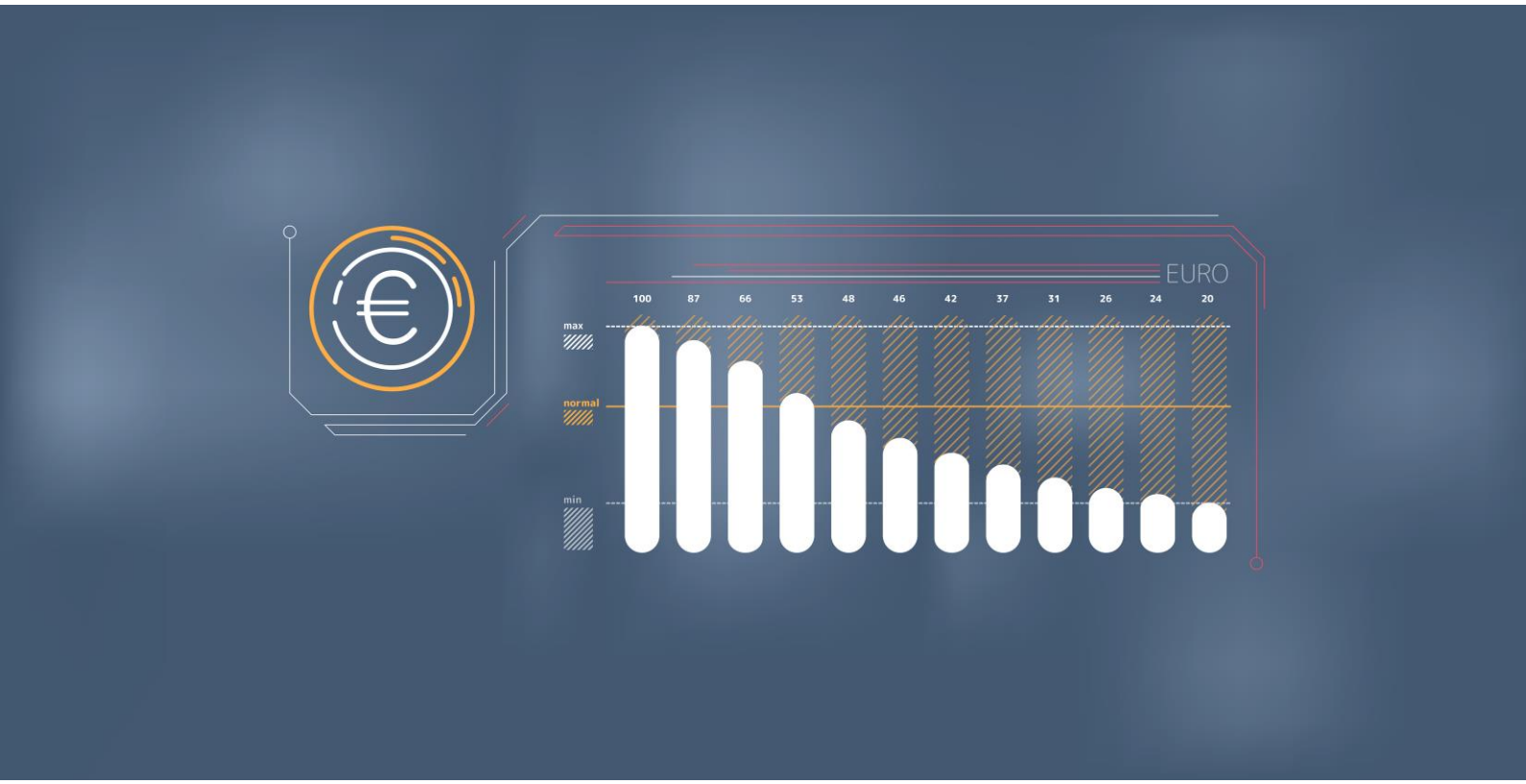
fermac risk

Estrategias Avanzadas de Gestión de Riesgos No Financieros

White Paper de FermacRisk | Abril 2024



www.fermacrisk.com | julia.tsedryk@fermakrisk.com

Prólogo

Bienvenido al curso sobre "Estrategias Avanzadas de Gestión de Riesgos No Financieros". En el panorama empresarial actual, en rápida evolución e interconectado, los bancos y las instituciones financieras se enfrentan a una serie de riesgos cada vez más complejos que van más allá de los riesgos financieros tradicionales. Los riesgos no financieros, como el riesgo operacional, el riesgo cibernético, el riesgo de cumplimiento y el riesgo reputacional, han surgido como desafíos críticos que pueden tener un impacto significativo en el rendimiento, la resiliencia y la confianza de una organización.

La crisis financiera mundial de 2008 y los acontecimientos posteriores de gran repercusión, como el escándalo del Libor, la controversia sobre las prácticas de venta de Wells Fargo y la filtración de datos de Equifax, han puesto de relieve la necesidad de que los bancos refuercen sus capacidades de gestión de riesgos no financieros. Los reguladores, los inversores y otras partes interesadas esperan cada vez más que los bancos demuestren marcos sólidos y eficaces para identificar, evaluar, supervisar y mitigar estos riesgos.

Este curso está diseñado para proporcionar a los participantes una comprensión completa de las últimas estrategias, herramientas y mejores prácticas para la gestión de riesgos no financieros en la banca. Se exploran entre otros temas:

- La evolución del panorama normativo y las expectativas de los supervisores en materia de gestión de riesgos no financieros
- Los principales tipos de riesgos no financieros y sus factores, repercusiones e interdependencias.
- El modelo de las tres líneas de defensa y los papeles y responsabilidades de las distintas funciones en la gestión de los riesgos no financieros.
- Metodologías y herramientas avanzadas para la identificación, evaluación, supervisión y mitigación de riesgos, como el análisis de escenarios, las pruebas de resistencia y el aprendizaje automático.
- La importancia de la cultura del riesgo, la gobernanza y la rendición de cuentas para impulsar una gestión eficaz de los riesgos no financieros.
- Tendencias y retos emergentes, como el impacto de la transformación digital, el cambio climático y los riesgos geopolíticos en la gestión de riesgos no financieros.

A lo largo del curso, utilizaremos estudios de casos, ejercicios interactivos y debates en grupo para ilustrar la aplicación práctica de estos conceptos y estrategias. Los participantes tendrán la oportunidad de aprender de profesionales experimentados y líderes de opinión en este campo, así como de establecer contactos con colegas de otros bancos e instituciones financieras.

Al finalizar este curso, los participantes habrán adquirido los conocimientos, las habilidades y la confianza necesarios para diseñar y aplicar marcos eficaces de gestión de riesgos no financieros en sus organizaciones. Estarán equipados para navegar por el complejo y dinámico panorama del riesgo, impulsar la toma de decisiones informadas sobre el riesgo y contribuir a la resiliencia general y al éxito de sus instituciones.

Esperamos emprender este viaje de aprendizaje con usted y explorar las fronteras de la gestión de riesgos no financieros en la banca.

1. Riesgo no financiero

El riesgo no financiero se refiere a los tipos de riesgo que no implican directamente transacciones financieras o pérdidas financieras, pero que pueden afectar significativamente a las operaciones, la reputación y la viabilidad a largo plazo de una organización. Estos riesgos suelen estar interconectados y pueden tener profundas implicaciones en los objetivos estratégicos, la eficiencia operativa y las obligaciones de cumplimiento de una organización. He aquí un desglose de los principales tipos de riesgos no financieros:

Riesgo operacional: se trata de los riesgos derivados de los procesos internos, las personas y los sistemas de una organización o de acontecimientos externos. Algunos ejemplos son los fallos del sistema, el fraude, los ciberataques y los errores humanos. Gestionar el riesgo operacional implica mejorar los procesos, formar a los empleados y aplicar controles eficaces y medidas de recuperación en caso de catástrofe.

Riesgo estratégico: Surge de decisiones empresariales adversas, de la aplicación incorrecta de las decisiones o de la falta de capacidad de respuesta a los cambios del sector. Los riesgos estratégicos pueden afectar a los objetivos estratégicos de la organización y originarse por cambios en el modelo de negocio, cambios en la gestión o falta de adaptación a un entorno empresarial cambiante.

Riesgo reputacional: Implica riesgos para la reputación de la empresa derivados de una opinión pública negativa, la cobertura de los medios de comunicación u otros acontecimientos. El daño a la reputación puede derivarse de un mal servicio al cliente, escándalos públicos y malas prácticas de gestión. Puede afectar a la fidelidad de los clientes, al valor de la empresa y repercutir significativamente en los ingresos.

Riesgo de cumplimiento: También conocido como riesgo normativo, implica riesgos asociados a la necesidad de cumplir las leyes, reglamentos y prácticas prescritas. Los cambios en las leyes o reglamentos, o el incumplimiento de los existentes, pueden dar lugar a sanciones legales, confiscación financiera y daños a la reputación.

Riesgo climático: Son los riesgos relacionados con el entorno físico, incluidas las catástrofes naturales y los efectos del cambio climático. Los riesgos medioambientales pueden perturbar las operaciones empresariales y exigir cambios significativos en las prácticas y estrategias empresariales.

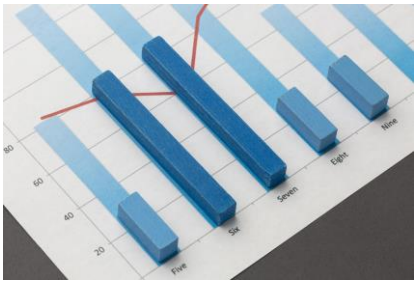
Riesgo de ciberseguridad: Como parte del riesgo operacional, pero cada vez más importante por sí mismo, implica riesgos asociados al uso, propiedad, funcionamiento, participación, influencia y adopción de TI dentro de una empresa. Incluye riesgos de ciberataques y violaciones de datos que pueden provocar importantes daños financieros y de reputación.

Riesgo de conducta: en banca se refiere al riesgo de que las instituciones financieras o sus empleados incurran en comportamientos poco éticos, ilegales o inapropiados que puedan perjudicar a los clientes, dañar la reputación de la institución o acarrear consecuencias legales y financieras.

Riesgo geopolítico: Estos riesgos se derivan de los cambios políticos o la inestabilidad en regiones nacionales o internacionales, que afectan a la inversión, las divisas, la normativa comercial y la política económica de forma que pueden afectar a los mercados, los costes y las operaciones de una empresa.

Las organizaciones gestionan los riesgos no financieros mediante una combinación de estrategias de identificación, evaluación, control y seguimiento de riesgos. Esto implica a menudo marcos integrales de gestión de riesgos y auditorías periódicas para garantizar que los riesgos se gestionan de forma proactiva y en consonancia con los objetivos estratégicos más amplios de la organización.

2. Gestión de Riesgos No Financieros



La gestión de riesgos no financieros en la banca implica un enfoque estructurado para identificar, evaluar, vigilar y mitigar los riesgos que no están directamente relacionados con los resultados financieros o las condiciones del mercado. Aunque las metodologías específicas pueden variar en función del tamaño, la complejidad y el perfil de riesgo del banco, existen algunos elementos comunes y buenas prácticas que se utilizan ampliamente en el sector.

Modelo de las tres líneas de defensa:
Este modelo es un marco de gobernanza que define las funciones y responsabilidades en materia de gestión y control de riesgos en toda la organización.

- Primera línea de defensa: Incluye las unidades de negocio y las funciones que poseen y gestionan los riesgos asociados a sus actividades. Son responsables de identificar, evaluar y mitigar los riesgos dentro de sus áreas de responsabilidad.
- Segunda línea de defensa: Incluye las funciones de gestión de riesgos y cumplimiento que proporcionan supervisión, apoyo y desafío a la primera línea. Son responsables de desarrollar políticas, herramientas y metodologías de gestión de riesgos, así como de supervisar e informar sobre la exposición al riesgo y la eficacia de los controles.
- Tercera línea de defensa: Incluye la función de auditoría interna, que proporciona una garantía independiente de la eficacia de los procesos de gestión y control de riesgos en toda la organización.

Autoevaluación de riesgos y controles (RCSA):
Se trata de un proceso en el que las unidades de negocio y las funciones evalúan periódicamente sus propios riesgos y controles, normalmente mediante talleres, cuestionarios o entrevistas. El RCSA ayuda a identificar y priorizar los riesgos, evaluar la eficacia de los controles existentes y desarrollar planes de acción para subsanar cualquier laguna o punto débil.

Indicadores clave de riesgo (KRI):
Se trata de métricas o puntos de datos que proporcionan señales de alerta temprana de posibles exposiciones a riesgos o fallos de control. Los KRI pueden utilizarse para supervisar tendencias, activar alertas y fundamentar decisiones de gestión de riesgos. Ejemplos de KRI para el riesgo operacional pueden ser el tiempo de inactividad del sistema, las quejas de los clientes o los índices de rotación de empleados.

Análisis de escenarios y pruebas de resistencia:
Esto implica el uso de escenarios hipotéticos o históricos para evaluar el impacto potencial de acontecimientos adversos sobre las operaciones, la reputación o la posición financiera del banco. El análisis de escenarios puede ayudar a identificar vulnerabilidades, comprobar la eficacia de las estrategias de mitigación de riesgos y fundamentar el apetito por el riesgo y la fijación de límites.

Gestión de incidentes y análisis de causas:
Se trata de los procesos de detección, notificación, investigación y resolución de incidentes de riesgo o fallos de control. El análisis de la causa raíz se utiliza para identificar los factores subyacentes que han contribuido al incidente y desarrollar medidas correctivas para evitar que se produzcan incidentes similares en el futuro.

Marco de apetito por el riesgo:
Se trata de una declaración formal que define los tipos y niveles de riesgo que el banco está dispuesto a aceptar en la consecución de sus objetivos estratégicos. El marco de apetito por el riesgo establece los límites de las actividades de asunción de riesgos y sirve de base para el seguimiento y la información sobre riesgos.

Gobernanza e información:
Una gestión eficaz de los riesgos no financieros requiere estructuras de gobierno, funciones y responsabilidades claras, así como la presentación periódica de informes a la alta dirección y al consejo de administración. Los comités y foros de riesgo pueden utilizarse para revisar la exposición al riesgo, debatir estrategias de gestión del riesgo y tomar decisiones basadas en el riesgo.

Estas metodologías y enfoques no son mutuamente excluyentes y a menudo se utilizan en combinación para proporcionar una visión global e integrada de los riesgos no financieros en toda la organización. Los bancos también pueden utilizar herramientas y tecnologías especializadas, como sistemas de información de gestión de riesgos, análisis de datos o aprendizaje automático, para apoyar sus procesos de gestión de riesgos no financieros. La eficacia de estas metodologías depende de factores como la calidad de los datos, las competencias y la experiencia de los profesionales del riesgo, el tono de la cúpula y la cultura general de riesgo de la organización.

3. Riesgo de conducta

El riesgo de conducta en la banca se refiere al riesgo de que las instituciones financieras o sus empleados incurran en comportamientos poco éticos, ilegales o inapropiados que puedan perjudicar a los clientes, dañar la reputación de la institución o acarrear consecuencias legales y financieras. Este tipo de riesgo es un subconjunto del riesgo no financiero y ha ganado mayor atención en los últimos años debido a los casos de mala conducta de alto perfil en la industria bancaria.

Algunos Ejemplos de riesgo de conducta en la banca

Venta indebida de productos financieros: Esto ocurre cuando los empleados del banco venden productos o servicios que no son adecuados para las necesidades de un cliente, a menudo para cumplir los objetivos de ventas o ganar comisiones.

Manipulación del mercado: Consiste en el intento deliberado de interferir en el funcionamiento justo y ordenado de los mercados financieros, por ejemplo mediante el uso de información privilegiada o la fijación de precios.

Blanqueo de capitales: Se refiere al proceso de disfrazar el producto de actividades ilegales como fondos legítimos, lo que puede ocurrir cuando los bancos no controlan e informan adecuadamente de las transacciones sospechosas.

Discriminación: Incluye el trato injusto a clientes o empleados por factores como la raza, el sexo o la religión.

Violación de la privacidad de los datos: Esto implica el acceso, uso o divulgación no autorizados de la información personal o financiera de los clientes.

Para gestionar el riesgo de conducta, los bancos deben establecer una sólida cultura ética, aplicar políticas y procedimientos sólidos y ofrecer formación periódica a los empleados. Esto puede incluir medidas como:

- Establecer normas de conducta claras y comunicarlas a todos los empleados.
- Implantación de programas eficaces de gestión de riesgos y cumplimiento
- Realización de auditorías y controles periódicos para detectar y prevenir conductas indebidas.
- Proporcionar canales para que los empleados y los clientes comuniquen sus preocupaciones o quejas.
- Investigar y abordar con prontitud cualquier caso de conducta indebida.
- Fomentar una cultura de transparencia, responsabilidad y comportamiento ético

Los reguladores también desempeñan un papel crucial en la supervisión y aplicación de las normas de conducta en el sector bancario. Los bancos que no gestionan eficazmente el riesgo de conducta pueden enfrentarse a importantes multas, acciones legales y daños a su reputación.

4. CiberRiesgo

El riesgo cibernético en la banca se refiere a la posibilidad de pérdidas financieras, interrupciones del negocio o daños a la reputación derivados de ciberataques, violaciones de datos u otros incidentes relacionados con la tecnología. A medida que los bancos dependen cada vez más de sistemas y redes digitales para llevar a cabo sus operaciones y atender a los clientes, se vuelven más vulnerables a las ciberamenazas. El riesgo cibernético es una preocupación crítica para los bancos, ya que puede comprometer información sensible de los clientes, interrumpir las transacciones financieras y socavar la confianza del público en la institución.

Algunos tipos comunes de riesgos cibernéticos en la banca incluyen:

- Ataques de malware y ransomware: Estos implican el uso de software malicioso para obtener acceso no autorizado a sistemas bancarios, robar datos o mantener los sistemas como rehenes hasta que se pague un rescate.
- Phishing e ingeniería social: Estas técnicas consisten en engañar a empleados bancarios o clientes para que revelen información sensible, como credenciales de acceso o datos financieros, a menudo a través de correos electrónicos o sitios web falsos.
- Denegación de servicio distribuida (DDoS): los ataques saturan de tráfico la red o los servidores de un banco, provocando su caída o que dejen de estar disponibles para los clientes.
- Amenazas internas: Implican a empleados o contratistas del banco que hacen un uso indebido de sus privilegios de acceso para robar datos o cometer fraude.
- Riesgos para terceros: Los bancos a menudo dependen de proveedores o socios externos para diversos servicios, y un ciberataque a estos terceros también puede afectar a las operaciones y la reputación del banco.

Para gestionar el riesgo cibernético, los bancos deben implantar un marco de ciberseguridad integral que incluya:

- Evaluación y gestión de riesgos: Identificar y evaluar periódicamente los ciberriesgos y aplicar los controles y estrategias de mitigación adecuados.
- Arquitectura de redes seguras: Diseño y mantenimiento de infraestructuras informáticas seguras, incluidos cortafuegos, sistemas de detección de intrusos y cifrado.
- Formación y concienciación de los empleados: Impartir formación periódica sobre ciberseguridad a los empleados y promover una cultura de concienciación sobre la seguridad.
- Respuesta a incidentes y recuperación: Desarrollar y probar planes para detectar, responder y recuperarse de incidentes cibernéticos.
- Cumplimiento de la normativa: Cumplimiento de las normativas y estándares de ciberseguridad pertinentes, como el Estándar de Seguridad de Datos del Sector de las Tarjetas de Pago (PCI DSS) o el Marco de Ciberseguridad del NIST.
- Colaboración con socios del sector: Compartir información sobre amenazas y mejores prácticas con otros bancos y grupos del sector para mantenerse informado sobre las ciberamenazas emergentes.

A medida que las amenazas cibernéticas siguen evolucionando, la gestión eficaz del riesgo cibernético es un proceso continuo que requiere supervisión, adaptación e inversión continuas en capacidades de ciberseguridad. Los bancos que no aborden adecuadamente el riesgo cibernético pueden enfrentarse a pérdidas financieras significativas, sanciones reglamentarias y erosión de la confianza de los clientes.

5. Riesgos operacionales

El riesgo operacional en banca se refiere al riesgo de pérdidas resultantes de procesos internos

inadecuados o fallidos, personas, sistemas o acontecimientos externos. Este tipo de riesgo es inherente a todas las actividades bancarias y puede tener importantes consecuencias financieras, de reputación y regulatorias. El riesgo operacional puede derivarse de una amplia gama de factores, como errores humanos, fraude, fallos de ciberseguridad, catástrofes naturales y fallos de terceros.

Algunos ejemplos comunes de riesgo operacional en la banca incluyen:

- Errores en el procesamiento de transacciones: Los errores en el procesamiento de pagos, transferencias u otras transacciones financieras pueden provocar pérdidas o insatisfacción de los clientes.
- Fraude y mala conducta: Incluyen tanto el fraude interno (por ejemplo, el robo de empleados o el uso de información privilegiada) como el fraude externo (por ejemplo, el robo de identidad o el fraude con cheques).
- Fallos de los sistemas informáticos: Las averías o interrupciones en los sistemas informáticos, redes o aplicaciones de un banco pueden interrumpir las operaciones comerciales y perjudicar el servicio al cliente.
- Cumplimiento y riesgos legales: El incumplimiento de leyes, reglamentos o políticas internas puede acarrear multas, acciones legales o daños a la reputación.
- Continuidad de la actividad y recuperación en caso de catástrofe: Los bancos deben estar preparados para mantener las operaciones críticas durante y después de acontecimientos perturbadores, como catástrofes naturales, cortes de electricidad o pandemias.

Para gestionar el riesgo operacional, los bancos suelen seguir un enfoque estructurado que incluye:

- Identificación y evaluación de riesgos: Identificación y evaluación periódicas de los riesgos operativos en todas las unidades de negocio y procesos.
- Diseño y aplicación de controles: Desarrollo e implantación de controles para prevenir, detectar o mitigar los riesgos operativos, como la segregación de funciones, los límites de autorización o las comprobaciones automatizadas.
- Supervisión e información: Seguimiento continuo de los indicadores e incidentes de riesgo operacionale información de estos a la alta dirección y al consejo de administración.
- Formación y sensibilización: Proporcionar a los empleados las habilidades y conocimientos necesarios para desempeñar sus funciones con eficacia y de conformidad con las políticas y procedimientos.
- Gestión de incidentes y respuesta: Establecer procesos para detectar, investigar y resolver rápidamente los incidentes de riesgo operacional, así como aprender de ellos para evitar que se repitan en el futuro.
- Seguros y transferencia de riesgos: Utilización de pólizas de seguros u otros mecanismos de transferencia de riesgos para mitigar el impacto financiero de determinados riesgos operativos.

Los bancos deben mantener un capital adecuado para cubrir sus exposiciones al riesgo operacional, según el marco de Basilea III. También deben informar periódicamente a los reguladores sobre sus prácticas y resultados en materia de gestión del riesgo operacional. Una gestión eficaz del riesgo operacional es esencial para garantizar la estabilidad, la eficiencia y la reputación de los bancos y del sistema financiero en general.

6. Riesgo geopolítico

El riesgo geopolítico en la banca se refiere al impacto potencial de los acontecimientos o condiciones políticas, sociales o económicas en diferentes países o regiones sobre las operaciones, inversiones o clientes de un banco. Estos riesgos pueden derivarse de diversos factores, como cambios en las políticas gubernamentales, conflictos internacionales, disputas comerciales, disturbios sociales o inestabilidad económica. Los acontecimientos geopolíticos pueden perturbar los mercados financieros, alterar los flujos de inversión y afectar a la solvencia de los prestatarios, provocando pérdidas o mayores costes para los bancos.

Algunos ejemplos de riesgos geopolíticos que pueden afectar a los bancos son:

- Inestabilidad política o cambios de régimen: Los cambios repentinos en el liderazgo político o en las políticas pueden crear incertidumbre y volatilidad en los mercados financieros, afectando al valor de las inversiones de un banco o a la capacidad de sus prestatarios para devolver los préstamos.
- Sanciones económicas o restricciones comerciales: Los gobiernos pueden imponer sanciones o barreras comerciales a determinados países, industrias o individuos, lo que puede perturbar las actividades comerciales de un banco o exponerlo a riesgos legales y de reputación.
- Conflictos o terrorismo: Los conflictos armados, los disturbios civiles o los atentados terroristas pueden dañar las infraestructuras, perturbar la actividad económica y crear riesgos de seguridad para los empleados y clientes de un banco.
- Crisis de deuda soberana: Cuando los países tienen dificultades para devolver su deuda, pueden producirse impagos, devaluaciones de la moneda o crisis bancarias, que afectan al valor de las inversiones de los bancos y a la estabilidad del sistema financiero.

Para gestionar el riesgo geopolítico, los bancos deben:

- Vigilar y evaluar los acontecimientos geopolíticos: Seguir y analizar continuamente los acontecimientos y tendencias geopolíticos y evaluar su posible impacto en las operaciones y carteras del banco.
- Diversificar la exposición geográfica: Repartir las inversiones y las actividades de préstamo entre distintos países y regiones para reducir el riesgo de concentración.
- Realizar pruebas de resistencia y análisis de escenarios: Simular el impacto potencial de los acontecimientos geopolíticos en la posición financiera y los resultados del banco y desarrollar planes de contingencia.
- Cumplir las sanciones y la normativa: Garantizar el cumplimiento de las leyes y reglamentos aplicables en materia de sanciones, lucha contra el blanqueo de capitales y financiación del terrorismo.
- Comprometerse con las partes interesadas y los responsables políticos: Mantener una comunicación abierta con clientes, inversores, reguladores y otras partes interesadas para comprender sus preocupaciones y expectativas, y ofrecer transparencia sobre las prácticas de gestión del riesgo geopolítico del banco.

Una gestión eficaz de los riesgos geopolíticos requiere una combinación de información sobre los mercados mundiales, una sólida evaluación y supervisión de los riesgos y una toma de decisiones ágil. Los bancos capaces de navegar por el complejo y cambiante panorama de los riesgos geopolíticos están mejor posicionados para proteger sus activos, mantener la confianza de sus clientes y respaldar un crecimiento sostenible.

7. Riesgos deTerceros

Los riesgos de terceros y la externalización en la banca se refieren a los riesgos potenciales que surgen cuando un banco contrata a partes externas, como vendedores, proveedores de servicios o socios, para realizar determinadas funciones o suministrar productos y servicios. La externalización es cada vez más común en el sector bancario para reducir costes, acceder a conocimientos especializados y centrarse en las competencias básicas. Sin embargo, también introduce nuevos riesgos que los bancos deben identificar, evaluar y gestionar eficazmente.

Algunos ejemplos de riesgos de terceros en la banca son:

- Interrupciones o fallos del servicio: Si un proveedor externo experimenta problemas

operativos o no presta los servicios esperados, puede interrumpir las operaciones del banco y perjudicar el servicio al cliente.

- Seguridad de los datos y violaciones de la privacidad: Cuando los bancos comparten datos sensibles de clientes o financieros con terceros, existe el riesgo de acceso no autorizado, divulgación o uso indebido de esa información.
- Cumplimiento e infracciones normativas: Los terceros pueden no cumplir las mismas normas legales y reglamentarias que el banco, exponiéndolo a posibles multas, sanciones o daños a su reputación.
- Inestabilidad financiera o insolvencia: Si un proveedor externo crítico atraviesa dificultades financieras o quiebra, puede interrumpir las operaciones del banco y requerir sustituciones costosas y lentas.
- Riesgo de concentración: Los bancos pueden llegar a depender excesivamente de un único proveedor externo, aumentando el impacto potencial de cualquier interrupción o fallo.

Para gestionar eficazmente los riesgos de terceros, los bancos deben:

- Realice una diligencia debida exhaustiva: Examine y seleccione cuidadosamente a los proveedores externos en función de su estabilidad financiera, reputación, prácticas de seguridad y capacidad para cumplir los requisitos del banco.
- Establezca contratos y acuerdos de nivel de servicio (SLA) claros: Defina por escrito las funciones, responsabilidades, expectativas de rendimiento y rendición de cuentas de ambas partes.
- Supervisar y evaluar el rendimiento: Revise periódicamente el rendimiento del tercero con respecto a las métricas acordadas y realice auditorías o evaluaciones periódicas para identificar cualquier problema o riesgo.
- Mantener la supervisión y el control: Conserve la responsabilidad última de las funciones externalizadas y mantenga la experiencia y los recursos necesarios para supervisar y controlar las actividades del tercero.
- Desarrolle planes de contingencia y de salida: Disponga de planes para garantizar la continuidad de los servicios en caso de interrupciones o finalización de la relación con terceros.
- Cumplir los requisitos normativos: Garantizar que los acuerdos de externalización del banco cumplen las leyes, normativas y expectativas de supervisión pertinentes, como los requisitos de protección de datos, privacidad y resistencia operativa.

La gestión eficaz del riesgo de terceros es un componente esencial del marco general de gestión de riesgos de un banco. Requiere la colaboración permanente de diversas funciones, como las de compras, legal, cumplimiento, TI y gestión de riesgos. Los bancos también deben mantener informados a sus altos directivos y al consejo de administración sobre el estado y el rendimiento de las relaciones críticas con terceros. Dado que el sector bancario está cada vez más interconectado y depende cada vez más de proveedores externos, una sólida gestión del riesgo de terceros es crucial para mantener la seguridad, la solidez y la reputación de los bancos individuales y del sistema financiero en general.

8. Riesgo estratégico

El riesgo estratégico en la banca se refiere a los posibles efectos adversos sobre los beneficios o el capital de un banco derivados de cambios en el entorno empresarial, malas decisiones empresariales, aplicación inadecuada de las decisiones o incapacidad para responder a los cambios en el panorama competitivo. Este riesgo puede afectar significativamente a la capacidad de un banco para alcanzar sus objetivos

estratégicos y mantener su posición competitiva. He aquí los componentes y consideraciones clave relacionados con el riesgo estratégico en el sector bancario:

Componentes clave del riesgo estratégico en la banca

- Vulnerabilidad del modelo de negocio: El riesgo estratégico puede surgir si el modelo de negocio de un banco no es resistente a los cambios en el entorno del mercado o en el comportamiento de los clientes. Por ejemplo, la dependencia de una única línea de productos o segmento de mercado puede plantear riesgos significativos si cambia la dinámica del mercado.
- La competencia: La aparición de nuevos competidores, especialmente losFintech y otros proveedores de servicios financieros no tradicionales, puede amenazar la cuota de mercado y la rentabilidad de los bancos establecidos. El riesgo estratégico implica evaluar y adaptarse a estas presiones competitivas.
- Cambios tecnológicos: Los rápidos avances tecnológicos, como la banca digital, el Blockchain y la inteligencia artificial, pueden dejar obsoletas las prácticas bancarias tradicionales. Los bancos se enfrentan a riesgos estratégicos si no innovan o no se adaptan a estas tendencias tecnológicas.
- Entorno normativo: Los cambios en los requisitos normativos pueden afectar significativamente a las operaciones y la dirección estratégica de un banco. Por ejemplo, el aumento de los requisitos de capital o leyes más estrictas de protección del consumidor pueden afectar a la planificación estratégica y la rentabilidad.
- Cambios económicos: Los cambios macroeconómicos, como las fluctuaciones de los tipos de interés, la inflación o las recesiones económicas, pueden plantear riesgos estratégicos al afectar a las actividades de inversión y préstamo de un banco.
- Reputación e imagen de marca: Los acontecimientos que dañan la reputación de un banco, como la implicación en escándalos financieros o fallos operativos, pueden tener consecuencias estratégicas a largo plazo, afectando a la confianza y fidelidad de los clientes.

Gestión del riesgo estratégico en la banca

- Planificación y análisis estratégicos: Las sesiones periódicas de planificación estratégica, que incluyen análisis de escenarios y pruebas de resistencia, pueden ayudar a los bancos a anticiparse y prepararse para posibles cambios en el entorno empresarial.
- Diversificación: Mediante la diversificación de productos, servicios y presencia geográfica, los bancos pueden reducir su vulnerabilidad ante acontecimientos adversos en cualquier área de su negocio.
- Innovación y adopción de tecnología: Invertir en tecnología e innovación puede ayudar a los bancos a seguir siendo competitivos y responder a los cambios en el comportamiento de los consumidores y los avances tecnológicos.
- Cumplimiento normativo y defensa: Mantenerse a la vanguardia de los cambios normativos y participar activamente en los debates sobre regulación puede ayudar a los bancos a gestionar y mitigar los riesgos asociados al cumplimiento normativo.
- Cultura y gobernanza del riesgo: Cultivar una cultura consciente del riesgo y unas estructuras de gobernanza sólidas garantiza que las decisiones estratégicas se tomen con una clara comprensión de sus implicaciones de riesgo.
- Supervisión y revisión: La supervisión continua del entorno externo y del rendimiento interno, junto con revisiones periódicas de las metas y objetivos estratégicos, ayuda a los bancos a ajustar sus estrategias en respuesta a los riesgos y oportunidades emergentes.

Importancia de gestionar el riesgo estratégico

Para los bancos, la gestión del riesgo estratégico es crucial para mantener el crecimiento y la rentabilidad. Implica no sólo protegerse frente a posibles inconvenientes, sino también aprovechar las oportunidades que se ajusten a la visión estratégica del banco. La gestión eficaz del riesgo estratégico ayuda a garantizar que un

banco siga siendo resistente, adaptable y competitivo en un panorama de servicios financieros en rápida evolución.

9. Riesgo climático

El riesgo climático en la banca se refiere a los riesgos financieros a los que se enfrentan los bancos debido al cambio climático. Estos riesgos pueden clasificarse a grandes rasgos en dos tipos principales: riesgos físicos y riesgos de transición. Ambos pueden afectar significativamente a la calidad de los activos del sector bancario, a sus estrategias de inversión y a su estabilidad financiera general. He aquí un desglose de cada tipo y cómo afectan a los bancos:

Riesgos físicos

Los riesgos físicos se derivan del impacto directo de los fenómenos relacionados con el cambio climático, como las condiciones meteorológicas adversas y las catástrofes naturales. Entre ellos figuran:

- Riesgos agudos: Se trata de riesgos provocados por acontecimientos como tormentas, inundaciones, incendios forestales y otros fenómenos meteorológicos extremos. Pueden dañar directamente la propiedad y las infraestructuras, afectando al valor de las garantías y a la capacidad de los prestatarios para devolver los préstamos.
- Riesgos crónicos: Son el resultado de cambios a largo plazo en los patrones climáticos, como la subida del nivel del mar, el aumento de la temperatura y la modificación de los regímenes de precipitaciones. Los riesgos crónicos pueden alterar la productividad agrícola, interrumpir el suministro de agua y afectar a la estabilidad económica de las regiones, influyendo así en los riesgos crediticios asociados a hipotecas, préstamos agrícolas y otros productos financieros.

Riesgos de la transición

Los riesgos de transición están asociados al proceso de ajuste hacia una economía con menos emisiones de carbono. Entre ellos figuran:

- Riesgos políticos y jurídicos: A medida que los gobiernos aplican políticas para mitigar el cambio climático, como la tarificación del carbono, la regulación de las emisiones o los incentivos a las energías renovables, los bancos pueden enfrentarse a riesgos relacionados con los cambios en el valor de los activos o el aumento de los costes de cumplimiento.
- Riesgos tecnológicos: El rápido desarrollo de tecnologías que contribuyen a una economía con bajas emisiones de carbono, como las tecnologías de energía renovable, los vehículos eléctricos y las soluciones de eficiencia energética, puede dar lugar a activos bloqueados o exigir cambios en las estrategias de inversión.
- Riesgos de mercado: Los cambios en la dinámica de la oferta y la demanda de materias primas, como los combustibles fósiles y los recursos renovables, pueden repercutir en los mercados financieros y en la valoración de los activos.
- Riesgos para la reputación: El aumento de la concienciación y la preocupación por el cambio climático puede influir en las preferencias y los comportamientos de los clientes, lo que repercute en la reputación de un banco en función de su postura y sus políticas medioambientales.

Gestión del riesgo climático en la banca

Los bancos reconocen cada vez más la importancia de gestionar los riesgos climáticos y adoptan diversas estrategias para mitigar su impacto:

- Evaluación e integración de riesgos: Los bancos están integrando los riesgos climáticos en sus marcos generales de gestión de riesgos. Esto implica evaluar la vulnerabilidad de sus carteras de préstamos a los riesgos relacionados con el clima y ajustar los procesos de evaluación del riesgo crediticio para tener en cuenta estos factores.

- Análisis de escenarios y pruebas de resistencia: Los bancos están utilizando el análisis de escenarios relacionados con el clima y las pruebas de estrés para comprender los impactos potenciales bajo diversos escenarios de calentamiento global. Esto ayuda a planificar la resiliencia y la adaptación estratégica.

- Inversión estratégica: Al invertir en proyectos verdes y sostenibles, como las energías renovables y las tecnologías energéticamente

eficientes, los bancos no sólo mitigan el riesgo climático, sino que también capitalizan nuevas oportunidades de negocio en la creciente economía verde.

- Mejora de la transparencia y la información: Los bancos están mejorando su divulgación de los riesgos climáticos en consonancia con marcos internacionales como el Grupo de Trabajo sobre Divulgación de Información Financiera relacionada con el Clima (TCFD). Esto aumenta la transparencia y permite a las partes interesadas tomar decisiones con conocimiento de causa.
- Compromiso y colaboración: Los bancos están colaborando con otras partes interesadas, como gobiernos, industrias y el público en general, para desarrollar estrategias integrales que aborden los riesgos climáticos. Esto incluye participar en iniciativas como los Principios para una Banca Responsable.

El riesgo climático presenta importantes retos y oportunidades para el sector bancario. Mediante una gestión eficaz de estos riesgos, los bancos no sólo pueden protegerse de posibles inconvenientes, sino también contribuir a una transición económica sostenible que mitigue los efectos del cambio climático. Este planteamiento proactivo es cada vez más crucial a medida que se acentúan los efectos del cambio climático y aumentan las presiones reguladoras y de los consumidores.