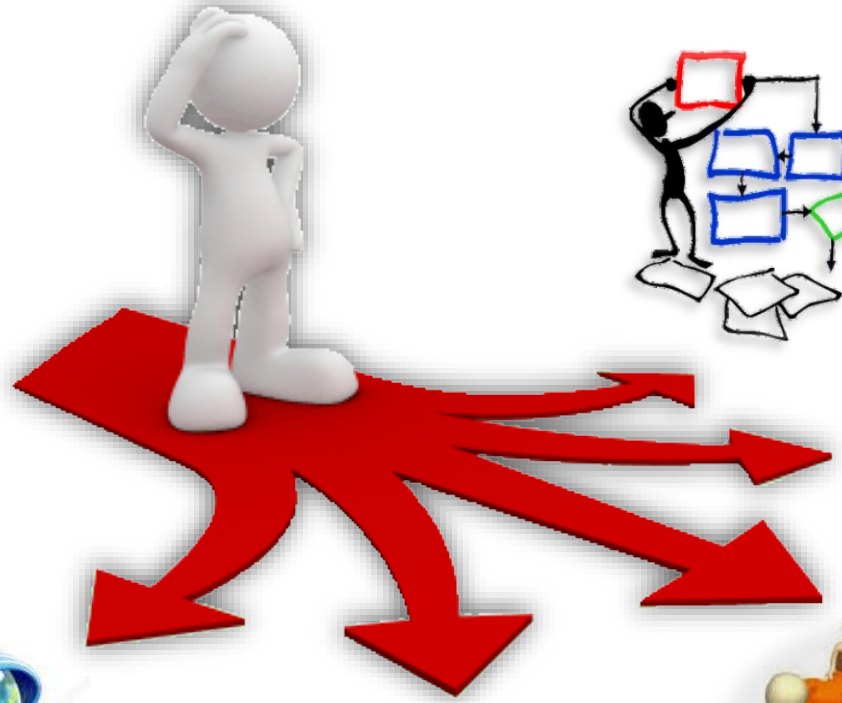
ASOBANCARIA
Construyendo la Confianza y Solidez del sector financiero

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

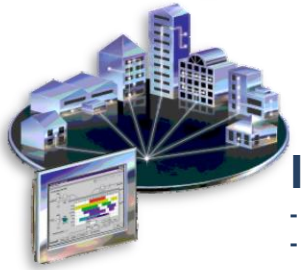
- Hardware
- Software
- Telecomunicaciones

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

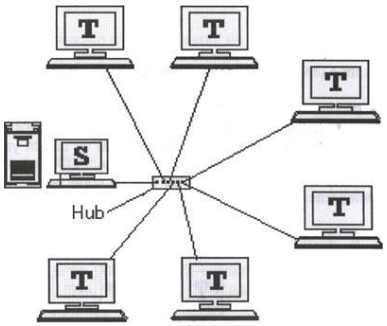
Recursos humanos

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

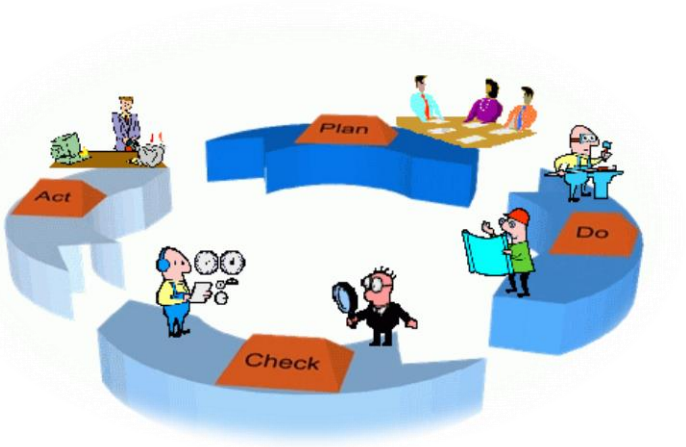
Control

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

Riesgo Residual

Monitoreo

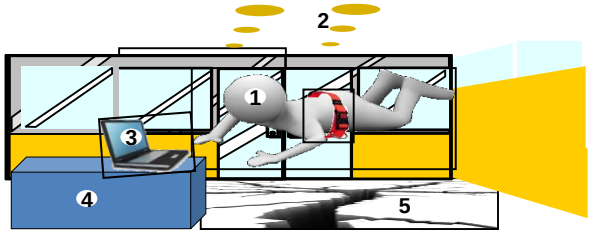
- Seguimiento del Perfil del Riesgo
- Exposición a pérdidas
- Indicadores SARO



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. 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

Telecomunicaciones - Eventos

Tipología de Riesgo	Eventos Presentados
Ejecución y administración de procesos	Caída del servicio por falla en ejecución de un protocolo.
Fallas tecnológicas	Indisponibilidad del servicio de aplicaciones. Intermitencia en servicio de internet. Penetración a los sistemas de información.
Clientes	Interrupción de los servicios.
Relaciones laborales	Demandas por Incumplimientos en los acuerdos contractuales con los empleados (salud ocupacional)
Daños a activos físicos	Daños de activos físicos que se presenten durante la ejecución de mantenimientos programados con terceros.
Fraude Interno	Colusión con el fin de permitir la fuga de información.
Fraude Externo	Acceso, alteración o fuga de información sensible para la compañía o sus clientes.
Cumplimiento	Incumplimiento en normatividad propia o de clientes por afectación del servicio.

Fuente: contratos con terceros y textos relacionados

Cajeros electrónicos - Eventos

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

Fuente: información interna

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.

Fuente: información interna

CALL CENTER - 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.

Fuente: información interna

CALL CENTER - Eventos

Tipología de Riesgo	Eventos Presentados
Ejecución y administración de procesos	No generar el reporte del bloqueo por pérdida o robo de tarjetas puede dar lugar a fraudes que el banco deberá asumir mediante el reintegro del dinero al cliente. Incumplimiento de normas legales y reglamentarias (consulta en centrales de riesgo sin autorización) Ventas Inconsistentes Incumplir con el marco legal de higiene y seguridad industrial en los puestos de trabajo Ingreso de personal y/o dispositivos de almacenamiento no autorizados a las áreas restringidas.
Fallas tecnológicas	Fallas en aplicativos de consulta La indisponibilidad del servicio puede ocasionar incumplimiento de metas comerciales.
Clientes	Pérdida de documentación confidencial Inconformismo de clientes por atención inadecuada por parte de los funcionarios del call center.
Relaciones laborales	Demandas por incumplimientos en los acuerdos contractuales con los empleados (salud ocupacional)
Daños a activos físicos	Instalaciones sin las condiciones de seguridad adecuadas: biométricos, puertas de exclusa, autorización de ingreso, sistemas antiincendios, sistemas de aire acondicionado.
Fraude Interno	Extracción no autorizada de información confidencial
Fraude Externo	Extracción no autorizada de información confidencial

Fuente: información interna

Cobranza - Riesgos

Factores de riesgo Factores Internos	Riesgos
Recurso humano	• Desconocimiento del proceso y falta de acompañamiento al momento de asignación, en el que detiene el proceso y activación del plan de contingencia
Procesos	• Recepción de pagos en cobro jurídico por recaudo empresarial y no conforme al proceso • Pagos ACH con rechazo por insuficiencia de fondos, generando gastos y reprocesos en la reversión de las operaciones. • Falla en la verificación de documentación para proceso jurídicos • Error en la aplicación de refinanciaciones por archivo de cargue • Recepción de pagos de clientes de Leasing Habitacional en el cual el dictamen del Juez es la restitución del bien • No bloqueo de productos de TC cuando se presentan unificación de productos y/o cancelación. • Administración y manejo de claves de acceso a los sistemas de información.
Tecnología	• Error en la integración de aplicativos, que genera retrasos y/o inconsistencias en la entrega de información al cliente. • Fallas en los transfer de llamadas de un servidor a otro. • Perdidas de grabación de llamadas • Fallas en el cierre de cobranzas

Fuente: información interna

Cobranza - Eventos

Tipología de Riesgo	Eventos Presentados
Fraude Externo	Fuga de información, dado a la existencia de una URL publica la cual se puede acceder desde cualquier ubicación y sin ninguna restricción , en donde se hayan documentos con información confidencial del Banco y de clientes.

Fuente: información interna

Corresponsales Bancarios - 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.

Fuente: información interna

Corresponsales Bancarios - Eventos

Tipología de Riesgo	Eventos Presentados
Ejecución y administración de procesos	Diferencias en las operaciones realizadas y reportadas.
Fallas tecnológicas	Interrupción del servicio a nivel nacional por falla en las comunicaciones.
Clientes	Cliente insatisfecho con la atención recibida por parte del Corresponsal Bancario.
Relaciones laborales	Demandas por Incumplimientos en los acuerdos contractuales con los empleados (salud ocupacional).
Daños a activos físicos	Daño de los datafonos suministrados a los corresponsales bancarios
Fraude Interno	Infidelidad de empleados o de los corresponsales bancarios da lugar a fraudes por copiado de información.
Fraude Externo	Robo y/o atraco.

Fuente: información interna

Desarrolladores de Software - 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.

Fuente: información interna

Desarrolladores de software – Riesgos - Eventos

Factores Internos

Factores de riesgo	Riesgos	Eventos
Recurso humano	• Actividades para beneficio propio o de terceros • Desconocimiento en ejecución de procesos • Falta de comunicación efectiva o con demoras importantes	• Fraude Interno por uso de información confidencial o código fuente. • Incapacidad para juzgar el alcance del software solicitado, error en la identificación de la funcionalidad requerida • Incompatibilidades técnicas, demoras en actividades ya planeadas, costos excesivos
Procesos	• Demoras en la instalación de software y aplicaciones • Concentración de actividades críticas o falta de segregación • Inexistencia de estándares en los procedimientos • Inadecuada definición de perfiles de cargos	• Incumplimiento de acuerdos de servicio • Pérdida económica por fallas técnicas en el software solicitado • Diseño inadecuado del software. • 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 • Fallas en comunicaciones entre Banco – Proveedor • Fallas en resguardo de línea base de aplicaciones.
Infraestructura	• Infraestructura física inadecuada (edificios, espacios de trabajo, almacenamiento y transporte). • No contar con los equipos de soporte requeridos (USO, servidores, racks, etc)	• Cancelación e incumplimiento del proyecto por parte del Proveedor. • 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

Seguridad de la información - 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.

Fuente: información interna

Seguridad de la información - Eventos

Tipología de Riesgo	Eventos Presentados
Ejecución y administración de procesos	El alcance y divulgación de políticas de seguridad no tiene una cobertura total del perímetro, lo cual dejó zonas descubiertas.
Fallas tecnológicas	Vulnerabilidades no detectadas que afectaron el servicio y permitieron el ingreso de troyanos.
Clientes	Pérdida de información.
Relaciones laborales	Demandas por Incumplimientos en los acuerdos contractuales con los empleados (salud ocupacional)
Daños a activos físicos	Daños de activos físicos que se presenten durante la ejecución de mantenimientos programados con terceros.
Fraude Interno	Pérdida de información por extracción de bases de datos.
Fraude Externo	Descargas de correos que contienen malware y generan pérdida o modificación de información.

Fuente: información interna

Tarjetas - 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.

Fuente: información interna

Tarjetas - Eventos

Tipología de Riesgo	Eventos Presentados
Ejecución y administración de procesos	Retrasos en la entrega de tarjetas. Personalización realizada en plástico errado.
Fallas tecnológicas	Caídas en el canal de comunicación.
Clientes	Productos defectuosos.
Relaciones laborales	Demandas por Incumplimientos en los acuerdos contractuales con los empleados (salud ocupacional)
Daños a activos físicos	Pérdida o deterioro durante la custodia de plásticos que son propiedad del banco.
Fraude Interno	Fuga de información.
Fraude Externo	Intrusión de terceros ajenos al proveedor a los lugares de custodia y personalización de tarjetas.

Fuente: información interna

Transporte de valores - 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.

Fuente: información interna

Transporte de valores - Eventos

Tipología de Riesgo	Eventos Presentados
Ejecución y administración de procesos	Entrega de dinero no acorde con lo solicitado por el cliente (excedentes / billetes falsos). Pérdidas de títulos valores. Incumplimiento de la ejecución de los recaudos o aprovisionamientos programados por eventos externos
Fallas tecnológicas	Caídas del sistema que impida la apertura de bóvedas con cerradura IP. Fallas en comunicaciones.
Clientes	Abuso de confianza con clientes. Proporción de información errada a clientes en las oficinas.
Relaciones laborales	Abuso de confianza entre los empleados y los funcionarios de la empresa transportadora. Incumplimiento de las condiciones legales y contractuales con los empleados en misión.
Daños a activos físicos	Fallas mecánicas en vehículos de transporte de valores. Colisión de vehículos transportadores. Falta de mantenimiento de los vehículos transportadores.
Fraude Interno	Colusión. Infidelidad de los funcionarios de la transportadora.
Fraude Externo	Ataque o hurto a vehículos transportadores de valores (camiones y helicópteros) Ataque o hurto a bóvedas. Suplantación del personal de la transportadora que ejecuta el servicio.

Fuente: información interna

Vigilancia privada - 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.

Fuente: información interna

Vigilancia privada - Eventos

Tipología de Riesgo	Eventos Presentados
Ejecución y administración de procesos	Por falta de presencia de vigilantes asignados se presentan robos a oficinas. Ingreso de personal no autorizado a zonas restringidas en oficinas. No tener el certificado de manejo de armas y los salvoconductos de las armas actualizado.
Fallas tecnológicas	Daños en sistemas de monitoreo y comunicación. Falta de oportunidad en el mantenimiento de las herramientas de monitoreo y control de la seguridad de las oficinas.
Clientes	No identificación de marcadores (delincuentes) en las oficinas que repercute en fleteo. Exceso de fuerza con los clientes por infringir las políticas de seguridad establecidas en las oficinas.
Relaciones laborales	Abuso de confianza entre los empleados y los funcionarios de la empresa de seguridad.
Daños a activos físicos	Intrusión de personal, dañando los vidrios de la ventanas y la puerta de ingreso a la sede del banco. Daños en bóveda.
Fraude Interno	Colusión con grupos al margen de la ley.
Fraude Externo	Ingreso a la sede del banco, intimidando al personal de vigilancia, para ejecutar hurto de oficinas.

Fuente: información interna

Outsourcing - Riesgos selección/canje/centrales de riesgo

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.

Fuente: información interna

Outsourcing - Eventos recursos humanos

Tipología de Riesgo	Eventos Presentados
Ejecución y administración de procesos	Suministro de información errada o no autorizada. Vinculación de personal relacionado con delincuencia común. Incumplimiento en el pago de obligaciones con los colaboradores en misión
Fallas tecnológicas	Pérdida de la integridad de la información para dispersión de nómina.
Clientes	Personal no cualificado que impacte la gestión operativa y de servicio del banco.
Relaciones laborales	Incumplimiento de las condiciones legales y contractuales con los empleados en misión.
Fraude Interno	Actos ilícitos, actos inmorales de los empleados en misión para con el Banco y sus clientes. Violación de los acuerdos de confidencialidad.

Fuente: información interna

Outsourcing- 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 Fraude interno (Violación de la confidencialidad de información)
Procesos	Concentración de actividades críticas o falta de segregación. Inadecuado diseño del procesos o procesos poco eficientes (Documentos) 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) Caída de las replicas en línea Fallas en hardware, software o comunicaciones
Infraestructura	Infraestructura física inadecuada (edificios, espacios de trabajo, almacenamiento y transporte). Recursos necesarios para la subcontratación del servicio requerido
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, protestas, manifestaciones, incendio, vandalismo, intrusiones y hacking (fraude externo).

Fuente: información interna

Outsourcing- Eventos

Tipología de Riesgo	Eventos Presentados
Ejecución y administración de procesos	Pérdida de documentos en el trasporte o custodia. Ingreso de personal no autorizado a zonas restringidas en oficinas (centros de computo). No tener la formación o experiencia en el manejo de personal (empresas de servicos temporales). No señalización de actividades realizadas (pisos húmedos, trabajos eléctricos, remodelaciones o caída de objetos) Inadecuada digitalización de documentos
Fallas tecnológicas	Daños en sistemas de monitoreo y comunicación. Falta de oportunidad en el mantenimiento de las herramientas Fallas en Scaners
Clientes	No atención de requerimientos, especialmente en temas de alta disponibilidad. No cumplimiento de los requisitos contractuales.
Relaciones laborales	Abuso de confianza entre los empleados y los funcionarios de la empresa del servicio contratado.
Daños a activos físicos	Daños a bienes de la entidad por acción, omisión o accidental. Daños en los equipos eléctricos. Daños por mal uso de activos.
Fraude Interno	Colusión con grupos al margen de la ley o apoyar por acción u omisión. Violación a los acuerdos de confidencialidad
Fraude Externo	Ingreso no autorizado a aplicaciones o a equipos. Robo. Ciberataques.

Fuente: información interna

Documentos- Riesgos

Factores de riesgo Factores Internos	Riesgos
Recurso humano	Ausencia del recurso humano o de personal crítico para realizar las actividades de digitación, digitalización o de disposición de documentos. Desconocimiento en la ejecución de procesos (Alta Rotación sin la debida capacitación). Actividades para beneficio propio o de terceros (Alteración de documentos, perdida de pagares) Apropiación indebida de activos propios o de terceros (Títulos valores, plásticos, pagares, etc.)
Procesos	Concentración de actividades críticas o falta de segregación (Captura, digitalización y validación documental ejecutada por el mismo funcionario) Inadecuado diseño del proceso. Tipos documentales nuevos gestionados fuera del proceso establecido. Inexistencia de estándares (Políticas para cada tipo documental) Inadecuada definición de perfiles de cargos para realizar la actividades del proceso
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.

Fuente: información interna

Documentos- Eventos

Tipología de Riesgo	Eventos Presentados
Ejecución y administración de procesos	Fallas en los procesos de control documental (Listas de chequeo de los tipos documentales recibidos). Informar inoportunamente inconsistencias en la documentación o no realizar el debido seguimiento para regularizarlos. Pérdidas de pagarés: implica no poder iniciar procesos ejecutivos. Errores de indexación o digitación de los documentos físicos en los aplicativos, digitalización o de disposición de documentos: el no poder soportar la operaciones puede ocasionara que el banco tenga que asumir pérdidas. Documentos no encontrados, pérdida de trazabilidad, no se puede sustentar reclamaciones de clientes o atender requerimientos de entes de vigilancia y control. Entrega de documentación trocada o digitalizar a nombre de clientes incorrectos. Incumplimiento de acuerdos de servicio que impacten procesos posteriores de análisis de crédito, legalizacion, desembolso, cobranza, cartera, recaudos (Bouchers), mercadeo (campañas), etc.
Fallas tecnológicas	Fallas en aplicativos de consulta de documentos digitalizados. Ventanas de mantenimiento que impacte el servicio en los procesos documentales. Perdida de información por cambios de software (Ejemplo: Fusiones o adquisiciones de empresas en las que se pierden los históricos documentales).
Clientes	Pérdidas de documentación confidencial y/o garantías.
Relaciones laborales	Pérdida de demandas laborales por falta de documentación soporte.
Daños a activos físicos	Deterioro de documentos custodiados por deficiencia en la infraestructura (Humedad o temperatura inadecuada para la custodia documental, sistemas de ventilación insuficientes, etc.).
Fraude Interno	Fuga de información confidencial.
Fraude Externo	Intrusión de terceros ajenos al proveedor a los lugares de custodia.

Fuente: información interna

ASOBANCARIA
Construyendo la Confianza y Solidez del sector financiero

Telecomunicaciones - Riesgos

Factores de riesgo Factores Internos	Riesgos
Recurso humano	Ausencia del recurso humano vital para la ejecución de procesos críticos. Desconocimiento e inexperiencia en la ejecución de procesos críticos. Ejecución de procedimientos para beneficio propio o de terceros Aprovechamiento de activos de la compañía o de terceros para beneficio propio
Procesos	Concentración de actividades críticas o falta de segregación. Inadecuado diseño y ejecución del proceso Inexistencia de estándares. Inadecuados niveles de autorización y escalamiento en los procesos.
Tecnología	Indisponibilidad total o parcial de servicios contratados Fallas en hardware, software o canales d comunicación Errores en implementación de actualizaciones Ciberataques Vulnerabilidades no gestionadas ni corregidas.
Infraestructura	Falla en condiciones físicas requeridas en datacenter Estimación inadecuada de la capacidad de procesamiento Infraestructura física inadecuada (capacidad limitada)
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. Daño en infraestructura por mantenimientos de proveedores de otros servicios.

Agenda

ASOBANCARIA

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