GUIA DE AUDITORIA BASADA EN RIESGOS PARA TECNOLOGIA DE INFORMACIÓN (TI) EN LA BANCA PÚBLICA

Maestría en Evaluación y Auditoría de Sistemas Tecnológicos

Integrantes:

Tannya Benalcázar Martínez

Carlos Quinga Collaguazo

Tutor:

Ing. Paulo Bermeo

AGENDA

1. Introducción
2. Objetivos
3. Marco Teórico
4. Auditoria Basada en Riesgos
5. Guía de Auditoría Basada en Riesgos
6. Conclusiones
7. Recomendaciones

Introducción

- La presente tesis pretende ser un referente para el desarrollo de auditorías a nivel de Sistemas Tecnológicos dentro del segmento de la Banca y específicamente para la Banca Publica, lo que permitirá mantener un ambiente de control definido con normas, políticas y procedimientos que garanticen calidad, confiabilidad y seguridad de la información.

- Ha cobrado gran importancia dentro de las organizaciones las tecnologías de información puesto que soportan las metas y objetivos del negocio.

- Ante la necesidad de minimizar el impacto provocado por los riesgos y para mitigarlos y a la vez dar cumplimiento a las disposiciones legales, es necesario disponer de una guía para el desarrollo de la auditoria de TI basada en Riesgos

Objetivos

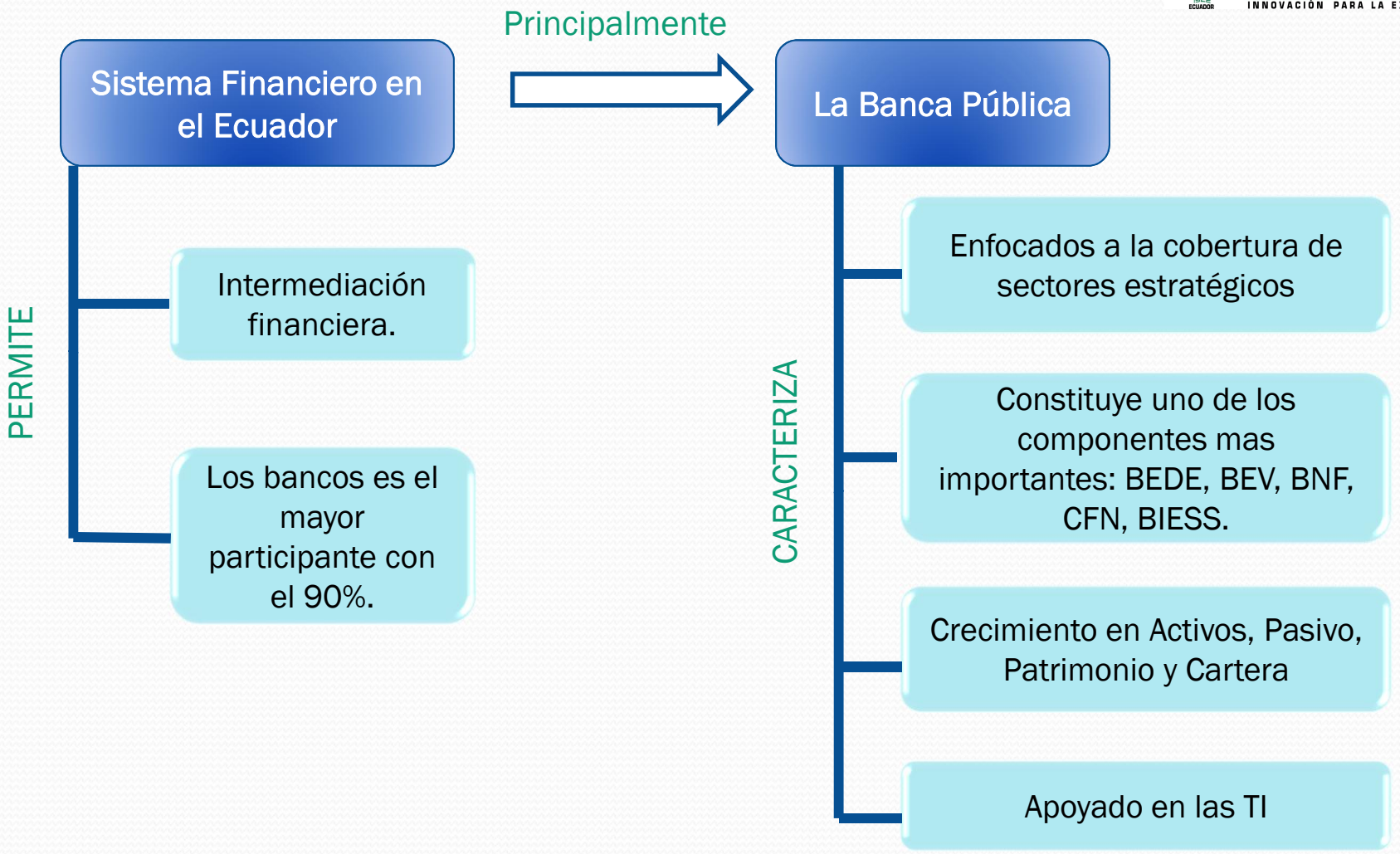
GENERAL

Desarrollar un marco de referencia que contribuya al área de auditoría interna y que sirva de apoyo para la realización de auditorías basada en riesgos tecnológicos en la banca pública.
.

ESPECÍFICOS

- Facilitar a la auditoría interna el dirigir, supervisar y revisar los procesos relacionados con las tecnologías de información a auditar.
- Mejorar los procesos de auditoría interna.
- Permitir evidenciar el grado de cumplimiento regulatorio sobre las tecnologías de información basada en las normas definidas por organismos de control.
- Ayudará a crear procedimientos de auditorías alineados con los estándares y mejores prácticas de TI para la administración de riesgo y control .

Marco Teórico

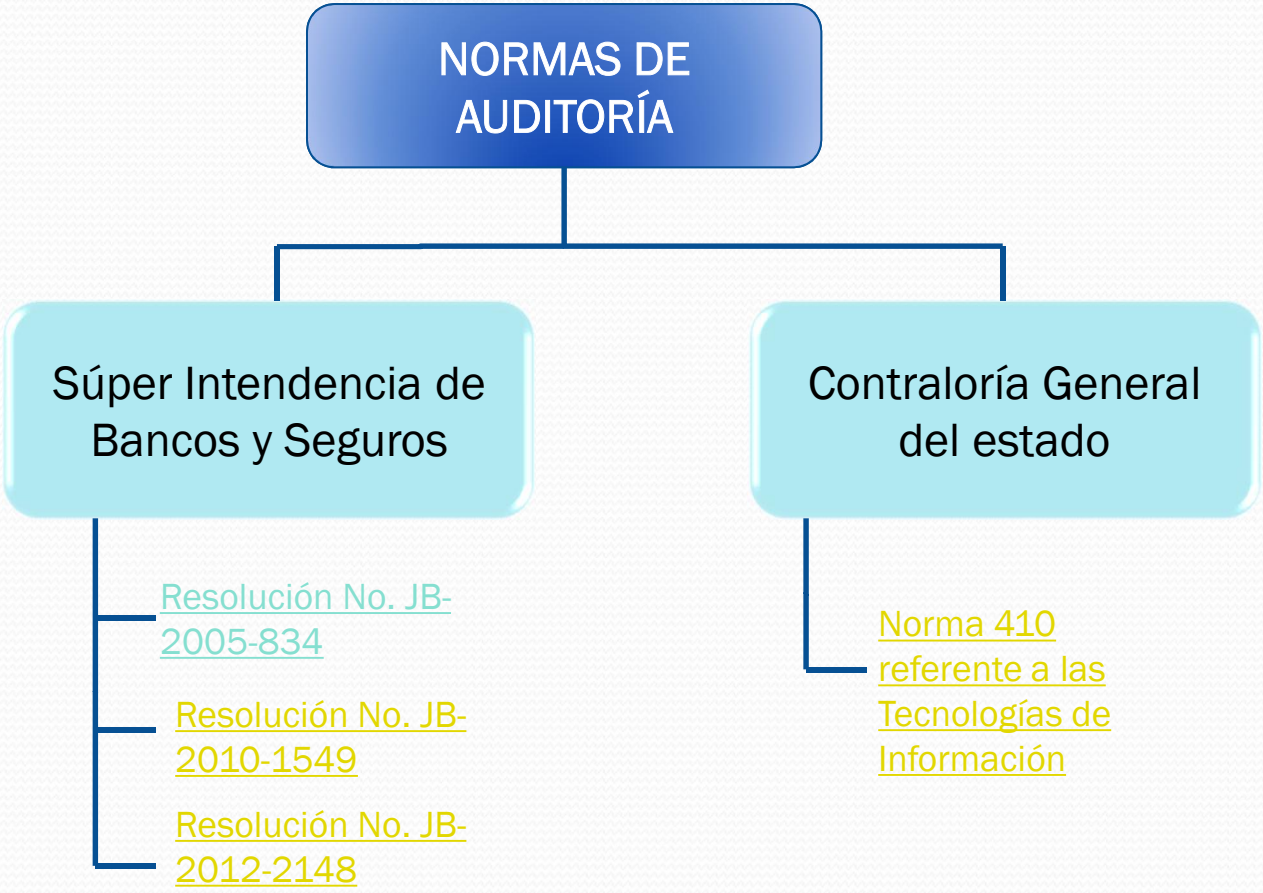


Crecimiento de La Banca Pública

A través de la innovación de las TI se ha logrado el mejoramiento en las operaciones y servicios que ofrecen.

- Indispensable disponga de mecanismos de control que permita identificar y mitigar los riesgos tecnológicos a los que puede estar expuesta.
  - Medidas de Seguridad
  - Procesos de Auditoría
- Cumplimiento regulatorio establecido por los organismos de control referentes a riesgos en las tecnologías de información, SBS y Contraloría General del Estado.

Las Normas de Auditoría Generales



Métodos de Gestión y Evaluación de Riesgos

Método	Descripción	Fases
MAGERIT	Metodología de Análisis y Gestión de Riesgos de TI	• Planificación • Análisis • Gestión • Salvaguardas
ISO 27005	Information Security Risk Management	• Valoración • Tratamiento • Aceptación • Comunicación • Monitoreo
RISK IT	Risk IT Management	• Gobierno • Evaluación • Respuesta

Control

Método	Descripción	Fases
COBIT 4.1	Gobierno TI	4 dominios 34 procesos 210 Objetivos de control
COBIT 5.0	Gobierno TI Empresarial	5 dominios 37 procesos (5 Obj. Control riesgos, 2 procesos para SI)
COSO	Manejo integrado de control	1. Ambiente de control 2. Evaluación de riesgos 3. Actividades de control 4. Información y comunicación 5. Supervisión y seguimiento del sistema de control.

Auditoría Basada en Riesgos de TI

La ABR de TI consiste en un conjunto de procesos mediante los cuales la auditoria provee aseguramiento independiente al directorio o al organismo acerca de:

- Los procesos y medidas de gestión del riesgo que se encuentran implementadas y están funcionando de acuerdo a lo esperado.
- Los procesos de gestión de riesgos son apropiados y están bien diseñados.
- Las medidas de control de riesgos implementado son adecuadas y efectivas.

Dependen del nivel de desarrollo que la propia institución del sistema financiero ha alcanzado en la gestión de riesgos en el área objeto de examen.

Se resume en cuatro fases: Planificación Basada en Riesgos, Ejecución, Comunicación de Resultados y Seguimiento.

1.- Planeación

- Realizar previamente la planificación de la auditoría, que le permita tener un entendimiento general del área a auditar.
  - Procesos del Negocio
  - Función que realiza
  - Marco Regulatorio
  - Sistemas de Información
- Comprender e identificar los procesos del negocio y de mayor riesgo soportados por las tecnologías de información.
- Comprender e identificar los controles existentes.
- Determinar las área o procesos Críticos.
- Identificar los procedimientos de auditoría a realizarse en la ejecución, quién y cuándo deben ejecutar y las tareas a desarrollar para que se cumplan en forma eficiente y efectiva.

1.- Planeación

Fases de la Planeación de ABR

Para realizar una adecuada planeación de la auditoría basada en riesgos el auditor de TI debe seguir una serie de pasos previos, que permitan dimensionar el tamaño y características del área de la entidad a ser auditada:

- Comprensión de Objetivos y procesos de negocio relacionados
- Identificación de Riesgos de TI
- Evaluación del Riesgo de TI
- Análisis de Riesgos
- Revisión de los controles relacionados con TI

1.- Planeación

Plan de ABR de TI

Actividades de Auditoría	Descripción de la Actividad
Diagnóstico General	Descripción y fines de la entidad.
Objetivo de la Auditoría	Origen de ser de la auditoría.
Alcance Auditoría	Extensión del trabajo a realizar.
Documentación Aplicable	Manuales, normas y normativa legal.
Identificación del equipo de Auditoría	Incluye el equipo de auditores.
Costo y cronograma de actividades	Define el costo y el cronograma.
Fecha de realización y Horario	Tiempo de ejecución de la auditoría
Áreas y Procesos críticos a Auditar	Asuntos más importantes identificados en la fase de planeación
Plan de Pruebas	Pruebas que se ejecutarán

2.- Ejecución

- Objetivos
  - Obtener y analizar toda la información posible del proceso que se audita
  - Obtener evidencias suficientes, adecuadas e importantes que permitan al auditor establecer conclusiones fundadas en el informe acerca de las situaciones analizadas en sitio

2.- Ejecución

- El nivel efectivo de exposición al riesgo;
- Las causas que lo originan;
- Los efectos o impactos que se podrían ocasionar al materializarse un riesgo y,
- En base a estos análisis, generar y fundamentar las recomendaciones que debería acoger los Directivos.

3.- Resultado

Como resultado de la auditoría, se debe presentar un informe por escrito, que debe contener los resultados, observaciones, conclusiones y comentarios. Este debe contener el objetivo, alcance y resultados del procedimiento de auditoría efectuados:

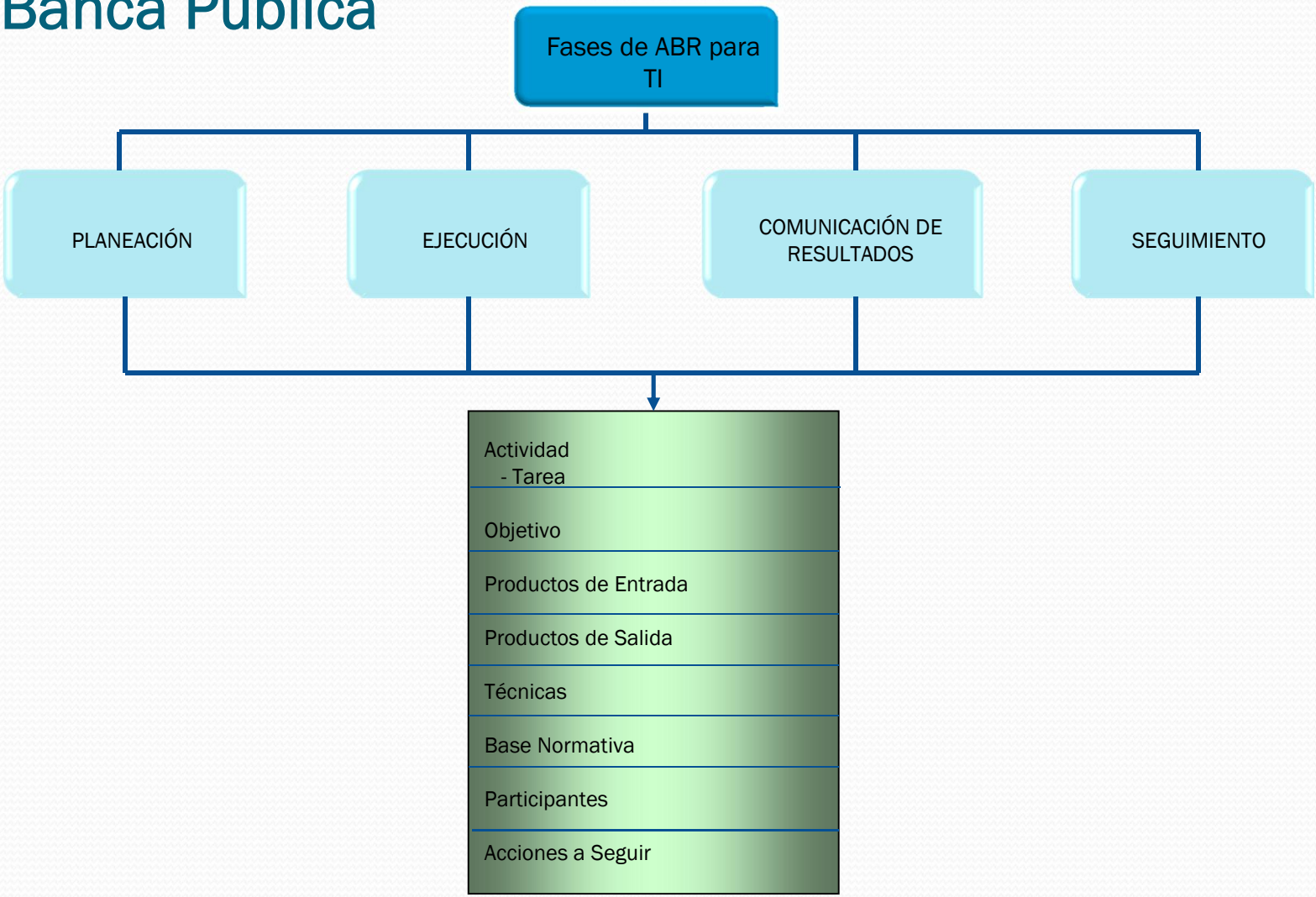
Esta Fase consta de las siguientes actividades:

1. Elaboración de informe preliminar
2. Comunicación de informe preliminar
3. Elaboración de informe final de auditoría

4.- Seguimiento

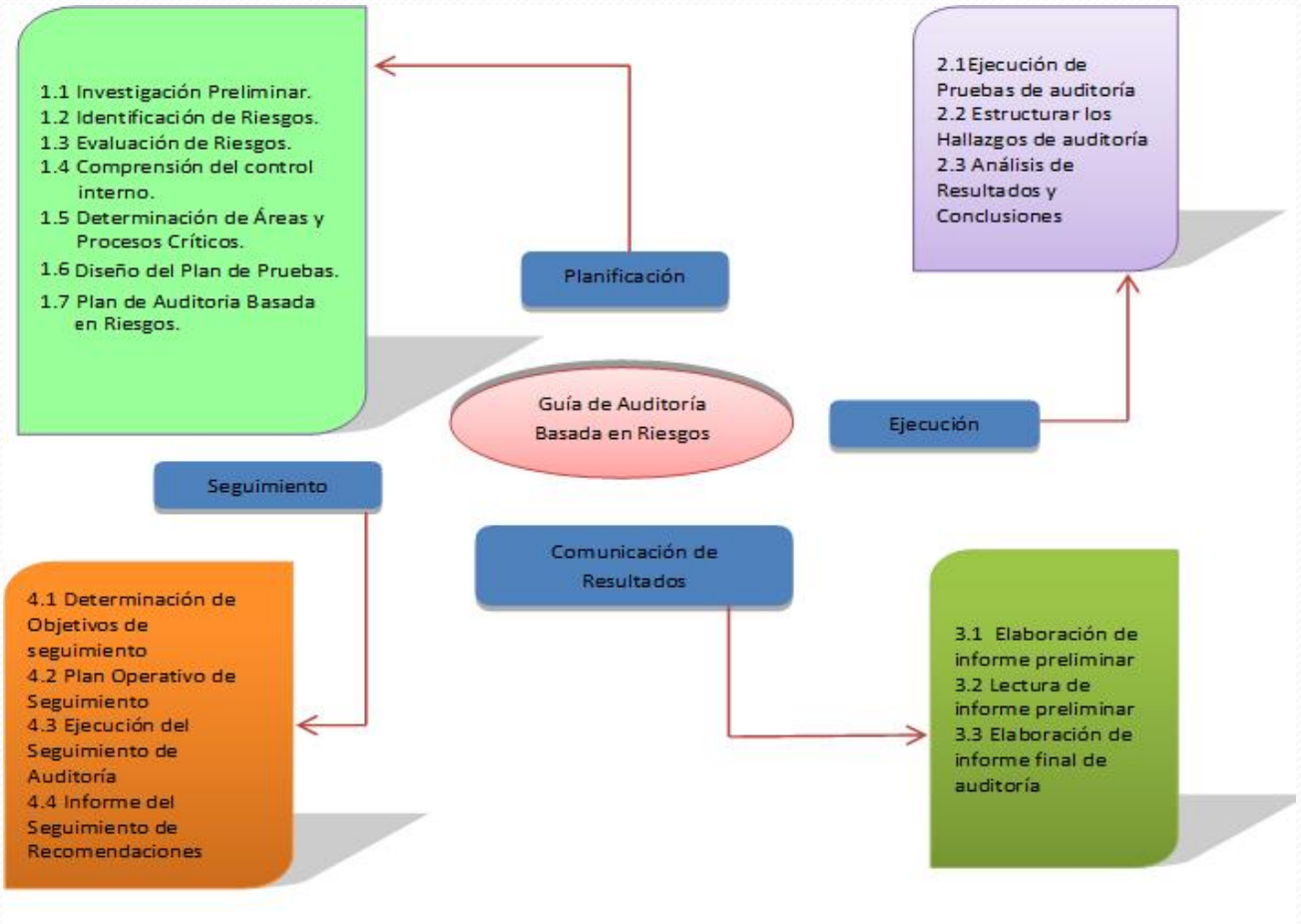
1. Determinación de Objetivos de seguimiento
2. Plan Operativo de Seguimiento
3. Ejecución del Seguimiento de Auditoría
4. Informe del Seguimiento de Recomendaciones

Desarrollo de la Guía de ABR para TI en la Banca Pública



Guía de Auditoría

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



Fase 1 Planeación Individual

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.

Fase 1 Planeación Individual

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.

Fase 1 Planeación Individual

1.5 Determinación de Áreas y Procesos Críticos.

1.5.1 Identificación de Áreas y Procesos Críticos.

1.6 Diseño del Plan de Pruebas.

1.6.1 Elaboración del Plan de Pruebas.

1.7 Plan de Auditoría Basada en Riesgos.

1.7.1 Elaboración del Plan de Auditoría Basada en Riesgos.

FASE 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

FASE 2: Ejecución de la Auditoría

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

FASE 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

FASE 4: Seguimiento

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 auditoría

4.4 Informe del Seguimiento de Recomendaciones

4.4.1 Informe de seguimiento

Conclusiones

- Servirá al auditor de TI como un marco de referencia que le facilitará, el dirigir, supervisar y revisar los procesos relacionados con las tecnologías de información a auditar en la Banca pública.
- Identificar, analizar y evaluar los riesgos tecnológicos a los que puede encontrarse expuesto la institución financiera, así como realizar la revisión y la evaluación de los controles existentes.
- 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 y en los estándares y mejores prácticas de TI.

Conclusiones

- Se ha podido evidenciar que si bien existen normas, estándares y las mejores prácticas de TI sobre la gestión del riesgo, no hay una guía o metodología específica de auditoría basada en riesgos de TI .
- Aportará considerables beneficios a la auditoría basada en riesgos de TI en la Banca Pública, como son: mayor eficiencia en el trabajo, contar con un marco de referencia que pueda retroalimentar a los auditores y apoyar sus funciones y mejoramiento en los procesos de ABR de TI.

Recomendaciones

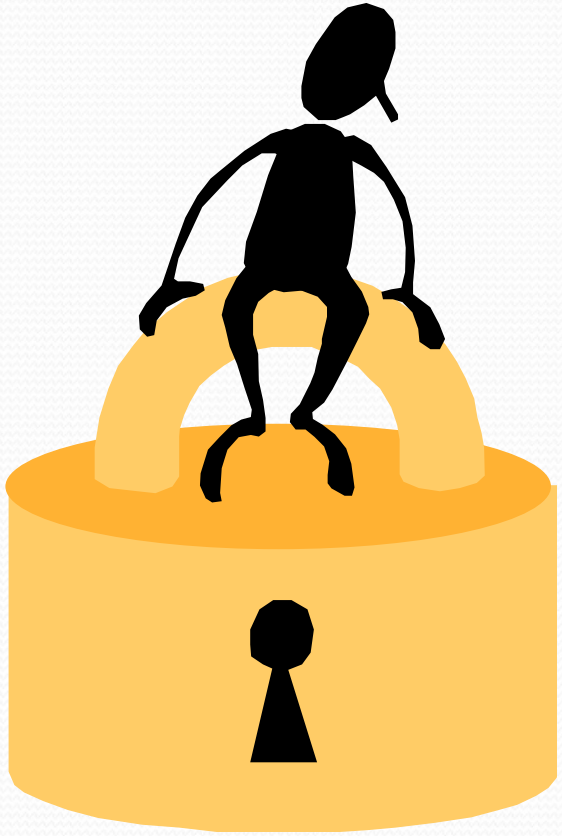
- Se sugiere a los auditores internos de la banca pública promover en realizar auditorías de TI basada en riesgos, bajo el enfoque de aplicación de los estándares y mejores prácticas de TI para la gestión de riesgo y control interno, con el objeto de priorizar las auditorías en aquellos procesos de mayor riesgo tecnológico.
-
- Se recomienda a los auditores internos considerar como parte del proceso de auditorías en la banca pública la guía propuesta, esto les ayudará a desempeñar las funciones de auditoría con un enfoque ordenado y simplificado que les permitirá mejorar la eficiencia de los proceso de gestión de riesgos de TI y control interno en la entidad a auditar.

Recomendaciones

- Finalmente se sugiere que los auditores tomen conciencia de la importancia que tiene el realizar auditorías en la banca pública basada en riesgos tecnológicos, debido a que hoy en día las tecnologías de información se han convertido en el soporte fundamental en el que manejan las operaciones, por lo que es necesario garantizar la disponibilidad, confiabilidad e integridad de la información así como su infraestructura tecnológica.

Anexos

- Formularios



GRACIAS POR SU ATENCIÓN