

**UNIVERSIDAD MAYOR DE SAN ANDRÉS
FACULTAD DE CIENCIAS PURAS Y NATURALES
CARRERA DE INFORMÁTICA
POSTGRADO EN INFORMÁTICA**



TESIS MAGISTER

**PROGRAMA DE MAESTRÍA EN CIENCIAS DE LA COMPUTACIÓN
VERSIÓN 1 GESTIÓN 2000 - 2002**

**MODELO MULTIAGENTE PARA LA GESTIÓN
INTEGRAL DE RIESGO OPERATIVO DE
INSTITUCIONES FINANCIERAS DE DESARROLLO EN LA
CIUDAD DE EL ALTO**

**POR: Lic. Carmen Rosa Mollinedo Laura
TUTOR: PhD. Yohoni Cuenca Sarzuri**

LA PAZ - BOLIVIA

2020

Dedicatoria

*A Dios porque siempre está a
mi lado a pesar de mis
miedos y mis dudas.*

*A mis amados padres
Félix(†) y Cinda, por su
apoyo tan incondicional.*

*A mi hermana Cintia, cuya
fortaleza y decisión me
inspiran cada día.*

*A mis niños Samuel y
Sebastián quienes me han
enseñado a no rendirme.*

“Sabemos que Dios dispone todas las cosas para el bien de quienes lo aman”

Agradecimientos

Quiero expresar mi más sincero agradecimiento a todas aquellas personas que me ayudaron en el desarrollo de esta tesis:

Al PhD. Yohoni Cuenca Sarzuri, por su guía, consejos y sugerencias para la escritura de este documento.

Quiero agradecer especialmente a mi hermana Cintia, quien siempre me ha motivado y apoyado en el desarrollo de esta investigación y ha sido mi cómplice incondicional en todos mis proyectos. A mis amados niños Samuel y Sebastián, quienes me han concedido su valioso tiempo y su incondicional cariño, en fin, a su inocente manera me dieron fortaleza. A William y Álvaro, por su invaluable apoyo.

A mis amigos Irene Vedia y Adrián Quisbert, porque siempre me han apoyado, tanto en los cursos de maestría como en el desarrollo de esta tesis, ellos están siempre con sus palabras de ánimo y sus valiosos consejos.

RESUMEN

Toda organización se encuentra expuesta a riesgos, especialmente en el sector financiero, la gestión del riesgo operativo ha cobrado notable importancia en los últimos años. Esta preocupación por este tipo de riesgo no solo es nacional, sino internacional, por tanto, se han desarrollado acuerdos y estándares regulatorios para gestionar este tipo de riesgo y establecer los mecanismos para su cobertura. Las Instituciones Financieras de Desarrollo (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. Se caracterizan porque trabajan principalmente en el área urbana, peri-urbana y rural de Bolivia y operar con tecnologías financieras, acordes a las condiciones económicas de los usuarios.

La fragilidad de la gestión del riesgo operativo en el sector financiero se ha puesto en evidencia en los últimos años, muy especialmente en las IFDs. La necesidad de las entidades financieras de implementar sistemas de control interno, que aseguren que el riesgo operativo sea controlado o que no llegue a plasmarse en otro tipo de riesgos, abre la posibilidad de proponer nuevas soluciones. La principal contribución de este trabajo consiste, en el diseño de un modelo de desarrollo de software, que aplicando las bondades de la Inteligencia Artificial Distribuida (IAD) específicamente los Sistemas Multiagente, brinde soporte a la gestión del riesgo operativo para IFDs. El personal de desarrollo de software contará con un marco de referencia que le permita incursionar en la aplicación de técnicas de la IAD, como parte de sus soluciones. La propuesta de aplicación de agentes inteligentes permitirá realizar procesos de control, que hasta el momento dependían principalmente de la experiencia del personal del área. El modelo emplea el diseño de ontologías para representar el dominio y un sistema de pizarra para el almacén de la información que se genera durante el diseño y ejecución del proceso de gestión de riesgo operativo, de esta forma proveer la herramienta de comunicación entre agentes. Se considera integral porque involucra a la estructura organizativa dotada de especialistas e infraestructura de sistemas y equipos, el marco de políticas actualizadas, conocidas, de fácil acceso y entendimiento.

SUMMARY

Every organization is exposed to risks, especially in the financial sector, operational risk management has gained considerable importance in recent years. This concern for this type of risk is not only national, but international, therefore, agreements and regulatory standards have been developed to manage this type of risk and establish mechanisms for its coverage. The Financial Institutions of Development (IFD) are non-bank financial intermediation entities incorporated into the scope of the Law on Banks and Financial Entities through the Resolution of the Superintendence of Banks and Financial Entities No. SB 034/2008 and which are organized as Associations or foundations Nonprofit civilians. They are characterized because they work mainly in the urban, peri-urban and rural areas of Bolivia and operate with financial technologies according to the economic conditions of the users.

The fragility of operational risk management in the financial sector has been evidenced in recent years, especially in IFDs. The need for financial institutions to implement internal control systems, which ensure that the operational risk is controlled or that it does not become reflected in other types of risks, opens up the possibility of proposing new solutions. The main contribution of this work consists in the design of a software development model that, applying the benefits of Distributed Artificial Intelligence (IAD) specifically Multiagent Systems, provides support for the management of operational risk for IFDs. The software development staff will have a framework that allows them to enter the application of IAD techniques, as part of their solutions. The proposal of application of intelligent agents will allow to carry out control processes, which until now depended mainly on the experience of the personnel of the area. The model uses the design of ontologies to represent the domain and a whiteboard system for the storage of information that is generated during the design and execution of the operational risk management process. It is considered integral because it involves the organizational structure endowed with specialists and infrastructure of systems and equipment, the framework of updated policies, known, easy access and understanding.

Índice General

INTRODUCCIÓN.....	1
CAPÍTULO I PRESENTACIÓN DEL PROBLEMA.....	2
1.1 ANTECEDENTES	2
1.2 PLANTEAMIENTO DEL PROBLEMA.....	3
1.2.1 FORMULACIÓN DEL PROBLEMA DE INVESTIGACIÓN	3
1.2.2 PREGUNTA DE INVESTIGACIÓN	4
1.3 OBJETIVO GENERAL Y OBJETIVOS ESPECÍFICOS DE LA INVESTIGACIÓN	5
1.3.1 OBJETIVO GENERAL.....	5
1.3.2 OBJETIVOS ESPECÍFICOS.....	5
1.4 HIPÓTESIS Y OPERACIONALIZACIÓN DE LAS VARIABLES DE INVESTIGACIÓN	5
1.4.1 PLANTEAMIENTO DE LA HIPÓTESIS	5
1.4.2 IDENTIFICACIÓN DE VARIABLES	5
1.4.2.1 VARIABLE INDEPENDIENTE	5
1.4.2.2 VARIABLE DEPENDIENTE	5
1.4.2.3 UNIDAD DE OBSERVACIÓN	6
1.4.3 OPERACIONALIZACIÓN DE VARIABLES DE LA INVESTIGACIÓN	6
1.5 RESULTADOS DE LA INVESTIGACIÓN	8
1.6 JUSTIFICACIÓN.....	9
1.6.1 JUSTIFICACIÓN CIENTÍFICA	9
1.6.2 JUSTIFICACIÓN SOCIAL.....	9
1.6.3 JUSTIFICACIÓN PRÁCTICA.....	9
CAPÍTULO II MARCO TEÓRICO	10
2.1 MARCO CONCEPTUAL.....	10
2.1.1 LAS INSTITUCIONES FINANCIERAS DE DESARROLLO	10
2.1.2 GESTIÓN DEL RIESGO OPERATIVO EN LAS IFD	10
2.1.2.1 RIESGO OPERATIVO.....	10
2.1.2.2 LA GESTIÓN DE RIESGO OPERATIVO	11
2.1.2.3 GESTIÓN INTEGRAL DE RIESGO OPERATIVO	13
2.1.3 TECNOLOGÍAS PARA LA INTELIGENCIA ARTIFICIAL DISTRIBUIDA	13
2.1.3.1 AGENTES INTELIGENTES	13
2.1.3.2 PROPIEDADES EN LOS AGENTES.....	14
2.1.3.3 CLASIFICACIÓN DE AGENTES	16
2.1.3.4 ARQUITECTURA DE AGENTES	17
2.1.3.5 SISTEMAS MULTIAGENTES.....	18
2.1.3.6 DEFINICIÓN FORMAL DE UN SISTEMA MULTIAGENTE	19
2.1.3.7 REPRESENTACIÓN DEL CONOCIMIENTO MEDIANTE ONTOLOGÍAS	19
2.1.3.7.1 LAS ONTOLOGÍAS	19
2.1.3.7.2 DEFINICIÓN FORMAL DE UNA ONTOLOGÍA	21
2.1.3.7.3 CLASIFICACIÓN	23
2.1.3.8 ARQUITECTURA	24
2.1.3.8.1 EL MODELO PIZARRA.....	25
2.1.3.9 METODOLOGÍAS PARA EL DESARROLLO DE SMA	26
2.1.3.9.1 METODOLOGÍA GAIA	26
2.1.3.9.2 AUML.....	26
2.1.3.9.3 COMPARACIÓN DE METODOLOGÍAS SMA	27
2.2 MARCO LEGAL.....	28
CAPÍTULO III METODOLOGÍA DE LA INVESTIGACIÓN.....	30
3.1 MÉTODOS DE INVESTIGACIÓN	30
3.2 TIPOS DE INVESTIGACIÓN	30

3.2.1 ESTUDIO DESCRIPTIVO.....	30
3.2.2 ESTUDIO PROYECTIVO	30
3.2.3 ESTUDIO DE ALCANCE CORRELACIONAL	30
3.3 UNIVERSO O POBLACIÓN DE ESTUDIO	31
3.4 FUENTES Y DISEÑO DE LOS INSTRUMENTOS DE RELEVAMIENTO DE INFORMACIÓN	31
3.4.1 FUENTES DE LA INVESTIGACIÓN.....	31
3.4.2 DISEÑO DE LOS INSTRUMENTOS DE RELEVAMIENTO DE LA INFORMACIÓN.....	31
CAPÍTULO IV MARCO PRÁCTICO	34
4.1 METODOLOGÍA DEL DESARROLLO DE LA SOLUCIÓN	34
4.1.1 ANÁLISIS PARA EL MODELO PROPUESTO.....	34
4.1.2 MODELO DE GESTIÓN DE RIESGO OPERATIVO.....	39
4.1.3 DEFINICIÓN FORMAL DEL SISTEMA MULTIAGENTE.....	40
4.1.3.1 ONTOLOGÍA PARA LA GESTIÓN INTEGRAL DE RIESGO OPERATIVO	43
4.1.3.2 ARQUITECTURA DE COMUNICACIÓN	47
4.1.3.3 SUBPROCESOS DE SMAGIRO	54
4.1.4 MODELO MULTIAGENTE DE GESTIÓN INTEGRAL DE RIESGO OPERATIVO	59
4.1.4.1 ESPECIFICACIÓN DE REQUISITOS	60
4.1.4.2 ANÁLISIS	61
4.1.4.3 DISEÑO.....	62
4.1.4.4 IMPLEMENTACIÓN.....	63
4.1.5 APLICACIÓN DEL MMAGIRO PARA EL RIESGO OPERATIVO DE TIPO FRAUDE INTERNO.....	64
4.1.5.1 ESPECIFICACIÓN DE REQUISITOS	64
4.1.5.1.1 CONCEPTUALIZACIÓN DEL PROBLEMA	64
4.1.5.1.2 IDENTIFICACIÓN DE ACTORES	65
4.1.5.1.3 CARACTERÍSTICAS DEL ENTORNO	65
4.1.5.1.4 LISTA DE REQUISITOS.....	66
4.1.5.1.5 DESCRIPCIÓN DETALLADA DE LOS REQUISITOS	66
4.1.5.2 ANÁLISIS	67
4.1.5.2.1 DIAGRAMA DE AGENTES	67
4.1.5.2.2 MODELO DE ROLES.....	72
4.1.5.3 DISEÑO.....	74
4.1.5.3.1 MODELO DE SERVICIOS.....	74
4.1.5.4 IMPLEMENTACIÓN.....	77
4.2 VALIDACIÓN DE RESULTADOS.....	82
4.2.1 FORMULACIÓN DE HIPÓTESIS NULA	82
4.2.2 SELECCIÓN DE VARIABLES	82
4.2.3 INSTRUMENTACIÓN	82
4.2.4 ANÁLISIS E INTERPRETACIÓN	91
CAPÍTULO V CONCLUSIONES Y RECOMENDACIONES DE LA INVESTIGACIÓN	95
5.1 CONCLUSIONES	95
5.2 RECOMENDACIONES	96
ANEXOS.....	97
GLOSARIO.....	103
BIBLIOGRAFÍA	104

Lista de tablas

Tabla 1 Operacionalización de variable independiente	6
Tabla 2 Operacionalización de variable dependiente.....	7
Tabla 3 Resultados de la investigación	8
Tabla 4 Arquitecturas de SMA	24
Tabla 5 Diagramas de análisis y diseño de algunas de las metodologías	27
Tabla 6 Matriz FODA	37
Tabla 7 Descripción Rendimiento, Entorno, Actuadores, Sensores del SMA _{GIRO}	43
Tabla 8 Estructura Ontológica	44
Tabla 9 Lenguaje Ontología OGIRO	44
Tabla 10 Parámetros globales del modelo SMA _{GIRO}	48
Tabla 11 Inventario de procesos	49
Tabla 12 Repositorios de datos con los interactúan los agentes	49
Tabla 13 Fases de identificación: responsables y descripción	55
Tabla 14 Fases del subsistema de control del modelo propuesto: responsables y descripción	56
Tabla 15 Diagrama de Agente (AUML)	61
Tabla 16 Diagrama de rol.....	62
Tabla 17 Conceptualización del problema: Fraude.....	64
Tabla 18 Conceptualización del problema: Fraude Interno	64
Tabla 19 Características del entorno	65
Tabla 20 Lista de requisitos	66
Tabla 21 Descripción detallada del Requisitos Req. 1	66
Tabla 22 Descripción detallada del Requisitos Req. 2.....	66
Tabla 23 Descripción detallada del Requisitos Req. 3.....	67
Tabla 24 Diagrama de agente: Agente Identificador	67
Tabla 25 Matriz de Riesgo	68
Tabla 26 Tabla de puntuaciones.....	69
Tabla 27 Diagrama de agente: Agente Medidor de Riesgos.....	69
Tabla 28 Diagrama de agente: Agente Mitigación	70
Tabla 29 Diagrama de agente: Agente Divulgación	70
Tabla 30 Roles de los Agentes.....	71
Tabla 31 Diagrama de rol del Agente Identificador.....	72
Tabla 32 Diagrama de rol del Agente Medidor	73
Tabla 33 Diagrama de rol del Agente Mitigación.....	73
Tabla 34 Diagrama de rol del Agente Divulgador.....	74
Tabla 35 Modelo de servicios Rol IPER_FI	75
Tabla 36 Modelo de servicios Rol MNR_FI.....	75
Tabla 37 Modelo de servicios Rol DI_FI.....	75

Tabla 38 Identificación de criterios de evaluación del MMAGIRO	83
Tabla 39 Escala y ponderación de valores de las respuestas	83
Tabla 40 Cálculo de ponderaciones de los criterios de evaluación.....	84
Tabla 41 Diseño del experimento con las etapas MMA GIRO	85
Tabla 42 Criterios de valoración de la eficiencia del modelo: Tiempo y Funcionalidad.....	86
Tabla 43 Escala y ponderación de los valores de las respuestas	87
Tabla 44 Evaluación de eficiencia del Modelo tradicional	88
Tabla 45 Evaluación de eficiencia de MMAGIRO	89
Tabla 46 Experiencia de los encuestados en el desarrollo de agentes	91
Tabla 47 <i>Estadísticos descriptivos de comparación de MMAGIRO con el modelo tradicional</i>	93
Tabla 48 Frecuencias observadas.....	93
Tabla 49 Frecuencias esperadas	93

Índice de Figuras

Figura 1: Ontología ejemplo.....	22
Figura 2 Diseño de la solución.....	32
Figura 3 Análisis de la situación actual.....	34
Figura 4 Organigrama de una IFD.	34
Figura 5 Proceso de Gestión de Riesgo Operativo.....	39
Figura 6 El Modelo Multiagente como parte de la estructura tecnológica de la IFD ..	40
Figura 7: Diagrama de conceptos y relaciones de la ontología MMA-GIRO.....	46
Figura 8 Comunicación entre agentes	47
Figura 9 Capas de la pizarra.....	48
Figura 10 Esquema de comunicación entre agentes sobre la tecnología de la IFD – Riesgo fraude interno	51
Figura 11 Esquema de comunicación entre agentes sobre la tecnología de la IFD – Riesgo fallas tecnológicas	52
Figura 12 Esquema de comunicación entre agentes sobre la tecnología de la IFD – Riesgo fallas por procesos.....	53
Figura 13 Modelo SMA pedagógico para la divulgación de RO apoyado	58
Figura 14 Fases del Modelo MA GIRO	59
Figura 15 Especificación de requisitos	60
Figura 16 Fase de análisis del MMAGIRO.....	62
Figura 17 Fase de diseño del MMAGIRO	63
Figura 18 Estructura de agentes sobre la plataforma tecnológica de la IFD.....	76
Figura 19 Subproceso de identificación de riesgos.....	77
Figura 20 Estado de la pizarra y el historial de operaciones después de la identificación	78
Figura 21 Representación gráfica de los riesgos identificados	78
Figura 22 Subproceso de medición de riesgo.....	79
Figura 23 Pizarra nivel medición	79
Figura 24 Calificación asignada para determinar el nivel de riesgo	80
Figura 25 Subproceso de monitoreo	80
Figura 26 Matriz de riesgo	81
Figura 27 Observaciones y recomendaciones del Agente Control	81
Figura 28 Resultados de evaluación del MMAGIRO	84
Figura 29 Análisis del modelo tradicional.	89
Figura 30 Análisis del modelo MMAGIRO.....	90
Figura 31 Experiencia de los encuestados	91
Figura 32 Comparación entre el modelo “tradicional” y MMAGIRO	92
Figura 33 Opinión del Personal de Riesgo.....	94

INTRODUCCIÓN

Según Lavell (2002) el riesgo es: “la probabilidad que se presente un nivel de consecuencias económicas, sociales o ambientales en un sitio particular y durante un período definido. Se obtiene de relacionar la amenaza con la vulnerabilidad de los elementos expuestos”. En general el riesgo se refiere a la teórica "posibilidad de daño" bajo determinadas circunstancias. En cuanto a las entidades financieras en particular, se puede mencionar; el riesgo de crédito, el riesgo de mercado, el de liquidez y el operativo. Éste último se define como: “La posibilidad o probabilidad de que una entidad supervisada incurra en pérdidas por fraude interno o externo, fallas en las personas, procesos y sistemas, eventos internos de orden estratégico y operativo” (ASFI 2015).

En noviembre de 2015, la Autoridad de Supervisión del Sistema Financiero de Bolivia ASFI publica las Directrices Básicas para la gestión de riesgo operativo en el Sistema Financiero boliviano, en éste documento se manifiesta la importancia de desarrollar Sistemas de Información para la gestión de riesgo operativo, definiendo éste como: “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, en el marco del conjunto de estrategias, objetivos, políticas, procedimientos y acciones, establecidas por la entidad para este propósito”, (ASFI 2015).

En tal sentido, la presente tesis se desarrolló con el propósito de definir un modelo que permita realizar el desarrollo de Sistemas de Información de Gestión de Riesgo Operativo para Instituciones Financieras de Desarrollo (IFD), aprovechando las bondades de la Inteligencia Artificial Distribuida, específicamente los Sistemas Multiagente, considerando las ventajas de estas para resolver grandes problemas en los que los datos podían estar distribuidos y ser de distinta naturaleza.

Capítulo I PRESENTACIÓN DEL PROBLEMA

1.1 Antecedentes

Las Instituciones Financiera de Desarrollo (IFDs), se constituyen jurídicamente como asociaciones y fundaciones civiles sin fines de lucro, con la Resolución 34/2008 de marzo de 2008 emitida por la entonces Superintendencia de Bancos y Entidades Financieras (SBEF), donde algunas entidades están reguladas y otras en proceso de regulación manteniendo la forma jurídica original de constitución (FINRURAL, 2019)

El Banco Interamericano de Desarrollo, en su calidad de administrador de los recursos del FOMIN y la Asociación de Instituciones Financieras de Desarrollo Rural (FINRURAL), suscribieron en fecha 25 de septiembre de 2009 el Convenio de Cooperación Técnica No Reembolsable ATN/ME-11665-BO para la ejecución del Proyecto “Adecuación de las Instituciones Financieras de Desarrollo (IFD) al nuevo marco regulatorio”. Particularmente, las IFD han autogestionado la gestión integral de riesgos, entre los que destaca la gestión del riesgo operativo. La mayor parte de las IFD, a la fecha ya consiguieron licencia de funcionamiento, incluyéndose al sistema financiero formalmente establecido entre el 2016 al 2018. Por lo tanto, están en la obligación de aplicar todos los lineamientos de la Ley 393 de Servicios Financieros y la Recopilación de Normas de Servicios Financieros (RNSF), la otra parte de las IDF se encuentran en proceso de adecuación para conseguir la licencia de funcionamiento como entidades reguladas y están implementado los lineamientos mínimos de la RNSF. En este ámbito, las IFD cuentan con sistemas de control interno que se van fortaleciendo a medida que se aplica la RNSF en sus instituciones, las auditorías internas y externas realizan sus actividades implementado la Gestión de Auditoria Interna basada en riesgos, que tiene como aspecto fundamental la revisión del cumplimiento del riesgo operativo en estas entidades financieras y las visitas de inspección de la ASFI que verifican la implementación de la gestión de riesgos.

La Autoridad de Supervisión del Sistema Financiero (ASFI), en respuesta a la Ley 393 de Servicios Financieros, ha emitido diferentes circulares y modificaciones a la RNSF con el fin de implementar los lineamientos de riesgo operativo, implementado además mediante la Unidad de Investigaciones Financieras (UIF) para la prevención de fraudes, siendo el fraude interno el tipo de evento de pérdida más frecuente en riesgo operativo en las entidades financieras a nivel

internacional y con un alto grado de frecuencia en las IFD debido a la remuneración por bonos que se tienen en la mayoría de estas entidades.

En este sentido varias IFD cuentan o están en proceso de implementación de Sistemas de Información de Riesgo Operativo (SIRO), que tienen como función implementar fases o etapas del Riesgo Operacional. Sin embargo, tienen diversos enfoques según las soluciones de los diferentes proveedores, en su mayoría cuentan con el registro de eventos de riesgo para responder al requerimiento de información de la ASFI, información que deriva directamente en la Central de Información de Riesgo Operativo (CIRO), que es el Sistema de información administrado por la ASFI. La CIRO consolida los datos proporcionados por las entidades supervisadas, con relación a los eventos de riesgo operativo y pérdidas.

1.2 Planteamiento del problema

1.2.1 Formulación del problema de investigación

El riesgo operativo, es la posibilidad o probabilidad de que una entidad supervisada incurra en pérdidas por fraude interno o externo, fallas en las personas, procesos y sistemas, eventos internos de orden estratégico y operativo y otros eventos externos. (RNSF Libro 3°, Título V, Capítulo II y Sección 1).

La naturaleza de las entidades financieras implica que constantemente se asuman riesgos en la realización de sus actividades financieras y por ende en potenciales pérdidas para la entidad, se ha identificado que antes de incurrir en riesgo de crédito, riesgo de liquidez y otros, se plasma el riesgo operativo. Razón por la cual, en los últimos años las recomendaciones de Basilea han abundado en lineamientos para su implementación. Es por todo ello, que el riesgo operativo en las IFD ha ido adquiriendo una importancia cada vez más relevante.

Según las instructivas de la Autoridad de Supervisión del Sistema Financiero (ASFI), se establece la obligatoriedad de contar con documentos de normativas y procedimientos para eventos de riesgo operativo. Así mismo, toda entidad financiera es responsable de administrar su riesgo operativo, a cuyo efecto debe contar con procesos formales para su gestión que le permitan: identificar, medir, monitorear, controlar, mitigar y divulgar las exposiciones de riesgo que está asumiendo. Por tanto, las entidades financieras desarrollaron documentos de normas y procedimientos para gestionar el riesgo operativo en los diferentes niveles organizacionales.

Debido a que la entidad supervisada debe desarrollar e implementar sistemas de información y mecanismos de divulgación que le permitan una adecuada gestión del riesgo operativo, surge la necesidad de plantear soluciones que permitan dicha implementación. Según lo cual, las IFD en todos los niveles organizacionales, dentro de sus competencias y de acuerdo con sus políticas para el tratamiento de la información, deben hacer seguimiento sistemático de las exposiciones del riesgo operativo y de los resultados de las acciones adoptadas, lo cual significa un monitoreo permanente a través de un sistema de información. Estos sistemas deben mantener información suficiente para apoyar los procesos de toma de decisiones, que permita la generación de informes permanentes, oportunos, objetivos, relevantes, consistentes y dirigidos a los correspondientes niveles de la administración. Los sistemas de información deben contar con información histórica que asegure una revisión periódica, continua y objetiva de su perfil de riesgo, siendo esto el desafío que enfrentan las IFD en la actualidad.

El no aplicar oportuna y eficientemente acciones referentes al riesgo operativo puede repercutir en que:

- Los fallos de sistemas puedan ser catastróficos y las pérdidas sean difícilmente cuantificables.
- La probabilidad de ocurrencia de fraude interno y externo sumado a problemas relacionados con la seguridad de los sistemas aumente, siendo el más frecuente el fraude interno.
- La captura de transacciones, el monitoreo, el reporte y la documentación de clientes, así como la gestión de cuentas deban ser evaluados frecuentemente para reconocer posibles riesgos operacionales, lo que implica desgaste de recursos.

1.2.2 Pregunta de investigación

¿Cuán eficiente es el desarrollo de sistemas de Gestión Integral de Riesgo Operativo aplicando un Modelo Multiagente en Instituciones Financieras de Desarrollo en la ciudad de El Alto?

1.3 Objetivo General y Objetivos Específicos de la Investigación

1.3.1 Objetivo general

Diseñar un Modelo Multiagente para el eficiente desarrollo de sistemas de Gestión Integral de Riesgo Operativo en Instituciones Financieras de Desarrollo en la ciudad de El Alto.

1.3.2 Objetivos específicos

- Formalizar el proceso de gestión de riesgo operativo, definiendo los elementos para una IFD y estableciendo la relación entre los mismos, en el marco de lo propuesto por la ASFI y el Comité Basilea.
- Definir los componentes de un Sistema Multiagente para la gestión de riesgo operativo, incluyendo una ontología genérica.
- Proponer las fases de desarrollo de software para la Gestión Integral de Riesgo Operativo en IFDs, que contemple la formalización y la definición de un Sistema Multiagente proveyendo un esquema claro, sencillo y eficiente.

1.4 Hipótesis y operacionalización de las variables de investigación

1.4.1 Planteamiento de la hipótesis

El uso de un Modelo Multiagente influye en el eficiente desarrollo de sistemas de Gestión Integral de Riesgo Operativo de Instituciones Financieras de Desarrollo en la ciudad de El Alto.

1.4.2 Identificación de variables

1.4.2.1 Variable independiente

Modelo Multiagente

1.4.2.2 Variable dependiente

Desarrollo de sistemas de Gestión Integral de Riesgo Operativo de Instituciones Financieras de Desarrollo en la ciudad de El Alto.

1.4.2.3 Unidad de observación

Instituciones Financieras de Desarrollo: Diaconía FRIF (Fondo Rotativo de Inversión y Fomento) El Alto

1.4.3 Operacionalización de Variables de la Investigación

Tabla 1

Operacionalización de variable independiente

VARIABLE	OPERACIONALIZACIÓN	DIMENSIONES	INDICADORES	MEDIDORES	ESCALA	INSTRUMENTOS
Modelo Multiagente	Marco de referencia que proporciona un proceso formal para el desarrollo de Sistemas de Información de Gestión de Riesgo Operativo, aplicando las bondades de los Sistemas Multiagente	Integración de las fases de Riesgo Operativo	Contiene la fase de Identificación	1. Totalmente en desacuerdo; 2. Desacuerdo; 3. Neutral; 4. De acuerdo; 5. Totalmente de acuerdo	5 = 100% 4 = 80%, 3 = 60%, 2 = 30%, 1 = 10%	Revisión documental
			Contiene la fase de Medición			
			Contiene la fase de Control			
			Contiene la fase de Monitoreo			
			Contiene la fase de Divulgación			
		Legal	Responde a las recomendaciones de Basilea			
			Responde a los lineamientos de la ley 393			
			Responde a la recopilación de normas de servicios financieros de la Asfi			
		Definición del SMA	Compleitud (Todos los elementos del SMA se encuentran definidos)			
		Ciclo de vida	Respuesta a los objetivos Compleitud del ciclo de vida Integración Validaciones Exactitud Comunicación Entorno dinámico Pedagogía Evolución Mejora			

Nota: El Modelo Multiagente se analiza como variable cualitativa. Sus indicadores proveen un nivel de medición ordinal. Los valores de escala de Likert sobre la media indican el nivel de aceptación del modelo y corresponden al equivalente porcentual de los cinco valores de la escala.

Fuente: elaboración propia

1.5 Resultados de la Investigación

Esta investigación busca alcanzar los siguientes resultados:

Tabla 3

Resultados de la investigación

Fuente: elaboración propia

OBJETIVO ESPECÍFICO	RESULTADOS ESPERADOS	PRINCIPALES ACTIVIDADES
<p>1. Formalizar el proceso de gestión de riesgo operativo, definiendo los elementos de riesgo operativo en una IFD y estableciendo la relación entre los mismos, en el marco de lo propuesto por la ASFI y el Comité Basilea</p>	<p>1.1 Contar con el Diseño de un modelo de Gestión de riesgo Operativo con base en la normativa ASFI</p>	<p>1.1.1 Relevamiento de información 1.1.2 Realizar la Matriz FODA de análisis de la situación de RO en una IFD 1.1.3 Identificación de elementos del modelo 1.1.4 Identificación de las relaciones entre los elementos</p>
<p>2. Definir los componentes de un Sistema Multiagente para la gestión de riesgo operativo, incluyendo una ontología genérica que provea información del proceso de riesgo operativo.</p>	<p>2.1 Definición formal del SMA GIRO (sistema multiagente para la gestión integral de riesgo operativo) y sus elementos. 2.2 Definición formal de la Ontología de representación de conocimientos 2.3 Representación del esquema de comunicación entre agentes y la arquitectura del SMA</p>	<p>2.1.1 Identificar los agentes que intervienen en la GRO. 2.1.2 Diseño del entorno, operaciones y leyes. 2.2.1 Identificación y representación de conceptos 2.2.2 Identificación y representación de relaciones entre conceptos 2.3.1 Diseño y representación del esquema de pizarra 2.3.2 Diseño y representación de la arquitectura del SMA</p>
<p>3. Proponer las fases de desarrollo de software para la Gestión Integral de Riesgo Operativo en IFDs, que contemple la formalización y la definición de un Sistema Multiagente proveyendo un esquema claro, sencillo y eficiente.</p>	<p>3.1 Modelo MMAGIRO</p>	<p>3.1.1 Describir cada una de las etapas del modelo. 3.1.2 Diseñar un prototipo que permita la aplicación del modelo propuesto.</p>

Fuente: elaboración propia

1.6 Justificación

1.6.1 Justificación científica

El desarrollo de la presente investigación implica estructurar e integrar conceptos de la gestión de riesgo operativo en IFDs con técnicas de la inteligencia artificial, como son los sistemas Multiagente. Al respecto, la aplicación del método científico permite brindar respuestas a los problemas planteados y sistematizar los resultados.

1.6.2 Justificación social

El desarrollo del modelo propuesto estará sujeto a las normas dispuestas por la ASFI para el sistema financiero del Estado Plurinacional de Bolivia y los acuerdos del Comité de Supervisión Bancaria de Basilea. Dichos lineamientos generan la necesidad de cambiar la estructura de los modelos existentes evolucionando a otros modelos y estructuras que permitan una mayor participación de los grupos implicados en la organización, que coadyuven de manera eficiente en la prevención y toma de decisiones referente al riesgo operativo. En tal sentido, éste estudio beneficiará tanto a los profesionales dedicados al desarrollo del software como a los usuarios del producto final.

1.6.3 Justificación práctica

La gestión integral del riesgo operativo es un problema que aqueja a toda organización, especialmente a las IFDs, cuya plataforma tecnológica se encuentra en proceso de desarrollo e implementación. Contar con un modelo de desarrollo de software, que cubra las etapas del riesgo operativo, se constituye en una solución práctica planteada para solucionar un problema real.

Capítulo II MARCO TEÓRICO

2.1 Marco Conceptual

2.1.1 Las Instituciones Financieras de Desarrollo

Las Instituciones Financieras de Desarrollo (IFD's) son instituciones organizadas bajo la figura jurídica de Asociaciones y Fundaciones sin fines de lucro, que permiten a microempresas, organizaciones económicas campesinas, personas y grupos desatendidos por el sistema financiero tradicional el acceso a servicios financieros, ofreciéndoles productos y tecnologías crediticias integrales no tradicionales que se acomodan al contexto económico, social y organizacional de sus prestatarios, cuya presencia, impacto y desempeño, se ha incrementado en los últimos años. Estas instituciones se encuentran bajo el marco legal de la Ley 393 de Servicios Financieros y son regulados por la Autoridad de Supervisión del Sistema Financiero (ASFI). (Finrural, 2019).

2.1.2 Gestión del Riesgo Operativo en las IFD

2.1.2.1 Riesgo Operativo

En el Segundo Documento Consultivo del Comité Basilea para la Supervisión Bancaria (BCBS, 2001a) y en el texto complementario denominado “Operational Risk” (BCBS, 2001b), se planteó una definición preliminar para riesgo operacional que excluía el riesgo estratégico y reputacional. En esta propuesta se define el Riesgo Operativo, como el riesgo de sufrir pérdidas como resultado de inadecuados procesos, y/o fallas en las personas o sistemas internos, o bien a causa de acontecimientos externos. Esta definición engloba el riesgo legal, pero excluye el riesgo estratégico y el riesgo reputacional.

A partir de esta primera definición se establece una clasificación y determinación de los principales factores y eventos de pérdida:

- Fraude Interno;
- Fraude Externo;
- Relaciones laborales y seguridad en el puesto de trabajo;

- Incidencias en el negocio y fallos en los sistemas;
- Daños a activos materiales;
- Clientes, productos y prácticas empresariales
- Ejecución, entrega y gestión de procesos.

2.1.2.2 La Gestión de Riesgo Operativo

La Gestión de Riesgo Operativo 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, en el marco del conjunto de estrategias, objetivos, políticas, procedimientos y acciones, establecidas por la entidad para este propósito”. Se entiende por eventos de riesgo operativo, a aquellos incidentes o conjunto de ellos, que provocan que los resultados difieran de los esperados, debido a procesos defectuosos, recursos humanos inadecuados, fallos en los sistemas o por causas externas (RNSF).

Según instructivo de la ASFI, toda entidad supervisada, en la implementación de la gestión del riesgo operativo, debe observar mínimamente los siguientes principios:

- a. Contar con una estrategia formal para la gestión del riesgo operativo, desarrollada a partir de la estrategia general de la entidad supervisada que responda a su modelo de negocios;
- b. Establecer una estructura organizativa con una clara segregación de funciones, acorde a la estrategia, tamaño y complejidad de las operaciones de la entidad supervisada, que facilite la gestión del riesgo operativo y evite posibles conflictos de interés;
- c. Desarrollar políticas, procedimientos y herramientas adecuadas a la estrategia, tamaño y complejidad de las operaciones de la entidad supervisada, que apoyen la gestión de riesgo operativo;
- d. Actualizar oportunamente el proceso de gestión del riesgo operativo en respuesta a los cambios en el entorno, modelo de negocios y/o el perfil de riesgo de la entidad supervisada;
- e. Promover una cultura de gestión del riesgo operativo al interior de la entidad supervisada;
- f. Implementar sistemas de información que permitan la divulgación del riesgo operativo al cual se encuentra expuesta la entidad supervisada, a las instancias que correspondan;
- g. Priorizar la implementación de acciones preventivas, antes que correctivas;

- h. Identificar y evaluar el riesgo operativo inherente a todos los productos, actividades, procesos y sistemas;
- i. Instaurar un proceso para el seguimiento regular de los perfiles de riesgo operativo y de su exposición a pérdidas;

El presente estudio incluye principalmente dar solución a los incisos (e) y (f), y proveer apoyo a lo requerido en el inciso (a), puesto que los demás incisos dependen de la Institución Financiera y de su propio proyecto institucional. Para promover una cultura de gestión del riesgo operativo al interior de la entidad, se modela el SMA.

La gestión integral de riesgos involucra al menos seis etapas adecuadamente estructuradas, consistentes y continuas, de acuerdo con lo siguiente:

a. Identificación: Es un proceso dirigido a reconocer y entender los diferentes tipos de riesgos que existen en las operaciones que realiza la entidad supervisada, y aquellos que pueden surgir de iniciativas de nuevos productos y operaciones. Esta etapa permite determinar de manera preventiva posibles acciones a seguir, dado que se identifican y clasifican los eventos adversos según el tipo de riesgo al que corresponden, la interrelación que puede existir entre estos, las áreas expuestas y el posible efecto que se produciría en la situación financiera de la entidad supervisada;

b. Medición: Es la etapa en la cual la entidad supervisada, a través de las herramientas que desarrolla, cuantifica sus niveles de exposición a los diferentes tipos de riesgos que se encuentran presentes en las operaciones que realiza. La medición efectuada considera la frecuencia e impacto de las pérdidas que podrían acontecer, dada la ocurrencia de eventos adversos;

c. Monitoreo: Consiste en el establecimiento de procesos de control al interior de la entidad supervisada, que está asociado entre otros a los sistemas de información que facilitan el seguimiento de la gestión integral de riesgos, ayudando a detectar y corregir oportunamente deficiencias y/o incumplimientos en las políticas, procesos y procedimientos para cada uno de los riesgos a los cuales se encuentra expuesta la entidad supervisada;

d. Control: Es el conjunto de actividades que se realizan con la finalidad de disminuir la probabilidad de ocurrencia de un evento adverso, que pueda originar pérdidas a la entidad supervisada;

e. Mitigación: Corresponde a las acciones realizadas, los mecanismos y/o coberturas implementadas por la entidad supervisada, para reducir al mínimo las pérdidas incurridas, como consecuencia de la materialización de los sucesos o eventos adversos de riesgo;

f. Divulgación: Es la acción orientada a establecer y desarrollar un plan de comunicación que asegure de forma periódica la distribución de información apropiada, veraz y oportuna, relacionada con la entidad supervisada y su proceso de gestión integral de riesgos. Dicha información se designa a todo el personal de la institución en sus diferentes niveles jerárquicos.

2.1.2.3 Gestión Integral de Riesgo Operativo

La ASFI (2018), en su artículo 3 f) define la gestión Integral de Riesgo Operativo como el proceso estructurado, consistente y continuo para identificar, medir, monitorear, controlar, mitigar y divulgar todos los riesgos a los cuales la entidad supervisada se encuentra expuesta, en el marco del conjunto de estrategias, objetivos, políticas, procedimientos y acciones, establecidas por la entidad para este propósito.

En los lineamientos para la gestión integral de riesgo la ASFI en el Art. 1, instruye que la entidad supervisada es responsable de administrar sus riesgos. El proceso de gestión de riesgos debe ser integral, para lo cual la entidad supervisada debe considerar la totalidad de los tipos de riesgo a los que se encuentra expuesta, así como las interrelaciones que pueden existir entre éstos.

2.1.3 Tecnologías para la Inteligencia Artificial Distribuida

2.1.3.1 Agentes inteligentes

Un agente se caracteriza por tres elementos fundamentales, el primero se refiere al hecho de producir un efecto, el segundo referido a la ejecución de una acción y el tercero referido a que este proceso ocurre en un entorno o medio ambiente.

A continuación, se presentan algunas definiciones de agente (Aguilar, Ríos, Hidrobo y Cerrada 2013):

- Shoham: “Usualmente, cuando la gente usa el término agente se refiere a una entidad que funciona continua y autónomamente, en un entorno en el cual otros procesos ocurren y existen otros agentes”
- Russel: “Un agente es una entidad que percibe su entorno y actúa bajo estas percepciones”
- Franklin y Gasser: “Un agente autónomo es un sistema situado en, y como parte de, un entorno, que detecta dicho entorno y actúa en él, en búsqueda de sus propios objetivos ...”.
- Wooldridge y Jennings: “Es un sistema de hardware o, principalmente, software, que es autónomo, reactivo y social”.
- Ferber: “Un agente es un hardware o software que puede actuar sobre sí mismo o sobre su ambiente. Además, tiene una representación parcial de su ambiente y puede comunicarse con otros agentes. Por otro lado, tiene objetivos individuales y su comportamiento es el resultado de las observaciones, conocimiento, habilidades e interrelaciones que él puede tener con otros agentes o con su ambiente”.
- Weiss: “Un agente es un sistema computacional que está situado en un ambiente, y que es capaz de tomar acciones autónomas en ese ambiente con el fin de cumplir sus objetivos de diseño”.

2.1.3.2 Propiedades en los agentes

Un agente, para ser considerado como tal, debe tener una combinación del siguiente conjunto de propiedades (Wooldridge, 1999).

- Reactividad. Un sistema reactivo mantiene interacción constante con su entorno, y responde a los cambios que ocurren en este. En especial, los agentes reactivos se caracterizan por la capacidad de emitir una acción inmediata al recibir una señal, o percibir un estado en el entorno. Esta propiedad de los agentes reactivos posibilita acciones rápidas, importantes en sistemas de tiempo real, que no necesariamente requieren reglas complejas.

- Proactividad. Referido al concepto de Estímulo → Respuesta, para cada estímulo se construiría la lógica que representa la respuesta. El comportamiento de estos agentes debe estar basado principalmente en objetivos o metas. Por tanto, sus acciones no están dirigidas solamente por estímulos, sino que ellos deben ser capaces de tomar iniciativas y planificar acciones, con el fin de alcanzar los objetivos del sistema.
- Comunicación. Es la capacidad de cada agente de “conversar”, es decir es la cualidad de intercambiar información, con otros agentes. La comunicación puede ser directa o indirecta. En el caso de comunicación directa se requiere de un lenguaje formal y realizar intervenciones, descritas como mensajes compuestos por dos partes:
 - El envoltorio: indica los datos del agente emisor, de los agentes receptores, y el lenguaje, la ontología y el protocolo utilizado
 - El contenido: compuesto por una parte formativa que indica la acción general del mensaje, y la frase construida usando la ontología usada, que indica sobre qué aspectos trata la parte formativa
- Sociabilidad. Los agentes son diseñados con la capacidad de obrar y cooperar recíprocamente con otros agentes, a través de un lenguaje de comunicación de agentes. Los agentes requieren cualidades de cooperación y cumplimiento de estrategias con el fin del cumplimiento de metas y objetivos.
- Movilidad. Es la habilidad del agente de moverse en el ambiente. Los agentes pueden migrar, trasladarse en una red de nodos de procesamiento, para ejecutar tareas específicas. Así, la movilidad tiene que ver con la capacidad de los agentes de moverse en un entorno dado. La movilidad implica contar con sistemas de nombramiento y localización, inherentes a los sistemas distribuidos.
- Autonomía. La autonomía es considerada por muchos autores como la principal propiedad de los agentes. Siendo esta propiedad, la capacidad de los agentes para actuar sin la intervención humana ni de otros sistemas externos; esto le permite tener un comportamiento propio, y reaccionar a los estímulos externos basándose en sus estados internos.

- Veracidad. La información que los agentes comunican debe ser verdadera, sin embargo, estos datos dependen de la intención con que fueron diseñados, en tal caso estarían actuando solamente en función del cumplimiento de sus metas u objetivos. En ese sentido, en una comunidad de agentes se supone que todos los agentes proveen el resultado veraz de su actuación.
- Benevolencia. Siempre que no entre en conflicto con sus propios objetivos, los agentes ayudan a otros agentes a través de la prestación de servicios específicos. En ese sentido, en una comunidad de agentes todos los agentes son propensos a colaborar, a trabajar en conjunto.
- Racionalidad. Un agente actúa racionalmente en el sentido que no ejecuta acciones si estas no lo llevan a cumplir sus objetivos. De manera general, los agentes tienen un conjunto de objetivos predefinidos y emprenden acciones para conseguirlos. La decisión de cual acción seguir, y en qué momento hacerlo, es hecha según un principio de racionalidad: se prefiere la acción más prometedora o eficiente para conseguir sus metas.
- Inteligencia. Debido a que un agente debe analizar, ordenar ideas y conocimiento sobre el entorno, para llegar a una conclusión, y tomar una acción de forma autónoma, es necesario esta propiedad. Ella conjuga la capacidad de acumular conocimiento (aprender) y de usarlo adecuadamente (razonar a partir de él). Para implantar esta propiedad se pueden utilizar técnicas computacionales inteligentes como los sistemas expertos, las redes neuronales artificiales, la lógica difusa, etc.
- Adaptativo. Un agente es capaz de cambiar su comportamiento basado en las experiencias previas y las percepciones que ha hecho de su entorno. De esta manera, puede irse auto reconfigurando para adaptarse a su entorno.

Otras cualidades que los autores mencionan son: la Persistencia y la Flexibilidad.

2.1.3.3 Clasificación de Agentes

En la presente investigación se considera la clasificación propuesta por Mas, A. (2004), que identifica características de los agentes para entablar la comunicación y la necesidad de los

agentes intermediarios especializados en conocer las posiciones de los otros y los servicios que ofrecen:

- **Facilitadores:** coordinan otros agentes subordinándolos a cambios de sus servicios.
- **Mediadores:** utilizan servicios de varios agentes para construir servicios de más alto nivel.
- **Bróker:** reciben y resuelven peticiones usando servicios de otros.
- **Buscador de pareja:** si recibe una petición, devuelve el ID del agente que tenga el servicio más adecuado a sus necesidades.
- **Páginas amarillas:** contiene el listado de los servicios y los agentes que los proveen.
- **Pizarra:** recibe peticiones que serán entregadas a otros agentes.

2.1.3.4 Arquitectura de Agentes

Se desarrolla un tipo de arquitectura deliberativa. En este tipo de arquitectura, tanto el comportamiento como el conocimiento de los agentes están representados de manera explícita, haciendo uso de algún modelo simbólico. Es una extensión del caso anterior, y al igual que en dicho caso, los agentes toman sus decisiones a través de procesos de razonamiento lógico. El ejemplo más importante de una arquitectura deliberativa es el de los agentes BDI. Un agente BDI es un agente racional que presenta actitudes mentales: Creencias (*Beliefs*), Deseos (*Desires*) e Intenciones (*Intentions*).

- a. **Creencias.** Están representadas por la información y conocimiento que tiene el agente sobre el entorno (sobre sí mismo y sobre otros agentes). Es decir, representan el conocimiento del agente acerca del mundo: qué es lo que el agente cree que es cierto acerca del mundo. Dicho conocimiento es usualmente almacenado en una base de datos especial, conocida como “base de conocimientos”. Debe tomarse en cuenta que el conocimiento de un agente puede variar con el tiempo, incluso puede llegar a ser falso.
- b. **Deseos.** Los deseos representan los objetivos del agente. Estos pueden ser estados a los que quiera llegar el agente, o situaciones que el agente quisiera lograr o causar. El uso de objetivos añade la restricción de que dicho conjunto debe ser consistente, evitando metas concurrentes o contradictorias.
- c. **Intenciones.** Las intenciones representan el estado deliberativo del agente; lo que el agente ha elegido hacer. Las intenciones pueden verse como los deseos en los cuales el agente tiene mayor grado de confianza. En menos palabras, son las metas que se fija

hacer el agente para cumplir sus deseos, dadas sus creencias. Una buena parte de los progresos importantes en ingeniería de software se basan en el uso de nuevas abstracciones (abstracciones procedimentales, tipos de datos abstractos, objetos, agentes, etc.). Así, el uso del concepto de intencionalidad se convierte en una herramienta de abstracción que permite, de manera conveniente, describir, explicar y especificar el comportamiento de sistemas complejos.

2.1.3.5 Sistemas Multiagentes

La Inteligencia Artificial Distribuida (IAD) es uno de los dominios que ha estudiado ese problema, en este caso, usando conceptos provenientes tanto de la Inteligencia Artificial (IA) como de los Sistemas Distribuidos. En general, los sistemas basados en IAD son cooperativos, compuestos por al menos dos agentes, los cuales interactúan para la resolución de un problema dado. Los agentes son frecuentemente heterogéneos, deben tener cierto grado de autonomía, con ciertas capacidades de razonamiento, planificación, aprendizaje, entre otros aspectos. Además, los agentes deben ser capaces de interactuar, negociar, coordinarse, y hasta competir con otros, para llevar a cabo sus tareas, las cuales pueden ser individuales o colectivas.

Así, la IAD puede verse como un subcampo de la IA, que tiene que ver con la resolución de problemas cooperativamente. Sus áreas principales son: La Resolución Distribuida de Problemas y los Sistemas Multiagentes (Aguilar, Ríos, Hidrobo y Cerrada 2013).

Un Sistema Multiagente (SMA) tiene que ver con el comportamiento de una colección de agentes autónomos tratando de resolver un problema dado, por lo cual comparten conocimiento acerca del problema y su(s) solución(es). Como menciona Dalmau (2015) la organización en los sistemas multiagente depende del tipo de comunicación (protocolo de comunicación) y el modo de cooperación entre agentes (protocolo de interacción) así como del tipo de agentes que conforman el grupo. En general se pueden distinguir tres tipos de configuraciones organizacionales:

- Estructura Centralizada: en este tipo de configuración existe un agente que controla la interacción de los demás agentes del sistema, porque tiene la información o la funcionalidad para hacerlo.
- Estructura Horizontal: este tipo de configuración existe cuando todos los agentes que integran un sistema están al mismo nivel, es decir, no hay ningún agente que haga las veces de maestro o supervisor, ni tampoco agentes esclavos.

- Estructura Jerárquica: esta configuración existe cuando los agentes trabajan en diferentes niveles de abstracción de un problema, es decir, bajo una configuración de niveles. En un mismo nivel se establece una configuración horizontal, si hay más de un agente. Para resolver un problema cada agente divide el problema en subproblemas que él puede resolver, subproblemas que puede resolver con la cooperación de los agentes que están al mismo nivel y subproblemas que sabe que los agentes de niveles inferiores de la jerarquía pueden resolver.
- Estructura ad hoc: esta configuración puede ser una mezcla de las tres anteriores, se caracteriza porque la dinamicidad de la estructura está regida por el ajuste mutuo entre los pequeños grupos de agentes en el sistema.

2.1.3.6 Definición formal de un Sistema Multiagente

En base a la propuesta de Ferber (1998) los SMA se pueden definir formalmente como una N-tupla:

$$SMA = (E, O, A, R, Op, LoU)$$

Donde:

- E es el entorno que tiene generalmente un volumen.
- O es un conjunto de objetos situados en E los cuales pueden ser estacionales o no, ser percibidos, creados, destruidos y modificados por los agentes.
- A es un conjunto de agentes que pueden ser representados como objetos específicos ($A \subseteq O$) y que participan como entidades activas dentro del sistema.
- R es un conjunto de relaciones que enlazan los objetos (entre ellos también agentes).
- Op es un conjunto de operaciones que permiten que los agentes A puedan percibir, producir, consumir, transformar y manipular objetos de O .
- LoU es el conjunto de las denominadas leyes del universo que son comunes en el entorno E y que modelan las reacciones del mundo a las acciones de los agentes.

2.1.3.7 Representación del conocimiento mediante Ontologías

2.1.3.7.1 Las Ontologías

La representación del conocimiento es uno de los retos fundamentales de la inteligencia Artificial, el conocimiento que está compuesto de componentes teóricos y heurísticos tiene una

estructura diferente a la información, por tanto, su representación debe usar técnicas diferentes para aprovechar todo su dominio.

La palabra ontología fue tomada de la filosofía, campo en el cual se define como “la explicación sistemática del ser”. Como resultado de la investigación realizada, se destacan las siguientes definiciones:

- Según Gruber (1993), ontología es “a formal, explicit specification of a shared conceptualization”. Que se refiere a una descripción de conceptos y relaciones que pueden existir para un agente o una comunidad de agentes. Un cuerpo de conocimiento representado formalmente que está basado en una conceptualización: los objetos, los conceptos y otras entidades que se presumen existentes en un área de interés y las relaciones que las contienen. La conceptualización es una forma abstracta y simplificada de ver el mundo que se quiere representar con algún propósito. La conceptualización se refiere a un modelo abstracto de algún fenómeno del mundo teniendo identificados los conceptos relevantes del fenómeno. Explicito significa que el tipo de conceptos usados y las restricciones en su uso son explícitamente definidas. Formal se refiere al hecho de que la ontología debiera ser computable. Compartido refleja la noción de que una ontología captura conocimiento no privado de algún individuo, sino aceptado por un grupo.
- Desde un punto de vista más aplicado, Noy y McGuinness (2001) describen la ontología como una descripción formal y explícita de los conceptos en un dominio de discurso (clases o conceptos), las propiedades de cada concepto que describen sus características y los atributos (*slots*, roles o propiedades) y las restricciones asociadas a esas propiedades (facetas o restricciones de rol).
- Para Neches y otros (1991) una ontología es una definición de los términos básicos y las relaciones que comprenden el vocabulario de un tema, como así también, define las reglas para combinar esos términos y relaciones y así introducir extensiones en el vocabulario. En base a esta definición una ontología no solo incluye los términos que son expresamente definidos en ella, sino también los que pueden ser inferidos de ella.
- Para Uschold y Jasper (1999) una ontología puede tomar varias formas, pero necesariamente deberá incluir un vocabulario de términos y alguna especificación de su

significado. Esto incluye definiciones y una indicación de como los conceptos son interrelacionados; esta interrelación impone colectivamente una estructura en el dominio y restringe la posible interpretación de términos.

En su tesis Dalmau (2015), extrae de las anteriores definiciones, las siguientes palabras clave: especificación, explícita, conceptos y relaciones, interrelacionados, formal, compartida y vocabulario y plantea como denominador común que se podría establecer que una ontología posibilita un conocimiento consensuado de un dominio en cuestión con el objetivo de poder compartirlo.

2.1.3.7.2 Definición formal de una ontología

Para realizar la definición formal, primero definimos los componentes de una ontología, según la investigación de Gruber (1993), que afirma que las ontologías están formadas por componentes que servirán para representar el conocimiento de algún dominio específico. Estos componentes son los siguientes:

- **Conceptos:** que son las ideas básicas que se intentan formalizar. Estos conceptos pueden ser clases de objetos, métodos, planes, estrategias, procesos de razonamiento, etc.
- **Relaciones:** que representan la interacción y el enlace entre los conceptos del dominio. Suelen formar la taxonomía del dominio. Por ejemplo: subclase-de, parte-de, etc.
- **Funciones:** que son un tipo concreto de relación donde se identifica un elemento mediante el cálculo de una función que considera varios elementos de la ontología. Por ejemplo: categorizar-clase.
- **Instancias:** utilizadas para representar objetos determinados de un concepto.
- **Axiomas:** que son teoremas que se declaran sobre relaciones que deben cumplir los elementos de la ontología. Por ejemplo: “Si X y Y son de la clase Z, entonces X no es subclase de Y” o “Para todo X que cumpla con la condición Cond1, A es B”.

En base a estas definiciones las ontologías se pueden ver como un conjunto de conceptos que tienen propiedades y que están ordenados en jerarquías de taxonomías.

De la adaptación realizada por Pretorius (2004) de la definición formal de ontología propuesta por Maedche (2002), la estructura ontológica O se define formalmente como:

$$O = \{C, R, A^o\}$$

Donde:

- C es un conjunto de elementos llamados conceptos/clases los cuales según Noy y McGuinness (2001) tienen propiedades que describen sus características y atributos.
- $R \subseteq C \times C$ es el conjunto de las relaciones existentes entre los conceptos/clases de C .
- A^o es el conjunto de axiomas en O .

En Maedche y Staab (2000) se propone también $H \subseteq C \times C$ como elemento que también forma parte de O y que representa la estructura jerárquica inherentemente existente entre los conceptos C (taxonomía jerárquica) pero tal y como se describe en Pretorius (2004) ésta es redundante dado que puede quedar expresada explícitamente en términos de R de la forma que se explica a continuación.

Dado $r \in R$ y $r = (c1, c2)$ donde $c1, c2 \in C$, si r expresa una relación de jerarquía existente entre los conceptos $c1$ y $c2$ entonces se asume que $c2$ es subclase de $c1$. De esta forma no se requiere la definición de H puesto que en R ya ha quedado definida de forma explícita. En base a dicha relación r , $c2$ heredara las propiedades que tiene definidas su clase padre (superclase) $c1$ (herencia simple). Las relaciones r se corresponden con relaciones de tipo “Es-un” o “Es un tipo de”.

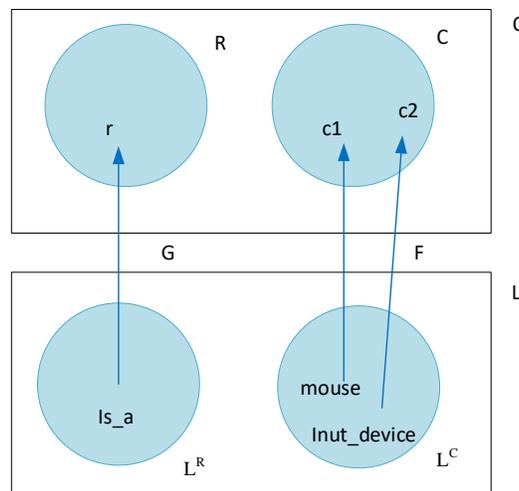


Figura 1: Ontología ejemplo
Elaborada a partir del gráfico de Pretorius (2004)

Para esta estructura ontológica O se define el léxico (lenguaje) L como:

$$L = \{L^C, L^R, F, G\}$$

Donde:

- L^C es el conjunto de elementos denominados entradas léxicas de conceptos.

- L^R es el conjunto de elementos denominados entradas léxicas de relaciones.
- $F \subseteq L^C \times C$ es una referencia a conceptos que cumple que

$$F(l_C) = \{c \in C : (l_C, c) \in F\}$$
 para todo $l_C \in L^C$,

$$F^{-1}(c) = \{l_C \in L^C : (l_C, c) \in F\}$$
 para todo $c \in C$.
- $G \subseteq L^R \times R$ es una referencia a relaciones que cumple que

$$G(l_R) = \{r \in R : (l_R, r) \in G\}$$
 para todo $l_R \in L^R$,

$$G^{-1}(r) = \{l_R \in L^R : (l_R, r) \in G\}$$
 para todo $r \in R$.

2.1.3.7.3 Clasificación

De acuerdo con el nivel de generalidad, clasificación según Guarino (1998):

- **Ontologías de Alto Nivel:** Describen conceptos generales como espacio, tiempo, materia, objeto. Son independientes de un dominio o problema particular. Su intención es unificar criterios entre grandes comunidades de usuarios.
- **Ontologías de Dominio:** Describen el vocabulario relacionado a un dominio genérico (por ejemplo, medicina o automotores), por medio de la especialización de los conceptos introducidos en las ontologías de alto nivel.
- **Ontologías de Tareas:** Describen el vocabulario relacionado con una tarea o actividad genérica (por ejemplo, de diagnóstico o de ventas), por medio de la especialización de los conceptos introducidos en las ontologías de alto nivel.
- **Ontologías de Aplicación:** Describen conceptos que pertenecen a la vez a un dominio y a una tarea particular, por medio de la especialización de los conceptos de las ontologías de dominio y de tareas. Generalmente corresponden a roles que juegan las entidades del dominio cuando ejecutan una actividad.

Clasificación según Fensel (2003):

- **Ontologías de Aplicación:** Describen conceptos que pertenecen a la vez a un dominio y a una tarea particular, por medio de la especialización de los conceptos de las ontologías de dominio y de tareas. Generalmente corresponden a roles que juegan las entidades del dominio cuando ejecutan una actividad.
- **Ontologías Genéricas o de Sentido Común:** Capturan conocimiento general acerca del mundo. Proveen nociones básicas y conceptos para cosas tales como espacio, tiempo, estado, eventos. Son válidas en varios dominios.

- **Ontologías Representacionales:** No se comprometen con ningún dominio en particular. Proveen entidades sin establecer que deberían representar, por lo tanto, definen conceptos para expresar conocimiento de manera orientada a objetos o a marcos de trabajo.
- **Ontologías de Dominio:** Capturan el conocimiento valido para un tipo particular de dominio (ej: electrónica, medicina, mecánica).
- **Ontologías de Métodos y Ontologías de Tareas:** Las primeras proveen términos específicos para métodos particulares de resolución de problemas, mientras que las segundas proveen términos para tareas específicas. Ambas proveen un punto de vista de razonamiento sobre conocimiento del dominio.

2.1.3.8 Arquitectura

La estructura interna y organización de un sistema multiagente están determinadas por la arquitectura. Las arquitecturas especifican cómo se descomponen los agentes en un conjunto de módulos que interactúan entre sí para lograr la funcionalidad esperada. Existe una amplia diversidad de propuestas (Wooldridge y Jennings 1999).

Tabla 4
Arquitecturas de SMA

Tipo de comunicación	Descripción
Sin comunicación	Los agentes pueden interactuar sin comunicarse, infiriendo las intenciones de otros agentes. Esta situación puede darse debido a fallos de hardware, a la imposibilidad de comunicarse o al deseo de que los agentes gocen de una mayor autonomía. Se supondrá que los agentes disponen de la información sensorial suficiente para poder inferir los objetivos e intenciones
Comunicación primitiva	La comunicación se restringe a un número de señales con interpretaciones fijas
Arquitectura pizarra	Estructura que consta de tres componentes: 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)
Paso de mensajes	Permiten el intercambio de mensajes entre agentes
Comunicación de alto nivel	Los agentes puedan razonar sobre las intenciones, deseos y objetivos de otros agentes y pueden comunicar deseos, objetivos e intenciones.
Interacción hombre máquina	Se consideran dos aproximaciones: Encapsular al agente humano modelando sus interacciones en un lenguaje de comunicación de agentes Aprovechar la tecnología Multiagente para simplificar las interfaces hombre-máquina.

Fuente: Elaboración propia

Los aspectos básicos que diferencia una arquitectura de otra son: el método de descomposición del trabajo en tareas particulares y la comunicación. La comunicación entre agentes es el mecanismo principal para gestionar su coordinación y coherencia, lo que permite responder a las interrogantes de qué, cómo y cuándo se comunican entre sí. La comunicación proporciona a los agentes el conocimiento necesario para desarrollar sus acciones con una visión menos local y poder sincronizarse con el resto de los agentes. Iglesias, C. (98) afirma que, una excesiva comunicación puede dar lugar a una sociedad de agentes burocráticos, cuya sobrecarga de comunicación sea mayor que el trabajo efectivo realizado. En la tabla 4 se distinguen diferentes formas de comunicación, que van desde la falta de comunicación hasta la comunicación de alto nivel y la interacción hombre máquina.

2.1.3.8.1 El modelo Pizarra

La arquitectura de 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.

Los Sistemas Pizarra (*Blackboard*) fueron los primeros sistemas cooperativos. Su principal objetivo es lograr un mecanismo flexible de resolución de problemas que permita dar soporte al *brainstorming* entre un conjunto de personas expertas que pretenden resolver un problema y que son incapaces de lograrlo de forma individual. La característica principal de estos sistemas es que están basados en un modelo de pizarra. Para Ramos (2000) este modelo constituye un modelo de resolución de problemas oportunista altamente estructurado que define la organización del conocimiento del dominio de un problema dado, además de los datos de entrada y soluciones parciales e intermedias necesarias para resolver dicho problema.

Históricamente, el modelo de pizarra surge con el sistema Hearsay-II, como menciona Lesser (1975) el cual propone una solución para coordinar procesos independientes de forma cooperativa en aras de resolver el problema del entendimiento del habla. El modelo de pizarra

es una descripción, a alto nivel, de una forma concreta de organización de un sistema computacional de la cual han surgido varias propuestas de implementación a lo largo del tiempo.

2.1.3.9 Metodologías para el desarrollo de SMA

2.1.3.9.1 Metodología GAIA

Gaia fue propuesta por Wooldridge el año 2000, Esta primera versión se creó con el objetivo de dar soporte al análisis y diseño de Sistemas Multi-Agente. Para esta metodología, un sistema Multi-Agente es visto como una organización computacional de agentes que interactúan entre sí para alcanzar un objetivo común de la aplicación:

- La etapa de análisis comprende los modelos de rol e interacción.
 - En el modelo de roles, para cada rol se especifica una plantilla compuesta de sus actividades, protocolos, permisos y responsabilidades.
 - Las actividades son funciones que puede llevar a cabo un agente por sí mismo.
 - En oposición a una actividad, un protocolo precisa de la interacción con uno o más roles.
 - Los permisos especifican de qué forma puede acceder un rol un a un recurso, estableciendo límites en su ámbito ejecución. Las responsabilidades expresan su nacionalidad y condiciones invariantes que deben cumplir en todo momento.
- En la fase de diseño se crean los modelos de agente, servicio y comunicación.
 - El modelo de agente, se agrupan los distintos roles en tipos de agente.
 - El modelo de servicio está compuesto por múltiples servicios que son bloques de funcionalidad derivados de las actividades los protocolos.
 - En el modelo comunicación, se definen las relaciones entre los diferentes agentes. Esta versión fue extendida por Zambonelli (2003) extendiendo la propuesta original con conceptos organizacionales.

La propuesta de esta tesis se desarrolla a partir de la extensión de Zambonelli.

2.1.3.9.2 AUML

Agente UML o AUML es un lenguaje de modelado gráfico basado en UML. Esta metodología provee distintos tipos de representación, cubre desde la descripción del sistema, los

componentes, la dinámica del sistema hasta el desarrollo. En Huhns (2004) se presentan los diagramas para la representación de agentes: protocolos de interacción, modelo de agentes, entre otros. Se expone en detalle la representación de cada agente del sistema, haciendo analogía entre los agentes reactivos y los deliberativos, incluyendo conceptos como los servicios y protocolos que soportan, sus objetivos, conocimientos, normas, deseos, intenciones, planes y acciones, como así también el lenguaje de comunicación que utiliza y con qué ontologías trabaja cada servicio.

2.1.3.9.3 Comparación de metodologías SMA

Tabla 5

Diagramas de análisis y diseño de algunas de las metodologías

	FASES DE ANALISIS	VISTAS O FASES DE DISEÑO
Kinny	Modelo de Agente Modelo de Interacción Modelos de creencias Objetivos y planes	Refinamiento de los modelos de análisis
AUML	Diagrama de casos de uso de agentes	Modelo de agentes Modelo de clases Modelo de roles
GAIA	Modelo de Roles Modelo de Interacción	Modelo de agente Modelo de servicios Modelo de conocimiento
Burneister	Modelo de agente Modelo de organización Modelo de cooperación	Refinamiento de los modelos de análisis
MAS-CommonKADS	Fase de conceptualización Modelo de organización Modelo de agente Modelo de tareas Modelo de la experiencia Modelo de coordinación y control	Diseño de red Diseño de agentes Diseño de plataforma
MASSIVE	Vista de tareas Vista de entorno Vista de sistema	Vista de Roles Vista de Interacción Vista de sociedad Vista de arquitectura Vista de sistema

TROPOS	Requerimientos iniciales Requerimientos finales (Modelos, actores y organizaciones)	Diseño arquitectónico (refinado y creación de agentes) Diseño detallado (Modelo interno de agentes)
MaSE	Captura de objetivos Aplicación casos de uso Transformación de roles Creación clases de agentes	Construcción de conversaciones Construcción de conversaciones Ensamblado clases de agente Diseño del sistema
MESSAGE	Modelo de organización Modelo de objetivos/tareas Modelo de Agente Modelo de Interacción Modelo de dominio	Refinamiento de modelos (Organización de Interacción) Modelo interno de agentes (Elección de la arquitectura)
MASINA	Modelo de inteligencia Modelo de coordinación Modelo de tareas Modelo de comunicación Modelo de agentes	

Nota: Elaborado a partir de la publicación de Julián y Botti (2003)

2.2 Marco Legal

El presente trabajo tiene como marco legal los siguientes documentos:

- a. Los Acuerdos de Basilea: son los acuerdos de supervisión bancaria o recomendaciones sobre regulación bancaria emitidos por el Comité de Basilea de Supervisión Bancaria. Están formados por los acuerdos Basilea I, Basilea II y Basilea III. Los cuales forman las bases y lineamientos de las diferentes leyes de los países en cuanto al sector financiero. Las recomendaciones del Comité de Basilea para la Supervisión Bancaria han contribuido en la modernización de la normativa boliviana vigente. En los últimos años, el Comité de Basilea emitió los Principios Básicos para una Supervisión Bancaria Efectiva, muchos de los cuales están, en mayor o menor medida, contenidos en la normativa boliviana vigente. Algunos otros, incluidos en normas con rango de ley, deben ser analizados al tratar los cambios establecidos por la implementación de la Ley N° 393 de Servicios Financieros de 21 de agosto de 2013.
- b. La Ley 393 de Servicios Financieros, esta Ley del Estado Plurinacional de Bolivia tiene por objeto regular las actividades de intermediación financiera y la prestación de los servicios financieros, así como la organización y funcionamiento de las entidades

financieras y prestadoras de servicios financieros; la protección del consumidor financiero; y la participación del Estado como rector del sistema financiero, velando por la universalidad de los servicios financieros y orientando su funcionamiento en apoyo de las políticas de desarrollo económico y social del país. Introduce las políticas para el riesgo sistema, la función de la Autoridad de Supervisión del Sistema Financiero (ASFI) para el control de la gestión de riesgo de las entidades financieras y la supervisión basada en riesgo.

- c. Recopilación de Normas para Servicios Financieros (RNSF): En el contexto de la Ley 393 la Recopilación de Normas para Servicios Financieros cuenta con el ordenamiento de la normativa aplicable a las Entidades de Intermediación Financiera (EIF), Empresas de Servicios Financieros Complementarios (ESFC) y Sociedades Controladoras de Grupos Financieros (SCGF), fue definido como uno de los objetivos básicos e iniciales para su posterior actualización. La Recopilación de Normas para Servicios Financieros (RNSF), documento que se pone a disposición de la colectividad financiera, responde al cumplimiento satisfactorio de dicho objetivo y contiene la compilación temática de toda la normativa vigente emitida desde 1987, año de la restitución de la ex Superintendencia de Bancos y Entidades Financieras actual ASFI, como organismo autónomo de regulación y control del sector financiero. La presente recopilación, contempla además las actualizaciones que han sido incorporadas en algunos textos, para su correcta aplicación, dentro del marco de lo dispuesto por la Ley N° 393 de Servicios Financieros y del ámbito moderno y globalizador del Comité de Basilea. Así, el objetivo de la RNSF es que tanto el Órgano de Control como las propias EIF,ESFC, SCGF y terceros interesados, cuenten con un documento único de consulta, que reúna toda la normativa prudencial y de control relativa a la constitución, funcionamiento y operación de éstas. El documento es de fácil uso por su estructura temática y permitirá a personas no especializadas en temas financieros, leer con facilidad toda la normativa aplicable a las EIF,ESFC y SCGF. Este documento cuenta en el Libro 3° REGULACIÓN DE RIESGOS con las normas aplicadas al Riesgo Operativo descritas en el Capítulo V. Toda nueva norma emitida por ASFI, incluyendo modificaciones a las contenidas en la presente Recopilación, será aprobada únicamente como incorporación o modificación a ésta.

Capítulo III METODOLOGÍA DE LA INVESTIGACIÓN

3.1 Métodos de investigación

Para el desarrollo de la tesis se emplea el tipo de investigación mixto. El método cualitativo permite describir las cualidades del modelo desarrollado y el método cuantitativo permitirá analizar los resultados de las encuestas de forma estadística.

3.2 Tipos de investigación

Descrito el problema propuesto y planteados los objetivos, el tipo de investigación que se propone realizar determina un estudio descriptivo, proyectivo y correlacional, de acuerdo con el registro de información y ocurrencia de los hechos.

3.2.1 Estudio descriptivo

El presente estudio se considera descriptivo porque como resultado de la investigación determina cuáles son las características propias de la institución financiera en estudio específicamente en cuanto a gestión de riesgo operativo se refiere.

3.2.2 Estudio proyectivo

La aplicación del estudio proyectivo consiste en la elaboración de un modelo, como solución a un problema o necesidad de tipo práctico de las IFDs, a partir del diagnóstico de las necesidades de incorporar Sistemas de Gestión de Riesgo Operativo, con base en los resultados del proceso investigativo.

3.2.3 Estudio de alcance correlacional

El presente estudio pretende responder a la pregunta de investigación, y como finalidad tiene conocer la relación o grado de asociación que exista entre el modelo de Sistema Multi Agente con respecto al proceso de desarrollo de sistemas de GRO para una IFD.

La utilidad principal de este estudio correlacional es saber cómo se comporta una variable al conocer el comportamiento de otras variables vinculadas, si dos variables están correlacionadas y se conoce la magnitud de la asociación.

3.3 Universo o población de estudio

- La investigación se realizará en la Institución Financiera de Desarrollo (IFD) Diaconía FRIF. Se trabajará en la regional del departamento de La Paz, específicamente en la ciudad de El Alto, para justificar esta decisión, se presentan los siguientes argumentos:
 - Diaconía FRIF, a pesar de ser una institución pequeña en relación con otras entidades del Sistema Financiero Nacional, ofrece la posibilidad de trabajar con datos en forma segura y transparente.
 - Diaconía FRIF es una de las Instituciones Financieras de Desarrollo que mayores avances ha realizado en cuanto a la gestión de riesgo operativo.
- Población: Personal del departamento de Sistemas y las unidades de Operaciones y Riesgo
- Se llevó a cabo un muestreo no probabilístico, debido a que los encuestados se seleccionaron por conveniencia de la población en cuestión.

3.4 Fuentes y diseño de los instrumentos de relevamiento de información

3.4.1 Fuentes de la investigación

Los datos obtenidos corresponden a la estructura actual Sistema de Riesgo Operativo y al Core financiero. No obstante, se emplearon datos de prueba.

Para el relevamiento de información del presente estudio se emplearán los siguientes documentos:

- Políticas Normas y Procedimientos de la institución caso de estudio.
- Recopilación de Normas para Entidades Financieras que se encuentran en el marco de regulación de la ASFI para la gestión de riesgo operativo y ley 393 de Servicios Financieros.
- Documentos del Comité Basilea I y II referentes al riesgo operativo

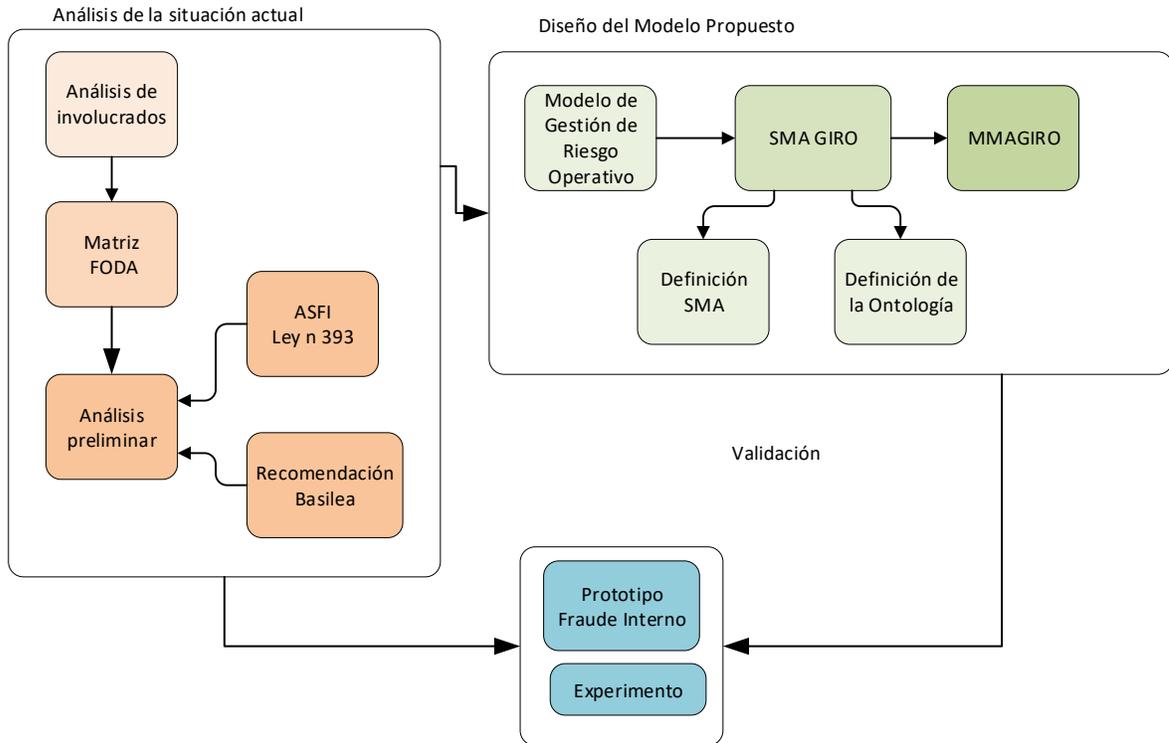
3.4.2 Diseño de los instrumentos de relevamiento de la información

Para el presente estudio se diseñaron instrumentos de recopilación de datos:

- Dirigido al personal de sistemas.
- Dirigido al personal de riesgo.

- Dirigido a estudiantes de Ingeniería de Sistemas de octavo semestre de la Universidad Salesiana de Bolivia.

En la Figura 2, se describe el diseño de solución planteado para el logro de los objetivos propuestos y la respectiva demostración de hipótesis.



*Figura 2 Diseño de la solución
Fuente: elaboración propia*

Se diseñaron tres etapas documentadas en el capítulo cuatro: en la primera se realiza el análisis de la situación actual a partir del análisis de involucrados donde se identifica los principales protagonistas en una IFD, luego se realiza la Matriz FODA con el personal involucrado con el fin de obtener un diagnóstico claro sobre la Gestión de Riesgo Operativo en la IFD, la recopilación de información de la recomendación Basilea y las directrices emitidas por la Asfi son indispensables para identificar correctamente los elementos involucrados, así como definir correctamente los procesos diseñados.

La segunda etapa consiste en el diseño del modelo, el cual a su vez consta de tres componentes: El modelo de GRO, el diseño del SMA y finalmente el modelo MMAGIRO que

añade los primeros dos componentes al diseño de fases de desarrollo de sistemas de Gestión Integral de Riesgo Operativo propuesto.

La validación permite verificar la correctitud de la solución propuesta. El prototipo permitirá probar el modelo propuesto, el experimento se completa con el análisis de opinión de los involucrados respecto a la solución, como herramienta de validación se emplea la encuesta.

Capítulo IV MARCO PRÁCTICO

4.1 METODOLOGÍA DEL DESARROLLO DE LA SOLUCIÓN

4.1.1 Análisis para el modelo propuesto

Antes de diseñar el Modelo Multiagente para la Gestión Integral de Riesgo Operativo, se realizó el análisis de la situación actual, esta fase comprende: análisis de involucrados, matriz de análisis FODA (Fortalezas, Oportunidades, Debilidades y Amenazas), recopilación de la ley Nro 393 y recomendaciones Basilea documentadas en el capítulo dos, este proceso se aprecia en la figura 3.

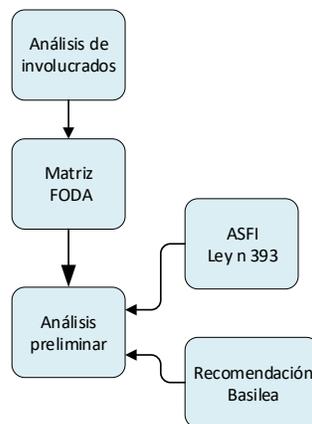


Figura 3 Análisis de la situación actual
Fuente: elaboración propia

Para el análisis de involucrados se describió una estructura jerárquica de una IFD, como se muestra en la figura 4:

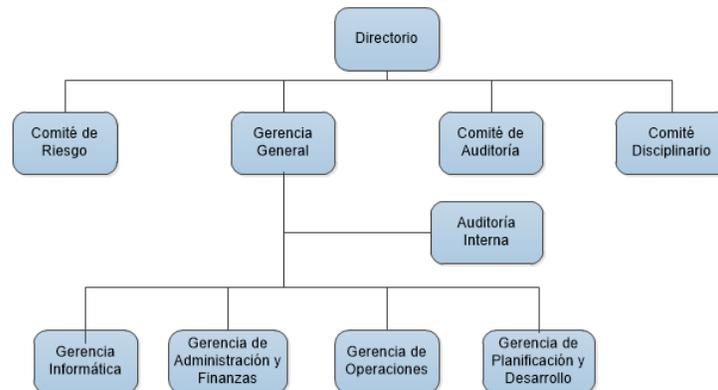


Figura 4 Organigrama de una IFD.

Elaboración propia, con información obtenida, como resultado de las entrevistas con el personal de la IFD

A continuación, se detallan las responsabilidades de los involucrados, respecto a la gestión de riesgo operativo:

a) Nivel táctico y estratégico.

Crear una cultura organizacional con principios y valores de comportamiento ético que priorice la gestión eficaz del riesgo operativo.

Aprobar las políticas y estrategias relacionadas con la administración y gestión del riesgo operativo y establecer los principios para definir, evaluar, seguir y controlar o mitigar este tipo de riesgos.

Recibir información pertinente de forma periódica que complemente la gestión activa del riesgo operativo.

b) Gerencia de operaciones.

Vigilar que el personal de la unidad de riesgos cumpla y haga cumplir de manera correcta y oportuna las políticas, procesos, procedimientos, metodologías, y estrategias de administración integral de riesgo operativo.

Vigilar que auditoría interna realice la evaluación sobre el cumplimiento del sistema de administración integral de riesgos.

Recibir información pertinente de forma periódica que complemente la gestión activa del riesgo operativo.

c) Gerencia general.

Implementar las políticas, procesos y estrategias definidas por el consejo de administración en relación con la administración de riesgos.

Facilitar la información al área de auditoría interna y al consejo de vigilancia para que puedan realizar la evaluación y seguimiento respecto a la implementación de la administración integral de riesgos.

Poner en práctica, el marco para la gestión del riesgo operativo aprobado por el consejo de administración.

d) Auditoría interna.

Apoyar el trabajo de la gerencia, actuando como facilitador para la identificación y evaluación de los riesgos; provee entrenamiento sobre riesgos, controles y respuesta a riesgos, a través de su experiencia en gestión de riesgos. Apoya en la consolidación de reportes sobre riesgo y coordina el mantenimiento. Sin embargo, el auditor interno: no

determina o establece el apetito de riesgo, no impone procesos para gestionar riesgos y controles, no toma decisiones referentes a la respuesta al riesgo, y no toma la responsabilidad en la gestión de riesgos, es decir debe mantener su independencia.

De encontrar deficiencias en los controles, auditoría interna, propondrá los controles que considere adecuados. Dichos controles, serán evaluados con el usuario experto, el responsable de la unidad de riesgos, el responsable del proceso y el responsable de la unidad de calidad y procesos.

e) Unidad de riesgos.

Identificar, medir, controlar, mitigar, monitorear y comunicar la exposición al riesgo operativo.

Diseñar las políticas y el proceso de administración del riesgo operativo.

Establecer las directrices para la evaluación de riesgos y controles, en coordinación con el área de control interno.

Analizar las matrices de riesgo y establecer los lineamientos de análisis para las evaluaciones de riesgo y control.

Proporcionar información relacionada a los eventos de riesgo y control.

Para aplicar el modelo desarrollado, las entidades deberán cumplir con características mínimas las cuales se detallan a continuación:

1. Procesos levantados a nivel de subproceso.
2. Inventario de procesos
3. Su estructura organizacional debe contar mínimamente con las áreas de: Comité de Riesgos y Comité de auditoría interna.

Estas características se cumplen en las IFDs, según las Normas de Servicios Financieros ASFI libro 3 Título I, Sec 4, Pag: 1-6.

Para el análisis realizado se entrevistó al personal de informática, operaciones y auditoría interna de la IFD. Con la información recopilada se elaboró la siguiente matriz de Análisis FODA de **Gestión de Riesgo Operativo (GRO)**.

Tabla 6
Matriz FODA

FORTALEZAS	OPORTUNIDADES
<ul style="list-style-type: none"> • Aumenta el valor para los accionistas a través de la mejora en la Gestión de Riesgo Operacional. • Mejora la comunicación a los “<i>stakeholders</i>”¹ con una gestión de riesgos de excelencia. • Crea ventajas competitivas a través de un alineamiento entre el apetito de riesgo, capital disponible y crecimiento deseado. • Prepara a la entidad para situaciones adversas económicas y/o de mercado que permitan evitar pérdidas financieras. • Menor requerimiento de capital a través de mejoras técnicas de medición del RO • La identificación del riesgo y del riesgo inherente en los diferentes procesos con los que cuenta una entidad ayuda a mejorar el control interno de esta. • La administración del riesgo operativo ayuda a reforzar y estandarizar el conocimiento que los empleados de una entidad tienen con respecto a los procesos que deben ejecutar en sus tareas diarias. • En la implementación de riesgo operativo contribuye a mejorar la eficiencia y efectividad de los procesos organizacionales permitiendo definir estrategias de mejoramiento continuo, brindándole un manejo sistémico a la entidad. • La implementación de la gestión de riesgo operativo produce por lo general maximización de resultados en una entidad. • La gestión de riesgo operativo genera una cultura de autocontrol y autoevaluación en la entidad. • La implementación de una gestión de riesgo operativo en una entidad reduce las pérdidas operaciones logrando así un incremento del capital y mejor distribución de valor para los accionistas. 	<ul style="list-style-type: none"> • Hace que la entidad fortalezca su reputación contribuyendo con las oportunidades de crecimiento o expansión de una entidad. • La implementación del riesgo operativo contribuye en mejorar la calificación de riesgo de las entidades. • La implementación de riesgo operativo contribuye al crecimiento organizaciones de las entidades que lo gestionan. • Como resultado de esto las calificadoras externas mejoran su calificación como reconocimiento a la GRO.

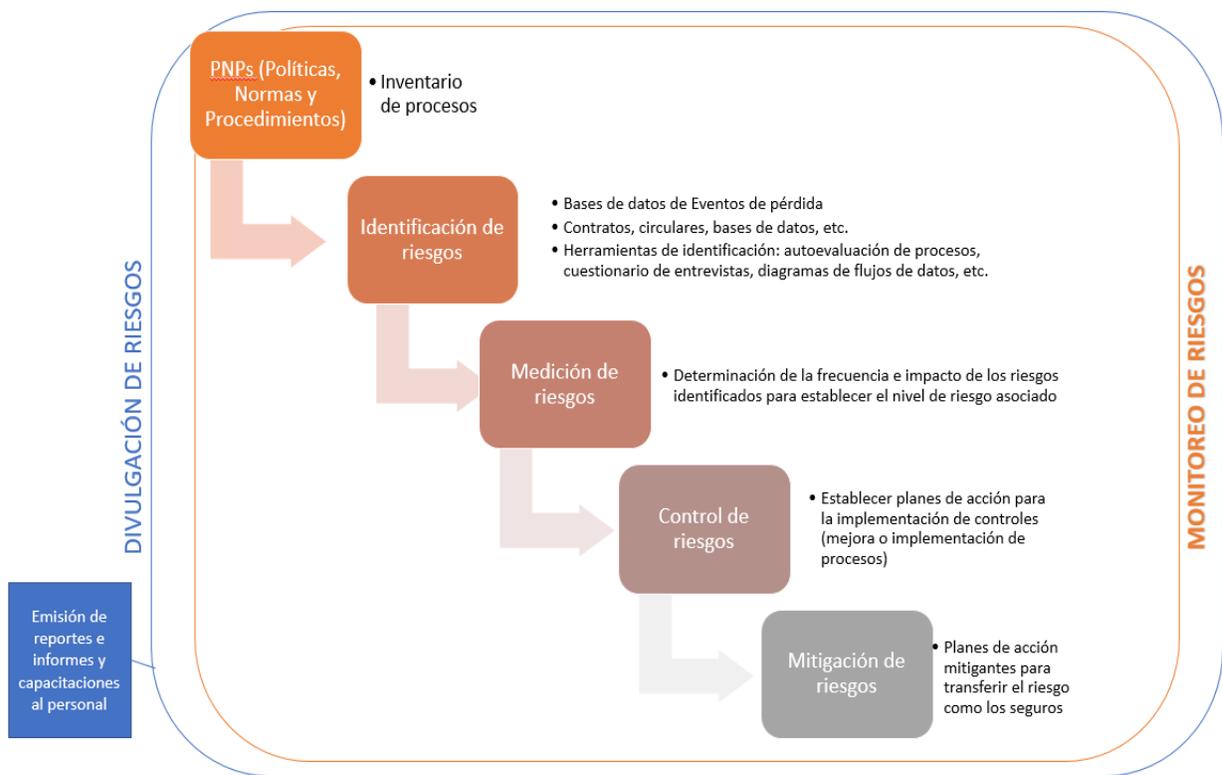
¹ “*stakeholders*” Partes interesadas

DEBILIDADES	AMENAZAS
<ul style="list-style-type: none"> • El riesgo operativo requiere de una gran inversión de tiempo en la elaboración de los procesos al considerar los posibles riesgos que tiene cada proceso. • La dificultad de mitigar o transferir algunos riesgos. • Falta de comprensión de la alta gerencia sobre el riesgo operativo, el ciclo del riesgo operativo y los procesos de implementación en una entidad, lo que dificulta la toma de decisiones para la implementación del riesgo operativo. • Capacitación superficial y con poco seguimiento para la implementación de procesos, metodologías de riesgo operativo. • Dificultad en poder concientizar al personal sobre la importancia del Riesgo Operacional. • Creación de indicadores inadecuados por procesos difusos y complicados de calcular. • Dificultad para la captura de eventos de riesgo por la existencia de diferentes actores y diferentes líneas de negocio. • El mayor reto al que se enfrentan las entidades es el de lograr implantar una verdadera cultura de RO, que incentive a las comunidades a comunicar sus propios errores y fomente la transparencia de las instituciones (Schulze, 2014). • Necesidad de contar con buenas prácticas de gestión y supervisión de RO, como precondition para aplicar metodologías de medición (Comité Basilea II). 	<ul style="list-style-type: none"> • Cambios contantes en los procesos de una entidad por efecto de un mundo globalizado. • Imposibilidad de cumplir con los objetivos en la implementación de riesgo operativo por cambios en factores externos a la entidad, tales como: cambios políticos, modificaciones a las normas del sector, cambios macroeconómicos, etc. • Posibilidad de utilizar modelos internos está sujeta a la aprobación del supervisor, junto con el cumplimiento de los requerimientos cualitativos adicionales.

NOTA: *Elaboración propia, realizada con ayuda del personal de operaciones de la IFD. Esta información se constituye en una guía para la administración del riesgo operativo*

4.1.2 Modelo de Gestión de Riesgo Operativo

Los pasos para la Gestión del Riesgo Operativo se elaboraron a partir de la literatura seleccionada: del Comité Basilea II los documentos “Nuevo Acuerdo de Capital” y “Sanas prácticas para la gestión y supervisión del riesgo operativo” y la Recopilación de Normas de Servicios Financieros (RNSF) de ASFI y la Ley 393 Ley de Servicios Financieros, además con el apoyo del juicio de especialistas y expertos, mediante entrevistas con los dueños del proceso y su personal operativo, se diseñó el siguiente submodelo.



*Figura 5 Proceso de Gestión de Riesgo Operativo
Elaboración propia*

La plataforma de una IFD se caracteriza por su complejidad y magnitud, el modelo propuesto no reemplazará los Sistemas de Información empleados, el Modelo Multiagente se diseña como un componente de apoyo a la estructura tecnológica existente, lo que se ilustra en la figura 6:

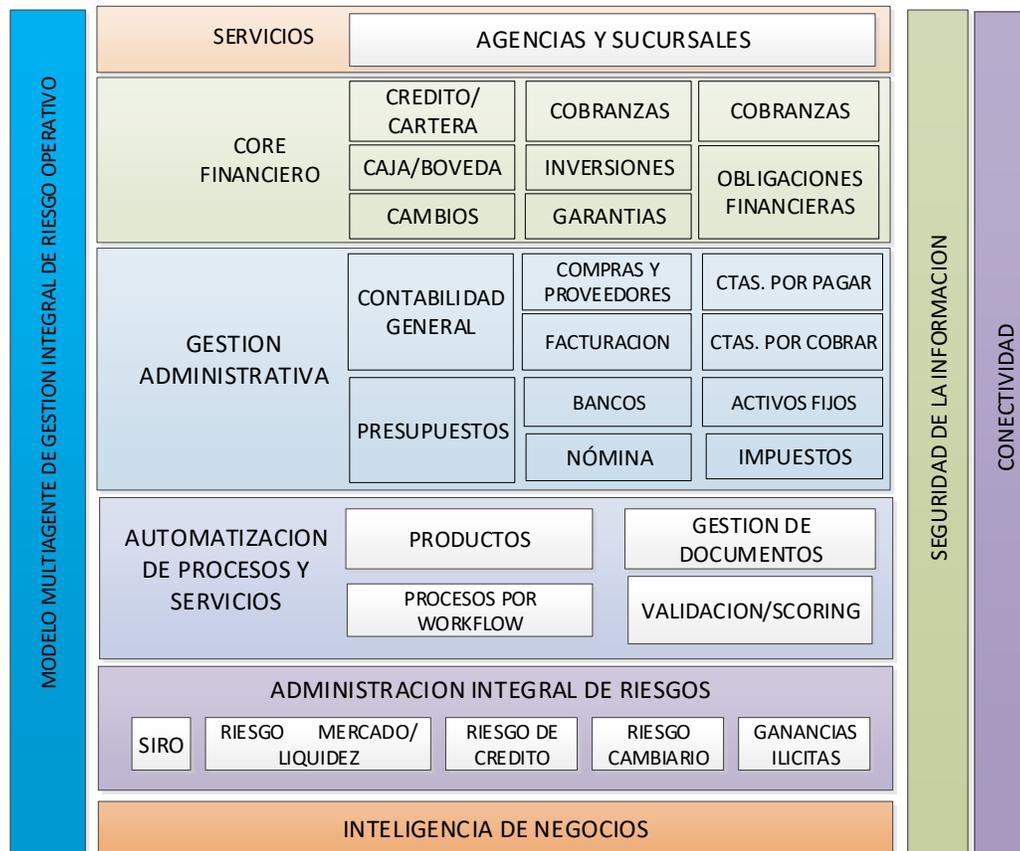


Figura 6: El Modelo Multiagente como parte de la estructura tecnológica de la IFD.
Elaboración propia

4.1.3 Definición formal del Sistema Multiagente

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

$$SMA_{GIRO} = (E, O, A, R, Op, L)$$

Que se define como:

- E representa el 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. Definiendo el entorno como un conjunto de estados discretos $E = \{e, e', \dots\}$, donde cada estado e representa el entorno en un momento dado. Y e puede ser descrito por un conjunto finito de variables accesibles que miden los fenómenos que ocurren en el entorno.

- O es un conjunto finito de instancias de conceptos pasivos (Ontologías) que representan la información y conocimiento relacionados con el estado e y con el proceso. Estas instancias forman parte del conjunto de Políticas, Normas y Procedimientos para la Gestión de Riesgo Operativo.
- A es el conjunto de agentes que participan en la GRO. Cada agente trabajara con las instancias y conceptos de O con el fin del logro de sus objetivos y los del sistema en general. A es el conjunto de conceptos activos definidos en la Ontología.
- R es un conjunto finito de instancias de relaciones entre conceptos pasivos (que representan dependencia) y entre conceptos activos y pasivos (que representan quien crea que).
- O_p es un conjunto finito de operaciones tipificadas como tareas que tienen que ser realizadas por los agentes dentro de la GRO.
- L es el conjunto de las denominadas leyes del universo que son comunes para el entorno E .

El conjunto E , está compuesto por los siguientes elementos:

e : Políticas, Normas y Procedimientos y toda la documentación que se tenga para la realización de procesos operativos en todas las tareas y actividades que se realizan en la entidad financiera para realizar su actividad. Adicionalmente se toma en cuenta el inventario de procesos correspondiente a cada uno de los procedimientos planteados en la entidad.

e' : La estructura organizacional que abarca a los niveles jerárquica con los que cuenta la entidad, el personal que son los responsables de ejecutar los procesos, los PAF con los que cuenta la entidad y la asignación de personal y responsabilidades que se tiene en el puesto de trabajo.

e'' : El sistema de control interno que debe estar plasmado en el inventario de procesos para su ejecución y debe ser controlado por los diferentes propietarios de la información, así como por las revisiones que prepararán las unidades de control.

e''' : La Plataforma Tecnológica que nos proporciona la información que combinada con los procesos contribuye a percibir lo que el agente debe hacer. La Plataforma Tecnológica mínima que una entidad financiera debe estar compuesta por: CORE Financiero que se

encargue de administrar, registrar y controlar las operaciones activas y pasivas que se tengan según las líneas de negocio pudiendo gestionar los productos y servicios, el Sistema Administrativo Organizacional que permita darnos la información necesaria sobre los activos, el personal siendo el factor clave la evaluación de personal, el control de asistencia, el registro de cambios en su estado civil, profesión entre otros, la administración de cuentas por cobrar, cuentas por pagar y otros procesos adicionales y el Sistema de gestión de filas que contribuye en ver la atención a los consumidores financieros en cuanto a tiempo, a tipo de transacción que realizan, así como los importes que se manejan en cada transacción, etc.

La caracterización del entorno se logra a través de las siguientes propiedades:

Observabilidad. El agente obtiene información precisa, completa y actualizada respecto a:

- Registro de reclamos y soluciones
- Detalle de transacciones (tipo de transacción, cajero, hora y fecha).
- Detalle de solicitudes de crédito registradas por oficial, fecha, hora y tipo de crédito
- Detalle de crédito registradas por oficial, fecha, hora y tipo de crédito y su relación con las garantías y documentos dejados en custodia
- Información de funcionarios; asignación de activos, manejo de caja chica
- Datos del personal: tipo de contrato, escala salarial, sueldos, anticipos, vacaciones y otros.
- Tiempos de espera para la atención al consumidor financiero, tiempos de atención al consumidor financiero, eficiencia de las estaciones de trabajo y otros, todo relacionado con el personal que realizó la atención y el PAF donde se registró el ticket.
- Registro de empleados codificados en el Sistema de Registro de Mercado Integrado de ASFI
- Registros de eventos de riesgo operativo pasados e incidentes.

Sin embargo, no todo el entorno es observable. La conducta de las personas que de una manera u otra influye en la ocurrencia de eventos de riesgo operativo, constituyen una limitante para el SMA_{GIRO} propuesto.

Determinismo. El entorno se considera no determinístico puesto que el entorno no está totalmente delimitado por el estado actual. Los ambientes no determinísticos representan un problema de mayor complejidad.

Dinamismo. El ambiente es dinámico debido a los eventos no controlables.

Tabla 7

Descripción Rendimiento, Entorno, Actuadores, Sensores del SMA_{GIRO}

Tipo de agente	Medidas de rendimiento	Entorno	Actuadores	Sensores
Agente Divulgación	Resultados de la evaluación de conocimientos de Frecuencia de errores	No determinista	Visualizar las actividades, sugerencias, correcciones Respuestas	Periféricos de entrada Programación de evaluaciones
Agente de Identificación	Casos identificados	No determinista	Matriz de riesgos	Algoritmo de búsqueda
Agente de Monitoreo	Indicadores de monitoreo	No determinista	Acciones de detección y corrección de procesos y procedimientos para gestionar los riesgos	Algoritmo de búsqueda
Agente de Control	Seguimiento de los indicadores de monitoreo e identificación	No determinista	Acciones de supervisión del proceso	Algoritmo de búsqueda
Agente de Medición	Resultado del análisis de riesgo	No determinista	Resultados de la medición de riesgos	Algoritmo de búsqueda

NOTA. Elaboración propia, se tomó como base Russel (2004):

4.1.3.1 Ontología para la gestión integral de riesgo operativo

En esta fase se diseña la ontología descrita en el capítulo dos. La ontología contiene los conceptos relativos a cada fase de la GRO, la cual posee un conjunto de propiedades de descripción y un conjunto de relaciones que establecen las dependencias entre las propiedades.

A continuación, se realiza la siguiente definición formal de O_{GIRO} :

$$O_{GIRO} = \langle C, R, A^o, L \rangle$$

Donde:

C es el conjunto de conceptos

R es el conjunto de relaciones

A^o es el de axiomas.

En la siguiente tabla se definen estos conjuntos:

Tabla 8
Estructura Ontológica

C	{C ₁ , C ₂ , C ₃ , C ₄ , C ₅ , C ₆ , C ₇ , C ₈ , C ₉ , C ₁₀ , C ₁₁ , C ₁₂ , C ₁₃ , C ₁₄ , C ₁₅ , C ₁₆ , C ₁₇ , C ₁₈ , C ₁₉ , C ₂₀ , C ₂₁ , C ₂₂ , C ₂₃ , C ₂₄ , C ₂₅ , C ₂₆ , C ₂₇ , C ₂₈ , C ₂₉ , C ₃₀ , C ₃₁ , C ₃₂ , C ₃₃ , C ₃₄ , C ₃₅ , C ₃₆ , C ₃₇ , C ₃₈ , C ₃₉ }
R	{Γ ₁ , Γ ₂ , Γ ₃ , Γ ₄ , Γ ₅ , Γ ₆ , Γ ₇ , Γ ₈ , Γ ₉ , Γ ₁₀ , Γ ₁₁ , Γ ₁₂ , Γ ₁₃ , Γ ₁₄ , Γ ₁₅ , Γ ₁₆ , Γ ₁₇ , Γ ₁₈ , Γ ₁₉ , Γ ₂₀ , Γ ₂₁ , Γ ₂₂ , Γ ₂₃ , Γ ₂₄ , Γ ₂₅ , Γ ₂₆ , Γ ₂₇ , Γ ₂₈ , Γ ₂₉ , Γ ₃₀ , Γ ₃₁ , Γ ₃₂ , Γ ₃₃ , Γ ₃₄ , Γ ₃₅ , Γ ₃₆ , Γ ₃₇ , Γ ₃₈ , Γ ₃₉ }
A ^o	∅

Fuente: Elaboración propia

El lenguaje se define como:

$$L = \{LC, LR, F, G\}$$

Donde:

L^C el conjunto de elementos denominados entradas léxicas de conceptos

L^R el conjunto de elementos denominados entradas léxicas de relaciones

F las referencias a conceptos

G las referencias a relaciones.

Además, se cumplen las siguientes propiedades:

- $\forall x r_x(c_x) = c_y$, todo concepto está relacionado con otro concepto.
- $\forall x 0 \leq x \leq 25$, $L_R(x) = 'Es-un_x'$ es la entrada léxica empleada para representar dentro de la taxonomía jerárquica las relaciones de herencia existente entre dos conceptos.
- $\forall x 1 \leq x \leq 39$, $F_x(L^{cx}) = c_x$ es la entrada léxica asociada a cada concepto de C .
- $\forall x 1 \leq x \leq 43$, $G_x(L^{rx}) = r_x$ es la entrada léxica asociada a cada relación.

Tabla 9
Lenguaje Ontología OGIRO

L ^C	{'FactorDeRiesgo', 'Fraude', 'FraudeInterno', 'FraudeExterno', 'RelacionesLaborales', 'SeguridadEnElPuestoDeTrabajo', 'IncidenciasEnElNegocio', 'FallosEnElSistema',
----------------	--

	<p>'DañosAActivosMateriales', 'ClientesProductosYPrácticasEmpresariales', 'EjecuciónEntregaYGestiónDeProcesos', 'LíneasDeNegocio', 'ServiciosDeAgencia', 'BancaMinorista', 'LineasDeNegocio', 'ServiciosDeGerencia', 'BancaMinorista', 'AdministraciónDeActivos', 'BancaComercial', 'Microcrédito', 'Inversiones', 'EventoDePérdida', 'ActividadDeGestión', 'RiesgoOperativo', 'RiesgoLegal', 'RiesgoTecnológico', 'ActividadDeGestión', 'Identificación', 'Monitoreo', 'Medición', 'Control', 'Divulgación', 'AgenteIdentificación', 'AgenteMonitorea', 'AgenteMedición', 'AgenteControl', 'AgenteDivulgación', 'Organización', 'Sistemas_Internos', 'Tecnología', 'Personas', 'Procesos'}</p>
L ^R	<p>{ Es_un0, Es_un1, Es_un2, Es_un3, Es_un4, Es_un5, Es_un6, Es_un7, Es_un8, Es_un9, Es_un10, Es_un11, Es_un12, Es_un13, Es_un14, Es_un15, Es_un16, Es_un17, Es_un18, Es_un19, Es_un20, Es_un21, Es_un22, Es_un23, Es_un24, Es_un25, Parte_de1, Parte_de2, Parte_de3, Parte_de4, Asociado_a1, Asociado_a2, Realiza1, Realiza2, Realiza3, Realiza4, Realiza5, Origina, Puede_provocar, Gestiona, Causa, Tiene_asociado }</p>
F	<p>{ F1, F2, F3, F4, F5, F6, F7, F8, F9, F10, F11, F12, F13, F14, F15, F16, F17, F18, F19, F20, F21, F22, F23, F24, F25, F26, F27, F28, F29, F30, F31, F32, F33, F34, F35, F36, F37, F38, F39 }</p>
G	<p>{ G1, G2, G3, G4, G5, G6, G7, G8, G9, G10, G11, G12, G13, G14, G15, G16, G17, G18, G19, G20, G21, G22, G23, G24, G25, G26, G27, G28, G29, G30, G31, G32, G33, G34, G35, G36, G37, G38, G39, G30, G41, G42, G43 }</p>

Fuente: Elaboración propia

En el siguiente diagrama se muestran los conceptos y relaciones de la ontología O_{GIRO} propuesta:

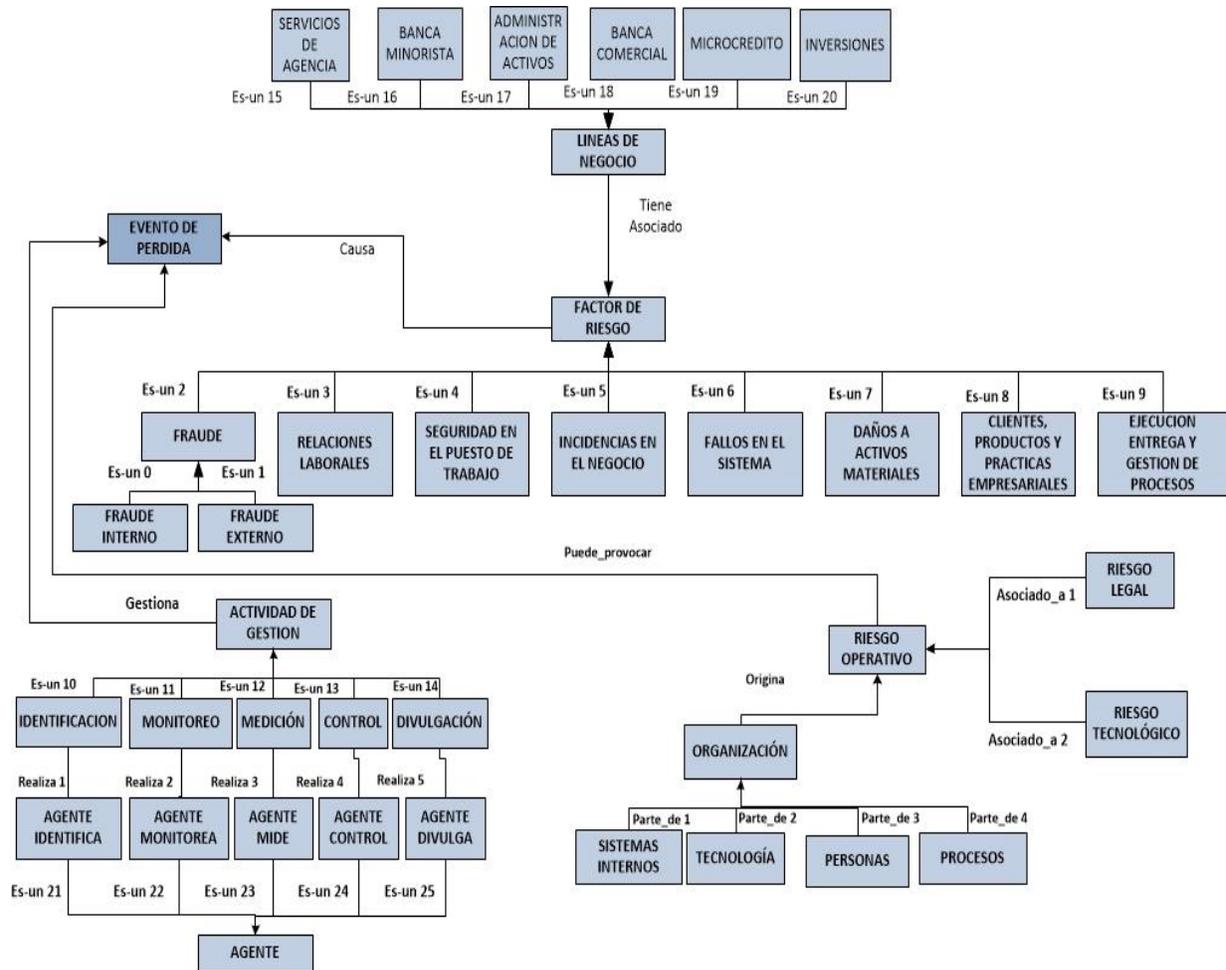


Figura 7: Diagrama de conceptos y relaciones de la ontología MMA-GIRO
Elaboración propia

En la anterior figura se identifican dos tipos de conceptos: pasivos y activos. Los conceptos pasivos son aquellos que albergan los hechos/información/conocimiento propios de los PNP institucionales y los conceptos activos constituyen el conjunto de instancias creadas de a partir de los hechos pasivos, el conjunto de hechos generados en la propia institución y que son sujeto de análisis en el procesos de gestión del riesgo operativo constituyen los conceptos activos son aquellos cuya entrada léxica contiene la palabra Agente.

Una aclaración respecto a las Líneas de Negocio, es que algunas de estas actividades son propuestas por el Comité de Basilea, pudiendo la IFD ajustar las mismas a sus propias características, abriendo subcategorías si fuera necesario. Según recomendación de la ASFI estas líneas de negocio pueden servir para reportar pérdidas actuales y proyectar pérdidas esperadas

por riesgo operativo, e incluso para posteriormente asignar capital económico, tal como sugieren las mejores prácticas internacionales.

4.1.3.2 Arquitectura de comunicación

La comunicación entre agentes se realiza a partir de la definición del esquema pizarra. La comunicación entre agentes, proveída por el esquema pizarra definida como una estructura se presenta en la figura 8, que contiene los posibles enlaces de comunicación existentes entre los diferentes tipos de agentes enumerados dentro del MMA_{GIRO}. Se puede apreciar que la principal tarea la ejerce el agente encargado de gestionar la pizarra, denominado agente control pizarra.

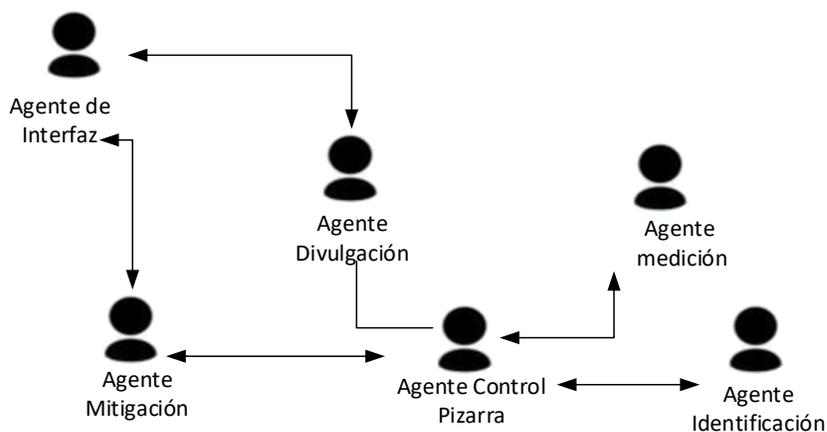


Figura 8 Comunicación entre agentes
Elaboración propia

El comportamiento básico de los agentes consiste en consultar periódicamente el esquema pizarra (excepto el agente Identificación). El agente que inicia el proceso de GRO es el Agente identificación, el mismo realiza el rastreo de transacciones de la estructura tecnológica de la IFD y comienza el proceso de GRO, este agente es el primero en registrar sus observaciones en la pizarra, este proceso concluye cuando de Agente Divulgación elabora los informes correspondientes y entregados jerárquicamente a los involucrados. No obstante, el Agente Identifica escucha permanentemente las transacciones, lo que implica que permanentemente se realice la GRO.

La estructura pizarra, se compone de un conjunto de secciones y se representa en figura 9, donde además se aprecia la participación de los agentes.

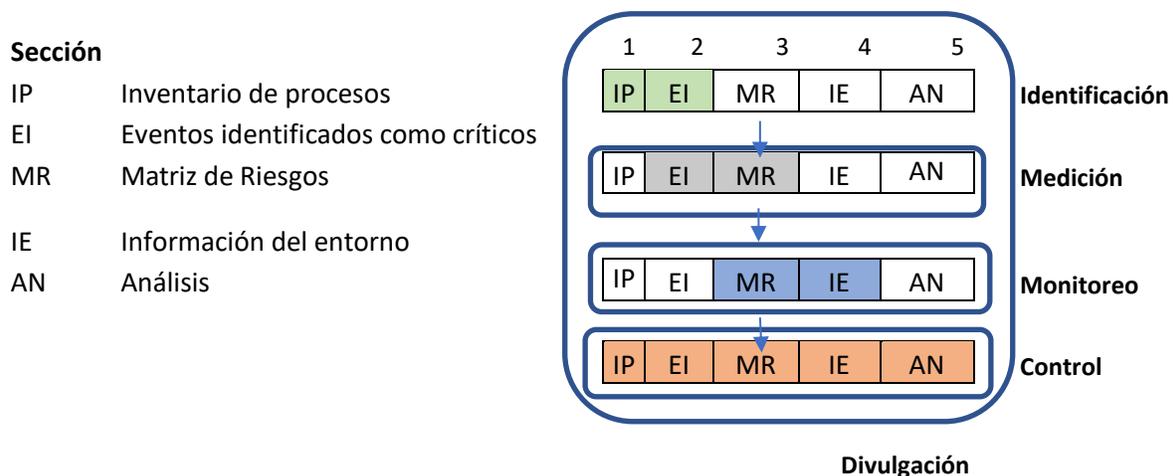


Figura 9 Capas de la pizarra
Elaboración propia

Los parámetros globales del SMA_{GIRO} que constituyen parte de la sección del modelo de comunicación pizarra, se describen en la tabla 10.

Tabla 10
Parámetros globales del modelo SMA_{GIRO}

Parámetro	Descripción
<i>LineaDeNegocio</i>	Líneas de negocio
<i>DueñosDeLaInformacion</i>	Dueños de la información
<i>Cuestionarios</i>	Cuestionarios y resultados de los cuestionarios
<i>InventarioDeProcesos</i>	Inventarios de procesos
<i>EventosDeRiesgoRecopilados</i>	Resultado de los eventos de riesgo recopilados
<i>IndicadoresEventosDePerdida</i>	Resultados de relacionar los indicadores con los eventos de pérdida

Fuente: Elaboración propia

En la tabla 10 se presentan los conjuntos de datos que se almacenan en la *pizarra* y que, al pasar por las diferentes fases del modelo, son consultados y/o modificados, tanto por los usuarios como por los agentes propuestos. En la tabla 11 se muestra el inventario de procesos con el conjunto de los posibles eventos de riesgo, además de su correspondiente frecuencia e impacto.

El inventario de procesos mínimamente contiene los siguientes datos (Art. 5 RNSF I3 t5 c2 s2): denominación del proceso, periodicidad de su ejecución, nivel de automatización, grado de descentralización, responsables de su ejecución, revisión y aprobación, documentación de entrada y de salida del proceso, productos y servicios que genera el proceso y clasificación como proceso crítico o no.

Tabla 11
Inventario de procesos

Identificador	Campo
URP	Unidad responsable del proceso
NP	Nombre del proceso
RRA	Responsable de revisión y aprobación
RE	Responsable de su ejecución
CP	Código del proceso
TP	Tipo de proceso
NA	Nivel de automatización
PEP	Periodicidad de la ejecución del proceso
DEP	Documentación de entrada del proceso
DSP	Documentación de salida del proceso
SGP	Servicios que genera el proceso
CI	Clientes internos
CE	Clientes externos
MR	Manual de referencia
FR	Fecha de registro
CP	Criticidad del proceso
LN	Línea de Negocio
VP	Versión del proceso
FAP	Fecha de aprobación del proceso
GD	Grado de descentralización
MTE	Monto tratado en la ejecución del proceso
DET	Detalle
RESP	Responsable
TEE	Tiempo Estimado de Ejecución

Elaboración propia

Los agentes interactúan de forma directa con los repositorios de datos descritos en la tabla 12:

Tabla 12
Repositorios de datos con los interactúan los agentes

Repositorios de datos	Descripción	Agentes involucrados	Lee	Escribe
Inventario de Procesos	Contiene los datos básicos de los procesos y su criticidad respecto al riesgo operativo	Identificación	Tipos de operación, frecuencia y nivel de riesgo	
		Medición	Criticidad	
Core financiero	Contiene las operaciones de depósitos y préstamos de dinero	Identificación	Transacciones con posibilidad de riesgo	

Gestión integral de riesgo operativo	Contiene las tablas que permiten dar soporte a las operaciones de GRO	Identificación		Historial de posibles eventos de riesgo
		Medición		Matriz de riesgo
		Control	Registro de eventos	
Gestión administrativa	Contiene información administrativa de la IFD, incluye información del personal: Evaluación de desempeño y personalidad, historial financiero y familiar	Medición	Datos del personal: personales, de evaluación de desempeño y personalidad, información financiera, familiar	
Base de Conocimiento	Contiene la ontología y la base de reglas que permiten evaluar los riesgos por funcionario, tecnología y otros (legal)	Monitoreo	Conocimiento de valoración de eventos de riesgo	

Fuente: Elaboración propia

En la figura 10 se muestra una instancia del esquema de comunicación entre agentes y su interacción sobre la plataforma tecnológica de la IFD, específicamente el caso de gestión de riesgo de eventos de tipo fraude interno.

En esta figura se aprecia la Base de Conocimientos, la misma contiene información de múltiples fuentes, entre ellas:

- Conocimientos de expertos
- Información del personal
- Estadísticas
- Procesos internos
- Inventario de procesos
- Historial de eventos de riesgo

El Sistema de Gestión Administrativa contiene información laboral y personal de los Recursos Humanos. La pizarra se constituye en un elemento de comunicación entre los agentes, que realizan de forma independiente sus respectivas actividades.

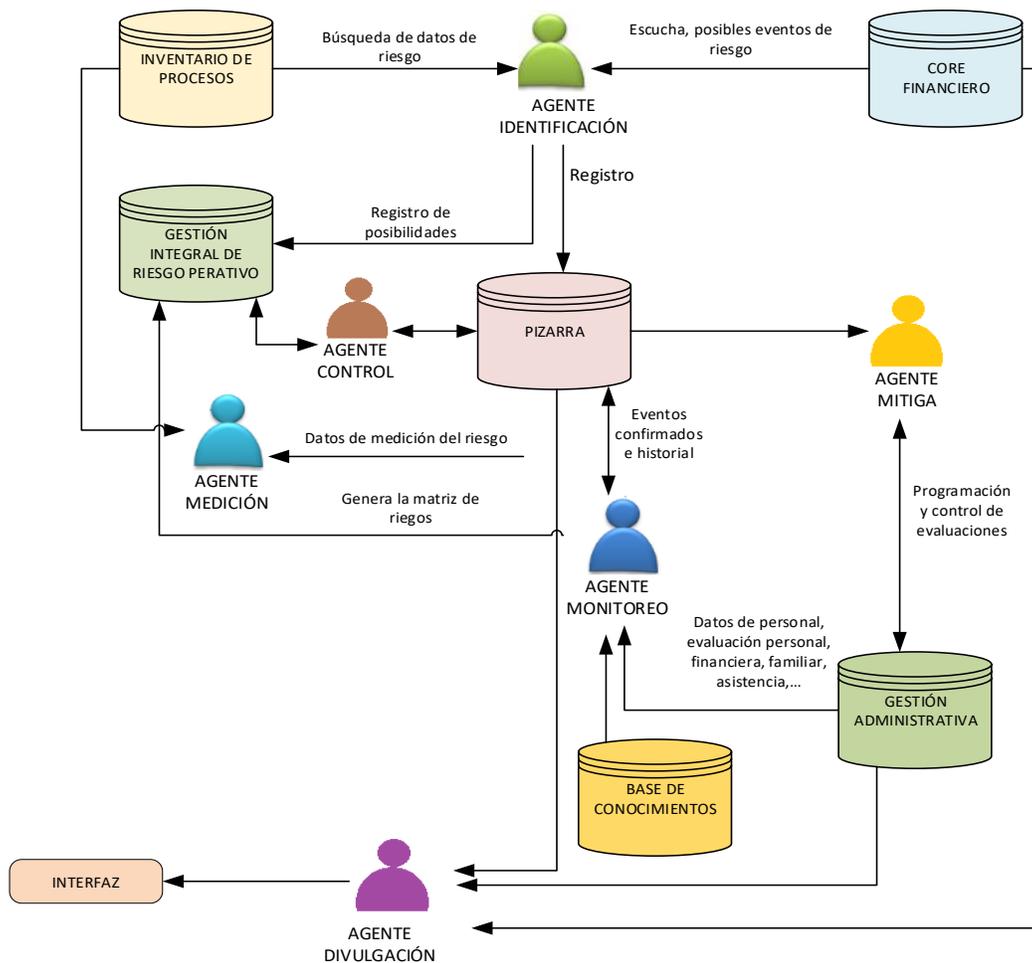


Figura 10 Esquema de comunicación entre agentes sobre la tecnología de la IFD – Riesgo fraude interno
Elaboración propia

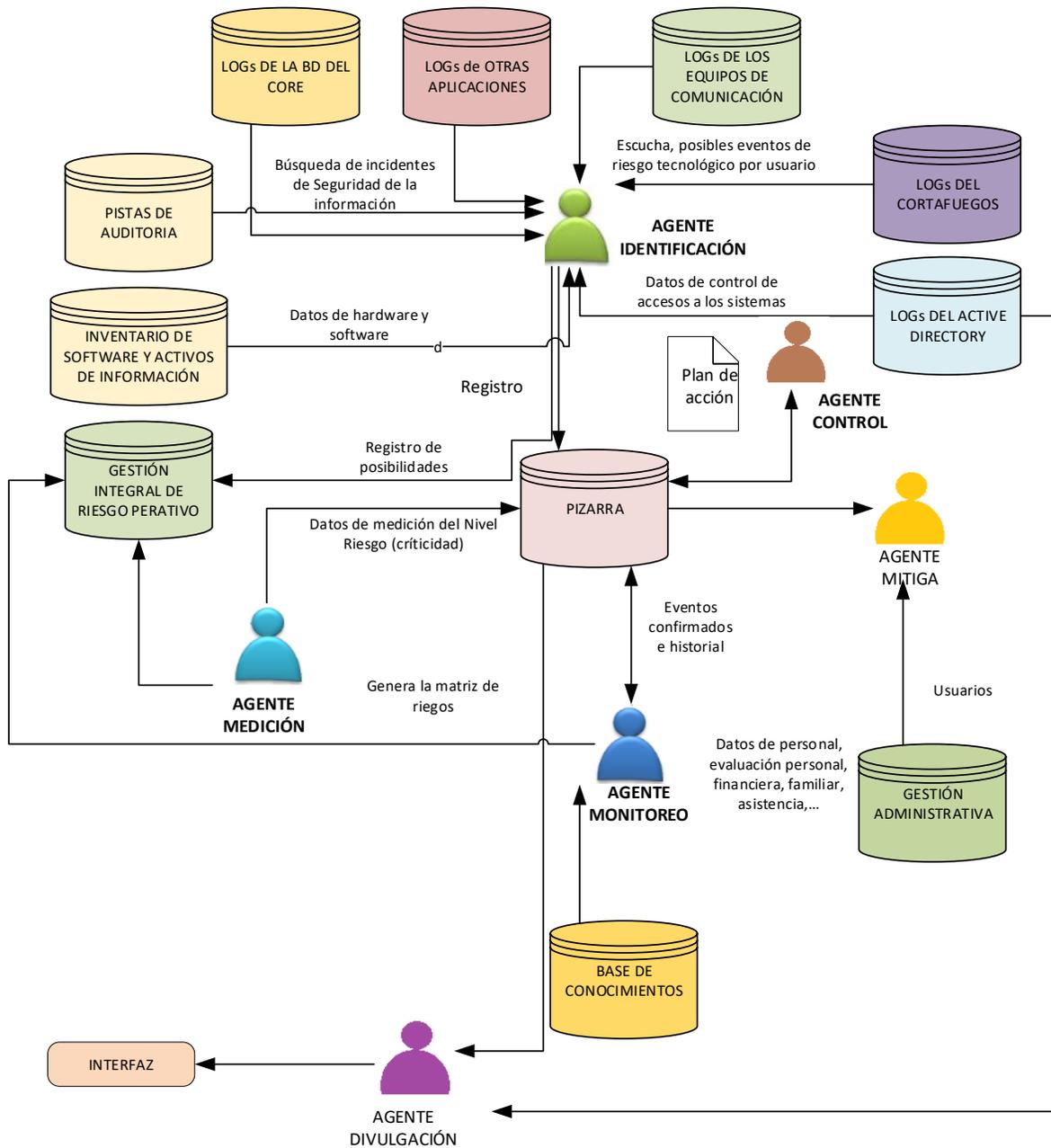


Figura 11 Esquema de comunicación entre agentes sobre la tecnología de la IFD – Riesgo fallas tecnológicas
Elaboración propia

El tipo de riesgo operativo que se origina por fallos en tecnología implica desde la identificación de logs generados por equipos hasta que el informe respectivo es generado por el agente de divulgación.

En la Figura 12 se representa la gestión de fallas por procesos.

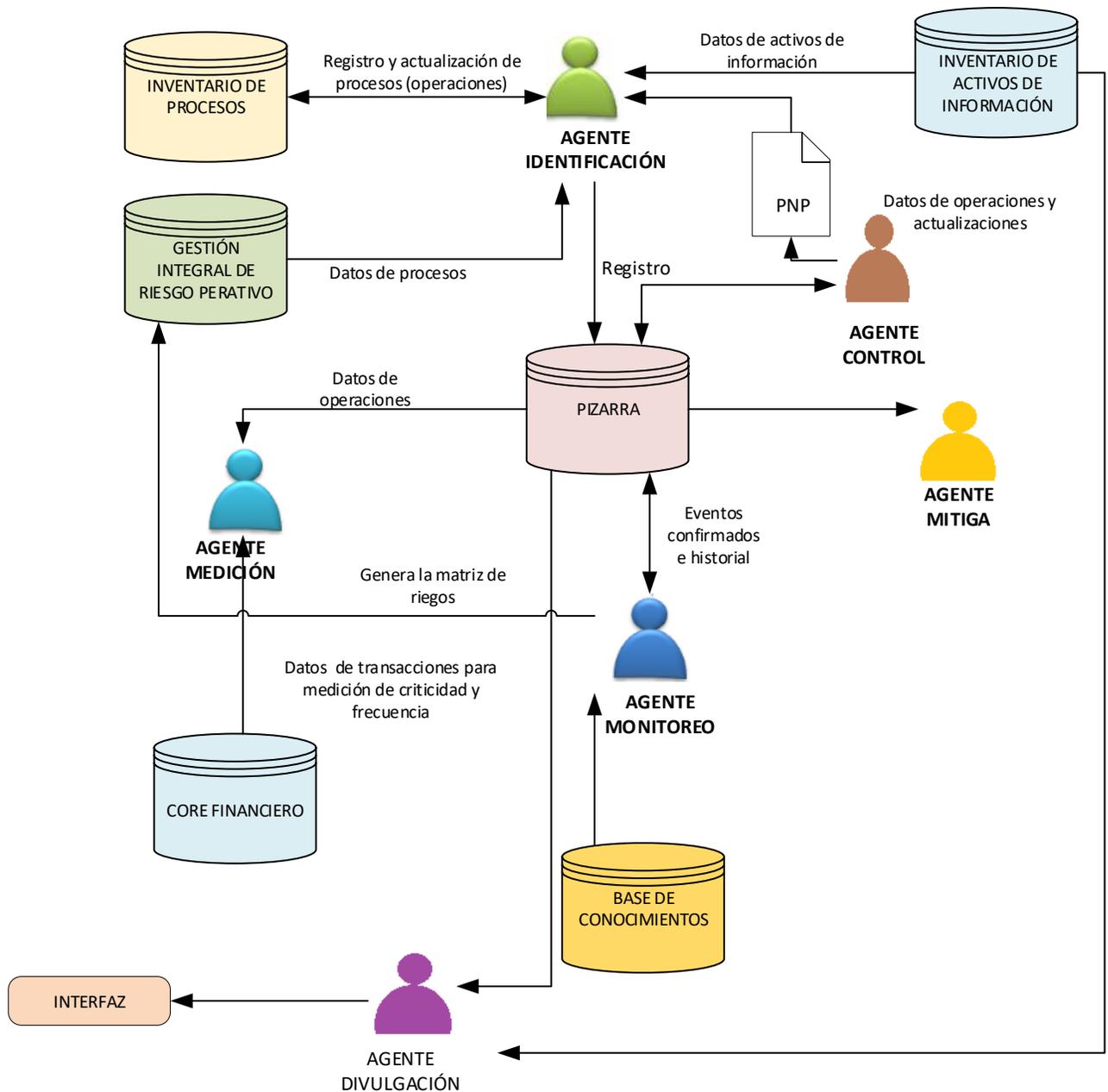


Figura 12 Esquema de comunicación entre agentes sobre la tecnología de la IFD – Riesgo fallas por procesos
Elaboración propia

Como se aprecia en las figuras 10, 11 y 12 la pizarra es el componente principal de comunicación de los agentes propuestos en el modelo.

4.1.3.3 Subprocesos de SMAGIRO

Los subprocesos de MMGIRO son:

- Identificación
- Medición
- Control
- Monitoreo
- Divulgación
- Mitigación

4.1.3.3.1 Subproceso de Identificación

En la fase de identificación se capturan registros de los eventos originarios del riesgo operativo, como: procesos internos, personal, tecnologías de información y factores externos, con estos resultados se realiza un mapeo con la base de datos de inventario de procesos. A partir de los resultados se registra la información de “historial de posibles riesgos” y “Pizarra de identificación de riesgos”.

El modelo propuesto comprende las siguientes fases del subproceso de identificación:

- Seleccionar las líneas de negocio
- Definir los dueños de la información
- Diseño de cuestionarios de autoevaluación
- Diseño del inventario de procesos
 - Categorizar los posibles eventos de pérdida por la línea de negocio
 - Definir niveles de severidad para los eventos de pérdida
 - Identificar niveles de riesgo
 - Identificar identificadores
 - Definir niveles
 - Establecer relaciones y orden de importancia
- Llenado de los inventarios de procesos
- Recopilación de eventos de riesgo
 - Recopilación de posibles eventos de riesgo de los diferentes procesos financieros

- Registro de denuncias de posibles eventos de riesgo
- Registro de posibles eventos de riesgo identificados en las revisiones de las áreas de control (Auditoría Interna, Auditoría Externa, Unidad Riegos)
- Establecer la relación entre los indicadores y los eventos de pérdida

En la siguiente tabla se muestra las responsabilidades en cada una de las fases:

Tabla 13

Fases de identificación: responsables y descripción

Fase	Responsable	Descripción
Seleccionar las líneas de negocio	Gerencia	El sistema presenta la interfaz
Definir los dueños de la información	Gerencia	El sistema presenta la interfaz
Diseño de cuestionarios de autoevaluación	Unidad de Riesgo Operativo	El sistema presenta la interfaz
Diseño del inventario de procesos <ul style="list-style-type: none"> ○ Categorizar los posibles eventos de pérdida por la línea de negocio ○ Definir niveles de severidad para los eventos de pérdida ○ Identificar niveles de riesgo ○ Identificar identificadores ○ Definir niveles ○ Establecer relaciones y orden de importancia 	Unidad de Riesgo Operativo	El sistema presenta la interfaz
Llenado de los inventarios de procesos	Dueños de la Información Agentes de identificación de procesos	El sistema presenta la interfaz El agente de identificación asiste al Usuario en el llenado del inventario de procesos.
Recopilación de eventos de riesgo <ul style="list-style-type: none"> ○ Recopilación de posibles eventos de riesgo de los diferentes procesos financieros ○ Registro de denuncias de posibles eventos de riesgo ○ Registro de posibles eventos de riesgo identificados en las revisiones de las áreas de control 	Agente de identificación de Dueños de la información Auditoría Interna, Auditoría Externa, Unidad Riegos	El sistema presenta la interfaz El agente realiza la búsqueda de eventos de RO
Establecer la relación entre los indicadores y los eventos de pérdida	Unidad de Riesgos	El sistema presenta la interfaz

Fuente: Elaboración propia

4.1.3.3.2 Subproceso de medición

El concepto de medición se refiere al proceso de estimar o cuantificar las pérdidas en las que podría incurrir la IFD por riesgo operativo, a nivel de línea de negocio, actividad, producto, área en particular, conjunto de actividades o portafolio. Para ello, la IFD puede recurrir al uso de metodologías y técnicas diversas, siendo algunas de tipo cualitativo, basadas en opiniones de expertos, y otras de carácter cuantitativo, orientadas a estimar el riesgo a un nivel dado de confianza, debiendo combinar ambas para lograr una mejor medición de este riesgo.

El Comité de Basilea propone cuatro métodos alternativos para la cuantificación de las pérdidas por riesgo operativo, y su correspondiente requerimiento de capital:

- Método del indicador básico (MIB)
- Método estándar (ME)
- Método estándar alternativo (MEA)
- Método de medición avanzado (AMA)

La elección del método empleado depende de la IFD.

4.1.3.3.3 Subproceso de control

La IFD debe evaluar el funcionamiento y la existencia de controles internos diseñados para la gestión de este riesgo.

Tabla 14

Fases del subsistema de control del modelo propuesto: responsables y descripción

Fase	Responsable	Descripción
Evaluación del inventario de procesos ○ Revisión de criticidad de procesos ○ Establecimiento de puntos de control	Unidad de Riesgo Operativo	El sistema presenta la interfaz
Registro de indicadores de cumplimiento	Unidad de Riesgo Operativo	El sistema presenta la interfaz El agente de control asiste al Usuario en el llenado de formularios de control.
Reportes que reflejen la diferencia entre las pérdidas reales y las pérdidas proyectadas, por tipo de evento y línea de negocio, para distintos horizontes de tiempo.	Unidad de Riesgo Operativo Agente de control	El sistema presenta la interfaz El agente de control asiste al Usuario en el llenado de formularios de control.
Seguimiento a encuestas de autoevaluación	Unidad de Riesgo Operativo Agente de control	El sistema presenta la interfaz El agente de control asiste al Usuario en el llenado de formularios de control.

Fuente: Elaboración propia

El seguimiento puede realizarse a través de procesos integrados a las operaciones usuales y/o mediante evaluaciones periódicas separadas, con el objeto de proveer información al Directorio u órgano equivalente y a la Alta Gerencia, acerca de las deficiencias o desviaciones encontradas.

- Evaluación del inventario de procesos
 - Revisión de criticidad de procesos
 - Establecimiento de puntos de control
- Registro de indicadores de cumplimiento
- Reportes que reflejen la diferencia entre las pérdidas reales y las pérdidas proyectadas, por tipo de evento y línea de negocio, para distintos horizontes de tiempo.
- Seguimiento a encuestas de autoevaluación

En la siguiente tabla se muestra las responsabilidades en cada una de las fases:

Los procesos que ameritan ser enfocados en el análisis, principalmente son:

- Procesos que hayan sido identificados como debilidades en las encuestas de autoevaluación.
- Procesos involucrados en los reportes de pérdidas, donde se registra además el punto de control.
- Procesos que hayan sido identificados como críticos en las encuestas de autoevaluación y demás procesos de la EIF.

Como producto del análisis y evaluación de estos procesos, se emitirán recomendaciones a las áreas de negocio, operativas, sistemas, y otras. Los agentes de control trabajaran con el personal de la Unidad de Riesgos, proveyendo conocimientos y sugerencias de etapas anteriores, esto permitirá sugerir la implementación de mecanismos de control y seguimiento para verificar el cumplimiento de dichas recomendaciones.

La Unidad de Gestión de Riesgos debe tener la posibilidad de realizar un monitoreo continuo de los niveles de exposición al riesgo operativo y del cumplimiento de los límites de tolerancia definidos por la IFD.

4.1.3.3.4 Subproceso de monitoreo

La IFD establece mecanismos para el continuo monitoreo de riesgos, es decir, el establecimiento de procesos que ayuden a detectar y corregir rápidamente deficiencias en las

políticas, procesos y procedimientos para gestionar el riesgo operativo. El alcance abarca todos los aspectos y etapas de la gestión de riesgos, en un ciclo completo, acorde con la naturaleza de los riesgos y el volumen, tamaño y complejidad de las operaciones.

El modelo propuesto, presenta las siguientes fases:

- Generación y evaluación de reportes de exposición: reportes en los que se evalúen los distintos indicadores de medición del riesgo operativo, bajo diferentes escenarios y supuestos. Estos reportes deberán posibilitar la incorporación de filtros personalizados por distintas variables.
- Guías para la gestión de riesgos, se llevará, además, el control y seguimiento de las pérdidas reales con respecto a las pérdidas proyectadas mediante indicadores de cumplimiento.
- Establecimiento de indicadores meta
- Costos de pérdida

4.1.3.3.5 Subproceso de divulgación

Consiste en la distribución de información apropiada, veraz y oportuna, relacionada con la IFD y sus RO, tanto al Directorio u órgano equivalente, como a la Gerencia y al personal pertinente. Se hace extensible a interesados externos, tales como: clientes, proveedores, reguladores y accionistas.

4.1.3.3.6 Subproceso de mitigación

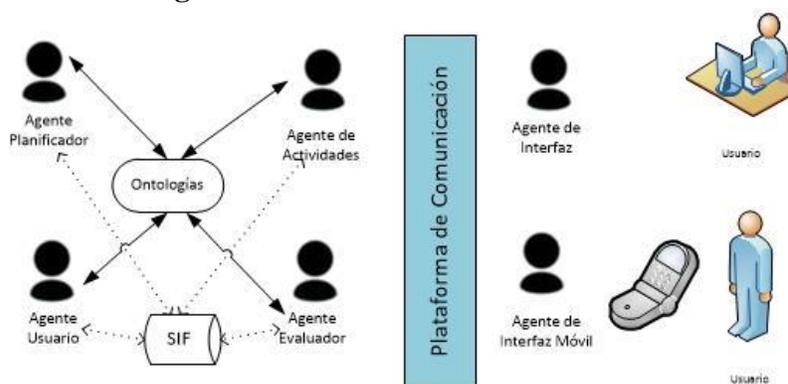


Figura 13 Modelo SMA pedagógico para la divulgación de RO apoyado
Elaboración propia

El riesgo operativo puede ser mitigado de las siguientes formas:

- a) Implementación de planes de continuidad del negocio y contingencias

- b) Cursos de capacitación a funcionarios
- c) Seguros tradicionales

El agente de mitigación se propone como una estructura de SMA de aprendizaje descrito en la figura 13. Para el diseño del SMA de aprendizaje, se toma como base el diseño de un Sistema Tutor Inteligente, cuyas fases son las siguientes:

- a. Especificación de la estructura organizacional
- b. Identificación de componentes principales del Modelo del Dominio
- c. Identificación de componentes principales del Modelo del Estudiante
- d. Selección de estrategias de planificación
- e. Identificación de los actores que participaran en el sistema
- f. Diseño del modelo SMA pedagógico adaptativo y sensible al contexto

4.1.4 Modelo Multiagente de Gestión Integral de Riesgo Operativo

A continuación, se presenta el modelo MMA GIRO en la Figura 14, el cual se diseña a partir de la propuesta de hibridación de GAIA y AUML descritos en el capítulo dos.

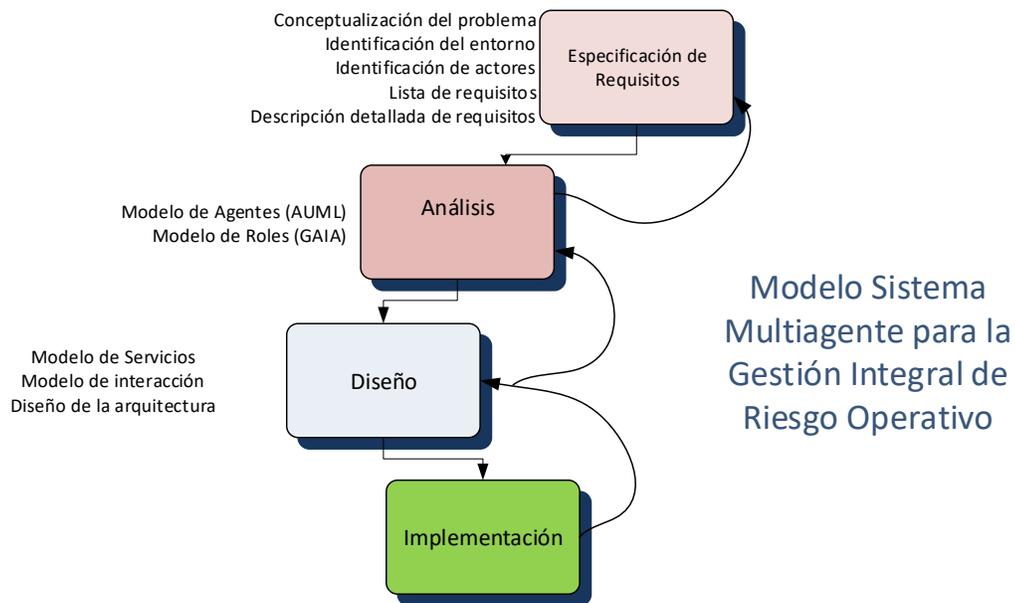


Figura 14: Fases del Modelo MA GIRO
Elaboración propia

4.1.4.1 Especificación de requisitos

La especificación de requisitos es la primera fase del modelo, en esta etapa se espera que el o los desarrolladores comprendan con claridad las especificaciones del software que se desarrollará. La especificación de requisitos propuesta consta de los siguientes componentes:

- *Conceptualización del problema*: Esta tarea consiste en la definición conceptual del problema. La información recolectada se plasma en la siguiente tabla:
- *Identificación de actores*
- *Características del entorno*
- *Lista de requisitos*
- *Descripción detallada de requisitos*

El proceso de especificación de requisitos se describe en la figura 15:

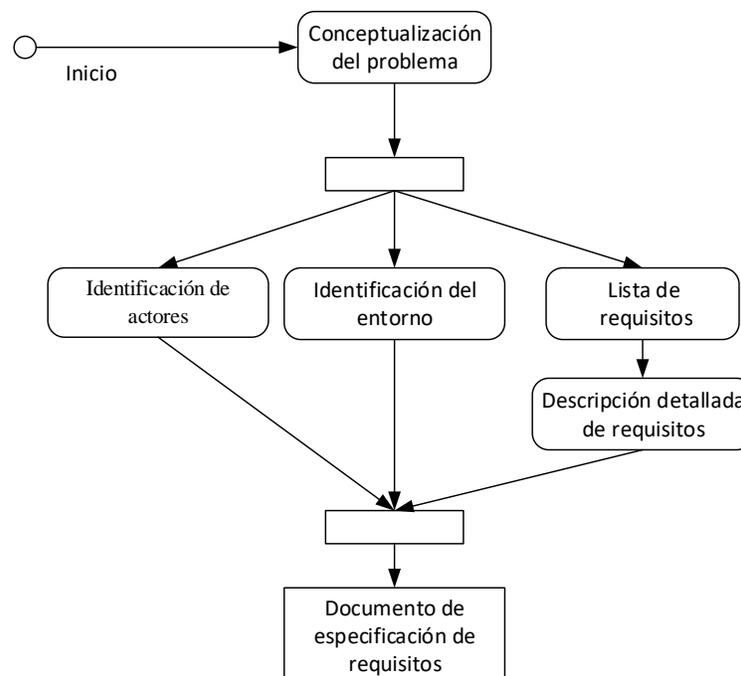


Figura 15: Especificación de requisitos
Elaboración propia

4.1.4.2 Análisis

- *Modelo de agentes.* En la metodología AUML, los agentes se definen utilizando diagramas de agentes, como se aprecia en la tabla 13.

Tabla 15
Diagrama de Agente (AUML)

«Agente»
Roles
Diagrama de estado 1, Diagrama de estado 2
Atributo 1, Atributo 2
Capacidades, servicios
Protocolo 1: rol, Protocolo 2: rol
Organización 1: rol, Organización 2: rol

Fuente: Elaboración propia

De acuerdo con el modelo de agentes propuesto en este trabajo, se consideran agentes deliberativos. Para ello se toman en cuenta los siguientes conceptos: roles, servicios que ofrecen, descripción del protocolo de comunicación, planes, objetivos, acciones y conocimiento (creencias). Teniendo en cuenta el rol descrito en el modelo de roles, se describen las características de los agentes para luego mostrar el modelo de agentes.

- *Modelo de roles:* El modelo de roles (*roles model*) identifica los roles que tienen los agentes dentro del sistema multiagente. Un rol queda definido en base a cuatro atributos: responsabilidades, permisos, actividades y protocolos.
 - *Las responsabilidades* determinan la funcionalidad y se dividen en propiedades de viveza y seguridad. Las primeras establecen las tareas que el agente debe llevar a cabo mientras que las segundas establecen los invariantes que deben cumplirse en su realización o al finalizar las mismas. Además, los permisos son los derechos de acceso a recursos que tiene el rol para llevar a cabo sus responsabilidades.
 - *Las actividades* son los cálculos que realiza el rol y que no requieren de interacción alguna con otro agente.
 - *Los protocolos* definen la forma en que un rol puede interactuar con otros roles.

El modelo de roles permite identificar los roles principales de cada agente. Cada rol puede verse como una descripción abstracta de la función esperada de una entidad en particular. Además, cada rol tiene asociados:

- *Atributos*: responsabilidades, está relacionado con el verbo 'hacer', cada agente se crea para hacer algo.
- *Permisos*: relacionados al tipo y cantidad de recursos que puede explotar el agente cuando tiene ese rol.

Se llena la siguiente tabla:

Tabla 16

Diagrama de rol

Diagrama de rol:
Descripción:
Protocolos y actividades:
Permisos
Responsabilidades:
Seguridad
Fuente: Elaboración propia

En la figura 16 se representa esta fase:

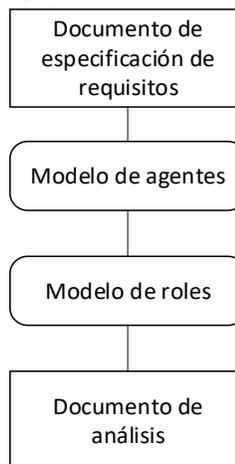


Figura 16: Fase de análisis del MMAGIRO
Elaboración propia

4.1.4.3 Diseño

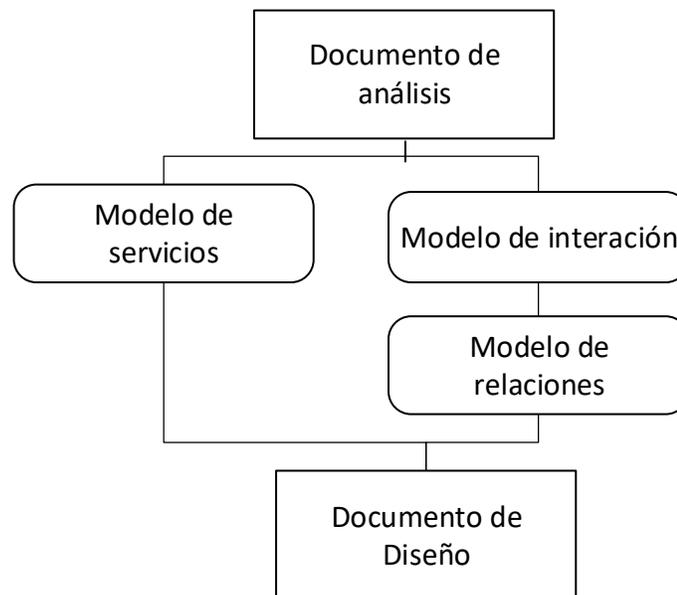
En la fase de diseño se definen:

- *Modelo de servicios*: El objetivo de este modelo es identificar los servicios asociados con cada rol de agente y especificar las propiedades principales de cada uno de ellos identificando sus entradas, salidas, precondiciones y postcondiciones. El conjunto de

servicios se obtiene a partir de los protocolos, actividades y responsabilidades de los roles

- *Modelo de interacción:* En el modelo de interacciones se detallan las dependencias y relaciones existentes entre los diferentes roles que han sido identificados dentro del Modelo de Roles.
- *Modelo de relaciones:* En el Modelo de Relaciones se determinan los posibles enlaces de comunicación existentes entre los diferentes tipos de agentes enumerados dentro del Modelo de Agentes.

La fase se representa en la figura 17.



*Figura 17: Fase de diseño del MMAGIRO
Elaboración propia*

4.1.4.4 Implementación

En esta fase se realizan los algoritmos, el diseño de pantallas y el diseño de comunicación.

Este capítulo no se elaboró con la intención de ser una guía exhaustiva y exclusiva de los procedimientos que deben realizarse para la gestión Integral del Riesgo operativo aplicando SMA, se trata de una referencia que ayude a entender la aplicación del modelo MMAGIRO.

4.1.5 Aplicación del MMAGIRO para el riesgo operativo de tipo fraude interno

A continuación, se aplica el modelo MMAGIRO, desarrollado en el anterior punto, por la magnitud de la Gestión del Riesgo Operativo, se toma como caso de estudio el Evento Fraude Interno, puesto que en este evento se puede apreciar la interacción de todos los elementos del modelo.

4.1.5.1 Especificación de requisitos

4.1.5.1.1 Conceptualización del problema

Tabla 17

Conceptualización del problema: Fraude

Subsistema: Fraude
Concepto: Acción contraria a la verdad y a la rectitud, que perjudica a la persona contra quién se comete. Acto tendente a eludir una disposición legal en perjuicio del Estado o de terceros. Delito que comete el encargado de vigilar la ejecución de contratos públicos, o de algunos privados, confabulándose con la representación de los intereses opuestos.
Referencia: RAE 22 ed.
Implicaciones: Manipulación, falsificación o alteración de registros o documentos. Malversación de activos. Supresión u omisión de los efectos de ciertas transacciones en los registros o documentos. Registro de transacciones sin sustancia o soporte. Aplicación mala de políticas contables.
Clasificación: Se denomina fraude interno a las pérdidas como consecuencia de actos fraudulentos intencionales, o de robo que involucra al personal, así como incumplimiento de leyes y políticas internas (de la financiera). El fraude interno se realiza con la intención financiera clara de malversación de activos de la empresa. El segundo tipo de fraude, es la presentación de información financiera fraudulenta como acto intencionado encaminado en alterar las cuentas anuales.

Fuente: Elaboración propia

Tabla 18

Conceptualización del problema: Fraude Interno

Subsistema: Fraude Interno
Las entidades de Intermediación tienen la obligación de implementar mecanismos efectivos de control operativo para evitar situaciones de fraude interno y externo. En el marco de la prudente administración de riesgo operativo, el directorio u órgano equivalente aprobará políticas y procedimientos para identificar y controlar los factores que podrían provocar fallas en los procesos operativos, cuyos impactos afectarían negativamente a los objetivos institucionales causándole a la entidad daños y pérdidas económicas. Especial atención merecerán los factores de riesgo operativo asociados a la sofisticación de los servicios financieros, la modernización continua de la tecnología y las telecomunicaciones, la incursión de nuevos mercados y las innovaciones financieras, que dan lugar a la creación de nuevos productos y servicios

Se refiere a los actos de intento de fraude, malversación de fondos o evasión de las regulaciones, leyes o políticas de la organización. Los ejemplos incluyen el empleo malintencionado de la información, hurto del empleado y negociación interna de valores a cuenta propia de un trabajador.

Referencia: Ley 393 Artículo 453 (GESTIÓN DE RIESGO OPERATIVO)

Ejemplos:

- Hurto, extorsión, malversación y robo.
- Actividad no autorizada
- Utilización de cheques sin fondos.
- Destrucción maliciosa de activos
- Falsificación
- Apropiación indebida de activos
- Inadecuada utilización de información confidencial de la institución
- Operaciones no registradas intencionalmente
- Operaciones no reveladas adecuadamente
- Valoración errónea de posiciones (Reportes de posiciones intencionalmente errados).
- Fraude, fraude crediticio y depósito sin valor.

Fuente: Elaboración propia

4.1.5.1.2 Identificación de actores

Es importante definir los roles y las responsabilidades del personal de la IFD. La institución objeto de estudio, tiene una estructura organizacional completa y cuenta con las siguientes áreas claves para poder aplicar el modelo:

- Auditoría interna (AI).
- Unidad de riesgos (UR).
- Unidad de control interno (UCI).
- Unidad de calidad y procesos (UCP).

4.1.5.1.3 Características del entorno

Tabla 19
Características del entorno

Identificación del entorno		
¿Es posible explorar toda la información necesaria?	Accesible	
	Inaccesible	
	Mixto	x
¿La evolución del entorno se sigue de un cómputo o hay actores que responden de forma no previsible?	Determinista	
	No Determinista	
	Mixto	x

¿La acción del agente se produce bajo demanda o el agente ha de ser proactivo?	Episódico	
	No episódico	
¿Cambia el entorno, aunque no entre en acción el agente?	Estático	
	Dinámico	x
¿El modelo del ambiente es continuo o discreto (simbólico)?	Discreto	
	Continuo	x

Fuente: Elaboración propia

4.1.5.1.4 Lista de requisitos

Tabla 20

Lista de requisitos

Nro	Descripción	Dueño de la información
Req 1	Evaluación periódica del personal	UC
Req 2	Ranking de puntos de alerta	UC
Req 3	Gestión de observaciones	UC
Req 5	

Fuente: Elaboración propia

4.1.5.1.5 Descripción detallada de los requisitos

Tabla 21

Descripción detallada del Requisitos Req. 1

Req 1: Evaluación periódica del personal

Descripción detallada

Para la evaluación del personal se usan herramientas, tales como: Registro de Bienes y parentesco y Tests Psicológicos de personalidad.

Definición de tareas

Llenado de los tests psicológicos de personalidad

Evaluación de respuestas de los tests (base de conocimientos)

Informe general y particular de resultados (por persona, agencia,

Análisis del registro de Bienes (base de conocimientos)

Fuente: Elaboración propia

Tabla 22

Descripción detallada del Requisitos Req. 2

Req 2: Ranking de puntos de alerta

Descripción detallada

Identificar y clasificar posibles eventos de riesgo interno

Definición de tareas

Registrar posibles eventos de riesgo por unidad de operación y usuario

Evaluación de transacciones

Ranking por cliente (cartera, mayores deudores)

Concentración de colocaciones

Fuente: Elaboración propia

Tabla 23

Descripción detallada del Requisitos Req. 3

Req 3: Gestión de Observaciones

Descripción detallada

Posibilidad de registro de las matrices de observación junto a los planes de observación

Definición de tareas

Automatizar la Matriz de Observaciones

Identificación de operaciones por unidad o persona y mapeo con la matriz de observaciones y evaluar con el Inventario de Procesos

Fuente: Elaboración propia

4.1.5.2 Análisis

4.1.5.2.1 Diagrama de agentes

A continuación, se desarrolla los diagramas de agentes:

Tabla 24

Diagrama de agente: 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 y coadyuvar a la construcción de la Matriz de Riesgos.

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

Fuente: Elaboración propia

Como resultado el Agente Identificador, llenará periódicamente la siguiente Matriz de Riesgos:

Tabla 25
Matriz de Riesgo

	Riesgo 1		Riesgo 2		Riesgo 3		Riesgo N	
	RI	CI	RI	CI	RI	CI	RI	CI
Departamento 1								
Departamento 2								
Departamento 3								
Departamento 4								
Departamento 5								

Fuente: Elaboración propia

La puntuación definida, se aprecia en la tabla 26:

Tabla 26
Tabla de puntuaciones

Tabla de puntuaciones	
No aplica	1
Riesgo Bajo	2
Riesgo Medio	3
Riesgo Medio Alto	4
Riesgo Alto	5
Riesgo Crítico	6

Fuente: Elaboración propia

Tabla 27

Diagrama de agente: 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 la frecuencia e impacto de las 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 PNP
- 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 PNP
- Lectura de Estados Financieros
- Lectura de Límites Financieros
- Lectura del apetito de Riesgo
- Cálculos del impacto y estadísticos
- Medición de frecuencias

Fuente: Elaboración propia

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.

Tabla 28

Diagrama de agente: Agente Mitigación

Agente Mitigación
<p>Descripción El agente divulgador es el encargado de programar y apoyar en las evaluaciones. Es encargado además de apoyar al personal de la IFD en el “aprendizaje” de la documentación PNP</p> <p>Roles Encargado de aprendizaje de la documentación PNP Asistente Virtual en el llenado y revisión de evaluaciones de personal</p> <p>Servicios Emitir informes de evaluación</p> <p>Creencias Pizarra PNP interno y externo Evaluaciones</p> <p>Deseos El personal “conoce” y aplica la documentación PNP El personal realiza las evaluaciones oportunamente Responder a las preguntas relacionadas con eventos de Fraude Interno</p> <p>Intenciones Registra la documentación PNP Almacena la información contextual del personal Realiza la programación de evaluaciones Asiste en el llenado de las evaluaciones</p>

Fuente: Elaboración propia

Tabla 29

Diagrama de agente: Agente Divulgación

Agente Divulgación
<p>Descripción El agente de divulgación es el encargado de distribuir la información apropiada al Directorio u órgano equivalente, Gerente General, gerentes de área y demás funcionarios de la IFD</p> <p>Roles Distribuye información de RO, según el nivel jerárquico.</p> <p>Servicios Responder consultar</p>

-
- Realizar informes
 - Gestionar alertas
 - Creencias**
 - Pizarra
 - PNP interno y externo
 - Información de RO
 - Base de Datos de Personal de IFD
 - Deseos**
 - Entregar información oportuna y de calidad
 - Intenciones**
 - Lectura de la pizarra
 - Lectura de la base de conocimientos
 - Elaboración de información
-

Fuente: Elaboración propia

Tabla 30
Roles de los Agentes

Tipo de agente	Agente	Rol	Abreviatura
Usuario	Identificador	Identificador de posibles eventos de riesgo de tipo Fraude Interno	IPER_FI
	Medidor	Medidor de niveles de RO	MNR_FI
	Mitigación	Encargado de aprendizaje de la documentación PNP Asistente Virtual en el llenado y revisión de evaluaciones de personal.	A_FI
			AV_FI
Divulgador	Distribuye información de RO, según el nivel jerárquico.	DI_FI	
Sistema	Control Tareas	Control de subprocesos	CS_FI

Fuente: Elaboración propia

Se considera información de RO a:

- Cálculo de frecuencia e impacto de pérdida, por la línea de negocio y evento de pérdida.
- Cálculo de pérdidas esperadas por riesgo operativo, por la línea de negocio y tipo de pérdida.
- Cálculo de pérdidas proyectadas, a diferentes plazos y bajo diferentes escenarios.
- Control y seguimiento de pérdidas reales con relación a las pérdidas proyectadas mediante indicadores de cumplimiento.
- Cálculo de costos y pérdidas promedio por la línea de negocio y tipo de evento.

- Registro de puntos de control de procesos.
- Generación de reportes por filtros múltiples
- Almacenamiento de reportes bajo diferentes filtros y supuestos

4.1.5.2.2 Modelo de roles

Los roles identificados, se aprecian en la tabla 30:

A continuación, se describe cada uno de los roles.

IPER_FI: 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.

MNR_FI: Este rol mide la frecuencia e impacto de eventos de RO, recuperando la información registrada por el IPER_FI y registra los nuevos datos en la pizarra

A_FI: Tutor de curso virtual adaptativo.

DI_FI: Este rol es el encargado de elaborar y entregar los resultados de la GRO al personal de la IFD según el nivel jerárquico.

CS_FI: Este rol gestiona el acceso a la pizarra y la comunicación entre agentes.

A continuación, se describen los diagramas de roles:

Tabla 31
Diagrama de rol del Agente Identificador

<p>Diagrama de rol: Identificador de posibles eventos de riesgo de tipo Fraude Interno (IPER_FI)</p> <hr/> <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: Evalua-Transaccion, Compara-Inventario, Compara-Histórico-Eventos-Fraude,Evalua-Caso,Registra-Pizarra</p> <p>Permisos Lectura-Transacción, Lectura-Inventario, Lectura-Histórico-Eventos,<u>Escritura-Pizarra</u>, Lee-Base_Conocimientos</p>

Responsabilidades:

Viveza

IPER-FI=((Lectura-Transacción. Compara-Inventario)^w|(Lectura-Transacción. Lectura-Histórico-Eventos)^w). Evalua-caso)|Registra-Pizarra

Seguridad

El registro en pizarra se realiza siempre y cuando exista un positivo de comparación entre la transacción leída y la comparación.

Fuente: Elaboración propia

Tabla 32

Diagrama de rol del Agente Medidor

Diagrama de rol: Medidor de niveles de RO (MNR_FI)

Descripción:

Este rol mide la frecuencia e impacto de eventos de RO, recuperando la información registrada por el IPER_FI y registra los nuevos datos en la pizarra estimando el nivel de RO (criticidad)

Protocolos y actividades:

Calculo-Impacto-Frecuencia, Calculo-Nivel-Riesgo, Calculo-Umbral-Riesgo

Permisos

Lectura-Estados-Financieros, Lectura-Limites. Lectura-Evento-Pizarra, Escribe-Resultado-Pizarra, Lectura-Matriz_Riesgos, Lectura-cuestionario

Responsabilidades:

Viveza

MNR_FI= (Lectura-Matriz_Riesgos. Lectura-cuestionario, Calculo-Impacto-Frecuencia, Calculo-Nivel-Riesgo, Calculo-Umbral-Riesgo. Escribe-Resultado-Pizarra)^w

Seguridad

Verdad

Fuente: Elaboración propia

Tabla 33

Diagrama de rol del Agente Mitigación

Diagrama de rol: Encargado de “aprendizaje” de la documentación PNP A_FI

Descripción:

El rol es el encargado de “aprendizaje” de los documentos PNP, según coordinación con Recursos Humanos y todas las áreas

Protocolos y actividades:

Solicitud-Tutoría, Tutoría, Registro-Material, Registro-Evaluaciones, Programación-Evaluaciones, Evaluaciones

Permisos

Escritura-Material, Escritura-Evaluaciones

Responsabilidades:

Viveza

AF_I=Solicitud-Tutoría, (Registro-Material|Tutoria).(Registro-
Evaluaciones,Programacion-Evaluaciones).Evaluaciones
Seguridad
Verdad

Fuente: Elaboración propia

Tabla 34
Diagrama de rol del Agente Divulgador

Diagrama de rol: Distribuye información de RO, según el nivel jerárquico.
DI_FI

Descripción:

El agente de divulgación es el encargado de distribuir la información resultante del MNR-FI al personal, según el nivel jerárquico (Directorio, Gerencia,...)

Protocolos y actividades:

Clasifica-según-jerarquia, Emitir-alertas,Espera-Solicitud-reportes

Permisos

Lectura-Pizarra

Responsabilidades:

Viveza

DI_FI=Lectura-Pizarra.Clasificar-según-jerarquia.(Emitir-
alertas|Espera-Solicitud-reportes)

Seguridad

Emite alerta para eventos críticos y altamente críticos o responde a solicitudes

Fuente: Elaboración propia

4.1.5.3 Diseño

4.1.5.3.1 Modelo de servicios

El modelo de servicios trata de identificar las funciones (servicios) asociados con el rol de cada agente, y para especificar las propiedades principales de esos servicios. Debemos identificar entonces por cada servicio las entradas, salidas y pre y post condiciones. A continuación, se detalla este modelo rol por rol.

Tabla 35*Modelo de servicios Rol IPER_FI*

Diagrama de servicios: Identificador de posibles eventos de riesgo de tipo Fraude Interno IPER_FI				
Servicios	Entradas	Salidas	Precondiciones	Postcondiciones
Recopilación de eventos de riesgo Recopilación de posibles eventos de riesgo de los diferentes procesos financieros (registros del SIRO y transacciones del Core Financiero)	Transacciones Evaluación de personal Observaciones	Registro en pizarra Matriz de Riesgos	Existe la estructura en el Core financiero y Administrativo	Eventos identificados
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				

Fuente: Elaboración propia

Tabla 36*Modelo de servicios Rol MNR_FI*

Diagrama de servicios: Identificador de posibles eventos de riesgo de tipo Fraude Interno IPER_FI				
Servicios	Entradas	Salidas	Precondiciones	Postcondiciones
Medición de nivel de RO	Pizarra Matriz de riesgos Estados	Registro en pizarra Registro del nivel	Existen nuevos registros en pizarra	Cálculos correctos
Medición de frecuencia e impacto de los eventos de RO	Financieros Limites	de RO (criticidad)		

Fuente: Elaboración propia

Tabla 37
Modelo de servicios Rol DI_FI

Diagrama de servicios: Identificador de posibles eventos de riesgo de tipo Fraude Interno IPER_FI				
Servicios	Entradas	Salidas	Precondiciones	Postcondiciones
Responder consultar	Solicitud de información Pizarra	Respuesta a las consultas Reportes e	Información verdadera	Información de calidad
Realizar informes	Matriz de riesgos	informes		
Gestionar alertas				

Fuente: Elaboración propia

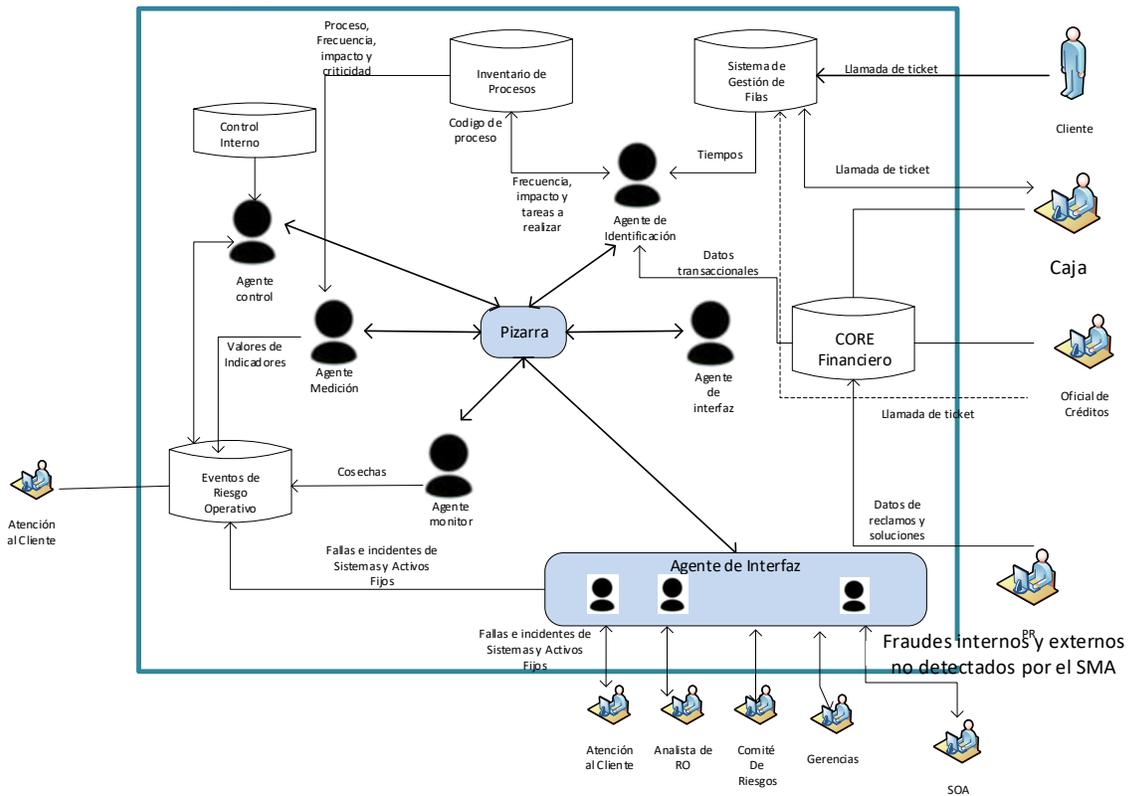


Figura 18 Estructura de agentes sobre la plataforma tecnológica de la IFD
 Elaboración propia

4.1.5.4 Implementación

Primero se establece el lugar de los agentes del modelo sobre la tecnología de la IFD, en la Figura 18. Luego se diseñan los algoritmos de los agentes en pseudocódigo. En el siguiente algoritmo se representa las acciones del agente de identificación:

```
Procedure AGENTE_identifica
Mientras funcione_Core_financiero hacer
  Lectura (transacción, Id_personal)
  Busca transacción en la Base de Conocimientos
  Si posible_evento_riesgo(transacción) entonces
    Band1->Buscar_Historial_personal(Id_personal)
    Band->2Buscar_Inventario(Transaccion)
    Mapeo_Datos(Band1,Band2)
    Si criticidad_alta entonces
      Registro en Pizarra
    Si_no
      Registro en Historial de posibilidades
  Fin_si
Fin_mientras
Fin_procedure
```

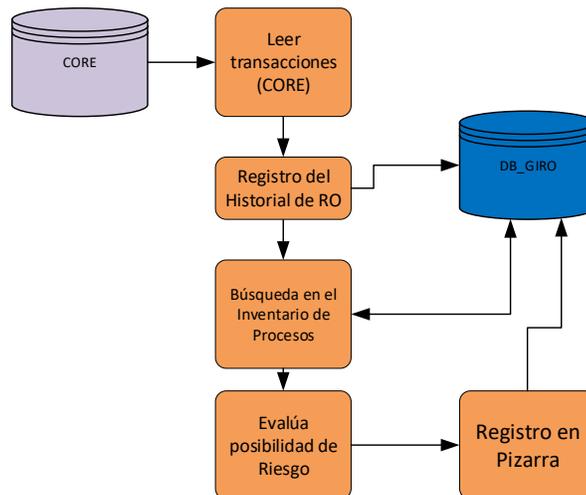


Figura 19: Subproceso de identificación de riesgos
Elaboración propia

Para la ejecución de los agentes se usaron datos de prueba que permiten analizar algunos casos extremos de identificación de eventos de riesgo, a partir de las transacciones del core financiero.

Historial de operaciones

Usuario	Operación	Fecha	Hora	Monto	Tipo de evento
3413001-JAIME ROCA	OP004-AMORIZACION DE CREDITOS CON RECIBO PROVISIONAL	2019-09-23	08:30:00	1500	PRO
3413001-JAIME ROCA	OP001-ANULACION DE CREDITOS	2019-09-23	08:30:00	1500	PRO

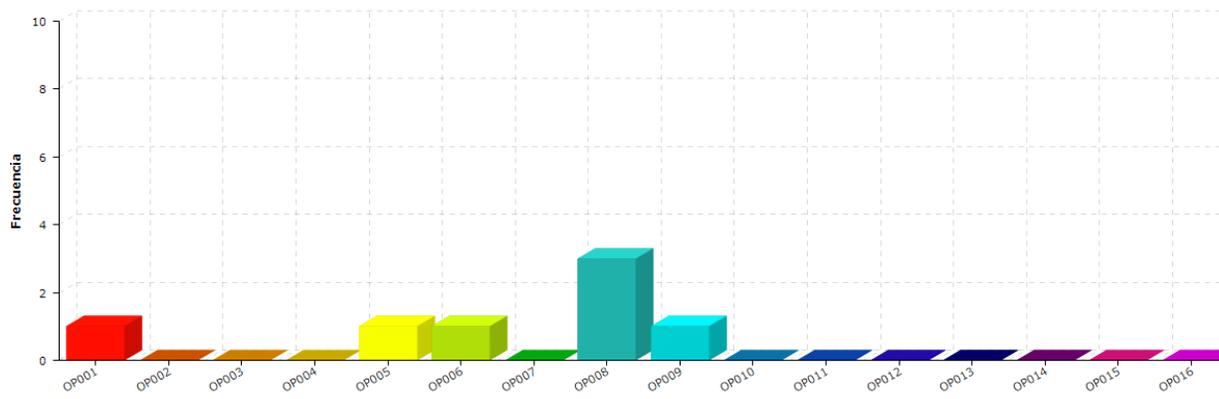
Pizarra Identificación

Operacion	Agencia	Usuario	Fecha de Registro	Frecuencia	Monto	Nivel de criticidad	Tipo de evaluación
OP001-ANULACION DE CREDITOS DESEMBOLSADOS	A001	3413001-JAIME ROCA	2019-09-23	2	2200	2-MEDIO	PRO
OP005-TRASPASO DE SALDOS	A001	3413001-JAIME ROCA	2019-09-23	1	15178	1-BAJO	HOR
OP006-DESEMBOLSO DE CREDITO	A001	3413001-JAIME ROCA	2019-09-23	1	10000	1-BAJO	HOR

*Figura 20 Estado de la pizarra y el historial de operaciones después de la identificación
Elaboración propia*

En la gráfica de la Figura 21 se puede apreciar que después del proceso de identificación de riesgos, aquellos que originaron posibles eventos de riesgo son: OP001 anulación de créditos desembolsados, OP005 traspaso de saldos, OP006 desembolso de crédito, OP008 anulación de traspasos y OP009 amortización de créditos.

Se identificaron los siguientes posibles eventos de riesgo



*Figura 21 Representación gráfica de los riesgos identificados
Elaboración propia*

El agente de medición, realizará las siguientes acciones: Realizar una minuciosa investigación del incidente, documentando apropiadamente todos los aspectos para llegar a una conclusión objetiva. Esta tarea se realiza con los resultados de la pizarra registrado por el agente de identificación y con la ayuda de los registrado en la base de conocimientos.

```

Procedure AGENTE medición
  Mientras noexistenregistrosenpizarra hacer
    Evaluaniveldecriticidad
    Evaluaniveldefrecuencia
    insertainformacionpizarramedicion
  Fin_mientras
Fin_procedure
  
```

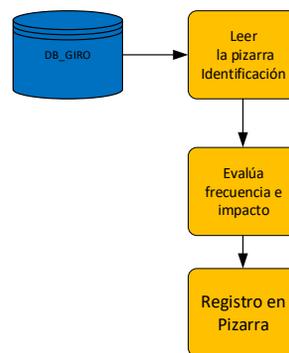


Figura 22 Subproceso de medición de riesgo
Elaboración propia

Después de la ejecución del agente de medición se llena la pizarra de nivel medición.

PIZARRA DE MEDICION

Operacion	Agencia	Usuario	Fecha de Registro	Frecuencia	Monto	Nivel de criticidad	Tipo de evaluación
OP001-ANULACION DE CREDITOS DESEMBOLSADOS	A001	3413001-JAIME ROCA	2019-09-23	2	2200	2-MEDIO	PRO
OP005-TRASPASO DE SALDOS	A001	3413001-JAIME ROCA	2019-09-23	1	15178	1-BAJO	HOR
OP006-DESEMBOLSO DE CREDITO	A001	3413001-JAIME ROCA	2019-09-23	1	10000	1-BAJO	HOR
OP008-ANULACION DE TRASPASOS	A001	4257002-MONICA ALVAREZ	2019-09-23	2	2200	2-MEDIO	PRO
OP008-ANULACION DE TRASPASOS	A001	4257002-MONICA ALVAREZ	2019-09-23	2	26278	3-ALTO	PRO
OP008-ANULACION DE TRASPASOS	A001	2890003-LUDOVIC GOMEZ	2019-09-23	2	26278	3-ALTO	PRO
OP009-AMORTIZACION DE CREDITOS	A001	3413001-JAIME ROCA	2019-09-23	1	470	1-BAJO	HOR

Figura 23 Pizarra nivel medición
Elaboración propia

En la figura 24 se aprecia junto a los procesos identificados como generadores de eventos de riesgo la criticidad del evento, dicha criticidad se obtiene multiplicando frecuencia por impacto.

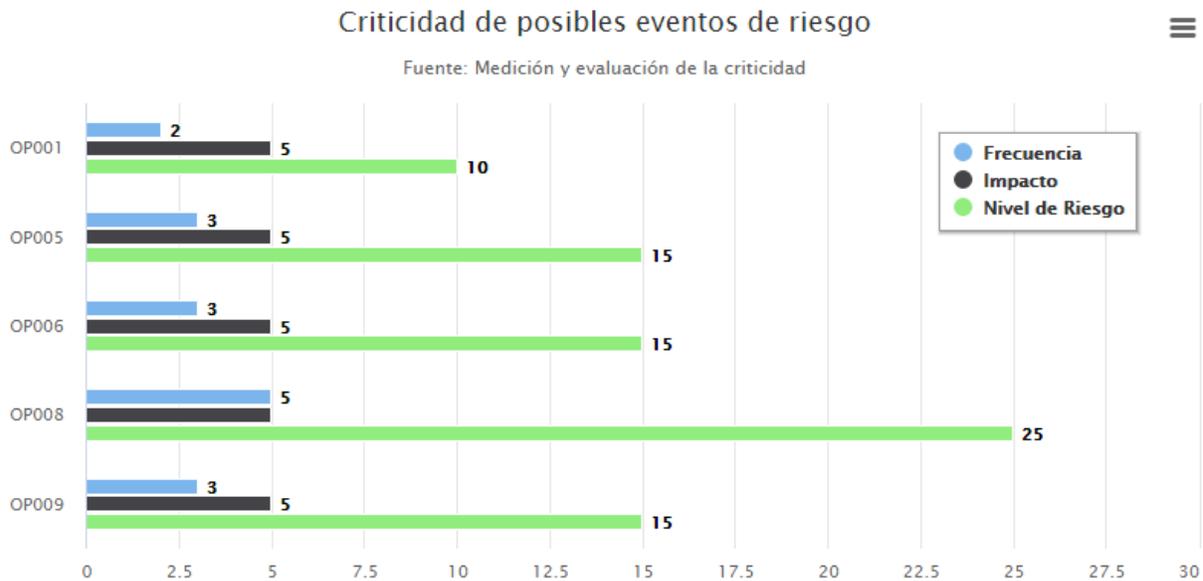


Figura 24 Calificación asignada para determinar el nivel de riesgo
Elaboración propia

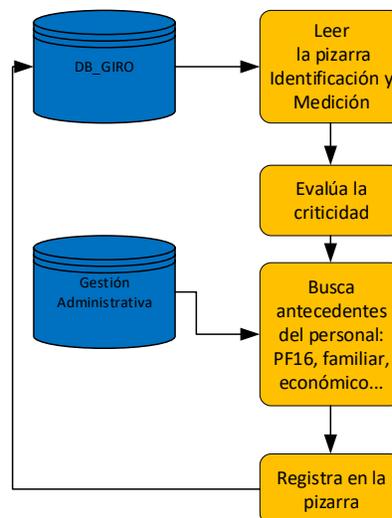


Figura 25 Subproceso de monitoreo
Elaboración propia

El subproceso de monitoreo de describe en la Figura 25, el agente de monitoreo es el encargado de buscar el historial del personal involucrado en algún evento de riesgo.

La información es analizada gracias a la base de conocimientos, donde se encuentran las reglas de decisión respecto a los datos encontrados. El resultado se plasma en un reporte individual del personal involucrado y en la Matriz de Riesgo Operativo, como se observa en la figura 26.

Matriz de riesgo == Ponderaciones

5	10	15	20	25
4	8	12	16	20
3	6	9	12	15
2	4	6	8	10
1	2	3	4	5

Matriz de riesgo == Procesos y recomendaciones

	OP001 Compartir mitigar	OP008 Compartir mitigar OP005 Compartir mitigar OP006 Compartir mitigar OP009 Compartir mitigar		OP008 Evitar Compartir Mit

*Figura 26 Matriz de riesgo
Elaboración propia*

El agente de control emite observaciones y recomendaciones respecto a la criticidad identificada, para ello el agente control trabaja con la base de conocimientos. Para el caso de estudio las recomendaciones son:

**No existen políticas para el tema mapeo entre personalidad y llamadas de atención.
Se encontraron irregularidades en transacciones fuera de horario**

*Figura 27 Observaciones y recomendaciones del Agente Control
Elaboración propia*

4.2 VALIDACIÓN DE RESULTADOS

4.2.1 Formulación de hipótesis nula

Con el propósito de demostrar la validez de la hipótesis planteada en el capítulo uno de la tesis, se define a continuación la hipótesis nula H_N y la hipótesis alterna H_1 .

H_1 : El uso de un Modelo Multiagente influye en el eficiente desarrollo de sistemas de Gestión Integral de Riesgo Operativo de Instituciones Financieras de Desarrollo en la ciudad de El Alto.

H_N : El uso de un Modelo Multiagente no influye en el eficiente desarrollo de sistemas de Gestión Integral de Riesgo Operativo de Instituciones Financieras de Desarrollo en la ciudad de El Alto.

4.2.2 Selección de variables

Variable independiente: Modelo Multiagente

Variable dependiente: desarrollo de sistemas de Gestión Integral de Riesgo Operativo de Instituciones Financieras de Desarrollo en la ciudad de El Alto.

4.2.3 Instrumentación

La evaluación del modelo se realiza en tres etapas (Anexo C):

- Primero se realizó la evaluación genérica del MMAGIRO, la misma se realizó con ayuda del personal de sistemas, quienes realizaron sugerencias y preguntas respecto al proceso. Finalmente llenaron una encuesta donde se centralizaron opiniones.
- En una segunda etapa, el modelo MMAGIRO fue evaluado por el personal de sistemas de la IFD y por estudiantes de octavo semestre de la carrera de Ingeniería de Sistemas. En esta etapa se evaluó el ciclo de vida del modelo. Con los estudiantes, se planteó una actividad práctica a dos grupos, el primer grupo resolvió el problema empleando el modelo MMAGIRO y el segundo grupo utilizó el modelo GAIA (el mismo es denominado modelo tradicional), la actividad práctica se realizó en un mes (cuatro sesiones).
- El personal de riesgo evaluó los resultados de la aplicación, brindando su opinión respecto a los resultados brindados. El personal de riesgo comparó los resultados del

MMAGIRO para Fraude Interno respecto a los resultados del Sistema Actual, sin embargo no valoraron el proceso de desarrollo del modelo.

A continuación, se muestra los criterios de evaluación genérica del Modelo MMAGIRO.

Tabla 38
Identificación de criterios de evaluación del MMAGIRO

Nro. de criterio	Criterio	Descripción
c1	Respuesta a los objetivos	El modelo se ajusta a los objetivos de la Gestión de RO
c2	Complejidad del ciclo de vida	El modelo cubre el ciclo entero de desarrollo de software
c3	Integración	El modelo integra las distintas fases del ciclo de desarrollo
c4	Validaciones	El modelo incluye la realización de validaciones
c5	Exactitud	El modelo soporta la determinación de la exactitud del sistema a través del ciclo de desarrollo.
c6	Comunicación	El modelo es la base de una comunicación efectiva.
c7	Entorno dinámico	El modelo funciona en un entorno dinámico orientado al usuario
c8	Pedagogía	El modelo se puede enseñar
c9	Herramienta CASE	El modelo es soportado por herramientas CASE
c10	Evolución	El modelo soporta la eventual evolución del sistema
c11	Mejora	El modelo contiene actividades conducentes a mejorar el proceso de desarrollo de software

NOTA. Elaboración propia. Los criterios de evaluación se diseñaron con base a la propuesta de Barzanallana referenciado por Méndez (2006)

Donde:

Tabla 39
Escala y ponderación de valores de las respuestas

Escala
1= Totalmente en desacuerdo; 2 = Desacuerdo; 3 = indeciso/neutral; 4 = De acuerdo; 5 = Totalmente de acuerdo
Ponderación
5 = 100%, 4 = 80%, 3 = 60%, 2 = 30%, 1 = 10%

Fuente: Elaboración propia

El personal del departamento de sistemas de la IFD, cuentan con experiencia en el desarrollo de sistemas de información y el empleo de modelos de desarrollo del software. Por lo general

aplican el modelo de desarrollo Cascada, el cual será denominado modelo tradicional. Los resultados de la valoración se ven en la tabla 40.

Tabla 40
Cálculo de ponderaciones de los criterios de evaluación

Criterio	Puntuación obtenida					Ponderada					Total
	1	2	3	4	5	0,1	0,3	0,6	0,8	1	
						1	2	3	4	5	
c1 Respuesta a los objetivos	0	1	0	3	3	0	0,143	0	0,4286	0,429	0,81
c2 Completitud del ciclo de vida	0	0	0	3	4	0	0	0	0,4286	0,571	0,91
c3 Integración	0	0	1	4	2	0	0	0,143	0,5714	0,286	0,83
c4 Validaciones	0	0	4	3	0	0	0	0,571	0,4286	0	0,69
c5 Exactitud	0	0	2	5	0	0	0	0,286	0,7143	0	0,74
c6 Comunicación	0	0	0	4	3	0	0	0	0,5714	0,429	0,89
c7 Entorno dinámico	0	0	2	3	2	0	0	0,286	0,4286	0,286	0,8
c8 Pedagogía	0	0	0	4	3	0	0	0	0,5714	0,429	0,89
c9 Herramienta CASE	7	0	0	0	0	1	0	0	0	0	0,1
c10 Evolución	0	0	1	3	3	0	0	0,143	0,4286	0,429	0,86
c11 Mejora	0	0	2	3	2	0	0	0,286	0,4286	0,286	0,8

Fuente: Elaboración propia

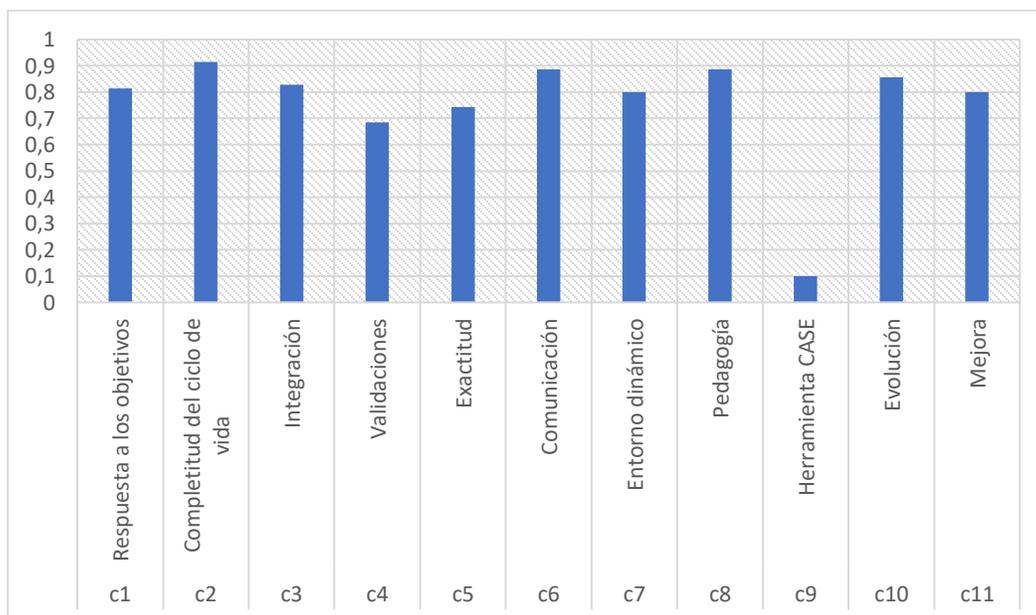


Figura 28: Resultados de evaluación del MMAGIRO
Elaboración propia

En la figura 28 se presentan los resultados. Como se puede apreciar, resultado de la encuesta, los criterios en los que hay acuerdo de cumplimiento y que obtuvieron mayor escala respecto al modelo MMAGIRO son: respuesta a los objetivos, completitud del ciclo de vida, integración, comunicación, pedagogía y evolución. Los criterios que están en el umbral de aceptación son entorno dinámico y mejora. Aquellos criterios en los cuales los resultados expresan indecisión o neutralidad son validaciones y exactitud. Y el criterio inexistente en el modelo es soporte de herramienta CASE.

El modelo MMAGIRO integra el ciclo de vida de un sistema desde la especificación de requisitos hasta el análisis de resultados. Para ello se diseñaron los siguientes instrumentos:

Tabla 41
Diseño del experimento con las etapas MMA GIRO

Tareas	Fase de desarrollo	Responsable
T1	Especificación de requisitos (ER)	Tecnología de la Información y personal de riesgo operativo
T2	Análisis (AN)	Tecnología de la Información
T3	Diseño (DI)	Tecnología de la Información
T4	Implementación (IM)	Tecnología de la Información
T5	Resultados (RR)	Tecnología de la Información personal de riesgo operativo

Fuente: Elaboración propia

Esta segunda fase de validación comprende el análisis de eficiencia respecto a la aplicación del modelo MMAGIRO. Steve McConnell, en su obra *Rapid Development*, propone los tres pilares que consiguen que un proyecto software o un desarrollo sea eficiente. Estos pilares de eficiencia se refieren a estar por encima de la media en la capacidad de terminar un proyecto en tiempo, dentro de coste y con la funcionalidad necesaria incluida (realizando una adecuación parcial de la ISO 25010). De forma que, para cada una de las fases de desarrollo del modelo se analiza:

-

-
- **Tabla 42**
Criterios de valoración de la eficiencia del modelo: Tiempo y Funcionalidad
- Fuente: Elaboración propia

Nº	Etapa	Criterio	Descripción de las preguntas	Valoración de las respuestas
P00	DE	Datos del encuestado	Cargo Experiencia en el desarrollo de soluciones de GRO	
P01	ER	Dificultad	El grado de dificultad de las tareas es aceptable	(0-4)
P02	ER	Claridad	¿Se tiene claridad en las tareas a realizar?	(0-4)
P03	ER	Utilidad	¿Esta tarea es importante?	(0-4)
P04	ER	Impacto	¿Esta tarea tiene impacto en la mejora del desarrollo de software?	(0-4)
P05	ER	Tiempo	Tiempo invertido en esta fase	(0-4)
P06	AN	Dificultad	El grado de dificultad de las tareas es aceptable	(0-4)
P07	AN	Claridad	¿Se tiene claridad en las tareas a realizar?	(0-4)
P08	AN	Utilidad	¿Esta tarea es importante para el desarrollo del software?	(0-4)
P09	AN	Impacto	¿Esta tarea tiene impacto en la mejora de la GRO?	(0-4)
P10	AN	Tiempo	Tiempo invertido en esta fase es aceptable.	
P11	DI	Dificultad	El grado de dificultad de las tareas es aceptable	(0-4)
P12	DI	Claridad	¿Se tiene claridad en las tareas a realizar?	(0-4)
P13	DI	Utilidad	Esta tarea es importante.	(0-4)
P14	DI	Impacto	¿Esta tarea tiene impacto en la mejora de la GRO?	(0-4)
P15	DI	Tiempo	Tiempo invertido en esta fase	
P16	IM	Dificultad	El grado de dificultad de las tareas es aceptable	(0-4)
P17	IM	Claridad	¿Se tiene claridad en las tareas a realizar?	(0-4)
P18	IM	Utilidad	Esta tarea es importante.	(0-4)
P19	IM	Impacto	¿Esta tarea tiene impacto en la mejora de la GRO?	(0-4)
P20	IM	Tiempo	El tiempo invertido en esta fase	(0-4)

Elaboración propia

- **Funcionalidad:** se refiere a la capacidad del producto de software para suministrar un conjunto de funciones que satisfagan las necesidades implícitas o explícitas de los usuarios, al ser utilizado bajo condiciones específicas. Para evaluar la funcionalidad se empleó los siguientes criterios:
 - Dificultad
 - Utilidad
 - Claridad
 - Impacto
 - Resultados

- **Tiempo:** se evaluó el tiempo, bajo el supuesto de que no se requieren recursos adicionales para el proceso de desarrollo de la solución. No obstante, el tiempo tiene influencia directa sobre el costo.

Se valoraron las siguientes etapas de desarrollo de software:

- ER: especificación de requisitos
- AN: análisis
- DI: diseño
- IM: implementación

Las preguntas de la encuesta se desarrollaron, agrupándolas según las etapas del ciclo de vida del desarrollo del software, comparando el enfoque tradicional utilizado en la IFD con el propuestos a partir de un desarrollo SMA.

Se diseñaron los instrumentos en la tabla 42 y en la tabla 43:

Tabla 43

Escala y ponderación de los valores de las respuestas

<i>Escala</i>
Dificultad, utilidad, claridad, impacto: 1= Totalmente en desacuerdo; 2 = Desacuerdo; 3 = indeciso/neutral; 4 = De acuerdo; 5 = Totalmente de acuerdo Tiempo: = Demasiado, 2= Mucho, 3= indeciso/neutral, 4= aceptable, 5= Muy aceptable
<i>Ponderación</i>
1. 10%, 2. 30%, 3. 60%, 4. 80%, 5. 100%

Fuente: Elaboración propia

Se comparan los resultados de realizar la Gestión de Riesgo Operativo entre el modelo tradicional (cascada) y el modelo MMAGIRO, la encuesta se realiza respecto a la eficiencia de la solución planteada. Se obtuvieron los siguientes resultados, después de la valoración del personal de sistemas y estudiantes de últimos semestres de la carrera de Ingeniería de Sistemas:

Tabla 44
Evaluación de eficiencia del Modelo tradicional

Etapa	Criterios		Puntuación obtenida					Ponderada					Total M. Tradicional
			1	2	3	4	5	0,1	0,3	0,6	0,8	1	
								1	2	3	4	5	
Especificación de requisitos	P01	Dificultad		1	2	2	8	0	0,077	0,154	0,154	0,615	0,8538
	P02	Claridad		1	5	5	2	0	0,077	0,385	0,385	0,154	0,7154
	P03	Utilidad	8	3	2			0,615	0,231	0,154	0	0	0,2231
	P04	Impacto	8	3	2			0,615	0,231	0,154	0	0	0,2231
	P05	Tiempo		1		1	10	0	0,077	0	0,077	0,769	0,8538
Análisis	P06	Dificultad	2	2	9			0,154	0,154	0,692	0	0	0,4769
	P07	Claridad	1	2	9	1		0,077	0,154	0,692	0,077	0	0,5308
	P08	Utilidad		3	9	1		0	0,231	0,692	0,077	0	0,5462
	P09	Impacto	1	3	9			0,077	0,231	0,692	0	0	0,4923
	P10	Tiempo	1	4	8			0,077	0,308	0,615	0	0	0,4692
Diseño	P11	Dificultad		4	9			0	0,308	0,692	0	0	0,5077
	P12	Claridad	2	1	9	1		0,154	0,077	0,692	0,077	0	0,5154
	P13	Utilidad	2	3	8			0,154	0,231	0,615	0	0	0,4538
	P14	Impacto	2	3	8			0,154	0,231	0,615	0	0	0,4538
	P15	Tiempo	1	2	9	1		0,077	0,154	0,692	0,077	0	0,5308
Implementación	P16	Dificultad		3	4	6	2	0	0,231	0,308	0,462	0,154	0,7769
	P17	Claridad	8	3	2			0,615	0,231	0,154	0	0	0,2231
	P18	Utilidad	4	1	4	4		0,308	0,077	0,308	0,308	0	0,4846
	P19	Impacto		7	6			0	0,538	0,462	0	0	0,4385
	P20	Tiempo		1	1	1	10	0	0,077	0,077	0,077	0,769	0,9

Fuente: Elaboración propia

En la figura 29, se muestran los resultados gráficamente:

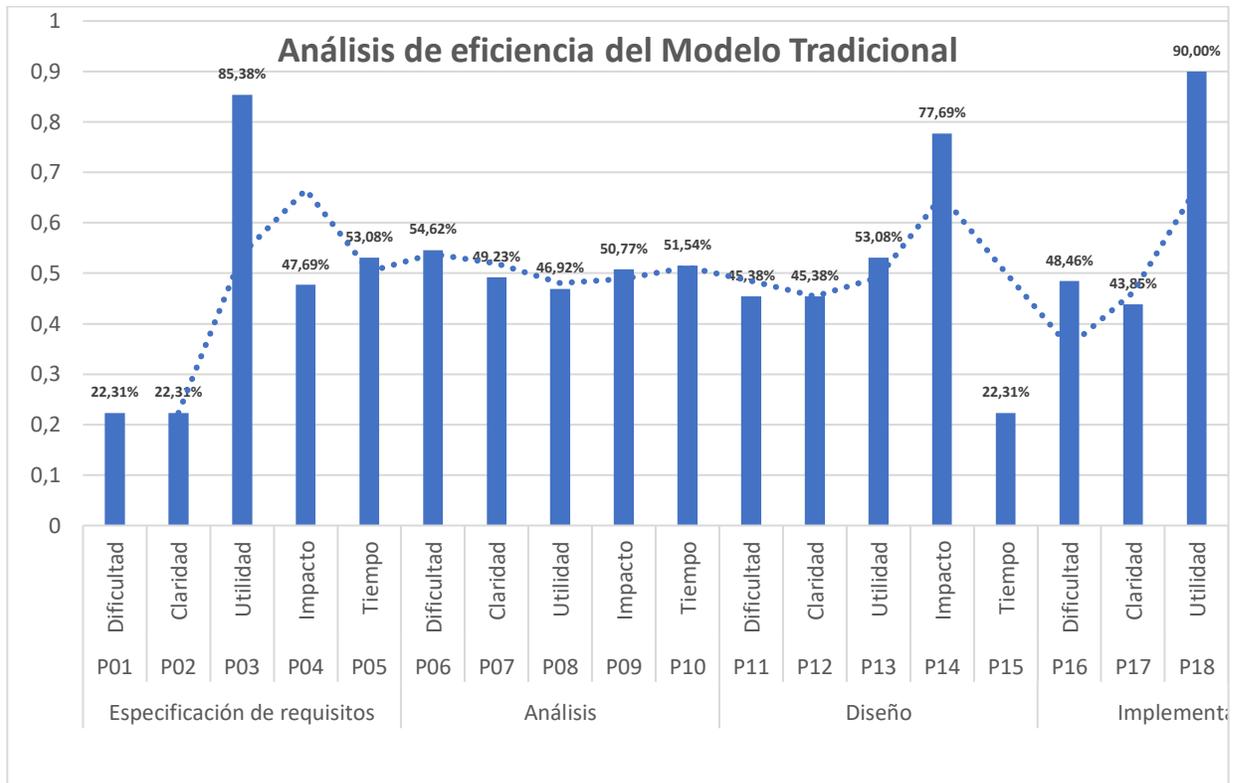


Figura 29: Análisis del modelo tradicional.
Elaboración propia

Como se puede apreciar en la figura 30, los encuestados expresan que la especificación de requisitos, como actividad principal para el desarrollo de la solución de GRO presenta dificultades a pesar de estar de acuerdo en tratarse de una fase sumamente útil. Finalmente, los encuestados le dan una alta ponderación a la utilidad de la implementación final.

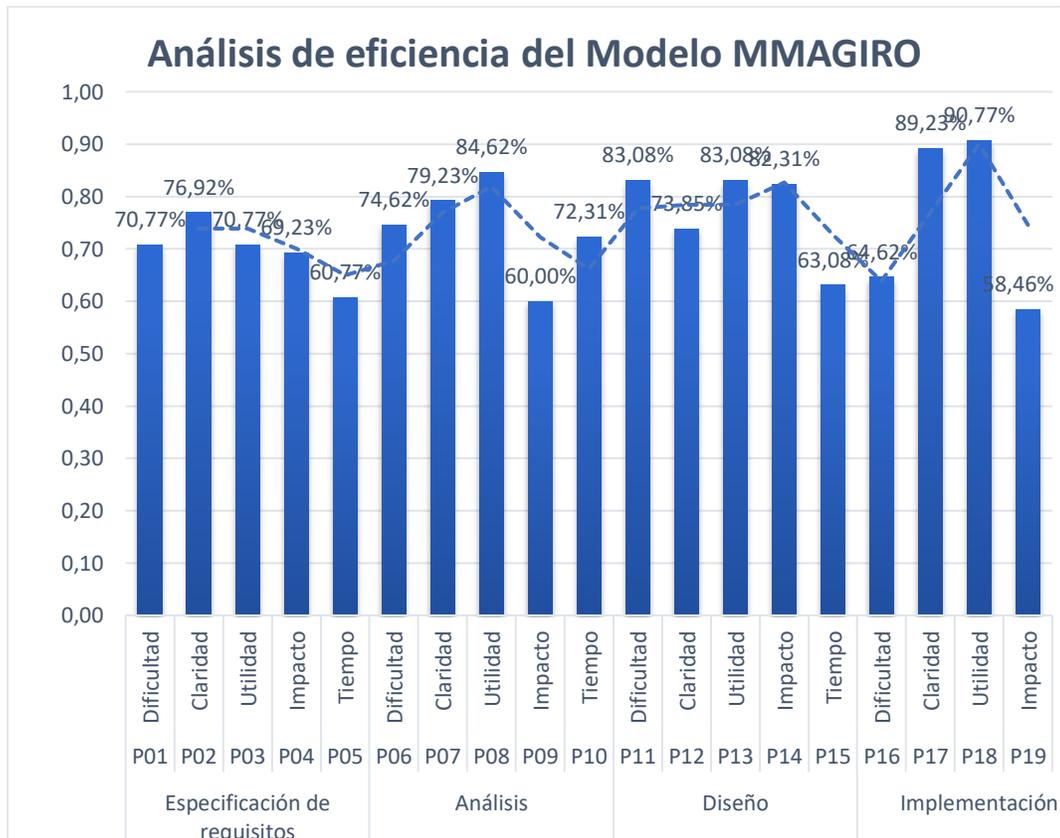
Tabla 45
Evaluación de eficiencia de MMAGIRO

Etapa	Criterios	Puntuación obtenida					Ponderada					Total MMAGIRO
							0,1	0,3	0,6	0,8	1	
		1	2	3	4	5	1	2	3	4	5	
Especificación de requisitos	P01 Dificultad	2	2	4	4	1	0,15	0,15	0,31	0,31	0,08	0,57
	P02 Claridad	0	2	3	6	2	0,00	0,15	0,23	0,46	0,15	0,71
	P03 Utilidad	0	0	4	7	2	0,00	0,00	0,31	0,54	0,15	0,77
	P04 Impacto	0	2	4	4	3	0,00	0,15	0,31	0,31	0,23	0,71
	P05 Tiempo	0	2	4	5	2	0,00	0,15	0,31	0,38	0,15	0,69
Análisis	P06 Dificultad	0	3	5	5	0	0,00	0,23	0,38	0,38	0,00	0,61

	P07	Claridad	1	0	3	6	3	0,08	0,00	0,23	0,46	0,23	0,75
	P08	Utilidad	1	0	2	5	5	0,08	0,00	0,15	0,38	0,38	0,79
	P09	Impacto	0	0	2	6	5	0,00	0,00	0,15	0,46	0,38	0,85
	P10	Tiempo	0	4	4	4	1	0,00	0,31	0,31	0,31	0,08	0,60
Diseño	P11	Dificultad	0	2	3	5	3	0,00	0,15	0,23	0,38	0,23	0,72
	P12	Claridad	0	0	3	5	5	0,00	0,00	0,23	0,38	0,38	0,83
	P13	Utilidad	1	1	1	7	3	0,08	0,08	0,08	0,54	0,23	0,74
	P14	Impacto	0	0	3	5	5	0,00	0,00	0,23	0,38	0,38	0,83
	P15	Tiempo	0	1	1	6	5	0,00	0,08	0,08	0,46	0,38	0,82
Implementación	P16	Dificultad	1	1	5	6	0	0,08	0,08	0,38	0,46	0,00	0,63
	P17	Claridad	1	1	4	7	0	0,08	0,08	0,31	0,54	0,00	0,65
	P18	Utilidad	0	0	1	5	7	0,00	0,00	0,08	0,38	0,54	0,89
	P19	Impacto	0	0	1	4	8	0,00	0,00	0,08	0,31	0,62	0,91
	P20	Tiempo	0	4	4	5	0	0,00	0,31	0,31	0,38	0,00	0,58

Fuente: Elaboración propia

El siguiente gráfico representa los resultados obtenidos:



*Figura 30: Análisis del modelo MMAGIRO
Elaboración propia*

Los encuestados mostraron aceptación por el modelo MMAGIRO, especialmente por la complejidad del tratamiento del Riesgo Operativo, la cantidad de datos y procesos involucrados, así como la posibilidad de trabajar con conocimientos claros provenientes de las normas y recomendaciones (ASFI y Basilea)

4.2.4 Análisis e Interpretación

De los resultados tenemos que: el 69% de los encuestados tienen experiencia en el uso de modelos *tradicionales*, para el desarrollo de software que responda a requisitos de riesgo operativo, no tenían experiencia en el desarrollo de multiagentes, pero sí tenían conocimientos teóricos al respecto. Por otra parte, el 31% de los encuestado han tenido *experiencias en el desarrollo de sistemas agentes* en diferentes soluciones dentro de su experiencia profesional.

Tabla 46
Experiencia de los encuestados en el desarrollo de agentes

Tipos de modelo de desarrollo del software	Cantidad de encuestas	%
1. Modelos tradicionales	9	69%
2. Experiencia con desarrollo de agentes	4	31%
Total, general	13	100%

Fuente: Elaboración propia

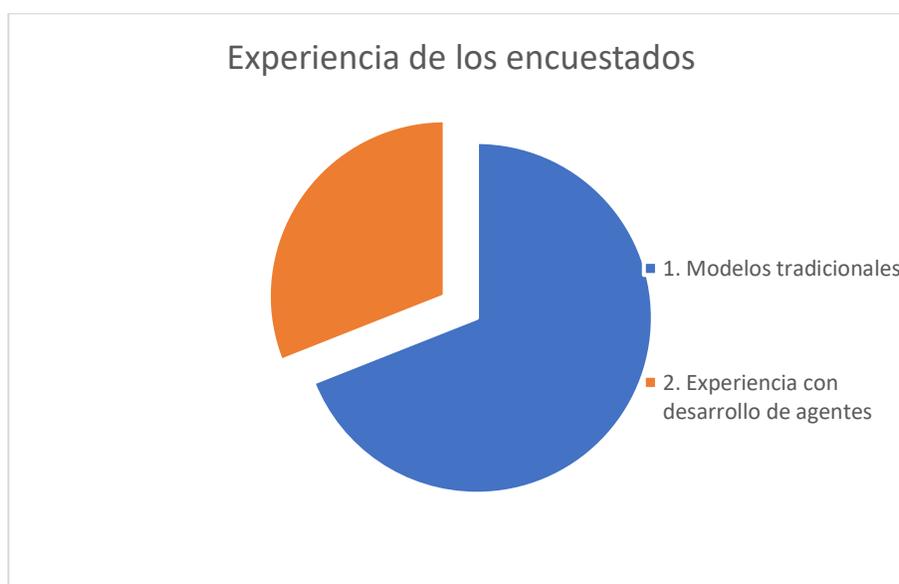
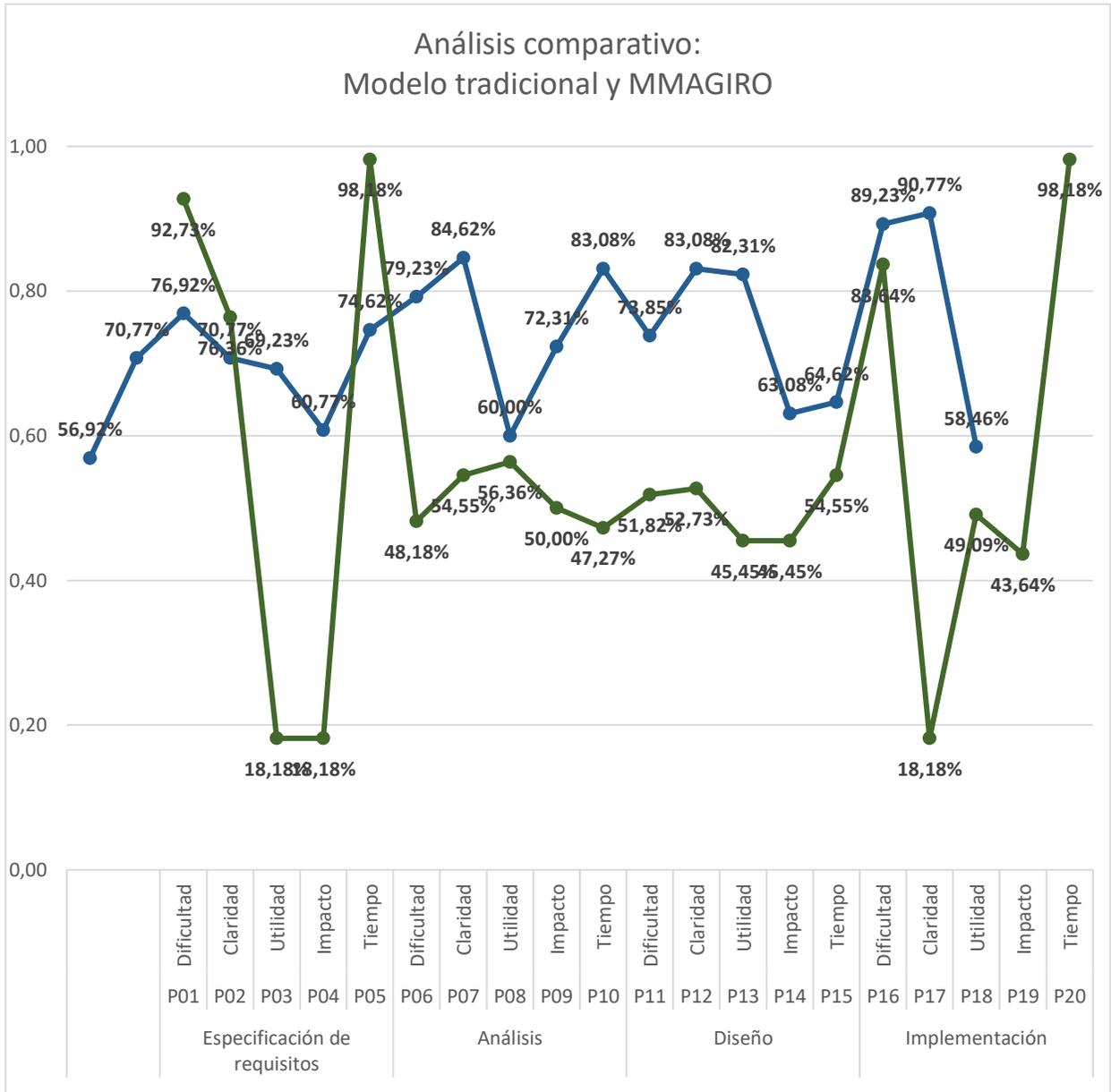


Figura 31: Experiencia de los encuestados
Elaboración propia

En las figuras 31 y 32, se puede ver la comparación entre ambos modelos: “tradicional” y MMAGIRO. La tabla 47 muestra los estadísticos descriptivos correspondientes a ambos modelos “tradicional” y MMAGIRO.



*Figura 32: Comparación entre el modelo “tradicional” y MMAGIRO
Elaboración propia*

Como se puede apreciar la distribución de datos no es normal, el tamaño muestral es muy pequeño y la información no es homogénea según se puede ver en la tabla 47.

Tabla 47*Estadísticos descriptivos de comparación de MMAGIRO con el modelo tradicional*

Origen	N	Promedio	Max	Min	DS	Mediana	Moda
MMAGIRO	13	0,73	0,91	0,57	0,10367282	0,73	0,7076923
Tradicional	13	0,533461538	0,9	0,22308	0,199380464	0,5	0,2230769

Fuente: Elaboración propia

Por tanto, se realizará la prueba de hipótesis relacionada con el origen de los diagramas, usando el test Chi cuadrado. Se precisa determinar la relación entre las variables, para confirmar o rechazar la hipótesis, por tanto, será necesario realizar un contraste de comparación de tendencia central. Realizando un análisis de medianas se aprecia:

$$\text{Mediana}_{\text{MMAGIRO}} > \text{Mediana}_{\text{Tradicional}}$$

Para confirmar o rechazar cualquier supuesto, primeramente, consideramos si los datos son independiente o apareados. Se halla la tabla 48 de frecuencias observadas:

Tabla 48*Frecuencias observadas*

	Escala de valoración					Total
	1	2	3	4	5	
Total M. Tradicional	41	53	118	27	37	276
MMAGIRO	8	27	64	111	65	275
Totales	49	80	182	138	102	551
Proporción	0,08892922	0,14519056	0,33030853	0,25045372	0,18511797	

Fuente: Elaboración propia

Con 4 grados de libertad y chi tabla 9,4877. Luego se construye la tabla de frecuencias esperadas:

Tabla 49*Frecuencias esperadas*

	1	2	3	4	5	Total
M. Tradicional	24,5444646	40,0725953	91,1651543	69,1252269	51,092559	276
MMAGiro	24,4555354	39,9274047	90,8348457	68,8747731	50,907441	275
	49	80	182	138	102	551

Finalmente, chi prueba nos da 10,551 que al ser mayor al chi tabla representa la negación de la hipótesis nula. Con una confiabilidad de 95%. Con lo cual se concluye que existe influencia entre la variable independiente y la dependiente. Por tanto, la hipótesis ha sido demostrada.

Finalmente, la evaluación realizada por el personal de Riesgo se aprecia en la siguiente tabla:

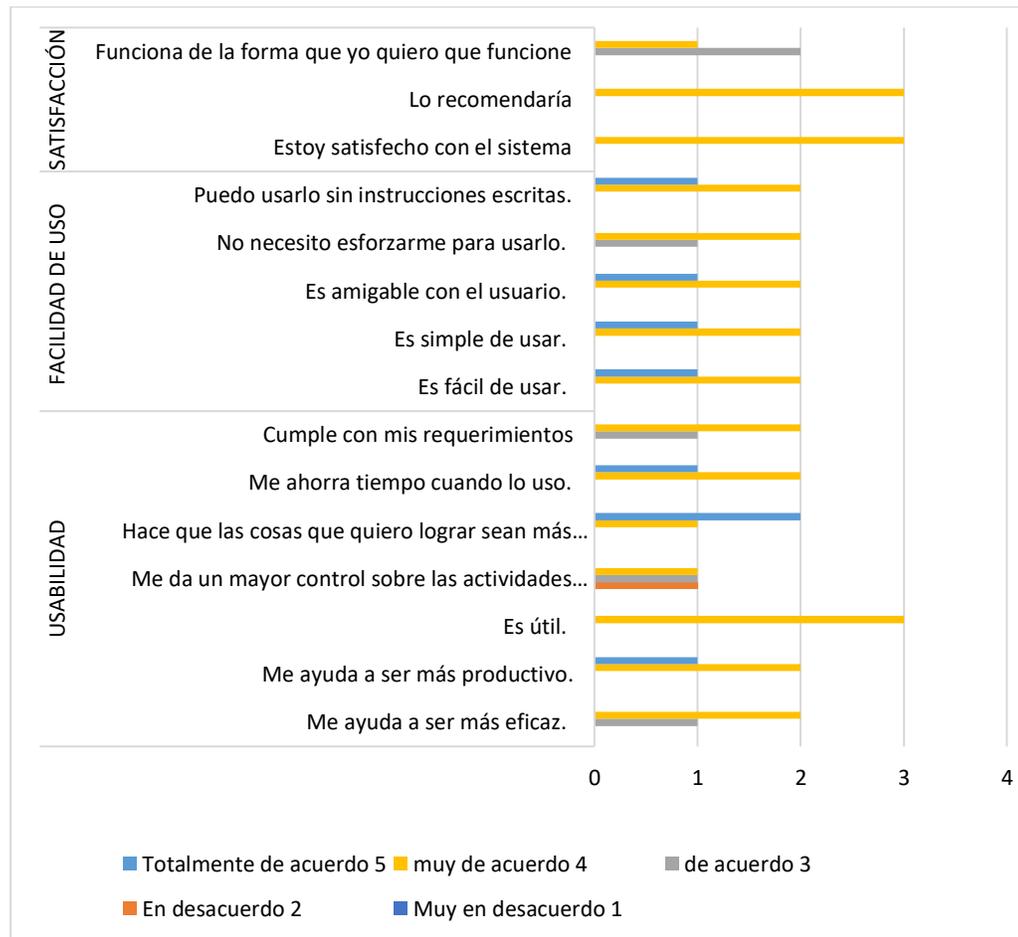


Figura 33 Opinión del Personal de Riesgo

Fuente Elaboración propia

Como se puede apreciar existe aceptación por parte del usuario final, respecto al modelo.

Capítulo V CONCLUSIONES Y RECOMENDACIONES DE LA INVESTIGACIÓN

5.1 Conclusiones

Los objetivos específicos se alcanzaron, como se describe a continuación:

- El modelo desarrollado comprende el diseño del modelo de Gestión de Riesgo Operativo para IFDs (cap. 4, pág. 39), formalizando el proceso del ciclo de vida del riesgo operativo, en cumplimiento de las normas establecidas en nuestro país y en contraste con la matriz FODA (cap. 4, pág. 37,38, Tabla 6).
- El Sistema Multiagente se definió con todos sus elementos (cap. 4, pág. 40), se diseñó como arquitectura de comunicación el esquema pizarra (cap. 4, pág. 47) y se describieron los procesos de Gestión de Riesgo Operativo (cap. 4, pág. 54), tanto la ontología (cap. 4, pág. 43) como el diseño de subprocesos se diseñó en respuesta de los lineamientos de Basilea y Asfi Ley N. 393.
- Se realizó la propuesta de las fases de desarrollo de software (cap. 4, pág. 59), fusionadas al modelo de Gestión de Riesgo Operativo y el Sistema Multiagente, referenciados en los anteriores puntos. Dicha propuesta, comprende desde la especificación de requisitos hasta la implementación, integrando de esta forma fases y componentes ausentes en la mayoría de los modelos de desarrollo de Sistemas Multiagente (SMA).
- La validez del modelo se evaluó mediante encuestas, cuyo análisis se realiza en el capítulo cuatro, los resultados ponderados se aprecian en la figura 28 (cap. 4, pág. 84). Los encuestados expresaron su aceptabilidad ante el modelo, que se desarrolló con el fin de crear un puente entre los Sistemas de Información y los SMA. La gran variedad de los modelos de desarrollo de SMA y la diversidad de formas de trabajo de cada una de ellas, influyen en la complejidad de aprendizaje de estos, por lo que el modelo desarrollado fue aceptado.

Finalmente, y para verificar que el modelo propuesto permite el desarrollo eficiente de Sistemas de Gestión de Riesgo Operativo, se procedió a la aplicación en un prototipo orientado al tipo de riesgo operativo “fraude interno” (cap. 4 pág.64). El mismo, fue evaluado desde la fase de especificación de requisitos hasta la implementación. El objetivo orientado a lograr la eficiencia en el desarrollo de Sistemas de Gestión de Riesgo Operativo se logró demostrar

comparando cada fase del desarrollo del modelo propuesto con el modelo tradicional (cascada). Los criterios de evaluación de eficiencia fueron; funcionalidad y tiempo (cap. 4, pág. 92).

La hipótesis propuesta en el capítulo uno, se demostró en el capítulo cuatro, cuyos resultados presentados en las tablas 46 y 47 permiten afirmar que existe suficiente evidencia estadística para aceptar la hipótesis. Los resultados de la encuesta demuestran asociación entre las variables dependiente e independiente de la hipótesis (cap. 4 pág. 93). Con lo que se afirma que el Modelo Multiagente MMAGIRO influye el desarrollo eficiente de sistemas de Gestión Integral de Riesgo Operativo en una IFD.

5.2 Recomendaciones

Se recomienda:

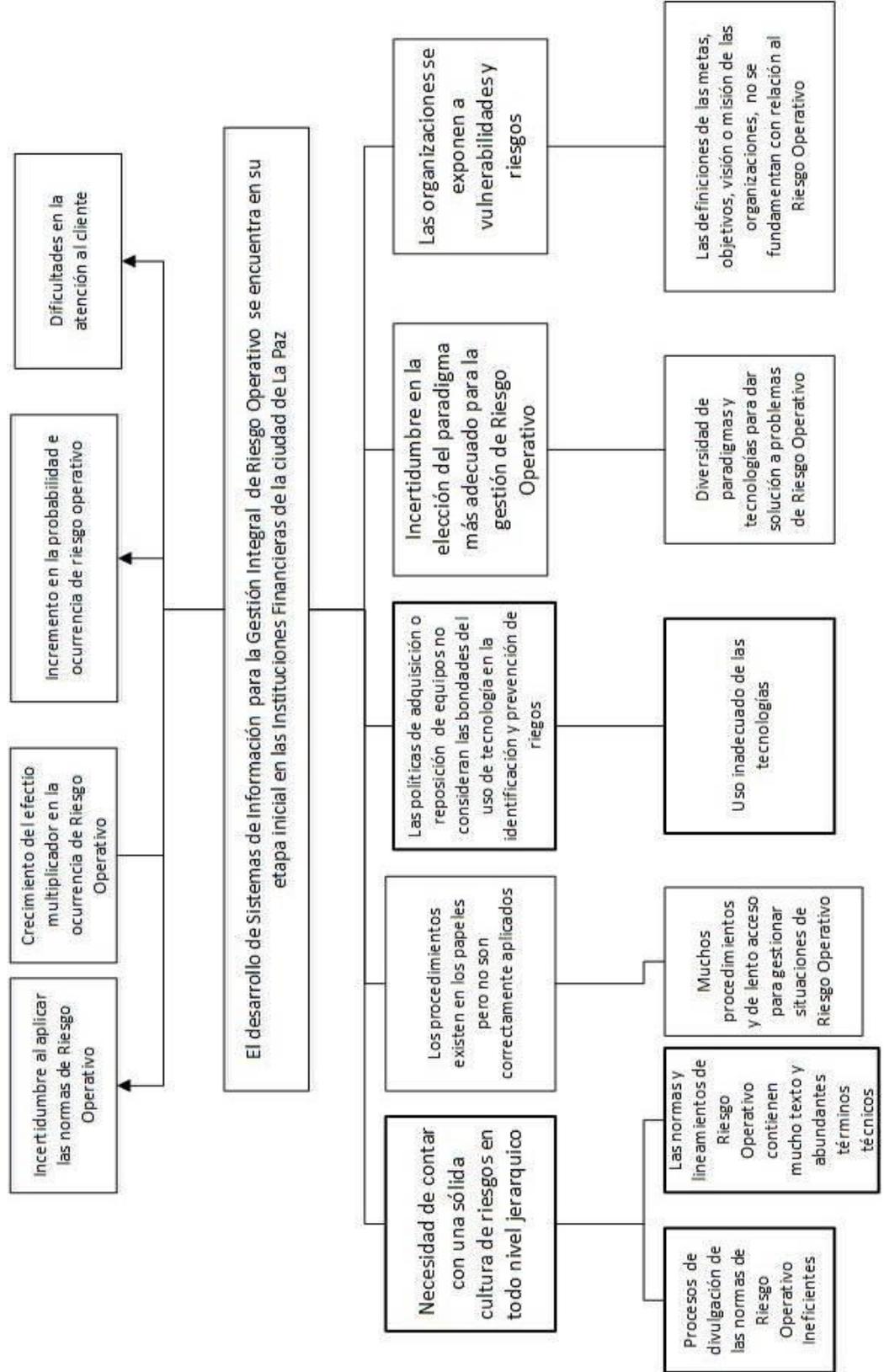
- Ampliar el desarrollo del agente de divulgación y mitigación, poniendo mayor énfasis en la capacitación y apoyo en el cambio de cultura organizacional. Considerar las necesidades de incursionar en los sistemas sensibles al contexto.
- Enriquecer las cualidades de los agentes propuestos empleando otras técnicas de la Inteligencia Artificial. Apoyar la identificación de patrones de comportamiento que permitan identificar eventos de riesgo operativo, con técnicas de *machine learning*, o apoyar la fase de mitigación, ampliando el desarrollo de agentes conversacionales.

Es justamente la posibilidad de realizar un sueño, lo que hace que la vida sea interesante.
Paulo Coelho

ANEXOS

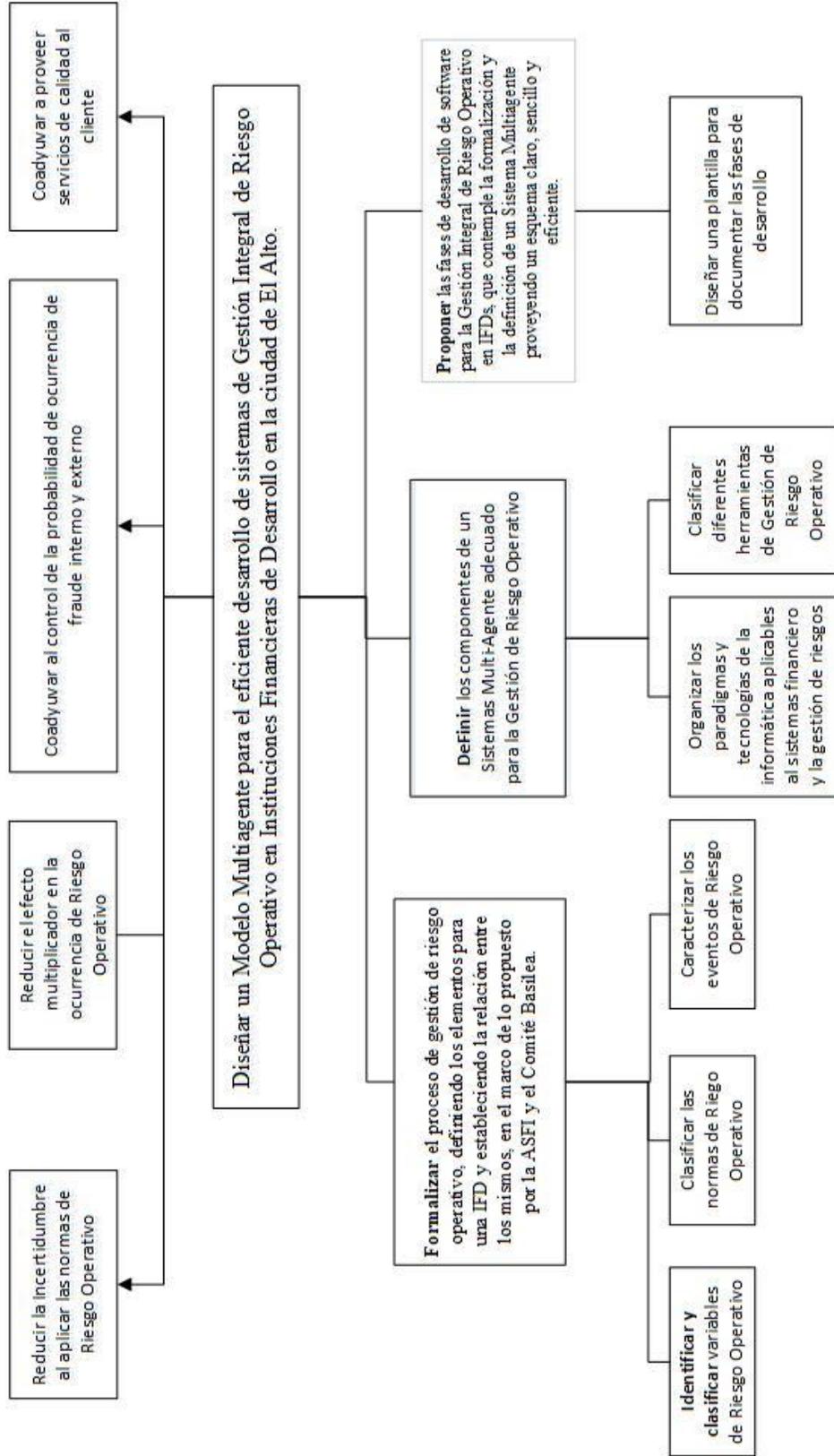
ANEXO A

ARBOL DE PROBLEMAS



ANEXO B

ARBOL DE OBJETIVOS



ANEXO C

ENCUESTA 1

EVALUACIÓN GENÉRICA DEL MODELO MULTIAGENTE PARA LA GESTIÓN INTEGRAL DE RIESGO OPERATIVO

			Totalmente en desacuerdo	En desacuerdo	Indeciso	De acuerdo	Totalmente de acuerdo
c ₁	Respuesta a los objetivos	El modelo se ajusta a los objetivos de la Gestión de RO					
c ₂	Complejidad del ciclo de vida	El modelo cubre el ciclo entero de desarrollo de software					
c ₃	Integración	El modelo integra las distintas fases del ciclo de desarrollo					
c ₄	Validaciones	El modelo incluye la realización de validaciones					
c ₅	Exactitud	El modelo soporta la determinación de la exactitud del sistema a través del ciclo de desarrollo.					
c ₆	Comunicación	El modelo es la base de una comunicación efectiva.					
c ₇	Entorno dinámico	El modelo funciona en un entorno dinámico orientado al usuario					
c ₈	Pedagogía	El modelo SE puede enseñar					
c ₉	Herramienta CASE	El modelo es soportado por herramientas CASE					
c ₁₀	Evolución	El modelo soporta la eventual evolución del sistema					
c ₁₁	Mejora	El modelo contiene actividades conducentes a mejorar el proceso de desarrollo de software					

ENCUESTA 2

EVALUACIÓN DEL CICLO DE VIDA DEL MODELO

		Totalmente en desacuerdo	En desacuerdo	Indeciso	De acuerdo	Totalmente de acuerdo
1	El modelo se ajusta a los objetivos de la Gestión de RO					
2	El modelo cubre el ciclo entero de desarrollo de software					
3	El modelo integra las distintas fases del ciclo de desarrollo					
4	El modelo incluye la realización de validaciones					
5	El modelo soporta la determinación de la exactitud del sistema a través del ciclo de desarrollo.					
6	El modelo es la base de una comunicación efectiva.					
7	El modelo funciona en un entorno dinámico orientado al usuario					
8	El modelo se puede enseñar					
9	El modelo es soportado por herramientas CASE					
10	El modelo soporta la eventual evolución del sistema					
11	El modelo contiene actividades conducentes a mejorar el proceso de desarrollo de software					

ENCUESTA 3

VALORACIÓN DEL MODELO REALIZADA POR EL USUARIO FINAL

	Muy en desacuerdo	En desacuerdo	de acuerdo	muy de acuerdo	Totalmente de acuerdo
	1	2	3	4	5
<i>El modelo MMAGIRO aplicado a la Gestión de Riesgo Operativo de tipo Fraude Interno</i>					
USABILIDAD					
Me ayuda a ser más eficaz.					
Me ayuda a ser más productivo.					
Es útil.					
Me da un mayor control sobre las actividades que realizo.					
Hace que las cosas que quiero lograr sean más fácil de hacer					
Me ahorra tiempo cuando lo uso.					
Cumple con mis requerimientos					
FACILIDAD DE USO					
Es fácil de usar.					
Es simple de usar.					
Es amigable con el usuario.					
No necesito esforzarme para usarlo.					
Puedo usarlo sin instrucciones escritas.					
SATISFACCIÓN					
Estoy satisfecho con el sistema					
Lo recomendaría					
Funciona de la forma que yo quiero que funcione					

GLOSARIO

ASFI Autoridad de Supervisión del Sistema Financiero

Comité Basilea El Comité de Basilea o Comité de Supervisión Bancaria de Basilea es una entidad que brinda orientación a nivel mundial en materia de regulación financiera. Sus recomendaciones, plasmadas en los Acuerdos de Basilea, no son de obligatorio acatamiento.

Eficiente: Uso racional de los recursos con que se cuenta para alcanzar un objetivo predeterminado. A mayor eficiencia menor la cantidad de recursos que se emplearán, logrando mejor optimización y rendimiento.

Fraude: Engaño económico con la intención de conseguir un beneficio, y con el cual alguien queda perjudicado.

FODA Matriz de Fortalezas, Oportunidades, Debilidades y Amenazas

Gestión En finanzas, es una de las tradicionales áreas funcionales de la gestión, hallada en cualquier organización, compitiéndole los análisis, decisiones y acciones relacionadas con los medios financieros necesarios a la actividad de dicha organización.

RNSF Recopilación de normas de servicios financieros

Stakeholders Partes interesadas

BIBLIOGRAFÍA

- Aguilar, J., Ríos Bolívar, A., Hidrobo, F. y Cerrada, M. (2013). *Sistemas Multi Agentes y sus Aplicaciones en Automatización Industrial*. Venezuela. Universidad de Los Andes.
- American Psychological Association (2010). *Manual de Publicaciones de la American Psychological Association (6 ed.)*. México, D.F.: Editorial El Manual Moderno
- Argente, Estefanía (2008), “GORMAS: *Guías Para el Desarrollo de Sistemas Multi Agente Abiertos Basados en Organizaciones*” (Tesis de Doctorado en Informática) Universidad Politécnica de Valencia, España
- 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
- Bernon, C., Cossentino, M., and Pavón, J. (2003). Agent-oriented software engineering. *The Knowledge Engineering Review.*, (2):99–11651–63.
- Baquero Herrera Mauricio (2010).” *Riesgo operativo: ¿Hacia dónde vamos?*” Director del Observatorio de Derecho Financiero y del Mercado de Valores. Universidad externado de Colombia -ASOBANCARIA. Noviembre 2016.
- Barzanallana, R. (2006) Universidad de Murcia (España). Página del profesor Rafael Barzanallana. Asignatura de informática aplicada a la gestión pública. Metodologías de desarrollo de software.16 de octubre de 2019
<http://www.um.es/docencia/barzana/IAGP/Iagp3.html#BM2>
- Cabrera, O. (2009), “*Enfoque de Gestión de riesgo operativo para Bancos del Sistema Financiero Boliviano*” (Tesis de Licenciatura Carrera de Contaduría), Universidad Técnica de Oruro
- 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.
- Ferber, J., (1998). “*Multi-agent systems: an introduction to distributed artificial intelligence*”. Addison-Wesley, Harlow.
- Finrural (2019) Nuestras socias. Recuperado de <https://www.finrural.org.bo/nuestras-socias.php>
- Genero, M., Cruz-Lemus, J., Piattini, M. (2014). *Métodos de investigación en Ingeniería del software*. Madrid España, Ed. Ra-Ma

- Gomez, N. (2009). *Universidad Nacional de Colombia, Medellín*. Recuperado el 09 de Septiembre de 2013, de http://www.unalmed.edu.co/~ndgiral/Archivos%20Lectura/Archivos%20curso%20Riesgo%20Operativo/gestion_riesgo_introduccion_2009.pdf
- Gruber, T.R., (1993). “*A translation approach to portable ontology specifications*”. Knowledge Acquisition 5, 199–220. doi:10.1006/knac.1993.1008
- Hernández, R., Fernandez Collao, C., Baptista, P. (2010) *Metodología de la Investigación*. México. McGraw-Hill
- Hurtado, J. (2000) *Metodología de la investigación holística*. Caracas Venezuela, Fundación Sypal.
- Hurtado, J. (2010) *Guía para la comprensión holística de la ciencia*. Caracas Venezuela, Fundación Sypal.
- Huhns, M. N. (2004). Agent uml notation for multiagent system design. In *IEEE Internet Computing*, pages 63–71.
- Jones, V. y Jo J. H. (2004). Ubiquitous learning environment: An adaptive teaching system using ubiquitous technology. Proceedings of the 21st ASCILITE Conference, 468 – 474.
- Julián, Vicente & Botti, V.. (2003). Desarrollo de sistemas multi-agente en tiempo real. *Inteligencia artificial: Revista Iberoamericana de Inteligencia Artificial*, ISSN 1137-3601, N°. 18, 2003, pags. 65-80. 7.
- Lavell, Allan. (2016). “*Conceptos y definiciones de relevancia en la gestión del riesgo*”. Colaboración del Programa de Naciones Unidas para el Desarrollo (PNUD) Octubre 2016. <http://cidbimena.desastres.hn/staticpages/index.php?>
- Lesser, V.R., Fennell, R.D., Erman, L.D., Reddy, D.R., (1975). Organization of the Hearsay-II Speech Understanding System. *IEEE Transactions on Acoustics, Speech, and Signal Processing ASSP-23*, 11–24.
- Llaguno, M. (2005). Gestión del riesgo operativo en las entidades de crédito: un camino sin retorno. *Cuadernos de Gestión*. 5(1) España
- López, O. (2018), “De riesgos operativos y operativos, el desafío boliviano”, *Agencia de Noticias Fides*,(21 23)
- Martínez, H. A. V., Moreno, F. J. T., & Miranda, C. A. L. (2010). Aprendizaje ubicuo en la enseñanza de las matemáticas. *Rev. Estud. Cult*, 5, 123-136.
- McConnell, S. (1996). “*Rapid Development: Taming Wild Software Schedules*”. Microsoft Press. United States of America.

- Mendez, E. (2006). *Modelo de evaluación de metodologías para el desarrollo del software*. Trabajo de postgrado. Universidad Católica Andrés Bello. Caracas Venezuela.
- Neches, R., Fikes, R., Finin, T., Gruber, T., Patil, R., Senator, T., Swartout, W.R., (1991). Enabling Technology for Knowledge Sharing. *AI Mag.* 12, 36–56.
- Noy, N.F., McGuinness, D.L., (2001). “*Ontology Development 101: A Guide to Creating Your First Ontology*”
- Pacheco, D. (2009). “Riesgo Operacional conceptos y mediciones”. *Comisión para el mercado financiero*. Chile
- Power, M. (2010). “*La invención del riesgo operacional*”. En *La gestión del riesgo operacional: De la teoría a su aplicación*, editado por Ana Fernández Laviada, 107-08. Madrid: Limusa Noriega Editores.
- Pretorius, A.J., (2004). Ontologies - Introduction and Overview (Adapted from: “Lexon Visualisation: Visualising Binary Fact Types in Ontology Bases”, MSc Thesis).
- Russell, S. J. y Norvig, P. (2004) *Inteligencia Artificial Un Enfoque Moderno*. Madrid. Prentice Hall.
- Salazar, Oscar (2014) “*Modelo de Sistema Multi-agente ubicuo, adaptativo y sensible al contexto para ofrecer recomendaciones personalizadas de recursos educativos basado en ontologías*” (Tesis de Maestría). Universidad Nacional de Colombia, Departamento de Ciencias de la Computación y de la Decisión, Medellín, Colombia.
- Sivila. J.A.(2013) “*Introducción a la gestión integral de riesgos*”, programa Diplomado en Control de Operaciones y Control de Riesgos, MicroFin, UDI: La Paz Bolivia
- Schulze, V.H.(2014) “*Gestión de Riesgo Operacional*”, programa Diplomado en Control de Operaciones y Control de Riesgos, MicroFin, UDI: La Paz Bolivia
- Somerville, I. (2005). “*Ingeniería del software*”. Madrid. Pearson.
- Uschold, M., Jasper, R., (1999). “*A Framework for Understanding and Classifying Ontology Applications*”. Presented at the Workshop on Ontologies and Problem-Solving Methods, Stockholm.
- Venturini, Verónica (2012) “*Sistema Multi-Agente basado en Contexto, Localización y Reputación para dominios de Inteligencia Ambiental*”, Programa Doctorado en Ciencia y Tecnología Informática, Universidad Carlos III de Madrid. Madrid, España.
- Viteri, M. (2018) “*Desarrollo de una metodología para la administración del riesgo operativo en una institución financiera del sector de economía popular y solidaria, basada en el*

marco integrado COSO ERM”, Programa Maestría en Finanzas y Gestión de Riesgos, Universidad Andina Simón Bolívar Sede Ecuador Área de Gestión.

Wooldridge, M..(2002) “*An Introduction to MultiAgent Systems*”. Inglaterra. John Wiley & Sons LTD.

Wooldridge, M..(1999). “*Intelligent Agents*”. In Weiss G. (ed) *Multiagents Systems. A modern Approach to Distributed Intelligence*. MIT Press, pp. 27-77.

Wooldridge, M. & Jennings, N. (1995) *Intelligent Agents: Theory and Practice*. The Knowledge Engineering Review.

Wohlin, C. (2014) Guidelines for Snowballing in Systematic Literature Studies and a Replication in Software Engineering (EASE), 312-330

Unzaga, S., Álvarez, M., Durán, E. (2015). *Modelo de requerimientos de una aplicación de apoyo al aprendizaje ubicuo para el ingreso universitario*. Congreso TE & ET, 455-462