La gestión de riesgo *TI* y la efectividad de los sistemas de seguridad de información: caso de procesos críticos en las pequeñas entidades financieras de Lambayeque

Risk management *TI* and the effectiveness of security systems information: case of critical processes in small financial entities of Lambayeque

Ernesto Karlo Celi Arévalo

Recibido: 25 de enero de 2016.
Aceptado: 12 de febrero de 2016.

Resumen

En el Perú, y específicamente en Lambayeque, las instituciones financieraS que cuentan con la autorización de la Superintendencia de Banca y Seguros (SBS), y que gozan de autonomía económica, financiera y administrativa, brindan servicios de ahorros, que es la captación de los fondos del público a través de las diferentes modalidades, y de créditos, que es la colocación de los fondos captados. Estas instituciones deben cumplir las normativas emitidas por el ente regulador. Una de las normativas está relacionada a la gestión del riesgo operacional, que es uno de los componentes del riesgo corporativo y que, según Basilea II, ha desplazado al tradicional interés por los riesgos de crédito y mercado, centrándose los esfuerzos a los riesgos asociados a las operaciones, como: personas, procesos, tecnología información y aspectos externos.

Específicamente, sobre los riesgos relacionados con las TI, es importante que las instituciones financieras incorporen procedimientos, métodos y herramientas que les permita aplicar mejores prácticas para gestionar este tipo de riesgo, tomando en consideración lo establecido en la normativa peruana y los criterios difundidos por el ente regulador.

Sin embargo, la complejidad de las *TI* hace que sea muy difícil de entender y tomar buenas decisiones acerca de los riesgos de *TI.* En nuestro medio la mayoría de las empresas utilizan un enfoque intuitivo para la gestión de riesgos: abordan los riesgos de alto perfil, reciben toda la atención, tales como virus o cortes de energía o caída de la red de datos, pero se deja de lado los riesgos de perfil más bajo, como por ejemplo: controles internos inadecuados o envejecimiento de las tecnologías y controles, aplicaciones frágiles, que podrían ocasionar pérdidas considerables. Otro aspecto que se debe tener en cuenta es que existe un alto componente cualitativo en el gobierno y en la gestión de riesgos de *TI* que dificulta el desarrollo de adecuadas herramientas de identificación, medición y control, y que sean concordantes con las exigencias de la SBS. Por ahora, la gestión de los riesgos operativos de *TI* adopta sólo estándares que generalmente desarrollan un procedimiento cuantitativo. Existe la necesidad de llegar a modelos cuantitativos y cualitativos.

Esta investigación propone un modelo para la gestión de riesgos operativos de *TI* como parte del Sistema de Gestión de la Seguridad de la Información, desde una perspectiva que integra técnicas cuantitativas y cualitativas para entidades financieras tipo pymes, cajas rurales o municipales.

Palabras claves: Gestión de riesgos de *TI*, perfil de riesgo, niveles de riesgo, método Delphi.

Abstract

In Peru, specifically in Lambayeque, financial institutions with the authorization of the Superintendency of Banking and Insurance (SBS), and that enjoy economic, financial and administrative autonomy, provide savings services, which is attracting the funds from the public through different forms, and credit, which is the placement of funds raised. These institutions must comply with the regulations issued by the regulator.

One of the regulations is related to operational risk management, which is one component of corporate risk and that, according to Basel II, it has displaced the traditional interest credit risks and market, focu-

1. M. Sc. Ing. Docente de la Universidad Nacional Pedro Ruiz Gallo de Lambayeque.

sing efforts on the risks associated with operations, such as people, processes, information technology and external aspects.

Specifically, about the risks related to *TI*, it is important that financial institutions incorporate procedures, methods and tools that allow them to apply best practices to manage this type of risk, taking into account the provisions of the Peruvian law and criteria disseminated by the regulator.

However, the complexity of *TI* makes it very difficult to understand and make good decisions about IT risks. In our area most companies use an intuitive approach to risk management: address the risks of high-profile, get all the attention, such as viruses or power outages or network outage data, but neglects risks lower profile, such as: inadequate internal controls or aging technologies and controls, fragile applications, which could cause considerable losses. Another aspect to consider is that there is a high qualitative component in the governance and management of *TI* risk hampering the development of appropriate tools for the identification, measurement and control, and are consistent with the requirements of the SBS . For now, the management of operational risks take only *TI* standards generally develop a quantitative procedure. There is a need to provide quantitative and qualitative models.

This research proposes a model for managing *TI* operational risks as part of the information security management system, from a perspective that integrates quantitative and qualitative techniques for financial institutions such SMEs, rural and municipal savings.

Keywords: *TI* risk management, risk profile, risk levels, Delphi method.

INTRODUCCIÓN

Las tecnologías y los sistemas de información (TSI) se han convertido en los elementos más esenciales para la supervivencia de las organizaciones, ya que de las TSI dependen el buen funcionamiento y la evolución de sus procesos de negocio, así como la información que necesitan para tomar todas sus decisiones operacionales, tácticas y estratégicas. (Fernández Sánchez & Piattini Velthuis, 2012).

Esto significa que el diseño de nuevos productos y servicios, la eficiencia de las operaciones y la capacidad de reaccionar ante cambios en el entorno competitivo depende, en gran medida, de la capacidad de adquirir, procesar y analizar información, lo que permite, a su vez, brindar a la alta dirección información de forma continua, oportuna y condensada para un adecuado proceso de toma de decisiones respecto a riesgos y controles.

Con el entorno y dinámicas competitivas de la actualidad, contar con tecnología de información y comunicaciones no supone por sí misma una ventaja competitiva para las organizaciones. Es la gestión de esa tecnología la que puede dar ventaja o marcar un factor diferencial para el éxito de ésta. De acuerdo a esto, apropiarse de un modelo de gobierno TI, para esta gestión, es un elemento clave para el cumplimiento de los objetivos de la empresa. (Marulanda Echevarría, López Trujillo, & Cuestas Iglesias, 2009).

Por ello cobran cada día más interés el gobierno y la gestión de las TSI, temas en los cuales el director de TI es llamado a desempeñar un papel crucial. El director de TI deberá implementar un conjunto de buenas prácticas de gobierno y de gestión en las diferentes áreas relacionadas con la prestación de servicios, desarrollo de software, seguridad, gestión de activos, etc. (Fernández Sánchez & Piattini Velthuis, 2012).

Según Westerman (2006), con la tecnología de la información convirtiéndose en una parte cada vez más importante en toda empresa, la gestión de riesgos de TI se ha convertido en vital importancia para las oficialías de seguridad de la información y sus contrapartes comerciales. Cada empresa se enfrenta a un gran número de riesgos como parte de hacer negocios. Algunos riesgos, como la pérdida de un ejecutivo clave, no están relacionados con TI. Otros, como el riesgo de crédito global, tienen un importante componente de TI.

Toda empresa desarrolla un “Perfil de Riesgo Empresarial”. Todavía, pocas organizaciones, al considerar una nueva iniciativa (producto o servicio), van más allá del retorno de la inversión y no consideran su efecto sobre el perfil de riesgo de la empresa. Se debe tener en cuenta que un cambio en TI afecta múltiples dimensiones dentro de la empresa. Muchas empresas caen en patrones de análisis de un solo tipo de riesgo -comúnmente disponibilidad-, dándosele prioridad sobre los demás. O, peor aún, no tienen la capacidad para analizar y examinar más de una dimensión de riesgo. Con el tiempo, esta forma de gestión del riesgo se convierte en una práctica habitual de la empresa, dando lugar a un perfil de riesgo en la que algunos riesgos están bien controlados, mientras que otros tienen enormes (a menudo desconocidas) exposiciones. (Westerman, 2006).

La pregunta es ¿cómo hacer que la gestión de TI desarrolle un modelo de perfil de riesgo de TI empresarial, concordante con su SGSI y capacidad instalada de TI; y a su vez que satisfaga todas las perspectivas funcionales de los responsables de la gobernanza y de la gestión de las TI internos y externos?

Definición del perfil de riesgo de TI de una empresa

En la gestión de TI es necesario tener en cuenta tres aspectos básicos: implantación eficaz de las TI, procesos de gobernanza del riesgo y la cultura con-

sciente sobre el riesgo, para lograr la efectiva gestión de los riesgos. Las empresas que logren constituir modelos de gestión de TI que incluyan estos tres aspectos, realizarán una gestión de riesgos más eficaz y sus ejecutivos de negocios tendrán una mejor comprensión de sus niveles de riesgo de TI y las formas como se pueden atenuar. Cuando se hace una buena gestión de riesgos de TI se madura, y pasa de una situación de difícil manejo de las actividades de cumplimiento y reducción de amenazas hasta llegar a servicios de TI ágiles que generen valor al negocio. (Westerman, 2006).

Un perfil de riesgo debe determinar e identificar cuatro componentes:

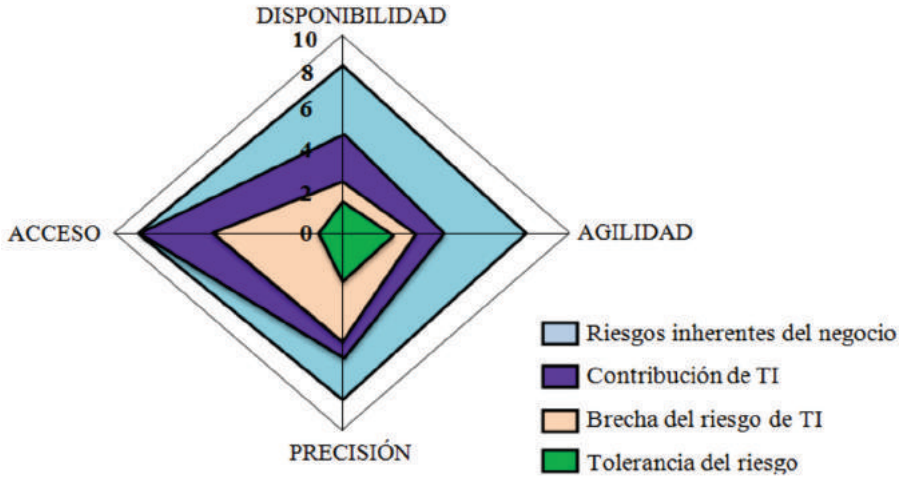
a. Nivel potencial e inherente de riesgo, que consiste en estimar el nivel de exposición a los riesgos que tiene la empresa, por las características propias del negocio, sin ninguna implementación de algún tipo de control.

b. Controles provenientes de las TI. La implementación de TI trae consigo una serie de controles relacionados con los activos o con los procesos de TI, que permiten mitigar los riesgos, obteniendo un nivel de riesgo conocido como riesgo intrínseco.

c. Tolerancia de riesgos. Cada empresa define, sobre la base a sus características, contexto y capacidad instalada, hasta qué niveles de riesgo está dispuesta tolerar (a partir de allí convivir con ellos) en cada una de las dimensiones del riesgo.

d. Brecha del riesgo de TI. Es el margen existente entre el riesgo intrínseco encontrado y la tolerancia de riesgo definido por la empresa para una determinada dimensión de riesgo. La identificación de esta brecha permitirá tomar las decisiones correctas sobre la implementación y priorización de los controles y sobre la inversión en seguridad de TI.

Figura N° 01: Ejemplo de un perfil de riesgo empresarial



Fuente: Adaptado de Westerman, (2006) y Merino Bada & Cañizares Sales (2011).

Como se muestra en el ejemplo, el perfil de riesgo se convierte en una herramienta que permite determinar y mostrar el nivel de exposición al riesgo relativo de una empresa y la tolerancia al riesgo en cada una de las cuatro dimensiones de riesgo. El diamante celeste representa el nivel potencial e inherente de riesgo del negocio visto como un todo, antes de realizar cualquier gestión de riesgos. El diamante morado representa el componente de riesgo relacionado con las TI de la empresa, en cada categoría. El diamante interior verde representa el nivel de tolerancia de riesgos de TI que la empresa acepta para convivir con ella. Por último, el color beige representa la brecha de riesgo que aún no ha sido mitigado, entre el riesgo inherente y el aporte de la TI.

El perfil de riesgo también puede servir como una herramienta de negociación. Los desacuerdos sobre las prioridades de TI se pueden resolver tomando en cuenta la exposición al riesgo de la empresa (diamantes de color beige) y la tolerancia al riesgo definida por la misma empresa (diamante verde), ayudando a forjar una dirección común para el futuro.

Se ha identificado cuatro dimensiones de riesgos de negocio: la disponibilidad, el acceso, la precisión y la agilidad. Casi todas las grandes decisiones de TI implican el análisis de estas cuatro dimensiones de riesgos mencionados. Estos riesgos se derivan de la forma como los activos y los procesos de TI son gestionados y organizados en la empresa. Por tanto, la comprensión de los niveles de riesgo de la empresa y de

la tolerancia al riesgo de estas cuatro dimensiones, es el primer paso en la implementación de un proceso maduro de gestión de riesgos de TI.

a. Disponibilidad: mantener operativo o en funcionamiento los procesos existentes y la recuperación de interrupciones.

b. Acceso: garantizar que las personas autorizadas tienen las facilidades necesarias para el acceso a la información y que las personas no autorizadas no tengan acceso.

c. Precisión: ofrecer información precisa, oportuna y completa, que cumpla con los requisitos de gestión, del personal, de los clientes, de los proveedores y reguladores.

d. Agilidad: permitir la implementación de nuevas iniciativas estratégicas, tales como la adquisición de una empresa, el rediseño de procesos de negocio o el lanzamiento de un nuevo producto/servicio.

Gestión eficaz de riesgo

Para determinar el perfil de riesgo se debe asociar las cuatro dimensiones del riesgo con los factores de riesgo, con la finalidad de comprender cuáles son las causas que determinan los valores estimados en cada dimensión de riesgo y, cuáles son los factores que lo originan. La figura N° 02 establece esta relación.

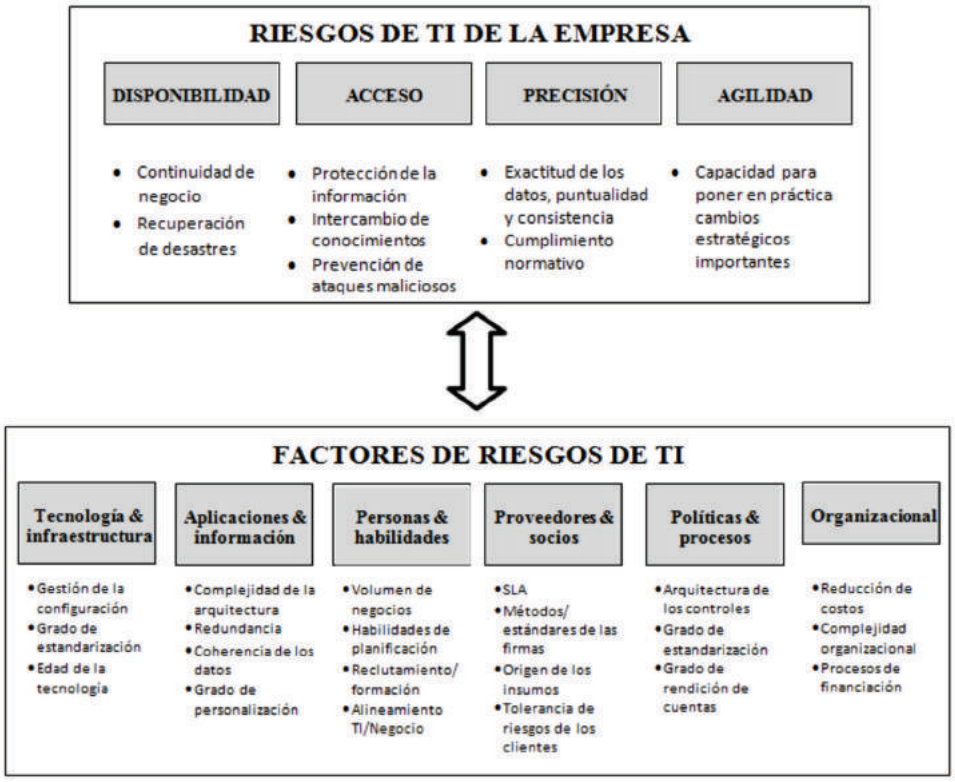
La gestión eficaz del riesgo es una combinación coherente de tres disciplinas básicas:

- Proceso de gobernanza del riesgo: políticas completas y eficaces relacionadas con el riesgo, combinado con un proceso maduro y consistente para identificar, evaluar, priorizar y supervisar los riesgos oportunamente.

- Cultura consciente sobre riesgos: personas cualificadas que saben cómo identificar y evaluar las amenazas e implementar la mitigación efectiva del riesgo.

- Implantación eficaz de TI: infraestructura y las aplicaciones de TI que tienen riesgos inherentemente inferiores a los tolerables, debido a que están bien gestionados y tienen una buena arquitectura.

Figura N° 02: Marco de referencia de la gestión de riesgos de TI en la empresa



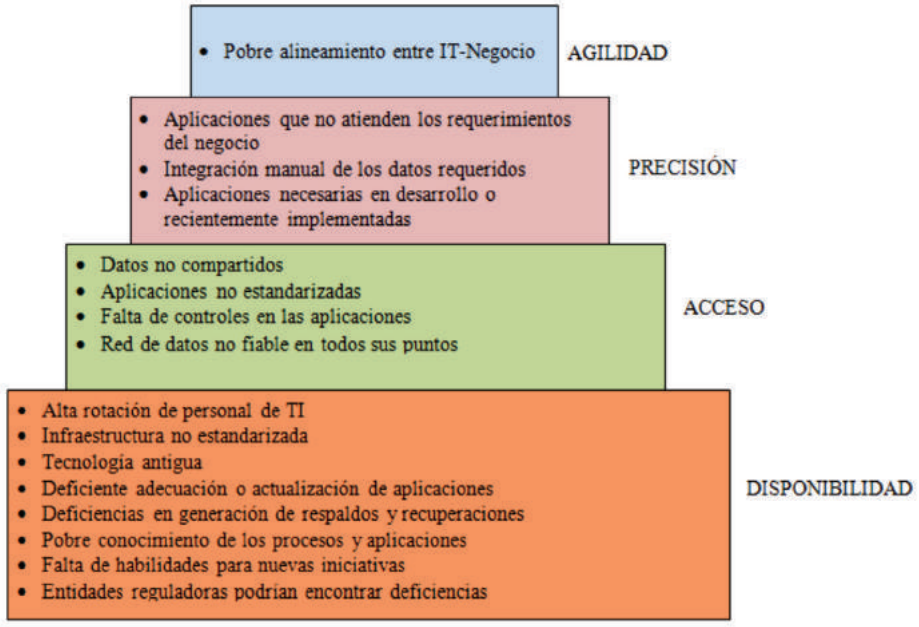
Fuente: Adaptado de Westerman, IT Risk Management: From IT Necessity to Strategic Business Value (2006) (Sallé, 2004).

Proveedores & Socios - SLA: Service Level Agreement . Acuerdos de Niveles de Servicio.

Si una empresa es deficiente en cualquiera de las tres disciplinas, no pueden ser eficaces en la gestión de riesgos de TI. Por ejemplo, se puede contar con procesos de gestión de riesgos muy aceptables y de mucha experiencia pero que superan la capacidad instalada de TI. Del mismo modo, la gobernanza del riesgo no puede ser eficaz sin los conocimientos necesarios para identificar y reducir los riesgos. Sin embargo, las empresas no tienen que ser "expertas y eficaces" en los tres disciplinas; puede ser en una, pero con niveles bajos (pero aceptables) en los otros dos. También hay que tomar en cuenta que las empresas que tienen una gestión de riesgos ineficaz no pueden convertirse de la noche a la mañana en eficaces; pues esta capacidad se construye en el tiempo mediante con mucha disciplina.

Desafortunadamente, los métodos de gestión de riesgos utilizados en la mayoría de las empresas son incapaces de hacer frente a la complejidad de los riesgos de TI, dejando a la empresa vulnerable a riesgos de TI que ocasionan costosas pérdidas. Los riesgos de TI se derivan de la forma como la infraestructura, las aplicaciones, las personas y las políticas de TI están siendo administradas y organizadas. Tecnologías no estandarizadas, inconsistentes procesos de mantenimiento de aplicaciones, políticas ineficaces o falta de habilidades del personal son sólo algunos de los factores que generan riesgos sobre la continuidad de los procesos, la gestión del acceso a los recursos de información, la integridad de la información, etc. Los factores de riesgo son interdependientes. En la figura N° 03 se muestra la interdependencia de los factores de riesgo en una pirámide.

Figura N° 03: Pirámide de los riesgos de TI



Fuente: Adaptado de Westerman (2006). Van Grembergen, De Haes, & Guldentops (2000).

Requerimientos de la Superintendencia de Banca y Seguros (SBS)

El ente encargado de regular y supervisar las entidades financieras en el Perú, incluidas las CRAC de Ahorro y Crédito es la Superintendencia de Banca, Seguro y AFP (SBS) que es un organismo que tiene dos tareas primordiales: la regulación y la supervisión. La regulación porque establece reglas para que las empresas supervisadas puedan cumplirlas y la supervisión que consiste en verificar el cumplimiento de las normas, políticas y prácticas por parte de las empresas supervisadas. (Superintendencia de Banca, Seguro y AFP, 2009).

La SBS ha determinado algunas normas específicas para tres ámbitos diferentes:

- Gestión de seguridad de la información:, que establece criterios para gestionar la seguridad de la información y toma como referencia estándares internacionales como el ISO 17799 e ISO 27001. (SBS - Superintendencia de Banca, Seguro y AFP, 2009).

- Gestión de continuidad del negocio: Circular N° G-139-2009 sobre gestión de continuidad del negocio, que establece criterios al respecto, y parte de la gestión de riesgo operacional que tienen que enfrentar las empresas supervisadas por la SBS, las cuales toman como referencia los estándares internacionales como el BS-25999. (SBS - Superintendencia de Banca, Seguros y AFP del Perú, 2009).

- Riesgos operativos de TI: Circular N° G-105-2002 sobre riesgos de tecnología de información, que establece criterios para identificar y gestionar los riesgos relacionados con las tecnologías de información. (SBS - Superintendencia de Banca, Seguros y AFP del Perú, 2002).

Las normativas indicadas determinan como marcos guías de referencia la norma ISO/IEC 27001, modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI), entendiéndose por seguridad de la información la preservación de la confidencialidad, integridad, y disponibilidad de la información y para la implementación de controles y de las medidas reactivas, correctivas y preventivas en la gestión de la información, que aseguren conseguir las tres características básicas de la seguridad de la información, plantea como estándar a la ISO/IEC 17799 (ISO/IEC 27002). (INDECOPI, 2007) (INDECOPI, 2008).

La realidad de la gestión de riesgos de TI en las pequeñas entidades financieras de Lambayeque

Según los informes sobre los sistemas de gestión de riesgos de TI, de auditorías externas, el contexto de la gestión de riesgos en las pequeñas entidades financieras de Lambayeque se resume de la siguiente manera:

- Existen problemas para definir los riesgos de TI de acuerdo a las categorías de información exigidas por la SBS.

- Los procedimientos para la evaluación de riesgos de TI no están integrados al modelo en la gestión de riesgos corporativo.

- Bajo nivel de concientización del personal en relación a la aplicabilidad de los controles de TI.

- No se está cumpliendo totalmente con los requisitos y exigencias mínimas en la normativa de la SBS, en relación a la gestión de riesgos (Avalos Ruiz, 2012).

- No existe un procedimiento adecuado para identificar y evaluar las amenazas vulnerabilidades, impactos, frecuencias. (Marcador de Posición1) (SBS - Superintendencia de Banca, Seguros y AFP del Perú, 2009).

- No es efectivo el procedimiento para el monitoreo de las actividades de gestión de riesgos de TI.

- Bajo nivel de aplicabilidad del proceso para la evaluar los riesgos de TI, en la actualidad. (Avalos Ruiz, 2012).

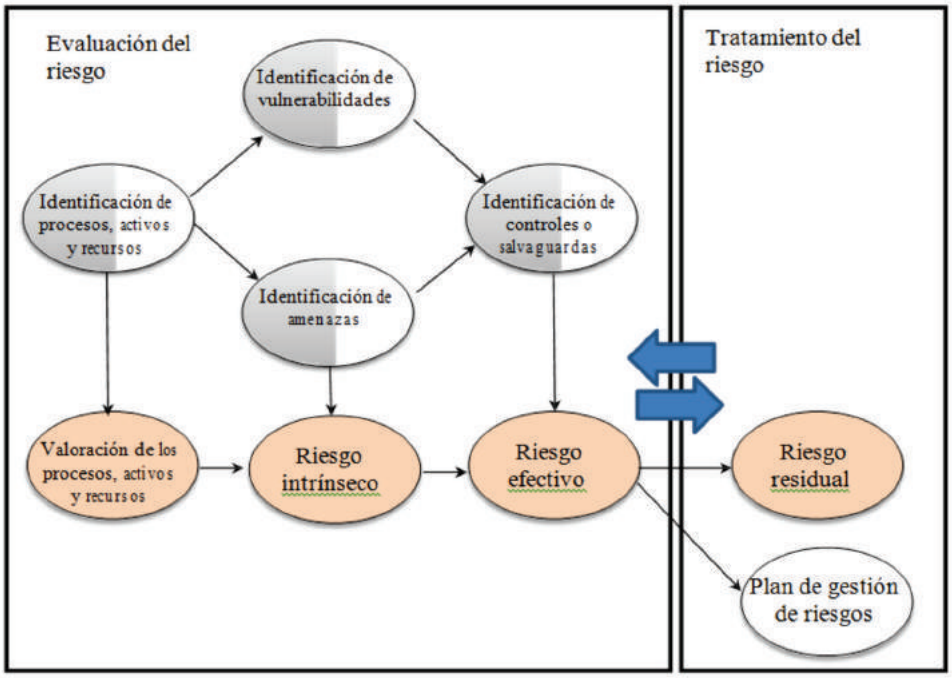
- Incoherencias en los resultados obtenidos con respecto a los cálculos actuales para determinar los niveles de riesgos inherentes de TI.

- Falta de un procedimiento para determinar los controles adecuados, según los niveles de exposición a los riesgos y para el seguimiento de las brechas de seguridad.

Modelo de gestión de riesgos propuesto para las pequeñas entidades financieras de Lambayeque

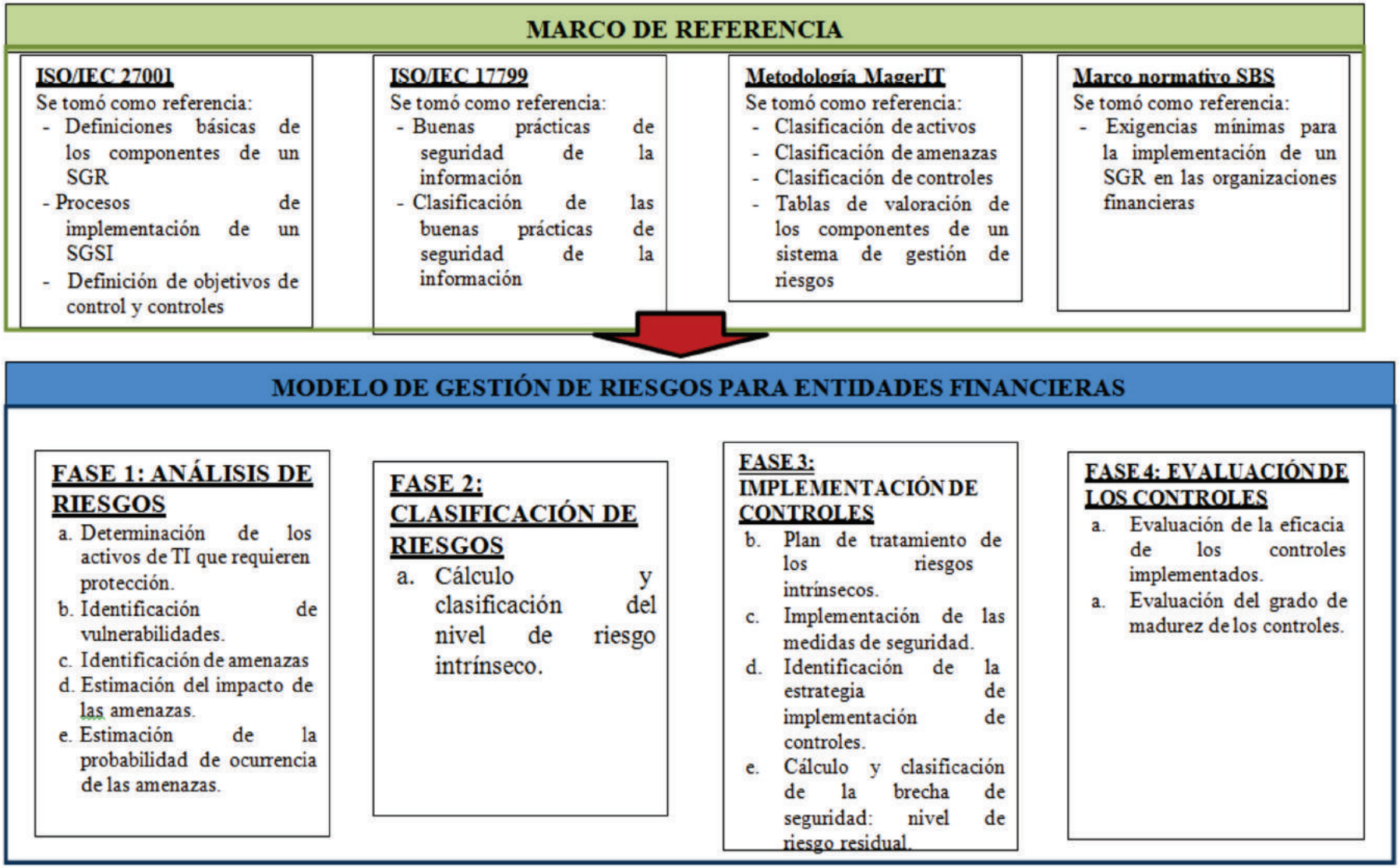
El modelo general de gestión de riesgos propuesto y la metodología para su aplicación están resumidos en los siguientes figuras:

Figura N° 04: Modelo general del modelo de análisis de riesgos propuesto



Fuente: Elaboración propia.

Figura N° 05: Metodología para la aplicación del modelo de análisis de riesgos propuesto



Metodología de recolección de datos y evaluación del modelo

Se utilizó como referencia el método Delphi propuesto por los matemáticos norteamericanos Norman Dalkey y Olaf Hermes en 1963, con el propósito de establecer el consenso de expertos (Trujillo, 2004). Se aplicó a las personas que tienen autoridad y desempeñan funciones de gestión de riesgos y de la continuidad de procesos en tres entidades financieras tomadas como muestra (no se mencionan por seguridad), con el fin de valorar objetivamente la efectividad en el diseño y la efectividad del modelo propuesto.

Se obtuvo la opinión y el conocimiento de las personas encargadas de las funciones de:

- Jefatura de TI.
- Jefatura de la Unidad de Riesgos.
- Oficialía de Seguridad de TI y de la Información.
- Jefatura de la Unidad de Continuidad de negocio.
- Auditor interno.

Para su aplicación se consideró las siguientes características:

- Anonimato: Durante su aplicación ninguna de las personas que evaluaron el modelo supieron que los otros también estaban evaluando el modelo. Esto permitió que ninguna de los evaluadores del modelo sea influenciado por el conocimiento y experiencia de otro.
- Iteración y realimentación controlada: La iteración se consiguió al presentar el mismo cuestionario a todos los evaluadores de forma independiente.
- Respuesta del grupo: La información que se presenta a los evaluadores no es sólo el punto de vista de la mayoría, sino que se presentan todas las opiniones indicando el grado de acuerdo obtenido.

El procedimiento realizado fue el siguiente:

1. Se elaboró un cuestionario.
2. Conseguir su compromiso de colaboración. Las personas elegidas conocen del tema y del modelo propuesto. Sin embargo, se socializó y explicó de forma individual al panel de personas seleccionadas, la metodología y los modelos propuestos.
3. Se determinó el contexto y el horizonte temporal (tiempo de aplicación) para la aplicación del cuestionario. En este caso la metodología y modelos propuestos fueron utilizados durante tres (03) meses, entre noviembre del 2013 a enero del 2014.
4. Posteriormente, se les envío a través de correo electrónico, un archivo con los cuestionarios diseñados en hojas electrónicas, que contienen los niveles, factores y variables definidas a través de preguntas, para que cada uno de ellos comparta sus opiniones sobre la relevancia del modelo propuesto en este trabajo. La asignación de la relevancia por parte del "experto", se realiza respondiendo "sí" o "no" a cada factor y variable del cuestionario y la asignación de los pesos, la realiza mediante el análisis y aplicación del criterio profesional y su función dentro de entidad, asignando o distribuyendo un peso porcentual utilizando la escala de (0% al 100%) para cada pregunta, rango, evento y nivel que conforman las variables, así:

Los diseños de los cuestionarios enviados al panel de personas seleccionadas fueron:

a. Cuestionario para la prueba de la efectividad del diseño:
Objetivo: Probar la efectividad del diseño del modelo propuesto determinando si los controles de la entidad son operados como fue prescrito por las personas que poseen la autoridad y competencias necesarias para desempeñar la gestión de la seguridad, el control y la gestión de riesgos y, si satisfacen los objetivos de control exigidos por la SBS para prevenir o detectar riesgos de TI.

b. Cuestionario para la prueba de la efectividad de operación:
Objetivo: Probar la efectividad de la operación del modelo propuesto determinando si está operando tal y como fue diseñado y si las personas que desempeñan la gestión de la seguridad, el control y la gestión de riesgos posee las competencias necesarias para desempeñar el control de manera efectiva.

Para cada uno de los cuestionarios se utilizará la siguiente tabla de referencia para calificar los pesos de cada una de los indicadores de cada variable:

Peso	Significado	Color
1	Clave	
2	Relevante	
3	Estándar	
4	Irrelevante	

Leyenda

- Clave: El indicador evaluado del modelo propuesto es importante considerarlo en el Sistema de Gestión de Riesgos de la entidad, porque cumple con los requisitos exigidos en la normativa la SBS y se adecúa a las funciones de la entidad.
- Relevante: El indicador evaluado del modelo propuesto puede considerarse en el Sistema de Gestión de Riesgos de la entidad, porque cumple con los requisitos exigidos en la normativa la SBS.
- Estándar: El indicador evaluado del modelo propuesto puede considerarse en el Sistema de Gestión de Riesgos de la entidad, con algunas modificaciones y mejoras para cumplir con los requisitos exigidos en la normativa la SBS y para que se adecúe a las funciones de la entidad.
- Irrelevante: El indicador evaluado del modelo propuesto no cumple con los requisitos exigidos en la normativa la SBS por lo que no podría considerase en el Sistema de Gestión de Riesgos de la entidad.

Los resultados del análisis Delphi se muestran en las siguientes tablas:

Tabla N 01: Resultado de la evaluación de los factores y variables para probar la efectividad del diseño del modelo propuesto

			Jefe de TI		Jefe Unidad Riesgos		Oficialía de Seguridad Info		Jefe Continuidad procesos		Auditor interno		TOTALES	
Variable		Factor Relevante (indicador)	SÍ/NO	Peso	SI/NO	Peso	SI/NO	Peso	SI/NO	Peso	SI/NO	Peso	SI/NO	Peso
Perspectiva: Gestión de riesgos de TI														
Estructuración de la metodología de análisis y tratamiento de riesgos	1	Se ha definido nítidamente las categorías –Í como disponibilidad, integridad y confidencialidad – en las que se pueden agrupar los riesgos de TI.	SÍ	2	SÍ	2	SÍ	1	SÍ	2	SÍ	2	100%	2
	2	La gestión de riesgos de TI se integra en la gestión de riesgos general para todos los riesgos a nivel corporativo.	SÍ	2	SÍ	2	SÍ	1	SÍ	2	NO	4	80%	2
	3	Su estructura está diseñada para que los empleados relacionados con la gestión de la seguridad de TI y de riesgos puedan entenderlo y alcanzar el grado de cultura y concientización deseado.	SÍ	2	SÍ	3	SÍ	2	SÍ	3	SÍ	2	100%	2
Gobierno de los riesgos de TI	4	Contempla todas las variables necesarias exigidas por la SBS para su evaluación.	SI	2	SI	2	SI	2	SI	2	SI	3	100%	2
	5	Se ha establecido pautas para evaluar la magnitud de los riesgos de modo coherente.	SÍ	2	SÍ	3	SÍ	3	SÍ	2	NO	4	80%	3
	6	Se cuenta con indicadores clave para monitorear periódicamente la eficacia de nuestras actividades de gestión de riesgos de TI.	SÍ	3	SÍ	3	SÍ	2	SÍ	2	SÍ	2	100%	2
		TOTAL (%)	100%		100%		100%		100 %		67%		93%	2

Tabla N° 02: Resultado de la evaluación de los factores y variables para probar la efectividad de la operación del modelo propuesto

			Jefe de TI		Jefe Unidad Riesgos		Oficialía de Seguridad Info		Jefe Continuidad procesos		Auditor interno		TOTALES	
Variable		Factor Relevante (indicador)	SI/NO	Peso	SI/NO	Peso	SI/NO	Peso	SI/NO	Peso	SI/NO	Peso	SI/NO	Peso
Perspectiva: Gestión de riesgos de TI														
Análisis y tratamiento de riesgos	1	A partir del modelo propuesto se puede establecer un proceso formal y coherente para evaluar periódicamente potenciales riesgos de TI.	SÍ	2	SÍ	2	SÍ	2	SÍ	2	SÍ	2	100%	2
	2	Se puede determinar con efectividad los niveles de riesgos inherentes de TI.	NO	2	SI	2	SI	2	SI	2	SI	2	80%	2
	3	Se puede evaluar la efectividad de los controles y hacer seguimiento de las brechas de seguridad.	SÍ	2	NO	4	SI	2	SI	2	NO	4	60%	3
Gobierno de los riesgos de TI	4	La información resultante del modelo es significativa para cumplir con los informes exigidos por la SBS en relación a la gestión de riesgos de TI.	SÍ	2	SÍ	2	SÍ	3	SÍ	2	SÍ	3	100%	2
	5	La información resultante del modelo sirve para tomar decisiones con efectividad en relación a las inversiones e importancia de los controles de seguridad.	NO	4	NO	4	NO	4	NO	4	NO	4	0%	4
		TOTAL (%)	60%		60%		80%		80%		60%		68%	3

De los resultados obtenidos se puede concluir lo siguiente:

Conclusiones

1. Se ha logrado implementar un modelo de gestión de riesgos de TI, que identifica, evalúa y trata nítidamente los activos de TI, sus amenazas, debilidades y niveles de riesgo relacionadas con las categorías: disponibilidad, integridad y confidencialidad de la información, que exige la SBS para este tipo de organizaciones en sus planes de seguridad (Circular G-139-2009 – SBS (Gestión de la continuidad del negocio), Circular G-140-2009 – SBS (Gestión de la seguridad de la información) y Resolución S.B.S. N° 2116 -2009). Esto ha permitido establecer pautas para evaluar la magnitud de los riesgos de modo coherente y contar con indicadores clave para monitorizar periódicamente la eficacia de las actividades de gestión de riesgos de TI en las entidades financieras tomadas como muestra, mediante la evaluación de brechas de efectividad de los controles de seguridad de la información.

2. El producto tangible de la metodología de gestión de riesgos es la matriz de riesgos y a través de ella se ha logrado disponer de un registro permanente y actualizado de los principales activos de TI a proteger, de modo que se garantice la continuidad operativa, vía los planes mitigación, de los riesgos inmersos en cada activo. Esto ha permitido una adecuada sinergia con los procedimientos de continuidad del negocio.

3. Queda demostrado que la metodología de gestión de riesgos de TI, permite identificar los niveles de riesgos de tal forma que sirve de información para la toma de decisiones en relación la inversión para la implementación de los controles que sirvan de salvaguardas en la protección del proceso contra posibles amenazas y vulnerabilidades.

Recomendaciones

1. Dado que la evaluación de los riesgos es permanente se recomienda que el modelo de matriz de riesgos que se propone sea implementada en una aplicación informática, que permita actualizaciones más dinámicas, con posibilidades de generar indicadores/resultados gráficos y generación de escenarios.

2. Es conveniente que la oficialía de la seguridad de la información designe responsabilidades que permitan, mediante la automatización de la propuesta metodológica, alimentar permanentemente de la información necesaria por los verdaderos dueños de los procesos: lista de procesos/servicios críticos, activos, riesgos, amenazas, vulnerabilidades, controles, etc., de tal forma que permita obtener rápidamente la información del nivel de criticidad de sus procesos, porcentaje de desviación de riesgo de los activos o procesos, capital necesario a invertir en la protección de un activo o proceso, entre otra información relevante.

3. Para lograr mejores resultados en la gestión de riesgos de TI, la Oficialía de seguridad de la información deberá de tener en cuenta factores estratégicos como: el apoyo y compromiso de la dirección, difusión y sensibilización permanente sobre control y seguridad de la información, orientación hacia la formalización de procesos y actividades, una permanente verificación y pruebas de control que garanticen la disponibilidad, integridad y confidencialidad de información y finalmente un adecuado plan de despliegue de la cultura de riesgos que garantice la participación general de los empleados.

Referencias bibliográficas

Avalos Ruiz, C. (2012). *Análisis, diseño e implementación del sistema de riesgo operacional para entidades financieras* - SIRO. Tesis. (P. U. Perú, Ed.) Lima, Perú:
s/e.

De Haes, S., & Van Grembergen, W. (2004). *IT Governance and Its Mechanisms.* (I. S. Inc., Ed.) Informations Sytems Control Journal.

Fernández Sánchez, C. M., & Piattini Velthuis, M. (2012). *Modelo para el gobierno de las TIC basado en las normas ISO.* A. Certificación, Ed. Madrid, España: AENOR Ediciones.

INDECOPI. (2007). EDI. *Tecnología de la información. Código de buenas prácticas para la gestión de la seguridad de la información.* Norma Técnica, Comisión de Reglamentos Técnicos y Comerciales - INDECOPI, Lima, Perú.

INDECOPI. (2008). EDI - *Tecnología de la Información. Técnicas de seguridad. Sistemas de Seguridad de la Información. Requisitos.* Norma Técnica.

Marulanda Echevarría, C. E., López Trujillo, M., & Cuestas Iglesias, C. A. (Mayo de 2009). Modelos de desarrollo para gobiernos de TI. (U. T. Pereira, Ed.) *Scientia et Technica,* Año XV(No 41).

Mataracioglu, T., & Ozkan, S. (2011). Governing information security in conjunction with COBIT and ISO 27001. Ankara, Turquía: Middle East Technical University, Informatics Institute.

Merino Bada, C., & Cañizares Sales, R. (2011). *Implantación de un sistema de gestión de seguridad de la información según ISO 27001: un enfoque práctico.* (F. CONFEMETAL, Ed.) Madrid, España: FC Editorial.
Peterson, R. (2003). Integration Strategies and Tactics for Information Technology Governance. Strategies for Information Technology Governance. Wim Van Grembergen, Idea Group.

Reinares Lara, D. (2009). Implantación de la ISO27001: *Factores críticos de éxito y visión de la norma como motor de generación de valor añadido.* Madrid, España: Innotec System.

Sallé, M. (2004). *IT Service Management and IT Governance: Review, Comparative Analysis and their Impact on Utility Computing.* H.-P. Company, Ed. Palo Alto, USA: HP Research Labs.

SBS - Superintendencia de Banca, Seguro y AFP. (2009). Circular N° G-140-2009.*Gestión de Seguridad de la Información.* Perú.

SBS - Superintendencia de Banca, Seguros y AFP del Perú. (2009). Circular Nº G- 139 -2009. *Gestión de la Continuidad del Negocio.* Perú.

SBS - Superintendencia de Banca, Seguro y AFP. (2009). Resolución S.B.S.N° 2116 -2009. *Reglamento para la Gestión del Riesgo Operacional.* Perú.

Van Grembergen, W., & De Haes, S. (2008). *Implementing Information Technology Governance:* Models, Practices and Cases. IGI Global.

Van Grembergen, W., De Haes, S., & Guldentops, E. (2000). Control and Governance Maturity Survey, Establishing a reference benchmark and a self-assessment tool. (I. T. Institute, Ed.)

Westerman, G. (2006). IT Risk Management: From IT Necessity to Strategic Business Value. M. S. Center for information systems research, Ed. *MIT Sloan Managment,* 12.