

Modelo Multiagente para la prevención de riesgo operativo de tipo fraude interno en IFDs

Carmen Rosa Mollinedo Laura
Postgrado en Informática
Universidad Mayor de San Andrés
La Paz - Bolivia
carmenrosamollinedo@gmail.com

Resumen—La gestión de riesgo operativo es un proceso complejo en toda organización. Particularmente, el tratamiento de eventos de fraude interno (evento de riesgo operativo) en Instituciones Financieras de Desarrollo (IFD), es una actividad que repercute en la necesidad de plantear soluciones cada vez más innovadoras, que permitan aplicar el conocimiento de expertos y aplicar soluciones que respondan a normativas y recomendaciones nacionales (Ley de Servicios Financieros) e internacionales (Basilea). En el presente artículo se plantea un modelo, como base referencial, que permita a profesionales en ciencias de la computación la incorporación de Sistemas Multiagente en el desarrollo de sistemas de gestión de riesgo operativo de tipo fraude interno. Las IFD principales en nuestro medio son: Promujer, Crecer y Diaconía. La investigación se realizó con datos de las publicaciones de Finrural y la ASFI, acerca de las IFD mencionadas y los resultados se validaron mediante encuestas a personal con experiencia en Sistemas, Riesgos y Operaciones en IFD.

Palabras clave—riesgo operativo, fraude interno, normativa, modelo, sistema multiagente

I. INTRODUCCIÓN

Las Instituciones Financieras de Desarrollo o IFD, son entidades de intermediación financiera no bancaria incorporadas al ámbito de la Ley de Bancos y Entidades Financieras mediante la Resolución de la Superintendencia de Bancos y Entidades Financieras N° SB 034/2008 y que están organizadas como Asociaciones o fundaciones civiles sin fines de lucro [1]. Las IFD, se caracterizan por trabajar en el área urbana, periurbana y rural, y operan con tecnologías financieras acordes a las condiciones económicas de los usuarios. La ASFI, gestiona la central de información de riesgo operativo (CIRO).

La Gestión de Riesgo Operativo (GRO) es el proceso estructurado, consistente y continuo para identificar, medir, monitorear, controlar, mitigar y divulgar el riesgo operativo al cual la entidad supervisada se encuentra expuesta [2]. Cuando un procedimiento no es desarrollado como fue definido, o el personal actúa de forma intencionada, para apropiarse de bienes de la institución financiera, se denomina fraude interno.

Los eventos de fraude interno (FI) han mostrado en los últimos años la fragilidad del sistema financiero [3] y la necesidad de incorporar soluciones cada vez más innovadoras. Los eventos de fraude interno, generalmente se detectan de forma reactiva y posterior al hecho. Las auditorías constituirían una aproximación más proactiva, como medio de análisis para

disminuir el tiempo entre el inicio del evento riesgoso y su detección, para poner medidas más o menos inmediatas [4].

La prevención de eventos de fraude interno (FI) requieren el conocimiento de expertos, quienes analizan e identifican patrones de comportamiento que salen de la norma y que podrían repercutir en eventos de FI. No obstante, el crecimiento de las IFDs conlleva crecimiento poblacional del personal, de los clientes, la tecnología y crecimiento de las necesidades de prevención. En la actualidad, los sistemas de información implementados (SIRO) contienen datos importantes acerca de los procesos y comportamientos del personal ante estos eventos.

En el último año, el desarrollo tecnológico en las IFD se ha impulsado de manera considerable, gracias a la pandemia. El desarrollo e implementación de la Automatización Robótica de Procesos (RPA) es cada vez más común. Sin embargo, no se encontraron desarrollos basados en agentes, aplicados a la gestión integral de riesgo operativo.

En el presente estudio se plantea la incorporación de agentes software, como parte del proceso de gestión de riesgo operativo. Para el planteamiento, se utiliza la concepción de Wooldridge y Jennings, quienes definen agente como “un programa autocontenido capaz de controlar su proceso de toma de decisiones y de actuar, basado en la percepción de su ambiente, en persecución de uno o varios objetivos” [5]. Se plantea también un sistema de agentes colaborativos, es decir, sistemas con más de un agente dedicado a satisfacer los requerimientos de sus usuarios.

Un sistema multiagente es aquel sistema que permite la gestión inteligente de otro sistema complejo, coordinando los distintos elementos que lo componen e integrando los objetivos particulares de cada subsistema en un objetivo común.

El esquema de comunicación que se plantea para la Gestión de Riesgo Operativo de tipo Fraude Interno (GROFI) es el de pizarra multicapa.

II. MODELO MULTIAGENTE FRAUDE INTERNO

El modelo se compone de: definición del ciclo de gestión de riesgo operativo, definición formal del agente y diseño del esquema de comunicación entre agentes.

A. Ciclo de gestión de riesgo operativo

Como resultado del relevamiento de información y con ayuda de los especialistas en el área, se plantea en la Figura 1, el



Para referenciar este artículo (IEEE):

[N] C. Mollinedo, «Modelo Multiagente para la prevención de riesgo operativo de tipo fraude interno en IFDs», *Revista PGI. Investigación, Ciencia y Tecnología en Informática*, n° 8, pp. 45-47, 2020.

ciclo de vida para la Gestión de Riesgo Operativo de tipo Fraude Interno (GROFI).

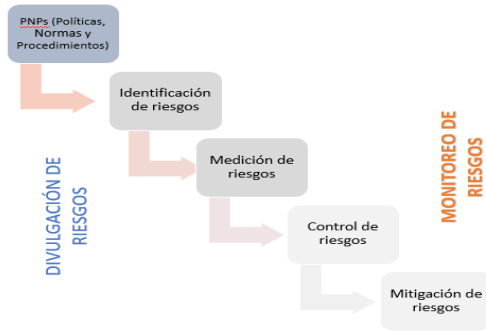


Fig. 1. Ciclo de gestión de riesgo operativo

B. Definición formal del agente

El sistema multiagente propuesto se representa como una n-tupla:

$$SMAFI = (E, C, A, R, Op, L) \quad (1)$$

Que se define como:

E: Entorno interno de la institución. E se caracteriza teniendo en cuenta las características del entorno propuestas por Russell y Norvig (2008) por ser parcialmente observable y no determinístico. El entorno está compuesto por:

- Core financiero
- Sistema de Información de Riesgo Operativo de tipo Fraude Interno
- Sistema administrativo

C: Base de conocimiento

A: es el conjunto de agentes que participan en la GROFI.

- Agente identifica
- Agente medición
- Agente divulgación
- Agente mitiga

Cada agente trabajara con las instancias y conceptos de C con el fin del logro de sus objetivos y los del sistema en general.

C. Comunicación

Para la comunicación entre agentes se usa el esquema de comunicación pizarra, tal y como se describe en la figura 2.

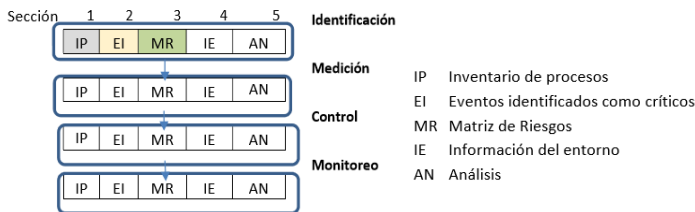


Fig. 2. Esquema pizarra

Un esquema de comunicación pizarra es considerada como un paradigma de comunicación, cuya estructura consta de tres componentes principales: la pizarra, un conjunto de fuentes de conocimiento (KSs, Knowledge sources) y un mecanismo de control. La pizarra es una base de datos global (compartida por todas las KSs) que contiene datos e hipótesis (soluciones parciales potenciales). Se suele estructurar la pizarra en niveles, asociando clases de hipótesis a un nivel, y las hipótesis suelen estar ligadas a hipótesis de otro nivel [5].

Este esquema permite que los agentes logren sus objetivos de forma independiente, registrando en la pizarra los eventos posibles (identificación), evaluarlos (medición), proponer estrategias y elabora la matriz de riesgos (control) y aplicar las estrategias (mitigación).

III. PROTOTIPO DEL SISTEMA

Se desarrolló el prototipo aplicando la metodología GAIA (metodología para el diseño de sistemas multiagente) y se pone especial énfasis en el diseño del agente identificador, puesto que la identificación del evento de riesgo se considera como el proceso más complejo:

A. Diagrama de agentes

TABLA I. DIAGRAMA DE AGENTE IDENTIFICADOR

Agente Identificador	
Descripción	
Lleva a cabo las tareas de búsqueda de posibles eventos de riesgo de tipo Fraude Interno. Accede a las transacciones del SIRO, al registro de Inventario de procesos y al histórico de fraudes y a los resultados de la evaluación del personal para generar información de posibles eventos de Fraude Interno.	
Roles	
Identificador de posibles eventos de riesgo de tipo Fraude Interno	
Servicios	
- Recopilación de eventos de riesgo (revisión de transacciones del sistema)	
- Recopilación de posibles eventos de riesgo de los diferentes procesos financieros (registros del SIRO y transacciones del Core Financiero)	
- Revisión de denuncias de posibles eventos de riesgo	
- Registro de posibles eventos de riesgo identificados en las revisiones de las áreas de control	
- Revisar fraudes históricos	
Creencias	
- Inventario de procesos	- SIRO
- Fraudes históricos	- Base de conocimientos
- Evaluación de personal	
Deseos	
- Identificar posibles eventos de Riesgo Operativo de Fraude Interno	
Intenciones	
- Generar la Matriz de Riesgos	
- Generar la trazabilidad de acciones susceptibles de riesgo del personal	
- Registro de eventos en la pizarra	

TABLA II. DIAGRAMA DE AGENTE MEDIDOR DE RIESGOS

Agente medidor de riesgos	
Descripción	
El Agente cuantifica los niveles de riesgo a los que está expuesto la IFD, realizando la medición de frecuencia e impacto de pérdidas que podrían ocurrir, como consecuencia de la materialización de los eventos adversos.	
Roles	
Medidor de niveles de RO	
Servicios	
- Cuantificación de pérdidas por Riesgo Operativo de Fraude Interno	
- Medición de frecuencia e impacto de los eventos de RO	
Creencias	
- Pizarra	- Base de conocimientos
- Estados Financieros	- Límites financieros
- Apetito de riesgo	
Deseos	
- Medición confiable y útil de los niveles de RO	
Intenciones	
- Lectura de eventos en la pizarra	- Lectura de Base de conocimientos
- Lectura de Estados Financieros	- Lectura de Límites Financieros
- Lectura del apetito de Riesgo	- Cálculos del impacto
- Medición de frecuencias	

Se denomina PNP al conjunto de Documentos de las Políticas Normas y Procedimientos detallados donde los funcionarios de la IFD acuden en caso de ocurrir posibles eventos de Riesgo Operativo.

B. Modelo de roles

En el modelo de roles se documenta los roles que ocurren en el sistema, permisos y responsabilidades, también se identifica los protocolos y actividades.

TABLA III. DIAGRAMA DE ROLES, AGENTE IDENTIFICADOR

<p>Diagrama de rol: Identificador de posibles eventos de riesgo de tipo Fraude Interno (IPER_FI)</p> <p>Descripción: Consiste en leer transacciones, evaluación de personal y eventos de riesgo del SIRO (eventos plasmados) que según la base de conocimiento de fraude interno tienen probabilidad de repercutir en eventos, dado que existe un patrón de comportamiento, establecimiento de pautas anómalas de fraude interno, aquellos con ranking alto (sospechosas) serán registrados en la pizarra.</p> <p>Protocolos y actividades: Evalúa-Transacción, Compara-Inventario, Compara-Histórico-EventosFraude, Evalúa-Caso, Registra-Pizarra Permisos Lectura-Transacción, Lectura-Inventario, Lectura-HistóricoEventos, Escritura-Pizarra, Lee-Base_Conocimientos</p> <p>Responsabilidades: <i>Viveza</i> IPER-FI = (((Lectura-Transacción. Compara-Inventario) w)(LecturaTransacción. Lectura-Histórico-Eventos) w). Evalúacaso) Registra-Pizarra</p> <p>Seguridad El registro en pizarra se realiza siempre y cuando exista un positivo de comparación entre la transacción leída y la comparación.</p>

C. Modelo de relaciones

El Modelo de Relaciones contiene los posibles enlaces de comunicación existentes entre los diferentes tipos de agentes dentro del MMA GIRO. En la figura 3 se puede apreciar la relación entre los agentes propuestos, donde la principal tarea la ejerce el agente encargado de gestionar la pizarra.

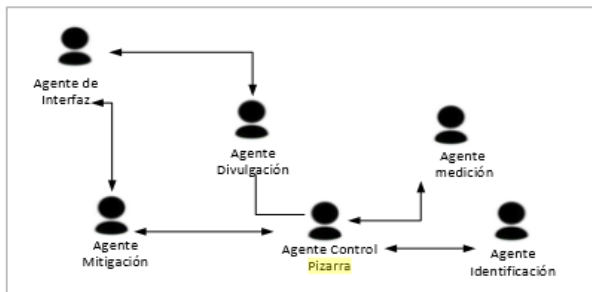


Fig. 3. Diagrama de relaciones

IV. RESULTADOS

Para evaluar la eficiencia de la solución propuesta se encuestó a profesionales con experiencia en desarrollo de aplicaciones en IFD. Se plantearon los siguientes criterios en

cada una de las etapas del modelo: respuesta a los objetivos, completitud del ciclo de vida, integración, validaciones, exactitud, comunicación, entorno dinámico, pedagogía, evolución y mejora. Los resultados obtenidos se ven en la fig. 4:

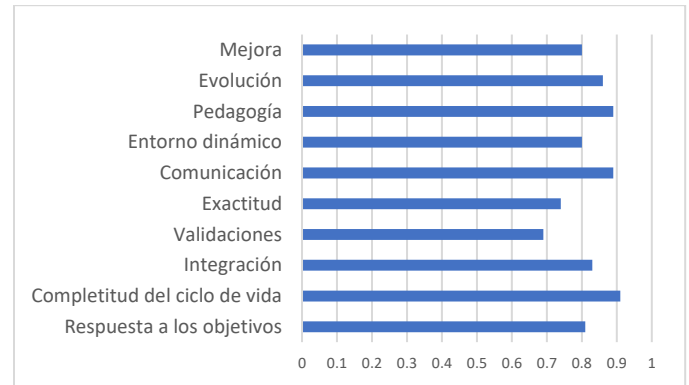


Fig. 4. Resultados de la valoración del modelo propuesto

Como se puede apreciar en la figura 4, los resultados son alentadores.

V. DISCUSIÓN

Es prácticamente imposible que un ser humano pueda monitorizar la actividad de cualquier organización en tiempo real [6]. Los Sistemas Multiagente, proveen una alternativa que permite apoyar el proceso de prevención de fraude, principalmente desde la identificación del riesgo. Particularmente las IFDs son instituciones en crecimiento y a pesar de que su tecnología aún no alcanza la magnitud ni organización de las financieras, las posibilidades de Riesgo Operativo de tipo Fraude Interno son latentes y requieren atención oportuna.

No obstante, no todas las variables son controlables, aún existe mucho por investigar y solucionar respecto al comportamiento de las personas.

REFERENCIAS

- [1] Finrural (2019). *Nuestras socias*. Recuperado de <https://www.finrural.org.bo/nuestras-socias.php>.
- [2] ASFI, Autoridad de Supervisión del Sistema Financiero de Bolivia (2015). "Normas para servicios financieros".sa diciembre de 2015. http://servdmzw.asfi.gob.bo/circular/circulares/ASFI_358.pdf
- [3] López, O. (2018), "De riesgos operativos y operativos, el desafío boliviano", Agencia de Noticias Fides, (21 23).
- [4] Jennings, N.; Wooldridge, M. *Agent Technology - Foundations, Applications, and Markets*. Springer-UNICOM. 1998.
- [5] Dalmau Espert, Juan (2015), "Sistema multiagente para el diseño, ejecución y seguimiento del proceso de planificación estratégica ágil en las organizaciones inteligentes" (Doctorado en Informática Avanzada). Universidad de Alicante, España.
- [6] Tomás y Valiente, F. *Instituto de Ingeniería del Conocimiento*. Machine Learning para detectar el fraude interno. Junio 2019.

Breve CV de la autora

Carmen Rosa Mollinedo Laura es Licenciada en Informática por la Universidad Mayor de San Andrés (La Paz, 1999). Email: carmenrosamollinedo@gmail.com.