

Riesgo Operativo



1. Conceptos

a) Generales

Riesgo

Eventos que pueden ocasionar pérdidas financieras o conflictos legales, sociales, ambientales, de imagen, entre otras.

Causa

Motivo por el que existe el riesgo, es una debilidad o vulnerabilidad.

Controles

Actividades que minimizan o disminuyen el impacto o la probabilidad de un riesgo.

Riesgo Operativo

Posibilidad que se ocasionen pérdidas financieras derivadas en fallas o insuficiencias en los procesos, personas, tecnologías, o eventos externos.

RIESGOS EN INSTITUCIONES FINANCIERAS



b) Factores de Riesgo Operativo



Procesos: Inadecuado diseño de procesos, proceso no documentado, políticas desactualizadas.



Personas: Proceso de selección inadecuado, accidente laboral, fraude interno, incumplimiento de procesos.



Tecnología / Seguridad de la Información: Fallas en la seguridad informática, error en el diseño de aplicativos, fallas en las telecomunicaciones, error en ejecución de procesos de sistemas.



Eventos Externos: Fraude externo, catástrofes naturales, robos y asaltos, cambios en las regulaciones.

c) Tipos de Riesgo



Fraude Interno: Cualquier apropiación indebida de activos o creación de pasivos falsos que involucre al menos una persona que labora en la institución.



Fraude Externo: Cualquier acto ejecutado por personas ajenas al banco, destinados a defraudar, usurpar la propiedad o evadir la ley.



Interrupción del negocio por Fallas en la Tecnología de la Información: Interrupción de las actividades del negocio por fallas o caídas en los sistemas de información.



Deficiencias en el diseño y/o Ejecución de procesos, procesamiento de operaciones y relaciones con proveedores y terceros: Eventos que hayan sido provocados por fallas en el diseño, levantamiento, actualización de políticas y procesos; específicamente funcionales a sistemas; manuales incompletos o no documentados; falta de automatización de procesos y/o controles; falta de difusión y desconocimiento.



Prácticas laborales y seguridad del ambiente de trabajo: Actos inconsistentes con las leyes o contratos de empleo, salud o seguridad que resulten en el pago de reclamos, perjuicios al personal, o reclamos relacionados con temas de discriminación.



Daños a los activos físicos: Pérdida o daños a los activos físicos por desastre natural u otros eventos.

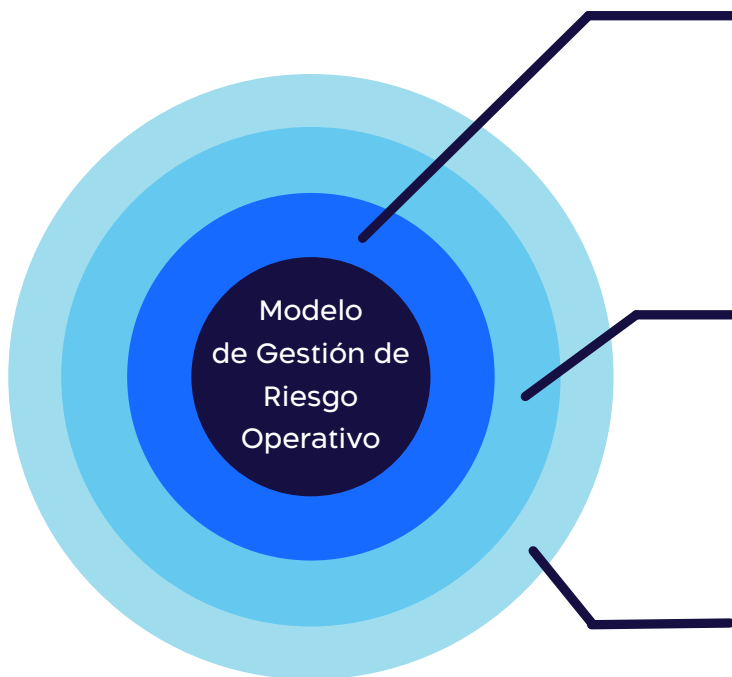


Prácticas relacionadas con los clientes, productos y el negocio: Fallas que impidan cumplir con las obligaciones profesionales con clientes, por la naturaleza o diseño del producto o servicio.



2. Modelo de Gestión de Riesgo Operativo

La gestión de riesgo operativo es un modelo de colaboración basado en el esquema de control en tres capas o líneas de defensa que permite una efectiva identificación de riesgos y controles de acuerdo a directrices y mejores prácticas a nivel mundial.



UNIDAD DE NEGOCIO Y SOPORTE:

Primera línea de defensa, responsable del negocio, incluyendo los riesgos y controles existentes o planes de acción de los procesos bajo su gestión.

UNIDAD DE RIESGO:

Segunda línea de defensa, responsable del diseño de metodologías y supervisión de los riesgos identificados en coordinación con el responsable de negocio o soporte.

AUDITORÍA:

Tercera línea de defensa, responsable de revisar la efectividad y eficacia de los controles implementados.



3. Herramienta de Reporte de Riesgo

Todos los colaboradores somos responsables de identificar riesgos, fallas o insuficiencias de sus procesos.

¡Todos podemos reportar la gestión de riesgos en la herramienta disponible en el portal Vamos!

