Los riesgos derivados de las TI son importantes para las compañías, en especial para los bancos. Este estudio recolecta las prácticas de cuatro bancos con operaciones en Colombia y analiza cómo estas medidas sirven para controlarlos y cómo los entes reguladores garantizan la efectividad de las mismas.

Riesgos de TI[1] en banca

Andrés Cheng C.
Santiago Pinilla M.
Juan D. Villa C.
Andrea Herrera S.

introducción

La Gestión de Riesgos de TI y el Sector Bancario Colombiano

Debido a la importancia de su rol en el desarrollo económico de un país, las instituciones financieras están sujetas a una estricta regulación. Ejemplos de estas son: los marcos Basilea I y II, la Ley de Sarbanes – Oxley y en Colombia, la ley 510 de 1999 [1].

Dichas regulaciones buscan mitigar los diferentes tipos de riesgos inherentes a las operaciones financieras y entre otros efectos

[1] TI acrónimo para Tecnologías de Información.

han tenido una repercusión importante sobre la madurez de este tipo de compañías en lo que respecta a la gestión de riesgos. Esta investigación ahonda en una categoría de estos riesgos en una muestra de bancos Colombianos: los riesgos de TI. Siendo una de las principales razones de interés al estudiar este tipo de compañías y de riesgos, la rápida y exitosa apropiación de TI en el sector.

En Colombia, el uso de TI como canal de comunicación con los clientes y herramienta de soporte a los procesos de negocio ha permitido que el área de TI se convierta en una ventaja competitiva que permite tener una mayor capacidad de adaptación a los cambios y una mayor productividad [8]. Para potenciar esta ventaja durante los últimos años se han creado marcos de referencia de gestión de riesgos de TI que buscan explicar y manejar las consecuencias de fallos en aplicaciones e infraestructura de TI en los procesos de negocio [3]. Justamente, este estudio de recolección y análisis de prácticas está enmarcado dentro de una investigación que busca construir una guía de mejores práctica en gestión de riesgos de TI para el sector mencionado [2].

Marco de Gestión de Riesgos 4A

A pesar de la madurez mencionada, el riesgo de TI todavía presenta dificultades en su gestión; siendo la principal que los ejecutivos del negocio, expertos en toma de decisiones frente al riesgo, no participan activamente por la falta de una comprensión clara del impacto que las TI tienen en el negocio, debido en muchas oportunidades a los términos técnicos propios del área. Esta problemática genera la necesidad de una herramienta que propicie un intercambio de información eficaz y eficiente en lo que concierne al riesgo de TI, en la organización.

Para lograr lo anterior, el marco 4A clasifica los riesgos de TI según el impacto que pueden generar teniendo como base cuatro objetivos: disponibilidad, acceso, precisión y agilidad. Adicionalmente, propone tres disciplinas que se deben desarrollar para disminuir los niveles de riesgo de TI, que son: base tecnológica, gobernabilidad del riesgo de TI y cultura sobre los riesgos de TI [8].

Teniendo claridad sobre estos objetivos y su contexto organizacional, primero las empresas identifican qué nivel de riesgo desean afrontar. Para esto, el marco provee un instrumento que les permite a los ejecutivos de negocio y de TI tener una perspectiva transversal a la organización del impacto de TI y por ende del nivel de riesgo deseado, construyendo el perfil de riesgos de TI de la compañía.

Este perfil se utiliza como "una herramienta para comunicar la exposición relativa y tolerancia al riesgo de una empresa, en los cuatro objetivos de negocio"[1] y su valor reside en que sirve como plano sobre el cual diseñar estrategias para acercarse al nivel deseado. El siguiente paso es construir capacidades para

[1] Westerman G., Hunter, R. IT Risk: Turning Business Threats Into Competitive Advantage. 2007.

alcanzar dicho perfil a través de las tres disciplinas mencionadas.

Una vez expuesto el marco de gestión de riesgos de TI utilizado se da paso a una breve descripción del sector objeto de estudio y de la regulación aplicable.

El Sector Bancario Colombiano y su Regulación de TI: Circular 052 de la SFC[2]

Entre 1923 y 1990 el sistema financiero siguió un modelo de banca especializada establecido por la ley 45 de 1923 [5]. El panorama actual de sector, es el producto de un proceso de fusiones y adquisiciones que dio paso al esquema Matriz – Filial [4] ampliando el portafolio de servicios a los clientes. Las actividades de regulación sobre el sector son llevadas a cabo por Banco República[3] y la SFC. En particular, la circular 052 de la SFC determina los "Requerimientos mínimos de seguridad y calidad en el manejo de información a través de medios y canales de distribución de productos y servicios para clientes y usuarios" [7].

A continuación los resultados consolidados del análisis del marco teórico.

Análisis bajo el marco 4A de la circular 052 de la SFC

La circular tiene siete numerales, los dos primeros hacen referencia a las instituciones que la deben cumplir y los restantes clasifican las medidas. El análisis hecho en [1], cuya síntesis se muestra a continuación, consiste en clasificar cada numeral del 3 al 7 según los objetivos y las disciplinas del marco 4A, para determinar qué aspectos son o no incluidos en la regulación colombiana.

Respecto a los objetivos se encuentra que el 79% de los numerales están bajo Acceso y Precisión. En lo referente a las disciplinas, la Figura 1 muestra que la mayoría de medidas busca mejorar la base tecnológica (74%) y la gobernabilidad de riesgos de TI en la organización (24%). Por otra parte, la disciplina de cultura

[2] SFC acrónimo para Superintendencia Financiera de Colombia, cuya misión es "preservar la confianza pública y la estabilidad del sistema financiero…"[6]

[3] Banco Central Colombiano.

con solo el 2% evidencia que este tema es incipiente, dejando la responsabilidad a los bancos del desarrollo de medidas para incentivarla.

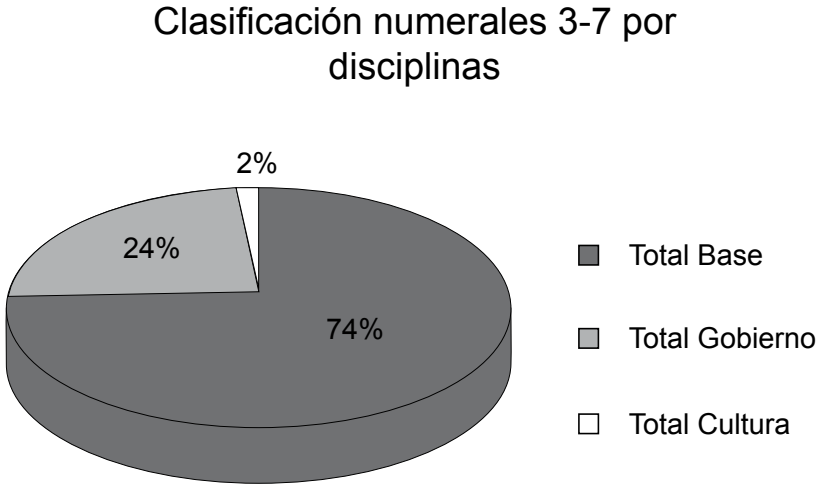

Figura 1: Análisis de la circular 052 bajo las disciplinas del marco 4A. [1]

Este análisis permite construir el perfil de riesgos de la circular, Figura 2.

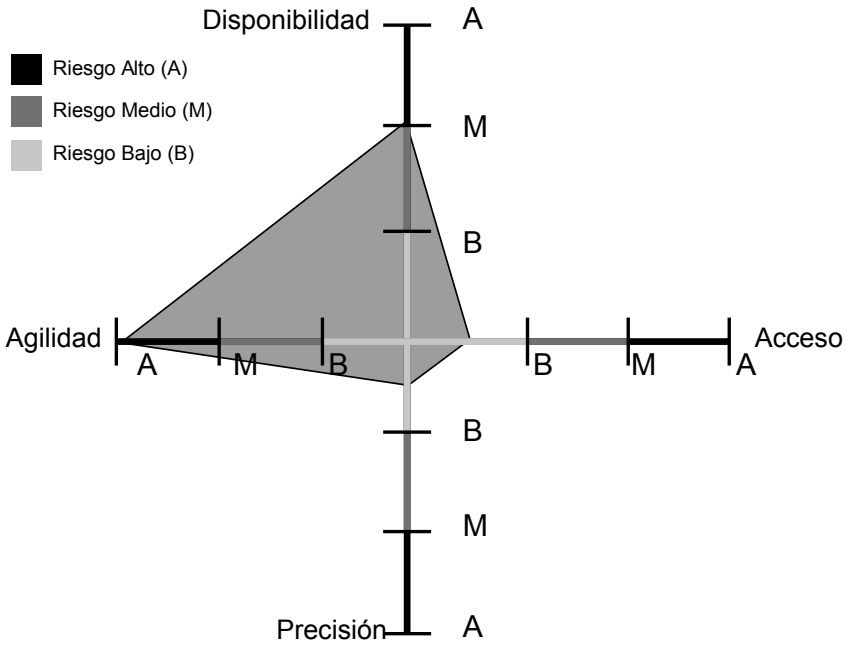

Figura 2: Perfil de riesgos de la circular 052 de la SFC [1]

Se concluye que la circular 052 tiene un perfil con niveles de riesgo altos para los objetivos de disponibilidad y agilidad; y bajos para acceso y precisión. Entonces, se puede suponer que un banco cuya gestión de riesgos de TI sea a través del cumplimiento de la circular, sería más vulnerable o tolerante al riesgo para los primeros objetivos mencionados con las implicaciones correspondientes [1].

A partir del análisis se presentan los resultados centrales de los casos de estudio.

Benchmarking de Gestión de Riesgos de TI en Bancos

Para comprender la manera en que los bancos reaccionan a su alta dependencia de TI, como trabajo de campo se analizan bajo la perspectiva del marco 4A y de la circular 052, las prácticas aplicadas en diferentes procesos de negocio por cuatro bancos con operaciones en Colombia, para implementar una gestión de riesgos de TI en términos de las necesidades del negocio. Esta muestra corresponde al 22% de los bancos colombianos y está compuesta por tres bancos de naturaleza privada y uno de naturaleza pública, el Banco de la República. Los nombres de los tres bancos privados han sido modificados por confidencialidad.

Los procesos de negocio son: para los Bancos A y C "Transacciones bancarias a través de internet", para el Banco B "Compra y venta de títulos valores en la Mesa de Dinero", y para el Banco de la República "Compensación de Cheques". Los principales resultados y conclusiones están basados en entrevistas con CIO's, ejecutivos de negocio y personal encargado de implementar la circular.

Construcción y Comparación de los Perfiles de Riesgo de TI Ideales

La metodología empleada para generar el perfil de riesgos de TI ideal consiste en aplicar el instrumento del marco 4A [8], luego evaluar las preguntas de nivel ejecutivo en cuatro variables de impacto (económico, sobre los clientes, regulatorio y en la reputación del Banco) que miden el efecto de TI en el negocio en términos cualitativos (Alto, Medio o Bajo) y para calcular el impacto promedio del riesgo de TI se asigna un valor numérico [1], como se muestra en la Figura 3.

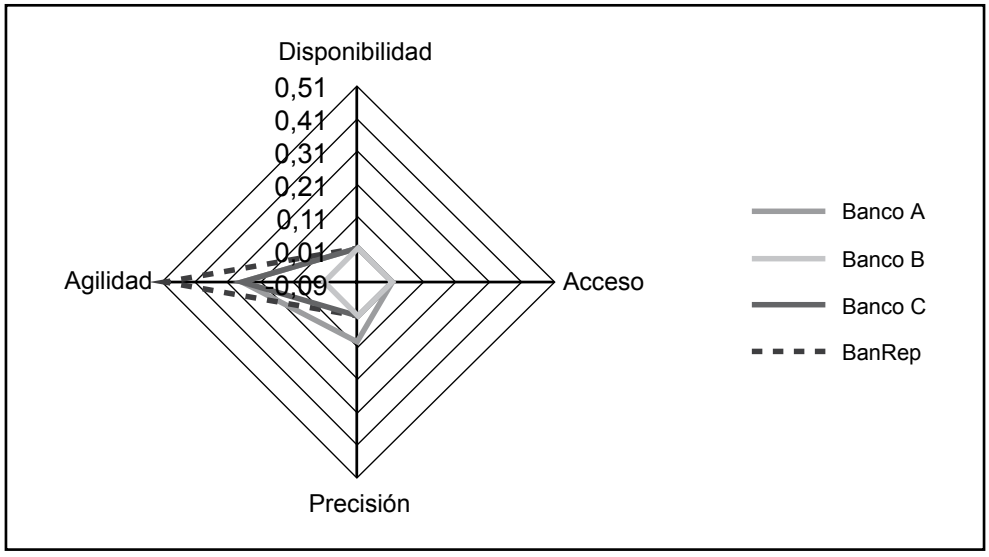

Figura 3: Perfiles Ideales de Riesgo de los Casos de Estudio [1]

Con base en este perfil se concluye que para un mismo proceso, bancos A y C, se puede dar más importancia a un objetivo que otro, de acuerdo con el apetito al riesgo de la organización, siendo estos perfiles la guía para dirigir los esfuerzos.

Comparación de los Perfiles de Riesgo de TI Actuales de los Casos de Estudio

La visión ideal es un camino a seguir, sin embargo, suele diferir de la situación actual. En la Figura 4 se muestran los perfiles de riesgo actuales, que se generaron aplicando un instrumento construido como parte de la investigación [1], en el

cual se clasifican las medidas de cada disciplina del marco 4A y se relacionan con el objetivo de negocio que busca mejorar, calculando el nivel de riesgos de TI que enfrenta cada Banco. Dicho nivel se obtiene al ordenar las medidas de cada objetivo de negocio por niveles de riesgo alto, medio y bajo.

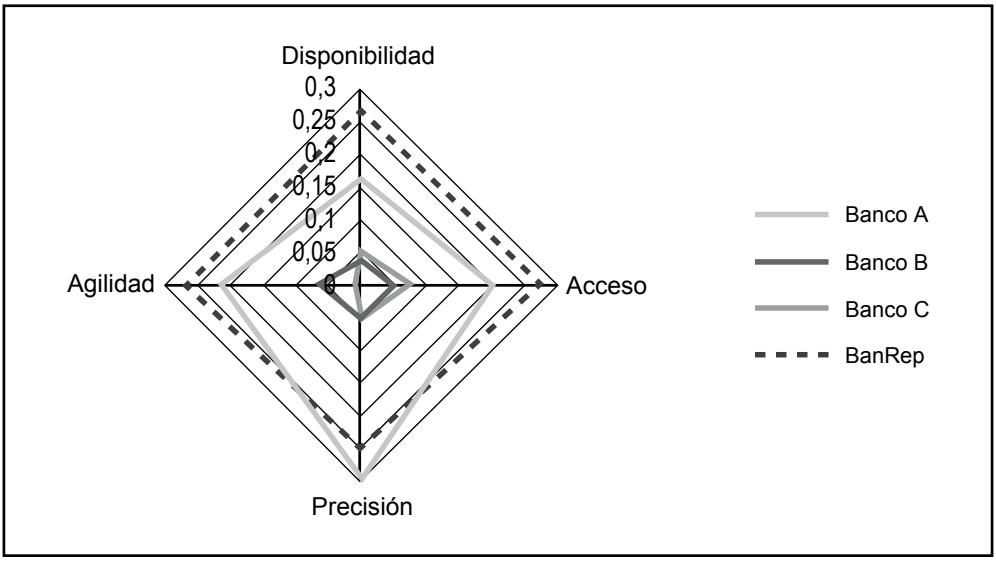

Figura 4: Perfiles Actuales de Riesgo de los casos de Estudio [1]

Al comparar los perfiles de riesgo ideal vs actual [1] se presentan diferencias que no son substanciales, toda vez que los valores están en los mismos rangos. Sin embargo, los bancos deben seguir disminuyendo sus niveles de riesgo de TI de acuerdo con su perfil, para lo cual podrían utilizar un marco como el 4A o guías específicas por sector como la que se encuentra en construcción.

Conclusiones del estudio

En síntesis, para una efectiva gestión de riesgos de TI las empresas, en particular los bancos, no deben conformarse con cumplir únicamente las exigencias que impone la ley.

Este estudio evidencia la necesidad de complementar la reglamentación con buenas prácticas que aporten a la visión transversal de esta gestión organizacional en el largo plazo [1], para que realmente se generen beneficios tanto para los clientes como a nivel interno.

La primera aproximación para lograrlo es comprender la razón de ser de TI dentro de la organización, visión que justamente aporta el marco 4A.

Agradecimientos

Los autores agradecen a Luis Carlos Figueroa por los aportes hechos en este trabajo y por supuesto a los Bancos que participaron, por su tiempo y apoyo.

Referencias

[1] Cheng Andrés, Pinilla Santiago, Villa Juan, Gestión de riesgos de las tecnologías de la información (TI) en el sector bancario colombiano, su implementación a través de la circular 052 de la superintendencia financiera colombiana y su estudio desde el marco de gestión de riesgos de TI 4A, Uniandes, 2009.

[2] Figueroa Luis, "Guía de mejores prácticas en gestión de riesgos de TI en el sector bancario colombiano", documento en desarrollo tesis de maestría en Ingeniería de Sistemas y Computación, uniandes, 2009.

[3] Grant Svetlana, Getting Smarter about IT risks 2008. Disponible en http://mitsloan.mit.edu/cisr/pdf/EIU_GettingSmarterAboutITRisks.pdf

[4] Superintendencia de Servicios Público, Ley 45 de 1990 Diario oficial No 39.607. Disponible en

http://www.superservicios.gov.co/basedoc/docs/leyes/l0045_90.html

[5] Serrano Javier, Mercados financieros: visión del sistema financiero colombiano y de los principales mercados financieros internacionales, ediciones uniandes, 2007.

[6] Superintendencia Financiera de Colombia, Misión de la entidad. Disponible en http://www.superfinanciera.gov.co/

[7] Superintendencia Financiera de Colombia, Circular Externa 052 de 2007: Requerimientos mínimos de seguridad y calidad en el manejo de información a través de medios y canales de distribución de productos y servicios para clientes y

usuarios. Disponible en http://www.superfinanciera.gov.co/NormativaFinanciera/Archivos/ ce052_07.rtf, 2007

[8] Westerman George, Hunter Richard, IT Risk: Turning Business Threats Into Competitive Advantage, HBSP, 2007.

Andrés Cheng C. *Ingeniero de Sistemas y Computación de la Universidad de los Andes.*

Santiago Pinilla M. *Ingeniero de Sistemas y Computación de la Universidad de los Andes cuyos últimos años de su carrera fueron dedicados al estudio de Gestión de TI, Gestión de Continuidad de Servicios de TI y Diseño organizacional con TIC. Así mismo, realizó su proyecto de grado en el primer semestre del 2009 sobre el tema de Riesgos de TI en el sector bancario colombiano.*

Juan David Villa C. *Ingeniero de Sistemas y Computación de la Universidad de los Andes. Estudiante de Maestría en Ingeniería de Sistemas y computación con énfasis en construcción de Software.*

Andrea Herrera S. *Ingeniera de Sistemas y Computación y MsC en Ingeniería de Sistemas y Computación de la Universidad de los Andes. Se desempeñó durante varios años como Ingeniera especializada en Continuidad del Negocio, con énfasis en recuperación tecnológica en el Banco de la República. En la actualidad, es Instructora del Departamento de Ingeniería de Sistemas y Computación de la Universidad de los Andes.*