DOI: https://doi.org/10.34069/AI/2023.71.11.1

How to Cite:
Cuellar-Orozco, M., Patiño-Ortiz, J., Cuellar-Orozco, L., Cuellar-Orozco, A., & Patiño-Ortiz, M. (2023). Modelo de sistema viable para la gestión de riesgo operacional en instituciones bancarias. *Amazonia Investiga*, *12*(71), 9-25. https://doi.org/10.34069/AI/2023.71.11.1

Modelo de sistema viable para la gestión de riesgo operacional en instituciones bancarias

Viable system model for operational risk management in banking institutions

Received: September 22, 2023 Accepted: November 15, 2023

Written by:
Maricela Cuellar-Orozco[1]
https://orcid.org/0000-0002-6558-4938
Julian Patiño-Ortiz[2]
https://orcid.org/0000-0001-8106-9293
Lorena Cuellar-Orozco[3]
https://orcid.org/0009-0001-8583-245X
Armando Cuellar-Orozco[4]
https://orcid.org/0009-0006-9766-6571
Miguel Patiño-Ortiz[5]
https://orcid.org/0000-0002-5630-8077

Resumen

A partir de los lineamientos que exigen las instancias reguladoras a las instituciones bancarias para poder gestionar sus riesgos operacionales, establecen estándares y marcos que definen sus estructuras de gestión de riesgo para permitir a las instituciones bancarias controlar, mitigar y evitar la materialización del riesgo. Desafortunadamente los marcos hacen que las instituciones bancarias corran el riesgo de desaparecer si no proponen soluciones flexibles en el manejo de reserva de capital para el riesgo operacional. La flexibilidad de la estructura organizacional es necesaria para la viabilidad en la situación actual por lo que la propuesta es la utilización del Modelo de Sistema Viable (VSM) que permite gestionar y supervisar el riesgo operacional de las instituciones bancarias como un marco adaptable e integral basado en un modelo científico con enfoque sistémico. La metodología se realiza en el contexto bancario mexicano, demostrando que al aplicar el VSM

Abstract

Based on the guidelines that regulatory bodies require from banking institutions in order to manage their operational risks, they establish standards and frameworks that define their risk management structures to allow banking institutions to control, mitigate and avoid the materialization of risk. Unfortunately, the frameworks put banking institutions at risk of disappearing if they do not propose flexible solutions in the management of capital reserve for operational risk. The flexibility of the organizational structure is necessary for viability in the current situation, so the proposal is the use of the Viable System Model (VSM) that allows managing and supervising the operational risk of banking institutions as an adaptable and comprehensive framework based in a scientific model with a systemic approach. The methodology is carried out in the Mexican banking context, demonstrating that by applying the VSM as a framework to manage operational risk, the

[1] Doctora en Ciencias en Administración, Profesora Investigadora en el Instituto Politécnico Nacional, ESIME Zacatenco, Ciudad de México, México. WoS Researcher ID: JVZ-8260-2024
[2] Doctor en Ciencias en Ingeniería Mecánica y Doctor en Ciencias en Administración, Profesor Investigador en el Instituto Politécnico Nacional, ESIME Zacatenco, Ciudad de México, México. WoS Researcher ID: HMV-3376-2023
[3] Candidata para el Doctorado en Ingeniería de Sistemas, Instituto Politécnico Nacional, ESIME Zacatenco, Ciudad de México, México. WoS Researcher ID: JVZ-8311-2024
[4] Maestro en Ciencias en Ingeniería de Sistemas, Profesor Titular en el Tecnológico Nacional de México, TES de Cuautitlán Izcalli, Estado de México, México. WoS Researcher ID: JVZ-8348-2024
[5] Doctor en Ciencias en Ingeniería Mecánica, Profesor Investigador en el Instituto Politécnico Nacional, ESIME Zacatenco, Ciudad de México, México. WoS Researcher ID: JVZ-7493-2024

como marco para gestionar el riesgo operacional se logra la viabilidad y flexibilidad de los criterios para el correcto manejo de las amenazas futuras. El modelo proporciona un marco integral de gestión del riesgo operacional con un enfoque sistémico.

Palabras clave: Gestión de riesgos, riesgo operacional, modelo de sistema viable, cibernética, sistema.

viability and flexibility of the criteria for the correct management of future threats is achieved. The model provides a comprehensive operational risk management framework with a systemic approach.

Key words: Risk management, operational risk, viable system model, cybernetics, system.

Introducción

A lo largo de las crisis financieras, se han registrado muchas pérdidas de alto perfil en la industria financiera que se han atribuido al riesgo operacional. Entre los sucesos de pérdidas por riesgo operacional se encuentran los registrados por Société Générale y JP-Morgan Chase con pérdidas de más de $7 mil millones y $5 mil millones de dólares respectivamente, en incidentes separados de transacciones no autorizadas (Berger et al., 2022). Una característica distintiva del riesgo operacional es su potencial sobre consecuencias devastadoras que van desde grandes pérdidas monetarias y reputaciones destrozadas hasta amenazas a la estabilidad de las instituciones financieras a nivel mundial (Curry, 2012).

A través del tiempo estos eventos han modificaron la mentalidad de las instituciones financieras respecto al manejo del riesgo operacional. Las instituciones financieras tienen el objetivo de generar ganancias, el beneficio es una devolución a los propietarios del negocio por las actividades operativas que realice la institución, la cual deberá asumir el riesgo operativo como la pérdida directa o indirecta de cada uno de los procesos (Corrigan, 2013). Ante la necesidad de controles en el sistema financiero internacional se crea el Comité de Supervisión Bancaria de Basilea (BSBC), como un organismo regulador con la función de introducir metodologías para que los bancos puedan calcular del capital regulatorio del riesgo operacional (Mignola et al., 2016).

El BCBS define al riesgo operacional como pérdidas ocasionadas por procesos internos de la institución, actividades de su personal, sistemas inadecuados o fallidos y/o factores exógenos como los eventos externos (BCBS-BIS, 2006). El riesgo operacional es ocasionado por diversas actividades que se realizan dentro y fuera de la organización. El riesgo operativo es considerado como la forma de riesgo más perniciosa debido a su contribución a numerosas fallas en las instituciones financieras (Jorion, 2007).

Las instituciones financieras requieren implementar la gestión de riesgo para prevenir y minimizar la ocurrencia de eventos, debe dar atención a los procesos y funciones, para evitar violar los procedimientos (Andersen et al., 2012). La combinación de una eficaz gestión del riesgo con el estricto cumplimiento de una gobernanza corporativa son elemento clave para el éxito en las instituciones bancarias (Aebi et al., 2012), la cuantificación de las probabilidades de pérdidas y efectos secundarios permite tomar decisiones preventivas, correctivas y reductivas (Balteş & Ciuhureanu, 2010), poder anticiparse con acciones que permita facilitar el conocimiento de los factores de riesgo a la gerencia (Beals et al., 2019).

El uso del proceso de gestión de riesgos ayuda a las instituciones a tener resultados favorables como la adopción de mejores prácticas con el apoyo de las partes interesadas (Ruiz-Canela, 2021), o mejorar su capacidad de gestión para enfrentar la incertidumbre y los impactos negativos (Raz & Hillson, 2005). Prioritariamente, la gestión de riesgos operacionales es minimizar las pérdidas de la institución bancaria y preservar su capital y activos, el impacto será obtener mejores resultados de la actividad para determinar, mantener y controlar el nivel de riesgo operacional (Chauhan et al., 2019).

La gestión de riesgos operacionales con enfoque de principios cibernéticos permitirá a las instituciones financieras mejorar sistemas con la complejidad que amerita el manejo de riesgos operacionales. En el presente trabajo se diseña el Modelado de Sistema Viable VSM de una institución financiera con la finalidad de poder optimizar el manejo de sus riesgos operacionales, lo que implicó mejorar los modelos internos y a futuro permitirá reconocerlos y optimizarlos con suficiente antelación. Las consecuencias de una gestión eficaz orientarán a una reestructura orgánica, mejorará la toma de decisiones, reducirá el cargo de capital, así como el

cumplimiento de las especificaciones normativas.

Marco Teórico o Revisión de literatura

Stafford Beer fundó la cibernética de gestión, actualmente conocida como Cibernética Organizacional (CO), en la que presenta a las organizaciones como sistemas que sobreviven al medio ambiente por su característica de adaptabilidad, definiendo a la organización como sistema viable cuando es capaz de mantener su existencia independiente. El modelo fue desarrollado por Beer y plasmado en diversas publicaciones, con enfoque teórico publicó dos trabajos, *Brain of the Firm* (1972) y *Heart of Enterprise* (1979), con un enfoque metodológico desarrolló *Diagnosing the System for Organizations (1985).*

El Modelo de Sistema Viable VSM utiliza principios cibernéticos, entre los conceptos relevantes tenemos la Ley de la Variedad de Ashby (1956) o la formalización matemática del comportamiento de redes neuronales enunciado en el Modelo de Neuronas de McCulloch y Pitts (1943). En relación a la CO el trabajo de Brocklesby y Cummings (1996) reconocen en el VSM el enfoque evolutivo y mesurado de los cambios en la institución como un modelo organizacional lo cual permite a las empresas fortalecerse con las similitudes entre organización y modelo, Espinosa y Harden (2008) consideran que las organizaciones deben ser diseñadas con fundamentos cibernéticos para que sean viables en medios ambientes adversos y para Hoverstadt y Loh (2017) el VSM debe ser modelado continuamente para una variedad de diferentes contextos, incluidos contextos con propósitos dispares.

Un VSM debe presentar características de retroalimentación y variedad, que son conceptos cibernéticos de manejo de transformaciones (Beer, 1984), que permiten comprender a las organizaciones y mejorar sistemas con extrema complejidad, autorregulación y probabilismo. El mecanismo de retroalimentación negativa se puede emplear para garantizar que estén regulados para lograr los objetivos preferidos. La ingeniería de variedades ofrece un medio para asegurar el control de los sistemas probabilísticos, cuyo comportamiento no se puede predecir de antemano (Jackson, 2003).

La teoría de los sistemas sociales ofrece la perspectiva sociológica en la complejidad sobre su forma de actuar ante los desafíos del medio ambiente, Luhmann (1995) postula que "un sistema es menos complejo que su medio ambiente", debido a que una organización vista como sistema selecciona únicamente una limitada cantidad de información disponible fuera de sus límites, para que pueda existir un sistema social su razón es la reducción de la complejidad entendida como el horizonte infinito de posibilidades de acción y experiencia (Schneider, Wickert & Marti, 2016).

El modelado de sistemas viables debe considerarse una de las herramientas más poderosas en el estudio de estructuras organizacionales (Espejo, Bowling & Hoverstadt, 1999). Para modelar un sistema social se utilizan metodologías como la de Sistemas Suaves (Checkland, 1981) que hace uso de modelos de actividad humana, con la finalidad de evaluar y analizar a los entes participantes de una situación problema en el mundo, las percepciones de esa situación y la disposición para seleccionar acciones concretas que permitan adaptarse a las percepciones y juicios de un conjunto de actores. Esta metodología, lo que hace es buscar soluciones a un conflicto establecido en donde intervienen elementos sociales, políticos y humanos.

Un sistema es viable cumpliendo los requisitos que la teoría específica, para que una organización sea viable debe de disponer de cinco sistemas gerenciales con sus interrelaciones (Fig. 1):

Sistema 1 (S1), denominado *"Operación"* tiene la función de gestionar las operaciones de las actividades primarias, así como los activos, que son definidas como unidades operativas (Huygh & Haes, 2019). Las unidades operativas producen resultados, los cuales pueden ser bienes o servicios en una organización (Sadi, Wilberg, Tommelein & Lindemann, 2016).

Sistema 2 (S2), denominado *"Coordinación"* es el proceso de autorregulación para hacer frente a las oscilaciones que surgen a través de las interacciones entre o dentro de los sistemas viables integrados, esta gestión reduce el conflicto entre ellas y crea cohesión para mantener la estabilidad (Beer, 1979).

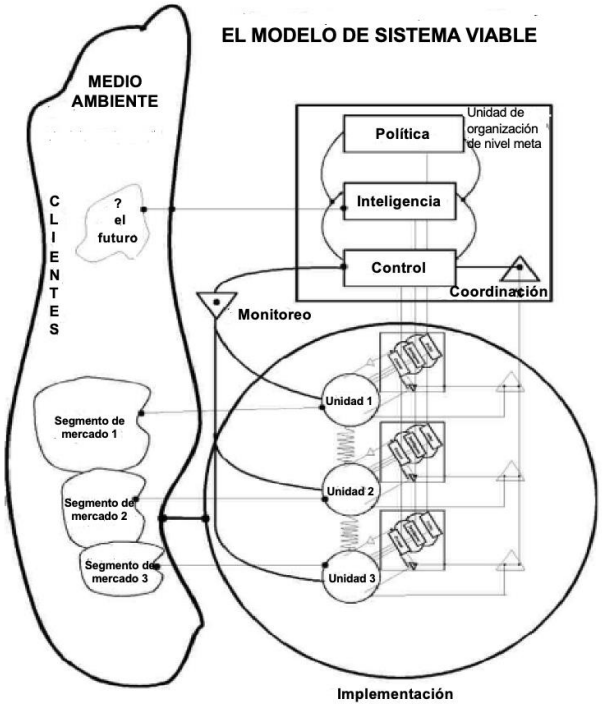


Figura 1. Modelo de Sistema Viable.
Source: Beer (1984)

Sistema 3 (S3), denominado *"Control"* gestiona los procesos (Shaw et al., 2020), controla la operación del sistema en foco (Beer, 1985). El S3 debe integrar los elementos operativos en un todo cohesivo (Jafarov & Lewis, 2014) y mantener en equilibrio la autonomía de cada uno de los sistemas viables conservando la cohesión total del sistema (Anderton, 1989).

Sistema 3* (S3*), denominado *"Auditoría"* es el canal de auditorías en el cual permite que el S3 obtenga información directamente de las unidades operativas del S1 (Beer, 1985), se complementa con la función de seguimiento y validación (Schwaninger & Scheef, 2016).

Sistema 4 (S4), denominado *"Inteligencia"* tiene la función de gestión de los posibles estados futuros del sistema (Hoverstadt, 2010). El S4 se ocupa de la vinculación entre la comunicación externa con el entorno total del sistema (Beer, 1985), recopila y analiza información del entorno para identificar desafíos y oportunidades (Huygh & Haes, 2019).

Sistema 5, Política.- Es la función de gestión de toma de decisiones. El S5 toma las decisiones finales dentro de una recursión del sistema viable, proporcionando un cierre lógico, así como decide la estrategia de la organización (Beer, 1985). Establece un equilibrio entre la orientación presente y futura de las acciones de inteligencia del S4 y el proceso de gestión del S3 (Schwaninger & Scheef, 2016).

El modelo analiza un nivel de recursión o también denominado "sistema *in focus*" de una organización y sus relaciones con los otros niveles. El principio de recursividad aborda el hecho de que "todo sistema viable contiene y está contenido en un sistema viable" (Beer, 1984). Así, el modelo cubre cualquier organización en su totalidad.

Metodología

Esta investigación se ha realizado con un enfoque sistémico presentado por Checkland y la estrategia es investigación-acción, la cual es un método de investigación cualitativo y se basa en la participación de investigadores y personal bancario. El método de investigación-acción (Checkland & Holwell, 1998) se basa en el marco FMA (donde F es un marco de ideas; M es la metodología aplicada y A es el área de interés) para guiar la planeación e implementación de investigación acción (Fig. 2).

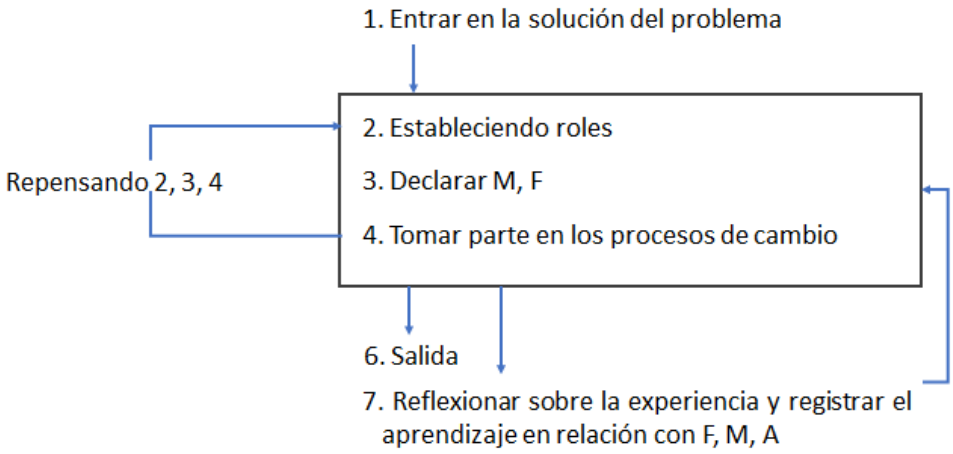


Figura 2. Proceso de investigación de acciones.
Source: Checkland & Holwell (1998)

El problema de investigación en el mundo real fue diagnosticar la estructura organizacional que permita optimizar el manejo del riesgo operacional en una institución bancaria mexicana como un área de preocupación para el sistema bancario nacional, con la finalidad de lograr la viabilidad. La investigación se realiza con un enfoque sistémico y estrategia de investigación acción (Checkland & Holwell, 1998). Uno de los autores es empleado bancario. Para guiar la planeación e implementación del proceso de investigación de acciones (Fig. 3), el equipo de investigación después de varias sesiones constituye el F (marco de ideas) y M (metodología aplicada), se inició el diagnóstico de la estructura organizacional. La investigación se realizó en la matriz de uno de los principales bancos mexicanos, dada la información y su manejo quedará sin enunciarlo debido a su protección. Los datos se recopilaron mediante examen de la experiencia pasada en riesgos en organizaciones similares y en la misma organización, opinión de expertos, entrevistas y observación personal. El modelo VSM fue desarrollado utilizando la metodología de Viplan que utilizo Espejo et al., (1999) el cual está compuesto por 1) Formación de declaración de identidad, 2) Modelado estructural, 3) Comprensión y desarrollo de la complejidad 4) Evaluación de la discrecionalidad de la gestión, 5) Puntos de diagnóstico y 6) Diseño S1-S5.

1) Formación de declaración de identidad

En el primer paso es conocer la identidad y el propósito de la institución bancaria mexicana, para ello se nombra el sistema, esto se ocupa como una herramienta para estudiar la identidad de las organizaciones, se describe la organización con un método de asignación de nombres apropiados a cada actividad del proceso de riesgo operacional en que involucra a todos los actores. La identidad y descripción de la institución bancaria se determina cuando los observadores puedan resolver los cuestionamientos que plantea el Método Viplan. En principio se determina el sistema *in focus.*

Determinar el sistema in focus: El análisis VSM se puede extender tanto hacia arriba como hacia abajo. Para determinar el sistema *in focus* se considera la estructura del sistema bancario por nivel de recursión y referente al riesgo operacional lo apropiado para su gestión en el banco mexicano (Fig. 3).

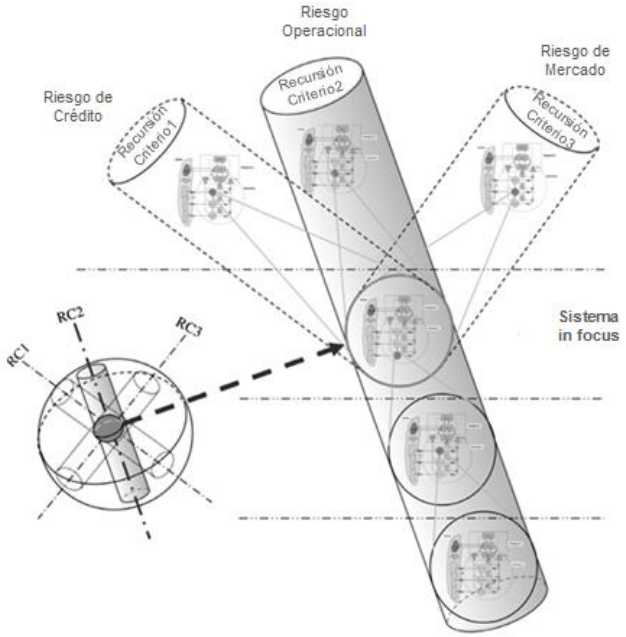


Figura 3. Sistema *in focus*, adaptado de Pérez-Ríos (2010).

Determinar la identidad con TASCOI: La estructura de la situación puede definirse en términos de nombres, Checkland (1981) establece el mnemotécnico CATWOE para las descripciones estructuradas concisas o definiciones raíz del problema o resultado deseado. Otra estructura la desarrolló Espejo (1988), Espejo et al., (1999) definiendo TASCOI, la cual será utilizada para este trabajo (Fig. 4):

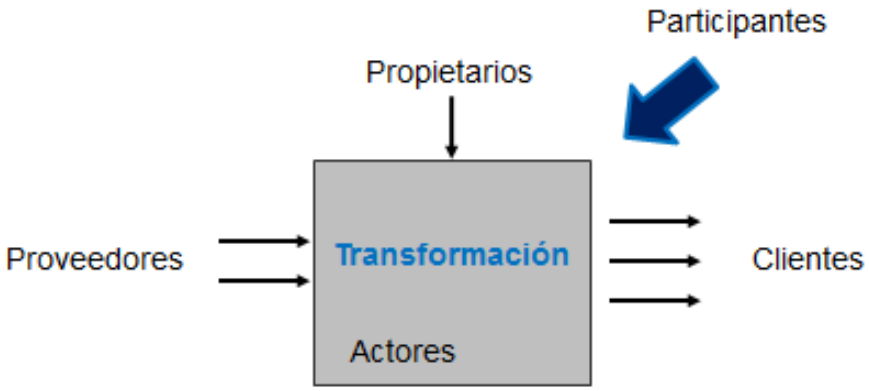


***Figura* 4.** TASCOI en términos de transformación como caja negra.
Source: Espejo (1988), Espejo et al., (1999)

Identificar la actividad principal: En este caso la actividad principal para la gestión de riesgo operacional es analizar como las instituciones bancarias realizan la gestión sin descuidar el interés de los accionistas y la operación de la institución bancaria. La gestión del riesgo operacional debe garantizar el cumplimiento de los objetivos para lo cual la institución bancaria toma riesgos para prosperar, en un ambiente tan complejo puede fallar debido a la ineficaz forma de gestionar los riesgos, por lo que debe destinar recursos para fortalecer la gestión y toma de decisiones.

Actividad de apoyo/reguladora: La actividad principal la realizan las unidades organizacionales que generan los productos o servicios y donde se presentan los riesgos en las instituciones bancarias. La actividad reguladora y de apoyo es la función de creación y regulación para que no se presente una gestión ineficaz en la administración de los riesgos operacionales.

La gestión del riesgo operacional en institución bancaria mexicana queda estructurada con TASCOI de la siguiente manera (Fig. 5).

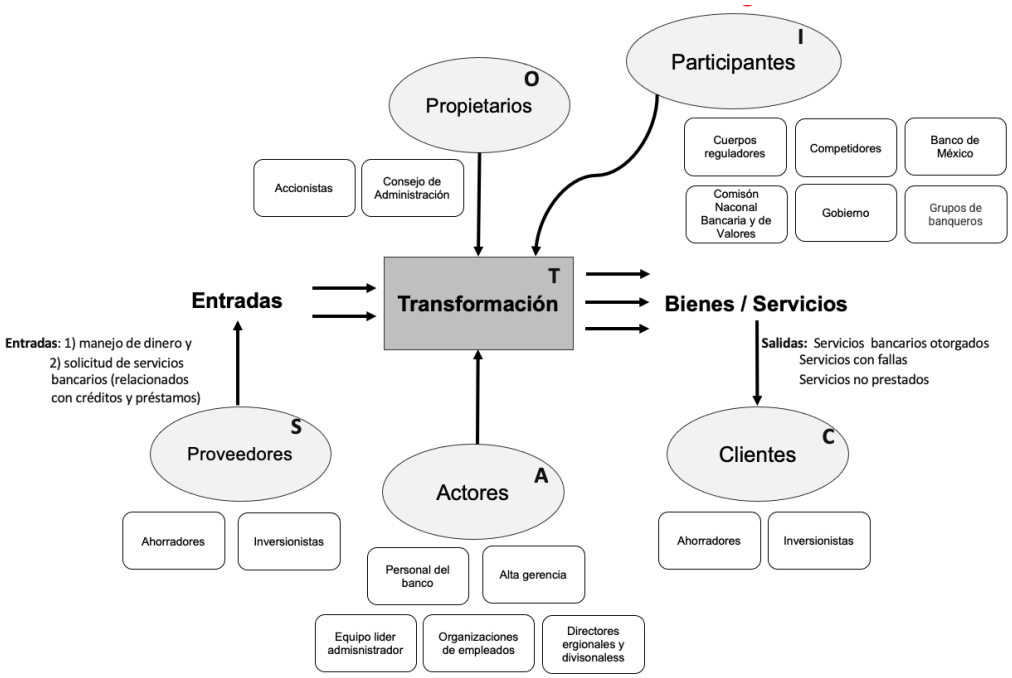
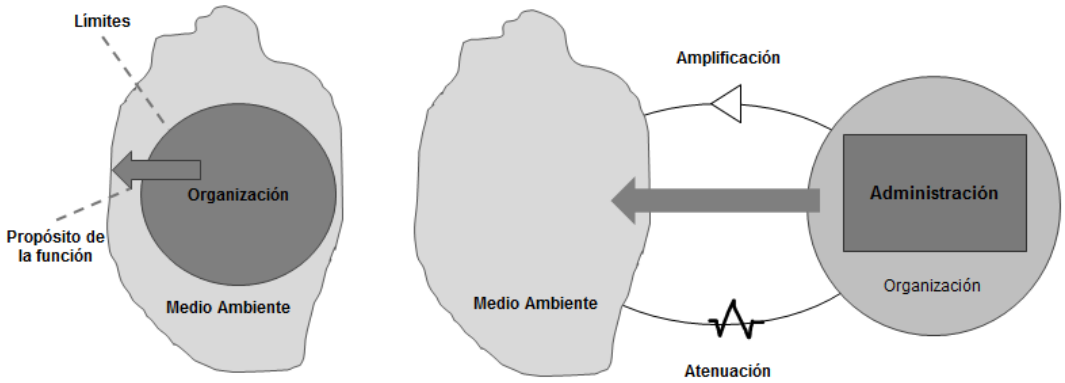


Figura 5. Determinando TASCOI para la gestión de riesgos operacionales.

2) Modelado estructural

El segundo paso del método Viplan es el modelado estructural (Fig. 6). En este paso se identifica el entorno de la institución bancaria. Dos aspectos a considerar son, conocer el entorno actual y el entorno a futuro, para ello es necesario conocer los cambios demográficos, tecnológicos, sociales y de comportamiento, la inestabilidad global, el auge y la interconectividad de los mercados emergentes, el auge del capitalismo dirigido por el estado y la guerra por los recursos naturales.



Nota: Interacción de la organización, con su administración y el medio ambiente.
Figura 6. La organización y su medio ambiente, Pérez-Ríos (2010).

Las instituciones deben identificar los límites y el medio ambiente en el presente y futuro en el que opera la institución bancaria, se han definido las presiones fiscales y el malestar político social, definiendo los elementos necesarios para estudiar la institución bancaria y evaluar su capacidad de cumplimiento de propósitos.

La evaluación de la capacidad de cumplimiento de propósitos utiliza dos dimensiones, la primera es la vertical se refiere a la variedad (complejidad) del entorno global que enfrenta la institución bancaria, identificando subambientes dentro del medio ambiente total, en su caso podría identificarse a su vez subambientes, y así sucesivamente. Al proceso se le conoce como "desdoblamiento de la complejidad" y permitirá potenciar la capacidad de la institución para absorber la complejidad. La segunda dimensión es la horizontal que define los diferentes niveles en el que está involucrada la institución respecto a su medio ambiente (Espejo & Harnden, 1989).

La selección de un nivel de estudio en particular se denominará "organización *in focus",* será el nivel de la organización donde a detalle se analice su entorno, la gestión y relaciones entre ellos.

3) Comprensión y desarrollo de la complejidad

El uso del VSM como herramienta de diagnóstico permite conocer parte de una intervención de la banca nacional bajo los conceptos de Beer. La estructura básica del VSM en la banca nacional (Fig. 7), muestra al sistema bancario respecto a la gestión de riesgos, las operaciones bancarias están definidas por criterios y niveles de recursividad. La gestión de riesgos debe ser manejada sistémicamente, los riesgos son clasificados en riesgo operacional, de crédito y de mercado y gestionados en diferentes niveles. Cada nivel representa un sistema viable para la gestión del riesgo operacional, en el nivel 0 se estable a nivel nacional la gestión del Banco Central, el nivel 1 corresponde la gestión a los bancos mexicanos por firma, el nivel 2 se estable al banco por región geográfica, y el nivel de recursión 3 corresponde a la sucursal.

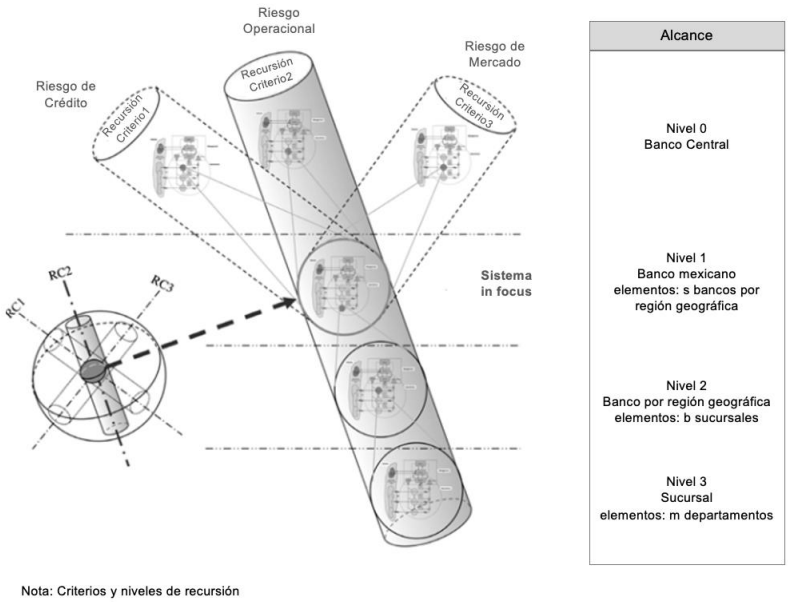


Figura 7. Sistema *in focus,* criterios y niveles de recursión, adaptado de Pérez-Ríos (2010).

4) Evaluación de la discrecionalidad.

El sistema viable presenta recursión descendiendo al siguiente nivel (Fig. 8), encontramos el Sistema *in focus* para la gestión de riesgos operacionales, compuesto por las unidades productivas establecidas por las fuentes que producen el riesgo operacional ocasionados por personas, procesos, sistemas y factores externos, cada uno de ellos serán atendidos por programas, debe observarse que su organización de sistemas viables no corresponde a una descomposición jerárquica, sino a sistemas dentro de sistemas.

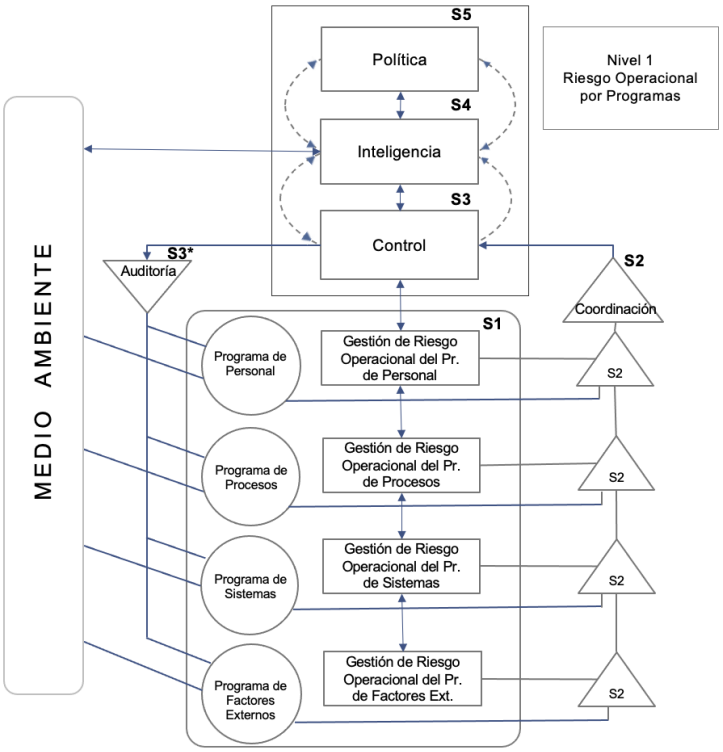


Figura 8. Gestión de riesgo operacional en la institución bancaria, nivel de recurrencia 1 *(in focus)*.

Existen niveles de recursividad, para cada uno de los programas, en el que cada institución bancaría definirá la gestión del riesgo operacional, para intégralos a cada programa y permitir gestionar de manera sistémica al riesgo operacional, y así sucesivamente definiendo los niveles de recursividad que se diseñe en el modelo.

Uno de los factores que se deben considerar es la discrecionalidad en la gestión de las evaluaciones, la cual consisten en identificar los elementos de la estructura en cada nivel de recursión, se determina los recursos discrecionales y las funciones relacionadas con la actividad principal de la institución bancaria.

5) Puntos de diagnóstico

Este paso es necesario aclarar la gestión del riesgo operacional para evaluar la alineación de la estrategia empresarial con el valor empresarial de la gestión. La implementación de un sistema de información en las instituciones financieras debe evaluarse de conformidad con los objetivos de la institución bancaria. Cada sistema de información debe alinearse con la estrategia de la institución, como ejemplo en el banco para lograr los objetivos del riesgo operacional contrato un equipo externo para mejorar un programa de riesgo tecnológico para cumplir con las expectativas regulatorias del BCBS, los recursos temporales en un objetivo específico, permitió liberar recursos al grupo de expertos técnicos y centrarse en crear mejoras. El resultado en este paso garantiza que la inversión de capital en los programas de riesgo tecnológico este alineada con los objetivos de la institución bancaria.

6) Diseño S1-S5

En este paso se realiza el diagnóstico y diseño de mecanismos estructurales, se elabora un VSM para la institución bancaria mexicana como paso final del método Viplan.

Sistema 1 (S1): Operaciones relacionadas con la identificación del riesgo operacional.

Las unidades operativas (UO) de gestión del riesgo operacional tienen la responsabilidad de ejecutar funciones de control y provisión de bienes y servicios bancarios. La identificación de los procesos clave y tipos de riesgo operacional surgen de los procesos de definición y categorización, a) el primero se ubican los riesgos, revisando y listando las exposiciones a pérdidas, se define el enfoque para la estimación de pérdidas operativas y calidad y uso de los datos y posteriormente b) el segundo tiene por objetivo revisar y listar todas las exposiciones a pérdidas, para lo cual se utilizan diversos métodos como cuestionarios, listas de verificación o estados financieros.

La atención de todos los referentes a las operaciones inadecuadas o fallidas de servicios bancarios son atendidas por el Comité Operativo del Riesgo Operacional. El comité se forma para la dirección de la actividad de cada programa por riesgo operacional, en el que deben conocer el perfil del riesgo operacional relacionado con a) personal, b) sistemas y tecnología de la información, c) procesos, y d) eventos naturales. La estructura se presenta con los expertos relacionados con cada riesgo operacional y los jefes divisionales del dominio del riesgo operacional.

La Figura 9 muestra cómo se define el S1 para identificar el riesgo operacional para que las instituciones bancarias definan y categoricen el riesgo para priorizarlo, se integra el sistema de planeación para que de manera holística, los subsistemas S1.1, S1.2, S1.3 y S1.4 se comuniquen entre sí, permitiendo planear los riesgos inherentes y residuales, definiendo el uso de técnicas tanto cualitativas como cuantitativas dichos riesgos se pueden clasificar siguiendo dos dimensiones; probabilidad de ocurrencia y gravedad de la pérdida. Los reguladores han determinado la identificación de riesgos como un tema principal, donde el establecimiento y la implementación de un proceso integral de identificación le permite a la institución y sus niveles de recursividad poder capturar y medir los riesgos.

Las unidades operativas deben detectar el grado de amenaza para alertar a los directivos a través de un canal algedónico.

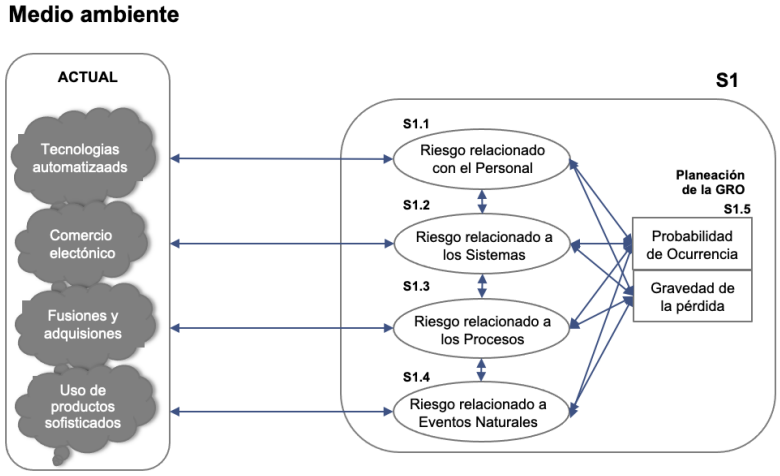


Figura 9. S1 Operaciones relacionadas con la identificación del riesgo operacional.

La identificación de riesgos operacionales es necesaria para conocer la exposición e identificar oportunidades para crear valor en los procesos. Las instituciones también deben priorizar los riesgos operacionales evaluando los modelos de gestión de riesgo y determinado el nivel de precisión, confiabilidad y transparencia requerido para los casos de uso relacionados. Un modelo que se usa para sugerir una decisión de bajo impacto tendrá un perfil de riesgo más bajo que un modelo que se requiere para tomar decisiones más especializadas.

Sistema 2 (S2): Coordinación de la gestión de riesgo de las operaciones del S1.

El S2 proporciona a las unidades operativas la coordinación para que pueda llevarse la implementación y monitoreo de las actividades realizadas en el S1, la coordinación de estas actividades permite al sistema la búsqueda de la máxima autonomía otorgada sujeta únicamente a que el todo continúa existiendo. El S2 es responsable de la declaración de gestión de riesgos definiendo objetivos y políticas de la organización, permite que los ejecutivos operativos tengan conocimiento del impacto de los RO y otorga la autoridad necesaria al gestor de riesgos. La coordinación rigurosa entre unidades operativas es vital para asegurar la cobertura global de la organización.

La finalidad del S2 es mantener la coordinación de la gestión del riesgo operacional entre cada subsistema 1, debe proporcionar estándares, políticas, procedimientos e instrucciones de trabajo de riesgos operacionales para el S1, referente a la atención de los requerimientos de los reguladores, el S2 proporciona políticas e instrucciones sobre estándares internacionales de riesgo operacional.

El S2 establece un proceso sistemático para evaluar el riesgo operacional, estableciendo procedimientos e instrucciones de riesgo operacional con definición de roles, obligaciones y responsabilidades respecto a las aplicaciones, capacitar a los empleados para mejorar el conocimiento respecto a los riesgos operacionales.

El S2 realiza actividades relacionadas con informar el estado el riesgo operacional a determinados periodos, de conformidad con los estándares o marcos. De la misma manera documentar los riesgos que se materializaron a causa de la aplicación de legislaciones extranjeras.

Las funciones del S2 son la de gestionar la coordinación de las actividades del S1, autorregular las oscilaciones entre o dentro de los sistemas viables, reducir el conflicto, crear cohesión para mantener la estabilidad y garantiza la comunicación entre el S1 y S3. El S2 es el responsable de autorregular las interacciones dentro de los sistemas viables integrados del S1, lo cual establece una compresión compartida de los riesgos operacionales (Fig. 10).

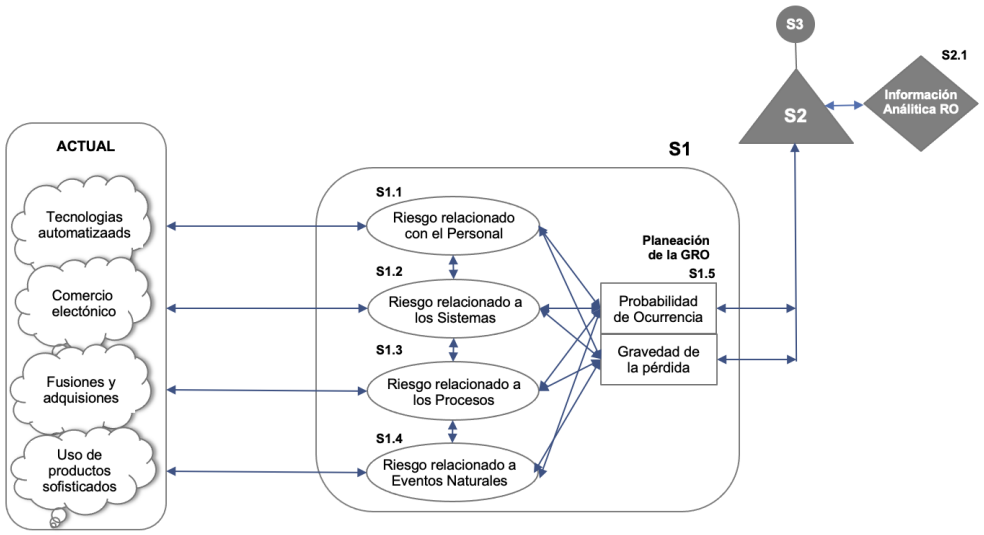


Figura 10. Coordinación de la gestión de riesgo de las operaciones del S1.

Sistema 3 (S3): Control de la gestión de riesgos operacionales.

El control de la gestión del riesgo operacional (S3) es responsable de regular las operaciones internas de institución bancaria respecto de la gestión de los riesgos operacionales, en este sistema se debe administrar, controlar y reportar el riesgo operacional, contribuyendo al diseño de programas y proyectos que mejoren el estado de los riesgos operacionales, lo cual deberá ser autorizado por los S4 y S5.

El S3 controla la operación del sistema S1, las gestiones que realiza es el análisis de la efectividad de las soluciones con el propósito de mantener controlado el perfil del riesgo, por lo que establece mecanismo que permitan realizar el análisis de riesgos. En primera instancia sí de manera anticipada el riesgo no se ha consumado se debe gestionar estrategias de control, las cuales permiten reducir la frecuencia o la gravedad de una pérdida definiendo la técnica para prevenir, reducir e impedir la pérdida, en segunda instancia sí se ha consumado la ocurrencia del evento se utiliza estrategias de financiación de pérdidas, entre ellas se utilizan la retención y transferencia de riesgo. El uso de estas estrategias garantiza la asignación de recursos y fomenta la cohesión, esta sinergia entre operaciones maximiza los resultados.

El control de gestión de riesgos operacionales es supervisado por el Comité de Auditoría y Control para la gestión de riesgos operacionales, conformado por el director de riesgos operacionales, el gerente de riesgos operacionales y el auditor líder de riesgos operacionales. Las funciones del comité es la comunicación y difusión que genera el S3, se realiza el informe interno sobre riesgos operacionales que contenga insumos financieros, operativos y de cumplimiento, así como datos externos relevantes que contenga información sobre eventos y condiciones. De la misma manera se elaboran los informes de riesgos que

contengan las descripciones cualitativas de las tendencias y desafíos respecto a los riesgos operacionales.

El Sistema de Auditoría (S3*) desempeña las funciones de obtener información del S3-S1, proporcionar información con alta precisión, complementar con seguimiento y validación y finalmente auditar el riesgo operacional en las unidades operativas, por lo que se considera vital la creación del Subsistema Axiológico S1.7 que permita el desempeño organizacional apegado a sus principios y valores (Fig. 11).

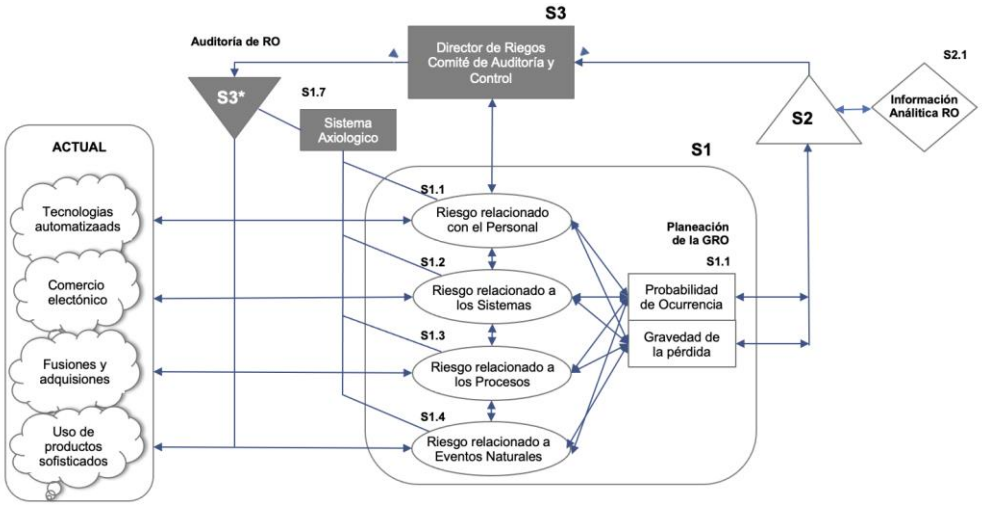


Figura 11. Control S3 y Auditoría S3* de la gestión de riesgos operacionales.

Sistema 4 (S4): Gestión del entorno de los riesgos operacionales.

El compromiso del S4 es la comunicación externa de los riesgos operacionales con el entono del sistema, se ocupa de las actividades externas y de mediano y largo plazo del sistema, monitoreando lo que está sucediendo, detecta las oportunidades y amenazas en el entorno del sistema. La responsabilidad es rastrear el riesgo relacionado con el futuro entorno de los riesgos operacionales y tener la capacidad de predecir, analizar y simular los cambios, lo que permitirá a las instituciones bancarias tomar decisiones que aumenten la probabilidad de lograr objetivos futuros, así como de reconfigurar los objetivos estratégicos de riesgos operacionales.

Este sistema ofrece posibles recomendaciones para acciones futuras respecto a los cambios que están aconteciendo en el entorno de la institución bancaria, con la finalidad de mantener un estado constante de preparación para el cambio y asegurar su adaptación.

Se crea el Comité de Riesgos el cual juntamente con la Alta Dirección gestionan las funciones del S4, entre las actividades que desarrolla están las de recopilar y analizar información para identificar desafíos y oportunidades, administrar afuera con visión a futuro, gestionar estados futuros para que la organización se adapte a los cambios del entorno externo y establecer canales de comunicación externa (Fig. 12).

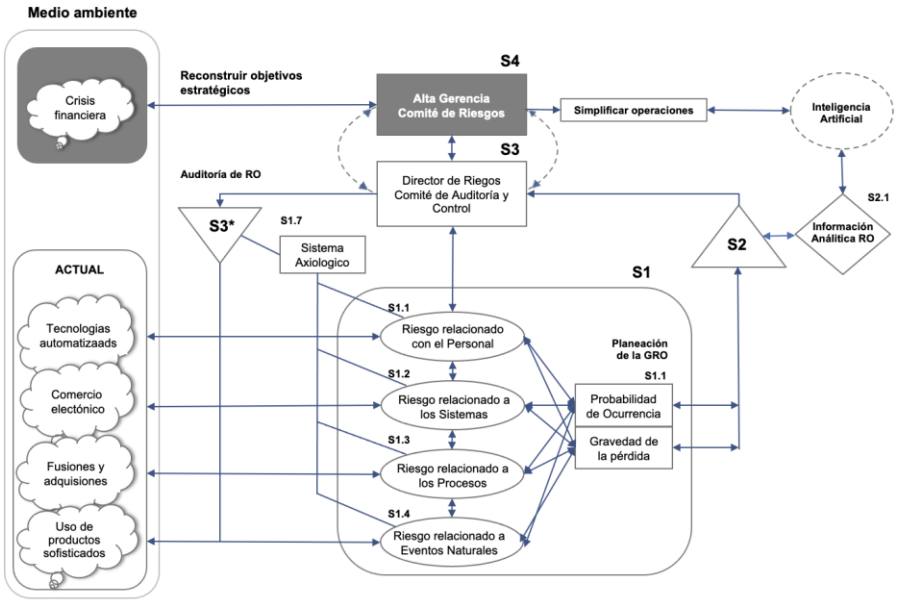


Figura 12. Gestión del entorno interno del riesgo operacional.

Sistema 5 (S5): Gestión del entorno externo del riesgo operacional.

El S5 actúa como árbitro en los S3 (entorno interno) y S4 (entorno externo) equilibrando las necesidades para tomar la decisión de cual rumbo se promulgará. Este sistema define la misión, visión, valores, y objetivos sobre los riesgos operacionales, asegurando que la institución bancaria tenga la capacidad de adaptabilidad con un grado aceptable de estabilidad interna, asegurándose que el riesgo operacional no supere el apetito de riesgo de la institución. El sistema tiene entre sus funciones la de generar políticas generales para la definición de la gestión de riesgos operacionales; establecer una visión del riesgo; gestionar proactivamente el riesgo, las regulaciones y el capital.

Se crea el Comité Ejecutivo el cual gestiona junto con el Consejo de Administración las funciones del S5, definen la estrategia de la organización, toman decisiones, crean y mantienen la identidad del sistema, establecen la dirección general, valores y propósitos y soluciona conflictos entre S3 y S4 (Fig. 13).

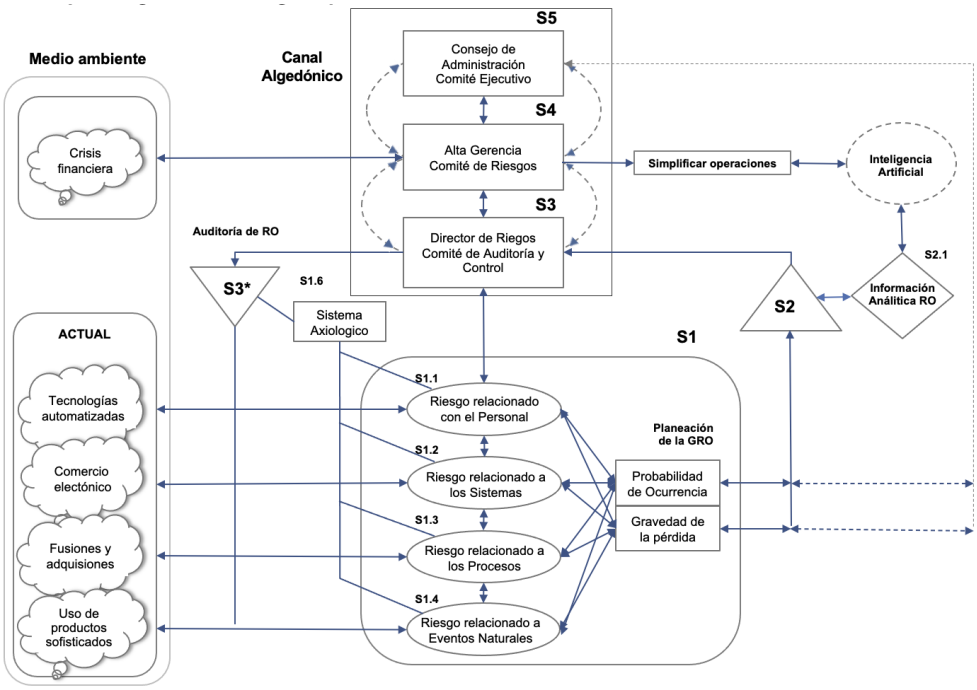


Figura 13. Modelo del Sistema Viable para la Gestión del Riesgo Operacional.

Resultados y discusión

Las instituciones bancarias deben adoptar respuestas en la institución completa y en todos los niveles dado que el riesgo operacional se presenta de una variedad de fuentes.

El Sistema 1 es responsable de la producción y entrega de los bienes o servicios de la institución bancaria al entorno pertinente, que permite al S1 gestionar el riesgo operacional ocasionado por el uso creciente de tecnologías automatizadas, el crecimiento del comercio electrónico, las fusiones y adquisiciones, y el uso de productos sofisticados que pueden conducir a errores del sistema, robo interno y externo, problemas de seguridad, entre otros. El S1 está compuesto por unidades organizativas operativas, cada uno de estos sistemas viables son responsables de las actividades o productos. Las principales actividades que una institución bancaria desarrolla respecto a la gestión de riesgo operacional es identificar los eventos que causan pérdidas, los cuales son ocasionadas por las personas S1.1, sistemas S1.2, procesos S1.3 y eventos naturales S1.4, cada uno de los cuatro componentes del S1 tienen su gestión y operación que pueden filtrar información al nivel superior, aminorando la heterogeneidad mediante un canal algedónico.

Subsistema de Planeación (S1.5), es claro, que su funcionamiento se requiere dado que la gestión del riesgo operacional es llevada por una dirección dentro de la estructura del banco central a cada una de las regiones geográficas y sus sucursales, por lo que los resultados que se produzcan requieren de la planeación de casos imprevistos, la identificación de las fuentes de los riesgos por errores y abusos internos; violaciones externas; problemas en el funcionamiento de las relaciones con los clientes, inadecuada comercialización de productos y los procedimientos comerciales; e implementación de procesos y decisiones comerciales permitirá al sistema de planeación identificar los eventos por probabilidad de ocurrencia y gravedad de pérdida y en consecuencia definir la forma de actuar ante estos.

El Sistema 2 coordina la implementación y el monitoreo para que funcionen armónicamente las unidades operativas del S1. Existe una interface en donde se conecta con el Subsistema de Planeación S1.5 como responsable de administrar la información, procesos y suministros, evitando generar conflictos para alcanzar los objetivos, lo que le permite fortalecer al S2 para que coordine los equipos, defina las bases de conocimiento, la programación de tareas, establezca las normas operativas destinadas a proporcionar estándares de comportamiento, sistematice las actividades, establezca el uso de instructivos o lineamientos, incorpore sistemas de calidad, la coordinación de estas actividades mejoraran las capacidades de gestión, reduciendo la materialización de los riesgos operacionales.

El Subsistema S2.1 referido a la Información Analítica del sistema es el área que se incorpora con la finalidad de que la institución bancaria maneje su información para poder modelar la exposición al riesgo operacional es la encargada de desarrollar la documentación adecuada, mejorar la calidad de los datos, conocer las tendencias de mercado, realizar el análisis de la forma funcional del algoritmo y parámetros que permita medir la exposición al riesgo y entender posibles problemas.

El Sistema 3 es el responsable de administrar las unidades operativas del S1, tiene la función de integrar al grupo para que funcione armónicamente y explorar las sinergias de las interacciones entre las unidades operativas del S1. El S3·da seguimiento diario a las operaciones de la institución bancaria, en el área central el director de riesgos administra el área para determinar los niveles aceptables de riesgo y determinar la exposición, a nivel de recursividad de las sucursales, coordina las actividades para que las ejecuten de conformidad con las políticas, establece de manera periódica una evaluación de control y riesgos, desarrolla planes de acción para monitorear el nivel de tolerancia. Las instituciones bancarias deben manejar un entorno de control sólido fortaleciendo su capacidad de monitoreo de controles e identificando las estrategias apropiadas de mitigación o transferencia de riesgos, las decisiones deben ser resueltas por el Consejo de Administración.

Sistema 3* es un sistema de apoyo al S3, su función es auditar el funcionamiento del S1, obtiene información que contiene registros históricos de los riesgos identificados y sus calificaciones, esta información es proporcionada por los departamentos de gestión legal, departamento de seguridad y gestión de riesgos, así como del sistema de información analítica que continente información de alta prioridad contra lavado de dinero o de inspecciones. La finalidad es poder registrar de manera adecuada el seguimiento de la auditoría para identificar los eventos de pérdidas.

En el banco se opera el Comité de Auditoría y Control cuya misión es revisar la efectividad de la gestión de Control Interno, informando al Consejo de Administración sobre el desempeño de los responsables de las funciones con riesgos clave, el estado del marco de control interno, informar de la ausencia de materialización de pérdidas, contingencias o incertidumbre ocasionadas por una gestión deficiente de controles internos, así como informes de Auditoría Interna y Externa e informes Regulatorios.

Sistemas de interrelaciones entre los sistemas tenemos el canal vertical entre Sistemas de relación (1-3), negociación de metas y recursos: rendición de cuentas, gestión por objetivos, control de presupuesto, gestión por excepción, intervención únicamente si la cohesión de toda la organización es amenazada)

Subsistema 3.1 definido como Subsistema Axiológico S3.1 cumple la función de otorgar valor axiológico a cada una de las Unidades Operativas de S1 y sus respectivas auditorías practicadas por el S3*, debe vigilar que se lleven las auditorías bajo parámetros éticos otorgando que los resultados se hallan evaluado con efectividad bajo controles clave que mitiguen los riesgos. El canal algedónico permite que la iniciativa del Consejo de Administración e implementada por el Comité Ejecutivo enfoca el sistema axiológico como parámetro de control a la gestión de riesgos operacionales permite que el banco tenga una cultura guiada por estándares sobre el comportamiento profesional y responsable.

El Sistema 4 es el responsable del futuro de la institución bancaria y su medio ambiente, a nivel central la estructura orgánica debe tener departamentos que sean responsables del futuro de la organización, cada uno de ellos deben formar un grupo de trabajo que permita determinar los planes estratégicos. Estos departamentos junto con el director general diseñan los planes estratégicos para adaptarse al futuro, la autorización es dada por el Comité de Riesgos el cual monitorea el estado de los riesgos de alta prioridad y emergentes, establece planes estratégicos que permita gestionar acciones de mitigación, además ante una solicitud de la administración se encarga de realizar el reporte cuando surgen perdidas inesperadas o incidentes que identifican deficiencias en el marco de control o incumplimiento de políticas. La Inteligencia Artificial es introducida como herramienta en la construcción del entorno, le dará al S4 fortaleza al poder reconocer patrones complejos sobre el ambiente y predicciones para mantener la estabilidad en turbulencias.

El Sistema 5 representa la máxima autoridad en la organización tomando decisiones estratégicas sobre la definición de la gestión de riesgos y gobernabilidad, tiene la misión de considerar los factores internos y externos que garanticen el equilibrio entre el presente y futuro de la institución bancaria y es el único subsistema que tiene la capacidad de regular las interacciones entre el S3 y S4. El S5 establece la identidad de la institución bancaria define la gestión del riesgo operacional y rechaza lo que no es válido. El uso del VSM para el sistema bancario es recursivo, en el nivel central el Consejo de Administración es la estructura de gobierno de máxima autoridad. El Comité Ejecutivo le informa al Consejo de Administración lo que se aprueba y revisa continuamente, permitiendo tomar las decisiones finales sobre su estrategia en equilibrio entre el presente de las decisiones de gestión y el futuro de las acciones de inteligencia en todos los niveles de la institución, productos, procesos y sistemas importantes.

Conclusiones

El sistema financiero opera generando ganancias analizando los riesgos potenciales en cualquier nivel del sistema, institución bancaria, sucursal, departamentos, etc. Para evitar que se materialice el riesgo operacional los bancos requieren un marco para lograr los mejores resultados. Para encontrar un desempeño estable los bancos deben observar el funcionamiento operativo el cual resulta muy complejo teniendo en cuenta que surge de la imperfección de los procesos y sistemas, de acciones incorrectas de las personas o de imprevistos ocasionados por eventos externos.

El riesgo operacional está establecido por la especificidad presente y dinámica en cada actividad, el éxito de la gestión se debe a la definición y precisión de los roles y responsabilidades de los interesados y de una estructura organizativa adecuada. El riesgo operacional es el resultado de un mal funcionamiento del sistema por lo que el uso del Modelo de Sistema Viable VSM en cualquier nivel de recursividad de la institución bancaria le permita gestionar el riesgo operacional con un diagnóstico y diseño de estructuras organizativas para funcionar con mayor eficiencia.

El modelo presenta cómo las instituciones bancarias son viables en cinco subsistemas gerenciales y sus interrelaciones, cuya capacidad

de gestión permite la simplificación o modificación de productos, operaciones y estructura organizacional. La transformación mejora los servicios y procesos, reduce los costos estructurales y los niveles del riesgo operacional.

Referentes Bibliográficas

Aebi, V., Sabato, G., & Schmid, M. M. (2012). Risk management, corporate governance, and bank performance in the financial crisis. *Journal of Banking & Finance*, 3636(12), 3213-3226

Andersen, L.B., Häger, D., Maberg, S., Næss, M.B., & Tungland, M. (2012). The financial crisis in an operational risk management context - A review of causes and influencing factors. *Reliability Engineering & System Safety*, 105, 3-12

Anderton, R. (1989). The need for formal development of the VSM. In Espejo, R. & Harnden, R. (eds.). *The Viable System Model: Interpretations and Applications of Stafford Beer's VSM*. Chichester: John Wiley. ISBN-10: 0471922889

Ashby, W. R. (1956). *An introduction to cybernetics*. London: Chapman & Hall

Balteş, N., & Ciuhureanu, A.T. (2010). Study on The Risk Management In Banking Institutions. *Studies in Business and Economics*, 5(3), 67-78

BCBS-BIS (2006). *International convergence of capital measurement and capital standards - A revised framework comprehensive version*. http://www.bis.org

Beals, S., Fox, C., & Minsky, S. (2015). *Why a Mature ERM Effort is Worth the Investment*. Risk Management and Insurance Society (RIMS) Executive Report. Disponible en: https://acortar.link/kk4yVi (consultado en enero de 2019)

Beer, S. (1972). *Brain of the Firm: A Development in Management Cybernetics*. New York: Herder and Herder

Beer, S. (1979). *The Heart of Enterprise*. Chichester: John Wiley

Beer, S. (1984). The Viable System Model: Its Provenance, Development, Methodology and Pathology. *The Journal of the Operational Research Society*, 35(1), 7-25

Beer, S. (1985). *Diagnosing the system for organizations*. Chichester: John Wiley

Berger, A.N., Curti, F., Mihov, A., & Sedunov, J. (2022). Operational Risk is More Systemic than You Think: Evidence from U.S. Bank Holding Companies. *Journal of Banking & Finance*, 143, 106619

Brocklesby, J., & Cummings, S. (1996). Designing a viable organization structure. *Range Planning*, 29(1), 49-57

Chauhan, V., Yadav, R., & Choudhary, V. (2019). Analyzing the impact of consumer innovative-ness and perceived risk in internet banking adoption: A study of Indian consumers. *International Journal of Bank Marketing*, 37(1), 323-39

Checkland, P. (1981). *Systems Thinking, Systems Practice*. Chichester, Wiley

Checkland, P., & Holwell, S. (1998). Action research: its nature and validity. *Syst Pract Action Res*, 11(1), 9-21. https://doi.org/10.1023/A:1022908820784

Corrigan, J., Luraschi, P., & Cantle, N. (2013). *Operational risk modelling framework*. New York (USA): Milliman. Recuperado de: https://acortar.link/sUODsx

Curry, T.J. (2012). Comptroller of the Currency. [*File PDF*]. Recuperado de: https://acortar.link/fe1kku

Espejo, R. (1988). "Seeing Complexity" - the cybernetic viewpoint. *Transactions of the Institute of Measurement & Control*, 10(3), 139-144

Espejo, R., & Harnden, R. (Eds.) (1989). *The Viable System Model: Interpretations and applications of Stafford Beer's VSM*. Chichester: John Wiley. ISBN-10: 0471922889

Espejo, R., Bowling, D., & Hoverstadt, P. (1999). The viable system model and the Viplan software. *Kybernetes*, 28(6/7), 661-678

Espinosa, A., & Harden, R. (2008). A complexity approach to sustainability – Stafford Beer revisited. *European Journal of Operational Research*, 187(2), 636-651

Hoverstadt, P. (2010). The Viable System Model. In: Reynolds, M., Holwell, S. (eds) *Systems Approaches to Managing Change: A Practical Guide*. Springer, London. https://doi.org/10.1007/978-1-84882-809-4_3

Hoverstadt, P., & Loh, L. (2017). *Patterns of strategy*. Abingdon: Routledge

Huygh, T., & Haes, S. (2019). Investigating IT Governance through the Viable System Model. *Information Systems Management*, *36*(2), 168-192

Jackson, M.C. (2003). Systems Thinking: Creative Holism for Managers. Chichester: John Wiley. https://acortar.link/oZA5pP

Jafarov, N., & Lewis, E. (2014). Mapping the Cybernetic Principles of Viable System Model to Enterprise Service Bus. *Information Technology in Industry*, 2(3).

Jorion, P. (2007). *Value at Risk: The New Benchmark for Managing Financial Risk*. New York: McGraw-Hill.

https://acortar.link/NW6VeQ

Luhmann, N. (1995). *Poder*. Barcelona: Anthropos-Universidad Iberoamericana

McCulloch, W.S., & Pitts, W. (1943). A logical calculus of the ideas immanent in nervous activity. *Bull Math Biol*, 5, 115-130

Mignola, G., Ugoccioni, R., & Cope, E. (2016). Comments on the Basel Committee on Banking Supervision Proposal for a New Standardized Approach for Operational Risk. *Journal of Operational Risk*, 11(3).

Pérez-Ríos, J (2010). Models of organizational cybernetics for diagnosis and design. *Kybernetes*, 39(9/10), 1529-1550

Raz, T., & Hillson, D. (2005). A Comparative Review of Risk Management Standards. *Risk Management*, 7(4), 53-66

Ruiz-Canela, J. (2021). How Can Enterprise Risk Management Help in Evaluating the Operational Risks for a Telecommunications Company? *Journal of Risk and Financial Management*, 14, 139

Sadi, T., Wilberg, J., Tommelein, I.D., & Lindemann, U. (8, 2016). Supporting the design of competitive organizations by a domain-specific application framework for the viable system model. *In DSM 2016: Sustainability in modern project management-Proceedings of the 18th International DSM Conference, São Paulo, August 29th and 30th, 2016* (pp. 077-087)

Schneider, A., Wickert, C., & Marti, E. (2016). Reducing Complexity by Creating Complexity: A systems theory perspective on how organizations respond to their environments. *Journal of Management Studies*, 54(2), 182-208

Schwaninger, M., & Scheef, C. (2016). A test of the viable system model: theoretical claim vs empirical evidence. *Cybernetics and Systems*, 47(7), 544-569

Shaw, D., Fattoum, A., Moreno, J., & Bealt, J. (2020). A structured methodology to peer review disaster risk reduction activities: The Viable System Review. *International Journal of Disaster Risk Reduction*, 46, 101486