GUÍA DE AUDITORÍA BASADA EN RIESGOS PARA TECNOLOGIAS DE INFORMACION (TI) EN LA BANCA PÚBLICA

Carlos Xavier Quinga Collaguazo
e-mail: cquinga@hotmail.com

Tannya Alexandra Benalcázar Martínez
e-mail: tannyabenalcazar@hotmail.com

UNIDAD DE POSTGRADOS

UNIVERSIDAD DE LAS FUERZAS ARMADAS

SANGOLQUÍ - ECUADOR

RESUMEN.

El Estado tiene instituciones financieras y/o bancos públicos que disponen y utilizan de tecnologías de información (TI) las cuales soportan las metas y objetivos del negocio. Los organismos de control han emitido requerimientos orientados a establecer y/o fortalecer la gestión de los riesgos y el control interno de las TI. Por ello, la banca pública está obligada a considerar la gestión de riesgos tecnológicos con el fin de precautelar su exposición a algún evento externo que pueda afectar el normal desenvolvimiento del negocio. Es así que se han adoptado normas y políticas tendientes a gestionar el riesgo para minimizar la posibilidad de que estos se produzcan y generen pérdidas económicas, pérdida en la reputación y credibilidad de la organización.

El presente estudio tiene como objetivo desarrollar una guía de auditoría basada en riesgos que permita determinar en la banca pública los riesgos existentes en las tecnologías de información a la que se encuentra expuesta, con el fin de aplicar mecanismos de control interno que permitan tomar medidas preventivas, basados en las normas y resoluciones establecidas por la Contraloría General del Estado y la Superintendencia de Bancos, y utilizando COBIT como marco de referencia de control en TI.

Palabras Clave

Amenazas, Auditoría, COBIT, Tecnología de la Información, Riesgo, Seguridad, Vulnerabilidad.

ABSTRACT.

The Government has financial institutions and/or public banks that make use of IT (Information Technologies) which support milestones and business objectives. Control Agencies have issued a set of requirements aimed at establishing and strengthening IT Risk Management and Internal Control. For that matter, public banking must consider technological risk management activities in order to safeguard its exposure to any external event that could potentially affect its normal functioning. This is why, a body of rules and policies has been adopted to manage risk and minimize to the deepest extent, the possibility of financial , reputation and credibility loss for the organization.

The present paper lays the groundwork for an auditing guide based on risk management , which will help target existing risks for public banking within the context of Information Technologies, so as to be able to apply preventive measures, based on rules and policies established by the General Attorney´s Office and the Banking Authorities, using COBIT as a reference for auditing IT.

Keywords

Threats, Audit, COBIT, Information Technology, Risk, Security, Vulnerability.

1. Introducción

El Estado tiene instituciones financieras y/o bancos públicos que ayudan a enfrentar los problemas económicos en la sociedad, adaptándose a nuevos modelos económicos, sectores y productos específicos para atender las diversas necesidades en el País. La banca pública en Ecuador,[1] en los últimos años, ha evolucionado los sistemas de información adaptándose a los nuevos requerimientos y necesidades del mercado.

Para satisfacer estas necesidades, la banca pública ha tomado conciencia de la importancia de las tecnologías de información (TI) debido a que se han convertido en un elemento imprescindible y en continuo desarrollo que soportan las metas y objetivos del negocio, lo que involucra una alta responsabilidad para sus directivos.

Organismos de control como la Superintendencia de Bancos y Seguros y la Contraloría General del Estado, conscientes de la necesidad de minimizar el impacto de los riesgos, han emitido en los últimos años, requerimientos dirigidos a las entidades financieras, orientados a fortalecer la gestión de los riesgos y el control interno en el ambiente tecnológico. Por ello, la banca pública está obligada a considerar la importancia de la gestión de riesgos con el fin de precautelar su exposición a algún evento externo que pueda llegar a afectar el normal desenvolvimiento de sus actividades, es así que se han adoptado normas y políticas tendientes a gestionar el riesgo para minimizar la posibilidad de que estos se produzcan y generen pérdidas económicas, pérdida en la reputación y credibilidad.

Bajo este esquema, el presente estudio tiene como finalidad desarrollar una guía de auditoría basada en riesgos que permita determinar en la banca pública las debilidades y vulnerabilidades en las tecnologías de información a la que se encuentra expuesta y que se consideren con mayor riesgo, con el propósito de aplicar mecanismos de control interno que permitan tomar medidas preventivas, basados en las normas y resoluciones establecidas por la Contraloría General del Estado y la Superintendencia de Bancos, y utilizando COBIT como marco de referencia de control en TI, para evaluar el cumplimiento de la normativa vigente respecto a la Tecnología de Información.

La guía de auditoría basada en riesgos a más de ser un mecanismo de control interno que permite gestionar de forma adecuada los riesgos tecnológicos ayuda a la banca pública a garantizar la calidad, seguridad, confiabilidad y cumplimiento legal de la información para la toma de decisiones, y pretende contribuir al análisis y aplicación práctica de la actividad de auditoría interna en los procesos de gestión de riesgos tecnológicos.

2. Desarrollo de la Guía de Auditoría

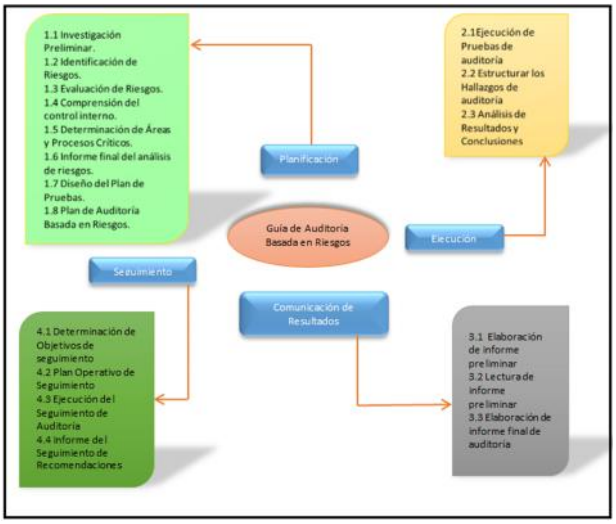
La guía propuesta servirá como referencia al auditor para realizar auditorías basadas en riesgos de TI. Permitirá, entre otros aspectos, identificar los riesgos a los que se encuentra expuesta la entidad, identificar los controles que se encuentran implementados, su eficiencia y el cumplimiento con las regulaciones emitidas por las entidades de control.

El Auditor de TI podrá aplicar los procedimientos necesarios para realizar la auditoría de la entidad sujeta a la evaluación, con el propósito de mejorar la gestión de riesgos tecnológicos, lo que le permitirá emitir las sugerencias y recomendaciones para optimizar o implementar los controles necesarios, con el objetivo de mejorar la eficiencia de su infraestructura y sistemas tecnológicos y lograr un alto grado de integridad, disponibilidad, confidencialidad, confiabilidad de la información, y aseguramiento de la calidad de los sistemas e infraestructura tecnológica, acorde a los estándares y mejores prácticas de TI.

La Guía de auditoría, propuesta en la presente tesis, se ha dividido en las 4 fases:

[1] La Banca pública en Ecuador está conformada por la Corporación Financiera Nacional (CFN), Banco Nacional de Fomento (BNF), Banco de IESS (BIESS), Banco Ecuatoriano de desarrollo (BEDE), Banco Ecuatoriano de la Vivienda (BEV) entre las más destacadas

Cada una de las fases se ha dividido en Actividades y las mismas en tareas, lo que facilitará al auditor realizar el cumplimiento del trabajo, como se indica a continuación:



Fases de la Auditoría Basada en Riesgos de TI en la Banca Pública.

La Auditoría Basada en Riesgos se basa en las siguientes actividades y tareas que el auditor debe considerar el momento de realizar la planificación.

1 Planificación de la Auditoría

- 1.1 Investigación Preliminar.
  - 1.1.1 Comprensión general de la entidad y los aspectos fundamentales.
  - 1.1.2 Comprensión general del área de TI y procesos relacionados.
- 1.2 Identificación de Riesgos.
  - 1.2.1 Identificar y clasificar lo activos.
  - 1.2.2 Identificación de amenazas.
  - 1.2.3 Identificación de vulnerabilidades.
  - 1.2.4 Determinación del Riesgo.
- 1.3 Evaluación de Riesgos.
  - 1.3.1 Evaluación de la Probabilidad.
  - 1.3.2 Evaluación del Impacto.
- 1.4 Comprensión del control interno.
  - 1.4.1 Identificar y Comprender los controles.
  - 1.4.2 Evaluar el control interno.
- 1.5 Determinación de Áreas y Procesos Críticos.
  - 1.5.1 Identificación de Áreas y Procesos Críticos.
- 1.6 Informe final del análisis de riesgos.
  - 1.6.1 Elaboración y aprobación del informe de diagnóstico general.
- 1.7 Diseño del Plan de Pruebas.
  - 1.7.1 Elaboración del Plan de Pruebas.
- 1.8 Plan de Auditoría Basada en Riesgos.
  - 1.8.1 Elaboración del Plan de Auditoría Basada en Riesgos.

2 Ejecución de la Auditoría

2.1 Ejecución de Pruebas de auditoría
- 2.1.1 Ejecución de los procedimientos de auditoría
- 2.1.2 Documentar las pruebas
- 2.1.3 Elaboración/Recopilación de Papeles de trabajo

2.2 Estructurar los Hallazgos de auditoría
- 2.2.1 Estructurar los hallazgos de auditoría

2.3 Análisis de Resultados y Conclusiones
- 2.3.1 Análisis de resultados y conclusiones

3 Resultado de la Auditoría

3.1 Elaboración de informe preliminar
- 3.1.1 Elaboración de informe preliminar

3.2 Lectura de informe preliminar
- 3.2.1 Lectura de informe preliminar

3.3 Elaboración de informe final de auditoría
- 3.3.1 Elaboración de informe final

4 Seguimiento [2]

En esta Fase se efectúan las siguientes actividades

4.1 Determinación de Objetivos de seguimiento
- 4.1.1 Determinación de objetivos de seguimiento

4.2 Plan Operativo de Seguimiento
- 4.2.1 Plan operativo de seguimiento

4.3 Ejecución del Seguimiento de Auditoría
- 4.3.1 Ejecución de seguimiento de auditoria

4.4 Informe del Seguimiento de Recomendaciones
- 4.4.1 Informe de seguimiento.

3. RESULTADOS

Tomando como base las normas establecidas por los organismos de control como son la Superintendencia de Bancos y Seguros y la Contraloría General del Estado, así como también los estándares y mejores prácticas de TI se logró desarrollar la guía para auditoria basada en riesgos para TI en la Banca Pública que brindará a los auditores la oportunidad de contar con un marco de referencia para realizar auditorías basadas en riesgos de TI.

La Guía de auditoría, propuesta en la presente tesis, consta de 4 fases definidas como:

- Planificación
- Ejecución
- Comunicación de Resultados
- Seguimiento

Estas fases se han dividido en Actividades las mismas que contienen el conjunto de tareas que el auditor de TI debe considerar para llevar a cabo el trabajo de auditoría.

El disponer de esta guía se agilitará el tiempo empleado en el desarrollo de la auditoría puesto que el auditor tendrá la posibilidad de seguir estos pasos como actividades básicas a las cuales acorde a sus necesidades podrá ir mejorando o adaptándolo para su uso.

4. CONCLUSIONES

Al finalizar el desarrollo de la presente tesis se ha llegado a las siguientes conclusiones:

- La propuesta de la presente Guía de Auditoría Basada en Riesgos para TI en la Banca Pública le servirá al auditor de TI como un marco de referencia que le facilitará realizar los procesos de auditoría en la Banca Pública, al aplicar cada una de las actividades y tareas que comprenden las fases de la auditoría que se detallan en la guía, con lo que se pretende que las Instituciones financieras reduzcan el nivel del riesgo al que se encuentran o pueden estar expuestos.

- El auditor de TI podrá identificar, analizar y evaluar los riesgos tecnológicos, así como realizar la revisión y la evaluación de los controles existentes en los sistemas, infraestructura y procedimientos de las tecnologías de información, su uso, eficiencia y seguridad, a fin de que por medio de este análisis se pueda dar las recomendaciones necesarias en el mejoramiento o implementación de nuevos controles para lograr la utilización más eficiente y segura de los activos de información de TI que minimicen el riesgo frente a posibles amenazas.

- La presente Guía de Auditoría Basada en Riesgos es aplicable para efectuar auditorías a las tecnologías de información en la banca pública, debido a la creciente transaccionalidad económica, uso de la información en forma electrónica, de procesos automatizados y de comunicación para la prestación de servicios a sus clientes lo que dependerá también del grado de madurez de la entidad en la gestión del riesgo.

- La Guía de Auditoría Basada en Riesgos se encuentra apoyada en las normas y controles establecidos por los organismos de control como es la Superintendencia de Bancos y Seguros y la Contraloría General del Estado lo que ha sido relevante considerar lo expuesto en las normas y/o resoluciones sobre la gestión del riesgo y el control para la elaboración del presente trabajo.

- Las Instituciones financieras en la banca pública han tenido un crecimiento importante en los últimos años lo que hace indispensable y necesario que se realicen auditorías basadas en riesgos a las tecnologías de información para precautelar y garantizar los intereses de sus clientes.

- Para el cumplimiento de normativas, estándares, resoluciones y metodologías enfocados a las auditorias de TI basada en riesgo, diversos organismos de control han realizado importantes esfuerzos, tanto a nivel nacional e internacional que ayudan a la normalización y estandarización y que además permiten a las auditorías internas contar con referentes para sus procesos de auditoría y análisis de riesgos.

- Se evidenció que si bien existen normas, estándares y las mejores prácticas de TI sobre la gestión del riesgo, no existe una guía o metodología específica de auditoría basada en riesgos de TI que dé los lineamientos requeridos de cómo poder llevar a cabo una auditoría con un enfoque basado en riesgos de TI, lo que sí existe son metodologías referentes al análisis de riesgo dentro de una auditoría, tal es el caso de las guías de auditoría de ISACA.

- En el desarrollo de la guía se utilizó las fases de Auditoría Basada en Riesgos que permitirá a cualquier auditor, con el conocimiento en las tecnologías de información, realizar en cualquier institución financiera dentro de la banca pública auditorías basadas en riesgos, logrando realizar el trabajo de manera más rápida al seguir las pautas, conforme lo establecido en la guía.

- Esta propuesta aportará considerables beneficios a la auditoría basada en riesgos de TI en la Banca Pública, como: mayor eficiencia en el trabajo, disponer de un marco de referencia que permita retroalimentar a los auditores y apoyar sus funciones y mejoramiento en los procesos de auditoría basado en riesgos de TI.

5. AGRADECIMIENTOS

Un agradecimiento especial a nuestro Director Ing. Paulo Bermeo Mancero por su guía y dirección para el desarrollo de este trabajo de investigación y de igual manera a nuestro oponente, Eco. Gabriel Chiriboga Barrera, quien mediante sus observaciones logró llevar a término la presente tesis.

6. REFERENCIAS

[1] Auditoría Informática, un enfoque práctico, Mario G. Piattinni, 2da Edición.

[2] Seguimientos en auditoria, Documento técnico No. 26, www.auditoriainternadegobierno.cl/index.php/menu/ShowFile/id/21

[3] Guía de Técnicas, MAGERIT