MAESTRÍA EN AUDITORIA DE TECNOLOGÍA DE LA INFORMACIÓN

MARCO METODOLÓGICO PARA LA SUPERVISIÓN DEL ÁREA DE TECNOLOGÍA, APLICABLE A LAS INSTITUCIONES FINANCIERAS DEL SEGMENTO 3, 4 Y 5 DE LA ECONOMÍA POPULAR Y SOLIDARIA.

Propuesta de artículo presentado como requisito para la obtención del título:

Magíster en Auditoría de Tecnologías de la Información

Por la estudiante:
Jessica Dolores CAMBI ALVARADO.

Bajo la dirección de:
Raúl Vicente GONZALEZ CARRIÓN.

Universidad Espíritu Santo
Maestría en Auditoría de Tecnología de la Información
Samborondón - Ecuador
Enero del 2017

Marco Metodológico para la supervisión del área de tecnología, aplicable a las instituciones financieras del segmento 3, 4 y 5 de la economía popular y solidaria

Methodological Framework for the supervision of the technology area, applicable to financial institutions of segments 3, 4 and 5 of the popular and solidarity

Jessica Dolores CAMBI ALVARADO[1]
Raúl Vicente GONZALEZ CARRIÓN[2]

Resumen

A pesar de la gran cantidad de material publicado sobre marcos y metodologías para la supervisión del área de tecnología, existe poca información sobre la aplicabilidad de estos a instituciones financieras de la Economía Popular y Solidaria con recursos limitados. Por lo que el presente estudio de investigación aborda este aspecto desde la perspectiva de supervisión al área de tecnología enfocada en riesgo operativo. La propuesta se fundamenta en una revisión literaria de los principales conceptos sobre riesgo, así como modelos aplicables a la auditoría de tecnología, entre los que se considera: COBIT 5, COSO 2013 e ISA-315. La investigación presenta un modelo de supervisión, a través de un esquema gráfico el cual se sustenta en normas internacionales de auditoria como es el caso de ISA-315 Norma Internacional de Auditoría referente a la identificación de riesgos, en dicho esquema se establece como tareas primordiales la identificación de riesgos y la verificación de controles implementados como medida de prevención de pérdidas económicas. Por otra parte y como complemento de la metodología propuesta se define una matriz de supervisión la cual considera las actividades necesarias para la identificación de controles en el área de tecnología sobre las siguientes categorías: validez de la información, centro de datos, seguridad de accesos, cambios en aplicaciones y adquisiciones.

La validación del marco metodológico propuesto, se realiza mediante la técnica de grupos focales, con la finalidad de obtener datos cualitativos que muestran la percepción de los participantes sobre el marco metodológico definido, para dicha validación se abarcó un grupo de profesionales con amplia experiencia en procesos de supervisión y análisis de riesgo operativo tecnológico en entidades financieras regidas por la Superintendencia de Economía Popular y Solidaria.

Palabras clave: Riesgo tecnológico, Supervisión tecnológica, ISA 315, Economía Popular y Solidaria, Riesgo Operativo

Abstract

There are several studies on the frameworks and methodologies for performing IT audits, however there is little information about its application in financial institutions of the Popular and Solidarity Economy with limited resources. This research study raises the IT audit with a focus on operational risk. The proposal is based on a literary review of the main risk concepts, as well as models applicable to IT auditing, including: COBIT 5, COSO 2013 and ISA-315. The research presents an audit model for IT, through a graphic scheme which is based on international auditing standards such as ISA-315 International Standard on Auditing in reference Identifying and assessing the risks, this scheme establishes as main tasks the identification of risks and the recognition of controls implemented as a measure to prevent economic losses. In addition, as a complement to the methodology, an audit matrix is proposed which serves as a tool for the identification of controls in the IT area, through the following categories: validity of information, data center, access security, changes in applications and system acquisitions.

The validation of the proposed methodological framework is done using the technique of focus groups, in

[1] Estudiante de Maestría en Auditoría de Tecnología de Información, Universidad Espíritu Santo – Ecuador. E-mail jcambi@uees.edu.ec.
[2] CISA, CBCP, CICA, ISO 22301 LI, ISO 22301 LA, ISO 27001 IA, COBIT, MSc. Docente de la Maestría en Auditoría en Tecnologías de la Información Universidad Espíritu Santo- Ecuador. E-mail rvgonzalez@deloitte.com

order to obtain qualitative data that show the participants' perception about the study, this validation is done with a group of professionals with extensive experience in processes of audit and analysis of technological operational risk in financial institutions of the Popular and Solidarity Economy.

Key words	Technological risk, Technological supervision, ISA 315, Popular and Solidarity Economy, Operational Risk

INTRODUCCIÓN

La información y la tecnología constituyen una pieza fundamental en el día a día de las organizaciones económicas, financieras y de las empresas productivas a nivel global, formando parte de sus activos más valiosos y necesarios para la prestación de servicios.

En este contexto en el Ecuador a partir del año 2008, en la nueva Constitución, en el artículo 283 se reconoce a la Economía Popular y Solidaria como una forma de organización económica; y, cuya Ley publicada en el año 2011, expresa la creación de la Superintendencia de Economía Popular y Solidaria (en adelante, SEPS) como ente de control para las instituciones financieras y no financieras. Entre las instituciones financieras se encuentran: cooperativas de ahorros crédito, bancos comunales, cajas de ahorro entre otros.

Cabe señalar que la Resolución Nro. 038-2015-F de la Junta de Política y Regulación Monetaria y Financiera, establece la segmentación de las entidades del sector financiero popular y solidario de acuerdo al tipo y al saldo de sus activos en 5 segmentos, estableciendo al segmento 1 como el más grande con activos mayores a 80’000.000,00 (La Junta de Política y Regulación Monetaria y Financiera, 2015). La tabla 1 detalla la segmentación de las instituciones financieras de acuerdo a sus activos:

Tabla 1
Segmentación de las Instituciones Financieras de la Economía Popular y Solidaria

Segmento		Activos (USD)		
1	Mayor a	80’000.000		
2	De	20’000.000	a	80’000.000
3	De	5’000.000	a	20’000.000
4	De	1’000.000	a	5’000.000
5	Menor a	1’000.000		
	Cajas de Ahorro, bancos comunales y cajas comunales			

Fuente: Resolución Nro. 038-2015-F de la Junta de Política y Regulación Monetaria y Financiera

La SEPS como parte de sus competencias y con el conocimiento sobre la importancia del área de tecnología para el sector financiero, realiza la supervisión del área de tecnología de las instituciones, con un enfoque basado en riesgo operativo, en el cual se verifica el acatamiento de las disposiciones y normativas, por parte de organismos de control; así como la ejecución de buenas prácticas en lo referente a los principios de seguridad de la información y continuidad del negocio, fomentando de esta manera una cultura de mejoramiento continuo en el sistema financiero.

El riesgo operativo es considerado como un elemento de evaluación por parte de organismos de control como la Superintendencia de Economía Popular y Solidaria y la Superintendencia de Bancos, quienes a través de la evaluación basado en riesgo operativo intentan minimizar la ocurrencia de pérdidas financieras debido a fallas en las áreas de tecnología, procesos, eventos externos, sistemas internos, inclusive en el recurso humano.

La SEPS en cumplimiento a lo estipulado en el artículo 280 del Código Orgánico Monetario y Financiero, Libro I, (2014a), “efectuar un proceso de supervisión permanente, in situ y extra situ, a las entidades financieras, que permita determinar la situación económica y financiera de las entidades, el manejo de sus negocios, evaluar la calidad y control de la gestión de riesgo (…)” (p.83); para el proceso de supervisión en lo referente al área de tecnologías, en las entidades financieras considera la aplicación de normativa y resoluciones emitida por la Superintendencia de Bancos, las cuales son factibles de aplicación para instituciones financieras del segmentos 1 y 2.

Ahora bien, para la evaluación de las instituciones financieras del segmento 3, 4 y 5 de la Economía Popular y Solidaria existe una evidente falta de normativa y resoluciones aplicables, debido a que la existente se basa en controles a instituciones con un alto valor en sus activos y recursos asignados a los departamentos de tecnología de las

instituciones, lo cual no es el caso en las analizadas.

La normativa emitida por la Superintendencia de Bancos implica componentes que no pueden ser evaluados por motivo de su inexistencia en las instituciones del segmento en mención; este comportamiento se debe al escaso análisis realizado a entidades financieras con una restringida presencia de recursos no solo para el área de tecnología, sino para toda la institución.

La situación antes descrita induce a que la evaluación a las instituciones del segmento 3, 4 y 5 sea un proceso impredecible cuyo resultado no represente el verdadero nivel de riesgo en el que se encuentra inmerso la entidad, en lo referente a la administración del área de tecnologías y el manejo de deficiencias registradas en la seguridad, integridad confiabilidad y disponibilidad de la información.

Con base a lo expuesto la presente investigación establece y contribuye con un marco metodológico de supervisión basado en riesgo y la verificación de controles para la evaluación del área de tecnología de las instituciones financieras pertenecientes al segmento 3, 4 y 5, con la finalidad de determinar su nivel de riesgo al que se encuentra expuesta la institución y como respuesta a la hipótesis plantea ¿Cómo supervisar el área tecnológica de las instituciones financieras del segmento 3, 4 y 5 de la Economía Popular Solidaria?.

Además la investigación planteada proveerá de una herramienta que permita conocer la situación real de la administración y gestión del área tecnológica en las instituciones financieras de menor tamaño pertenecientes a la Economía Popular y Solidaria, así como la identificación de oportunidades de mejora luego del proceso de supervisión de dichas instituciones y como método de control interno.

La importancia de la definición de nuevos marcos metodológicos para la supervisión del área tecnológica, en instituciones financieras, genera nuevas posiciones en el hecho de la participación de sus actores y como una cultura de control interno de una entidad, ya que los mismos permiten evaluar los procesos en referencia a calidad, rendimiento y flexibilidad y definir nuevos métodos de control y vigilancia que se acoplen a sus realidades.

Los avances en tecnología han logrado que los procesos en las entidades financieras sean mejores y que se mantengan a niveles competitivos. Esta publicación canaliza un nuevo paradigma en lo referente a la supervisión tecnológica constituyendo una alternativa en el proceso de supervisión, la cual genera estructuras de control para combatir los riesgos y permite la emisión de nuevas actividades de valor técnico que permitan a las entidades financieras actuar con mayor certeza y contribuyendo a cerrar puertas de fraudes económicos en lo relativo a la información financiera.

Para la presente estudio se realiza una revisión bibliográfica sobre los principales marcos y buenas prácticas referentes a la supervisión, evaluación y control interno del área de tecnología y que su aplicación e implementación sea factible en instituciones financieras de menor tamaño entre los marcos revisados se hace mención a: Control Objectives for Information and related Technology 5 (por sus siglas en inglés, en adelante, COBIT5), Committee of Sponsoring Organizations of the Treadway Commission (por sus siglas en inglés, en adelante, COSO), International Standard on Auditing “Identifying and Assessing the Risks of Material Misstatement through Understanding the Entity and Its Enviroment” (por sus siglas en inglés, en adelante, ISA 315), en lo referente al concepto de riesgo se amplía la revisión literaria a través de International Organization for Standardization. Guide 73:2009 Risk management – Vocabulary (por sus siglas en inglés, en adelante, ISO Guide 73:2009) y el Sistema de Gestión de la Seguridad de la información para la Gestión Organización (en adelante, ISO 27000).

En una segunda instancia y como parte de la metodología propuesta se construye un esquema de supervisión, el cual es validado a través de una metodología cualitativa y cuyas bases se fundamentan en International Standard on Auditing 315, más conocido como ISA 315 - Norma Internacional Estándar en Auditoría, como punto de partida para la elaboración del marco metodológico de supervisión; así como para la definición de criterios de evaluación, los cuales se fundamentan a través del conocimiento de la entidad y su entorno.

Finalmente para la estimación de la validez del marco metodológico propuesto, así como de su aplicabilidad, se define como instrumento de validación un grupo focal de 5 profesionales de la rama de auditoría tecnológica, especializados en supervisión de instituciones financieras de la Economía Popular y Solidaria, quienes evaluaran el marco propuesto y su pertinencia para la identificación de debilidades y oportunidades de mejora en los controles, acordes al riesgo operativo y normas de auditoría internacionales, con la finalidad de inferir acciones y recomendaciones tendientes a optimizar los resultados obtenidos a través del marco de supervisión propuesto.

MARCO TEÓRICO

La Economía Popular y Solidaria en el Ecuador

La Economía Popular y Solidaria es una forma de organización económica reconocida por la constitución de la República del Ecuador 2008, en su artículo 283 el cual establece que el sistema económico se integra por las formas de organización económica pública, privada, mixta, popular y solidaria y las demás que la Constitución determine. (Asamblea General Constituyente, 2008).

Para estructurar lo establecido anteriormente se emite la Ley Orgánica de la Economía Popular y Solidaria y del Sector Financiero Popular y Solidario (LOEPS), en la que se define en el artículo 1 a la Economía Popular y Solidaria, "como la forma de organización económica, donde sus integrantes, individual o colectivamente se organizan y desarrollan procesos de producción, intercambio, comercialización, financiamiento, organizan y consumo de bienes y servicios, para satisfacer necesidades y generar ingresos, basados en relaciones de solidaridad, cooperación y reciprocidad" (Ministerio Coordinador de Desarrollo Social (MCDS) ; Ministerio de Inclusión Económica y Social (MIES) ; Corporación Nacional de Finanzas Populares y Solidarias (CONAFIPS), 2012, pág. 4).

Inicios de la Superintendencia de Economía Popular y Solidaria SEPS

Con el amparo de la constitución y en cumplimiento con la LOEPS, se da la creación de la Superintendencia de Economía Popular y Solidaria (SEPS), como ente de control para las instituciones del sector financiero y no financiero de la Economía Popular y Solidaria, el cual empieza sus funciones en noviembre 2012. Dentro de sus atribuciones se estable la supervisión de entidades financieras, la cual tiene un enfoque basado en riesgos, con la finalidad de fomentar una cultura de mejoramiento continuo y como herramienta para precautelar los fondos de los socios (Superintendencia de Economía Popular y Solidaria, 2015).

En la actualidad un enfoque basado en riesgos es una práctica aceptada, es así que la Junta de Política y Regulación Monetaria y Financiera (2015) define en su Resolución Nro. 128-2015-F a la matriz de riesgos como: "una herramienta de control y gestión en la que se identifican y cuantifican los riesgos, con base en el nivel de probabilidad y el impacto de los mismos; facilitando la administración de los riesgos que pudieran afectar los resultados y el logro de los objetivos institucionales" (p.2).

Segmentación de las Entidades Financieras

El artículo 447 del Código Orgánico Monetario y Financiero define que las entidades financieras del sector financiero, popular y solidario se

ubicarán en los segmentos que la Junta determine (Asamblea Nacional Constituyente, 2014b), actualizándose de manera anual y de acuerdo con la variación del índice de precios del consumidor y el vínculo con sus territorios.

Tabla 2
Segmentación de las Instituciones Financieras de la Economía Popular y Solidaria por Activos y Vínculo Territorial

Segmento	Activos (USD)	Vínculo Territorial
1	Mayor a 80'000.000,00	No aplica
2	20'000.000,01 - 80'000.000,00	No aplica
3	5'000.000,01 - 20'000.000,00	Cuando coloquen al menos el 50% de los recursos en los territorios donde estos fueron captados
4	1'000.000,01 - 5'000.000,00	
5	Hasta 1'000.000,00	
	Cajas de Ahorro, bancos comunales y cajas comunales	

Fuente: Resolución Nro. 038-2015-F de la Junta de Política y Regulación Monetaria y Financiera

Las Tecnologías de la Información y el Sector Financiero de la Economía Popular y Solidaria

La SEPS dentro de su plan de supervisión incluye como elemento de evaluación al riesgo operativo al cual el Comité de Basilea (2004) lo define como "la perdida debido a la inadecuación o a fallos de los procesos, el personal y los sistemas internos o bien a causa de acontecimientos externos" (p.6). Por otro lado el riesgo operativo es considerado como elemento de evaluación por parte de organismos de control como la SEPS y la Superintendencia de Bancos la cual define al riesgo operativo como aquel que puede producir pérdidas financieras en las instituciones y sus factores se origina por procesos, eventos externos, personas, y tecnologías de la información (Superintendencia de Economía Popular y Solidaria, 2015).

Es importante destacar que en este sentido las entidades financieras de la Economía Popular y Solidaria, se encuentran sujetas al control y regulación por parte de la SEPS, misma que ejecuta auditorias y revisiones a las áreas de tecnología, de acuerdo con las normas, leyes y reglamentos definidos para el cumplimiento regulatorios referentes a la administración y gestión de tecnologías, la cual es factible de aplicación en los casos de las instituciones financieras pertenecientes a los segmentos 1 y 2, por el contrario para los segmentos inferiores se vuelve algo complejo debido a sus recursos limitados en esta área.

Hay que mencionar que desafortunadamente el uso de la tecnología en las instituciones financieras no solo significa beneficios y ventajas, sino en varias ocasiones es foco de problemas para las instituciones. Además representa un desafío para el auditor informático, quien requiere de una preparación adecuada y de nuevos procedimientos y conocimientos en lo referente a controles y riesgos involucrados en las instituciones financieras que funcionan soportadas en las Tecnologías de la Información y Comunicaciones (Gubba, Gutfraind, & Rodríguez, 2001).

En referencia a las exigencias requeridas, para el auditor informático existen varios estudios desde años atrás, en la que algunos organismos mundiales como es el caso de International Federation of Accountants (IFAC), ha emitido guías de educación las cuales plantea una serie de lineamientos sobre Tecnologías de la Información y su importancia (International Federation of Accountants, IFAC, 2009a), es así que se menciona a: International Education Standards (IES 2) y la aplicación del mismo a través de International Education Practice Statement – Information Technology for Professional Accountants (IEPS 2.1).

Además la formalización de la importancia del buen desempeño y del conocimiento requerido por parte del auditor, referente a las Tecnologías de Información y Comunicación, se puede observar de manera más detallada en las Normas Internacionales de Auditoria 315 (ISA-

315) (International Federation of Accountants (IFAC), 2015a).

En el mismo sentido otro organismo mundial que ha demostrado su interés sobre este tipo de estudios son los realizados por Information Systems Audit and Control Association (por sus siglas en inglés, en adelante, ISACA), el cual sobresale Control Objectives for Information and related Technology, COBIT por su siglas en inglés, el cual plantea una serie de estructuras, controles y habilidades vinculadas con Tecnologías de la Información y Comunicación y los sistemas de información, en sus diferentes niveles: evaluación, control, mantenimiento, construcción y diseño y que puede ser aplicado a cualquier tipo de institución sin distinguir su tamaño o línea de servicios (ISACA, 2012).

COBIT establece que el auditor debe obtener un entendimiento de cómo la entidad ha respondido a los riesgos que surgen de la aplicación de las Tecnologías de la Información y Comunicaciones, y la identificación de aquellos riesgos que si no se mitigan, podrían resultar en situaciones que comprometerían la estabilidad de una entidad (Radovanović, Radojević, Lučić, & Sarac, 2010).

Finalmente se debe agregar que al ser el sector financiero de la Economía Popular y Solidaria, un nuevo tipo de organización económica reconocida en el Ecuador, existen algunos estudios de investigación, que se centran en las seguridades y controles que deberían existir en las áreas de tecnología de las entidades financieras, es así el caso de la propuesta doctoral “Las mejores prácticas aplicadas a un análisis de riesgos de seguridad de la información para las entidades financieras controlas por la Superintendencia de Economía Popular y solidaria (Cooperativas de Ahorro y Crédito) que conforman el grupo de asistencia” (Cevallos Guera, 2015), en el cual se plantea un análisis de seguridad informática con base a denuncias presentadas en la Fiscalía General del Estado por socios de cooperativas de ahorro y crédito.

Por otra parte Pazmiño (2015) en su investigación presenta una herramienta metodológica enfocada en la continuidad del negocio para las instituciones financieras de la Economía Popular y Solidaria, la cual permite determinar el nivel de madurez en la gestión de continuidad del negocio, dirigido a las instituciones financieras del segmento 4.

Para concluir la revisión de estudios sobre Economía Popular y Solidaria, se hace referencia al artículo de “Auditoría basada en coso ERM a la Gestión de Riesgo Operativo para Cooperativas de Ahorro y Crédito”, el cual presenta un análisis de riesgo basado en riesgo operativo, en el cual se analiza de manera detallada cada uno de sus factores: procesos, personas, tecnología y eventos externos, (Obando Changuán, 2014).

La Auditoría y las Tecnologías de la Información

La auditoría presente a lo largo de la historia en las organizaciones, es definido por Porter y Burton (1980) como “el examen de la información, por una tercera persona distinta de quién la preparó y del usuario, con la intención de establecer su veracidad; y el dar a conocer los resultados de este examen, con la finalidad de aumentar la utilidad de tal información para el usuario”; atendiendo a estas consideraciones, Senft & Gallegos (2008) determinan que la auditoría en la actualidad asume un papel protagónico dentro de las organizaciones, ya que permite garantizar un buen sistema de control interno y el cumplimiento de requisitos.

Mientras tanto Méndez & Oliveros (2016) revelan que la auditoría se encuentra presente en varias áreas de la organización, al ser considerada como una herramienta valiosa, la cual permite identificar problemas y riesgos presentes dentro de las organizaciones, atendiendo a esta consideración, es importante recalcar que el ámbito de la tecnología no es la excepción; es así que varios autores han dado sus definiciones con respecto a este tema; como el de Joseph P. Martino (1994) quien describe a la auditoría de la tecnología como el

proceso de evaluación del estado de los recursos tecnológicos de la organización, con el fin de revelar las fortalezas y debilidades del negocio en este sentido; además de, evaluar las situaciones de mejora referente a los competitividad y mejora continua.

Por otra parte la OLACEFs (2011) define a la Auditoría de Gestión de las Tecnologías de Información y Comunicación, como un examen de carácter objetivo, crítico, sistemático, independiente y selectivo de las normas y políticas, cuyo objetivo es la de emitir una opinión profesional sobre el uso de recursos informáticos, controles implementados, optimización de los recursos y la oportunidad de la información, dentro de la organización.

Definición de Riesgo

El análisis de riesgos y gestión de riesgos son disciplinas que han aumentado en popularidad en los últimos años (Vaughn Jr. Rayford B., 2004). Sin embargo es importante el entender en una primera instancia que es el riesgo:

ISO Guide 73:2009 Risk management – Vocabulary (2009), lo describe como la combinación de las consecuencias de un suceso (incluyendo cambios en las circunstancias) y la probabilidad asociada de la ocurrencia. Por otro lado la norma ISO 31000 caracterizada por ser aplicada a cualquier tipo de riesgo ya sea este financiero, corporativo, de infraestructura, entre otros; a tratado al riesgo con un ajuste en cuanto a su definición dada en la Guide 73:2009, determinando al riesgo en términos del efecto de la incertidumbre en los objetivos, así también hace referencia a las situaciones positivas como oportunidades y negativas en términos de pérdidas (Ormella Meyer, 2014).

La Familia de la ISO 27000 (2013) ha adoptado el concepto de riesgo como la combinación de probabilidad y consecuencia, definiéndola como la posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.

Por otra parte los riesgos referente a TI son definidos por ISACA (2009), como parte del universo de riesgos a los que está expuesta una organización, en ciertas ocasiones los considera como parte del riesgo operativo, y en otras como riesgo financiero cuando se hace mención al riesgo estratégico de TI, como consecuencia de lo anterior expuesto se puede decir que el Riesgo de TI o Risk IT se lo define como el riesgo asociado con: la operación, participación, uso, propiedad, influencia y adopción de las TI en la organización, con influencia en lo referente a la frecuencia y magnitud incierta.

Marcos metodológicos para la Gestión de Riesgo en Tecnologías de la Información.

En la actualidad existe algunas metodologías enfocadas en riesgo las cuales permiten obtener una mejor perspectiva referente al riesgo así es el caso de Magerit Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información y cuya primera tarea es el análisis de los riesgos, se enfoca en realizar una identificación de las amenazas latentes sobre los activos, así como de la vulnerabilidad existente en los mismos sobre las amenazas, gracias a este análisis es posible la estimación del grado de perjuicio que podría ocasionar una falta en la seguridad dentro de la organización (AMUTIO, Candau, & Mañas, 2012).

Por otra parte tenemos la metodología de evaluación de los riesgos a la seguridad de la información denominada OCTAVE, cuya evaluación estratégica se basa en riesgos y es un proceso auto dirigido, lo que quiere decir que las personas no solo participan en la evaluación sino que comparten la responsabilidad, priorizando de esta manera los recursos críticos y las áreas de mejora. Siendo sus 3 principales aspectos claves: el riesgo operacional, las prácticas de seguridad y la tecnología. Su evaluación es implementada a través de la construcción de perfiles de amenazas con base en los recursos, la identificación de vulnerabilidades en referencia a la infraestructura y el desarrollo de estrategias y

planes de seguridad (Gómez Ramirez & Ospina Gil, 2014).

De igual manera existen otras metodologías sobre la evaluación de riesgos, las cuales no son objeto de estudio; sin embargo es necesario mencionar su relevancia con respecto al riesgo, ISO/IEC 27005 (2011) la cual sustituye a otras normas como la de Gestión de la Información y Comunicaciones Tecnología de Seguridad, la norma ISO/IEC TR 13335-3:1998 y la norma ISO/IEC TR 13335-4:2000. Que de igual manera que otras metodologías define al riesgo como una amenaza que explota la vulnerabilidad de un activo pudiendo causar daño, así mismo los criterios incluyen la evaluación del riesgo, aceptación de riesgos y criterios de evaluación de impacto (Mcube U & Von Solms, 2016).

Mejores prácticas de Auditoría para las Tecnologías de la Información.

Debido a la exigibilidad de afianzar su información, que se requiere en el área tecnológica para las empresas financieras hoy se presenta una serie de prácticas necesarias con la finalidad de encontrar soluciones a estas exigencias, a continuación se detallan algunas prácticas como:

COSO (2013) Marco Integrado de Control Interno permite a las organizaciones desarrollar con eficacia y eficiencia los sistemas de control interno que se adapten a los ambientes operativos cambiantes de las organizaciones; así como también contribuyen a la mitigación de riesgos a niveles aceptables.

Por otra parte Deloitte Galaz, Yamazaki, Ruiz Urquiza y S.C., (2015) describen al marco de control, a través de sus cinco componentes en los que se fundamenta sus 17 principios, reflejando una relevancia hacia los Sistemas de Información, los cuales se relacionan con 14 de sus principios, los cuales hacen referencia al tema de TI. En este sentido Anderson y Eubanks (2015) destacan dentro de los principios y como primera línea de defensa, a las actividades desarrolladas por la organización sobre tecnología, como sustento para el logro de objetivos, al mismo tiempo incluye la creación, comunicación de políticas y procedimientos relativos a TI, siendo parte de la garantía de los controles y el apoyo de procesos de monitoreo y evaluación frente al riesgo.

COBIT 5, se describe como un marco que ayuda a las organizaciones a crear un valor óptimo a partir de la tecnologías de la información, estableciendo balance entre recursos, beneficios y riesgo, con un enfoque holístico para gobernar y administrar la información y tecnología relacionada con toda la empresa (Nugroho, 2014). El proceso de administración de TI de COBIT 5, tiene un impacto directo significativo en el control interno, los objetivos de gobierno de TI, la calidad de la información y en el valor del negocio (Zaitar & Ouzarf, 2012). COBIT 5 expuesto por Information Systems Audit and Control Association (Asociación de Auditoría y Control de Sistemas de Información) ISACA (2012), posibilita que las tecnologías de la información y relacionadas se gestionen y gobiernen como un todo, es decir, de forma holística en todos los niveles de la organización, en el que se incluye a todas las áreas funcionales y de negocios, considerando los intereses relacionados con TI.

Cabe señalar que para que el proceso sea exitoso Aloini, Dulmin, & Mininno (2012) manifiestan que el proceso de administración de Tecnologías de la Información de COBIT 5, puede ayudar a una organización a conseguir los objetivos de la gobernanza y finalmente la creación de valor del negocio.

Por otra parte para procesos de auditoría al área de tecnología se puede hacer uso de la Norma ISA 315 de la International Federation of Accountansts IFCA (2012) o conocida también como NIA 315, la cual formaliza la identificación y evaluación del riesgo material, por medio del conocimiento y la comprensión de la entidad y su entorno; por lo que define al control interno como un proceso diseñado, implementado y monitoreado por los responsables de la gobernanza y la administración y cuyo propósito

es brindar una seguridad razonable sobre el logro de los objetivos de una entidad en referencia, a la confiabilidad de la información financiera, así como de la eficacia y eficiencia de las operaciones y cumplimiento de las leyes.

En este sentido Al-Thuneibat, Awad, Al-Rehail y Yousef (2015) manifiestan que los objetivos dentro de los sistemas de control interno son amplios e interrelacionados, lo que contribuye al bienestar de la corporación, así como de que sus resultados se vean reflejados en términos de rentabilidad, liquidez y solvencia.

Norma International Standard on Auditing - ISA 315 – Identificación y evaluación del riesgo de error material a través del conocimiento y la compresión de la entidad y de su entorno

En la versión revisada de la Norma Internacional Estándar on Auditing ISA 315, (2015a) se estable como requerimiento para el auditor el conocimiento de la entidad y de su entorno, el cual forma parte del control interno; la figura 1 detalla los conocimientos requeridos.

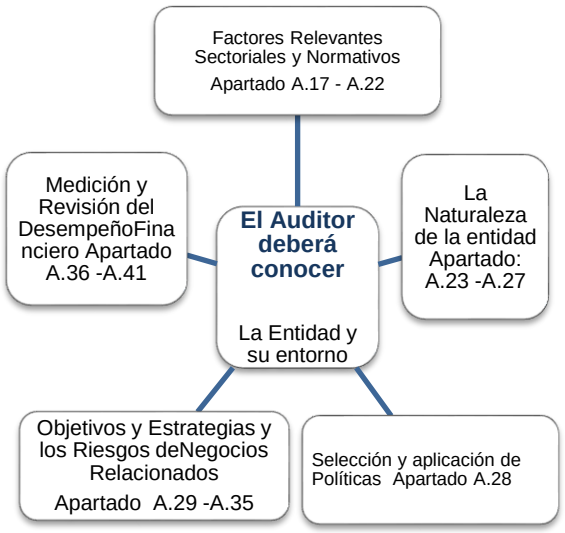

Figura 1: **Conocimientos Requeridos por el Auditor.** Elaboración propia**.** Fuente: (International Federation of Accountants (IFAC), 2015a).

ISA 315 caracterizada por su enfoque basado en control interno y cuya definición se complementa, con las sugerencias emitidas en la publicación de Professional Accountants in Business Commitee (2011), de su estudio "Global Survey on Risk Global Management and Internal Control", en el cual considera a las estrategias de gestión de riesgos y políticas de control interno, para alcanzar objetivos a través de: a) Procesos estratégicos y operativos eficaces y eficaces; b) Suministro de información confiable a los usuarios internos y externos para la toma de decisiones oportuna; c) Garantiza la conformidad con las leyes y reglamentos; d) Salvaguarda los recursos de la entidad contra pérdidas, fraude, mal uso y daño; y e) Resguarda la disponibilidad, la confidencialidad y la integridad de los sistemas informáticos de la entidad.

La Norma Internacional Estándar on Auditing ISA 315, (2015a) plantea una división en lo referente al control interno, a través de 5 componentes de COSO 2013, los cuales suministran un marco para que el auditor pueda considerar los aspectos referentes al control interno dentro de una auditoría, dichos componentes son detallados a continuación en la figura 2.

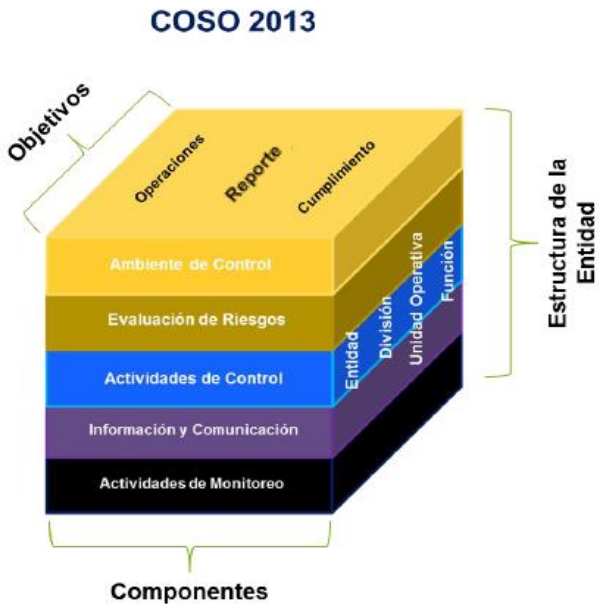

Figura 2: **Cubo COSO – 2013** Fuente: (Committee of Sponsoring Organizations of the Treadway Commission. COSO, 2013)

En el apartado ISA 315.A44 en lo concerniente sobre la finalidad del control interno, se revela que es diseñado, implementado y se lo mantiene, con la finalidad de responder a los riesgos del negocio, que amenazan contra los objetivos definidos por la entidad, los cuales se categorizan en: a) Información financiera - reportes, b) Cumplimiento a las normas y los reglamentos establecidos y c) la eficiencia y la eficacia de sus operaciones (International Federation of Accountants (IFAC), 2015b).

ISA 315. A60 - 61 Características de los elementos manuales y automatizados del control interno relevantes para la valoración del riesgo.

Se debe prestar atención referente a los elementos manuales y automatizados, definidos en el sistema de control interno de la entidad; así como en las características de dichos elementos los cuales son relevantes para la valoración del riesgo, e influyen en el modo en que se inician, registran y procesan las transacciones. Por otra la implementación de los controles en los sistemas de Tecnologías de la Información consisten en una combinación de controles automatizados y manuales para el control interno y pueden variar según de su naturaleza y complejidad (International Federation of Accountants (IFAC), 2015c)

ISA 315.A62 – A.63 Control Interno, Beneficios y Riesgos de aplicar Tecnologías de la Información.

Las tecnologías de la información (TI), dentro del control interno presentan beneficios, así como también plantea riesgos específicos dentro de los controles. En la figura 3, se realiza el detalle de los beneficios y riesgos en concordancia con el apartado ISA 315.A62 y A.63.

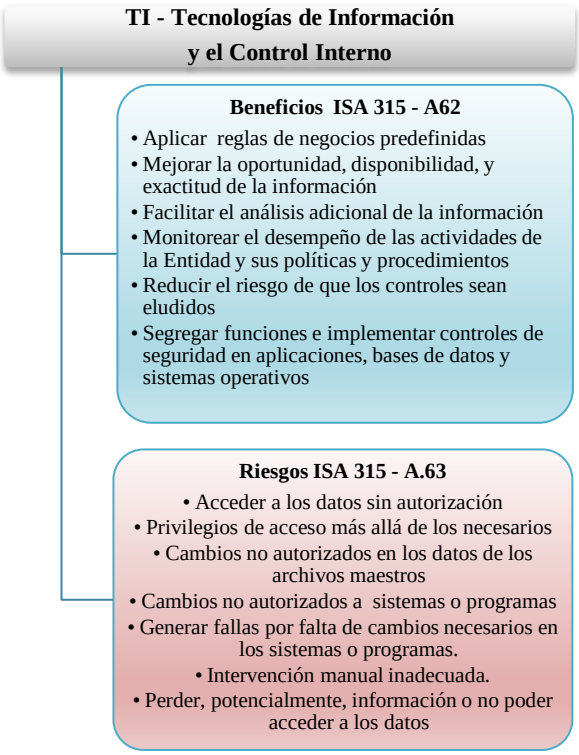

Figura 3: **Beneficios y Riesgos de TI-Tecnologías de la Información y el Control Interno en la entidad.** Elaboración propia**.** Fuente: (International Federation of Accountants (IFAC), 2015d).

METODOLOGÍA.

Para la construcción del presente marco metodológico se seleccionó una metodología de investigación cualitativa, la cual tiene como función primordial la de calificar el riesgo como medio de solución ante la situación planteada en el proceso de indagación, antes descripto.

Hipótesis planteada

La hipótesis se encuentra sujeta a ensayos de prueba y toma como base el razonamiento, recopilación bibliográfica de conceptos e ideas concernientes con la realidad de la supervisión de las áreas de tecnología de las instituciones financieras de segmento 3, 4 y 5 pertenecientes a la Economía Popular y Solidaria; la complejidad en la aplicabilidad de procesos de supervisión y control al área tecnológica, da origen a la siguiente interrogante: ¿Cómo

supervisar el área tecnológica de las instituciones financieras de segmento 3, 4 y 5 de la Economía Popular Solidaria?.

Población objetivo del estudio

Para la elección de la población objetivo, se considera como elemento fundamental y premisa técnica del estudio, las áreas de tecnología de las instituciones financieras pertenecientes a los segmentos 3, 4 y 5 de la Economía Popular y Solidaria, cuyos activos registrados se fijan con un valor igual o menor a veinte millones de dólares (20'000.000,00), por lo tanto, se excluye las instituciones financieras pertenecientes a los segmentos 1 y 2 cuyos activos son superiores a los fijados para el estudio. Para la realización de dicha segmentación, se hizo uso de la resolución 038-2015-F vigente fijada por la Junta de Regulación Monetaria y Financiera.

Método de investigación

Como método de la presente investigación se plantea la realización de una descripción breve sobre el diseño y planeación a considerar dentro de un método de auditoría integral, seguido por el desarrollo del esquema gráfico (Flujograma), en el cual se describen los pasos a seguir para el proceso de supervisión in situ, el cual se fundamenta en el revisión bibliográfica realizada previamente y describe los pasos a seguir para la identificación de riesgos y verificación de controles implementados en el área de tecnología, como medida de control interno por parte de la entidad.

En la etapa de validación del riesgo es necesario estimar la significatividad del riesgo, como su probabilidad de ocurrencia, para lo cual se realiza la elaboración de tablas para la definición de criterios de impacto y probabilidad de ocurrencia, las cuales fueron diseñadas en función del nivel de impacto que representa cierto riesgo para las instituciones financieras del segmento 3, 4 y 5 de la Economía Popular y Solidaria.

Como una siguiente etapa se desarrolla una matriz de evaluación la cual permite incorporar los elementos en los que deben existir controles y las actividades necesarias para realizar su verificación e incorpora los factores de riesgo operativo que se ven involucrados en dichos controles, como complemento del riesgo involucrado.

Recolección de la Información

Como método de recolección de información y validación del marco metodológico propuesto, se proyecta la ejecución de un grupo focal con 5 profesionales expertos en el área de supervisión de tecnología, los cuales darán sus perspectivas sobre la factibilidad de su uso en supervisiones a instituciones financieras de los segmentos 3, 4 y 5 de la Economía Popular y Solidaria.

Además se establecen como variables de estudio a las categorías definidas en la matriz de evaluación, en las cuales se describe la necesidad de la implementación de controles y el esquema grafico de supervisión. Lo antes detallado servirá como medio para recolectar información y el esquema del proceso de supervisión permitirá conocer las opiniones sobre la factibilidad de su aplicación.

Finalmente las respuestas de los participantes serán recopiladas a través de cartillas en las cuales se presentarán las variables de estudio y sus posibles repuestas, así como comentarios, los cuales serán codificados como medio para la consolidación de resultados.

Estructura del Marco Metodológico

El presente estudio tiene como fundamento el planteamiento de un nuevo marco de supervisión para el área tecnológica, con la finalidad de evaluar las Tecnologías de Información y Comunicaciones en adelante (TIC) de una manera efectiva y eficiente, acorde a la cantidad de sus activos, y resguardando de manera primordial la información financiera.

Además es importante señalar que un proceso de auditoría se ejecuta considerando la fase de

planeación, ejecución e informe; para lo cual, los auditores o supervisores toman en cuenta las normas y procedimientos generales establecidos en la metodología de auditoría integral; sin embargo, la ejecución del proceso y los controles sujetos a supervisión específicos a aplicar en referencia al área de tecnologías de información y comunicaciones, es el aspecto a fortalecer en la presente investigación.

Dentro de la fase I de planificación, se considera los objetivos principales de la auditoría, los cuales deberán estar acordes al tamaño de la entidad (segmento 3, 4 y 5), tiempo de visita y en función de sus activos, los cuales pueden ser verificados; a través de la revisión de estados financieros precedentes, los cuales permitirán dar un conocimiento sobre la situación financiera de la entidad.

Como un segundo paso y dentro de esta misma fase, se deriva una visita previa a la entidad con el propósito de solicitar información referente a su área tecnológica, a fin de obtener un entendimiento sobre su funcionamiento y la identificación de activos y riesgos asociados, en los que se incluye sistemas y equipos. Para completar esta fase, se plantea la elaboración de un plan de trabajo general, el cual se encuentre acorde con las condiciones existentes para la ejecución de la auditoría y aplicable a cualquier tipo de entidad financiera del segmento 3, 4 y 5 de la Economía Popular y Solidaria.

A continuación y como parte de la fase II - Ejecución de la Auditoría, se expone en el apéndice de una manera holística el esquema de manera gráfica propuesto para la supervisión del área de tecnología. En el cual se describe claramente los pasos a considerar para el proceso de supervisión del área de tecnología de las instituciones del segmento 3, 4 y 5, con una consideración especial en los riesgos asociados a los activos críticos.

Según procedimiento propuesto, la tarea de estimar la significatividad o impacto del riesgo en tecnología la calificación estará con base a la figura 5 propuesta, la cual se construye con criterios cualitativos, es decir, hace referencia la magnitud de las consecuencias que se detallan a continuación:

IMPACTO / SIGNIFICATIVIDAD DEL RIESGO	DESCRIPCIÓN	CRITERIO
	Los hallazgos son severos / catastróficos e implican la situación financiera de la institucional en referencia a los mínimos exigidos, requieren de acciones inmediatas en pro de superar los mismos.	Catastrófico
	La ausencia de control se manifiesta en hallazgos críticos, los cuales si no se resuelven la viabilidad de la institución puede comprometerse, se deben tomar acciones inmediatas a corto plazo	Crítico
	Los hallazgos representan debilidad moderada, debido a la falta de control, no afecta su capacidad financiera; sin embargo requiere de acciones a largo plazo.	Moderado
	Los hallazgos representan una debilidad menor, debido a la ausencia de cualquier control, requieren de un tratamiento como medida de prevención, para evitar se conviertan en moderado.	Menor
	Los hallazgos encontrados responden a la ausencia de cualquier control, existe un bajo riesgo que se convierta en significativo en los proximos periodos	Insignificante

Figura 5: **Criterios de Impacto de los Riesgos.** Elaboración propia**.**

En lo referente a valorar la probabilidad de ocurrencia, en base a la cantidad de ocurrencias relacionadas con el riesgo tecnológico, se considera la figura 6 que de manera cualitativa califica en base al impacto y probabilidad de ocurrencia.

IMPACTO / CRITERIO	RIESGOS				
Catastrófico	5	10	15	20	25
Crítico	4	8	12	16	20
Moderado	3	6	9	12	15
Menor	2	4	6	8	10
Insignificante	1	2	3	4	5
	Probable	Poco Probable	Ocasional	Probable	Muy Probable
	Muy Baja	Baja	Media	Alta	Muy Alta

Figura 6: **Criterios de Calificación de Impacto por Probabilidad de Riesgo.** Elaboración propia**.**

Además de la calificación de los riesgos con base a su probabilidad e impacto, se deberá considerar la atención de los mismos, por parte

de los directivos de la entidad dentro de los siguientes rangos de calificación Ver tabla 3.

Tabla 3
Atención del riesgo con base al rango de calificación de probabilidad por impacto

Atención del Riesgo		
Descripción	**Rango Calificación**	
Solucionar con procedimientos cotidiano (prevención)	01- 03	Muy Baja
Atención por parte de mandos medios	04-06	Baja
Atención por parte de mandos directivos	05-09	Media
Requiere atención por Gerencia	10-12	Alta
Requiere atención de la Alta Gerencia (Consejo de Administración)	15-25	Muy Alta

Como complemento al esquema propuesto en el apéndice en la figura 7 se presenta una matriz de supervisión para realizar la evaluación del área de tecnología para las instituciones financieras de los segmentos 3, 4 y 5 de la Economía Popular y Solidaria. En la que se ha considerado las categorías en las que debe existir un análisis de controles implementados, los cuales son evaluados a través de actividades que permitan verificar su existencia, su uso y efectividad, además que son considerados indispensables para cualquier tamaño de institución financiera.

En una primera columna de la matriz se presenta las categorías sobre los cuales deberán verificarse la existencia de controles, en los cuales se encuentran: el valor de la información financiera, la implementación de seguridad referente a los accesos, centros de datos, adquisición y cambios en lo referido al software y hardware.

En segundo lugar en la matriz se consideran las actividades, a efectuarse como parte de la evaluación y verificación de la existencia de controles en alusión a los riesgos, identificados para el área de tecnología en instituciones financieras, y que constituyen un riesgo latente para los activos principales de la entidad. Como complementos para este tema se plantea la utilización del flujo del procedimiento para el proceso de supervisión, detallado en el apéndice.

Una vez concluida las actividades de evaluación y en base a las evidencias y observaciones realizadas, se puede efectuar la calificación en función de la probabilidad de ocurrencia e impacto definidos anteriormente.

Finalmente la matriz presenta la sección “Fuentes de Riesgo Operacional”, en la que se hace referencia a los aspectos valorados como fundamentales para el desarrollo de esta solución y que forman parte de los factores considerados en el riesgo operativo, como claves para minimizar las pérdidas financieras, así como para establecer actividades a futuro que permitan definir estrategias y controles no solo de carácter operativo.

Además dentro de este último componente de la matriz, se consideran los factores del riesgo operativo para la columna de categorización, los cuales se encuentran acordes a las actividades de evaluación propuestas. Como parte de este componente, se presenta la columna “nivel 1”, la cual hace referencia a los riesgos en función de su categorización, el “nivel 2” específica a mayor detalle el riego asociado, no solo a nivel de factor de riesgo operativo, sino en función de los procesos del negocio, la efectividad de la implementación e influencia de TI en los procesos del negocio.

ANÁLISIS DE RESULTADOS

El objetivo de realizar el grupo focal, fue la de conocer la percepción de aplicabilidad del modelo propuesto para la supervisión del área de tecnología de las instituciones financieras de los segmentos 3, 4 y 5 de la Economía Popular y Solidaria.

El tamaño del grupo focal se constituyó de 5 profesionales 3 hombres y 2 mujeres, en el cual se trató de captar heterogeneidad de los informantes en cuanto a años de experiencia en la rama de auditoría tecnológica.

La conformación del grupo focal se establece con el 60% de los participantes con una experiencia de más de 10 años como auditores de entidades financieras y en cuyos perfiles destaca la existencia de títulos como: Magister en Gerencia de la Seguridad y Riesgo, Magister en telecomunicaciones, Magister en Gerencia de Sistemas informáticos y de Computación y con certificaciones reconocidas a nivel internacional como Fundamentos en ITIL.

Un 20% basa su experiencia como perito informático de la fiscalía y ha realizado trabajo de auditoría tecnológica a instituciones financieras, en casos de fraude financiero y estafas, en referencia a su perfil profesional, es importante resaltar que se trata de un profesional que ha realizado ponencias a nivel internacional en países como Chile y México y se han desempeñado en cargos como Director de la Red Latinoamericana de Informática Forense y como Coordinador del Laboratorio de Informática Forense de la Fiscalía General del Estado.

Finalmente, el porcentaje restante corresponde a profesionales del área informática con experiencia de al menos 5 años en procesos de auditoría en entidades financieras.

Todos los participantes, tienen experiencia en el sector de la Economía Popular y Solidaria y conocen la segmentación de las instituciones financieras, ya sean como auditores de la SEPS, de firmas auditoras externas o como peritos informáticos, con lo que sus aportes y testimonios son de mucho valor al marco propuesto.

A continuación se presentan los resultados con base en las respuestas obtenidas durante la sesión, los cuales fueron divididos en 2 aspectos fundamentales: 1) Procedimiento de supervisión y 2) Matriz de evaluación, además se incluye en ciertos casos la síntesis del punto de vista dado por los participantes de acuerdo a sus interpretaciones, experiencias y comentarios realizados.

La sesión realizada con el grupo focal, tuvo como fecha de encuentro el día 14 de enero del año 2017, en la cual se realiza un conversatorio con los participantes con el fin de conocer su criterio referente el marco metodológico propuesto de supervisión al área de tecnología, se evita la realización de entrevistas, sino se construye la sesión con base a estructuras de análisis y plantear como guía de estudio la hipótesis formulada, algunos de los temas tratados son llevados a manera de preguntas y respuestas como parte de la secuencia de la conversación estructurada.

Procedimiento Para Supervisión

La primera etapa del grupo focal se inició con la discusión de temas relacionados con la funcionalidad y la experiencia sobre modelos de auditoría para el área de tecnología de la información, en el cual se presentó el esquema gráfico propuesto para el proceso de supervisión, para evaluar su aceptación.

Desde el punto de vista de la experiencia de los participantes, se comprobó la aceptación, así como la funcionalidad del flujograma o esquema del proceso de supervisión propuesto, el cual tiende a estructurar la supervisión, a través de la evaluación de controles implementados; sin embargo, se mencionó que no es posible dicha evaluación cuando los controles son inexistentes.

Además se estableció como origen de la inexistencia de controles por parte de los participantes los siguientes aspectos: a) Un 60% establece que se debe a la falta de cultura por parte de los directivos, en lo referente a mecanismos de control interno, b) Mientras que el 40% lo define como una deficiencia relativa a la identificación de riesgos relevantes, por parte de los directivos.

En esta primera etapa de evaluación del esquema de supervisión propuesto, se constató que los participantes del grupo focal distinguieron que se trata de un modelo basado

en características asociadas a la evaluación de controles existentes. Dentro de esta etapa los participantes manifestaron, que en entidades del segmento 5, siendo las más pequeñas no es común una implementación de controles, debido a la falta de control interno existente.

Otra característica vinculada a la categoría del esquema de supervisión, es la relacionada con controles implementados por proveedores externos a la entidad, razón por la cual algunos participantes mencionan que requieren de estrategias como la visita a proveedores, para poder obtener información sobre los mecanismos de control implementados, esto en concordancia a lo establecido en el Código Orgánico Monetario y Financiero, en el artículo 473 en los que se consideran entre los servicios auxiliares de las instituciones financiera a: empresas de software bancario, transaccionales, de transporte de especies monetarias y de valores y cajeros automáticos, contables y de computación.

Matriz de Evaluación - Actividades establecidas para la supervisión

A través de la interpretación de la matriz de evaluación, así como de la capacidad de los participantes, se realiza el análisis y síntesis de la información extraída del grupo focal, y de su naturaleza interactiva.

Cabe mencionar que para este estudio, durante la sesión de validación del grupo focal, se estableció como variantes de discusión a las categorías en las cuales debe existir un control y las cuales fueron determinadas en la matriz de supervisión y se realiza cartillas con las actividades definidas para la verificación de controles, así como sus factores de riesgo y preguntas sobre los mismos, para el registro de la participación se hizo uso de hojas autoadhesivas de varias dimensiones y colores, para identificar a los participantes y presentar las temáticas durante la interacción.

Finalmente el análisis de resultados, se realiza a través de la codificación de los temas tratados de acuerdo a su relevancia y mención, así como la frecuencia de cada código.

Los elementos de supervisión con mayor relevancia citados, en los resultados fueron mencionados al menos por el 40% de los participantes y ordenados de acuerdo a su mención y frecuencia. Al mismo tiempo se debe tener en cuenta que se trata de un estudio cualitativo de naturaleza exploratoria, cuyo objetivo es captar las principales preocupaciones y sensibilidades que subyacen a la experiencia en la supervisión en el área tecnológica, en entidades financieras de la Economía Popular y Solidaria, del segmento 3, 4 y 5.

Al presentar las cartillas con las variables definidas por las categorías identificadas en las cuales debe existir controles implementados se detalla: 1) Validez de la información, 2) Centro de datos, 3) Adquisición, reposición y mantenimiento de software de sistemas y aplicaciones, 4) Cambios en programas, 5) Seguridad de accesos, los participantes que tienen mayor conocimiento de la supervisión a los segmentos 3, 4 y 5; vincularon estos aspectos como métodos de control para cumplir con los objetivos de la supervisión.

Validez de la información

Cuando se consultó por la opinión de los participantes en referente a las actividades definidas para validar la información financiera, el

100% de los participantes, opinó acerca de las pruebas de recorrido asociándolo con la relevancia de la información financiera y la integridad que debe tener la misma, además se realizaron opiniones en referencia al mismo ver tabla 4.

Tabla 4

Opinión de participantes, sobre "pruebas de recorrido como método para la validación de la información (integridad)

Participante	Opinión
1	"Sirve de ayuda al auditor para la comprensión del proceso "
2	"Permite la verificación del funcionamiento de software transaccional de la entidad"
3	"Es un control clave para la verificación de controles en actividades cotidianas como créditos, depósitos a plazo fijo, depósitos a la vista"
4	"Previamente el auditor debe tener conocimiento de los principales riesgos que puedan existir durante este tipo de pruebas de recorrido y los controles necesarios que deben existir para mitigarlos, para validarlo de la mejor manera"
5	"Las pruebas de recorrido es un paso fundamental para cualquier proceso de supervisión, sobre los principales procesos del giro del negocio"

En referencia al análisis de impacto de los riesgos asociados a la validez de la información financiera y de la evaluación de las actividades definidas en la matriz de supervisión para esta categoría, los participantes en consenso acordaron que el mayor riesgo es la falta de integridad en la información y la catalizaron con un impacto catastrófico para la institución financiera.

Centro de Datos

En esta segunda etapa, de la evaluación de las actividades sugeridas en la matriz de evaluación propuesto, gran parte de las mismas tienen una aceptación por parte de los participantes, un punto que es puesto a discusión hace referencia al almacenamiento de los respaldos: en la que la mayor parte del quórum, cree que es una buena opción, que los mismos sean almacenados en un lugar externo a la entidad, mientras que otros plantean que podrían alojarse dentro de la misma entidad pero en un lugar adecuado por cuestiones de seguridad, debido a que este tipo de entidades no cuentan con un presupuesto destinado para este fin.

Además otro punto tratado dentro de esta etapa y planteada de manera general y como inquietud por parte del grupo es: si dentro de esta categoría se debería incluir la calificación de la tecnología utilizada por las entidades financieras, en referencia a si satisfacen las necesidades del negocio y se plantea como escala de valores subjetivos: a) muy buena, b) buena, c) regular o d) mala, y cuya interpretación pueda dar de alguna manera un sentido de criterio y empleada a futuro como estrategia para el mejoramiento continuo.

En referencia al impacto de los riesgos analizados que se encuentran asociados al centro de datos, se determina los siguientes. Ver tabla 5.

Tabla 5
Impacto de Riesgos asociados a centro de datos

Riesgos	Impacto de Riesgo	% Participantes en consenso
Robo de hardware de la institución	Catastrófico	100
Deterioro de respaldo de información del sistema transaccional	Catastrófico	100
Centro de computo sin condiciones físicas adecuadas	Crítico	80
Falta de seguridades físicas de equipos principales	Crítico	80
Modificación de configuración de equipos	Moderado	60
Falta de equipos de apoyo como: ups y plantas eléctricas	Crítico	80

Adquisición, reposición y mantenimiento de software de sistemas y aplicaciones

Al presentar esta tercera etapa las intervenciones generadas en referencia a las actividades planteadas, fueron de aceptación por parte del quórum; sin embargo, es importante destacar la detección de carácter crítico, realizada por los participantes, luego de la pauta de análisis, quienes evaluaron varias

falencias asociados a los contratos de adquisición y mantenimiento, dentro del marco operativo por parte de las instituciones financieras, con terceros (proveedores), los cuales son asociados con los factores de riesgo operativo como personas y procesos ver tabla 6.

Tabla 6
Porcentaje de acuerdo de los participantes sobre causas de las falencias en contratos con proveedores

% participantes que estuvieron de acuerdo	Falencias críticos en contratos	Factor de Riesgo
100	El contrato no garantiza el retorno de la inversión deseado	Proceso
80	La no ejecución de penalización en referencia a incumplimiento por parte del proveedor	Personas
100	Falta de especificaciones en contratos sobre nivel de operativo y de servicios	Proceso
60	Contratos demasiados vagos, no contemplan entregables, tiempos, calidad, rendimiento	Proceso
100	Ausencia de gestión en la administración de contratos por parte de la entidad	Personas
60	Falta de políticas para proveedores con base a contratos y proveedores	Proceso

Los riesgos mencionados en función del análisis realizado en referencia a la adquisición, reposición y mantenimiento de software de sistemas y aplicaciones son: ver tabla 7.

Tabla 7
Impacto de Riesgos asociados a procesos de Adquisición, reposición y mantenimiento de software de sistemas y aplicaciones

Riesgos	Impacto de Riesgo	% Participantes en consenso
Falta de personal con competencias idóneas	Crítico	100
Falta de acuerdos de confidencial de la información	Catastrófico	80
Concentración de funciones que facilita fraudes	Catastrófico	100
Ausencia de Procedimiento formal para adquisiciones	Crítico	60
Falta de licencias de software	Moderado	60
Carece de Procedimiento formal para monitoreo de servicio prestado por terceros	Crítico	100
Ausencia de prácticas de mantenimiento preventivo y correctivo de los equipos	Moderado	60

Cambios en Programas

A partir de la información proporcionada por los participantes, en referencia a las actividades y controles planteados, se obtuvo las siguientes apreciaciones en referencia al impacto de ciertos riesgos, en los cambios de las aplicaciones, y en los que existe un cierto porcentaje de consenso por parte de los miembros del grupo focal. La tabla 8 muestra el impacto de los riesgos revisados:

Tabla 8
Impacto de Riesgos asociados a cambios en aplicaciones

Riesgo	Impacto de Riesgo	% Participantes en consenso
Software no cumple con los requisitos mínimos funcionales	Catastrófico	100
El cambio en el aplicación tarda más de lo esperado	Moderado	40
No existe una metodología definida	Moderado	40
No se realizan pruebas de validación de los cambios	Crítico	80
Falta personal capacitado para efectuar el cambio	Moderado	60
No existe un manejo de versiones de aplicaciones	Crítico	100
No existe un ambiente de pruebas para las pruebas	Crítico	60

Seguridad de Accesos

Los aspectos y actividades destinadas a verificar el control en referencia a la seguridad, estuvieron representados por las dificultades, en relación con desaciertos en cuanto a la mitigación de riesgos, los cuales se vuelven nulos en la mayor parte de las instituciones financieras del segmento 3, 4 y 5. A continuación en la tabla 9, se presenta el análisis de impacto referente a los riesgos asociados a esta categoría.

Tabla 9
Impacto de Riesgos asociados a procesos de seguridad de accesos.

Riesgos	Impacto de Riesgo	% Participantes en consenso
Usos de claves compartidas	Catastrófico	100
Usuarios activos en el sistema correspondiente a exempleados de la entidad	Crítico	80
Falta de gestión en la administración de usuarios	Moderado	80
Abuso de información registrada como confidencial	Catastrófico	80
La red LAN no presenta segmentación alguna	Moderado	60
Instalación de software no autorizado en equipos	Crítico	100
No se realiza cambios de claves de equipos como: servidores y base de datos	Crítico	80

Adicionalmente los participantes estuvieron de acuerdo que generalmente, las dificultades en cuanto a seguridad, se encuentran caracterizadas por la diversidad cultural de sus directivos, así como el enfrentar limitaciones en referencia a conocimientos sobre buenas prácticas en el área de tecnología y el desconocimiento de recursos tecnológicos adecuados.

La aceptación por parte de los participantes del grupo focal, sobre las actividades planteadas para la verificación de controles en referencia a la seguridad fueron positivas en la mayoría de los casos con excepción de la pregunta sobre los recursos físicos asignados a la seguridad de la información, ya que se les dificultó el poder decidir los controles adecuados que se acoplen a todos los segmentos de las instituciones financieras del estudio planteado. Las opciones de respuesta tales como “seguridad perimetral” tuvieron poca aceptación por considerarla, poco realista y alejada a la situación real de las entidades del segmento 5, en las que en la mayoría de las ocasiones no tiene una persona encargada del área de TI.

Finalmente dentro de este estudio, se plantearon críticas a la falta de gestión en el área de tecnología por parte de los directivos de las instituciones financieras, cuyo origen es la falta de cultura en referencia a la tecnología y sus beneficios.

CONCLUSIONES

El control interno y la supervisión de las instituciones financieras no deben dirigirse únicamente a los análisis económicos, sino a los mecanismos y herramientas utilizados para el giro del negocio y el área de tecnología es un área clave para hacer frente a la información financiera, a través de la cual la entidad ofrece sus productos y servicios.

Los modelos de supervisión basada en riesgos para el área de tecnología, son dinámicos y cambian a lo largo del tiempo, esto como consecuencia de la implementación de controles, variaciones en los datos, normativa de los entes de control, así como por efecto del propio ciclo económico de las entidades financieras.

Una vez identificado el riesgo es importante estimar la relevancia del riesgo y valorar la probabilidad de ocurrencia, esta definición no obedece a una única escala de valoración, sino que depende del giro del negocio, la posibilidad

de variación de su impacto y ocurrencia, frente a los riesgos; para el caso de estudio se ha definido una escala en función del riesgo operativo.

Además el marco de evaluación tiene como eje central la constatación de controles, como medida para prevenir los riesgos, tanto por unidades internas como externas. Los cuales deben ser verificados por el departamento de auditoria interna, firmas de consultorías externas y entidades de control, con la finalidad de monitorizar su funcionamiento y detectar posibles errores.

La evaluación de controles en el marco propuesto forma parte del proceso de verificación de las acciones frente al riesgo y constituye una comprobación para la verificación de información relevante y como medida para evaluar las acciones adoptadas por la entidad para minimizar su impacto frente al riesgo.

El marco metodológico propuesto establece para la supervisión del área de tecnología, la identificación de riesgos de manera previa, como insumo para la verificación de controles, esta etapa requiere de la experiencia del auditor para la identificación de los mismos y considera los recursos internos con los que cuenta la entidad y que son necesarios valorarlos, para definir la estrategia de supervisión en el contexto de la gestión tecnológica.

El proceso para la supervisión del área tecnológica basado en verificación de controles, para instituciones del segmento 3, 4 y 5 de la Economía Popular y Solidaria se presenta como un proceso complejo, cuando se lo evalúa bajo un único marco de supervisión, ya que se debe considerar los riesgos y sus controles de acuerdo con los recursos financieros de cada entidad; la estructura propuesta en el modelo de supervisión ver figura 8, contempla los aspectos a ser considerados para realizar este tipo de supervisión.

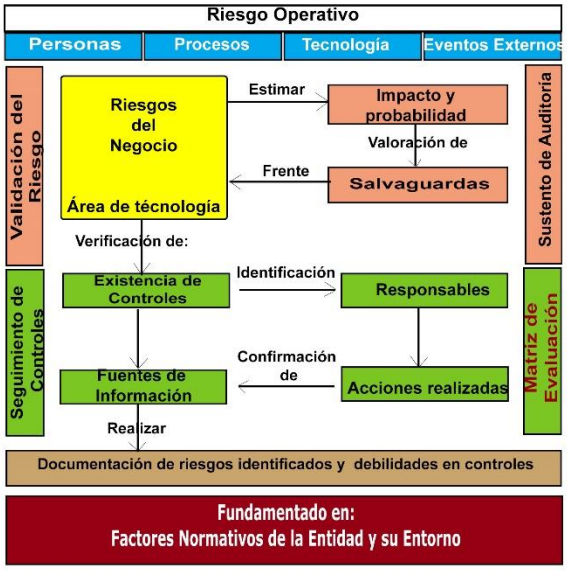

Figura 8: **Resumen del Modelo de Supervisión del Área de Tecnología.** Elaboración propia**.**

En referencia a la etapa de seguimiento de controles, es necesaria la colaboración del personal interno de la entidad financiera, como medio para determinar el grado de validez con respecto a la información, otorgada para el proceso de supervisión.

Finalmente para la etapa de documentación los resultados obtenidos con el marco propuesto, deben ser previamente analizados por el supervisor, para presentar su interpretación en referencia al riesgo y debilidades de control detectadas durante la supervisión.

Una revisión a una fecha de corte por parte del ente de control como la SEPS no es suficiente, el proceso de supervisión es un proceso continuo y que debe respaldarse con el seguimiento de un modelo el cual contenga las pautas para la verificación de los principales procesos del giro del negocio, los cuales mantienen una relación directa con el área de tecnología.

Los resultados del estudio sugieren el uso del marco propuesto de supervisión, como alternativa a las metodologías tradicionales existentes, no solo para procesos de supervisión del área de tecnología, sino como

mecanismos de control interno. Además permite disponer de información sobre los puntos críticos en los cuales el control es necesario.

La validación del modelo se lo realiza a través de la conformación de un grupo focal, el cual provee información valiosa a través de datos cualitativos, los cuales sirven de instrumento para el diseño, análisis y verificación del marco de supervisión y se hace uso de herramientas como la percepción y reacción de los participantes, en referencia al tema de investigación.

Una limitación de este estudio recae, en que ciertos participantes del grupo focal, cuya experiencia se sustenta en instituciones financieras del segmento 1 y 2, pudo haber influido en el tipo de respuestas dadas; sin embargo, se plantearon algunas críticas que sirvieron de sustento para el dialogo y análisis realizado con el grupo.

A pesar de lo mencionado anteriormente, se observó una tendencia favorable en las respuestas en base al marco propuesto para la supervisión, para las instituciones financieras del segmento 3, 4 y 5 de la Economía Popular y Solidaria, el cual mantiene lineamientos para la validación del estudio.

De manera general, todas las actividades y flujograma del proceso de supervisión planteado, fueron comprendidos en su contenido y propósito. Las opciones de respuestas absolutas como nunca o siempre no tuvieron aceptación por los participantes, ya que los mismos basan sus respuestas y criterios en la experiencia adquirida a través de los años, los cuales son expresados en grados de severidad de impacto que podría ocasionar un determinado riesgo, dentro de una institución financiera.

Tal y como se ha demostrado en la validación del marco metodológico, la implementación de controles es una actividad básica para cualquier institución financiera y la supervisión se basa en el monitoreo y mejora continua de dichos controles.

De la experiencia propia y los testimonios analizados de los participantes del grupo, se determinó que sin la existencia de controles un proceso de supervisión, se convierte en una consultoría en la que se realiza recomendaciones.

Para finalizar se debe señalar que los resultados de este estudio tienen implicaciones en referencia a los programas de supervisión, los cuales deben adaptarse a las restricciones existentes dentro de las instituciones financieras. Es importante tener presente que la falta de dichos controles pudiese estar causando deficiencias en la institución financiera y generando pérdidas económicas.

Como trabajos futuros se plantea la aplicación del marco propuesto para la supervisión, como proceso experimental para evaluar la validez del modelo en el campo de la auditoría. Para la aplicación de este marco metodológico, se requerirá de un conocimiento profundo de las particularidades de las entidades financieras del segmento 3, 4 y 5 de la Economía Popular y Solidaria, como medida para establecer las estrategias de supervisión.

Así como lo resultados de la aplicación deberán establecer estrategias que contribuyan con el incremento del grado de conocimiento por parte de la alta dirección en temas de tecnología, y como medida para la implementación de controles internos correctivos efectivos.

Referencias Bibliográficas

Aloini, D., Dulmin, R., & Mininno, V. (2012). Risk assessment in ERP projects. *Information Systems, 37*(3), 183-199.

Al-Thuneibat, A. A., Awad, S., & Al-Rehaily, Y. (2015). The impact of internal control requirements on profitability of Saudi shareholding companies. *International Journal of Commerce and Management, 25*, 196 - 217.

AMUTIO, M., Candau, J., & Mañas, J. A. (2012). MAGERIT–versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. En *Libro II-Catálogo de Elementos.*

Anderson, D. J., & Eubanks, G. (2015). Leveraging COSO across the three line of defense. *The Institute of Internal Auditors*. Obtenido de http://www.coso.org/documents/COSO-2015-3LOD-PDF.pdf

Asamblea General Constituyente. (2008). Constitución de la República del Ecuador. Montecristi, Manabí, Ecuador.

Asamblea General Constituyente. (2014a). Código Orgánico Monetario y Financiero, Libro I. *Publicada en el suplemento del Registro Oficial No. 332 de 12 de septiembre del 2014.*, 83. Ecuador.

Asamblea Nacional Constituyente. (2014b). Código Orgánico Monetario y Financiero, Libro I. *Publicada en el suplemento del Registro Oficial No. 332 de 12 de septiembre del 2014.*, 127. Ecuador.

Cevallos Guera, D. F. (2015). Las mejores prácticas aplicadas a un análisis de riesgos de seguridad de la información para las entidades financieras controlas por la Superintendencia de Economía Popular y solidaria (Cooperativas de Ahorro y Crédito) que conforman el grupo de asistenci.

Committee of Sponsoring Organizations of the Treadway Commission. COSO. (2013). Control Interno–Marco Integrado.

De Basilea, Comité de Supervisión Bancaria. (2004). Convergencia internacional de medidas y normas de capital. En *Banco de Pagos Internacionales.* Basilea, Suiza.

Deloitte Galaz, Yamazaki , Ruiz Urquiza, & S.C. (2015). COSO Marco de referencia para la implementación, gestión y control de un adecuado Sistema de Control Interno.

Gómez Ramirez, V. M., & Ospina Gil, A. (2014). Evaluación de la seguridad de la información con la metodología OCTAVE. *Revista CINTEX, 17*, 127-134.

Gubba, H., Gutfraind, J., & Rodríguez, R. &. (2001). Auditoría de evidencia virtual: cambio filosófico o adaptación del profesional a las nuevas modalidades. *Revista de Antiguos Alumnos del Instituto de Estudios Empresariales de Montevideo, IEEM, I*(4), 32-44.

International Federation of Accountansts, (IFAC). (2012). Red de publicaciones IFAC. Obtenido de

http://www.ifac.org/publications-resources

International Federation of Accountants (IFAC). (2015a). *Handbook of International Quality Control, Auditing, Review, Other Assurance, and Related Services Pronouncemente* (Vol. I). New York, USA: IFAC.

International Federation of Accountants (IFAC). (2015b). *Handbook of International Quality Control, Auditing, Review, Other Assurance, and Related Services Pronouncements* (Vol. I). New York, USA: IFAC. doi:ISBN: 978-1-60815-250-G

International Federation of Accountants (IFAC). (2015c). *Handbook of International Quality Control, Auditing, Review, Other Assurance, and Related Services Pronouncements* (Vol. I). New York, USA: IFAC. doi:ISBN: 978-1-60815-250-G

International Federation of Accountants (IFAC). (2015d). *Handbook of International Quality Control, Auditing, Review, Other Assurance, and Related Services Pronouncements* (Vol. I). New York, USA: IFAC. doi:ISBN: 978-1-60815-250-G

International Federation of Accountants, IFAC. (2009a). International Education Standards – IES 2. *Content of Professional Accounting Education Programs.* Recuperado el 15 de Diciembre de 2016, de https://www.ifac.org/sites/default/files/publications/files/ies-2-content-of-professi.pdf

International Organization for Standardization. (2009). ISO Guide 73:2009 Risk management – Vocabulary .

ISACA. (2009). *The Risk IT Framework. ISACA.* Obtenido de http://www.isaca.org/knowledge-center/risk-it-it-risk-management/pages/default.aspx

ISACA. (2012). COBIT 5: A Business Framework for the Governance and Management of Enterprise IT. . ISACA.

ISO/IEC 27001. (2013). Information technology - Security techniques - Information security management systems - Requirements.

ISO/IEC 27005. (2011). Information security risk management.

La Junta de Política y Regulación Monetaria y Financiera. (13 de Febrero de 2015). Resolución No. 038-2015-F:. *Norma para la Segmentación de las Entidades del Sector Financiero Popular y Solidario*. Quito, Ecuador.

La Junta de Política y Regulación Monetaria y Financiera. (2015 de Septiembre de 2015). Resolución No. 128-2015-F:. *Normas para la Administración Integral de Riesgo en las Cooperativas de Ahorro y Crédito y Cajas Centrales*, 2. Quito, Ecuador.

Martino, J. P. (1994). A technology audit: Key to technology planning. *In Aerospace and Electronics Conference, 1994. NAECON 1994, Proceedings of the IEEE 1994 National* (págs. 1241-1247). IEEE.

Mcube U, G. M., & Von Solms, R. (2016). Scenario-based IT risk assessment in local government. *In IST-Africa Week Conference, 2016* (págs. 1-9). IEEE.

Méndez, A. C., & Oliveros, I. L. (2016). SIE, una herramienta de apoyo para la auditoría académica. *Tecnología Investigación y Academia, I*(4), 108-116.

Ministerio Coordinador de Desarrollo Social (MCDS) ; Ministerio de Inclusión Económica y Social (MIES) ; Corporación Nacional de Finanzas Populares y Solidarias (CONAFIPS). (2012). Ley Orgánica de Economía Popular y Solidaria y del Sector Financiero Popular y Solidario, y su reglamento. 4.

Nugroho, H. (2014). Conceptual model of IT governance for higher education based on COBIT 5 framework. *Journal of Theoretical and Applied Information Technology, 60*(2), 216-221.

Obando Changuán, C. A. (2014). Auditoría basada en coso ERM a la Gestión de Riesgo Operativo para COAC Alianza del Valle (Doctoral dissertation, Universidad de las Fuerzas Armadas ESPE-Maestría en Evaluación y Auditoría de Sistemas Tecnológicos). .

OLACEFs, X. C. (2011). *Manual de Auditoría de Gestión a las Tecnologías de Información y Comunicaciones.*

Ormella Meyer, C. (2014). Norma ISO 31000 de Riesgos Corporativos. Gestión y Auditoría de Riesgos y Seguridad de la Información. 1-5.

Pazmiño, S. R. (2015). Estudio del Nivel de Madurez en el Manejo de la Gestión de Continuidad del Negocio en las Cooperativas de Ahorro y Crédito del Segmento 4 de la Economía Popular y Solidaria (Tesis de Postgrado). Quito, Ecuador.

Porter, T. W., & Burton, J. C. (1980). *Auditoría: un análisis conceptual.* México DF: Diana.

Professional Accountants in Business Commitee. (2011). Global Survey on Risk Management and Internal Control Results: Analysis, and Proposed Next Steps. *International Federation of Accountants –IFAC*.

Radovanović, D., Radojević, T., Lučić, D., & Sarac, M. (2010). IT audit in accordance with Cobit standard. *In MIPRO Proceedings of the 33rd International Convention* (pp. 1137-1141). IEEE.

Senft, S., & Gallegos, F. (2008). IT Today and Tomorroy. En *En Information technology control and audit.* (págs. 5-6). CRC Press.

Superintendencia de Bancos. (2005). De la Gestión del Riesgo Operativo. En *Libro I: Normas Generales para las Instituciones del Sector Financiero* (págs. 626-630).

Superintendencia de Economía Popular y Solidaria. (2015). *Rendición de Cuentas 2015.* Quito. Recuperado el 14 de Diciembre de 2016, de http://www.seps.gob.ec/documents/20181/378585/Rendicio%CC%81n+de+Cuentas

Vaughn Jr. Rayford B., D. D. (2004). “Building an Information Security Education Program” ACM InfoSecCD Conference’04, October 8, 2004, Kennesaw, US.

Zaitar, Y., & Ouzarf, M. (2012). ERP Projects: Key success factors and risk of failure a proposed model of governance of

enterprise resource planning. *International Journal of Computer Applications, 46*(8).

APÉNDICE

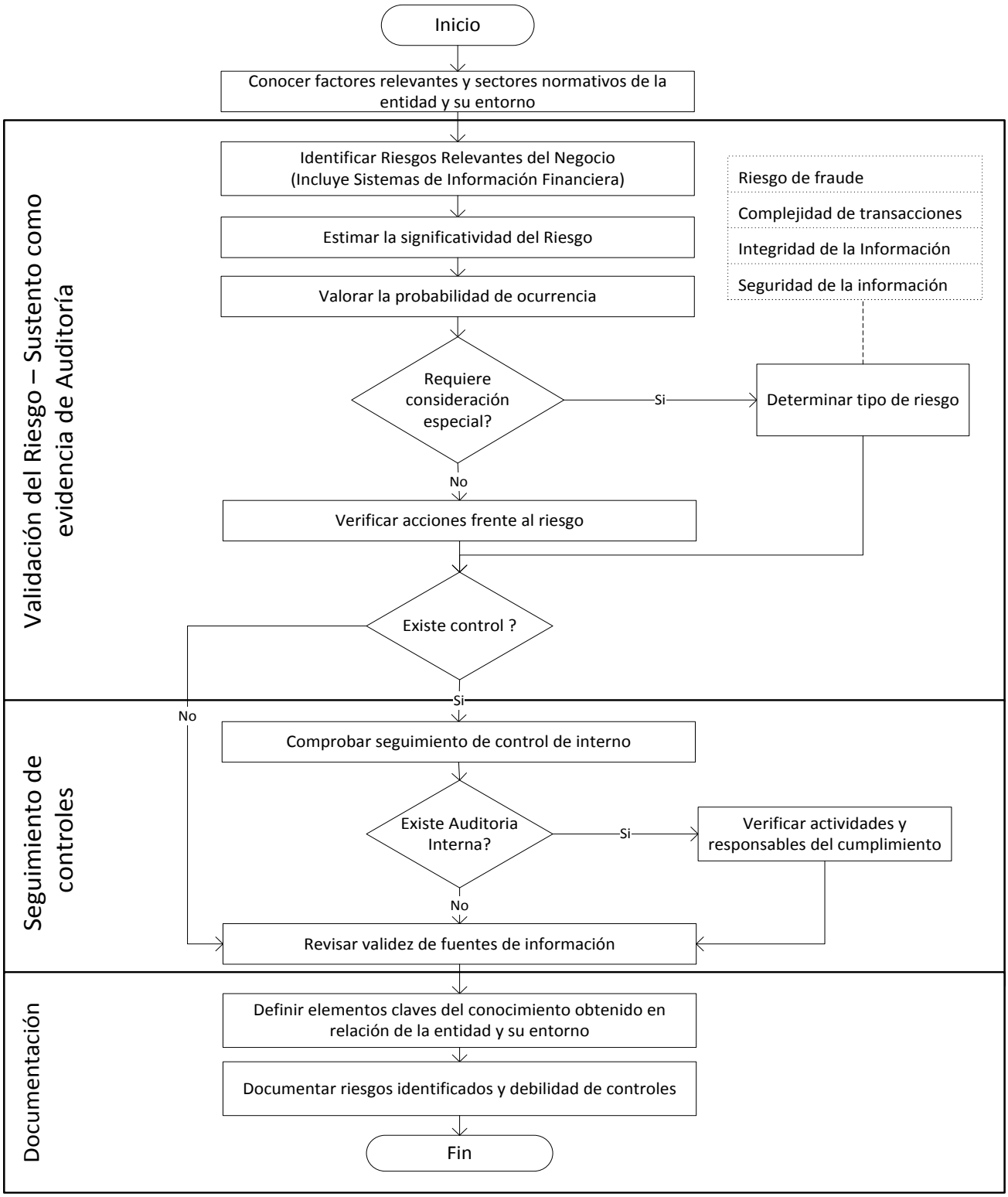

Figura 4: **Esquema de supervisión para el área tecnológica.** Elaboración propia**.**

MATRIZ DE EVALUACIÓN	
Controles sobre:	**Actividades a realizar:**
Validez de la Información financiera	Verificación de valores de parámetros en cumplimiento de disposiciones legales y reglamentarias
	Análisis de registro de información en el sistema contable de una transacción válida del sistema financiero a través de todo el proceso, empezando por el inicio de la transacción a partir del hecho generador, su autorización, registro, procesamiento, hasta su contabilización según plan de cuentas registrado
	Integridad de la información. Verificación de transacciones válidas a través de un recorrido del flujo de procesamiento de una transacción real utilizando los mismos documentos y operaciones informáticas que utiliza el personal de la entidad
	Validez de procedimientos de cálculos complejos en procesamiento de grandes volúmenes de transacciones o datos (procesos de inicio y fin de día)
Centro de datos	Área destinada para servidores de la entidad y equipos críticos de la entidad
	Controles ambientales implementados para control de humedad, temperatura
	Equipos para detección de incendios y control de fuego
	Existencia de instalaciones y equipos de apoyo como: planta eléctrica, UPS´s
	Inventario de hardware y software con características y ubicación
	Existencia de diagramas de redes y comunicaciones que definan los canales de flujo de la información, y software que lo soporta
	Área de los servidores deberá estar aislado de tuberías de aguas blancas y servidas, o instalaciones de otros elementos.
	Seguridad física: control de acceso físico a través de bitácora de acceso o cámaras de seguridad.
	Verificación de los procesos de administración de respaldos de información, en los que se incluya la periodicidad de su ejecución y los mecanismos utilizados para proceder con el respaldo de la información
	Almacenamiento de respaldos de Información en sitio externo que cuente con condiciones ambientales adecuadas para su conservación.

FUENTES DE RIESGO OPERACIONAL		
Categoria Factores Riesgo Operativo	**Nivel 1** (Riesgo)	**Nivel 2** (Detalle de Riesgo)
Personas	Fraude cometido por empleados	Colusión / Robo
		Malversación de fondos
		Operaciones fraudulentas
Procesos	Incumplimiento de normativa	Incumplimiento en el manejo de información reservada
Tecnologías de la Información	Confiabilidad de la información	Procesos de migración
Procesos	Seguridad de la Información	Deficiencia en controles para proteger información
Eventos Externos	Factores climáticos	Daños a equipos
	Robos	Asaltos a la entidad
	Catástrofes	
Personas	Daños físicos a equipos críticos	
Tecnologías de la Información	Respaldo de la Información	Restauración de la base de datos

Controles sobre:	**Actividades a realizar:**	**Categoria** Factores Riesgo Operativo	**Nivel 1** (Riesgo)	**Nivel 2** (Detalle de Riesgo)
Adquisición, reposición y mantenimiento de software de sistemas y aplicaciones	Revisión de contratos de adquisición y soporte con terceros en los que se defina el alcance del contrato y las cláusulas de confidencialidad, propiedad intelectual, acuerdos de niveles de servicio o calidad del producto, multas y penalizaciones por incumplimiento, garantías técnicas.	Tecnologías de la Información	Capacidad de los sistemas	Daños físicos a los servidores
	Administración de versiones y cambios en las aplicaciones y software			Licencias software
	Parámetros de configuración, servicios e infraestructura.			Software inadecuado
	Procedimientos de adquisición y /o desarrollo de aplicaciones e infraestructura que incluyan planes de prueba que considere impacto y la integración con la plataforma actual.	Personas	Dependencias de empleados	
	Procedimientos de mantenimiento preventivo y correctivo, en lo referente al software, sistema operativo, redes, base de datos, aplicativos	Procesos	Procesos de Contratación	Dependencia de Proveedores
	Software utilizado y licencias de uso			
	Procedimientos de soporte referente al software y hardware instalado			
Cambios en los programas	Metodología implementada para cambio en aplicaciones (Plan de pruebas, actas de entrega recepción)	Procesos	Administración de cambios	
	Verificar existencia de manuales de usuarios actualizados de aplicaciones			
	Diversidad de ambientes (pruebas y producción), los cuales cuenten con la capacidad requerida para cumplir con los objetivos.	Personas	Cambios no autorizados	
Seguridad de accesos	Seguridades sobre la base de datos a través del aplicativo: movimientos de usuario, fecha, valor, saldo, cambio de tasas entre otros	Tecnologías de la Información	Violación de los sistemas	Fallo en la seguridad interna
	Existencia de pistas de auditoria			Violación de seguridad externa
	Administración de las manejo de las claves de administrador de equipos crítico: base de datos, aplicativos			Acceso no Autorizado a ordenadores y redes
	Administración de usuarios en aplicativos y manejo de confidencialidad de los mismos (accesos no autorizados)			
	Existencia de políticas y procedimientos de seguridad de la información aprobados formalmente por el Directorio y difundidos al personal correspondiente			Violación externa de la base de datos
	Seguridades sobre la red de la entidad a través de la LAN , WIRELESS y WAN			
	Verificar seguridades sobre la (s) base(s) de datos a través del (los) aplicativo(s)			
	Recurso de seguridad asignados a la seguridad de la información tanto hardware como software: Firewalls, IDS-IPS, Administrador de QoS, switches, hubs, routers, etc.	Personas	Ejecución de Programas que Modifican y Destruyen los Datos	
	Controles para mitigación de riesgos ocasionados por la acción de virus informáticos		Falta de personal idóneo	

Figura 7: Matriz de Evaluación para Entidades del Sector Financiero Segmento 3, 4 y 5 de la Economía Popular y Solidaria. Elaboración Propia.