Gestión de riesgos operativos y digitales en el mundo financiero

Procesos de identificación, valoración, registro y reporte

Rafael Salas, Septiembre 2021

Reglas del Zoom

- Colocar Nombre y Apellido
- Identificar su organización, ej: Rafael Salas – Noesis
- Todos estan con el micrófono en mudo
- Es gentil estar con los videos abiertos.
- Para preguntas vamos a abrir los microfonos anotense las preguntas para no perderlas.
- Vamos a tener Break en intervalos.

Agenda

Modulo I – Riesgo Operativo

Modulo II – Riesgos en la Digitalización

Modulo III – Registro y evaluación de Riesgos Efectivos

Modulo IV - Reportes

MODULO I

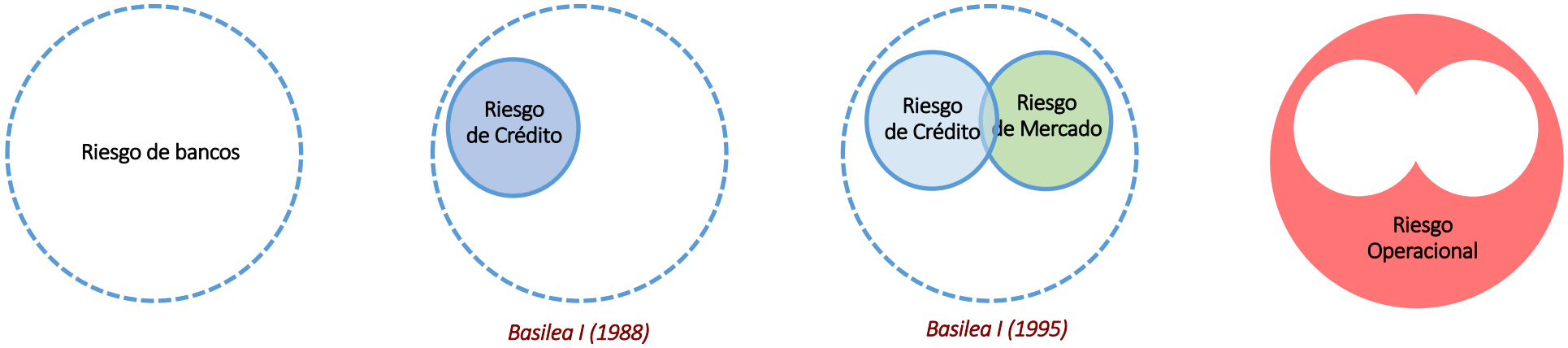
GESTIÓN DE RIESGO OPERATIVO EN EL MUNDO FINANCIERO

Introducción

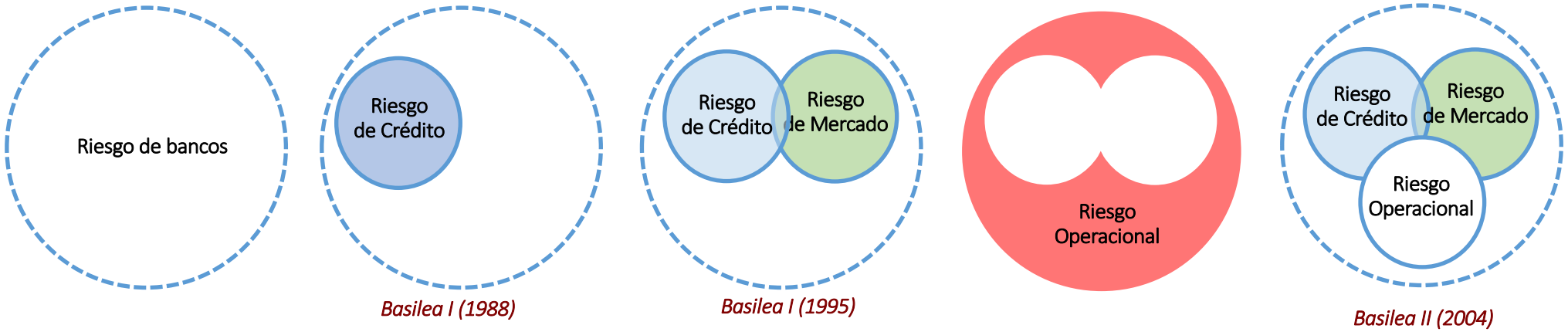
Los riesgos operativos son la causa fundamental de muchas de las fallas financieras importantes de las últimas décadas. Los estudios señalan que los riesgos operativos no son nuevos: errores humanos, fraude, robo, fallas de procesos, errores del sistema y peligros externos, como incendios e inundaciones, existen desde hace décadas. Sin embargo, el impacto de los riesgos operativos fue a menudo relativamente insignificante. Por el contrario, las tendencias recientes como la globalización, la conectividad global a Internet y las dependencias de la cadena de valor han hecho que los riesgos operativos sean más importantes que nunca.

Introducción

La gestión del riesgo operacional se había definido en el pasado como todo riesgo que no se refleja en los programas de gestión de riesgo crediticio y de mercado. Los primeros programas de riesgo operacional, por lo tanto, consideraron que si no era riesgo de mercado y no era riesgo de crédito, entonces debía ser riesgo operacional.



Definición



La definición de riesgo operativo de Basilea II es:

el riesgo de pérdida directa o indirecta como reultado de procesos inadecuados, falla interna humana, sistemas inadecuados o de eventos de carácter externo.

Esta definición incluye el riesgo legal, pero excluye el riesgo estratégico y reputacional.

¿Que hacemos con Mickey Mouse?

Basilea II (2004)

Riesgo Estratégico o Reputacional

La definición en sus componentes.

1.- Debe haber riesgo de pérdida. Entonces, para que exista un riesgo operacional, debe haber una pérdida asociada anticipada.

2.- Las causas definidas de esta pérdida. La definición anterior proporciona cuatro causas que pueden dar lugar a pérdidas por riesgo operacional. Estas cuatro causas son:

- procesos inadecuados o fallidos,
- fallas relacionadas al factor humano
- sistemas inadecuados o fallidos
- eventos de carácter externos.

Veamos las noticias

ÚLTIMAS NOTICIAS Hemeroteca Código de ética Contáctenos

Página SIETE

Diario Nacional Independiente

6°

mas info

SECCIONES OPINIÓN CAMPEONES SUPLEMENTOS

Crece polémica por dedo en una hamburguesa, hay antecedentes

El viceministro Silva criticó a Gobernador y Alcalde cruceños por salir en defensa de la empresa. Conminan a indemnizar al empleado afectado.

ÚLTIMAS NOTICIAS Hemeroteca Código de ética Contáctenos

Página SIETE

Diario Nacional Independiente

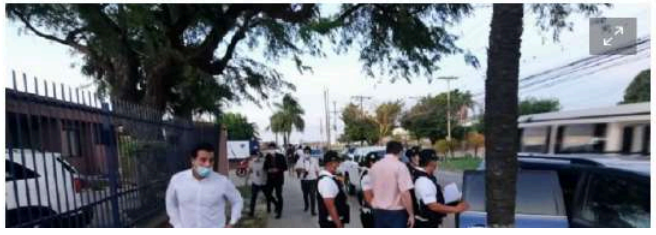
6°

mas info

SECCIONES OPINIÓN CAMPEONES SUPLEMENTOS

Caso Multipartes: allanan una imprenta y hallan más indicios de falsificación de repuestos

El lunes se llevó a cabo el allanamiento de una imprenta donde se falsificaban etiquetas para autopartes de la marca Toyota.



DW Made for minds.

ACTUALIDAD MULTIMEDIA TV APRENDER ALEMÁN

AMÉRICA LATINA CORONAVIRUS POLÍTICA ECONOMÍA CULTURA CIENCIA Y ECOLOGÍA

ACTUALIDAD / AMÉRICA LATINA

América Latina: Tendencias y pronósticos de metales & minería, la cadena de suministro, factores ambientales y sociales, telecomunicaciones, y más.

AMÉRICA LATINA

Ciberataques aumentaron 24% en América latina este año

El gigante ruso Kaspersky detectó más de 173.000 intentos de infección a dispositivos móviles entre enero y agosto de 2021 en la región (casi 20 ataques por hora), siendo los troyanos una de las principales amenazas.

Los Tiempos NO SE DETIENE

Actualidad Deportes Tendencias Doble Click OH! Lecturas Es

Actualidad

Inicio Últimas Mundo País Economía Cochabamba Seguridad Editorial y Puntos de Vis

Banco Unión: Fraude fue contra la cuenta de una persona utilizando documentación falsa

Economía

Pregunta

¿Cuáles son los 10 riesgos operativos que su empresa va a enfrentar durante el 2021 y 2022?

¿Porqué?

Top 10 Operational Risks

- Fuente: Risk.net Agosto, 2021

	2021	2020	Change
IT disruption	1	1	
Data compromise	2	2	
Resilience risk	3	5	↑
Theft and fraud	4	3	↓
Third-party risk	5	4	↓
Conduct risk	6	7	↑
Regulatory risk	7	8	↑
Organisational change	8	6	↓
Geopolitical risk	9	9	↑
Employee wellbeing	10	-	

Un punto de partida eficaz es evaluar las causas clave de las fallas de sus compañías.

Market Risk

Eventos catastróficos

Errores Operativos

Tercerización
Relaciones con Terceros

Forex

Legal

Regulación

Reputación

Liquidity Risk

Interrupciones de IT

Datos

Reportes

Fallas en Inversiones

Falla en las reservas

Strategic Risk

Incompetencia

Fraude

Habilidades/Capacidades del personal

Cambio Organizacional

Proyectos mal manejados

Drivers Actuales

- Hoy, cada vez es más complejo para los directivos de las empresas poder **controlar las variables** que pueden afectarlas, hay mucho que hacer en áreas cada vez más complejas, el tiempo es un gran limitante y **la información está incompleta** (Porter, 2009)
- **Para poder mejorar la *performance* de una empresa** se debe cumplir con una serie de principios de acción a saber: **actuar con transparencia**, **alcanzar los compromisos adquiridos** y **conseguir confianza** (Covey, Whitman, & England, 2011)
- **Cada vez es más complejo alcanzar las metas corporativas** (Prahalad & Hamel, 2016).
- **La incertidumbre es considerada un estado constante**, un elemento de la vida de la organización, la cual surge de dos factores: la complejidad y el dinamismo (Bateman & Snell, 2009).

Drivers Actuales

- La emergencia sanitaria ocasionada por el COVID19 **ha puesto en jaque a la mayoría de las empresas**, alrededor del mundo, como también, ha generado **cambios en los comportamientos, percepciones y actitudes de los consumidores y empresarios**; conlleva una gran pérdida sanitaria, social y económica para los países, personas y empresas, que buscan la mejor manera de superar esta situación, **adoptando medidas y propuestas de diversa índole para intentar revertirla**.

Importancia de Riesgo Operativo

- Pone en riesgo la existencia del negocio
- Impide lograr objetivos
- Obstaculiza alcanzar las metas de rentabilidad
- No permite mejorar la competitividad y productividad
- Afecta la reputación de la empresa

Naturaleza del Riesgo Operativo

- Deriva de la realiación de las actividades propias del negocio
- Es medible, gestionable y mitigable

Exposiciones

Canales de distribución claves
Clientes principales
Principales proveedores y terceros
Sistemas criticos
Regulación
Principales “drivers” de los ingresos y del valor
Valor de la marca

Vulnerabilidades

Eslabon más frágil
Sistemas frágiles
Fuentes de ingresos en riesgo
Procesos no integrados
Sistemas no integrados
Partes del negocio resistentes a la gestión de riesgos
Personas u operaciones no monitoreadas
Sistemas no mantenidos
Planes de continudad inexistentes o frágiles

Motivos para gestionar el RO

Mejora el control de los procesos.

Moderniza sistemas y equipos.

Se puede asegurar ciertos eventos

Categorías de Riesgo Operativo

Categorias de RO

Fraude interno: pérdidas debidas a actos de un tipo destinado a defraudar, apropiarse indebidamente de la propiedad o eludir las regulaciones, las leyes o la política de la empresa, excluyendo los eventos de diversidad / discriminación, que involucran al menos a una parte interna.

Fraude externo: Pérdidas debidas a actos de un tipo destinado a defraudar, apropiarse indebidamente de la propiedad o eludir la ley por parte de un tercero.

Prácticas de empleo y seguridad en el lugar de trabajo: Pérdidas que surgen de actos incompatibles con las leyes o acuerdos de empleo, salud o seguridad; del pago de reclamaciones por lesiones personales; o de eventos de diversidad / discriminación.

Clientes, productos y prácticas comerciales: pérdidas que surgen de un incumplimiento involuntario o negligente de una obligación profesional con clientes específicos (incluidos los requisitos fiduciarios y de idoneidad), o de la naturaleza o el diseño de un producto.

Daños a los activos físicos: Pérdidas que surgen de la pérdida o daño a los activos físicos por desastres naturales u otros eventos.

Interrupción del negocio y fallas del sistemas: pérdidas que surgen de la interrupción del negocio o fallas de los sistemas.

Gestión de ejecución, entrega y procesos: Pérdidas por procesamiento de transacciones fallidas o gestión de procesos, por relaciones con contrapartes comerciales y proveedores.

Subcategorías de RO

Nivel 1	Nivel 2
Clientes, Productos y Prácticas empresariales	Fallas em los productos
	Prácticas impropias em los negocios o em marketing
	Actividades de asesoramiento
Daños a activos materiales	Desastres naturales y otros eventos
	Accidentes y seguridad pública
	Daño intencional y terrorismo
Ejecución, entrega y gestón de procesos	Introducción, mantenimiento o ejecución de transacciones
	Monitoramiento y reporte
	Ingreso de clientes y documentación
	Administración de cuentas de clientes
Fraude Externo	Robo o fraude externo
	Seguridad externa de los sistemas - Daño Intencional
Fraude Interno	Actividades no autorizadas
	Robo o fraude interno
	Seguridad interna de los sistemas - Daño Intencional
Incidencias em el negocio o fallos em los sistemas	Fallas em la infraestructura tecnológica (hardware)
	Fallas em las aplicaciones (software)
Relaciones laborales y seguridad em el ambiente de trabajo	Relaciones laborales
	Ambiente seguro de trabajo
	Discriminación y diversidad de empleados

¿Fue Riesgo Operativo?

¿Que tipo de evento fue?

Riesgo Operativo y Otros Riesgos

La gestión de riesgos operacionales nos permite observar la empresa de una manera holística para crear un mapa detallado de los riesgos de sus procesos. Los gerentes de línea y los gerentes de negocio pueden usar esta disciplina para conducir su negocio de mejor manera

¿Que hacemos con Mickey Mouse?

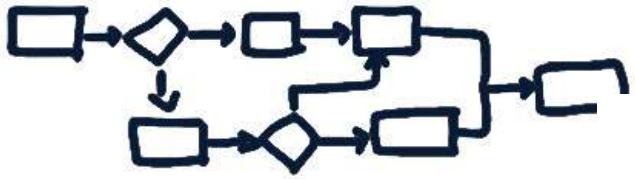
Basilea II (2004)

Riesgo Estratégico o Reputacional

Riesgo Operacional vs. Excelencia Operacional

- Todavía se ve como dos viajes separados (y paralelos) ... y a menudo se los percibe como los enemigos
- La excelencia operativa se centra principalmente en el procesamiento, lo que garantiza un "riesgo de procesamiento" aceptable (Lean, 6S, TQM)
- Unir ambos es un factor clave para el éxito y los ahorros a largo plazo.

Gestión de riesgos operacionales



- Documentacion transaccional/contractual
- Documentación de procesos
- Diseño de procesos
- Ejecución de procesos
- Falla en productos
- Datos Internos y externos
- Reportes internos y externos
- Gestión de cambios y proyectos
- Servicio e interacciones con los clientes.
- Erores en modelos de valoración/precificación

- Hardware
- Software
- Redes
- Interfases
- Comunicaciones
- Seguridad
- Fallas en desarrollo
- Recursos inadecuados

- Falta de personal clave
- Habilidades y capacidades
- Fraude del empleado
- Actividad no autorizada
- Seguridad ambiental
- Relaciones de los empleados
- Diversidad y discriminación
- Inadecuado Entrenamiento/Supervisión

- Outsourcing
- Eventos naturales y hechos por el hombre
- Legislación y regulación
- Fraude externo y actividad criminal

El riesgo operativo es esencialmente un riesgo empresarial y está en el centro de la gestión de riesgos empresariales.

¿Cuándo debo utilizar el proceso de Riesgo Operativo?

1. Para tomar las decisiones importantes del negocio
   - Outsourcing de operaciones / sistemas de TI
   - Creación de nuevos productos
   - Para iniciar proyectos de cambios importantes en el negocio
   - Para iniciar proyectos importantes de IT
2. Definir la estrategia y objetivos de negocio
3. Desarrollar y analizar escenarios
4. Cuando algo significativo ocurre en el ambiente interno o externo del negocio
5. Cuando en un punto en el tiempo se requiere analizar una exposición a un riesgo (ej. RCSA, Control Evaluation).

Top 10 Operational Risks 2021

	2021	2020	Change
IT disruption	1	1	
Data compromise	2	2	
Resilience risk	3	5	↑
Theft and fraud	4	3	↓
Third-party risk	5	4	↓
Conduct risk	6	7	↑
Regulatory risk	7	8	↑
Organisational change	8	6	↓
Geopolitical risk	9	9	↑
Employee wellbeing	10	-	

Preocupaciones de IT

- El 2020 fue el año en el que la amenaza de interrupción de la TI, un evento que abarca todo, desde apagones accidentales de sistemas hasta ataques deliberados de actores externos, explotó en millones de oficinas y en el hogar en todo el mundo.
- El cambio al trabajo remoto dejó a las firmas financieras más expuestas que nunca a ciberataques, amenazas de puerta trasera introducidas a través de nuevos proveedores externos críticos o piratas informáticos con la intención de causar el caos.
- Si bien la industria se sorprendió a sí misma con su capacidad para funcionar con tanta eficacia desde casa, algunos problemas iniciales eran inevitables. Los empleados confinados en casa se quejaron con la confusión creada por las dudosas conexiones Wi-Fi, una red privada virtual que se cae en el peor momento posible, o el sistema que están tratando de controlar de forma remota cae bajo el peso del tráfico.
- Mientras tanto, amenazas como los intentos de ransomware, que podrían ser fáciles de administrar en conjunto y descartar en la oficina, adquirieron una dimension nueva y letal al trabajar fuera de la oficina.

Preocupaciones de IT

- Las amenazas del ransomware siguen aumentando y buscan nuevas formas de facilitar el fraude, como dirigirse a las bandejas de entrada de correo de la alta dirección.
- Pero las fallas tecnológicas en varios bancos y proveedores de tecnología y plataformas comerciales llevaron al caos en mercados clave como los futuros y el comercio de divisas durante la volatilidad cruzada de mercados sin precedentes de marzo.
- A los clientes y otras partes interesadas rara vez les importa qué causa una interrupción, lo que significa que cualquier falla operativa también puede tener graves consecuencias para la reputación, particularmente cuando los sistemas orientados al cliente, como las aplicaciones bancarias o los servicios de pago, se ven afectados.
- La introducción de una mejora para cubrir necesitades tecnológicas sale mal y, como resultado, los sistemas fallan. Experimentamos eso cuando implementamos una nueva plataforma en línea sin muchas pruebas por restricicones de tiempo. Se debe comprender la importancia y el impacto en el cliente cualquier tipo de interrupción del servicio, ya sea fraude o relacionada con el ciberespacio o la gestión de cambios normal.

Preocupaciones con los datos
La Seguridad de la Información

- Para los encargados de realizar un seguimiento de los datos confidenciales, el 2021 se perfila como un año difícil. Muchas personas que trabajan de forma remota tiene que acceder a los sistemas a través de VPN, a menudo a través de redes inalámbricas domésticas, lo que aumenta la posibilidad de vulnerabilidades cibernéticas.
- Con el personal disperso, los gerentes también carecen de supervisión física de los posibles malos actores.
- El fuerte incremento en los ataques de ransomware y phishing reportados este año, las amenazas a la seguridad de la información se ubican en un estrecho segundo lugar en el Top 10 de riesgos operativos de 2021, solo detrás del funcionamiento básico de los sistemas.
- La rápida adopción de la nube gracias a Covid significa que hay que redoblar la gobernanza y la supervisión.
- En la raíz de la mayoría de los eventos de compromiso de datos se encuentran los procesos y procedimientos defectuosos. El error humano también puede ser un factor, o, en una era en la que muchos empleados corren el riesgo de recortes de empleo o de horarios reducidos, malversación.
- La gestión de la identidad y el acceso son controles importantes para proteger el entorno de TI
- Las firmas financieras han establecido controles como la autenticación de múltiples factores y privilegios de usuario limitados para ingresar y cambiar datos comerciales críticos, con gerentes de

Preocupaciones con Resiliencia Organizacional

- En los escenarios de Continuidad de Negocio no se incorporaron eventos en los cuales un tercio dela fuerza laboral se vea excluido de sus oficinas sin previo aviso debido a una pandemia.
- Las firmas financieras de todo tipo y en todos los rincones del mundo han resistido el tumulto relacionado con el coronavirus este año, probando su capacidad para lidiar con desafíos como una volatilidad sin precedentes del mercado, cuellos de botella administrativos y rupturas comerciales, todo mientras se apresuraban a equipar adecuadamente a los empleados para el trabajo remoto a largo plazo.
- Los gerentes de riesgos mencionaron las amenazas a su capacidad de recuperación operativa, solo detrás de los riesgos que amenazan específicamente el funcionamiento básico de los sistemas y la seguridad de los datos.

Preocupaciones cobre Fraude

- Incluso en tiempos normales, el riesgo de robo y fraude ocupa un lugar destacado en la lista de prioridades de las entidades financieras. En la era post-Covid, el riesgo se ha intensificado a medida que se transforma en formas nuevas y peligrosas.
- Los cambios relacionados con la pandemia en las prácticas comerciales y los hábitos de los consumidores han abierto o exacerbado al menos cuatro áreas de vulnerabilidad.
- Los programas de estímulo del gobierno han brindado jugosos bocados de efectivo para que los estafadores los apunten. Los sistemas de detección de fraudes de los bancos se han activado por el repentino cambio a la banca en línea. Los delincuentes se están aprovechando del aumento del trabajo a domicilio para engañar a los consumidores para que transfieran dinero a sus propias arcas.
- Con más personal trabajando de forma remota, el potencial de fechorías internas está creciendo.

Preocupaciones con Proveedores

- Con las oficinas de proveedores críticos cerradas sin previo, la dependencia de la tercerización es una de las peores pesadillas de los gerentes de riesgo operativo.
- Las empresas enfrentan otro año de incertidumbre, en el que los empleados y proveedores están parcialmente exiliados de sus oficinas, otro año en el que la mayoría de las empresas dependerán de un puñado de proveedores para proporcionar videoconferencias, acceso remoto a servidores o almacenamiento en la nube. Se prevé que el riesgo de provedores/terceros seguirá siendo una prioridad hasta fines de 2021.
- Una de las preocupaciones de las instituciones financieras es evaluar las debilidades de seguridad de sus proveedores de servicios críticos, o para las empresas subcontratadas más pequeñas, incluso su viabilidad financiera básica.
- Ahora es mas crucial que nunca para los gerentes de riesgo operacional tener en cuenta a los proveedores de servicios tercerizados críticos de su empresa. Nunca ha sido tan alto el riesgo de falla de sus provedores críticos que pueden impactar en las operaciones comerciales diarias de las empresas.

Preocupciones con el comportamiento

- Para los gerentes de riesgo operacional, dar vueltas en el piso de operaciones, encontrarse con colegas en los pasillos o en la máquina de café e ir a reuniones han sido durante mucho tiempo formas vitales de detectar comportamientos ocultos.
- Al trabajar en la oficina se puede captar señales informales que pueden apuntar a problemas.Con muchos empleados confinados en sus hogares desde principios de 2020, esa fuente de inteligencia se ha perdido.
- Al mismo tiempo, se han erosionado los controles informales sobre el comportamiento inadecuado, como el comercio deshonesto y las ventas indebidas, y ha aumentado el riesgo de mala conducta de los empleados.

Preocupaciones con la regulación

- Los supervisores intervinieron en los mercados durante los últimos 12 meses, fue más a menudo para proteger a los clientes que para sancionar a las empresas con multas. Las sanciones regulatorias en 2020 se desplomaron a medida que Covid-19 se extendía por todo el mundo.
- Aún así, el riesgo regulatorio (el temor de que los cambios en los conjuntos de reglas y las expectativas de los supervisores) nunca está lejos.
- También durante el proceso de teletrabajo, las empresas se han visto obligadas a saltarse controles de procesos, dejar evidencia de documentación en papeles e inclusive modificar los procedimientos para realizarlos en esa nueva modalidad de trabajo. Esto puede conducir a sanciones en caso que no se corrijan las "irregularidades" que sucedieron durante la pandemia.
- Los cambios radicales en el panorama político también pueden conducir a un cambio de las actitudes de los supervisores hacia áreas de riesgo emergente, y también a muchas oportunidades para dar pasos en falso en el cumplimiento

Preocupación con el Cambio Organizacional

- Cuando HSBC, el banco más grande de Europa, anunció que planeaba reducir el espacio de oficinas en un 40%, resumió lo que a lo largo de varios meses desde el inicio de la crisis del coronavirus han vivido muchos bancos que llevaron sus operaciones de la oficina hasta la casa.
- Muchos de los cambios en los entornos operativos producidos por el Covid serán permanente.
- En una era en la que muchos clientes han aprendido a vivir sin poder visitar las oficinas de sus provedores de servicios financieros, muchos están contemplando abiertamente un futuro en el que los bancos pueden ser aún más esbeltos, más baratos y más resilientes. De todos modos, ese es el plan: llegar allí significará una inmensa cantidad de trastornos y muchas oportunidades para dar pasos en falso.
- Los gerentes de riesgo operativo estaban preocupados por las respuestas de sus empresas a los cambios, pero el Covid ha acelerado el ritmo del cambio y ha demostrado que las grandes organizaciones pueden ser sorprendentemente ágiles para resistir las crisis.
- El rápido cambio del trabajo in situ al trabajo desde casa es un ejemplo de la necesidad de una gestión eficaz del cambio en los procesos y servicios para que sea permanente.
- Se debe poner foco a los cambios en los entornos de control de las empresas que solo han sido parchado durante este periodo.

¿Cree que eventos de riesgo operacional significativo impactarán el valor a los accionistas en el largo plazo?

1.- Si

2.- No

3.- No Sabe / No Aplica

MODULO II

COMO IMPLANTAR LA GESTIÓN DE RIESGO OPERATIVO

Gestión de riesgos operativos y digitales en el mundo financiero

Procesos de identificación, valoración, registro y reporte

Rafael Salas, Septiembre 2021

Reglas del Zoom

- Colocar Nombre y Apellido
- Identificar su organización, ej: Rafael Salas – Noesis
- Todos estan con el micrófono en mudo
- Es gentil estar con los videos abiertos.
- Para preguntas vamos a abrir los microfonos anotense las preguntas para no perderlas.
- Vamos a tener Break en intervalos.

Agenda

Modulo I – Riesgo Operativo

Modulo II – Riesgos en la Digitalización

Modulo III – Registro y evaluación de Riesgos Efectivos

Modulo IV - Reportes

MODULO I

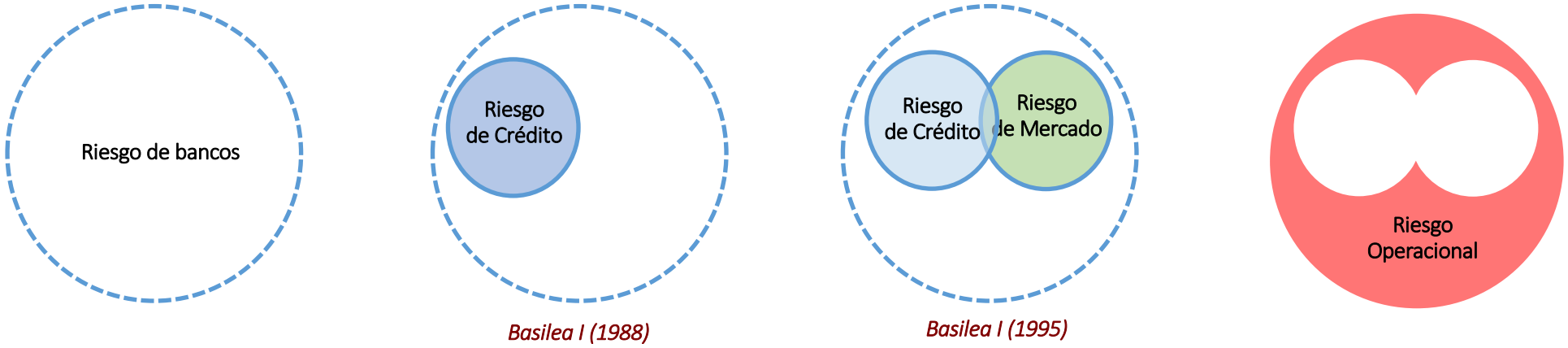
GESTIÓN DE RIESGO OPERATIVO EN EL MUNDO FINANCIERO

Introducción

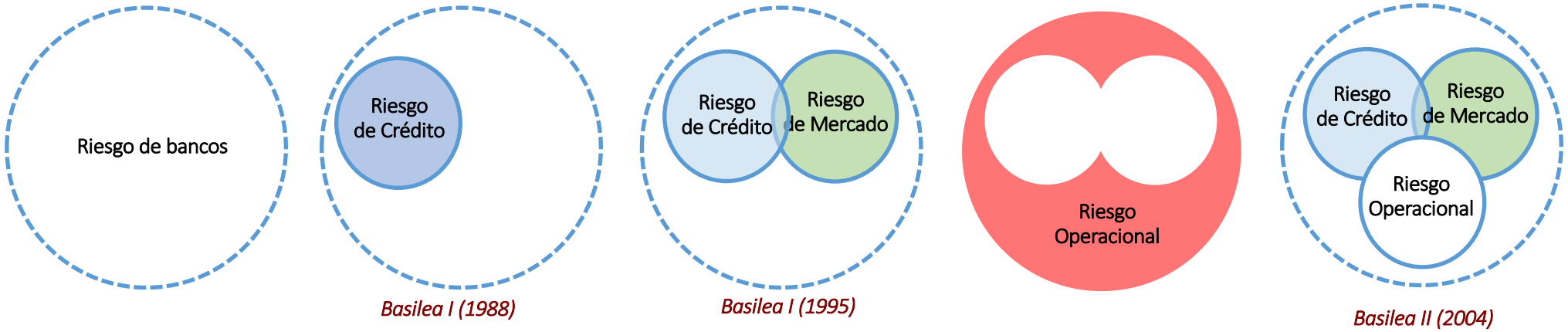
Los riesgos operativos son la causa fundamental de muchas de las fallas financieras importantes de las últimas décadas. Los estudios señalan que los riesgos operativos no son nuevos: errores humanos, fraude, robo, fallas de procesos, errores del sistema y peligros externos, como incendios e inundaciones, existen desde hace décadas. Sin embargo, el impacto de los riesgos operativos fue a menudo relativamente insignificante. Por el contrario, las tendencias recientes como la globalización, la conectividad global a Internet y las dependencias de la cadena de valor han hecho que los riesgos operativos sean más importantes que nunca.

Introducción

La gestión del riesgo operacional se había definido en el pasado como todo riesgo que no se refleja en los programas de gestión de riesgo crediticio y de mercado. Los primeros programas de riesgo operacional, por lo tanto, consideraron que si no era riesgo de mercado y no era riesgo de crédito, entonces debía ser riesgo operacional.



Definición



La definición de riesgo operativo de Basilea II es:

el riesgo de pérdida directa o indirecta como reultado de procesos inadecuados, falla interna humana, sistemas inadecuados o de eventos de carácter externo.

Esta definición incluye el riesgo legal, pero excluye el riesgo estratégico y reputacional.

¿Que hacemos con Mickey Mouse?

Basilea II (2004)

Riesgo Estratégico o Reputacional

La definición en sus componentes.

1.- Debe haber riesgo de pérdida. Entonces, para que exista un riesgo operacional, debe haber una pérdida asociada anticipada.

2.- Las causas definidas de esta pérdida. La definición anterior proporciona cuatro causas que pueden dar lugar a pérdidas por riesgo operacional. Estas cuatro causas son:

- procesos inadecuados o fallidos,
- fallas relacionadas al factor humano
- sistemas inadecuados o fallidos
- eventos de carácter externos.

Veamos las noticias

ÚLTIMAS NOTICIAS Hemeroteca Código de ética Contáctenos

Página SIETE

Diario Nacional Independiente

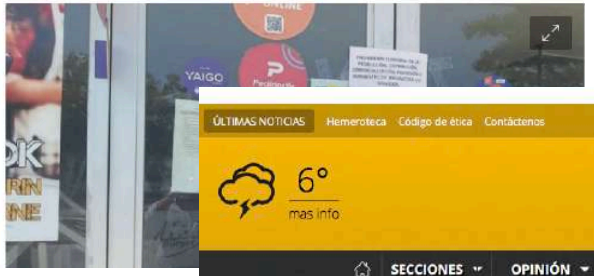
6°

mas info

SECCIONES OPINIÓN CAMPEONES SUPLEMENTOS RASCACIE

Crece polémica por dedo en una hamburguesa, hay antecedentes

El viceministro Silva criticó a Gobernador y Alcalde cruceños por salir en defensa de la empresa. Conminan a indemnizar al empleado afectado.



ÚLTIMAS NOTICIAS Hemeroteca Código de ética Contáctenos

Página SIETE

Diario Nacional Independiente

6°

mas info

SECCIONES OPINIÓN CAMPEONES SUPLEMENTOS

Caso Multipartes: allanan una imprenta y hallan más indicios de falsificación de repuestos

El lunes se llevó a cabo el allanamiento de una imprenta donde se falsificaban etiquetas para autopartes de la marca Toyota.

DW Made for minds.

ACTUALIDAD MULTIMEDIA TV APRENDER ALEMÁN

AMÉRICA LATINA CORONAVIRUS POLÍTICA ECONOMÍA CULTURA CIENCIA Y ECOLOGÍA

ACTUALIDAD / AMÉRICA LATINA

América Latina: Tendencias y pronósticos de metales & minería, la cadena de suministro, factores ambientales y sociales, telecomunicaciones, y más.

AMÉRICA LATINA

Ciberataques aumentaron 24% en América latina este año

El gigante ruso Kaspersky detectó más de 173.000 intentos de infección a dispositivos móviles entre enero y agosto de 2021 en la región (casi 20 ataques por hora), siendo los troyanos una de las principales amenazas.

Los Tiempos NO SE DETIENE

Actualidad Deportes Tendencias Doble Click OH! Lecturas Es

Actualidad

Inicio Últimas Mundo País Economía Cochabamba Seguridad Editorial y Puntos de Vis

Banco Unión: Fraude fue contra la cuenta de una persona utilizando documentación falsa

Economía

Pregunta

¿Cuáles son los 10 riesgos operativos que su empresa va a enfrentar durante el 2021 y 2022?

¿Porqué?

Top 10 Operational Risks

- Fuente: Risk.net Agosto, 2021

	2021	2020	Change
IT disruption	1	1	
Data compromise	2	2	
Resilience risk	3	5	↑
Theft and fraud	4	3	↓
Third-party risk	5	4	↓
Conduct risk	6	7	↑
Regulatory risk	7	8	↑
Organisational change	8	6	↓
Geopolitical risk	9	9	↑
Employee wellbeing	10	-	

Un punto de partida eficaz es evaluar las causas clave de las fallas de sus compañías.

Market Risk

Eventos catastróficos

Errores Operativos

Tercerización
Relaciones con Terceros

Forex

Legal

Interrupciones de IT

Regulación

Datos

Reputación

Liquidity Risk

Reportes

Fallas en Inversiones

Falla en las reservas

Strategic Risk

Incompetencia

Fraude

Habilidades/Capacidades del personal

Cambio Organizacional

Proyectos mal manejados

Drivers Actuales

- Hoy, cada vez es más complejo para los directivos de las empresas poder **controlar las variables** que pueden afectarlas, hay mucho que hacer en áreas cada vez más complejas, el tiempo es un gran limitante y **la información está incompleta** (Porter, 2009)
- **Para poder mejorar la *performance* de una empresa** se debe cumplir con una serie de principios de acción a saber: **actuar con transparencia**, **alcanzar los compromisos adquiridos** y **conseguir confianza** (Covey, Whitman, & England, 2011)
- **Cada vez es más complejo alcanzar las metas corporativas** (Prahalad & Hamel, 2016).
- **La incertidumbre es considerada un estado constante**, un elemento de la vida de la organización, la cual surge de dos factores: la complejidad y el dinamismo (Bateman & Snell, 2009).

Drivers Actuales

- La emergencia sanitaria ocasionada por el COVID19 **ha puesto en jaque a la mayoría de las empresas**, alrededor del mundo, como también, ha generado **cambios en los comportamientos, percepciones y actitudes de los consumidores y empresarios**; conlleva una gran pérdida sanitaria, social y económica para los países, personas y empresas, que buscan la mejor manera de superar esta situación, **adoptando medidas y propuestas de diversa índole para intentar revertirla**.

Importancia de Riesgo Operativo

- Pone en riesgo la existencia del negocio
- Impide lograr objetivos
- Obstaculiza alcanzar las metas de rentabilidad
- No permite mejorar la competitividad y productividad
- Afecta la reputación de la empresa

Naturaleza del Riesgo Operativo

- Deriva de la realiación de las actividades propias del negocio
- Es medible, gestionable y mitigable

Exposiciones

Canales de distribución claves
Clientes principales
Principales proveedores y terceros
Sistemas criticos
Regulación
Principales “drivers” de los ingresos y del valor
Valor de la marca

Vulnerabilidades

Eslabon más frágil
Sistemas frágiles
Fuentes de ingresos en riesgo
Procesos no integrados
Sistemas no integrados
Partes del negocio resistentes a la gestión de riesgos
Personas u operaciones no monitoreadas
Sistemas no mantenidos
Planes de continudad inexistentes o frágiles

Motivos para gestionar el RO

Mejora el control de los procesos.

Moderniza sistemas y equipos.

Se puede asegurar ciertos eventos

Categorías de Riesgo Operativo

Categorias de RO

Fraude interno: pérdidas debidas a actos de un tipo destinado a defraudar, apropiarse indebidamente de la propiedad o eludir las regulaciones, las leyes o la política de la empresa, excluyendo los eventos de diversidad / discriminación, que involucran al menos a una parte interna.

Fraude externo: Pérdidas debidas a actos de un tipo destinado a defraudar, apropiarse indebidamente de la propiedad o eludir la ley por parte de un tercero.

Prácticas de empleo y seguridad en el lugar de trabajo: Pérdidas que surgen de actos incompatibles con las leyes o acuerdos de empleo, salud o seguridad; del pago de reclamaciones por lesiones personales; o de eventos de diversidad / discriminación.

Clientes, productos y prácticas comerciales: pérdidas que surgen de un incumplimiento involuntario o negligente de una obligación profesional con clientes específicos (incluidos los requisitos fiduciarios y de idoneidad), o de la naturaleza o el diseño de un producto.

Daños a los activos físicos: Pérdidas que surgen de la pérdida o daño a los activos físicos por desastres naturales u otros eventos.

Interrupción del negocio y fallas del sistemas: pérdidas que surgen de la interrupción del negocio o fallas de los sistemas.

Gestión de ejecución, entrega y procesos: Pérdidas por procesamiento de transacciones fallidas o gestión de procesos, por relaciones con contrapartes comerciales y proveedores.

Subcategorías de RO

Nivel 1	Nivel 2
Clientes, Productos y Prácticas empresariales	Fallas em los productos
	Prácticas impropias em los negocios o em marketing
	Actividades de asesoramiento
Daños a activos materiales	Desastres naturales y otros eventos
	Accidentes y seguridad pública
	Daño intencional y terrorismo
Ejecución, entrega y gestón de procesos	Introducción, mantenimiento o ejecución de transacciones
	Monitoramiento y reporte
	Ingreso de clientes y documentación
	Administración de cuentas de clientes
Fraude Externo	Robo o fraude externo
	Seguridad externa de los sistemas - Daño Intencional
Fraude Interno	Actividades no autorizadas
	Robo o fraude interno
	Seguridad interna de los sistemas - Daño Intencional
Incidencias em el negocio o fallos em los sistemas	Fallas em la infraestructura tecnológica (hardware)
	Fallas em las aplicaciones (software)
Relaciones laborales y seguridad em el ambiente de trabajo	Relaciones laborales
	Ambiente seguro de trabajo
	Discriminación y diversidad de empleados

¿Fue Riesgo Operativo?

¿Que tipo de evento fue?

Riesgo Operativo y Otros Riesgos

La gestión de riesgos operacionales nos permite observar la empresa de una manera holística para crear un mapa detallado de los riesgos de sus procesos. Los gerentes de línea y los gerentes de negocio pueden usar esta disciplina para conducir su negocio de mejor manera

¿Que hacemos con Mickey Mouse?

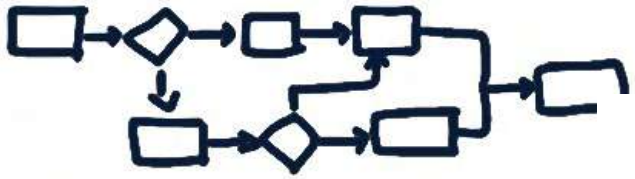
Basilea II (2004)

Riesgo Estratégico o Reputacional

Riesgo Operacional vs. Excelencia Operacional

- Todavía se ve como dos viajes separados (y paralelos) ... y a menudo se los percibe como los enemigos
- La excelencia operativa se centra principalmente en el procesamiento, lo que garantiza un "riesgo de procesamiento" aceptable (Lean, 6S, TQM)
- Unir ambos es un factor clave para el éxito y los ahorros a largo plazo.

Gestión de riesgos operacionales



- Documentacion transaccional/contractual
- Documentación de procesos
- Diseño de procesos
- Ejecución de procesos
- Falla en productos
- Datos Internos y externos
- Reportes internos y externos
- Gestión de cambios y proyectos
- Servicio e interacciones con los clientes.
- Erores en modelos de valoración/precificación

- Hardware
- Software
- Redes
- Interfases
- Comunicaciones
- Seguridad
- Fallas en desarrollo
- Recursos inadecuados

- Falta de personal clave
- Habilidades y capacidades
- Fraude del empleado
- Actividad no autorizada
- Seguridad ambiental
- Relaciones de los empleados
- Diversidad y discriminación
- Inadecuado Entrenamiento/Supervisión

- Outsourcing
- Eventos naturales y hechos por el hombre
- Legislación y regulación
- Fraude externo y actividad criminal

El riesgo operativo es esencialmente un riesgo empresarial y está en el centro de la gestión de riesgos empresariales.

¿Cuándo debo utilizar el proceso de Riesgo Operativo?

1. Para tomar las decisiones importantes del negocio
   - Outsourcing de operaciones / sistemas de TI
   - Creación de nuevos productos
   - Para iniciar proyectos de cambios importantes en el negocio
   - Para iniciar proyectos importantes de IT
2. Definir la estrategia y objetivos de negocio
3. Desarrollar y analizar escenarios
4. Cuando algo significativo ocurre en el ambiente interno o externo del negocio
5. Cuando en un punto en el tiempo se requiere analizar una exposición a un riesgo (ej. RCSA, Control Evaluation).

Top 10 Operational Risks 2021

	2021	2020	Change
IT disruption	1	1	
Data compromise	2	2	
Resilience risk	3	5	↑
Theft and fraud	4	3	↓
Third-party risk	5	4	↓
Conduct risk	6	7	↑
Regulatory risk	7	8	↑
Organisational change	8	6	↓
Geopolitical risk	9	9	↑
Employee wellbeing	10	-	

Preocupaciones de IT

- El 2020 fue el año en el que la amenaza de interrupción de la TI, un evento que abarca todo, desde apagones accidentales de sistemas hasta ataques deliberados de actores externos, explotó en millones de oficinas y en el hogar en todo el mundo.
- El cambio al trabajo remoto dejó a las firmas financieras más expuestas que nunca a ciberataques, amenazas de puerta trasera introducidas a través de nuevos proveedores externos críticos o piratas informáticos con la intención de causar el caos.
- Si bien la industria se sorprendió a sí misma con su capacidad para funcionar con tanta eficacia desde casa, algunos problemas iniciales eran inevitables. Los empleados confinados en casa se quejaron con la confusión creada por las dudosas conexiones Wi-Fi, una red privada virtual que se cae en el peor momento posible, o el sistema que están tratando de controlar de forma remota cae bajo el peso del tráfico.
- Mientras tanto, amenazas como los intentos de ransomware, que podrían ser fáciles de administrar en conjunto y descartar en la oficina, adquirieron una dimension nueva y letal al trabajar fuera de la oficina.

Preocupaciones de IT

- Las amenazas del ransomware siguen aumentando y buscan nuevas formas de facilitar el fraude, como dirigirse a las bandejas de entrada de correo de la alta dirección.
- Pero las fallas tecnológicas en varios bancos y proveedores de tecnología y plataformas comerciales llevaron al caos en mercados clave como los futuros y el comercio de divisas durante la volatilidad cruzada de mercados sin precedentes de marzo.
- A los clientes y otras partes interesadas rara vez les importa qué causa una interrupción, lo que significa que cualquier falla operativa también puede tener graves consecuencias para la reputación, particularmente cuando los sistemas orientados al cliente, como las aplicaciones bancarias o los servicios de pago, se ven afectados.
- La introducción de una mejora para cubrir necesitades tecnológicas sale mal y, como resultado, los sistemas fallan. Experimentamos eso cuando implementamos una nueva plataforma en línea sin muchas pruebas por restricicones de tiempo. Se debe comprender la importancia y el impacto en el cliente cualquier tipo de interrupción del servicio, ya sea fraude o relacionada con el ciberespacio o la gestión de cambios normal.

Preocupaciones con los datos
La Seguridad de la Información

- Para los encargados de realizar un seguimiento de los datos confidenciales, el 2021 se perfila como un año difícil. Muchas personas que trabajan de forma remota tiene que acceder a los sistemas a través de VPN, a menudo a través de redes inalámbricas domésticas, lo que aumenta la posibilidad de vulnerabilidades cibernéticas.
- Con el personal disperso, los gerentes también carecen de supervisión física de los posibles malos actores.
- El fuerte incremento en los ataques de ransomware y phishing reportados este año, las amenazas a la seguridad de la información se ubican en un estrecho segundo lugar en el Top 10 de riesgos operativos de 2021, solo detrás del funcionamiento básico de los sistemas.
- La rápida adopción de la nube gracias a Covid significa que hay que redoblar la gobernanza y la supervisión.
- En la raíz de la mayoría de los eventos de compromiso de datos se encuentran los procesos y procedimientos defectuosos. El error humano también puede ser un factor, o, en una era en la que muchos empleados corren el riesgo de recortes de empleo o de horarios reducidos, malversación.
- La gestión de la identidad y el acceso son controles importantes para proteger el entorno de TI
- Las firmas financieras han establecido controles como la autenticación de múltiples factores y privilegios de usuario limitados para ingresar y cambiar datos comerciales críticos, con gerentes de

Preocupaciones con Resiliencia Organizacional

- En los escenarios de Continuidad de Negocio no se incorporaron eventos en los cuales un tercio dela fuerza laboral se vea excluido de sus oficinas sin previo aviso debido a una pandemia.
- Las firmas financieras de todo tipo y en todos los rincones del mundo han resistido el tumulto relacionado con el coronavirus este año, probando su capacidad para lidiar con desafíos como una volatilidad sin precedentes del mercado, cuellos de botella administrativos y rupturas comerciales, todo mientras se apresuraban a equipar adecuadamente a los empleados para el trabajo remoto a largo plazo.
- Los gerentes de riesgos mencionaron las amenazas a su capacidad de recuperación operativa, solo detrás de los riesgos que amenazan específicamente el funcionamiento básico de los sistemas y la seguridad de los datos.

Preocupaciones cobre Fraude

- Incluso en tiempos normales, el riesgo de robo y fraude ocupa un lugar destacado en la lista de prioridades de las entidades financieras. En la era post-Covid, el riesgo se ha intensificado a medida que se transforma en formas nuevas y peligrosas.
- Los cambios relacionados con la pandemia en las prácticas comerciales y los hábitos de los consumidores han abierto o exacerbado al menos cuatro áreas de vulnerabilidad.
- Los programas de estímulo del gobierno han brindado jugosos bocados de efectivo para que los estafadores los apunten. Los sistemas de detección de fraudes de los bancos se han activado por el repentino cambio a la banca en línea. Los delincuentes se están aprovechando del aumento del trabajo a domicilio para engañar a los consumidores para que transfieran dinero a sus propias arcas.
- Con más personal trabajando de forma remota, el potencial de fechorías internas está creciendo.

Preocupaciones con Proveedores

- Con las oficinas de proveedores críticos cerradas sin previo, la dependencia de la tercerización es una de las peores pesadillas de los gerentes de riesgo operativo.
- Las empresas enfrentan otro año de incertidumbre, en el que los empleados y proveedores están parcialmente exiliados de sus oficinas, otro año en el que la mayoría de las empresas dependerán de un puñado de proveedores para proporcionar videoconferencias, acceso remoto a servidores o almacenamiento en la nube. Se prevé que el riesgo de provedores/terceros seguirá siendo una prioridad hasta fines de 2021.
- Una de las preocupaciones de las instituciones financieras es evaluar las debilidades de seguridad de sus proveedores de servicios críticos, o para las empresas subcontratadas más pequeñas, incluso su viabilidad financiera básica.
- Ahora es mas crucial que nunca para los gerentes de riesgo operacional tener en cuenta a los proveedores de servicios tercerizados críticos de su empresa. Nunca ha sido tan alto el riesgo de falla de sus provedores críticos que pueden impactar en las operaciones comerciales diarias de las empresas.

Preocupciones con el comportamiento

- Para los gerentes de riesgo operacional, dar vueltas en el piso de operaciones, encontrarse con colegas en los pasillos o en la máquina de café e ir a reuniones han sido durante mucho tiempo formas vitales de detectar comportamientos ocultos.
- Al trabajar en la oficina se puede captar señales informales que pueden apuntar a problemas.Con muchos empleados confinados en sus hogares desde principios de 2020, esa fuente de inteligencia se ha perdido.
- Al mismo tiempo, se han erosionado los controles informales sobre el comportamiento inadecuado, como el comercio deshonesto y las ventas indebidas, y ha aumentado el riesgo de mala conducta de los empleados.

Preocupaciones con la regulación

- Los supervisores intervinieron en los mercados durante los últimos 12 meses, fue más a menudo para proteger a los clientes que para sancionar a las empresas con multas. Las sanciones regulatorias en 2020 se desplomaron a medida que Covid-19 se extendía por todo el mundo.
- Aún así, el riesgo regulatorio (el temor de que los cambios en los conjuntos de reglas y las expectativas de los supervisores) nunca está lejos.
- También durante el proceso de teletrabajo, las empresas se han visto obligadas a saltarse controles de procesos, dejar evidencia de documentación en papeles e inclusive modificar los procedimientos para realizarlos en esa nueva modalidad de trabajo. Esto puede conducir a sanciones en caso que no se corrijan las "irregularidades" que sucedieron durante la pandemia.
- Los cambios radicales en el panorama político también pueden conducir a un cambio de las actitudes de los supervisores hacia áreas de riesgo emergente, y también a muchas oportunidades para dar pasos en falso en el cumplimiento

Preocupación con el Cambio Organizacional

- Cuando HSBC, el banco más grande de Europa, anunció que planeaba reducir el espacio de oficinas en un 40%, resumió lo que a lo largo de varios meses desde el inicio de la crisis del coronavirus han vivido muchos bancos que llevaron sus operaciones de la oficina hasta la casa.
- Muchos de los cambios en los entornos operativos producidos por el Covid serán permanente.
- En una era en la que muchos clientes han aprendido a vivir sin poder visitar las oficinas de sus provedores de servicios financieros, muchos están contemplando abiertamente un futuro en el que los bancos pueden ser aún más esbeltos, más baratos y más resilientes. De todos modos, ese es el plan: llegar allí significará una inmensa cantidad de trastornos y muchas oportunidades para dar pasos en falso.
- Los gerentes de riesgo operativo estaban preocupados por las respuestas de sus empresas a los cambios, pero el Covid ha acelerado el ritmo del cambio y ha demostrado que las grandes organizaciones pueden ser sorprendentemente ágiles para resistir las crisis.
- El rápido cambio del trabajo in situ al trabajo desde casa es un ejemplo de la necesidad de una gestión eficaz del cambio en los procesos y servicios para que sea permanente.
- Se debe poner foco a los cambios en los entornos de control de las empresas que solo han sido parchado durante este periodo.

¿Cree que eventos de riesgo operacional significativo impactarán el valor a los accionistas en el largo plazo?

1.- Si

2.- No

3.- No Sabe / No Aplica

Gestión de riesgos operativos y digitales en el mundo financiero

Procesos de identificación, valoración, registro y reporte

Rafael Salas, Septiembre 2021

Quizzz

- Para participar en las preguntas y respuestas

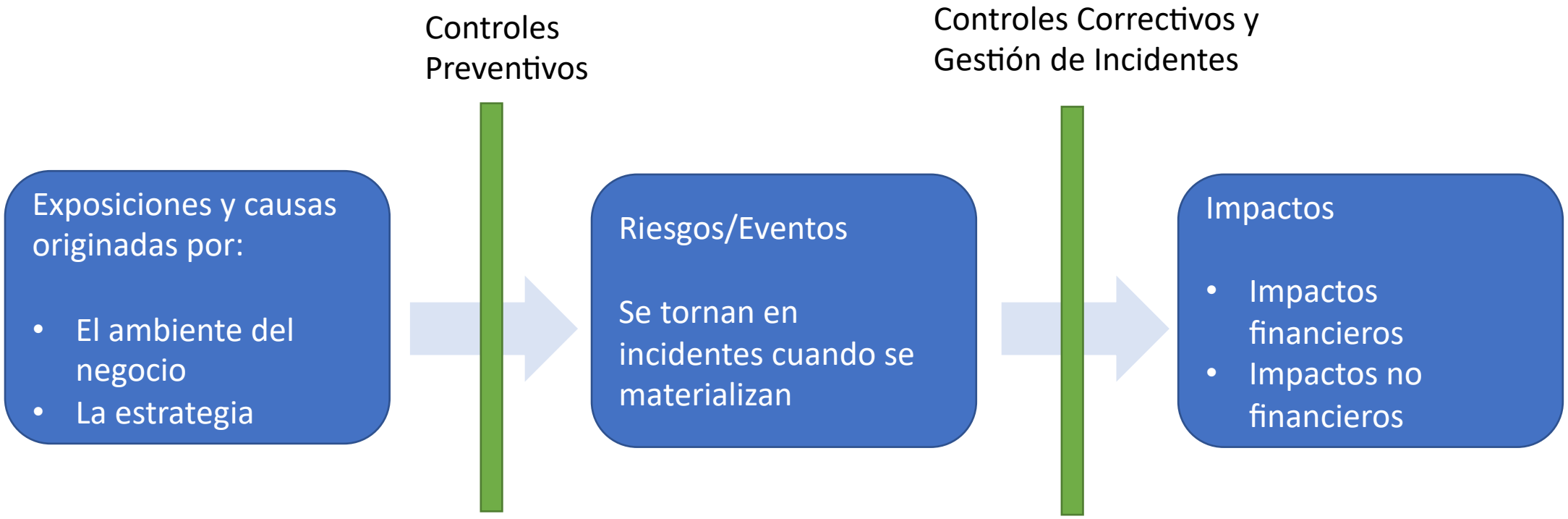
MODULO II

COMO IMPLANTAR LA GESTIÓN DE RIESGO OPERATIVO

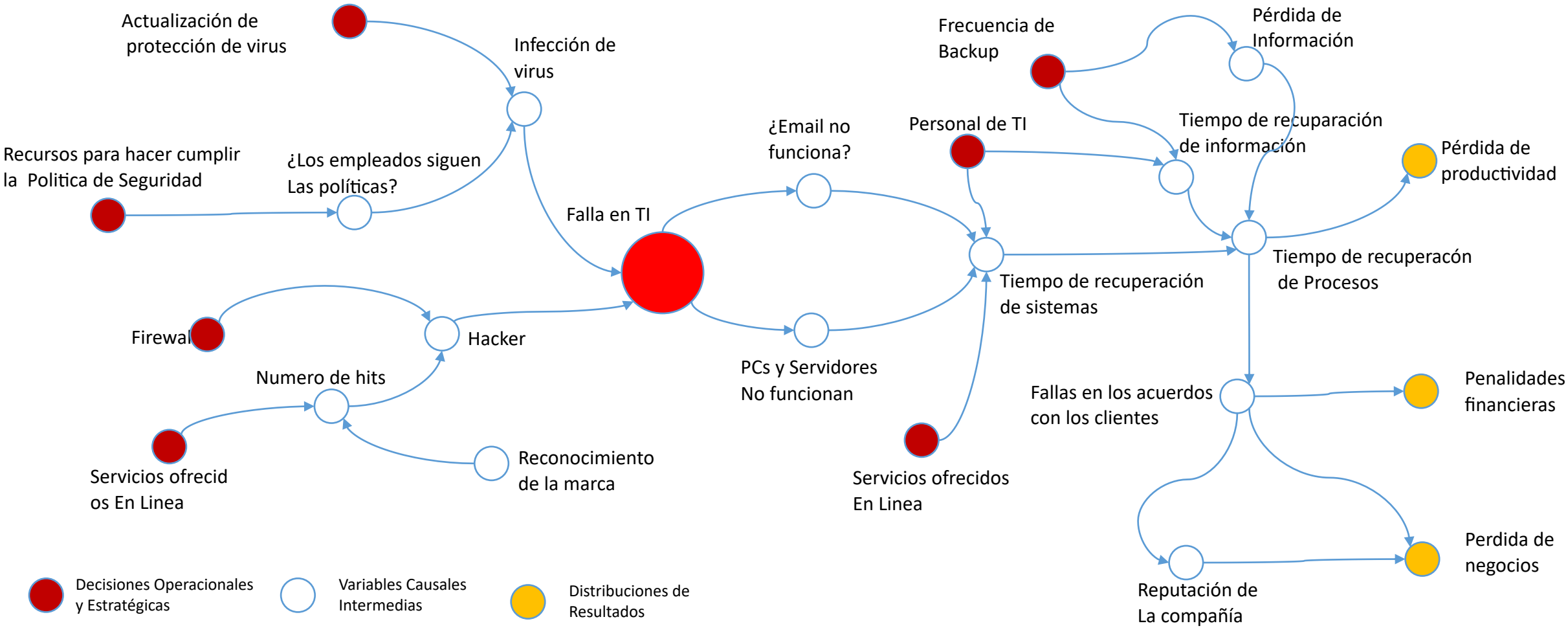
Reglas del Zoom

- Colocar Nombre y Apellido
- Identificar su organización, ej: Rafael Salas – Noesis
- Todos estan con el micrófono en mudo
- Es gentil estar con los videos activados.
- Para preguntas vamos a abrir los microfonos anotense las preguntas para no perderlas.
- Vamos a tener Break en intervalos.

Naturaleza del Riesgo Operativo



Ejemplo: Interrupción de negocio por fallas en los servicios de IT



Causa

Exposición: la superficie en riesgo. Va desde la distancia recorrida en automóvil (exposición a accidentes) hasta el número de empleados con acceso a transferencias bancarias de alto valor (exposición al fraude interno). La única forma de eliminar el riesgo es eliminar la exposición, pero eso también eliminará el negocio.

Entorno: se refiere tanto a entornos externos como internos, que son controlables solo hasta cierto punto. Por ejemplo, externamente, una empresa puede elegir dónde expandir su negocio, pero no puede elegir las condiciones comerciales en su país de origen. El entorno empresarial interno se refiere a las características organizativas de la empresa, como el procesamiento eficiente, el personal competente y los líderes inspiradores, que normalmente generarán muchos menos riesgos operativos que las empresas desorganizadas con procesos inconexos y una cultura del miedo.

Estrategia: la parte más controlable de las causas de riesgo. Una empresa puede decidir expandirse al extranjero, lanzar una nueva línea de negocios, reemplazar los procesos manuales por la automatización y subcontratar sus call centers o sus sistemas de pago. Cada decisión importante afectará el perfil de riesgo de la empresa y su exposición al riesgo operacional. La estrategia, junto con el entorno operativo, es el principal factor de exposición al riesgo operativo.

Eventos

Los riesgos se convierten en "eventos" o "incidentes" cuando se convierten en una realidad, ellos ya no son más una posibilidad.

Un evento es la materialización de un riesgo. Por ejemplo, una colisión con otro vehículo es una materialización del riesgo de accidente automovilístico, pero no la única.

El análisis detallado de incidentes pasados es de gran ayuda para la prevención futura.

Impactos

Las consecuencias de los incidentes no siempre son inmediatament financieras, pero inevitablemente hay un impacto financiero en algún momento. El daño a la reputación, la pérdida de clientes, la infracción regulatoria y la interrupción del servicio, todos descritos típicamente como impactos no financieros en las evaluaciones de riesgo operativo, eventualmente resultan en pérdidas financieras.

Los costos internos son también parte de la pérdida financiera. Idealmente el personal debe estar trabajando en hacer que el producto/servicio llegue al cliente y hacer que los objetivos empresariales se alcancen.

Gestión de Riesgos

Controles preventivos: además del diseño de procesos y la organización sensata de tareas, los controles internos, tanto preventivos como de detección, son los principales métodos para la reducción de riesgos.

Controles correctivos y gestión de incidentes: la prevención no es la única mitigación de riesgos; una vez que ocurre un incidente, la intervención temprana y la planificación de contingencias son fundamentales para reducir los impactos. Ejemplos obvios son los detectores de incendios y los extintores de incendios accesibles. Las copias de seguridad de datos y las medidas de redundancia también son controles correctivos típicos. Si bien ninguno de ellos ayuda a prevenir el riesgo, son particularmente efectivos para reducir el daño cuando ocurre un incidente.

Cómo Implementar la Gestión de Riesgo Operativo

Preguntas Clave

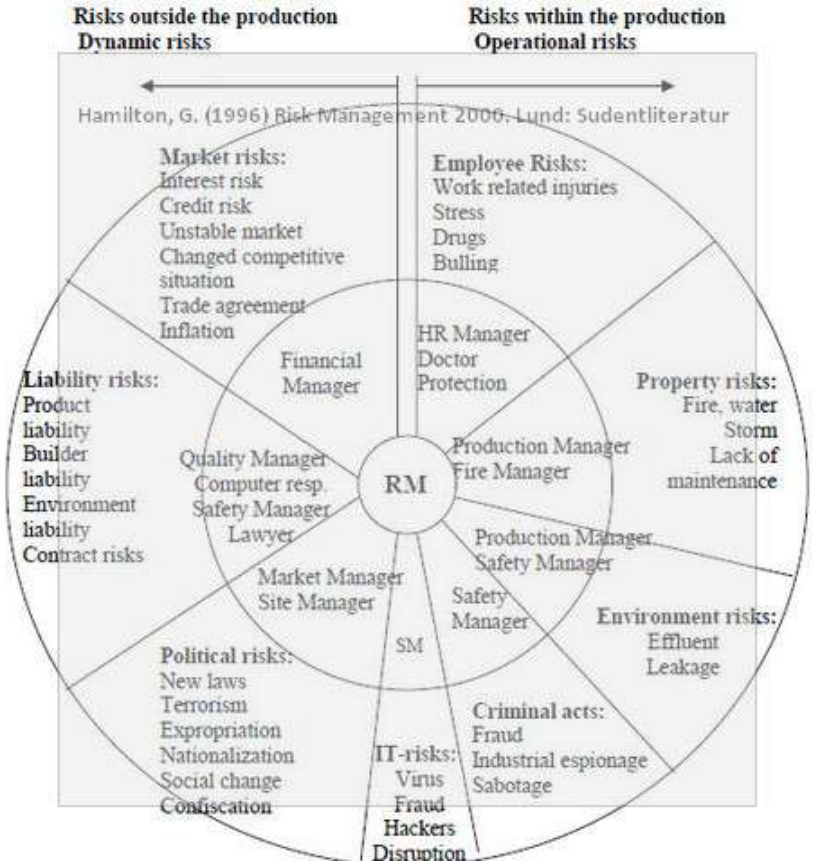
Todo responsable de la implementación de Riesgo Operativo tiene las siguientes dudas:

- ¿Qué debo hacer?
- ¿Cómo lo hago?

¿Qué debo hacer?
Proceso de Gestión de Riesgo Operativo

Las prácticas de gestión de riesgos eficaces requieren un proceso estructurado.

En 1974, Gustav Hamilton desarrolló el "círculo de gestión de riesgos" que muestra la gestión de riesgos como un proceso continuo. La publicación de Hamilton se describe como la primera en describir los tipos y actividades de gestión de riesgos aplicados en un contexto de gestión de riesgos organizativos.

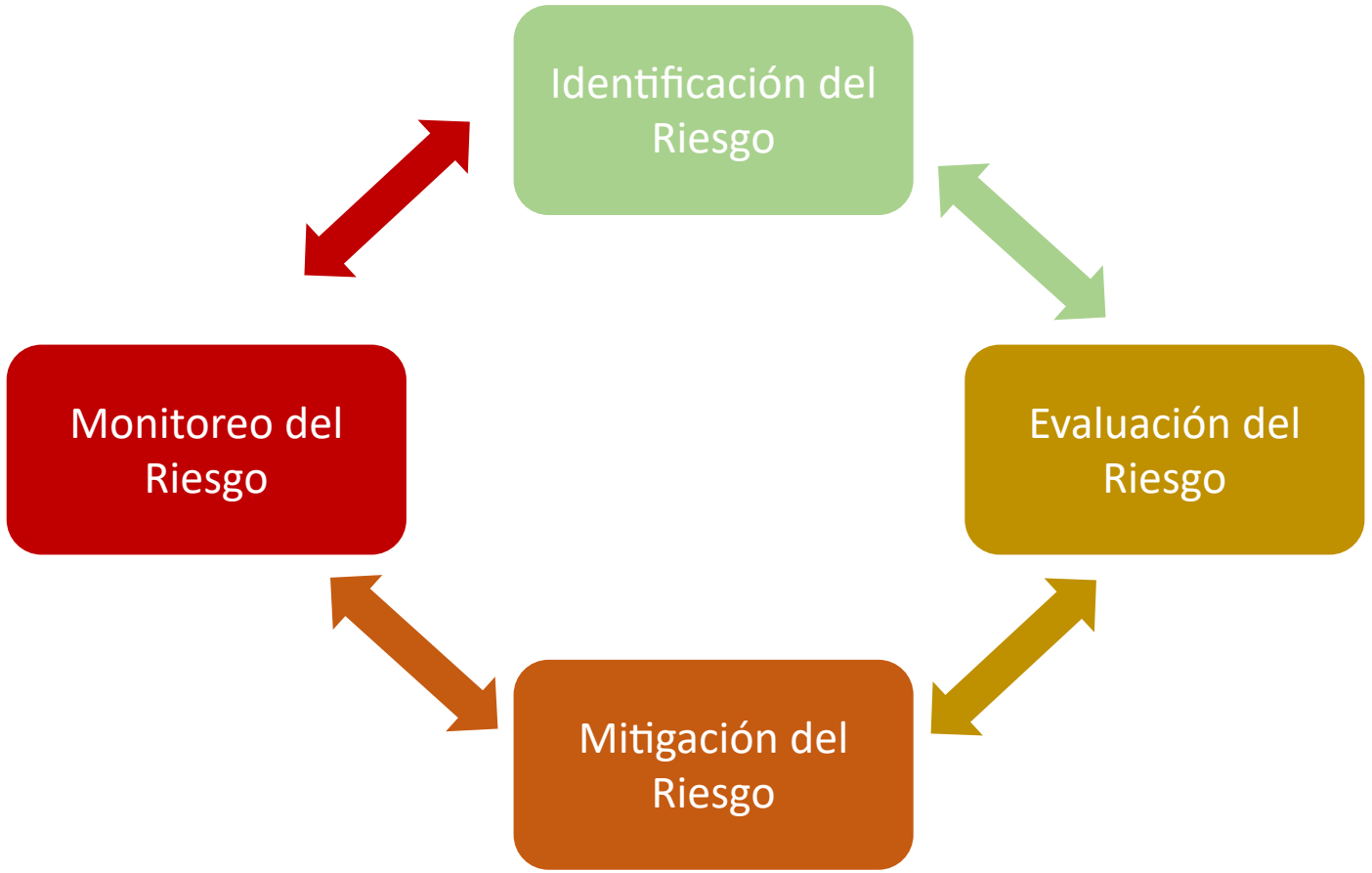


Proceso de Gestión de Riesgos Marcos de Referencia

Table 2. Comparing process activities between COSO ERM and ISO 31000.

COSO ERM [37]	ISO 31000 [48]
Internal Environment	Internal and external environment
Objective setting	Identifying and describing objectives
Risk Assessment: 1. Event identification 2. Risk assessment 3. Risk response	Risk Assessment: 1. Risk identification 2. Risk analysis 3. Risk evaluation
Control activities	Risk Treatment
Information and communication	Communication and consultation
Monitoring activities	Monitoring and review

Proceso de Gestión de Riesgo Operativo Simplificado



Preguntas

¿Cómo lo hago?

Las “Buenas Prácticas para la Gestión y Supervisión del Riesgo Operacional” del Comité de Supervisión Bancaria de Basilea proporcionan pautas útiles para las mejores prácticas para los departamentos de riesgo operacional. Al cumplir con estos estándares, es necesario desarrollar un marco de riesgo operativo que se ajuste a la cultura del banco y refleje las mejores prácticas en la industria.

Los principales bloques de construcción de datos de un marco de riesgo operativo son:

- Recopilación de datos sobre pérdidas
- Autoevaluación de riesgos y controles
- Análisis de escenarios
- Indicadores clave de riesgo

El marco también debe abordar la gobernanza, proporcionar políticas y procedimientos, impulsar el cambio de cultura y responder e informar el apetito por el riesgo. Además, el marco debe incorporar datos en cualquier modelo de capital y debe incorporar datos y análisis en los informes de riesgos.

Principios

Principio 1 : El Directorio debe liderar el establecimiento de una fuerte cultura de gestión de riesgos, implementada por la alta dirección. El Directorio y la alta dirección deben establecer una cultura corporativa guiada por una sólida gestión de riesgos, establecer estándares e incentivos para un comportamiento profesional y responsable, y garantizar que el personal reciba entrenamiento adecuado en gestión de riesgos y la formación ética.

Principio 2 : Los bancos deben desarrollar, implementar y mantener un marco de gestión de riesgos operativos (ORMF) que esté completamente integrado en los procesos generales de gestión de riesgos del banco. El ORMF adoptado por un banco individual dependerá de una variedad de factores, que incluyen la naturaleza, tamaño, complejidad y perfil de riesgo del banco.

Principios

Gobernancia

El Directorio

Principio 3: El Directorio debe supervisar los riesgos operacionales importantes y la eficacia de los controles clave, y garantizar que la alta dirección implemente las políticas, procesos y sistemas del ORMF de manera efectiva en todos los niveles de decisión.

Principio 4: El Directorio debe aprobar y revisar periódicamente una declaración de apetito de riesgo y tolerancia para el riesgo operacional que articula la naturaleza, los tipos y los niveles de riesgo operacional que el banco está dispuesto a asumir.

Principios

Alta Gerencia

Principio 5: La alta gerencia debe desarrollar para la aprobación del Directorio una estructura de gobierno clara, efectiva y sólida con líneas de responsabilidad bien definidas, transparentes y consistentes. La alta gerencia es responsable de implementar y mantener consistentemente en toda la organización políticas, procesos y sistemas para administrar el riesgo operacional en todos los productos, actividades, procesos y sistemas materiales del banco de acuerdo con la declaración de tolerancia y apetito de riesgo del banco.

Principios

Ambiente de gestión de riesgos

Identificación y evaluación

Principio 6: La alta gerencia debe garantizar la identificación y evaluación integrales del riesgo operacional inherente a todos los productos, actividades, procesos y sistemas materiales para asegurarse de que los riesgos e incentivos inherentes se entiendan bien.

Principio 7: La alta gerencia debe garantizar que el proceso de gestión de cambios del banco sea integral, que cuente con los recursos adecuados e incluya evaluaciones continuas de riesgo y control, articuladas adecuadamente entre las líneas de defensa relevantes.

Principios

Monitoreo e informes

Principio 8: La alta gerencia debe implementar un proceso para monitorear regularmente los perfiles de riesgo operacional y las exposiciones operacionales materiales. Deben establecerse mecanismos de notificación adecuados en los niveles del Directorio, la alta gerencia y las unidades de negocios para respaldar la gestión proactiva del riesgo operativo.

Control y Mitigación

Principio 9: Los bancos deberían tener un entorno de control sólido que utilice políticas, procesos y sistemas; controles internos apropiados; y estrategias apropiadas de mitigación y/o transferencia de riesgos.

Principios

Tecnología de la información y la comunicación

Principio 10: Los bancos deberían implementar una gobernanza solida de TIC que sea coherente con su apetito por el riesgo y la declaración de tolerancia para el riesgo operacional y garantice que sus TIC respalden y faciliten completamente sus operaciones. Las TIC deben estar sujetas a los programas apropiados de identificación, protección, detección, respuesta y recuperación de riesgos que se prueban regularmente, incorporan una conciencia situacional adecuada y transmiten información relevante a los usuarios de manera oportuna.

Planificación de la Continuidad del Negocio

Principio 11: Los bancos deben tener planes de continuidad del negocio establecidos para garantizar su capacidad de operar de manera continua y limitar las pérdidas en caso de una interrupción grave del negocio

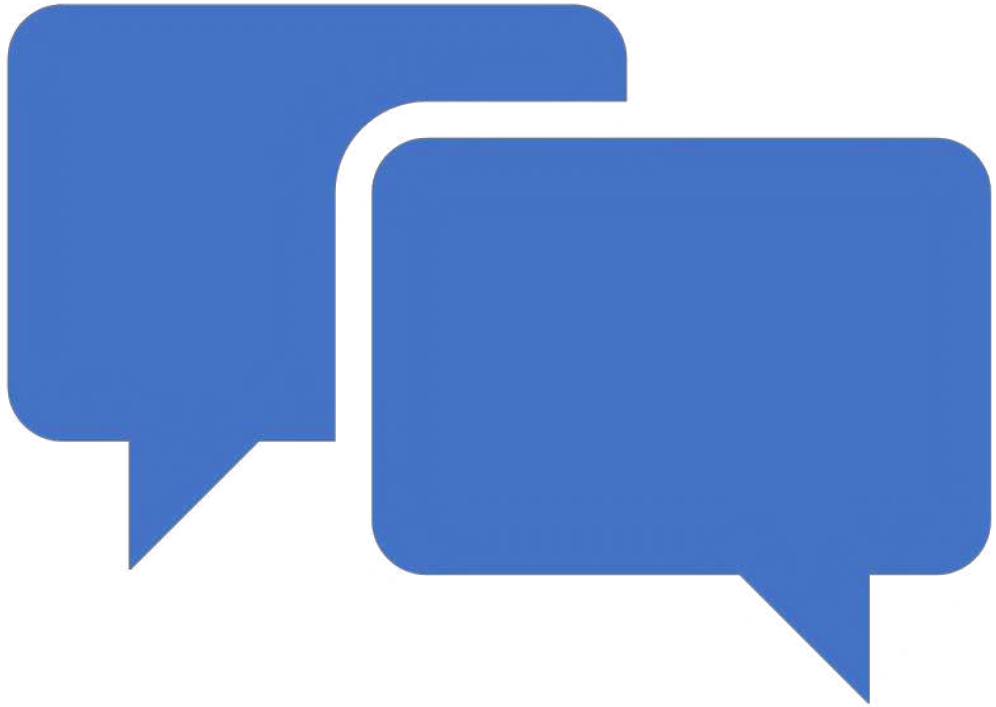
Principios

Rol de Divulgación

Principio 12: Las divulgaciones públicas de un banco deberían permitir a las partes interesadas evaluar su enfoque para la gestión del riesgo operacional y su exposición al riesgo operacional.

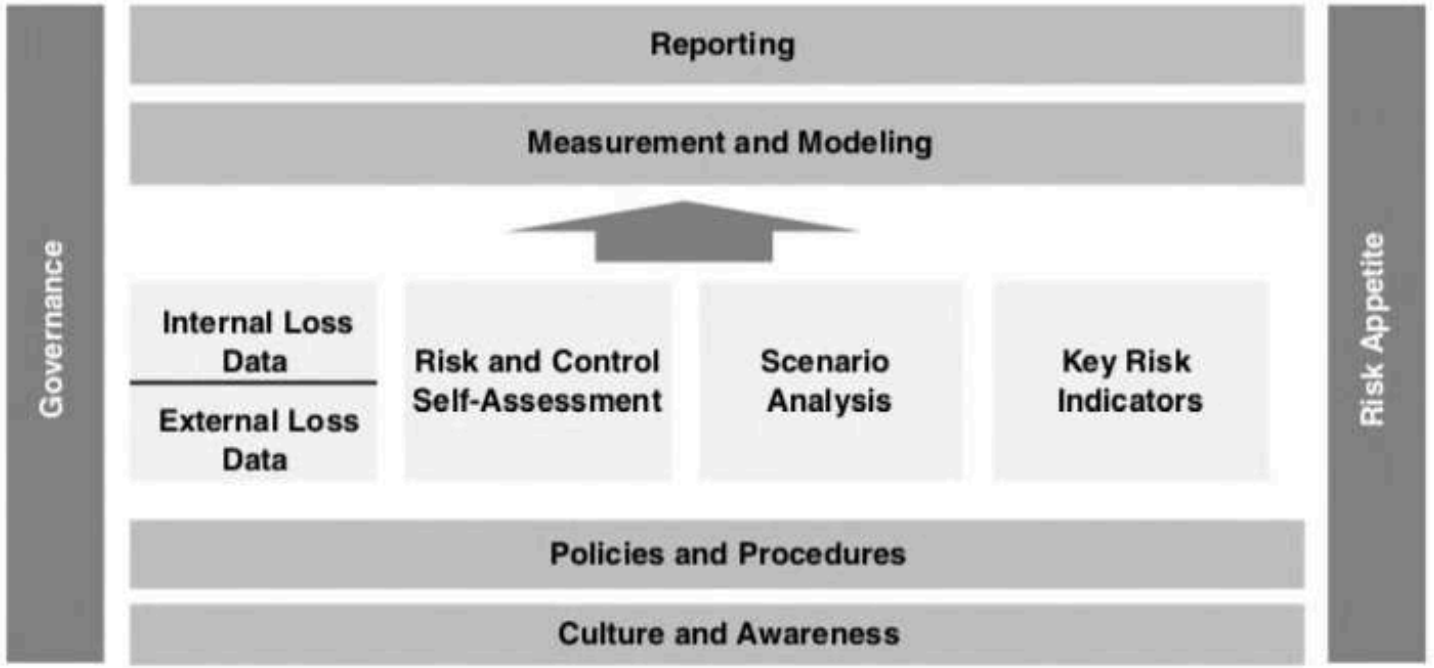
Rol de los supervisores

Comentarios

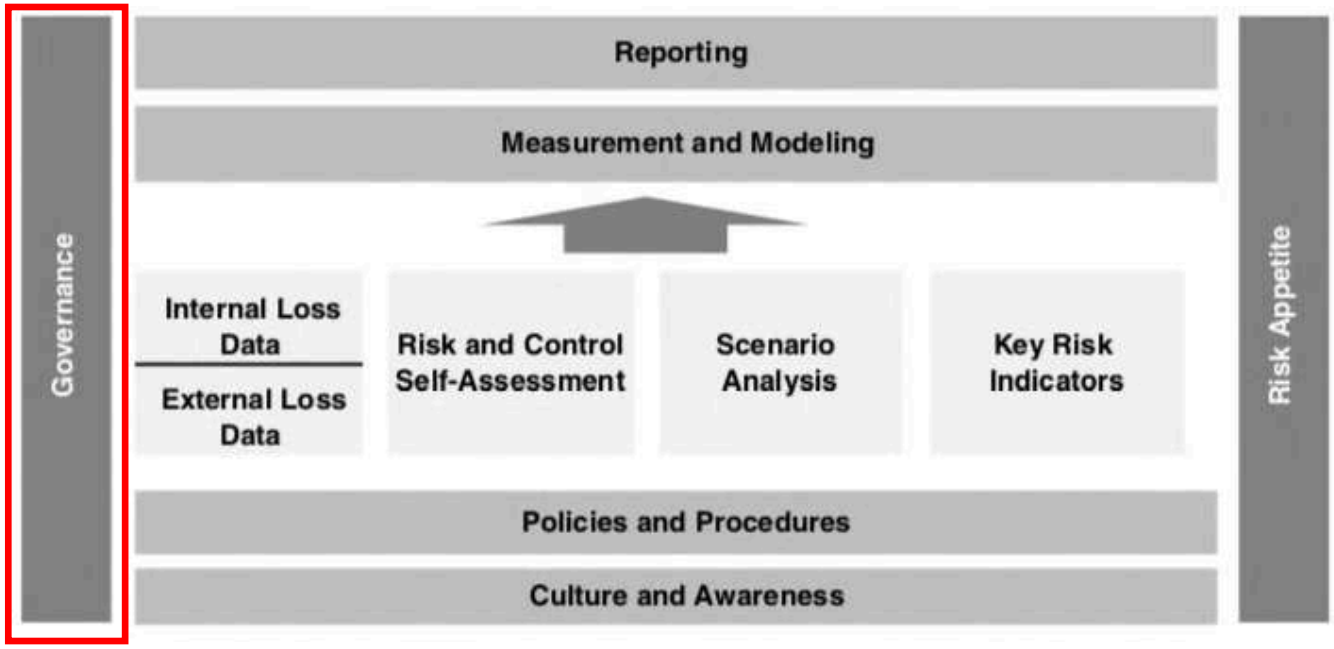


Riesgo Operativo Marco de Referencia

Buenas Prácticas para la Gestión y Supervisión del Riesgo Operacional (2003 - 2020)



GOVERNANCE


Governance
Reporting
Measurement and Modeling
Internal Loss Data
External Loss Data
Risk and Control Self-Assessment
Scenario Analysis
Key Risk Indicators
Policies and Procedures
Culture and Awareness
Risk Appetite

Governance

El Gobierno Corporativo determina los roles y responsabilidades del responsable de la función de riesgo operacional y su equipo que administra el marco de referencia seleccionado, los comités que supervisan y toman decisiones clave sobre la gestión de riesgos, los gerentes de riesgo operacional en las líneas de negocio y cada empleado. que pueden encontrarse con riesgo operacional.

Para desarrollar un marco de riesgo operativo que sea eficaz, se debe considerar cuidadosamente desde el principio una estructura de gobierno adecuada. La gobernanza también debe revisarse al menos una vez al año para comprobar si sigue funcionando según lo previsto. El buen gobierno permite escalar el riesgo y asegura que la transparencia del riesgo sea efectiva a través de todos los niveles de gestión del riesgo operativo que puedan existir.

Governance

La gestión adecuada de los riesgos operativos se describe como un modelo de "tres líneas de defensa". Los eventos de riesgo operacional y sus consecuencias deben manejarse en la función de la organización en la que ocurren; sin embargo, las consecuencias graves deben informarse directamente a la junta y otras partes interesadas. La ejecución adecuada de las acciones de mitigación de riesgo operativo en las primeras líneas debe ser gestionada y supervisada por una función (independiente) dentro de la organización, denominada segunda línea de defensa. La tercera línea de defensa está formada por un comité de auditoría (independiente) que evalúa periódicamente la estructura, el proceso y la implementación de la gestión del riesgo operativo.

Modelo de las 3 líneas de defensa

En términos simples…

La primera línea:

- Identificar, evaluar, controlar, mitigar y gestionar el riesgo. Cumplir con el marco de gestión de riesgo
- Asegurar un diseño, implementación y operación efectivos de los controles.
- Escalar las amenazas materiales y las exposiciones al riesgo
- Operar con un buen gobierno de la función empresarial

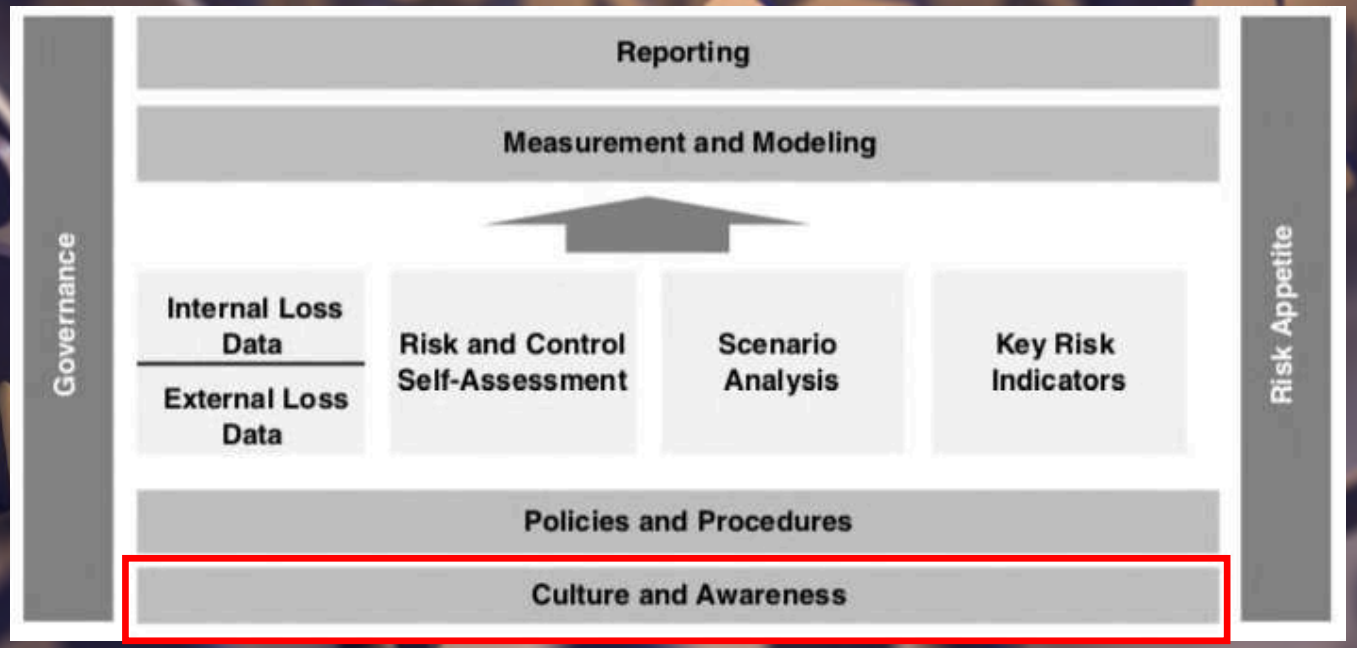
La segunda línea:

- Proporcionar política y marco
- Monitorear, supervisar y desafía a la 1ra línea
- Apoyar el buen gobierno de la empresa
- Informar y escalar amenazas y exposiciones a riesgos

La tercera línea:

- Aseguramiento independiente sobre las dos primeras líneas de defensa
- Asegura la calidad en la aplicación del marco
- Evaluación de la adecuación de los controles

CULTURE AND AWARENESS

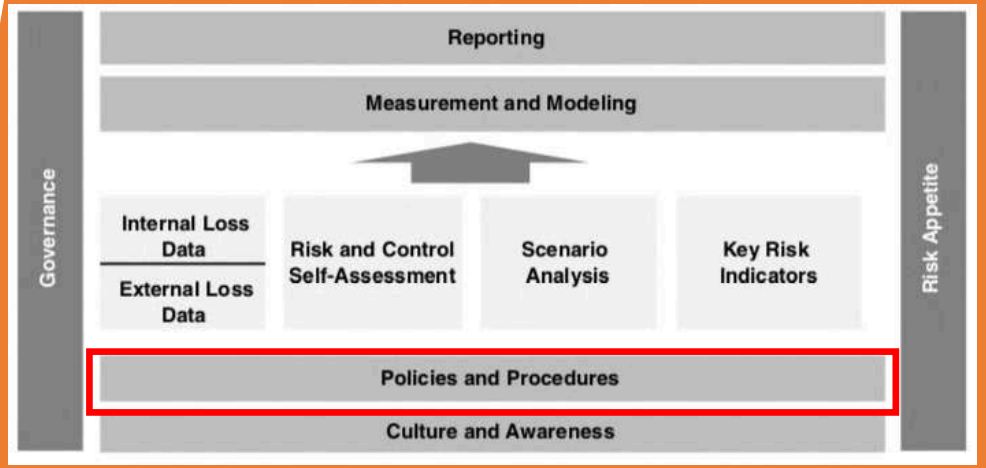


Culture and Awareness

Una vez que se ha abordado la gobernanza, el siguiente paso en el desarrollo de un marco de riesgo operativo es abordar de manera proactiva la cultura y la conciencia. Si bien puede ser tentador saltar al desarrollo de los componentes básicos de la gestión de riesgos operativos, como la recopilación de datos de pérdida y la autoevaluación del riesgo y el control, esos componentes básicos solo tendrán éxito si se ha invertido suficiente tiempo y energía en la cultura y el control. conciencia.

La implementación de un marco de riesgo operacional exitoso requiere ganarse el corazón y la mente de los empleados de la empresa. Detectar riesgos operativos es una habilidad desarrollada. Si bien los riesgos existen en todas las líneas de negocio, se deber dar el tono correcto en la parte superior, se debe capacitar y concienciar para tener una exitosa identificación y reporte de los riesgos operativos.

POLICIES AND PROCEDURES

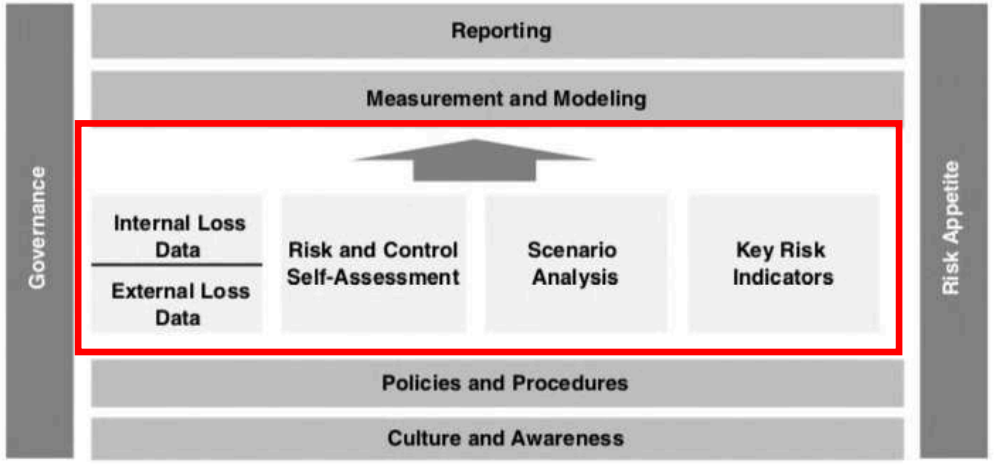


Policies and Procedures

El siguiente elemento fundamental del marco son las políticas y los procedimientos. Hubo un tiempo, no hace mucho tiempo, en que los bancos y las instituciones financieras no se tomaban muy en serio sus programas de políticas y procedimientos. Hoy, eso ha cambiado drásticamente bajo la atenta mirada de los reguladores. Se espera que las empresas tengan políticas y procedimientos claros, procesables y medibles.

De hecho, existe una tendencia en los servicios financieros a prestar más atención a la redacción y gestión activa de políticas y procedimientos. Un marco de políticas bien administrado brinda a las líneas de negocio una mayor flexibilidad porque las reglas no son ambiguas. Tener políticas y procedimientos bien administrados le da a la firma financiera una ventaja y una mayor autonomía al interactuar con los reguladores. Un buen marco de riesgo operativo tendrá políticas y procedimientos bien documentados que reflejen los requisitos de cada uno de los elementos.

RISK ASESSMENT



Risk Assessment

Con la gobernanza, la cultura y la conciencia, y las políticas y los procedimientos que unen el marco, ahora podemos pasar a las cuatro (*) piezas principales de trabajo que se necesitan para tener un marco de riesgo operativo eficaz:

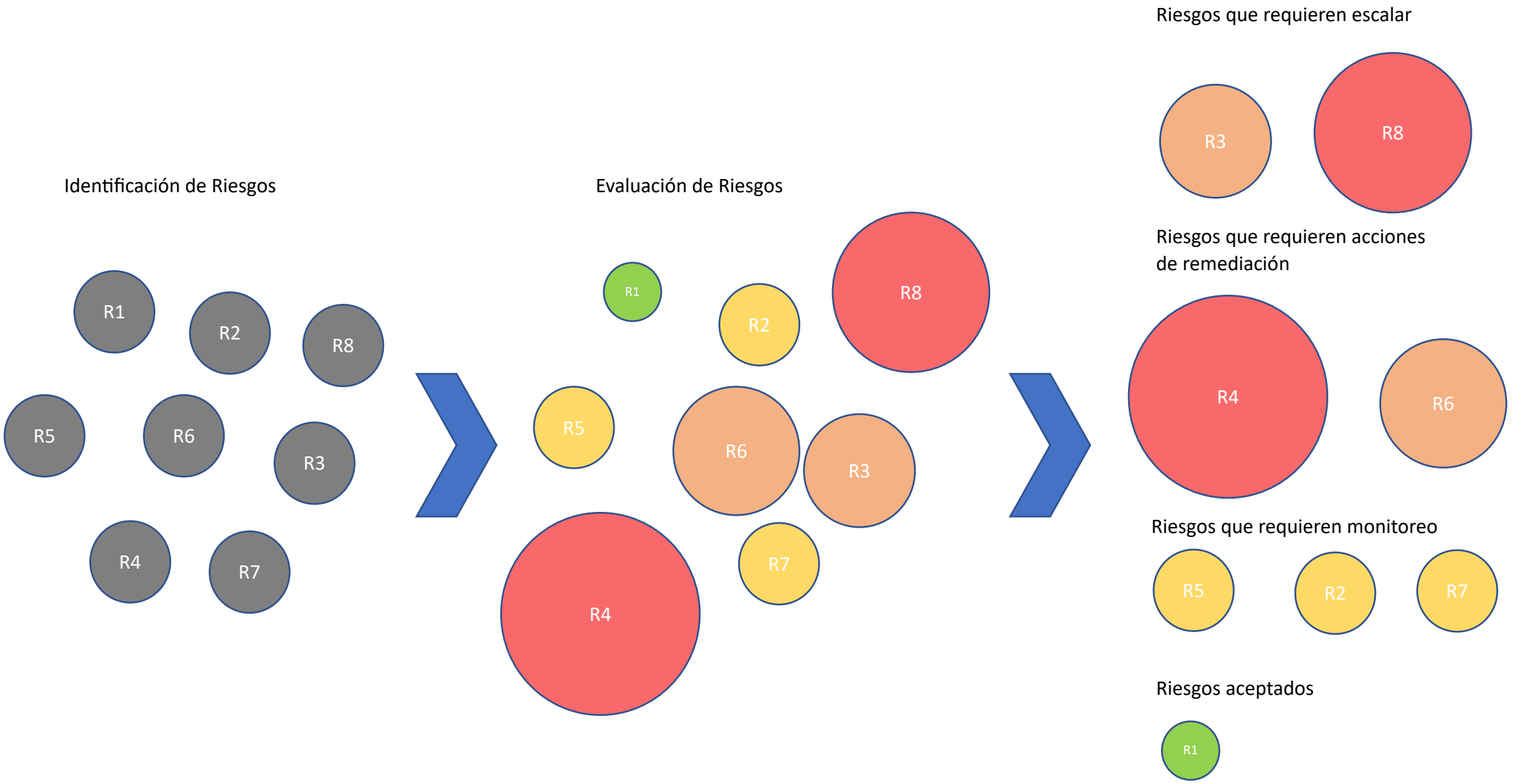
I. recopilación de datos de pérdidas,

II. autoevaluación de riesgos y controles

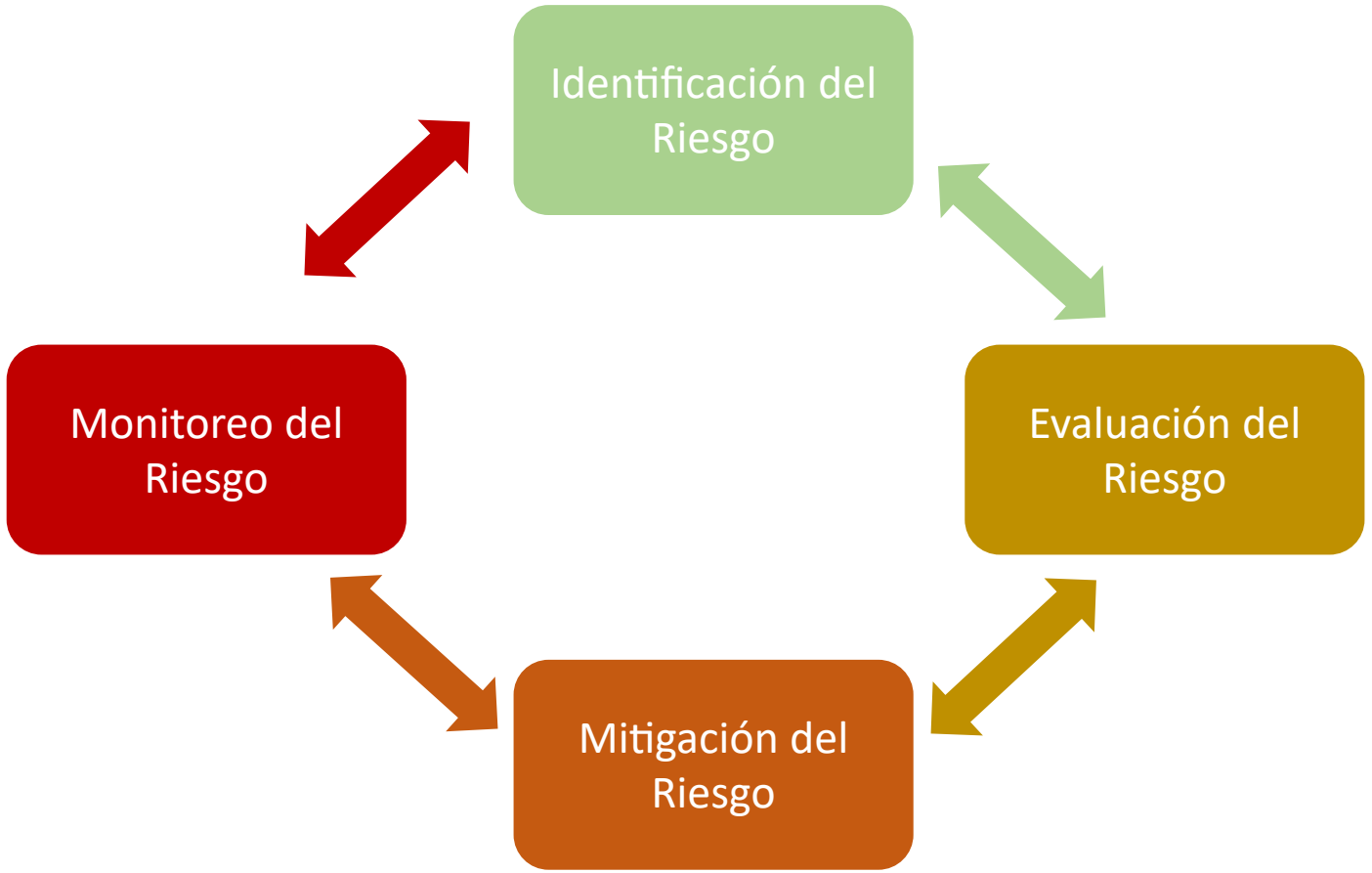
III. análisis de escenarios

IV. indicadores clave de riesgo.

Proceso de Riesgos



Proceso de Gestión de Riesgo Operativo Simplificado



Herramientas de Gestión de Riesgo Operativo

Identificación del Riesgo	Exposiciones y vulnerabilidades, Análisis de causa raíz, Pérdidas y cuasi pérdidas pasadas, Mapeo de procesos, Entrevistas
Evaluación del Riesgo	Pérdidas esperadas RCSA Escenarios Key Risk Indicators
Mitigación del Riesgo	Controles Internos & Pruebas Análisis Bow-Tie Planes de Acción preventivos Planes de contingencia
Monitoreo del Riesgo	Key Performance Indicators Key Risk Indicators Reporte de Riesgos Cálculo del capital

NEW 2021

Gestión de Eventos
Marco de aseguramiento y monitoreo de control
Benchmarking y análisis comparativo

Quizz

¿Qué herramientas usas principalmente para identificación de Riesgos Operativos?

Identificación de riesgos

La identificación de riesgos en una organización debe tener lugar tanto de arriba hacia abajo, a nivel de alta dirección, observando las grandes exposiciones y amenazas para el negocio, como de abajo hacia arriba, a nivel de procesos de negocio, observando vulnerabilidades o ineficiencias locales o específicas.

Estos procedimientos son diferentes pero complementarios, y ambos son vitales porque no es suficiente tener uno sin el otro.

De arriba hacia abajo:

- Riesgos para la estrategia
- Riesgos emergentes
- Tendencias globales
- Grandes amenazas

De abajo hacia arriba:

- Eficiencia operacional
- Procesos organizados
- Sistemas eficientes
- Personal competente