



# ESPE

**UNIVERSIDAD DE LAS FUERZAS ARMADAS**  
**INNOVACIÓN PARA LA EXCELENCIA**

**VICERRECTORADO DE INVESTIGACIÓN Y VINCULACIÓN CON  
LA COLECTIVIDAD**

**MAESTRÍA EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS  
TECNOLÓGICOS**

**PROMOCIÓN I**

**TESIS DE GRADO**

**“GUÍA DE AUDITORÍA BASADA EN RIESGOS PARA  
TECNOLOGÍAS DE INFORMACIÓN (TI) EN LA BANCA PÚBLICA”**

**AUTORES:**

**BENALCÁZAR MARTÍNEZ, TANNYA ALEXANDRA**

**QUINGA COLLAGUAZO, CARLOS XAVIER**

**DIRECTOR:**

**ING. BERMEO MANCERO, PAULO**

**SANGOLQUÍ, JUNIO DE 2014**

## CERTIFICACIÓN

Se certifica que el trabajo titulado “**GUÍA DE AUDITORÍA BASADA EN RIESGOS PARA TECNOLOGÍAS DE INFORMACIÓN (TI) EN LA BANCA PÚBLICA**”, fue desarrollado en su totalidad por los Ing(s). Tannya Alexandra Benalcázar Martínez y Carlos Xavier Quinga Collaguazo, investigación que ha sido dirigida bajo nuestra supervisión, orientando sus conocimientos y competencias para un eficiente desarrollo del tema y cumple normas estatutarias establecidas por la ESPE, en el Reglamento de Estudiantes de la Universidad de las Fuerzas Armadas ESPE.

Sangolquí, Junio de 2014

---

Ing. Paulo Bermeo M.

**DIRECTOR DE TESIS**

---

Eco. Gabriel Chiriboga

**OPONENTE DE TESIS**

## **DECLARACIÓN DE RESPONSABILIDAD**

**Nosotros:** Ing. Carlos Quinga C.  
Ing. Tannya Benalcázar M.

### **DECLARAMOS QUE:**

El proyecto de Grado denominado “**GUÍA DE AUDITORÍA BASADA EN RIESGOS PARA TECNOLOGÍAS DE INFORMACIÓN (TI) EN LA BANCA PÚBLICA**”, ha sido desarrollado con base a una investigación exhaustiva, respetando derechos intelectuales de terceros, cuyas fuentes se incorporan en la bibliografía. Consecuentemente este trabajo es de nuestra autoría.

En virtud de esta declaración, nos responsabilizamos del contenido, veracidad y alcance científico del proyecto de grado en mención.

Sangolquí, Junio del 2014

---

---

## AUTORIZACION DE PUBLICACION

**Nosotros:** Ing. Carlos Quinga C.

Ing. Tannya Benalcázar M.

Autorizamos a la Universidad de las Fuerzas Armadas ESPE, la publicación en la biblioteca virtual de la Institución, del trabajo denominado **“GUÍA DE AUDITORÍA BASADA EN RIESGOS PARA TECNOLOGÍAS DE INFORMACIÓN (TI) EN LA BANCA PÚBLICA”**, cuyo contenido, ideas y criterios son de nuestra exclusiva responsabilidad y autoría.

Sangolquí, Junio del 2014

---

---

## *Dedicatoria*

Con todo mi cariño y mi amor a mis padres, por ser el modelo a seguir, dándome ejemplos dignos de superación y entrega, por impulsarme siempre a seguir adelante, por su amor, cariño paciencia y comprensión. Gracias por haber fomentado en mí el deseo de superación y el anhelo de triunfo en la vida.

A mis hermanos, sobrinos y abuela, por todo el cariño y apoyo brindado y en especial a mi hermana por su apoyo incondicional, comprensión y consejos brindados en todo momento.

*Tannya Benalcázar*

Con infinito amor y agradecimiento este trabajo es dedicado a mis Padres Carlos y Rosita, a quienes debo todo lo que soy, por su apoyo incondicional durante toda mi vida.

Con mucho amor y cariño a mi esposa Mayra y a mis hijos Carlos Andrés, David Alejandro y Sebastián Ariel por su apoyo y sacrificio, privándonos de muchos tiempo juntos, porque supieron comprender el esfuerzo y tiempo que dediqué a la consecución de este grado.

*Carlos Xavier*

## *Agradecimiento*

A Dios, por darme la sabiduría y fuerzas para seguir cada día y haber culminado esta etapa académica. A mis padres, hermanos sobrinos y abuela que constituyen un motivo valioso por el cual me he esforzado y he alcanzado mis objetivos y metas.

Le agradezco también de manera especial a nuestro Director de Tesis Ing. Paulo Bermeo que con sus valiosos conocimientos nos permitió culminar con el desarrollo de esta investigación.

*Tannya Benalcázar*

A Dios, por haberme dado salud y vida para lograr culminar este proceso.

A toda mi familia, mis padres, hermanos, sobrinos que de una u otra manera apoyaron mi esfuerzo

Al Director de Tesis, Ing. Paulo Bermeo, por su valioso aporte en la dirección para la consecución de esta tesis.

*Carlos Xavier*

## CONTENIDO

Guía de Auditoría Basada en Riesgos para TI en la Banca Pública.....	1
1.1 Justificación e Importancia.....	3
1.2 Planteamiento del problema .....	4
1.3 Objetivo General .....	5
1.4 Objetivos Específicos.....	6
2 CAPITULO II.....	7
2.1 Marco Teórico.....	7
2.1.1 El Sistema Financiero en el Ecuador.....	7
2.1.1.1 Inicios de la Banca Pública.....	7
2.1.1.2 Análisis de la Banca Pública con Otras Instituciones Financieras. ....	8
2.1.1.3 Las Tecnologías de Información y la Banca Pública.....	12
2.1.2 Las Normas de Auditoría Generales .....	13
2.1.2.1 Normas de Auditoría Establecidos por los Organismos de Control. ....	13
2.1.2.2 Métodos de Gestión y Evaluación de Riesgos.....	15
2.1.2.2.1 Marco de Gestión de Riesgos de IT (MAGERIT) .....	15
2.1.2.2.2 ISO/IEC 27005 Sistema de Gestión de Riesgos .....	30
2.1.2.2.3 RISK IT (ISACA, 2009).....	41
2.1.2.2.4 COBIT (ISACA, 2007).....	45
2.1.2.2.5 COSO-ERM (COSO, 2004).....	58
3 CAPITULO III.....	63
3.1 Auditoría Basada en Riesgos de TI.....	63
3.1.1 Auditoría Basada en Riesgos .....	63
3.1.2 Fundamentos de la Auditoría Basada en Riesgos en la Banca.....	66
3.1.3 Aplicación de la Auditoría Basada en Riesgos .....	67
3.2 Fases de una Auditoría Basada en Riesgos de TI.....	68
3.2.1 Planeación de la Auditoría Basada en Riesgos de TI.....	69
3.2.1.1 Actividades de la Fases de la Planeación de ABR de TI.....	70
3.2.1.2 Comprensión de Objetivos y procesos de negocio relacionados.....	71
3.2.1.3 Análisis de riesgo .....	72
3.2.1.4 Efecto de las Leyes y Regulaciones sobre la planificación de ABR .....	73
3.2.1.5 Llevar a cabo a revisión de los controles internos relacionados con TI .....	75

3.2.1.6	Definición del Plan de Auditoría Basada en Riesgos de TI.....	76
3.2.2	Ejecución de la ABR de TI .....	77
3.2.2.1	Planificación de la Ejecución de la Auditoría.....	78
3.2.2.2	Actividades de ejecución de la Auditoría .....	78
3.2.3	Comunicación de los resultados de la ABR de TI .....	83
4	CAPITULO IV .....	86
	Desarrollo de la Guía de Auditoría Basada en Riesgos para TI en la Banca Pública. ....	86
1	FASE 1: Planificación Individual .....	87
1.1	Investigación Preliminar .....	89
1.1.1	Comprensión general de la entidad y los aspectos fundamentales.....	89
1.1.2	Comprensión general del área de TI y procesos relacionados .....	90
1.2	Identificación de Riesgos .....	93
1.2.1	Identificar y clasificar lo activos .....	93
1.2.2	Identificación de amenazas. ....	95
1.2.3	Identificación de vulnerabilidades .....	96
1.2.4	Determinación del Riesgo.....	98
1.3	Evaluación de Riesgos .....	100
1.3.1	Evaluación de la Probabilidad.....	100
1.3.2	Evaluación del Impacto.....	101
1.4	Comprensión del control interno.....	103
1.4.1	Identificar y Comprender los controles.....	103
1.4.2	Evaluar el control interno.....	104
1.5	Determinación de Áreas y Procesos Críticos .....	106
1.5.1	Identificación de Áreas y Procesos Críticos.....	106
1.6	Diseño del Plan de Pruebas .....	107
1.6.1	Elaboración del Plan de Pruebas .....	107
1.7	Plan de Auditoría Basada en Riesgos.....	108
1.7.1	Elaboración del Plan de Auditoría Basada en Riesgos .....	108
2	FASE 2: Ejecución de la Auditoría.....	110
2.1	Ejecución de Pruebas de auditoría .....	111
2.1.1	Ejecución de los procedimientos de auditoría.....	111
2.1.2	Documentación de las pruebas.....	113
2.1.3	Elaboración/Recopilación de Papeles de trabajo .....	114



2.2 Estructurar los Hallazgos de auditoría.....	116
2.3 Análisis de Resultados y Conclusiones .....	118
3 FASE 3: Resultado de la Auditoría.....	120
3.1 Elaboración de informe preliminar .....	120
3.2 Lectura de informe preliminar.....	122
3.3 Elaboración de informe final de auditoría.....	123
4 FASE 4: Seguimiento (Consejo de Auditoría Interna General de Gobierno, 2008).....	125
4.1 Determinación de Objetivos de seguimiento.....	125
4.2 Plan Operativo de Seguimiento.....	126
4.3 Ejecución del Seguimiento de Auditoría.....	128
4.4 Informe del Seguimiento de Recomendaciones .....	129
5 CAPITULO V .....	131
5.1 CONCLUSIONES Y RECOMENDACIONES.....	131
6 Bibliografía .....	136
ANEXOS .....	139
ANEXO No. 1 .Resolución No. JB-2005-834 de 20 de octubre del 2005.....	139
ANEXO No. 2. Resolución No. JB-2012-2148 de 26 de abril del 2012 .....	167
ANEXO No. 3. Resolución No. JB-2010-1549 del 21 de Enero de 2010 .....	180
ANEXO No. 4. Directrices de ISACA para Auditoría de TI.....	186
ANEXO No. 5. Normas 410 de Control Interno para TI.....	193
ANEXO No. 6. Formulario de Reuniones de Trabajo.....	199
ANEXO No. 7. Formulario de Encuesta.....	200
ANEXO No. 8. Formulario de Observación.....	201
ANEXO No. 9. Formulario de Normativas. ....	202
ANEXO No. 11. Información del Área de TI.....	204
ANEXO No. 12. Activos de Información.....	205
ANEXO No. 13. Matriz de Riesgos.....	206
ANEXO No. 14. Matriz de Evaluación de Riesgos .....	207
ANEXO No. 15. Matriz de identificación de Controles Existentes.....	209
ANEXO No. 16. Matriz de Priorización de Controles.....	211
ANEXO No. 17. Formulario de Plan de Pruebas. ....	213
ANEXO No. 18. Modelo Plan de Auditoría Basada en Riesgos. ....	214
ANEXO No. 19. Registro de ejecución de los procedimientos de auditoría .....	216

ANEXO No. 20. Documentación Registro de las pruebas .....	217
ANEXO No. 21. Papeles de Trabajo .....	218
ANEXO No. 22. Informe de Auditoría.....	219

## Índice de Figuras

Figura No. 1. Comparación de Activos de las Instituciones Financieras.....	9
Figura No. 2. Comparación de Pasivos de las Instituciones Financieras.....	9
Figura No. 3. Comparación de Patrimonio de las Instituciones Financieras .....	10
Figura No. 4. Crecimiento de la Banca Pública frente a la Banca Privada.....	11
Figura No. 5. Elementos de análisis de riesgo potenciales. ....	18
Figura No. 6. El riesgo en función del impacto y la probabilidad. ....	20
Figura No. 7. Acciones a tomar luego del análisis de riesgos.....	26
Figura No. 8. Principios Básicos de COBIT .....	47
Figura No. 9. Dominios de COBIT.....	49
Figura No. 10. Representación gráfica de los modelos de madurez. ....	54
Figura No. 11. Componentes de Control .....	59
Figura No. 12. Fases de la Auditoría Basada en Riesgos de TI en la Banca Pública. ....	87

## Índice de Tablas

Tabla No. 1. Tabla de variación de la Cartera Crediticia.....	10
---	----

## Índice de Cuadros

Cuadro No. 1. Escala Cualitativa de valores.....	19
Cuadro No. 2. Tipo de Controles .....	21
Cuadro No. 3. Criterios de Control de COBIT .....	47
Cuadro No. 4. Resumen de recursos de TI identificados en COBIT. ....	48
Cuadro No. 5. Proceso Evaluar y Administrar los Riesgos de TI.....	55
Cuadro No. 6. Etapas de la Auditoría Basada en Riesgos de TI.....	68

Cuadro No. 7. Actividades de Planificación de Auditoría .....	76
Cuadro No. 8. Formato de Informe de auditoría.....	84

## 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**

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

## **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**

Audit, COBIT, Information Technology, Risk, Security

## **CAPITULO I**

### **Guía de Auditoría Basada en Riesgos para TI en la Banca Pública**

En un inicio los bancos privados dominaban el ámbito financiero del país, porque de sus créditos dependían otros sectores de la economía, siendo el Estado uno de los grandes deudores de los bancos privados.

El Estado inicia la creación de las instituciones financieras o bancos públicos para enfrentar los problemas que podían generarse en la sociedad o realidad económica, adaptándose a nuevos modelos económicos, sectores y productos específicos para atender las diversas necesidades en el País.

Es así que la banca pública en el Ecuador en los últimos años ha evolucionado de manera importante, y con ello sus sistemas de información se han ido adaptando a los nuevos requerimientos y necesidades del mercado, los que permiten dar el soporte a los procesos del negocio convirtiéndose 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, los mismos que requieren tener certeza de que la información crítica sobre la que sustentan sus decisiones es confiable, segura y está disponible cuando se necesita.

En tal virtud, 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, por ello 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 igual forma, 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.

Bajo este esquema, este 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, para evaluar el cumplimiento de la normativa vigente respecto a la Tecnología de Información, y utilizando estándares y mejores prácticas de TI que se consideró para el presente estudio.

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 ayudando a la banca pública a garantizar la calidad, seguridad, confiabilidad y cumplimiento legal de la información para la toma de decisiones, también pretende contribuir al análisis y aplicación práctica de la actividad de auditoría interna en los procesos de gestión de riesgos tecnológicos.

Esta guía pretende establecer un marco de referencia basado en la gestión del riesgo que sirva de guía para los auditores y Gerentes de TI con la finalidad de que

puedan gestionar manera adecuada los riesgos tecnológicos que se puedan presentar, considerando que se trata de precautelar los intereses financieros de la sociedad.

### **1.1 Justificación e Importancia**

La gestión de riesgos tecnológicos se ha convertido en un tema de gran preocupación e importancia en la banca pública, ya que actualmente constituye la base fundamental para la identificación, análisis, evaluación y tratamiento de riesgos, lo que ha permitido la implementación de un ambiente de control interno bien definido con normas y procedimientos que garanticen calidad, confiabilidad y seguridad de la información.

Es así que el área de Auditoría Interna, entre sus funciones, tiene a cargo determinar el grado de cumplimiento de normas y políticas orientadas a la gestión del riesgo tecnológico y verificar que existan los controles necesarios que garanticen los niveles de servicio que la TI puedan ofrecer, ante lo cual es necesario que realicen auditorías periódicas enfocadas a la gestión de la TI que permitan determinar los riesgos tecnológicos a los que está expuesta.

Para esto, la auditoría interna necesita contar con normas, políticas y procedimientos que les permita evaluar los riesgos tecnológicos a los que se enfrentan y eventualmente poder alertar a la misma, y emitir de ser necesario, recomendaciones sobre los controles requeridos que ayuden en la prevención y detección de riesgos para asegurar una adecuada toma de decisiones.

Por otro lado, deben contar con el personal técnico especializado y conocer sobre las técnicas y métodos para realizar las auditorías basadas en riesgos tecnológicos.



Los aspectos que han sido indicados, forman el conjunto de razones que conllevan al desarrollo del presente estudio con la finalidad de contar con una guía de auditoría de TI basada en riesgos, como marco de referencia para la auditoría en la banca pública.

El presente proyecto está dirigido al área de auditoría interna en la banca pública que no posea una guía de referencia apropiada a seguir para la ejecución de auditorías basada en riesgos de TI que contribuya a fortalecer la gestión tecnológica de la banca pública, y a la auditoría interna al ser un marco referencial que simplifica y mejora los procesos de auditoría.

## **1.2 Planteamiento del problema**

Actualmente las TI's se han convertido en un habilitador importante dentro de cualquier Institución Financiera, incluyendo a la banca pública, el contribuir al cumplimiento de los objetivos y metas planteadas por la organización, pero al mismo tiempo su inadecuada gestión, como puede ser el no contar con normas y procedimientos bien definidos o tener insuficientes controles internos de TI, pueden generar riesgos tecnológicos, que si no son gestionados adecuadamente y a tiempo, podrían impactar las operaciones del negocio, al afectar al cumplimiento de los objetivos y metas de la institución.

No obstante es donde la auditoría interna tiene gran importancia debido a que son los encargados de identificar además el nivel de exposición al riesgo a los que se enfrentan la institución en el desarrollo de sus actividades y operaciones diarias. Por lo tanto es relevante que realicen una adecuada planeación de la auditoría de TI basadas en riesgos mediante una serie de pasos previos con un conocimiento general

razonable que permita determinar el tamaño y alcance del área a auditar, sus sistemas y procesos.

Es así que al no poseer el área de auditoría interna una guía apropiada a seguir para el desarrollo de auditorías basada en riesgos de TI o al no disponer del conocimiento técnico requerido, los auditores no tendrán la capacidad suficiente para realizar una auditoría de los procesos tecnológicos de TI. Es por ello que un escenario negativo pondría en riesgo la continuidad del servicio, lo que traería como consecuencia directa la afectación de los objetivos institucionales planteados.

Para esto, las áreas de Auditoría Interna y de Sistemas deben cumplir las recomendaciones emitidas por los organismos de control como son la Superintendencia de Bancos y Seguros del Ecuador y la Contraloría General del Estado, los cuales establecen que el plan anual de la auditoría debe realizarse con un enfoque "basado en valoración de riesgos".

Por otro lado, resulta imprescindible que las auditorías internas, tanto de la banca privada como de la banca pública, tomen conciencia de la importancia que tiene la auditoría basada en riesgos, pues permite garantizar el cumplimiento de políticas, normas y estándares así como también la aplicación de controles al ayudar a prevenir posibles riesgos o a minimizar el impacto en caso de ocurrir, brindando mejoras medibles, eficientes y efectivas de los procesos relacionados con la institución.

### **1.3 Objetivo General**

Crear un marco de referencia que contribuya al área de auditoría interna mediante la elaboración de una Guía de Auditoría basada en Riesgos para TI que permita realizar auditorías en la banca pública.

#### **1.4 Objetivos Específicos**

- Desarrollar una guía de auditoría basada en riesgos de TI que facilite a la auditoría interna de la banca pública el dirigir, supervisar y revisar los procesos relacionados con las tecnologías de información a auditar.
- Desarrollar una guía de auditoría basada en riesgos de TI que contribuya a mejorar los procesos de auditoría interna de TI, identificar los riesgos y controles que se deben implementar.
- Desarrollar procedimientos basados en riesgos tecnológicos que permitan evidenciar el grado de cumplimiento regulatorio sobre las tecnologías de información, requeridas para la administración del riesgo, basada en normas de control y auditoría definidas por la Contraloría General del Estado y la Superintendencia de Bancos y Seguros.
- Desarrollar una guía que sirva de apoyo para el desarrollo de las auditorías basadas en riesgos de TI, alineados con los estándares y mejores prácticas de TI para la gestión de riesgo y control interno.

## **2 CAPITULO II**

### **2.1 Marco Teórico**

#### **2.1.1 El Sistema Financiero en el Ecuador**

Actualmente el Sistema Financiero se caracteriza por ser la encargada de la intermediación financiera crediticia entre los clientes y la entidad, quienes captan los depósitos y por otro prestan a los demandantes de recursos, constituyéndose así los bancos en el mayor y más importante participante del mercado con más del 90% de las operaciones del total del sistema financiero.

De acuerdo a la estructura de la Ley General de Instituciones del Sistema Financiero, entre uno de sus componentes más importantes se encuentra la banca pública.

##### **2.1.1.1 Inicios de la Banca Pública**

A inicios del siglo XX los bancos privados dominaban el ámbito financiero del país, dado que eran los encargados de la emisión monetaria y porque de sus créditos dependían otros sectores de la economía, siendo el Estado uno de los grandes deudores de los bancos privados.

Bajo este contexto el Estado inicia la creación de las instituciones financieras o bancos públicos para enfrentar los problemas que podían llegar a generarse en la sociedad o realidad económica, y que serían modificadas a lo largo de los años, adaptándose a nuevos modelos económicos, sectores y productos específicos para atender las diversas necesidades que se presentaban en el País.

Es así que hoy en día los bancos públicos en el Ecuador están enfocados a la cobertura de sectores estratégicos como el productivo, infraestructura, pequeños y micro empresarios, entre otros, apoyados principalmente por las tecnologías de información e infraestructura tecnológica.

En la actualidad la Banca Pública está constituido por 5 entidades financieras:

- Banco del Estado (BEDE)
- Banco Ecuatoriano de la Vivienda (BEV)
- Banco Nacional de Fomento (BNF)
- Corporación Financiera Nacional (CFN)
- Banco del Instituto Ecuatoriano de Seguridad Social (BIESS)

No incluye al Instituto de Crédito Educativo y Becas (IECE), institución dedicada exclusivamente a la colocación de cartera hacia la educación.

#### **2.1.1.2 Análisis de la Banca Pública con Otras Instituciones Financieras.**

De acuerdo a los datos financieros publicados a través del sitio web de la Superintendencia de Bancos y Seguros (SBS) hasta el mes de diciembre de 2012, la banca pública del país tuvo un crecimiento en sus principales componentes como activos, pasivos, patrimonio, cartera y depósitos de los clientes mostrando niveles significativos de participación e inyectando grandes cantidades de dinero en los diferentes sectores de la economía ecuatoriana.

Al comparar la banca pública con otras Instituciones Financieras como los Bancos Privados, Mutualistas y Cooperativas, según la SBS, la participación de activos de la

Banca Pública (Figura No.1) ha ido en aumento llegando al 16%, para los Bancos Privados del 72%, para las Mutualistas del 1% y para las Cooperativas el 11%.

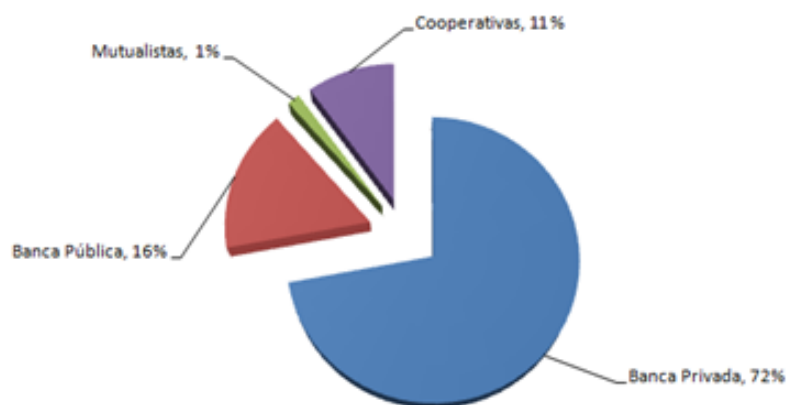


Figura No. 1. Comparación de Activos de las Instituciones Financieras

Mientras que en los pasivos (Figura No.2), se evidencia que los porcentajes de participación en la Banca Pública es del 13%, de la Banca Privada el 75%, de las Cooperativas el 10% y de las Mutualistas el 2%, lo que indica que los porcentajes en banca pública han ido aumentando.

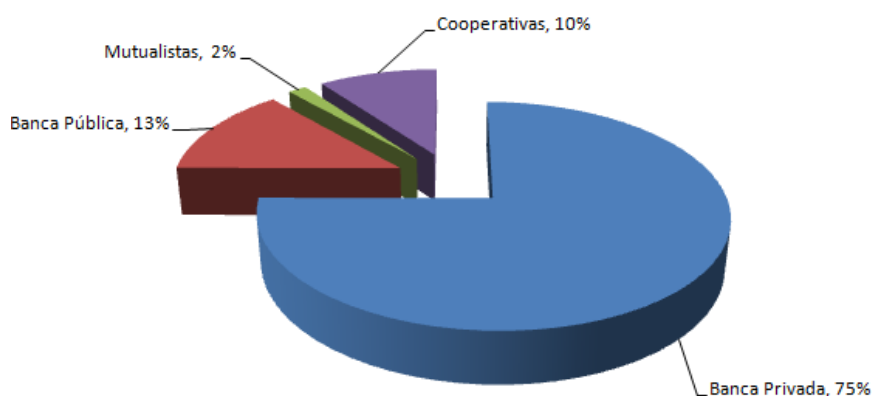


Figura No. 2. Comparación de Pasivos de las Instituciones Financieras

En lo que respecta al Patrimonio (Figura No.3) los porcentajes de participación de la banca pública es del 35%, de la banca privada del 53%, las mutualistas del 1% y las cooperativas del 11%. Así, la banca pública es el segundo sector financiero en crecimiento de Patrimonio después de la banca privada.

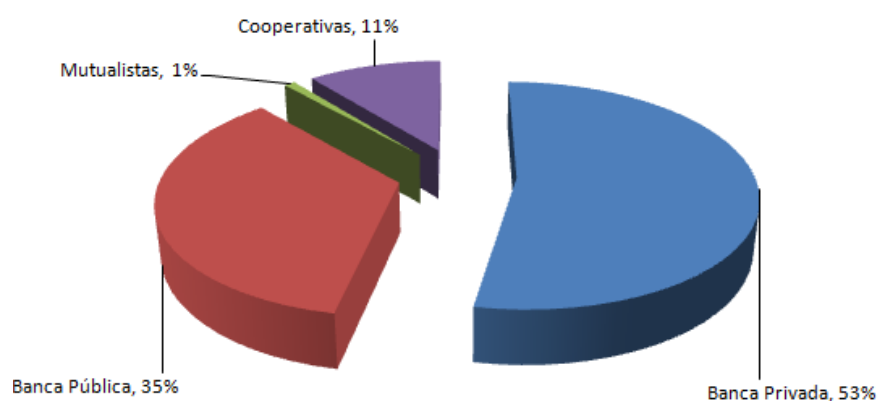


Figura No. 3. Comparación de Patrimonio de las Instituciones Financieras

En cuanto a la evolución de la cartera crediticia únicamente entre la banca pública y la banca privada en los últimos seis años se puede observar las variaciones crediticias, según la Tabla No. 1.

Tabla No. 1. Tabla de variación de la Cartera Crediticia

<b>CRECIMIENTO DE LA CARTERA CREDITICIA</b>		
<b>Período</b>	<b>Banca Pública</b>	<b>Banca Privada</b>
2007-2008	28%	56%
2008-2009	-3%	42%
2009-2010	21%	33%
2010-2011	20%	8%
2011-2012	14%	8%

Pese a que el porcentaje de crecimiento de la cartera crediticia en los dos últimos años no ha sido significativo, se puede decir que su crecimiento ha sido más rápido que la banca privada (Figura No.4).

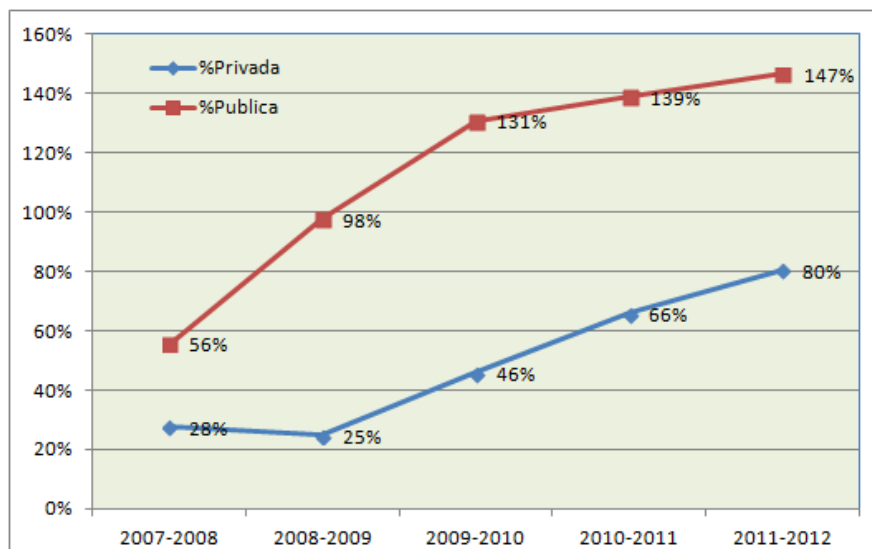


Figura No. 4. Crecimiento de la Banca Pública frente a la Banca Privada

Con el análisis realizado se puede decir que las instituciones que tienen mayor participación en el sistema financiero son los bancos, considerándose a la banca pública como unos de los sectores financieros más fuertes, debido a su participación y crecimiento en el desarrollo social, económico y financiero del país.

Cabe destacar que el crecimiento de la banca pública en activos, pasivos, patrimonio y cartera crediticia se ha logrado también por el gran aporte de las tecnologías de información, lo que ha permitido aumentar la confianza de los clientes debido a su estabilidad financiera.

Por lo antes mencionado, es indispensable que la banca pública disponga de mecanismos de control que permita identificar y mitigar los riesgos tecnológicos a los que puede estar expuesta a través de la implementación de medidas de seguridad



y procesos de auditoría que permitan evidenciar el estado en que se encuentran las tecnologías de información, así como el cumplimiento regulatorio establecido por los organismos de control referentes a riesgos en las tecnologías de información.

### **2.1.1.3 Las Tecnologías de Información y la Banca Pública**

Con el crecimiento de la banca pública, las TI han cobrado más importancia, puesto que aportan al cumplimiento de los objetivos institucionales al ofrecer sus servicios de forma efectiva y eficiente, lo que les ha permitido competir con éxito en el mercado financiero.

A través de la innovación de las TI en la banca pública se ha logrado el mejoramiento en las operaciones y servicios que ofrecen, tales como créditos, transacciones en línea, cajeros automáticos, banca móvil, cuentas corrientes y de ahorros, entre otros; por lo que es necesario garantizar la fiabilidad de sus operaciones a través del manejo adecuado de la información y las tecnologías que lo soportan considerando una adecuada gestión del riesgo.

En este sentido, la banca pública se encuentra sujeta al control y regulación de la Superintendencia de Bancos y Seguros y de la Contraloría General del Estado las mismas que realizan evaluaciones y revisiones especiales también a las tecnologías de información. Dichas entidades cuentan con leyes, reglamentos, resoluciones y normativas para el cumplimiento regulatorio en las TI.

## **2.1.2 Las Normas de Auditoría Generales**

### **2.1.2.1 Normas de Auditoría Establecidos por los Organismos de Control.**

Entre las normas de auditoría interna establecidas por la Superintendencia de Bancos y Seguros, se emitió el 20 de octubre del 2005 la Resolución No. JB-2005-834 (Ver anexo No.1) que modifica la norma sobre Gestión de Riesgo Operativo en donde indica una serie de disposiciones que obligan a las instituciones del sistema financiero a establecer los lineamientos que deben cumplir para garantizar la continuidad del negocio ocasionado por fallas o insuficiencia de procesos, personas, tecnologías de información y eventos externos, complementada posteriormente con la Resolución No. JB-2012-2148 de 26 de abril del 2012 (Ver anexo No. 2) sobre seguridad en canales electrónicos, cajeros automáticos, Puntos de venta (POS y PIN Pad), Banca Electrónica y Banca Móvil, entre otros.

Además las normas de auditoría indican que una de las funciones del auditor es también realizar Auditorías Basadas en Riesgos, las cuales se enuncia en la Resolución No. JB-2010-1549 del 21 de Enero de 2010 (Ver anexo No. 3).

Entre las directrices que establece la Superintendencia de Bancos y Seguros en lo que se refiere a Auditoría Basada en Riesgos, las instituciones financieras serán auditadas dependiendo del grado de madurez alcanzado por la Institución respecto a la gestión del riesgo, es decir que si el área objeto a ser auditada cuenta con un adecuado sistema de gestión de riesgos, la auditoría basada en riesgos puede confiar en su evaluación de riesgos que la propia institución ha realizado siempre y cuando esté acorde a las necesidades de la auditoría a efectuarse, caso contrario la auditoría deberá desarrollar su propio método de evaluación de riesgos.

Además la norma dispone que la unidad de auditoría interna de la institución financiera cuente con un auditor de sistemas, que tenga el conocimiento y expertise necesarios para el cumplimiento de sus funciones, el mismo que debe estar encaminado al cumplimiento de los objetivos de la organización.

En este sentido la norma indica que como función del auditor interno, referente a las tecnologías de información, está el evaluar los recursos informáticos y sistemas de información con el objetivo de:

- Evidenciar si son adecuados para proporcionar información oportuna y suficiente para la toma de decisiones
- Identificar la exposición al riesgo
- Verificar que cuente con medidas de seguridad

Para las actividades de las auditorías internas en las Instituciones del Sistema Financiero se aplicarán lo mencionado en el artículo 20 de la Resolución JB-2010-1549 (Ver anexo No. 3) que establece que:

“En lo que no se opongan a lo previsto en la normativa de la Superintendencia de Bancos y Seguros será de aplicación las normas internacionales para el Ejercicio Profesional de la Auditoría Interna, así como del Código de Ética emitidos por The Institute of Internal Auditors (IIA).

En el caso de los auditores de sistemas, se tomarán en consideración las directrices de auditoría previstas por el Information Systems Audit and Control Association (ISACA)”, que se detallan en el anexo No. 4.

Por otro lado, la Contraloría General del Estado, con el propósito de asegurar la correcta y eficiente administración de los recursos y bienes de las entidades y organismos del sector público, el 14 de diciembre del 2009 bajo Registro Oficial No.87 emitió, las Normas de Control Interno para las Entidades, Organismos del Sector Público y Personas Jurídicas de Derecho Privado que dispongan de Recursos Públicos, que contiene la Norma 410 referente a las Tecnologías de Información (Ver anexo No. 5), las mismas que deben cumplir las entidades sujetas al control, referente a políticas, procedimientos, planes estratégicos, infraestructura, seguridades, planes de contingencia, mantenimiento de las aplicaciones, soporte, entre otras.

### **2.1.2.2 Métodos de Gestión y Evaluación de Riesgos**

#### **2.1.2.2.1 Marco de Gestión de Riesgos de IT (MAGERIT)**

(Ministerio de Hacienda y Administraciones Públicas, 2012)

MAGERIT es una metodología de Análisis y Gestión de Riesgos de los Sistemas de Información que implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno decidan, considerando el riesgo en el uso de tecnologías de información para lograr los objetivos institucionales los cuales deben ser gestionados de manera adecuada con medidas de seguridad que sustenten la confianza de los usuarios en los servicios prestados.

MAGERIT es de interés para quienes trabajan con información digital y sistemas de información y cuya información sea crítica, permite valorar el riesgo al que están expuestos es esencial para poder gestionarlos.

MAGERIT persigue los siguientes objetivos:

- Concienciar a los responsables de la información de la existencia de riesgos y la necesidad de gestionarlos.
- Ofrecer un método sistemático para analizar los riesgos que impliquen el uso de las TI.
- Identificar los riesgos y planificar el tratamiento oportuno para mantener estos bajo control.
- Preparar a la organización para afrontar procesos de evaluación, auditoría, certificación o acreditación.

#### **2.1.2.2.1.1 Análisis y Gestión de Riesgos**

El análisis y el tratamiento del riesgo son parte de la actividad continua de la Gestión de Seguridad y son necesarias cuando una organización dispone de sistemas de información y comunicaciones que permitirá tomar decisiones de gestión y asignar recursos con perspectiva, sean estas tecnológicas, humanas o financieras.

El análisis de riesgos permite determinar cómo es, cuánto vale y cuán protegido se encuentra un sistema de información. Proporciona un modelo en términos de activos, amenazas y controles, y es el fundamento para controlar las actividades.

Efectuar un análisis de riesgos requiere de mucho trabajo, coordinación y es muy costoso, debe ser justificada y planificada. Generar un mapa de activos y su valoración requiere de la colaboración de muchos perfiles, desde los técnicos hasta la Gerencia. Implica uniformizar el criterio de todos los participantes para llegar a un consenso. Como puede existir una gran cantidad de datos, la forma de afrontar esta complejidad es concentrarse en las más importantes (máximo impacto, máximo riesgo) y omitir lo que no es importante.

MAGERIT considera dos grandes tareas a realizar:

- a) **Análisis del riesgo** que permite determinar lo que la organización dispone y estimar lo que podría suceder
- b) **Tratamiento del Riesgo** que permite organizar las acciones de defensa contra algún incidente que podría suceder y seguir operando en las mejores condiciones, asumiendo un nivel residual.

El Análisis de Riesgo considera:

- Los activos o elementos de los sistemas de información,
- Las amenazas o lo que podría sucederles a los activos y
- Los controles que son las medidas dispuestas para mitigar los daños.

Con estos elementos definidos se puede estimar el impacto de lo que podría suceder, y el riesgo de lo que podría ocasionar.

#### **2.1.2.2.1.1 Método de Análisis de Riesgo**

El análisis de riesgos para determinar el nivel de riesgo efectúa los siguientes pasos:

1. Identificar los activos críticos para la institución, su interrelación y su valor, suponiendo el costo que tendría su degradación.
2. Identificar las amenazas a la que están expuestos estos activos
3. Determinar los controles dispuestos y el nivel de efectividad frente al riesgo
4. Estimar el impacto como consecuencia de la materialización de la amenaza
5. Estimar el riesgo, que es el impacto que ocasionaría de acuerdo a la frecuencia de ocurrencia de la amenaza.

La figura No.5 muestra la relación existente entre los activos, amenazas, riesgo e impacto que intervienen para el análisis de riesgo.

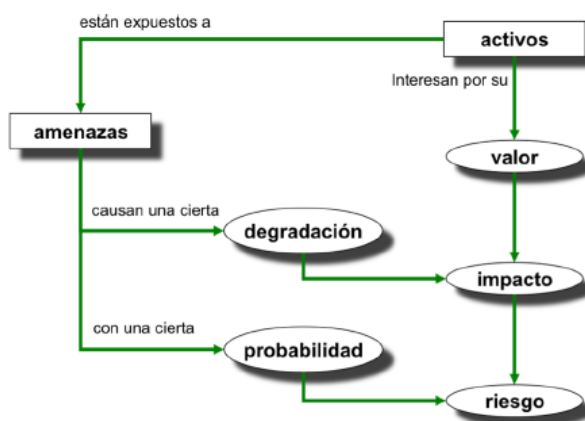


Figura No. 5. Elementos de análisis de riesgo potenciales.  
(Ministerio de Hacienda y Administraciones Públicas, 2012)

#### 2.1.2.2.1.1.1.1 Activos

Los activos esenciales son la información que maneja y los servicios que presta y estos dependen de otros activos incluidos las personas. Un activo interesa por lo que vale, no por lo que cuesta y la valoración se ve desde la perspectiva de la necesidad de proteger, pues mientras más valioso es un activo, mayor nivel de protección se requerirá para este activo.

#### 2.1.2.2.1.1.1.2 Amenazas

Cada activo puede estar sujeto a diversas amenazas y estas pueden ser de tipo: natural, del entorno (de origen industrial), defecto de las aplicaciones, causadas por personas de forma accidental, causadas por personas de forma deliberada.

Cuando el activo es víctima de una amenaza, no se afecta en toda su dimensión, ni en la misma cuantía, entonces hay que valorar su influencia en el valor del activo respecto a la:

- *Degradación*: cuán perjudicado resultaría el valor del activo, es decir, mide el daño causado por un incidente en el supuesto de que ocurriera, y
- *Probabilidad*: cuán probable o improbable es que se materialice la amenaza, es decir, la ocurrencia, y es más difícil de determinar y expresar, por lo que se lo hace cualitativamente a través de una escala nominal como la expresada:

Cuadro No. 1. Escala Cualitativa de valores

<b>MA</b>	Muy alta	Casi seguro	Fácil
<b>A</b>	Alta	Muy alto	Medio
<b>M</b>	Media	Posible	Difícil
<b>B</b>	Baja	Poco probable	Muy difícil
<b>MB</b>	Muy baja	Muy raro	Extremadamente difícil

**a) Determinación del Impacto Potencial**

Conociendo el valor de los activos y la degradación que ocasionan las amenazas se puede determinar el impacto que tendrían estas sobre el sistema.

Se debe considerar además la dependencia entre activos, puesto que las amenazas suelen estar presentes en todos los activos.

**b) Determinación del Riesgo Potencial**

Una vez conocido el impacto de las amenazas sobre los activos, se puede determinar el riesgo considerando únicamente la probabilidad de ocurrencia. El riesgo depende directamente del impacto y la probabilidad, pudiendo distinguir zonas a considerar para el tratamiento del riesgo (Figura No. 6):

*Zona 1*: Riesgos con alta probabilidad y alto impacto



*Zona 2:* Franja amarilla, cubre un amplio rango desde situaciones improbables y de impacto medio

*Zona 3:* Riesgos improbables y de bajo impacto

*Zona 4:* Riesgos improbables pero de muy alto impacto

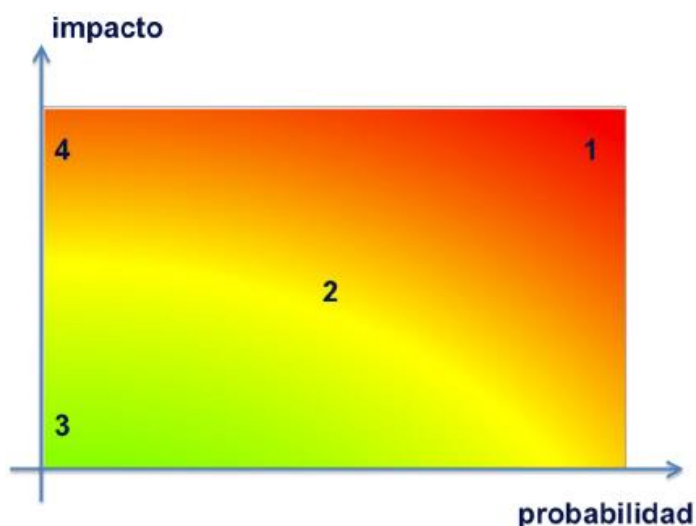


Figura No. 6. El riesgo en función del impacto y la probabilidad.

(Ministerio de Hacienda y Administraciones Públicas, 2012)

#### 2.1.2.2.1.1.1.3 Controles

Pueden existir amenazas que se controlan simplemente con la organización dentro de la institución, otras que requieren elementos técnicos, otras con seguridad física, y otras con políticas.

Ante la cantidad de controles que pueden existir se deben hacer una selección de las más relevantes considerando los siguientes aspectos:

1. Tipo de activos a proteger
2. Dimensión de seguridad que requiere protección
3. Amenazas de las que se necesitan proteger
4. Si existen controles alternativos.

Además, se debe establecer un principio de proporcionalidad y tener en cuenta:

1. El mayor o menor valor propio o acumulado de un activo, tomando únicamente los más valiosos.
2. La mayor o menor probabilidad de que una amenaza ocurra, considerando los riesgos más importantes.
3. La cobertura de riesgo que proporcionan los controles alternativos.

Todo esto conlleva a excluir ciertos controles de todo el conjunto y analizar si no aplica cuando su aplicación no es técnicamente adecuada al tipo de activos que se van a proteger o no se justifica cuando aplica pero es desproporcionada respecto al riesgo que tenemos que proteger.

El efecto de los controles se nota cuando:

- Reducen la probabilidad de las amenazas, o
- Reducen el daño ocasionado

El cuadro de abajo indica el efecto de los tipos de protección que se pueden aplicar.

#### Cuadro No. 2. Tipo de Controles

(Ministerio de Hacienda y Administraciones Públicas, 2012)

<b>EFEECTO</b>	<b>TIPO</b>
Preventivas	Preventivas Disuasorias Eliminatorias
Reducir la degradación	Minimizadoras Correctivas De recuperación
Consolidan el efecto de las demás	De monitorización De detección De concienciación Administrativas

**a) Eficacia de la protección**

Los controles están caracterizados por su eficacia frente al riesgo que pretenden proteger. Los controles son eficaces cuando combina el punto de vista técnico y el de operación de los controles.

Desde el punto de vista técnico:

- Es técnicamente adecuado para enfrentar el riesgo que protege
- Se emplea siempre

Desde el punto de vista de operación

- está perfectamente desplegada, configurada y mantenida
- existen procedimientos explícitos de uso normal y en caso de incidencias
- los usuarios están formados y concienciados
- existen controles que notifican de posibles fallos

**2.1.2.2.1.1.1.4 Impacto Residual**

Una vez aplicados los controles, el sistema queda en una situación de posible impacto denominado impacto residual, es decir se ha modificado el impacto desde un valor potencial a un valor residual.

Para calcular el impacto residual, como no ha cambiado el valor de los activos, sino únicamente la magnitud de la degradación, se debe repetir los cálculos con el nuevo nivel de degradación.

#### *2.1.2.2.1.1.1.5 Riesgo Residual*

Con el conjunto de controles desplegados, el sistema queda en una situación de riesgo que se denomina riesgo residual, es decir, se ha modificado el riesgo desde un valor potencial a un valor residual.

Para calcular el riesgo residual, como no ha cambiado el valor de los activos, sino únicamente la magnitud de la degradación y la probabilidad de las amenazas, se debe repetir los cálculos con el impacto residual y la probabilidad residual de ocurrencia.

La magnitud de la degradación se toma en consideración en el cálculo del impacto residual. La magnitud de la probabilidad residual tomando en cuenta la eficacia de los controles.

#### **2.1.2.2.1.1.2 Formalización de las actividades**

Este conjunto de actividades persigue:

- Realizar un modelo de valor del sistema, identificando y valorando los activos relevantes.
- Efectuar un mapa de riesgos del sistema que identifique y valore las amenazas sobre los activos relevantes.
- Efectuar el reconocimiento de la situación actual de los controles
- Evaluar el impacto sobre el sistema tanto potencial como residual
- Evaluar el riesgo sobre el sistema tanto potencial como residual
- Notificar a las áreas de mayor impacto y/o riesgo a fin de que puedan tomar las decisiones adecuadas para su tratamiento.

El análisis de riesgos se debe efectuar mediante el desarrollo de las siguientes tareas:

*Determinación de los activos.*- Identificar los activos relevantes en el sistema a analizar por tipo de activo, relaciones entre ellos determinando las dimensiones de seguridad que son importantes y valorando esta importancia.

*Determinación de las amenazas.*- Identificar las amenazas relevantes del sistema por probabilidad y daño que podría ocasionar. Aquí se obtiene el mapa de riesgos.

*Determinación de los controles.*- Identificar los controles existentes utilizados en el sistema a analizar de acuerdo a la eficacia frente a las amenazas que se desean mitigar.

*Estimación del estado de riesgo.*- Procesar todos los datos recopilados de las actividades previas para estimar el impacto y riesgo; y determinar deficiencias y debilidades en el sistema de controles.

#### **2.1.2.2.1.1.3 Documentación**

Permite mantener documentada todas las actividades realizadas y sus resultados, que pueden ser entrevistas, estadísticas, observaciones de expertos y analistas, información existente a utilizar, documentación auxiliar, Informes y evaluaciones anteriores.

En la documentación debe incluir el modelo de valor, mapa de riesgos, evaluación de controles, declaración de aplicabilidad, informe de insuficiencias o vulnerabilidades, estado del riesgo.

#### 2.1.2.2.1.1.4 Proceso de Gestión de Riesgos

Cuando se han determinado los impactos y los riesgos a los que está expuesto el sistema, se deben decidir sobre las acciones a tomar en base a diversos factores como:

- La gravedad del impacto y/o riesgo
- La legislación a la que está obligada a cumplir la organización.
- Los reglamentos a cumplir por parte de la organización

Y estas acciones llevan a otorgar una calificación de riesgo en la que puede ser:

1. *Critico*.- cuando requiere atención urgente
2. *Grave*.- cuando requiere atención
3. *Considerable*.- que puede ser analizado para darle un tratamiento
4. *Aceptable*.- no se toman acciones y se acepta como tal. Para ello se considera si el riesgo o impacto residual es asumible, el costo de los controles es mucho mayor respecto al impacto o riesgo residual.

El resultado del análisis de riesgo es solamente un análisis. Con estos datos se efectuarán los siguientes pasos:

1. Evaluación
2. Tratamiento

La Figura No.7 muestra las acciones a tomar luego de analizar los riesgos.

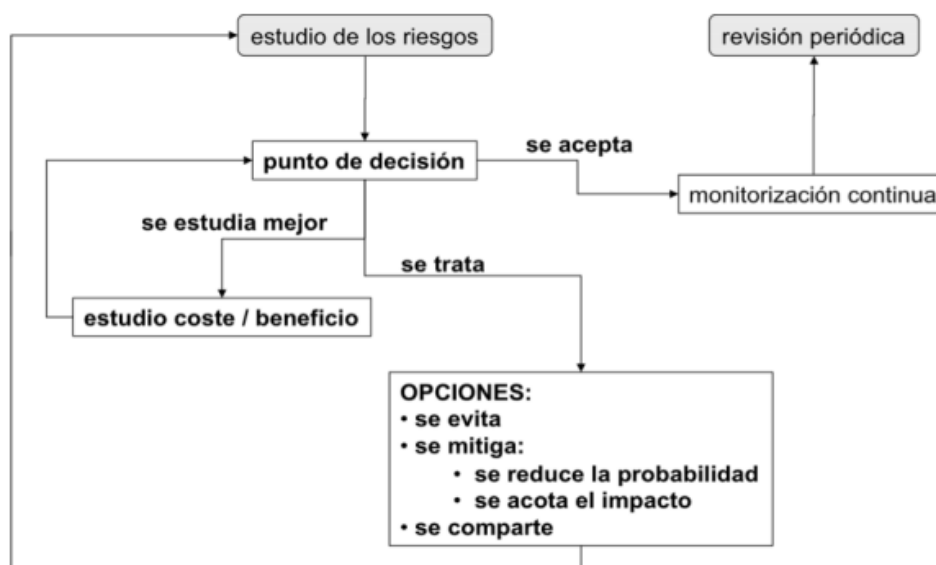


Figura No. 7. Acciones a tomar luego del análisis de riesgos.  
(Ministerio de Hacienda y Administraciones Públicas, 2012)

#### 2.1.2.2.1.1.4.1 Evaluación

##### *Interpretación de los valores de impacto y riesgos residuales*

Impacto y riesgos residuales son una medida del estado actual entre la inseguridad potencial y los controles adecuados que podrían reducir el impacto y riesgos a valores aceptables. El valor residual es la relación de lo que se debería hacer y no se ha hecho.

#### 2.1.2.2.1.1.4.2 Aceptación de riesgo

La organización debe determinar el nivel de impacto y riesgo aceptables, es decir, deberá aceptar la responsabilidad de la falta o carencia de controles adecuados. Los niveles de aceptación pueden ser aplicables por activos o la agregación de activos. Cualquier nivel de impacto y/o riesgo es aceptable si este es conocido y aceptado formalmente por los interesados o stakeholders.

#### *2.1.2.2.1.1.4.3 Tratamiento*

El tratamiento a aplicar lo deciden los interesados o stakeholders y para ello tiene dos opciones:

- Reducir el riesgo residual o
- Ampliar el riesgo residual

#### *2.1.2.2.1.1.4.4 Estudio cuantitativo de costo-beneficio*

No se puede invertir en controles más allá de lo que costaría lo que queremos proteger, pero a veces esto no ocurre así tanto por la parte del cálculo del riesgo como por el cálculo del costo del control

#### *2.1.2.2.1.1.4.5 Estudio cualitativo de costo-beneficio*

En la realización de un análisis cualitativo aparecen intangibles que dificultan el cálculo numérico. Los intangibles pueden ser:

- Reputación o imagen
- Competencia con otras organizaciones
- Cumplimiento normativo que puede ser obligatorio o voluntario
- Capacidad de operar
- Productividad

#### **2.1.2.2.1.1.5 Formalización de las Actividades**

##### *2.1.2.2.1.1.5.1 Roles y funciones*

En el proceso de gestión de los riesgos pueden aparecer varios actores con diferentes funciones y responsabilidades como:



- Órganos de Gobierno
- Dirección ejecutiva
- Dirección operacional

Además se pueden identificar ciertos roles que estarán involucrados para el proceso de gestión de riesgos como:

- Responsable de la Información
- Responsable del servicio
- Responsable de la seguridad
- Responsable del sistema
- Administradores y operadores.

Para ello se utiliza la matriz RACI que sirve para asignar responsabilidades y se usa en la gestión de proyectos para relacionar actividades con recursos, logrando que cada tarea se asigne a una persona o área.

#### *2.1.2.2.1.1.5.2 Contexto*

Se debe documentar todo el ambiente externo a la organización que puede ser cultural, social o político. También se debe identificar las leyes y cumplimiento de las observaciones por parte de las entidades de control.

#### *2.1.2.2.1.1.5.3 Criterios*

Las estimaciones deben ser lo más objetivas posible puesto que múltiples aspectos relacionados con los riesgos son objeto de estimaciones. Además conviene establecer escalas para valorar:

- Requisitos de seguridad de la información

- Requisitos de disponibilidad de los servicios
- La probabilidad de amenazas
- Consecuencias de un incidente de seguridad

#### *2.1.2.2.1.1.5.4 Decisión de tratamiento*

Existen varias formas de reducir el riesgo como:

- Eliminar el riesgo eliminando las causas
- Reducir o limitar el impacto
- Reducir la probabilidad de que una amenaza se materialice
- Implantar nuevos controles o mejorar los ya existentes
- Contratar seguros de cobertura

#### *2.1.2.2.1.1.5.5 Comunicación y consulta.*

Es necesario entender para qué se requiere el sistema y la manera de utilizarlo. Se debe interactuar con varios actores como:

- Los órganos de gobierno y decisión
- Los usuarios y técnicos del sistema
- Los proveedores

#### *2.1.2.2.1.1.5.6 Seguimiento y Revisión*

Es necesario que los sistemas estén bajo monitoreo permanente y se debe preparar un sistema de detección de posibles incidentes. Como resultado de esto se pueden disponer de indicadores que ayudarán a la evaluación del riesgo.

#### **2.1.2.2.2 ISO/IEC 27005 Sistema de Gestión de Riesgos**

(International Standards Organization, 2008)

La información es lo más importante para las organizaciones, por lo cual requiere estar protegida de cualquier amenaza, sea esta interna o externa, que pueda poner en peligro a las empresas tanto públicas como privadas. Esta debe protegerse a través de la implantación de nuevas y mejores medidas de seguridad para que cualquier negocio logre sus objetivos empresariales y garantice el cumplimiento legal.

Actualmente las empresas se enfrentan a un alto número de riesgos procedentes de varios orígenes, entre ellos, nuevos negocios (redes sociales, e-mailing, B2B) y nuevas herramientas (Cloud Computing, Mobility, BYOD) utilizadas por las TI, las cuales deben aplicarse hacia los objetivos organizacionales, garantizando la confidencialidad, integridad y disponibilidad de la información crítica.

La base del Sistema de Gestión de Seguridad de la Información es el análisis y gestión de los riesgos basados en procesos de servicios de TI. Este análisis es útil para evaluar y controlar los riesgos de los sistemas de información. Así, estos procesos se fundamentan en los activos de TI que soportan los mismos. Una vez evaluados los riesgos y aplicados los controles necesarios, queda un efecto residual el cual puede ser aceptado o no y deberá ser revisado periódicamente.

El Análisis de Riesgos es una herramienta muy importante que permite identificar las amenazas a la que están expuestos los activos, estimar la periodicidad de ocurrencia y valorar el impacto que tendría esta ocurrencia.

La Norma ISO/IEC 27005 del sistema de Gestión de Riesgos para la Seguridad de la Información proporciona recomendaciones y lineamientos de métodos y técnicas de evaluación de riesgos.

## **1. Valoración del Riesgo para la Seguridad de la Información**

### **Descripción de la Evaluación del Riesgo**

Es importante definir el propósito de la Gestión del Riesgo para la Seguridad de la Información, puesto que influye en todo el proceso, y particularmente, al establecimiento del contexto. Para establecer el contexto se requiere de toda la información que es pertinente acerca de la organización. Con ello se pretende establecer los criterios básicos para la gestión del riesgo para la Seguridad de la Información, definir el alcance y los límites y establecer una adecuada organización para operarla.

El principal propósito de la evaluación del riesgo es determinar qué podría suceder para ocasionar una pérdida potencial y entender cómo, dónde y por qué ocurriría. Para lograr este propósito es necesario realizar estas actividades:

### **Análisis del Riesgo**

Los activos de información deben ser evaluados para identificar su impacto en la organización. Para ello se debe realizar un análisis para determinar qué activos están bajo riesgo. Se debe decidir sobre el riesgo aceptable en la organización y los controles a implementar para mitigar el riesgo.

En el proceso de análisis de riesgo se deben seguir los siguientes pasos:

- a) Identificar el riesgo
- b) Estimar el riesgo
- c) Evaluar el riesgo

**a) *Identificación del Riesgo***

Un evento es considerado un riesgo si existe asociado a él un grado de incertidumbre. El valor de un activo puede variar con el transcurso del tiempo, por tanto se debe identificar el riesgo como tal, y no sus causas o efectos. Para ello se deben realizar las siguientes actividades:

- a) Identificar los activos
- b) Identificar las amenazas
- c) Identificar los controles existentes
- d) Identificar las vulnerabilidades
- e) Identificar las consecuencias

El resultado de esta actividad es una lista de escenarios de incidentes con sus consecuencias relacionadas con los activos y procesos del negocio.

**b) *Estimación del Riesgo***

La estimación de riesgo se puede realizar con diferentes grados de detalle dependiendo de la criticidad de los activos, las vulnerabilidades conocidas e incidentes anteriores que pudieron haber involucrado a la organización.

El análisis debe ser consistente con los criterios de evaluación del riesgo desarrollados en el establecimiento del contexto. Las actividades a desarrollar en esta etapa son:

- a. Evaluación de las consecuencias
- b. Evaluación de la probabilidad de incidentes
- c. Nivel de estimación de riesgo

**c) *Evaluación del Riesgo***

Para comprender los efectos de los eventos adversos que se podrían presentar en una organización, es indispensable establecer una relación entre los escenarios de riesgos de TI y el impacto a la organización que estos generarían.

Para evaluar los riesgos, las organizaciones deben comparar los riesgos estimados con los criterios de evaluación de riesgos definidos en el establecimiento del contexto para la gestión adecuada del riesgo en la seguridad de la información interna y externa y deben tomar en consideración los objetivos de la organización y los puntos de vista de los stakeholders. Las decisiones se basan principalmente en el nivel de aceptación del riesgo.

La evaluación de riesgos se realiza siempre en más de una iteración, donde en la primera se determinan los riesgos altos y en las iteraciones posteriores, se determinan riesgos principales y tolerables. Esta evaluación de riesgos se realiza periódicamente y los factores que determinan el grado de riesgo son a menudo:

- Probabilidad
- Impacto
- Ocurrencia
- Urgencia

- Dependencia

La evaluación del riesgo requiere de 4 puntos:

1. El estudio de las vulnerabilidades, amenazas, probabilidad e impacto donde los resultados de estas evaluaciones son utilizados para desarrollar los requerimientos de seguridad y sus especificaciones.
2. Estimar el efecto y establecer el grado de aceptación mediante el proceso de evaluación de estas amenazas y vulnerabilidades.
3. La identificación de los activos que podrían resultar afectadas por las amenazas y vulnerabilidades.
4. Análisis de los activos y las vulnerabilidades para establecer las probabilidades de ocurrencia y el estimado de la ocurrencia de ciertos eventos.

El resultado de esta acción es una lista de los riesgos con prioridad de acuerdo con los criterios de evaluación del riesgo, con relación a los *escenarios de incidentes* que llevan a tales riesgos.

## **2. Tratamiento del Riesgo**

En esta etapa se debe seleccionar los controles y debe definirse un plan para el tratamiento del riesgo.

La opción para el tratamiento del riesgo se selecciona basada en el resultado de la evaluación del riesgo, el costo esperado para implementar estas opciones y los beneficios esperados como consecuencia de ellas.

Existen 4 opciones para tratar los riesgos:

1. Reducir
2. Aceptar
3. Evitar
4. Transferir

**a) *Reducir el Riesgo***

Esta acción debe reducir el nivel de riesgo mediante la selección de controles de modo que el riesgo residual, en las siguientes iteraciones se pueda evaluar como aceptable.

Es recomendable seleccionar controles adecuados y justificados que satisfagan los requisitos identificados en la evaluación y tratamiento del riesgo. Para la selección de los controles se debe considerar el tiempo para la implementación de los controles y ponderar el costo de adquirir, implementar, administrar, operar, monitorear y mantener los controles contra el valor de los activos que se protegen.

De igual manera se debe tener en cuenta los criterios de aceptación del riesgo así como requisitos legales y reglamentarios.

**b) *Aceptar el Riesgo***

Si el nivel de riesgo satisface los criterios para su aceptación, no es necesario implementar controles adicionales y el riesgo como tal se acepta. Se aceptará los riesgos siempre y cuando ellos satisfagan claramente las políticas de la organización y los criterios para la aceptación de los riesgos, así como requisitos legales y reglamentarios.



*c) Eliminar el Riesgo*

Cuando los riesgos identificados se consideran muy altos, o si los costos para implementar otras opciones de tratamiento del riesgo exceden los beneficios, se puede tomar una decisión para evitar por completo el riesgo, mediante el retiro de una actividad o un conjunto de actividades planificadas o existentes, o mediante el cambio en las condiciones bajo las cuales se efectúa tal actividad.

*d) Transferir el Riesgo*

La transferencia del riesgo involucra la decisión para compartir algunos riesgos con un tercero. La transferencia del riesgo puede crear riesgos nuevos o reducir los riesgos identificados existentes. Por lo tanto, puede ser necesario el tratamiento adicional para el riesgo. La transferencia se puede hacer mediante un seguro que dará soporte a las consecuencias o mediante subcontratación de un asociado cuya función será monitorear el sistema de información y tomar acciones inmediatas para detener un ataque antes de que éste produzca un nivel definido de daño. Cabe indicar que puede ser posible transferir la responsabilidad para la gestión del riesgo, pero normalmente no es posible transferir la responsabilidad de un impacto. Los clientes por lo general atribuirán un impacto adverso a fallas de la organización.

### **3. Aceptación del Riesgo**

Los planes para el tratamiento del riesgo deberían describir la forma en que los riesgos evaluados se deben tratar con el fin de satisfacer los criterios de aceptación del riesgo. Es importante que los responsables revisen y aprueben los planes

propuestos para el tratamiento del riesgo y los riesgos residuales resultantes, y que registren todas las condiciones asociadas a dicha aprobación. En algunos casos, es posible que el nivel del riesgo residual no satisfaga los criterios de aceptación del riesgo porque los criterios que se aplican no toman en consideración las circunstancias predominantes.

No obstante, no siempre es posible revisar los criterios de aceptación del riesgo de manera oportuna. En tales casos, quienes toman las decisiones pueden tener que aceptar riesgos que no satisfacen los criterios normales de aceptación y deberían comentar explícitamente los riesgos e incluir una justificación para la decisión de hacer caso omiso de los criterios normales de aceptación del riesgo.

El resultado de esta actividad es una lista de los riesgos aceptados con la justificación para aquellos que no satisfacen los criterios normales de aceptación de riesgos de la organización.

#### **4. Comunicación del Riesgo**

La comunicación del riesgo es una actividad para lograr un acuerdo sobre la manera de gestionar los riesgos al intercambiar y/o compartir la información acerca de los riesgos, entre quienes toman las decisiones y los stakeholders.

La comunicación eficaz es importante dado que puede tener un impacto significativo en las decisiones que se deben tomar y ésta garantizará que aquellos responsables de la implementación de la gestión del riesgo y aquellos con derechos adquiridos comprenden las bases sobre las cuales se toman las decisiones y el por qué se requieren acciones particulares. La comunicación es bidireccional.

Las percepciones del riesgo pueden variar debido a las diferencias en las estimaciones, los conceptos y las necesidades, los problemas y los intereses de los stakeholders en cuanto se relacionan con el riesgo.

La comunicación del riesgo se debe realizar con la finalidad de:

- Brindar seguridad del resultado de la gestión del riesgo en la organización
- Recolectar información sobre el riesgo
- Compartir los resultados de la evaluación del riesgo y presentar el plan para el tratamiento del riesgo
- Evitar o reducir tanto la ocurrencia como la consecuencia de las brechas en la seguridad de la información debidas a la falta de comprensión mutua entre quienes toman las decisiones y los stakeholders
- Brindar soporte para la toma de decisiones
- Obtener conocimientos nuevos sobre la seguridad de la información
- Coordinar con otras partes y planificar las respuestas para reducir las consecuencias de cualquier incidente
- Dar a quienes toman las decisiones y a los stakeholders un sentido de responsabilidad acerca de los riesgos
- Mejorar la concienciación

La organización debería desarrollar planes de comunicación del riesgo para las operaciones normales así como para las situaciones de emergencia. Por lo tanto, la actividad de comunicación del riesgo se debería realizar de manera continua.

El resultado de esta actividad es la comprensión continua del proceso y los resultados de la gestión del riesgo en la seguridad de la información de la organización.

## **5. Monitoreo y Revisión del Riesgo**

Los riesgos y sus factores (el valor de los activos, impactos, amenazas, vulnerabilidades, probabilidad de ocurrencia, etc.) deben ser monitoreados y revisados en una etapa temprana con el fin de visualizar la perspectiva completa de riesgo ante cualquier cambio en el contexto de la organización.

Las organizaciones deben garantizar el monitoreo permanente de los siguientes aspectos:

- Activos nuevos que se han añadido dentro del alcance de la gestión del riesgo
- Si cambian en los objetivos del negocio, los valores de los activos pueden modificarse, debido a amenazas nuevas que podrían estar activas tanto fuera como dentro de la organización y que no se han considerado
- La probabilidad de que nuevas vulnerabilidades puedan permitir que las amenazas las exploten
- El impacto o las consecuencias de las amenazas evaluadas, las vulnerabilidades y los riesgos en conjunto que dan como resultado un nivel inaceptable de riesgo
- Incidentes de la seguridad de la información

Las amenazas, vulnerabilidades o cambios en la probabilidad o las consecuencias pueden variar los riesgos evaluados previamente como riesgos bajos y éstos se

debería considerar independientemente y también todos estos riesgos como un conjunto, para evaluar su impacto acumulado potencial.

Las actividades de monitoreo del riesgo se deben hacer de manera regular y el tratamiento del riesgo se debe revisar periódicamente.

El resultado de las actividades de monitoreo del riesgo puede ser la entrada para otras actividades de revisión del riesgo.

El monitoreo y revisión debe cubrir los siguientes aspectos:

- contexto legal y regulatorio
- enfoque para la evaluación del riesgo
- categorías y valor de los activos
- criterios del impacto
- criterios de evaluación del riesgo
- criterios de aceptación del riesgo
- recursos necesarios

La organización debe garantizar que los recursos para el tratamiento y la evaluación del riesgo estén disponibles continuamente para revisar el riesgo, tratar las amenazas o nuevas vulnerabilidades y asesorar a la Dirección.

### **2.1.2.2.3 RISK IT (ISACA, 2009)**

Es un documento que forma parte de la Iniciativa de los riesgos de TI de ISACA. Es un marco basado en un conjunto de principios y guías, procesos de negocios y directrices ajustados a estos principios.

Este marco es complementario a COBIT, y establece las mejores prácticas para crear un marco para las organizaciones con la finalidad de identificar, gobernar y administrar los riesgos asociados. En las organizaciones que han adoptado o están por adoptar COBIT como el marco de gobierno, se puede utilizar RISK IT para mejorar la gestión de los riesgos.

RISK IT es una herramienta para la gestión de los riesgos basado en el valor y beneficios que la empresa obtiene a través de las iniciativas de TI. El riesgo de TI considera el riesgo de la empresa que está asociado con la utilización de TI, su operación, influencia y la propiedad de TI.

COBIT gestiona todas las actividades relacionadas con TI dentro de la organización. En RISK IT, los procesos se relacionan con eventos internos y externos. Los internos pueden incluir los incidentes operacionales, falencias en los proyectos, cambios en la estrategia de TI y las fusiones. En los externos, incluyen cambios en las condiciones del mercado, nuevos competidores, nuevas tecnologías disponibles y nuevas regulaciones que pueden afectar a las organizaciones. Estos eventos, plantean riesgos y una oportunidad para evaluarlos y generar soluciones oportunas.

El modelo de proceso en la gestión de riesgos define actividades claves en procesos agrupados dentro de tres ámbitos y cada uno con tres procesos y varias actividades:

### ***1. Gobierno del Riesgo***

1. Establecer una visión común del riesgo
  - Realizar la evaluación de riesgo de TI de la organización
  - Proponer umbrales de tolerancia al riesgo de TI
  - Aprobar la tolerancia al riesgo de TI
  - Alinear a la política de riesgos de TI
  - Promover la cultura de prevención de riesgos de TI
  - Promover la comunicación efectiva de los riesgos de TI
2. Integrar con ERM
  - Establecer y mantener la responsabilidad de la gestión de riesgos de TI.
  - Coordinar la estrategia de riesgos de IT y la estrategia de riesgo empresarial.
  - Adaptar las prácticas de riesgo de TI a las prácticas de riesgo de la empresa.
  - Proporcionar los recursos adecuados para la gestión de riesgos de TI.
  - Ofrecer una garantía independiente sobre la gestión de riesgos.
3. Tomar decisiones conscientes del riesgo
  - Acordar la gestión para el enfoque de análisis de riesgos de TI.
  - Aprobar el análisis de riesgos de TI.

- Integrar consideraciones de riesgos de TI en la toma de decisiones estratégicas
- Aceptar los riesgos de TI.
- Priorizar las actividades de respuesta al riesgo de TI

## **2. Evaluación del Riesgo**

### 1. Recolectar datos

- Establecer y mantener un modelo para recolección de datos.
- Recopilar datos sobre el entorno operativo.
- Recopilar datos sobre eventos de riesgo.
- Identificar los factores de riesgo

### 2. Analizar los Riesgos

- Definir el alcance de análisis de riesgos de TI.
- Estimación del riesgo de TI.
- Identificar las opciones de respuesta a los riesgos.
- Realizar una revisión por pares de análisis de riesgos de TI.

### 3. Mantener el perfil de riesgo

- Mapear los recursos de TI a los procesos de negocio.
- Determinar la criticidad del negocio de los recursos de TI.
- Entender las capacidades de TI.
- Actualización de los componentes del escenario de riesgos de TI
- Mantener el registro de riesgos de TI y el mapa de riesgos de TI.
- Desarrollar indicadores de riesgos de TI.

## **3. Respuesta del Riesgo**

### 1. Articular los riesgos



- Comunicar los resultados del análisis de riesgos de TI
  - Informar las actividades de gestión de riesgos de TI y el estado de cumplimiento.
  - Interpretar los resultados de las evaluaciones de TI.
  - Identificar las oportunidades relacionados con TI.
2. Gestionar los riesgos de TI
- Controles de inventario.
  - Seguimiento operacional con umbrales de tolerancia al riesgo.
  - Respuesta la exposición al riesgo descubierto y las oportunidades.
  - Implementar controles.
  - Informe el progreso de plan de acción de riesgos de TI
3. Reaccionar ante eventos
- Mantener los planes de respuesta a incidentes
  - Seguimiento de riesgos de TI
  - Iniciar la respuesta a incidentes
  - Comunicar las lecciones aprendidas de los eventos de riesgo

#### **2.1.2.2.4 COBIT (ISACA, 2007)**

### **1. Mejores Prácticas de las Tecnologías de Información**

Hoy en día la información y las tecnologías que las soportan se han convertido, para varias organizaciones, en los activos más valiosos debido a que contribuyen al cumplimiento de los objetivos del negocio, por lo que han visto la necesidad de minimizar el riesgo en un entorno sujeto a amenazas internas o externas debido a eventos inesperados o indeseados que pueden afectar el normal funcionamiento de las actividades dentro de la organización.

Tales eventos deben ser prevenidos, detectados, y corregidos por lo que es necesario establecer mecanismos de control que garanticen un mejor gobierno o un rendimiento más óptimo de las TI en una organización.

Es precisamente COBIT (Control Objective for Information Technology) aceptado internacionalmente que establece el desarrollo de políticas, procedimientos y buenas prácticas para el control de TI en las organizaciones, el mismo que permite estructurar y controlar los procesos de TI, entender y administrar los riesgos de tal forma que se atiendan las necesidades de la organización y entidades externas de forma oportuna, así como también el aseguramiento en el cumplimiento de órganos regulatorios.

COBIT permite establecer un conjunto de procesos que permiten alinear las metas de negocio con las metas de TI, permitiendo la adaptación de las operaciones de TI con las operaciones de la organización, es aplicable en toda el área de TI de cualquier organización, con procesos que pueden ser cuantificables para medir sus logros.

Permite la identificación de responsabilidades asociadas a los dueños del proceso y con un modelo de madurez de los procesos de la organización enfocado en el mejoramiento continuo.

El objetivo principal de COBIT es brindar confianza y seguridad a los directivos de una organización referente a las TI, a través de la aplicación de las buenas prácticas para el control de TI permitiendo alinearse los objetivos de TI con los objetivos de la organización y de esta manera satisfacer los requerimientos al mantener un entendimiento compartido entre todos los interesados en base a un lenguaje común.

## **2. Publicación de COBIT**

Los Objetivos de Control para la Información y la Tecnología relacionada COBIT fue creado por ISACA (Information Systems Audit and Control Association) y el ITGI (IT Governance Institute) y publicada por primera vez en 1996, a partir de esta fecha han ido evolucionando con la última edición de COBIT 5 basado en COBIT 4.1 el cual proporciona una visión empresarial del Gobierno de TI. Constantemente COBIT se actualiza con otros estándares como COSO, ISO27000 e ITIL.

Cabe mencionar que además del Marco de Trabajo de COBIT 4.1, se han elaborado las guías de auditoría que en la versión 4.1 pasaron a ser las "Guías de aseguramiento de tecnología de información usando Cobit", que se encuentran en el documento "IT Assurance Guide Using Cobit", que tiene como objetivo proporcionar orientación sobre el uso de COBIT para apoyar a las actividades de aseguramiento de TI.

Para el desarrollo del presente tema nos basaremos en COBIT 4.1 que a continuación se detalla:

### 3. Principios Básicos de COBIT

COBIT se encuentra orientado al negocio, a procesos y basado en controles, de acuerdo a como se ilustra en la Figura No. 8

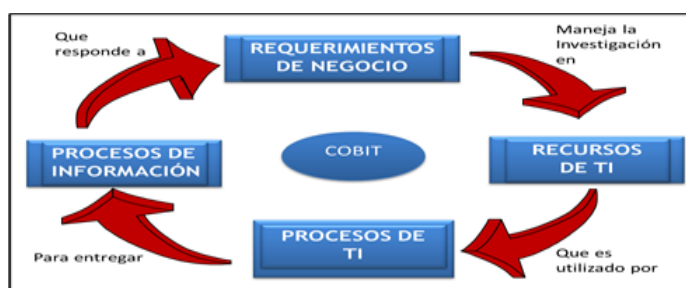


Figura No. 8. Principios Básicos de COBIT  
(ISACA, 2007)

#### Orientado al Negocio

Para el cumplimiento de los objetivos del negocio la información necesita adaptarse a siete criterios distintos de controles referidos y combinados por COBIT conocidos como requerimientos de información del negocio, con base a los requerimientos de calidad, fiduciarios y de seguridad estos son:

Cuadro No. 3. Criterios de Control de COBIT

(ISACA, 2007)

<b>Efectividad</b>	La información sea relevante y pertinente a los procesos del negocio, y se proporcione de una manera oportuna, correcta, consistente y utilizable.
<b>Eficiencia</b>	La información sea generada con el óptimo (más productivo y económico) uso de los recursos.
<b>Confidencialidad</b>	La protección de información sensible contra revelación no autorizada.
<b>Integridad</b>	Relacionada con la precisión y completitud de la

Continúa ➡

	información, así como con su validez de acuerdo a los valores y expectativas del negocio.
<b>Disponibilidad</b>	La información esté disponible cuando sea requerida por los procesos del negocio en cualquier momento. También concierne a la protección de los recursos y las capacidades necesarias asociadas.
<b>Cumplimiento</b>	Acatar aquellas leyes, reglamentos y acuerdos contractuales a los cuales está sujeto el proceso de negocios, es decir, criterios de negocios impuestos externamente, así como políticas internas.
<b>Confiabilidad</b>	Proporcionar la información apropiada para que la gerencia administre la entidad y ejerza sus responsabilidades fiduciarias y de gobierno.

COBIT y su enfoque de alto nivel orientado al negocio también identifica los recursos de TI requeridos en toda organización para responder a los requerimientos que el negocio tiene hacia TI como son:

Cuadro No. 4. Resumen de recursos de TI identificados en COBIT.  
(ISACA, 2007)

<b>Aplicaciones</b>	Se entiende como sistemas de usuario automatizados como procedimientos manuales que procesan información.
<b>Información</b>	Los datos en todas sus formas, de entrada, procesados y generados por los sistemas de información, en cualquier forma en que sean utilizados por el negocio.
<b>Infraestructura</b>	La tecnología y las instalaciones que permiten el procesamiento de las aplicaciones.
<b>Personas</b>	Personal requerido para planear, organizar, adquirir, implementar, entregar, soportar, monitorear y evaluar los sistemas y los servicios de información. Pueden ser internas, por outsourcing o contratadas, de acuerdo a como se requieran.

COBIT, está diseñado para ser utilizado por proveedores de servicios, usuarios, auditores de TI y como guía integral para la gerencia y los dueños de los procesos de negocio.

## Orientado a Procesos

COBIT, clasifica los procesos de las unidades de tecnología de información en 34 procesos que se denominan también objetivos de control de alto nivel, agrupados en 4 dominios los mismos que permiten lograr la mejora continua de la gestión de TI como se ilustra en la Figura No. 9.

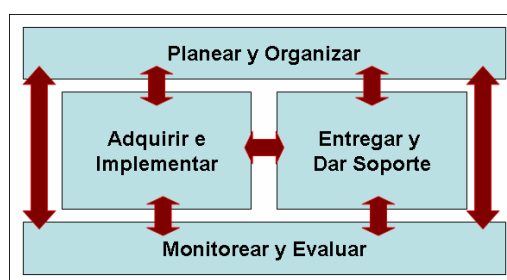


Figura No. 9. Dominios de COBIT.  
(ISACA, 2007)

*Planear y Organizar:* Cubre las estrategias y las tácticas, y tiene que ver con identificar la manera en que TI puede contribuir al logro de los objetivos del negocio. Es así que la visión estratégica requiere ser planeada, comunicada y administrada desde diferentes perspectivas. Finalmente, requiere implementar una estructura organizacional y una estructura tecnológica apropiada. Este dominio cubre los siguientes procesos:

- PO1 Definir un Plan Estratégico de TI
- PO2 Definir la Arquitectura de la Información
- PO3 Determinar la Dirección Tecnológica
- PO4 Definir los Procesos, Organización y Relaciones de TI
- PO5 Administrar la Inversión en TI
- PO6 Comunicar las Aspiraciones y la Dirección de la Gerencia

- PO7 Administrar Recursos Humanos de TI
- PO8 Administrar la Calidad
- PO9 Evaluar y Administrar los Riesgos de TI
- PO10 Administrar Proyectos

*Adquirir e implementar:* Para llevar a cabo la estrategia de TI, las soluciones de TI necesitan ser identificadas, desarrolladas o adquiridas así como implementadas e integradas en los procesos del negocio. Además los cambios y el mantenimiento realizado a sistemas existentes son necesarios para garantizar que las soluciones sigan satisfaciendo los objetivos del negocio. Los procesos que abarca este dominio son:

- AI1 Identificar soluciones automatizadas
- AI2 Adquirir y mantener software aplicativo
- AI3 Adquirir y mantener infraestructura tecnológica
- AI4 Facilitar la operación y el uso
- AI5 Adquirir recursos de TI
- AI6 Administrar cambios
- AI7 Instalar y acreditar soluciones y cambios

*Entregar y Dar Soporte:* Se preocupa de la entrega en sí de los servicios requeridos, lo que incluye la prestación del servicio, la administración de la seguridad y de la continuidad, el soporte del servicio a los usuarios, la administración de los datos y de las instalaciones operativos. Los procesos que conforman este dominio son:

- DS1 Definir y administrar los niveles de servicio

- DS2 Administrar los servicios de terceros
- DS3 Administrar el desempeño y la capacidad
- DS4 Garantizar la continuidad del servicio
- DS5 Garantizar la seguridad de los sistemas
- DS6 Identificar y asignar costos
- DS7 Educar y entrenar a los usuarios
- DS8 Administrar la mesa de servicio y los incidentes
- DS9 Administrar la configuración
- DS10 Administrar los problemas
- DS11 Administrar los datos
- DS12 Administrar el ambiente físico
- DS13 Administrar las operaciones

*Monitorear y Evaluar:* Este dominio abarca la administración del desempeño, el monitoreo del control interno, el cumplimiento regulatorio y la aplicación del gobierno. Los procesos que forman este dominio son:

- ME1 Monitorear y Evaluar el Desempeño de TI
- ME2 Monitorear y Evaluar el Control Interno
- ME3 Garantizar el Cumplimiento Regulatorio
- ME4 Proporcionar Gobierno de TI

### **Basado en Controles**

Para cada uno de los procesos de TI, COBIT define 318 objetivos de control tanto para el proceso general como para los procesos específicos, los mismos que



implementan procedimientos de control diseñadas para garantizar que los objetivos del negocio serán alcanzados y que eventos no deseables serán prevenidos detectados o corregidos.

De los procesos de control indicados anteriormente se tomará en consideración los que se relacionan a riesgos de TI y que se explican a continuación:

*PO9 Evaluar y Administrar los Riesgos de TI:* Este proceso se encuentra dentro del dominio Planear y Organizar el mismo que crea, administra y comunica los riesgos de TI y su impacto potencial sobre los procesos y metas de la organización causado por algún evento inesperado, el cual se debe identificar, analizar y evaluar, así como también adoptar estrategias de mitigación de riesgos para minimizarlos.

### **Objetivos de Control**

**PO9.1 Marco de Trabajo de Administración de Riesgos:** Permite establecer un marco de trabajo de administración de riesgos de TI que deberán estar alineado al marco de trabajo de administración de riesgos de la organización. Este Marco de Administración de riesgos deberá contener una evaluación regular de los riesgos de TI más importantes, con la finalidad de determinar la manera en que los riesgos puedan ser manejados a un nivel aceptable y además deberá asegurar actualizaciones regulares sobre la evaluación de riesgos.

**PO9.2 Establecimiento del Contexto del Riesgo:** Permite establecer el contexto en el cual el marco de trabajo de evaluación de riesgos se aplica para garantizar resultados apropiados. Esto incluye la determinación del contexto

interno y externo de cada evaluación de riesgos, la meta de la evaluación y los criterios contra los cuales se evaluarán los riesgos.

**PO9.3 Identificación de Eventos:** Permite identificar eventos (una amenaza importante y realista que explota una vulnerabilidad aplicable y significativa) con un impacto potencial negativo sobre las metas o las operaciones de la empresa, incluyendo aspectos de negocio, regulatorios, legales, tecnológicos, de sociedad comercial, de recursos humanos y operativos.

**PO9.4 Evaluación de Riesgos de TI:** Permite evaluar de forma recurrente la probabilidad e impacto de todos los riesgos identificados, usando métodos cualitativos y cuantitativos. Además deberá evaluarse la capacidad de aceptación de riesgos de la organización.

**PO9.5 Respuesta a los Riesgos:** Permite desarrollar y mantener un proceso de respuesta a riesgos diseñado para asegurar que controles efectivos en costo mitigan la exposición de riesgos en forma continua, se debe identificar estrategias tales como evitar, reducir, compartir o aceptar riesgos; determinar responsabilidades y considerar los niveles de tolerancia a riesgos.

**PO9.6 Mantenimiento y Monitoreo de un Plan de Acción de Riesgos:** Permite priorizar y planear las actividades de control a todos los niveles para implementar las respuestas a los riesgos, identificadas como necesarias, incluyendo la identificación de costos, beneficios y la responsabilidad de la ejecución. Requiere obtener la aprobación para las acciones recomendadas y la aceptación de cualquier riesgo residual, y además asegurarse de que las acciones comprometidas están a cargo del dueño (s) de los procesos

afectados. Además es necesario Monitorear la ejecución de los planes y reportar cualquier desviación a la alta dirección.

### Modelo de Madurez

COBIT provee Modelos de Madurez para la administración y control de los procesos de TI de tal forma que se pueda determinar el punto donde la organización se encuentra. Este modelo consiste en un método de asignación de puntos que puede calificarse desde Inexistente hasta Optimizado (0 a 5).

Es así que utilizando los modelos de madurez desarrollados para cada uno de los 34 procesos de TI definidos en COBIT, la gerencia podrá identificar:

- El desempeño real de la empresa - Dónde se encuentra la empresa hoy
- El estatus actual de la industria - La comparación
- El objetivo de mejora de la empresa - Dónde desea estar la empresa
- El crecimiento requerido entre “como es” y “como será”.

Mediante el siguiente gráfico permite que los resultados sean utilizados con facilidad en resúmenes gerenciales como se indica a continuación (Figura No. 10):

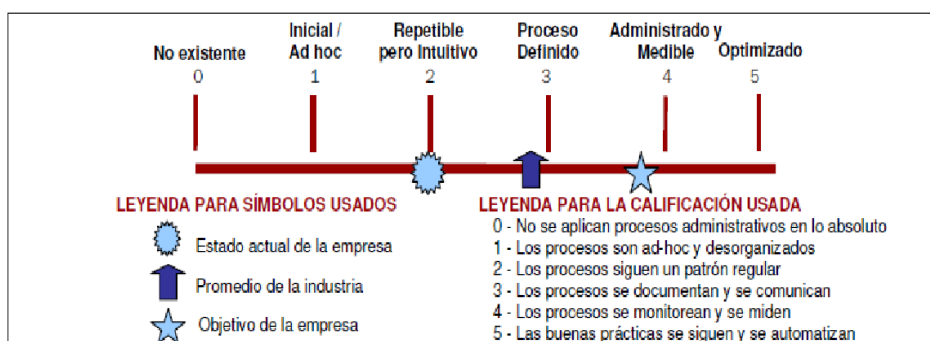


Figura No. 10. Representación gráfica de los modelos de madurez.

(ISACA, 2007)

Dentro del Modelo de Madurez referente al Proceso Evaluar y Administrar los Riesgos de TI se definen las siguientes mediciones con la finalidad de determinar cuál es el desempeño real de la empresa en sus procesos de TI.

Cuadro No. 5. Proceso Evaluar y Administrar los Riesgos de TI.  
(ISACA, 2007)

<b>Modelo de Madurez - Proceso Evaluar y Administrar los Riesgos de TI</b>	
<b>0 No Existente</b>	<ul style="list-style-type: none"> <li>• La evaluación de riesgos para los procesos y las decisiones de negocio no ocurre</li> <li>• No se considera los impactos en el negocio asociados a las vulnerabilidades de seguridad y del desarrollo de proyectos</li> <li>• La administración de riesgos no se ha identificado como algo relevante para adquirir soluciones y prestar servicios de TI</li> </ul>
<b>1 Inicial</b>	<ul style="list-style-type: none"> <li>• Se realizan evaluaciones informales de riesgos según lo determine cada proyecto.</li> <li>• En ocasiones se identifican evaluaciones de riesgos en un plan de proyectos pero se asignan rara vez a gerentes específicos.</li> <li>• Los riesgos específicos relacionados con TI se toman en cuenta ocasionalmente proyecto por proyecto.</li> <li>• Los riesgos relativos a TI que afectan las operaciones del día a día, son rara vez discutidas en reuniones gerenciales.</li> <li>• Cuando se toman en cuenta los riesgos, la mitigación es inconsistente.</li> <li>• Existe un entendimiento emergente de que los riesgos de TI son importantes y necesitan ser considerados.</li> </ul>
<b>2 Repetible pero Intuitivo</b>	<ul style="list-style-type: none"> <li>• Existe un enfoque de evaluación de riesgos en desarrollo y se implementa a discreción de los gerentes de proyecto.</li> <li>• La administración de riesgos se da por lo general a alto nivel y típicamente se aplica solo a proyectos grandes o como respuesta a problemas.</li> <li>• Los procesos de mitigación de riesgos están empezando a ser implementados donde se identifican riesgos.</li> </ul>
<b>3 Definido</b>	<ul style="list-style-type: none"> <li>• Una política de administración de riesgos para toda la organización define cuándo y cómo realizar las evaluaciones de riesgos.</li> <li>• La administración de riesgos sigue un proceso definido, el cual está documentado.</li> </ul>

Continúa ➡

- 
- El entrenamiento sobre administración de riesgos está disponible para todo el personal.
  - La decisión de seguir el proceso de administración de riesgos y de recibir entrenamiento se deja a la discreción del individuo.
  - La metodología para la evaluación de riesgos es convincente y sólida, y garantiza que los riesgos claves para el negocio sean identificados.
  - Un proceso para mitigar los riesgos clave por lo general se institucionaliza una vez que los riesgos se identifican.
  - Las descripciones de puestos consideran las responsabilidades de administración de riesgos.
- La evaluación y administración de riesgos son procedimientos estándar.
  - Las excepciones al proceso de administración de riesgos se reportan a la gerencia de TI.
  - La administración de riesgos de TI es una responsabilidad de alto nivel.
  - Los riesgos se evalúan y se mitigan a nivel de proyecto individual y también por lo regular se hace con respecto a la operación global de TI.
  - La gerencia recibe notificación sobre los cambios en el ambiente de negocios y de TI que pudieran afectar de manera significativa los escenarios de riesgo relacionados con TI.
  - La gerencia puede monitorear la posición de riesgo y tomar decisiones informadas respecto a la exposición que está dispuesta a aceptar.
  - Todos los riesgos identificados tienen un dueño nombrado, y la alta dirección, así como la gerencia de TI han determinado los niveles de riesgo que la organización está dispuesta a tolerar.
  - La gerencia de TI ha elaborado medidas estándar para evaluar el riesgo y para definir las proporciones riesgo/retorno.
  - La gerencia presupuesta un proyecto de administración de riesgo operativo para re-evaluar los riesgos de manera regular.
  - Se establece una base de datos de administración de riesgos, y parte del proceso de administración de riesgos se empieza a automatizar.
  - La gerencia de TI considera las estrategias de mitigación de riesgo.
- 5 • La administración de riesgos ha evolucionado al nivel en que
-

---

<b>Optimizado</b>	<p>un proceso estructurado está implantado en toda la organización y es bien administrado.</p> <ul style="list-style-type: none"><li>• Las buenas prácticas se aplican en toda la organización.</li><li>• La captura, análisis y reporte de los datos de administración de riesgos están altamente automatizados.</li><li>• La orientación se toma de los líderes en el campo y la organización de TI participa en grupos de interés para intercambiar experiencias.</li><li>• La administración de riesgos está altamente integrada en todo el negocio y en las operaciones de TI, está bien aceptada, y abarca a los usuarios de servicios de TI.</li><li>• La dirección detecta y actúa cuando se toman decisiones grandes de inversión o de operación de TI, sin considerar el plan de administración de riesgos.</li><li>• La dirección evalúa las estrategias de mitigación de riesgos de manera continua.</li></ul>
-------------------	--

---

#### **2.1.2.2.5 COSO-ERM (COSO, 2004)**

##### **Marco de Control Interno**

El control interno es un proceso efectuado por la dirección y el resto del personal de una entidad, diseñado con el objeto de proporcionar un grado de seguridad razonable en cuanto a la consecución de objetivos dentro de las siguientes categorías:

- Eficacia y eficiencia de las operaciones
- Confiabilidad de la información financiera
- Cumplimiento de las leyes, reglamentos y normas que sean aplicables

Ante la necesidad de mejorar la gestión de riesgo en las organizaciones en septiembre de 2004 se publica un nuevo marco de Gestión de Riesgos, llamado Enterprise Risk Management - Integrated Framework, el mismo que detalla los componentes esenciales para la administración integral de riesgos.

##### **Coso II - Enterprise Risk Management (ERM)**

La gestión integral de riesgos es un proceso efectuado por toda la organización, es aplicado desde la definición estratégica hasta las actividades del día a día, diseñado para identificar eventos potenciales que pudieran afectar a la organización y gestionar los riesgos dentro de su apetito de riesgo, a fin de proporcionar una seguridad razonable respecto al logro de los objetivos de la organización.

##### **Componentes de COSO – ERM**

El marco de gestión de riesgos de COSO – ERM consta de ocho componentes que son:

- Ambiente de Control

- Establecimiento de Objetivos
- Identificación de Eventos
- Evaluación de Riesgos
- Respuesta a los Riesgos
- Actividades de Control
- Información y Comunicaciones
- Monitoreo

En la Figura No. 11 se indica como estos componentes se encuentran interrelacionados especialmente con lo que tienen que ver con la gestión de riesgos.

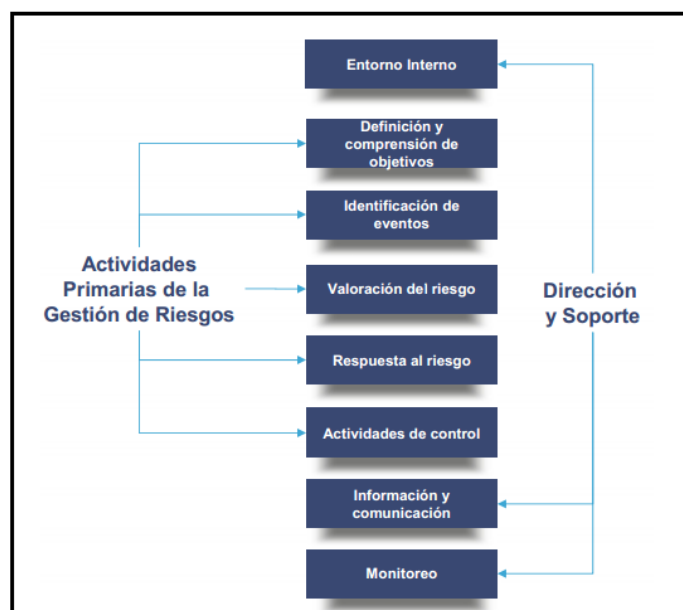


Figura No. 11. Componentes de Control  
(COSO, 2004)

## 1. Ambiente de Control

Este componente forma la base de los otros componentes de control de la gestión de riesgo, establece como los miembros de una organización perciben y tratan los riesgos, identificando los eventos esperados o inesperados que pueden ocurrir.



Permite establecer estrategias para el establecimiento de una cultura proactiva hacia el riesgo mediante la aplicación de roles, responsabilidades y competencias del personal se basa en la integridad y el compromiso con los valores éticos, aportando disciplina y estructura de las actividades de la organización, en el establecimiento de objetivos y en la identificación evaluación e interpretación de los riesgos.

## **2. Establecimiento de Objetivos**

El establecimiento de objetivos se fija a nivel estratégico y deben ser identificados antes de que posibles eventos inesperados puedan afectar al cumplimiento de los mismos.

Asegura que la organización ha establecido un proceso mediante la gestión integral del riesgo, para alinear los objetivos con la visión, misión de la organización y con el riesgo aceptado por la entidad, que orienta a su vez los niveles de tolerancia al riesgo.

## **3. Identificación de eventos**

Este evento permite identificar posibles acontecimientos internos o externos que puedan afectar a los objetivos de la organización, teniendo un impacto positivo y negativo, los eventos negativos representan un riesgo el que requiere una evaluación y una respuesta por parte de la dirección en la organización, mientras que los eventos positivos pueden representar una oportunidad.

Para la identificación de eventos la dirección en una organización debe considerar como factores externos los políticos, sociales, económicos y tecnológicos, mientras que los factores internos las personas y los procesos.

#### **4. Evaluación de Riesgo**

Permite que una entidad entienda el grado en el cual los eventos potenciales pudieran afectar al logro de los objetivos del negocio, es así que en la evaluación de los riesgos la dirección analiza estos acontecimientos desde las siguientes perspectivas:

- Clasificado de acuerdo a la relevancia y probabilidad e impacto de ocurrencia
- Entre técnicas que se utiliza para determinar riesgos
- Considerando eventos previstos e inesperados.
- Evaluando los riesgos con un enfoque de riesgos inherentes y residuales.

Bajo estos lineamientos las organizaciones identifican los riesgos evaluando el nivel de control existente y determinan los puntos de mejora que se deben realizar.

#### **5. Actividades de Control**

Dichas actividades podrán estar constituidas por los procedimientos y políticas específicos que ayudan a asegurar que las respuestas a los riesgos se lleven a cabo adecuadamente y oportunamente, orientados primordialmente hacia la prevención y neutralización de los riesgos.

Las actividades de control se ejecutan en todos los niveles de la organización y en todas las funciones, incluye controles sobre la estructura informática en cuanto a sus sistemas y equipos.

#### **6. Información y Comunicación**

Este evento permite al personal de la entidad identificar, captar y comunicar la información requerida para desarrollar, gestionar y controlar sus operaciones, es así

que deben existir los medios de comunicación idóneos que permitan la entrega de la información en forma oportuna, confiable, disponible y pertinente.

Es responsabilidad de la Dirección comunicar a toda la organización desde abajo hacia arriba y de forma clara las responsabilidades de cada miembro dentro del sistema de control interno y cómo las actividades individuales están relacionadas con el trabajo del resto.

## **7. Supervisión**

La administración del riesgo es monitoreada y le incumbe a la dirección la existencia de una estructura de control interno idónea y eficiente, así como su revisión y actualización periódica para mantenerla en un nivel adecuado.

La evaluación de las actividades de control de los sistemas es a través del tiempo, pues toda organización tiene áreas donde los mismos están en desarrollo y necesitan ser reforzados o se impone directamente su reemplazo debido a que perdieron su eficacia o resultaron inaplicables. El objetivo es asegurar que el control interno funciona adecuadamente, a través de dos modalidades de supervisión: actividades continuas o evaluaciones puntuales.

### **3 CAPITULO III**

#### **3.1 Auditoría Basada en Riesgos de TI**

##### **3.1.1 Auditoría Basada en Riesgos**

(Superintendencia de Bancos y Seguros, 2010)

De acuerdo a la Resolución JB-2010-1549 de 21 de enero del 2010, en el artículo No. 8 establece que:

La auditoría basada en riesgos consiste en un conjunto de procesos mediante los cuales la auditoría provee aseguramiento independiente al directorio u organismo que haga sus veces, acerca de:

8.1 Si los procesos y medidas de gestión del riesgo que se encuentran implementadas están funcionando de acuerdo a lo esperado;

8.2 Si los procesos de gestión de riesgos son apropiados y están bien diseñados; y,

8.3 Si las medidas de control de riesgos que la gerencia ha implementado son adecuadas y efectivas, y reducen el riesgo al nivel de tolerancia aceptado por el directorio u organismo que haga sus veces.

La auditoría basada en riesgos depende del nivel de desarrollo que la propia institución del sistema financiero ha alcanzado en la gestión de riesgos en el área objeto de examen, y el grado en que han sido definidos objetivos determinados por la gerencia contra los cuales pueden medirse los riesgos asociados.

Cuando la institución del sistema financiero cuenta con un sistema de gestión del riesgo adecuado en las área bajo examen, sin perjuicio de la necesidad de verificaciones adicionales propias del debido cuidado profesional, la auditoría basada en riesgos puede confiar en mayor grado en la evaluación del riesgo que la propia institución ha realizado, y desarrollar un plan basado en riesgos que complemente las acciones realizadas por la entidad y aumente el valor de las actividades de la auditoría interna.

Cuando la institución del sistema financiero cuenta con un sistema de gestión de riesgos menos desarrollado, la auditoría basada en riesgos requiere descansar más en la evaluación del riesgo que hace la propia auditoría.

En un entorno cambiante y complejo, se convierte en una necesidad del negocio que la auditoría realice sus actividades considerando:

- Un enfoque basado en riesgos
- La creciente importancia de las auditorías de sistemas
- La adopción de estándares internacionales

Más organizaciones están cambiando a un enfoque de auditoría basado en riesgos que está adaptado para desarrollar y mejorar el proceso de auditoría. Este enfoque es utilizado para valorar los riesgos y en base a ello apoyar la decisión del auditor de TI para efectuar pruebas de cumplimiento o sustantivas.

En este enfoque los auditores no solamente se fundamentan en los riesgos sino además en los controles, tanto internos como operativos y también con el conocimiento de la naturaleza del negocio, lo que puede ayudarlos a identificar y clasificar los riesgos y permitir seleccionar el modelo de riesgo o la metodología a usar en la auditoría más adecuada. La valoración de riesgos puede ser tan simple como ponderar los riesgos asociados a TI, o tan compleja como la ponderación elaborada basada en la naturaleza del negocio y la criticidad del riesgo de TI.

Un enfoque de auditoría basado en riesgos puede considerar lo siguiente:

#### *Recopilación de Información y Planificación*

- Conocimiento del negocio
- Resultados de auditorías de años anteriores
- Información financiera vigente
- Estatutos regulatorios
- Evaluaciones de riesgo inherente

#### *Entendimiento del control interno*

- Ambiente de control
- Procedimientos de Control
- Evaluación de riesgo de detección
- Evaluación de riesgo de control
- Calculo de riesgo total

#### *Realización de Pruebas de Cumplimiento*

- Comprobar las políticas y los procedimientos

- Realizar pruebas de confiabilidad, prevención de riesgos y adherencia a políticas y procedimientos de la organización

#### *Realización de Pruebas sustantivas*

- Procedimientos analíticos
- Otros procedimientos sustantivos de auditoría

#### *Conclusión de la Auditoría*

- Desarrollar recomendaciones
- Redactar el informe de la auditoría

### **3.1.2 Fundamentos de la Auditoría Basada en Riesgos en la Banca**

Las Normas Internacionales para el Ejercicio Profesional de la Auditoría Interna, en la sección de Normas de Desempeño, 2010 – Planificación indica “*El director ejecutivo de auditoría debe establecer un plan basado en riesgos, a fin de determinar las prioridades de la actividad de auditoría interna*”, para ello se debe tener en cuenta el enfoque de gestión de riesgos de TI en la que se incluyan los niveles de aceptación de riesgo establecido por la organización. Una vez definido, debe generar la planeación individual de auditoría basada en riesgos.

El llevar a cabo auditorías basadas en riesgos de TI también requiere la evaluación de la efectividad y eficiencia en los procesos, procedimientos y los controles existentes en los Sistemas de Información.

### **3.1.3 Aplicación de la Auditoría Basada en Riesgos**

Existen diversos métodos para el análisis de los riesgos que plantean una metodología de evaluación que distinga tanto amenazas y vulnerabilidades. Entre los métodos que se utilizan están los de análisis cualitativos y cuantitativos. Los métodos cuantitativos, cuando se los puede aplicar, ofrece un mayor nivel de objetividad. Sin embargo, la carencia de datos generalmente no permite su aplicación y es ahí cuando es necesario recurrir al análisis cualitativo.

Para permitir una eficiente gestión del riesgo, es más importante identificar correctamente las causas que ocasionan el riesgo que disponer de datos "exactos" sobre los riesgos en sí, las cuales influyen sobre su aumento o reducción, tanto del lado de las amenazas como del lado de las vulnerabilidades.

Los métodos cuantitativos para el cálculo de riesgo implican generalmente el uso de análisis estadísticos y probabilísticos para determinar la probabilidad de ocurrencia de los fenómenos, la vulnerabilidad de los elementos en riesgo y el riesgo inducido.

En el análisis de riesgos, la aplicación de métodos cualitativos implica el conocimiento exacto de amenazas, de los elementos en riesgo y sus vulnerabilidades, pero expresados de manera cualitativa, es decir, basados en la experiencia. Las probabilidades de ocurrencia de los eventos peligrosos son estimaciones que partiendo de la experiencia de los expertos, las vulnerabilidades y el riesgo son determinados también de forma relativa.



### 3.2 Fases de una Auditoría Basada en Riesgos de TI

Al igual que cualquier otra actividad de auditoría, el proceso de Auditoría Basada en Riesgos de TI está constituido por una serie de pasos, cada una de los cuales es fundamental para la consecución del siguiente, permitiendo al auditor dimensionar el tamaño y características del área a auditar y así poder llegar a emitir su propio criterio sobre los proceso, sistemas o infraestructura tecnológica.

De manera general el proceso de Auditoría Basada en Riesgos de TI se resume en las siguientes fases: Planificación Basada en Riesgos, Ejecución, Comunicación de Resultados y Seguimiento que se muestra en el cuadro No. 6.

Cuadro No. 6. Etapas de la Auditoría Basada en Riesgos de TI

<b>ETAPA</b>	<b>OBJETIVO</b>	<b>RESULTADO</b>
<b>PLANIFICACIÓN BASADA EN RIESGOS</b>	Comprender los objetivos del negocio y de TI en el que se ha de realizar la auditoría, así como los riesgos relacionados con las TI y controles asociados.	Plan de Auditoría
<b>EJECUCIÓN</b>	Obtener elementos de Juicio, a través de la aplicación de los procedimientos planificados	Evidencias/Hallazgos
<b>COMUNICACIÓN DE RESULTADOS</b>	Desarrollar el informe de auditoría y dar seguimiento y control de las acciones propuestas	Informe de Auditoría

Continúa ➡

---

<b>SEGUIMIENTO</b>	Dar seguimiento a las recomendaciones emitidas de acuerdo a los hallazgos encontrados en la fase de ejecución	Informe de Seguimiento
--------------------	---	------------------------

---

### **3.2.1 Planeación de la Auditoría Basada en Riesgos de TI**

#### **Planeación Anual**

En la Planeación de la ABR se debe considerar que se puede realizar a corto o a largo plazo y por lo menos una vez al año debido a que es necesario tomar en consideración el análisis de cambios dentro del ambiente de riesgos ya sea en las tecnologías de información, en los procesos, en las técnicas mejoradas de evaluación, así como nuevas implementaciones o actualizaciones de los controles existentes, los resultados obtenidos del análisis de cambios pueden modificar la planeación, deben ser revisados por la dirección, aprobados por el comité de auditoría y comunicados a los niveles de gerencia importantes.

#### **Auditoría Individual**

Basados en la Planeación Anual de la Auditoría en la asignación de la Auditoría Individual el Auditor de TI debe realizar la planeación de la Auditoría apropiadamente en donde debe tener un entendimiento general de los procesos del negocio, las funciones que realizan, marco regulatorio que rige al negocio, los tipos de sistemas de información, la tecnología que lo soporta, los riesgos a los que está expuesto y sus controles entre otros.

Bajo este contexto el presente estudio se enfoca en la auditoría individual basada en los riesgos tecnológicos.

### **3.2.1.1 Actividades de la Fases de la Planeación de ABR de TI**

El proceso de planeamiento o planificación es el primer paso necesario para realizar auditorías, que permiten al auditor de TI obtener los datos o información necesarios para comprender e identificar los procesos del negocio y de mayor riesgo soportados por las tecnologías de información.

Se basa en el conocimiento de la actividad de la entidad a ser auditada, debiendo estar adecuadamente planificada para llegar al objetivo de la auditoría y así 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.

Las normas de Auditoría de TI de ISACA requieren que el auditor de TI planee el trabajo de auditoría de SI para alcanzar los objetivos de auditoría y cumplir con las normas profesionales de auditoría aplicables (Planeación S5). El auditor del TI debe desarrollar un plan de auditoría que tome en consideración los objetivos del auditado relevante al área auditada y a su infraestructura tecnológica. Si es necesario, el auditor de TI debería también considerar el área bajo revisión y su relación con la organización (estrategia, financiera y/u operativa) y obtener información sobre el plan estratégico, incluyendo al plan estratégico de TI. El auditor de TI debería tener un entendimiento de la arquitectura de la tecnología de la información y de la dirección tecnológica del auditado para diseñar un plan apropiado para la

tecnología actual y donde aplique, para la tecnología futura del auditado.  
(ISACA, 2009)

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, su información, sistemas, e infraestructura tecnológica las mismas que se pueden resumir en las siguientes fases:

### **3.2.1.2 Comprensión de Objetivos y procesos de negocio relacionados**

En esta fase al planificar una auditoría basada en riesgos de TI, el auditor lo primero que requiere es obtener información general de la entidad a ser auditada con el fin de tener una comprensión total sobre el modelo de negocio, que incluye los objetivos de la entidad y la forma en que los procesos del negocio se estructuran para lograr los objetivos que implica:

Identificar

- La Cadena de Valor
- Los procesos de la organización (mapas de procesos, indicadores KPI)

Comprender

- La visión, misión, valores y metas
- Los objetivos organizativos (estratégicos, operativos, de elaboración de informes y de cumplimiento).
- Estrategias, servicios, clientes entre otros.

Incluye también, el entendimiento de las tecnologías de información a través de la identificación

- De los objetivos de tecnología para evaluar su alineación con los objetivos del negocio
- De los procesos de TI, los procedimientos operativos asociados y la tecnología que soportan cada uno de los procesos del negocio

En este sentido los pasos que el auditor puede seguir para tener un entendimiento del área de TI son:

- Revisar los Planes estratégicos de TI
- Revisar los aportes anteriores o informes relacionados con TI (provenientes de auditorías externas o internas o revisiones específicas tales como revisiones regulatorias)
- Identificar las regulaciones específicas aplicables a TI
- Identificar las funciones de TI o las actividades relacionadas que han sido contratadas externamente

### **3.2.1.3 Análisis de riesgo**

#### *Identificación de Objetivos y Riesgos de TI*

En base a la identificación de los objetivos del negocio y los procesos claves correspondientes, el auditor de TI realiza la identificación de los riesgos relevantes de TI que podrían impedir la consecución de los objetivos del negocio ya sean de origen interno como externo parte fundamental que le permite al auditor comprender los riesgos que la entidad tendrían que afrontar.

### *Evaluación del Riesgo de TI*

En esta fase el Auditor debe realizar la evaluación de los riesgos de TI que podría impedir el cumplimiento de los objetivos del negocio mediante la utilización de un modelo de riesgos que determine las categorías y tipos de riesgos esto ayudará al auditor a identificar los riesgos que se consideren como más sensibles o críticos para cada objetivo estratégico y que podrían afectar a la entidad a ser auditada, evaluados en términos de probabilidad de ocurrencia y de impacto.

La evaluación de los riesgos se debe realizar considerando y evaluando si ya existe un modelo de riesgos generado como parte de la gestión de riesgos y dependiendo del grado de madurez, en caso de existir el auditor deberá complementar en la medida de lo necesario para concluir el plan.

### *Análisis de Procesos y Riesgos*

Es la fase en la que el auditor realiza un análisis del proceso y de los riesgos de TI en donde determina si existe una asociación entre el riesgo y el proceso de manera directa o indirecta. El resultado del análisis obtenido permite al auditor determinar la clasificación y priorización de los procesos a ser auditados que tengan mayor exposición al riesgo basándose en la identificación de los riesgos críticos e importantes, y en los ciclos de revisión, punto de partida para realizar el plan de auditoría basada en riesgos de TI.

#### **3.2.1.4 Efecto de las Leyes y Regulaciones sobre la planificación de ABR**

Dada la importancia y dependencia de las tecnologías de información en una entidad, en la auditoría a los sistemas de información deben revisar leyes y

regulaciones que se aplican en la entidad a ser auditada como son, políticas de la gerencia sobre privacidad para determinar si toman en cuenta los requisitos legales y regulatorios de privacidad aplicables.

Bajo este antecedente los pasos que seguirá el auditor de TI para determinar el nivel de cumplimiento de una entidad con los requisitos externos se podrían resumir en:

- Identificar los requisitos gubernamentales u otros externos relevantes que se refieren a:
  - Datos electrónicos, datos personales, derechos de autor, comercio electrónico, firmas digitales, etc.
  - Prácticas y controles de sistemas de información
  - La manera en que se almacenan los programas y datos
  - La organización
  - Las actividades de los servicios de tecnología de información
  - La auditoría de SI
- Documentar las leyes y regulaciones pertinentes
- Determinar si la gerencia de la organización y la función de los SI han tomado en consideración los requisitos externos relevantes al realizar planes y a fijar normas y procedimientos, así como también funciones de aplicación del negocio.
- Revisar los documentos internos del departamento/función/actividad de SI que se ocupan del cumplimiento de las leyes aplicables a la industria.
- Determinar el cumplimiento con los procedimientos establecidos que se ocupan de estos requisitos.

- Determinar si hay procedimientos instalados para asegurar que los controles o acuerdo con proveedores externos de servicios de TI reflejen cualquier requisito legal relacionado con las responsabilidades.

### **3.2.1.5 Llevar a cabo revisión de los controles internos relacionados con TI**

En la auditoría de TI el auditor debe tener en consideración los controles existentes en los procesos relacionados con las TI en la entidad a auditar, existiendo dos aspectos claves que deberían ser considerados al evaluar la fortaleza de un control pudiendo ser de prevención, detección y corrección de acuerdo a su naturaleza.

Cada procedimiento de un sistema de información debería contar con controles contruidos en el mismo para todas sus funciones sensibles o críticas entre los que podría incluir:

- Estrategia y dirección
- Organización general y gestión
- Acceso a los recursos de TI, incluyendo datos y programas
- Metodologías de desarrollo de sistemas y control de cambios
- Procedimientos de operación
- Programación de sistemas y funciones de soporte técnico
- Procedimientos de aseguramiento de calidad
- Controles de acceso físico
- Planeación de continuidad del negocio/recuperación ante desastres
- Redes y comunicaciones
- Administración de base de datos



- Protección y mecanismos de detección contra ataques internos y externos.

Con estas consideraciones, el auditor de TI debe entender los controles que existen para todas sus funciones y procedimientos y cómo aplicarlos en la planeación de auditoría.

### 3.2.1.6 Definición del Plan de Auditoría Basada en Riesgos de TI

En esta etapa tras la revisión preliminar realizada de acuerdo a lo mencionado en los ítems anteriores, se desarrolla el plan de Auditoría el mismo que contienen la estrategia que se debe seguir para la ejecución de la auditoría, que comprende el establecimiento de objetivos, tiempo, plazo, responsabilidades, recursos, procedimientos y costos del proceso.

El Plan de ABR de TI por lo general puede contener los siguientes puntos:

Cuadro No. 7. Actividades de Planificación de Auditoría

Actividades de Auditoría	Descripción de la Actividad
Diagnóstico General	Incluye diversos aspectos considerados durante la planeación de la auditoría como es descripción y fines de la entidad.
Objetivo de la Auditoría	Detalla la razón u origen de ser de la auditoría
Alcance y Metodología de la Auditoría	Describe la extensión del trabajo a realizar para cumplir con el objetivo de Auditoría y el periodo objeto de examen
Documentación Aplicable	Se explica la existencia de Manuales, normas y normativa legal
Identificación del equipo de Auditoría	Incluye el equipo de auditores que llevarán a cabo el proceso de auditoría
Costo y cronograma de actividades	Define el costo de la auditoría y el cronograma de actividades que se efectuará.
Fecha de realización y Horario	Define el tiempo de ejecución de la auditoría

Continúa ➡

---

Áreas y Procesos críticos a Auditar	Efectúa la descripción de los asuntos más importantes identificados en la fase de planeación
-------------------------------------	--

---

Definido y concluido el Plan de auditoría el auditor de TI da inicio a la fase de ejecución de la ABR de TI

### **3.2.2 Ejecución de la ABR de TI**

En la etapa de ejecución el objetivo primordial es obtener y analizar toda la información posible del proceso que se audita, con el fin de obtener evidencias suficientes, adecuadas e importantes, es decir, se debe contar con todos o gran parte de elementos que permitan al auditor establecer conclusiones fundadas en el informe acerca de las situaciones analizadas en sitio, que entre otras deben incluir:

- 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.

En esta etapa se debe dar cumplimiento a las Normas que regulan la actividad de ejecución del trabajo en auditoría las que en general señalan que los auditores internos deben:

- Obtener, identificar, analizar y registrar suficiente información de manera tal que les permita cumplir con los objetivos del trabajo.

- Contar con suficiente información, la que tiene que ser de carácter confiable, relevante y útil de manera que permita alcanzar los objetivos del trabajo.
- Basar sus conclusiones y los resultados del trabajo en adecuados análisis y evaluaciones.
- Registrar información relevante que les permita soportar las conclusiones y los resultados del trabajo. Los registros que contienen dicha información deben ser controlados y custodiados mediante políticas y procedimientos que regulen el acceso y conocimiento por terceros a la organización.
- Supervisar adecuadamente la ejecución de la auditoría, para asegurar el desarrollo profesional del personal, el logro de los objetivos y la calidad del trabajo.

### **3.2.2.1 Planificación de la Ejecución de la Auditoría**

Una vez que se tiene el programa de auditoría elaborado, aprobado, socializado y los equipos auditores conformados, comienza la ejecución de la auditoría, realizando las siguientes actividades previas:

- Elaboración y registro de plan de auditoría
- Asignación de tareas al equipo auditor
- Preparación de los documentos de trabajo

Posterior a esto, se inicia la auditoría como tal.

### **3.2.2.2 Actividades de ejecución de la Auditoría**

#### **1. *Recolección de la información***

Se debe acudir a las diversas fuentes de información utilizando varias técnicas de recopilación como entrevistas, documentación de auditorías anteriores, manuales.

## 2. *Determinación de los hallazgos*

La evidencia de auditoría es la información que tiene el auditor para extraer conclusiones en las cuales sustenta su opinión de manera objetiva y verifica el cumplimiento o incumplimiento.

Una evidencia es competente y suficiente si cumple con ser:

- Relevante
- Auténtica
- Verificable
- Neutral

Se debe considerar lo siguiente al determinar los hallazgos de auditoría:

- Registros y conclusiones de auditorías previas
- Requerimientos de la Institución
- Hallazgos que pueden ser mejorables
- El tamaño de la muestra, lo que puede o no ser significativo
- Categorizar los hallazgos

Estas pueden ser categorizadas en:

1. No conformidades.- en caso de incumplimiento de un requisito de una norma de un sistema de gestión
2. Desviaciones.- incumplimiento puntual.
3. Observaciones.- cuando cumpliendo los requisitos, el auditor ve una oportunidad de mejora.

El hallazgo de auditoría debe tener los siguientes atributos:

*Condición.-* se refiere a situaciones reales encontradas, es decir, lo que es

*Criterio.-* son las normas que se aplicarán, por tanto se refiere a lo que debería ser.

*Causa.-* se refiere a la razón del por qué sucedió, es la causa fundamental por la cual sucedió la condición.

*Efecto.-* Es la consecuencia real o potencial que podría ocasionar. Con esta se pueden dar recomendaciones para corregir las condiciones.

### 3. *Determinación de Niveles de Riesgo*

Es el resultado de confrontar el impacto y la probabilidad con los controles existentes en los diversos procesos y procedimientos.

Estos niveles de riesgo pueden ser:

- Alto
- Medio
- Bajo

Y son graficados en la matriz de riesgos que permitirá tomar decisiones adecuadas para controlar los riesgos existentes.

### 4. *Elaboración del informe preliminar*

El informe de auditoría es el producto que presenta el Auditor. La importancia del mismo se mide por la calidad de los hallazgos, conclusiones y recomendaciones.

El informe de auditoría puede tener la siguiente estructura:

- Presentación del Auditor
- Ficha de identificación del auditor
- Contenido
  - Resumen ejecutivo
  - Informe
    - Introducción
    - Antecedentes
    - Objetivo específico
    - Objetivo generales
    - Alcance
  - Criterios de revisión
  - Análisis situacional
    - Observaciones
    - Conclusiones y recomendaciones
- Observaciones Finales
- Anexos

##### 5. *Documentación de la Auditoría Basada en Riesgos*

La Documentación de la Auditoría es la evidencia requerida que soporta las conclusiones alcanzadas por el auditor, que tiene que ser clara, completa, recuperable y comprensible, la misma que es de propiedad de la entidad de auditoría y es accesible solo por el personal autorizado bajo permiso específico o general. En caso

de que sea solicitada por personas externas, el auditor debe tener previa aprobación de la alta dirección.

Dicha documentación también debe contener información que es solicitada por leyes y regulaciones, estipulaciones contractuales y normas profesionales.

“El contenido que puede incluir la documentación de auditoría se resume en:

- La planeación y preparación del alcance y objetivos de la auditoría
- La descripción y/o recorridos del área de auditoría vista
- El programa de auditoría
- Los pasos de auditoría realizados y la evidencia de auditoría recopilada
- El uso de servicios de otros auditores y expertos
- Los hallazgos, conclusiones y recomendaciones de auditoría
- La documentación de auditoría relacionada con la identificación y fechas de documentos
- Copia del informe emitido como resultado del trabajo de auditoría
- Evidencia de revisión supervisora de auditoría” (ISACA, 2010)

La documentación de auditoría de acuerdo a la debida diligencia y las mejores prácticas requieren que estén fechados, inicializados, numeradas sus páginas, relevantes, claros, completos, auto contenidos y debidamente etiquetados, archivados y mantenidos en custodia, siendo responsabilidad del auditor mantener la integridad y la protección de la evidencia de prueba de la auditoría para preservar su valor de prueba en soporte de los resultados de auditoría.

En lo que respecta a la custodia de la información el auditor debe elaborar políticas, referente a requisitos de retención y liberación de la documentación, con la finalidad de garantizar la seguridad de la documentación de la auditoría realizada.

### **3.2.3 Comunicación de los resultados de la ABR de TI**

El auditor debe resumir los resultados del trabajo final de la auditoría después de finalizar el proceso de ejecución en donde comunicará los resultados obtenidos a los distintos niveles de la alta dirección, mediante la elaboración de un informe por medio del cual expondrá sus hallazgos, recomendaciones y conclusiones, con las siguientes consideraciones:

- Que los hechos presentados en el informe sean correctos
- Que las recomendaciones sean realistas y rentables, en caso de no serlo buscar alternativas negociando con la gerencia de la entidad auditada
- Proponer fechas de implementación para las recomendaciones acordadas

Se debe considerar que antes de que de que el auditor comunique los resultados obtenidos a la alta dirección, deberá discutir sobre los hallazgos con el personal directivo de la entidad auditada, con la finalidad de llegar a un acuerdo sobre los hallazgos encontrados y desarrollar un planteamiento de acción correctiva.

En caso de estar de acuerdo la entidad auditada, la gerencia de auditoría de TI debería enviar un corto resumen a la alta dirección de la entidad, caso contrario el auditor debería profundizar sobre la importancia del hallazgo, los riesgos y efectos de no corregir las debilidades de control.



Para la elaboración del informe del auditor de TI no existe un formato específico, dependerá de las políticas y los procedimientos de auditoría de la entidad pero usualmente tendrán el contenido y estructura siguiente:

Cuadro No. 8. Formato de Informe de auditoría

<b>CONTENIDO</b>	<b>DESCRIPCIÓN</b>
Introducción al Informe	Incluye: <ul style="list-style-type: none"> <li>- La declaración de los objetivos, limitaciones y alcance de la auditoría</li> <li>- El periodo cubierto por la auditoría,</li> <li>- Un detalle general sobre el carácter y la extensión de los procedimientos de auditoría efectuados</li> <li>- Los procesos examinados durante la auditoría</li> <li>- Declaración de la metodología de ABR y lineamientos seguidos</li> </ul>
Hallazgos de la Auditoría	Especifica los hallazgos detallados encontrados durante la fase de ejecución de la auditoría, dependiendo del auditor incluirá en el informe los hallazgos específicos, con base a la importancia de los hallazgos y los destinatarios proyectados del informe de auditoría.
Conclusiones y la opinión general del Auditor	Incluye las conclusiones y opiniones del auditor respecto a si los controles y procedimientos examinados durante la auditoría son los adecuados así como los riesgos potenciales identificados como consecuencia de las deficiencias detectadas
La reserva o calificación del auditor de TI con relación a la auditoría	Se refiere a la calificación de los controles existentes en donde el auditor indica que los controles o procedimientos examinados son adecuados o inadecuados. Toda conclusión debe estar debidamente respaldada.
Recomendaciones de la Auditoría	Son las recomendaciones que el auditor realiza sobre los controles a que se deben implantar con la finalidad de mejorar el sistema de control interno de la entidad.

Cabe recalcar que en el informe de auditoría no solo describe los aspectos negativos en términos de hallazgos sino también comentarios sobre controles y procesos en perfeccionamiento o sobre controles efectivos ya existentes.

Antes de concluir el Informe el Auditor de TI deberá discutir las recomendaciones y las fechas planeadas de implementación, considerando las restricciones diversas, tales como limitaciones del personal, presupuestos u otros proyectos que pueden impedir la implementación inmediata, por eso es importante obtener un compromiso por parte de la entidad auditada sobre la fecha en que el plan de acción será implementado y la manera en que se llevará a cabo.

Es obligación de la auditoría de TI realizar el seguimiento de las recomendaciones u observaciones emitidas en el informe, para ello debe contar con un programa de seguimiento con la finalidad de poder verificar si la entidad auditada ha implementado las acciones correctivas acordadas, dicho seguimiento dependerá de la criticidad de los hallazgos y los resultados obtenidos del proceso de seguimiento deben ser comunicados a los niveles apropiados de la gerencia.

## **4 CAPITULO IV**

### **Desarrollo de la Guía de Auditoría Basada en Riesgos para TI en la Banca Pública.**

En el presente Capítulo se desarrollará la guía de auditoría basada en riesgos para TI en la Banca Pública, el mismo que servirá al auditor como referencia para realizar auditorías basadas en riesgos de TI.

Permitirá al auditor entre otros aspectos identificar los riesgos a los que se encuentra expuesta la entidad, identificar los controles que se encuentran implementados, si son eficientes así como también los cumplimientos regulatorios emitidos por los organismos de control.

Mediante la guía de auditoría, 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 permitirá al auditor emitir las sugerencias y recomendaciones para que se optimicen o implementen los controles necesarios, con el objetivo de mejorar la eficiencia de su infraestructura y sistemas tecnológicos y así lograr un alto grado de integridad, disponibilidad, confidencialidad, confiabilidad de su 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 de acuerdo a lo explicado en el capítulo anterior:

- PLANIFICACIÓN BASADA EN RIESGOS

- EJECUCIÓN
- COMUNICACIÓN DE RESULTADOS
- SEGUIMIENTO

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:



Figura No. 12. Fases de la Auditoría Basada en Riesgos de TI en la Banca Pública.

## 1 FASE 1: Planificación Individual

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

### 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 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

## Desarrollo de la Guía

### 1.1 Investigación Preliminar

#### 1.1.1 Comprensión general de la entidad y los aspectos fundamentales

Cuadro No. 1. 1 Comprensión general de la entidad y los aspectos fundamentales

---

#### *Fase 1: Planificación Inicial*

Actividad A1.1: Investigación Preliminar

Tarea T1.1.1: Comprensión general de la entidad y los aspectos fundamentales

#### **Objetivo:**

Obtener conocimiento general de la entidad a ser auditada

- Recopilar la información necesaria que permita tener un entendimiento general de la entidad.
- Conocimiento de la misión, visión, metas, objetivos, productos o servicios
- Conocimiento del ambiente legal y normativo en el que opera la entidad.

#### **Productos de Entrada**

- Plan Operativo Institucional.
- Estructura Organizacional.
- Políticas
- Base legal
- Normas
- Productos y Servicios

#### **Productos de salida**

- Entendimiento de Normativas Aplicadas. (Ver anexo No. 9).
- Entendimiento general de la entidad. (Ver anexo No. 10).
- Entendimiento general de los procesos o servicios del negocio.
- Entendimiento de la Situación actual de la organización.

#### **Técnicas, prácticas y pautas**

- Reuniones de trabajo (Ver anexo No. 6).
- Entrevistas. (Ver anexo No. 7).
- Observación (Ver anexo No. 8).

---

Continúa ➡

- Solicitud de Información

#### ***Base Normativa***

N/A

#### ***Participantes***

- Director General
- Personal directivo seleccionado de la Entidad

#### ***Acción a seguir***

- El auditor, en base a la información recopilada de la entidad, debe realizar una revisión y análisis de la misma, para tener una comprensión general de la organización, su estructura y proceso del negocio relacionado y situación actual en que se encuentra la organización.
- Debe visualizar el contexto general del área donde se desenvuelve la auditoría.
- Debe también tener un entendimiento general del ambiente legal y normativo en el que opera el negocio.

### **1.1.2 Comprensión general del área de TI y procesos relacionados**

Cuadro No. 1. 2 Comprensión general del área de TI y procesos relacionados objeto de la auditoría

#### ***Fase 1: Planificación***

Actividad A1.1: Investigación Preliminar

Tarea T1.1.2: Comprensión general del área de TI y procesos relacionados objeto de la auditoría

#### ***Objetivo:***

- Reunir la información necesaria que permita conocer con un grado de detalle apropiado el área de TI, los objetivos, estrategia, planes, sus funciones, estructura, recurso humano, la normativa vigente y los procesos del negocio relacionados.
- Reunir la información necesaria que permita conocer la infraestructura tecnológica, aplicaciones, arquitectura, recurso técnico, proveedores y otros.
- Reunir la información necesaria acerca de los procesos a auditar.

Continúa ➡

- Reunir la información necesaria acerca de las actividades a evaluar.

#### ***Productos de Entrada***

- Plan Estratégico de Tecnología de Información (PETI)
- Estructura del Área de TI (Organigrama, Asignación de responsabilidades)
- Competencias del personal técnico
- Contratos con proveedores de TI
- Presupuesto Tecnológico
- Regulaciones específicas aplicadas a TI
- Plan Operativo
- Infraestructura
- Aplicaciones
- Servicios de TI
- Antecedentes de Informes de la Auditoría Interna del Organismo, si la tuviere o de informes anteriores emitidos por la Auditoría General
- Evaluación de Riesgo (Si cuenta con un sistema/método de evaluación de riesgos)
- Inventario de políticas y normas establecidas para TI, incluyendo el Comité de Tecnología

#### ***Productos de salida***

- Conocimiento general del área de TI. (Ver anexo No. 11)
- Comprensión suficiente del ambiente total que se revisará o auditará, lo que incluye:
  - Comprensión general de políticas que se aplican
  - Diseño conceptual
  - Niveles de seguridad
  - Uso de comunicaciones para la gestión de información
  - Tipos de sistemas de información
  - Gestión de los servicios tecnológicos
- Estado general del proceso objeto de la auditoría su situación dentro del área de TI
- Resumen de situación actual del proceso a auditar
- Documentación de la actividad realizando un registro de acuerdo a los



aspectos más relevantes encontrados en papeles de trabajo

***Técnicas, prácticas y pautas***

- Reuniones de trabajo
- Entrevistas
- Observaciones de lugares físicos o instalaciones a auditar
- Análisis y revisión documental

***Base Normativa***

N/A

***Participantes***

- Director de TI
- Gerencia de TI
- Miembros del comité de tecnología/planeación/dirección de la función de servicios de información
- Oficial de Seguridad

***Acción a seguir***

- En base a la información recopilada debe verificar si existe la información solicitada, si es o no necesaria, si está formalmente aprobada y la fecha de su última actualización.
- Debe realizar un análisis preliminar revisando la información obtenida y en caso de no existir lo requerido se debe hacer el análisis mediante técnicas de observación y entrevistas.
- Debe revisar los Informes de auditoría realizados anteriormente, que le puedan proveer información de utilidad para la identificación de problemas potenciales, sobre los siguientes aspectos:
  - Observaciones y recomendaciones
  - Áreas y procesos críticos examinados
  - Implantación de medidas correctivas
  - Recomendaciones importantes pendientes de implantación
  - Identificación de áreas no auditadas.
- Si la entidad, cuenta con un sistema/método de evaluación de riesgos debe revisar y validar si dicha información le ayudarán a identificar áreas críticas y posibles riesgos que aún no han sido mitigados.

## 1.2 Identificación de Riesgos

### 1.2.1 Identificar y clasificar lo activos

#### Cuadro No. 1. 3 Identificar y clasificar los activos

---

#### ***Fase 1: Planificación***

Actividad A1.1: Identificación de Riesgos

Tarea T1.2.1: Identificar y clasificar los activos

#### ***Objetivos***

- Identificar los activos de información relevantes, para determinar su sensibilidad y criticidad
- Obtener la clasificación de los activos de información de acuerdo a sus características y atributos
- En caso de que la entidad no disponga de un proceso formal de gestión de riesgos, obtener la información necesaria que le permita al auditor realizar un análisis de riesgos para identificar áreas de mayor exposición

#### ***Productos de entrada***

- Resultados de la Tarea T1.1.1: Comprensión general del área de TI y procesos relacionados objeto de la auditoría
- Inventario de procesos tecnológicos
- Matrices de riesgo que la entidad disponga

#### ***Productos de salida***

- Lista de procesos del negocio relacionados con los activos y su importancia. (Ver anexo No. 12)
- Categorización de los activos de información
- Procesos o áreas críticas o de mayor exposición
- Documentación de la actividad realizando un registro de acuerdo a los aspectos más relevantes encontrados

#### ***Técnicas, prácticas y pautas***

- Documentación existente
- Reuniones
- Metodología Delphi

---

Continúa ➡

***Base Normativa.***

- Libro I.- Normas generales para la aplicación de la ley general de instituciones del sistema financiero; Título X.- De la gestión y administración de riesgos; Capítulo V.- De la gestión del riesgo operativo, emitido por la Superintendencia de Bancos y Seguros de la República del Ecuador.
- Libro I.- Normas generales para la aplicación de la Ley General de Instituciones del Sistema Financiero; Título XXI.- De las calificaciones otorgadas por la Superintendencia de Bancos y Seguros; Capítulo III.- Normas para la calificación de las firmas calificadoras de riesgo de las instituciones del sistema financiero.
- Normas 410 de auditoría interna para Tecnología de la Información.

***Participantes***

- Gerente de TI
- Analista de Riesgo
- Oficial de Seguridad de la Información

***Acción a seguir***

- En base a la información recopilada, debe identificar los activos de información relevantes para la organización, como son:
  - La información
  - Los servicios
  - Las aplicaciones informáticas
  - Los equipos informáticos
  - Las redes de comunicaciones
  - Las instalaciones
  - Las personas
  - Servicios de proveedores externos.
  - Soportes de información.
- Debe clasificar y agrupar los activos de información (Nombre del Activo y Nombre del Procedimiento) de acuerdo a sus características e importancia
- Finalmente debe categorizar de acuerdo a la dependencia y relación existente entre ellos

## 1.2.2 Identificación de amenazas.

### Cuadro No. 1. 4. Identificación de amenazas

#### *Fase 1: Planificación*

Actividad A1.1: Identificación de Riesgos

Tarea T1.2.2: Identificación de amenazas

#### *Objetivos*

- Identificar las amenazas relevantes que puedan afectar o causar daño a los principales activos de información
- Identificar las amenazas relevantes considerando los factores internos o externos que puedan afectar los objetivos de la organización
- Validar las amenazas identificadas por la entidad que puedan afectar a los activos de información
- Identificar el tipo de amenaza y su origen

#### *Productos de entrada*

- Resultados de la Tarea: T 1.2.1 Identificar y clasificar los activos
- Catálogo de amenazas posibles sobre los activos de información
- Información disponible de antecedentes de amenazas de la organización

#### *Productos de salida*

- Identificación de amenazas posibles que afectan a los activos de información de la organización, de acuerdo al tipo y origen
- Descripción y documentación de amenazas identificadas. (Ver anexo No. 13)

#### *Técnicas, prácticas y pautas.*

- Catálogo de Amenazas (Magerit) (**Ministerio de Hacienda y Administraciones Públicas, 2012**)
- Entrevistas
- Reuniones de trabajo
- Método Delphi

#### *Base Normativa.*

- Libro I.- Normas generales para la aplicación de la ley general de instituciones del sistema financiero; Título X.- De la gestión y administración de riesgos;

Continúa ➡

Capítulo V.- De la gestión del riesgo operativo, emitido por la Superintendencia de Bancos y Seguros de la República del Ecuador.

- Libro I.- Normas generales para la aplicación de la Ley General de Instituciones del Sistema Financiero; Título XXI.- De las calificaciones otorgadas por la Superintendencia de Bancos y Seguros; Capítulo III.- Normas para la calificación de las firmas calificadoras de riesgo de las instituciones del sistema financiero.
- Normas 410 de auditoría interna para Tecnología de la Información.

### ***Participantes***

- Gerente de TI
- Analista de Riesgo
- Oficial de Seguridad de la Información

### ***Acción a seguir***

- El auditor debe identificar/validar las amenazas más significativas que considere, de acuerdo a su experiencia o con la ayuda de un catálogo de amenazas, considerando:
  - El tipo de activo
  - La dimensión en que el activo es valioso
  - La experiencia de la Organización
- Para cada amenaza sobre cada activo de información debe registrar la siguiente información:
  - Descripción de la Amenaza
  - Deducción de la amenaza, es decir cómo fue identificada (entrevistas, reuniones, experiencia de la organización, etc.)
  - Antecedentes si fuera el caso de la misma organización o externos.

## **1.2.3 Identificación de vulnerabilidades**

### **Cuadro No. 1. 5 Identificación de vulnerabilidades**

#### ***Fase 1: Planificación***

Actividad A1.1: Identificación de Riesgos

Tarea T1.2.3: Identificación de Vulnerabilidades

Continúa ➡

**Objetivos**

Identificar posibles fallas o vulnerabilidades existentes en los activos de información de la organización que pueden ser causa del aprovechamiento de una amenaza.

**Productos de entrada**

- Resultados de la Tarea: T 1.2.1 Identificar y clasificar los activos
- Identificación de vulnerabilidades posibles sobre los activos de información
- Información disponible de antecedentes de vulnerabilidades de los activos de información de la organización

**Productos de salida**

- Identificación de vulnerabilidades que afectan a los activos de información de la organización, de acuerdo al tipo y origen
- Identificación de vulnerabilidades agrupadas por aspectos relevantes de seguridad
- Descripción y documentación de vulnerabilidades identificadas. (Ver anexo No. 13)

**Técnicas, prácticas y pautas**

- Entrevistas
- Reuniones de trabajo
- Método Delphi

**Base Normativa**

- Libro I.- Normas generales para la aplicación de la ley general de instituciones del sistema financiero; Título X.- De la gestión y administración de riesgos; Capítulo V.- De la gestión del riesgo operativo, emitido por la Superintendencia de Bancos y Seguros de la República del Ecuador.
- Libro I.- Normas generales para la aplicación de la Ley General de Instituciones del Sistema Financiero; Título XXI.- De las calificaciones otorgadas por la Superintendencia de Bancos y Seguros; Capítulo III.- Normas para la calificación de las firmas calificadoras de riesgo de las instituciones del sistema financiero.
- Normas 410 de auditoría interna para Tecnología de la Información.

***Participantes***

- Gerente de TI
- Analista de Riesgo
- Oficial de Seguridad de la Información

***Acción a seguir***

- Revisar cuidadosamente la información recopilada a fin de que pueda identificar hechos que sean causa de posibles vulnerabilidades latentes en los diferentes activos de información.
- Debe registrar la siguiente información:
  - Descripción de la vulnerabilidad
  - Deducción de la vulnerabilidad, es decir cómo fue identificada (entrevistas, reuniones, documentación, experiencia de la organización, etc.)
  - Antecedentes si fuera el caso de la misma organización o externos, de vulnerabilidades identificadas que aún existen o que ya lo han sido solventadas

**1.2.4 Determinación del Riesgo****Cuadro No. 1. 6 Determinación del Riesgo*****Fase 1: Planificación***

Actividad A1.2: Identificación de Riesgos

Tarea T1.2.4: Determinación del Riesgo

***Objetivos***

- Determinar los riesgos, asociados a cada activo de información
- Determinar el daño que puede ocurrir a causa de la materialización de una amenaza sobre una vulnerabilidad

***Productos de entrada***

- Resultado de la Tarea T1.2.2: Identificación de amenazas
- Resultado de la Tarea T1.2.3: Identificación de vulnerabilidades
- Matriz de riesgos de la entidad, en caso de existir

***Productos de salida***

Continúa 

- Lista de Riesgos identificados para cada activo de información
- Detalle del riesgo, para cada activo de información
- Matriz de Riesgos validada. (Ver anexo No. 13)

#### ***Técnicas, prácticas y pautas***

- Entrevistas
- Reuniones de trabajo
- Método Delphi

#### ***Base Normativa***

- Libro I.- Normas generales para la aplicación de la ley general de instituciones del sistema financiero; Título X.- De la gestión y administración de riesgos; Capítulo V.- De la gestión del riesgo operativo, emitido por la Superintendencia de Bancos y Seguros de la República del Ecuador.
- Libro I.- Normas generales para la aplicación de la Ley General de Instituciones del Sistema Financiero; Título XXI.- De las calificaciones otorgadas por la Superintendencia de Bancos y Seguros; Capítulo III.- Normas para la calificación de las firmas calificadoras de riesgo de las instituciones del sistema financiero.
- Normas 410 de auditoría interna para Tecnología de la Información.

#### ***Participantes***

- Gerente de TI
- Analista de Riesgo
- Oficial de Seguridad de la Información

#### ***Acción a seguir***

- Analizar cuidadosamente las amenazas y vulnerabilidades levantadas en función de cada activo de información
- Identificar posibles riesgos para cada activo de información
- Registrar la lista de riesgos y su detalle
- Elaboración de Matriz de Riesgos



### 1.3 Evaluación de Riesgos

#### 1.3.1 Evaluación de la Probabilidad

##### Cuadro No. 1. 7. Evaluación de la Probabilidad

###### ***Fase 1: Planificación***

Actividad A1.3: Evaluación de Riesgos

Tarea T1.3.1: Evaluación de la Probabilidad

###### ***Objetivos***

- Analizar la probabilidad de ocurrencia a las que se encuentran expuestas los activos de información, en base a las amenazas y vulnerabilidades
- Evaluar la probabilidad de ocurrencia a las diferentes amenazas y vulnerabilidades detectadas

###### ***Productos de entrada***

- Resultados de la Tarea T1.2.4: Determinación del Riesgo
- Resultado de la Tarea T1.2.2: Identificación de amenazas
- Resultado de la Tarea T1.1.2: Identificación de vulnerabilidades

###### ***Productos de salida***

- Estimación de la probabilidad de ocurrencia de los activos de información mediante: matriz de evaluación de riesgos y mapa de riesgos (Ver anexo No. 14)

###### ***Técnicas, prácticas y pautas***

- Entrevistas
- Reuniones de trabajo
- Método Delphi

###### ***Base Normativa***

- Libro I.- Normas generales para la aplicación de la ley general de instituciones del sistema financiero; Título X.- De la gestión y administración de riesgos; Capítulo V.- De la gestión del riesgo operativo, emitido por la Superintendencia de Bancos y Seguros de la República del Ecuador.
- Libro I.- Normas generales para la aplicación de la Ley General de Instituciones del Sistema Financiero; Título XXI.- De las calificaciones otorgadas por la Superintendencia de Bancos y Seguros; Capítulo III.- Normas para la calificación de las firmas calificadoras de riesgo de las instituciones del

Continúa ➡

sistema financiero.

- Normas 410 de auditoría interna para Tecnología de la Información.

#### ***Participantes***

- Gerente de TI
- Analista de Riesgo
- Oficial de Seguridad de la Información

#### ***Acción a seguir***

- Analizar y evaluar la probabilidad de las amenazas identificadas, en las Tareas: Identificación de Amenazas y Vulnerabilidades realizadas en el paso anterior, considerando:
  - La matriz de riesgos de la propia organización en caso de existir
  - La función que realiza cada activo de información
  - Incidentes de antecedentes de la propia organización
- Registrar en el Mapa de Riesgos la probabilidad de acuerdo a su frecuencia de ocurrencia

### **1.3.2 Evaluación del Impacto**

#### **Cuadro No. 1. 8 Evaluación del Impacto**

#### ***Fase 1: Planificación***

Actividad A1.3: Evaluación de Riesgos

Tarea T1.3.2: Evaluación del Impacto


#### ***Objetivos***

- Analizar el impacto de ocurrencia a las que se encuentran expuestas los activos de información, en base a las amenazas.
- Valorar el Impacto de ocurrencia en base del activo de información y las amenazas.

#### ***Productos de entrada***

- Resultado de la Tarea T1.2.4: Determinación del Riesgo
- Resultado de la Tarea T1.2.2: Identificación de amenazas
- Resultado de la Tarea T1.2.3: Identificación de vulnerabilidades

#### ***Productos de salida***

Continúa 

- Estimación del impacto de ocurrencia de los activos de información, mediante: matriz de evaluación de riesgos y mapa de riesgos (Ver anexo No. 14)

#### ***Técnicas, prácticas y pautas***

- Reuniones de trabajo
- Método Delphi
- Matriz de Riesgos de la Organización

#### ***Base Normativa***

- Libro I.- Normas generales para la aplicación de la ley general de instituciones del sistema financiero; Título X.- De la gestión y administración de riesgos; Capítulo V.- De la gestión del riesgo operativo, emitido por la Superintendencia de Bancos y Seguros de la República del Ecuador.
- Libro I.- Normas generales para la aplicación de la Ley General de Instituciones del Sistema Financiero; Título XXI.- De las calificaciones otorgadas por la Superintendencia de Bancos y Seguros; Capítulo III.- Normas para la calificación de las firmas calificadoras de riesgo de las instituciones del sistema financiero.
- Normas 410 de auditoría interna para Tecnología de la Información.

#### ***Participantes***

- Gerente de TI
- Analista de Riesgo
- Oficial de Seguridad de la Información

#### ***Acción a seguir***

- Analizar y valorar el impacto de acuerdo a las amenazas identificadas, en las Tareas: Identificación de Amenazas y Vulnerabilidades realizadas en el paso anterior, considerando:
  - La matriz de riesgos de la propia organización en caso de existir
  - La función que realiza cada activo de información
  - Incidentes de antecedentes de la propia organización
- Registrar en el Mapa de Riesgos el impacto que provocaría a los activos de información.

## 1.4 Comprensión del control interno

### 1.4.1 Identificar y Comprender los controles

#### Cuadro No. 1. 9 Identificar y Comprender los controles

##### ***Fase 1: Planificación***

Actividad A1.4: Comprensión del control interno

Tarea T1.4.1: Identificar y Comprender los controles

##### ***Objetivo:***

- Identificar y comprender los controles existentes y que se encuentran implementados
- Planificación de controles que permitan aumentar el valor o reducir el riesgo

##### ***Productos de Entrada***

- Matriz de Riesgos, con la identificación de los controles existentes, propia de la organización
- Plan de Mitigación de Riesgos
- Revisión de resultados de auditorías previas
- Documentación de controles

##### ***Productos de salida***

- Listado de todos los controles existentes, controles en planificación, en ejecución y su estado
- Elaboración de documento de controles. (Ver anexo No. 15)

##### ***Técnicas, prácticas y pautas***

- Reuniones de trabajo
- Entrevistas
- Informes de Auditorías internas o externas
- Documentación

##### ***Base Normativa.***

- Libro I.- Normas generales para la aplicación de la ley general de instituciones del sistema financiero; Título X.- De la gestión y administración de riesgos; Capítulo V.- De la gestión del riesgo operativo, emitido por la Superintendencia de Bancos y Seguros de la República del Ecuador.

Continúa ➡

- Libro I.- Normas generales para la aplicación de la Ley General de Instituciones del Sistema Financiero; Título XXI.- De las calificaciones otorgadas por la Superintendencia de Bancos y Seguros; Capítulo III.- Normas para la calificación de las firmas calificadoras de riesgo de las instituciones del sistema financiero.
- Normas 410 de auditoría interna para Tecnología de la Información.

### ***Participantes***

- Gerencia de TI
- Personal Técnico
- Oficial de Seguridad

### ***Acción a seguir***

En base a la información obtenida se debe:

- Identificar los controles existentes, que garanticen que los riesgos significativos están siendo tratados
- Identificar los controles que puedan ser probados
- Determinar si faltan controles que sean necesarios
- Determinar la dependencia de los controles sobre los activos de Información

## **1.4.2 Evaluar el control interno**

### **Cuadro No. 1. 10 Evaluar el control interno**

#### ***Fase 1: Planificación***

Actividad A1.4: Comprensión del control interno

Tarea T1.4.2: Evaluar el control interno

#### ***Objetivo:***

- Evaluar si el control interno, está bien diseñado mediante la utilización de pruebas de recorrido

#### ***Productos de Entrada***

- Resultados de la Tarea: Tarea T1.4.1: Identificar y comprender los controles existentes

#### ***Productos de salida***

- Informe del diseño del control es, Adecuado, Parcialmente Adecuado o

Continúa ➡

Inadecuado. (Ver anexo No. 15)

***Técnicas, prácticas y pautas***

- Reuniones de Trabajo
- Entrevistas
- Matriz de Evaluación de Controles
- Documentación Adicional

***Base Normativa.***

- Libro I.- Normas generales para la aplicación de la ley general de instituciones del sistema financiero; Título X.- De la gestión y administración de riesgos; Capítulo V.- De la gestión del riesgo operativo, emitido por la Superintendencia de Bancos y Seguros de la República del Ecuador.
- Libro I.- Normas generales para la aplicación de la Ley General de Instituciones del Sistema Financiero; Título XXI.- De las calificaciones otorgadas por la Superintendencia de Bancos y Seguros; Capítulo III.- Normas para la calificación de las firmas calificadoras de riesgo de las instituciones del sistema financiero.
- Normas 410 de auditoría interna para Tecnología de la Información.

***Participantes***

- Gerencia de TI
- Personal Técnico
- Oficial de Seguridad

***Acción a seguir***

En base a la comprensión de los controles se verificar el diseño de los controles y determinar si las medidas que la entidad ha establecido se orientan a reducir, transferir o asumir el riesgo:

- Que el control identificado previene o mitiga los riesgos de la actividad a controlar
- Si hay una persona responsable de ejecutar el control, si la persona que aplica los controles se ajusta al cargo que desempeña y si existe segregación de funciones
- La periodicidad de la aplicación del control es correspondiente con la

Continúa ➡

frecuencia de ejecución de las actividades para las cuales se estableció el control

- El control se encuentra debidamente formalizado (Políticas / Manuales de procedimiento y de funciones)

## 1.5 Determinación de Áreas y Procesos Críticos

### 1.5.1 Identificación de Áreas y Procesos Críticos

#### Cuadro No. 1. 11 Identificación de Áreas y Procesos Críticos

##### *Fase 1: Planificación*

Actividad A1.5: Determinación de Áreas y Procesos Críticos

Tarea T1.5.1: Identificación de Áreas y Procesos Críticos

##### *Objetivos*

- Obtener y documentar el entendimiento de procesos y áreas críticas suficiente para planificar y realizar la auditoría acorde con los estándares y requerimientos.

##### *Productos de entrada*

- Documentos que contienen la estructura de control interno de la organización
- Reportes de problemas de auditorías previas
- Sistemas que soporten áreas claves que son de interés para la auditoría
- Documento de comprensión de controles internos priorizados

##### *Productos de salida*

- Documento donde se priorice procesos y áreas claves de interés para la auditoría. (Ver anexo No. 16).

##### *Técnicas, prácticas y pautas*

- Reuniones de Trabajo
- Documentación
- Talleres de Trabajo
- Entrevistas

##### *Base Normativa*

- Libro I.- Normas generales para la aplicación de la ley general de instituciones

Continúa ➡

del sistema financiero; Título X.- De la gestión y administración de riesgos; Capítulo V.- De la gestión del riesgo operativo, emitido por la Superintendencia de Bancos y Seguros de la República del Ecuador.

- Libro I.- Normas generales para la aplicación de la Ley General de Instituciones del Sistema Financiero; Título XXI.- De las calificaciones otorgadas por la Superintendencia de Bancos y Seguros; Capítulo III.- Normas para la calificación de las firmas calificadoras de riesgo de las instituciones del sistema financiero.
- Normas 410 de auditoría interna para Tecnología de la Información.

### ***Participantes***

- Dueños de los procesos
- Gerente de TI

### ***Acción a seguir***

- Entender las operaciones y áreas críticas de la organización que permita al auditor identificar, responder y resolver problemas de manera temprana en la auditoría.
- Determinar la importancia de áreas o procesos críticos considerados para el proceso de auditoría que le permita llevar adelante los objetivos de auditoría.
- Identificar posibles requisitos de control.

## **1.6 Diseño del Plan de Pruebas**

### **1.6.1 Elaboración del Plan de Pruebas**

Cuadro No. 1. 12 Elaboración del Plan de Pruebas

#### ***Fase 1: Planificación***

Actividad A1.6: Diseño del Plan de Pruebas

Tarea T1.6.1: Elaboración del Plan de Pruebas

#### ***Objetivos***

- Elaborar el diseño del plan de pruebas de las áreas y procesos críticos identificados, que se realizarán en la fase de ejecución.

Continúa ➡



***Productos de entrada***

- Resultados de la Tarea T1.5.1: Identificación de Áreas y Procesos críticos

***Productos de salida***

- Plan de Pruebas de las áreas y procesos críticos. (Ver anexo No. 17).

***Técnicas, prácticas y pautas***

- Reuniones de Trabajo

***Base Normativa***

N/A.

***Participantes***

- Supervisor de Auditoría asignado
- Equipo de Auditoría

***Acción a seguir***

- El auditor deberá describir los procedimientos de auditoría que serán necesarios aplicar en cada una de las áreas o procesos que haya decidido auditar.
- Debe determinar en términos generales:
  - Objetivo de la Prueba
  - Tipo de Prueba
  - Técnica que utilizará
  - Recursos requeridos
- Existen dos tipos de pruebas que debe utilizar:
  - Pruebas de cumplimiento: Buscan determinar si existe el control para el riesgo identificado.
  - Pruebas sustantivas: Buscan conocer la forma en que está implementado el control, en caso de que exista.
- Para la evaluación de los controles se puede hacer uso de los controles establecidos en COBIT.

**1.7 Plan de Auditoría Basada en Riesgos****1.7.1 Elaboración del Plan de Auditoría Basada en Riesgos**

Cuadro No. 1. 13 Elaboración del Plan de Auditoría Basada en Riesgos

---

### ***Fase 1: Planificación***

Actividad A1.7: Plan de Auditoría Basada en Riesgos

Tarea T1.7.1: Elaboración del Plan de Auditoría Basada en Riesgos

#### ***Objetivos***

- Elaborar el plan de Auditoría Basada en Riesgos, en donde se estimará los recursos humanos necesarios y el tiempo necesario para la ejecución.

#### ***Productos de entrada***

- Resultados de la Tarea T1.6.1: Elaboración del Plan de Pruebas.

#### ***Productos de salida***

- Desarrollo del Plan de Auditoría Basada en Riesgos para TI. (Ver anexo No. 18).

#### ***Técnicas, prácticas y pautas***

- Reuniones de Trabajo

#### ***Base Normativa***

N/A.

#### ***Participantes***

- Supervisor de Auditoría asignado
- Equipo de Auditoría

#### ***Acción a seguir***

- El auditor deberá elaborar el plan de auditoría basada en riesgos en el que debe detallar los procedimientos de auditoría en los que debe considerar los siguientes pasos:
  - Procedimientos  
Procedimientos que realizará el auditor, en base al plan de pruebas en donde se indica las pruebas cumplimiento y sustantivas que debe ejecutar.
  - Identificación del Equipo de Auditoría  
Es el equipo de auditoría designado para llevar a cabo las tareas de auditoría que se ejecutarán.
  - Costo y cronograma de actividades Programa  
Es el costo que implica la ejecución como tal de la auditoría

Continúa ➡

Es el tiempo estimado de las horas previstas para la realización de la auditoría, en donde se debe identificar la actividad, tarea, y recurso.

- Propósito de la Auditoría.

Describe el motivo que origina la realización de la auditoría.

- Resumen del Diagnóstico General

Detalle algunos aspectos importantes durante la planeación, tales como: normativas, leyes, estructura organizacional, sistemas y cualquier otra información de relevancia que se considere.

- Objetivos.

Comprende la definición de los objetivos de la auditoría, es decir se debe describir que es lo que se pretende lograr.

- Alcance y Metodología

Comprende el alcance que tendrá la auditoría, para el cumplimiento de los objetivos que se pretende lograr, objeto del examen.

- Documentación aplicable.

Comprende las Normas, leyes, resoluciones aplicadas por los organismos de control, estándares y mejores prácticas.

- Áreas o procesos críticos a ser auditados.

Comprende el detalle del área o procesos críticos a ser auditados identificados durante la fase de planeación.

- Una vez que se ha finalizado la elaboración del Plan de Auditoría Basada en Riesgos, el auditor deberá realizar la aprobación del Supervisor auditor, para su posterior ejecución.

## 2 FASE 2: Ejecución de la Auditoría

La etapa de ejecución de la auditoría tiene por objeto desarrollar los procedimientos contenidos en los programas de auditoría.

La Ejecución de la Auditoría propuesta consta de las siguientes actividades y tareas:

### 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

## 2.1 Ejecución de Pruebas de auditoría

### 2.1.1 Ejecución de los procedimientos de auditoría

Cuadro No. 2. 1 Ejecución de los procedimientos de auditoría

---

#### *Fase 2: Ejecución de la Auditoría*

Actividad A2.1: Ejecución de pruebas de auditoría

Tarea T2.1.1: Ejecución de los procedimientos de auditoría

#### *Objetivos*

- Ejecutar los programas de auditoría a través del uso de procedimientos de auditoría y pruebas definidas en el plan (el alcance debe estar definido en el plan) con la finalidad de obtener evidencia suficiente, competente y pertinente que sustente las conclusiones de cada uno de los procesos auditados.

#### *Productos de entrada*

- Documento de plan de pruebas
- Documento de procedimiento de auditoría
- Documento con cronograma de plan de pruebas y personal asignado

#### *Productos de salida*

- Documento con registro de las pruebas realizadas (Ver anexo No. 19)

#### *Técnicas, prácticas y pautas*

- Medios y actividades utilizados y aplicados por los auditores en la ejecución de la auditoría

---

Continúa ➡

***Base Normativa***

- Libro I.- Normas generales para la aplicación de la ley general de instituciones del sistema financiero; Título X.- De la gestión y administración de riesgos; Capítulo V.- De la gestión del riesgo operativo, emitido por la Superintendencia de Bancos y Seguros de la República del Ecuador.
- Normas 410 de auditoría interna para Tecnología de la Información

***Participantes***

- Jefe Auditor
- Auditores

***Acción a seguir***

- El Equipo multidisciplinario debe aplicar los programas de auditoría que incluyen las pruebas y los procedimientos previamente definidos en el plan de ejecución.
- Verificar o validar la información que fue proporcionada en la etapa de evaluación
- Es importante considerar además que pueden realizar:
  - *Pruebas Sustantivas*: para determinar la validez e integridad de los datos, que se cumplen y son correctos, generalmente se usa en el cálculo de los datos utilizados. Se puede tomar todos los datos para validar o hacer un muestreo dependiendo de la cantidad de datos a validar.
  - *Pruebas de Cumplimiento*: para determinar si los controles se aplican y cumplen con la política de gestión. Deben usarse para garantizar la existencia y efectividad de un determinado proceso
- El auditor debe estar en capacidad de decidir sobre cuando efectuar pruebas de cumplimiento o pruebas sustantivas.
- La imposibilidad de efectuar análisis debe ser registrada indicando las razones tanto técnicas como físicas que pudo impedir esto.
- Debe indicarse las actividades efectuadas en la aplicación de pruebas sustantivas y cumplimiento y debe quedar registrado en papeles de trabajo para ser utilizado como sustento en la generación de las conclusiones.

## 2.1.2 Documentación de las pruebas

### Cuadro No. 2. 2 Documentar las pruebas

#### ***Fase 2: Ejecución de la Auditoría***

Actividad A2.1: Ejecución de pruebas de auditoría

Tarea T2.1.2: Documentar las pruebas

#### ***Objetivos***

- Documentar las pruebas de auditoría definidas en el plan de pruebas

#### ***Productos de entrada***

- Documento de plan de pruebas
- Documento de procedimiento de pruebas
- Resultados previos de pruebas efectuadas

#### ***Productos de salida***

- Documento con registro de pruebas de auditoría (Ver anexo No. 20)

#### ***Técnicas, prácticas y pautas***

- Recopilación de información, documentación y exámenes.

#### ***Base Normativa***

- Libro I.- Normas generales para la aplicación de la ley general de instituciones del sistema financiero; Título X.- De la gestión y administración de riesgos; Capítulo V.- De la gestión del riesgo operativo, emitido por la Superintendencia de Bancos y Seguros de la República del Ecuador.
- Normas 410 de auditoría interna para Tecnología de la Información

#### ***Participantes***

- Auditor
- Funcionarios técnicos
- Funcionarios de negocio

#### ***Acción a seguir***

- Documentar los resultados de las pruebas efectuadas basados en normas para documentación
- La imposibilidad de ejecutar pruebas debe ser registrada indicando las razones tanto técnicas como físicas que pudo impedir esto.
- Debe registrarse las actividades efectuadas en la aplicación de pruebas

Continúa ➡

sustantivas y de cumplimiento y debe quedar registrado en papeles de trabajo para luego ser utilizado como sustento en la generación de las conclusiones y para que el Jefe auditor o responsable de la auditoría hagan las revisiones y sugerencias de manera oportuna.

### 2.1.3 Elaboración/Recopilación de Papeles de trabajo

#### Cuadro No. 2. 3 Elaboración de Papeles de trabajo

##### *Fase 2: Ejecución de la Auditoría*

Actividad A2.1: Ejecución de pruebas de auditoría

Tarea T2.1.3: Elaboración de Papeles de trabajo

##### **Objetivos**

- Soportar por escrito la planificación del trabajo de auditoría
- Registrar las evidencias como respaldo de la auditoría y del informe
- Constituir un soporte legal en caso de requerir pruebas
- Disponer de una memoria escrita de la auditoría, que permita supervisar y revisar el trabajo de auditoría.

##### **Productos de entrada**

- Información concerniente al entorno económico y legislativo dentro de los que opera la entidad
- Evidencia del proceso de planificación que incluye programas de auditoría
- Evidencia de la comprensión de los sistemas de información y de control interno
- Evidencia de evaluaciones de los riesgos inherentes y de control
- Evidencia sobre la evaluación del trabajo de auditores internos y las conclusiones alcanzadas
- Evidencia de que los trabajos realizados por terceros fue supervisado y revisado
- Un registro de la naturaleza, tiempo y grado de los procedimientos de auditoría desarrollados y de los resultados de dichos procedimientos
- Una indicación sobre quién desarrolló los procedimientos de auditoría y cuándo fueron desarrollados

- Copias de comunicación con otros auditores, expertos y otras terceras partes
- Copias de documentos relativos a asuntos de auditoría comunicados, o discutidos con la entidad, incluyendo los términos del trabajo y las debilidades existentes en control interno.
- Conclusiones alcanzadas por el auditor, concernientes a aspectos importantes de la auditoría, incluyendo cómo se resolvieron los asuntos excepcionales o inusuales, revelados por los procedimientos del auditor.
- Copias de los dictámenes u otros informes del auditor, etc.

#### ***Productos de salida***

- Documento con registro de todos los datos, información y resultados recopilados a los largo del proceso de auditoría (Ver anexo No. 21).

#### ***Técnicas, prácticas y pautas***

- Técnicas de Documentación

#### ***Base Normativa***

- Libro I.- Normas generales para la aplicación de la ley general de instituciones del sistema financiero; Título X.- De la gestión y administración de riesgos; Capítulo V.- De la gestión del riesgo operativo, emitido por la Superintendencia de Bancos y Seguros de la República del Ecuador.
- Normas 410 de auditoría interna para Tecnología de la Información

#### ***Participantes***

- Auditor
- Jefe Auditor

#### ***Acción a seguir***

- El equipo multidisciplinario de auditoría debe elaborar/recopilar los papeles de trabajo las cuales deben contener las suficientes evidencias con el sustento y que sean suficientes, competentes y pertinentes. Estos deben ser claros, completos y concisos los cuales deben proveer un testimonio real del trabajo realizado y las razones que fundamentan las decisiones que se emitan.
- Este equipo debe documentar y/o registrar la planificación, naturaleza, oportunidades y el alcance de los procedimientos de la auditoría



desarrollados, dando prioridad a la calidad y no a la cantidad.

- El equipo debe considerar en los papeles de trabajo, entre otros, lo siguiente:
  - Nombre de la organización
  - Fecha del examen
  - Explicación del objetivo de la prueba
  - Descripción concisa del trabajo efectuado y sus resultados
  - Fuentes de información obtenidas
  - Conclusiones si estas aplican
  - Evidencias de la revisión

## 2.2 Estructurar los Hallazgos de auditoría

### Cuadro No. 2. 4 Estructurar los hallazgos de auditoría

#### *Fase 2: Ejecución de la Auditoría*

Actividad A2.2: Estructurar los hallazgos de auditoría

Tarea T2.2.1: Estructurar los hallazgos de auditoría

#### ***Objetivos***

- Determinar la existencia de fraude o identificar las fallas de control
- Soportar en papeles de auditoría para el informe
- Determinar el nivel de cumplimiento de la organización
- Obtener evidencia suficiente, competente y pertinente que permita al auditor determinar que se cuenta con procedimientos adecuados para mitigar los riesgos de negocio

#### ***Productos de entrada***

- Documento con registro de pruebas de auditoría.

#### ***Productos de salida***

- Documento con detalle de pruebas de auditoría con registro de desarrollo de hallazgos (Ver anexo No. 20).

#### ***Técnicas, prácticas y pautas***

- Reuniones de trabajo
- Comparación de criterio y condición

***Base Normativa***

- Libro I.- Normas generales para la aplicación de la ley general de instituciones del sistema financiero; Título X.- De la gestión y administración de riesgos; Capítulo V.- De la gestión del riesgo operativo, emitido por la Superintendencia de Bancos y Seguros de la República del Ecuador.
- Normas 410 de auditoría interna para Tecnología de la Información

***Participantes***

- Grupo Auditor
- Auditor
- Responsables de la ejecución

***Acción a seguir***

- El jefe del equipo de auditores y el supervisor debe elaborar las hojas resumen de los hallazgos encontrados que sean significativos para el o los componentes que se analizan.
- Determinar situaciones o hechos determinados como producto de la comparación de lo que debe ser (criterio de auditoría) con una situación determinada (condición encontrada). Este puede ser positivo o negativo.
- Deben considerarse aquellos que están relacionados con asuntos significativos, es decir, corresponden a cualquier situación deficiente determinada como consecuencia de la ejecución de los procedimientos de auditoría.
- El hallazgo debe cumplir al menos con:
  - Tener una importancia que amerite su comunicación
  - Debe basarse en evidencias o hechos precisos
  - Debe ser convincente para cualquier persona
- Para estructurar el hallazgo el equipo auditor debe:
  - Identificar los defectos, deficiencias o debilidades.
  - Identificar la línea a autoridad y responsabilidad
  - Verificar la causa de las deficiencias o debilidades
  - Determinar si la deficiencia es un caso aislado o generalizado
  - Determinar la afectación legal de la deficiencia
  - Determinar los efectos que ocasionarían las deficiencias

- Recabar comentarios de personas que pueden estar afectadas por el hallazgo.
- Realizar conclusiones en base a evidencias reunidas
- Determinar recomendaciones o acciones correctivas
- Se debe considerar la suficiencia, pertinencia y utilidad de las evidencias para considerarla como respaldo del hallazgo. Si se llega a resultados similares utilizando diversas técnicas estas resultarán más confiables.

## 2.3 Análisis de Resultados y Conclusiones

### Cuadro No. 2. 5 Análisis de Resultados y conclusiones

#### *Fase 2: Ejecución de la Auditoría*

#### Actividad A2.3: Análisis de Resultados y Conclusiones

#### Tarea T2.3.1: Análisis de Resultados y conclusiones

#### **Objetivos**

- Obtener resultados valederos en base a los hallazgos encontrados, con las evidencias suficientes, competentes y pertinentes y que estas puedan ser sustentadas de manera documentada.
- Relacionar criterio y condición del resultado de la ejecución de las pruebas

#### **Productos de entrada**

- Documento con registro de pruebas de auditoría

#### **Productos de salida**

- Desviaciones de la comparación entre el criterio y la condición.
- Conclusiones y recomendación relativas a cada uno de los hallazgos, así como de la auditoría en general (Ver anexo No. 20).

#### **Técnicas, prácticas y pautas**

- Reuniones de Trabajo
- Comparación criterio y condición

#### **Base Normativa**

- Libro I.- Normas generales para la aplicación de la ley general de instituciones del sistema financiero; Título X.- De la gestión y administración de riesgos; Capítulo V.- De la gestión del riesgo operativo, emitido por la

Continúa ➡

Superintendencia de Bancos y Seguros de la República del Ecuador.

- Normas 410 de auditoría interna para Tecnología de la Información

### ***Participantes***

- Jefe auditor
- Auditor

### ***Acción a seguir***

- El jefe del equipo de auditores y el supervisor deben analizar, validar y aprobar los hallazgos significativos que fueron determinados previamente y redactar los resultados de dichos hallazgos y las conclusiones para cada una de ellas y de manera general a la auditoría.
- Las desviaciones de la comparación entre el criterio y la condición deben ser consideradas previo a la determinación del hallazgo.
- Las causas más frecuentes encontradas de estas desviaciones son:
  - Debilidades en el control para detectar oportunamente
  - Carencia de mecanismos de monitoreo y seguimiento.
  - Deficiencias de comunicación entre las personas
  - Procedimientos inadecuados o inexistentes.
- Los efectos pueden ser:
  - Incumplimiento de disposiciones
  - Control inadecuado de los recursos o tareas
  - Uso ineficiente de recursos
- Los resultados y conclusiones del análisis efectuado debe reflejar que:
  - Los procedimientos de auditoría se han llevado a cabo de manera satisfactoria.
  - Se han identificado las causas y efectos de los hallazgos determinados
- Las Recomendaciones deben ser realizadas mencionando la necesidad de mejorar, para lo cual se debe considerar además, la factibilidad y el costo de aplicar dichas recomendaciones y los efectos que estas podrían ocasionar.

### 3 FASE 3: Resultado de la Auditoría

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:

#### 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

### 3.1 Elaboración de informe preliminar

#### Cuadro No. 3. 1 Elaboración de Informe Preliminar

---

##### *Fase 3: Resultado de Auditoría*

Actividad A3.1: Elaboración de Informe Preliminar

Tarea T3.1.1: Elaboración de Informe Preliminar

##### ***Objetivos***

- Dar cumplimiento a los objetivos por los cuales se originó la auditoría
- Dar a conocer los resultados de la auditoría
- Presentar las conclusiones y recomendaciones de manera objetiva e imparcial.
- Presentar la evaluación del control interno

##### ***Productos de entrada***

- Papeles de trabajo
- Desarrollo de los hallazgos

##### ***Productos de salida***

- Documento que contiene información preliminar con resultados de la auditoría de manera precisa, objetiva, concisa sustentada y oportuna (Ver anexo No. 22).

##### ***Técnicas, prácticas y pautas***

---

Continúa ➡

- Técnicas de Documentación

### ***Base Normativa***

- Libro I.- Normas generales para la aplicación de la ley general de instituciones del sistema financiero; Título X.- De la gestión y administración de riesgos; Capítulo V.- De la gestión del riesgo operativo, emitido por la Superintendencia de Bancos y Seguros de la República del Ecuador.

### ***Participantes***

- Jefe Auditor
- Grupo de auditores

### ***Acción a seguir***

- El jefe del equipo de auditores y su grupo de trabajo deben materializar el resultado de la auditoría en un informe preliminar donde se comunicará los resultados parciales a los interesados, en el cual se resume el cumplimiento de los objetivos definidos en el plan de auditoría y basado en las conclusiones obtenidas en la fase de ejecución de la auditoría.
- La estructura del informe debe contener:
  - *Identificación del Informe.*- identificación para distinguirse de otros informes
  - *Identificación del Cliente.*- identificación de los destinatarios y a las personas que requieren la auditoría
  - *Información de la entidad auditada.*- identificación de la entidad objeto de la auditoría
  - *Objetivos de la auditoría.*- Declarar los objetivos de la auditoría para identificar su propósito, señalando los objetivos incumplidos.
  - *Normativa aplicada y excepciones.*- Identificación de normas legales y profesionales utilizadas, así como el posible impacto de los resultados de la auditoría.
  - *Alcance.*- Concretar la naturaleza y extensión del trabajo
  - *Limitaciones.*- razones por las cuales no se pudo cumplir los objetivos previstos, las cuales deben ser mencionadas expresamente.
  - *Conclusiones: Informe corto de opinión o Ejecutivo*

- *Resultados Generales.*- se incluirán comentarios, conclusiones y recomendaciones sobre la entidad auditada que esté relacionada con el cumplimiento de objetivos y metas de la entidad.
- *Resultados específicos por hallazgo.*- detalle de cada uno de los hallazgos que contendrá conclusiones y recomendaciones.
  - *Resultados: Informe largo y otros informes.*
  - *Fecha del Informe.*- es importante para conocer la magnitud del trabajo. Se debe precisar las fechas de inicio y conclusión del trabajo de campo, incluso del cierre de la auditoría.
  - *Identificación y firma del Auditor.*- es la parte formal del informe, indispensable para identificar al autor.
  - *Distribución del Informe.*- Debe definirse quién o quienes podrán hacer uso del informe, así como los usos concretos que tendrá.
- El equipo de auditores deben, en el informe, describir de manera clara los hallazgos sobre las deficiencias o debilidades encontradas durante el examen de la auditoría y este es resultado del desarrollo de la información, la recolección lógica de datos y la presentación objetiva de los hechos, la cual será la base para la realización de las conclusiones y recomendaciones.
- Debe realizarse una reunión con los interesados para dar a conocer el borrador del informe
- Este informe debe ser redactado de manera precisa, concisa, objetiva, sustentada y oportuna

### 3.2 Lectura de informe preliminar

#### Cuadro No. 3. 2 Lectura de Informe Preliminar

##### *Fase 3: Resultado de la Auditoría*

##### Actividad A3.2: Lectura de Informe preliminar

##### Tarea T3.2.1: Lectura de Informe Preliminar

##### **Objetivos**

- Dar a conocer a los interesados los resultados preliminares de la auditoría realizada a la entidad

Continúa ➡

***Productos de entrada***

- Informe Preliminar

***Productos de salida***

- N/A

***Técnicas, prácticas y pautas***

- Reunión con los interesados
- Lectura

***Base Normativa***

Libro I.- Normas generales para la aplicación de la ley general de instituciones del sistema financiero; Título X.- De la gestión y administración de riesgos; Capítulo V.- De la gestión del riesgo operativo, emitido por la Superintendencia de Bancos y Seguros de la República del Ecuador.

***Participantes***

- Jefe Auditor
- Interesados de la auditoría efectuada

***Acción a seguir***

- Convocar a reunión a los interesados de los resultados preliminares de la auditoría
- Comunicar los resultados con conclusiones y recomendaciones sobre hallazgos encontrados durante la ejecución de las pruebas.
- Validar el informe preliminar de los resultados de la auditoría y analizar las observaciones realizadas a cada una de los hallazgos para determinar si proceden ajustes al informe

**3.3 Elaboración de informe final de auditoría****Cuadro No. 3. 3 Elaboración Informe final de Auditoría*****Fase 3: Resultado de la Auditoría***

Actividad A3.3: Elaboración Informe final de Auditoría

Tarea T3.3.1: Elaboración de Informe Final de Auditoría

***Objetivos***

- Dar cumplimiento a los objetivos por los cuales se originó la auditoría

Continúa ➡



- Dar a conocer los resultados de la auditoría
- Presentar las conclusiones y recomendaciones definitivas de manera objetiva e imparcial.

#### ***Productos de entrada***

- Informe preliminar
- Documento de observaciones de la reunión mantenida para la lectura del informe preliminar

#### ***Productos de salida***

- Documento que contiene información con resultados definitivos de la auditoría de manera precisa, objetiva, concisa, sustentada y oportuna.

#### ***Técnicas, prácticas y pautas***

- Reuniones de trabajo

#### ***Base Normativa***

Libro I.- Normas generales para la aplicación de la ley general de instituciones del sistema financiero; Título X.- De la gestión y administración de riesgos; Capítulo V.- De la gestión del riesgo operativo, emitido por la Superintendencia de Bancos y Seguros de la República del Ecuador.

#### ***Participantes***

- Grupo de auditores

#### ***Acción a seguir***

- Una vez realizada la reunión de lectura del informe preliminar y levantadas las observaciones, con base en los resultados de validación de respuestas y efectuados, los ajustes que pueden haber dado lugar, debe generarse el documento de informe definitivo que será entregado a los interesados.

#### **4 FASE 4: Seguimiento (Consejo de Auditoría Interna General de Gobierno, 2008)**

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 auditoría

##### 4.4 Informe del Seguimiento de Recomendaciones

###### 4.4.1 Informe de seguimiento

#### **4.1 Determinación de Objetivos de seguimiento**

##### **Cuadro No. 4. 1 Determinación de Objetivos de seguimiento**

---

###### *Fase 4: Seguimiento*

Actividad A4.1: Determinación de objetivos de seguimiento

Tarea T4.1.1: Determinación de Objetivos de seguimiento

###### ***Objetivos***

- Establecer los objetivos planteados para el cumplimiento total o parcial de las recomendaciones brindadas en el informe final

###### ***Productos de entrada***

- Reportes de no conformidad
- Informe Final
- Recomendaciones

###### ***Productos de salida***

- Objetivos del seguimiento

###### ***Técnicas, prácticas y pautas***

- Valoración Delphi
- Análisis costo beneficio
- Reuniones de trabajo

**Base Normativa**

- Libro I.- Normas generales para la aplicación de la ley general de instituciones del sistema financiero; Título X.- De la gestión y administración de riesgos; Capítulo V.- De la gestión del riesgo operativo, emitido por la Superintendencia de Bancos y Seguros de la República del Ecuador.
- Libro I.- Normas generales para la aplicación de la ley general de instituciones del sistema financiero; Título XXI.- De las calificaciones otorgadas por la Superintendencia de Bancos y Seguros; Capítulo II.- Normas para la calificación de auditores internos de las entidades sujetas al control de la Superintendencia de Bancos y Seguros.
- Normas 410 de auditoría interna para Tecnología de la Información

**Participantes**

- Auditor
- Auditados

**Acción a seguir**

- Conocimiento y análisis de las recomendaciones emitidas en el informe final
- Definir la prioridad de cumplimiento de las recomendaciones, esto es entre el auditor y el auditado.
- Se debe considerar el reporte de no conformidad para establecer los objetivos.

**4.2 Plan Operativo de Seguimiento****Cuadro No. 4. 2 Plan operativo de seguimiento****Fase 4: Seguimiento**

Actividad A4.2: Plan Operativo de seguimiento

Tarea T4.2.1: Plan operativo de seguimiento

**Objetivos**

- Planificar el proceso de seguimiento del cumplimiento de las recomendaciones efectuadas en el informe final y en base a los objetivos del seguimiento.

Continúa ➡

---

***Productos de entrada***

- Informe final de auditoría
- Documento de acuerdos y responsabilidades para el cumplimiento de las recomendaciones o no conformidades
- Documento de riesgos

***Productos de salida***

- Plan de Seguimiento

***Técnicas, prácticas y pautas***

- Reuniones

***Base Normativa***

- Libro I.- Normas generales para la aplicación de la ley general de instituciones del sistema financiero; Título X.- De la gestión y administración de riesgos; Capítulo V.- De la gestión del riesgo operativo, emitido por la Superintendencia de Bancos y Seguros de la República del Ecuador.
- Libro I.- Normas generales para la aplicación de la ley general de instituciones del sistema financiero; Título XXI.- De las calificaciones otorgadas por la Superintendencia de Bancos y Seguros; Capítulo II.- Normas para la calificación de auditores internos de las entidades sujetas al control de la Superintendencia de Bancos y Seguros.
- Normas 410 de auditoría interna para Tecnología de la Información

***Participantes***

- Auditor
- Auditados

***Acción a seguir***

- El equipo auditor y los interesados deben generar el plan de seguimiento que permita dar cumplimientos a las recomendaciones efectuadas durante el proceso de auditoría. La prioridad de la implementación de estos riesgos se basará en el análisis de riesgos obtenido.
- El Plan de seguimiento debe contener al menos:
  - Objetivos del plan de seguimiento
  - Alcance del seguimiento
  - Equipo de trabajo involucrado

- Horas de auditoría a utilizar en el seguimiento
- Cronograma de trabajo
- Metodología a utilizar
- Contenido en detalle del plan de seguimiento

### 4.3 Ejecución del Seguimiento de Auditoría

#### Cuadro No. 4. 3 Ejecución de seguimiento de auditoría

##### *Fase 4: Seguimiento*

Actividad A4.3: Ejecución del Seguimiento de Auditoría

Tarea T4.3.1: Ejecución de seguimiento de auditoría

##### **Objetivos**

- Dar cumplimiento a los objetivos de seguimiento y efectuar las tareas de cumplimiento para la remediación de las recomendaciones basado en los compromisos de cumplimiento.

##### **Productos de entrada**

- Plan detallado de seguimiento
- Documento de compromisos

##### **Productos de salida**

- Papeles de trabajo del seguimiento

##### **Técnicas, prácticas y pautas**

- Medios y actividades utilizados y aplicados por los auditores en la ejecución de la auditoría

##### **Base Normativa**

- Libro I.- Normas generales para la aplicación de la ley general de instituciones del sistema financiero; Título X.- De la gestión y administración de riesgos; Capítulo V.- De la gestión del riesgo operativo, emitido por la Superintendencia de Bancos y Seguros de la República del Ecuador.
- Normas 410 de auditoría interna para Tecnología de la Información

##### **Participantes**

- Auditor
- Responsables de los procesos

- Auditados

#### ***Acción a seguir***

- Disponer de toda la información posible y los antecedentes contenidos en el Plan de Seguimiento, que considere cronograma de trabajo, detalle de recomendaciones, detalle de compromisos formales, plazos de implementación, responsables.
- Mantener reuniones con los responsables, antes y después de la ejecución, para visualizar el avance y resultado de la implementación de las recomendaciones.
- Supervisar el desarrollo normal y dentro de los plazos establecidos de las actividades de seguimiento.

## **4.4 Informe del Seguimiento de Recomendaciones**

### **Cuadro No. 4. 4 Informe de seguimiento**

#### ***Fase 4: Seguimiento***

Actividad A4.4: Informe de seguimiento de recomendaciones

Tarea T4.4.1: Informe de seguimiento

#### ***Objetivos***

- Informar sobre el nivel de avance efectuado durante el seguimiento

#### ***Productos de entrada***

- Papeles de trabajo del seguimiento

#### ***Productos de salida***

- Informe de seguimiento

#### ***Técnicas, prácticas y pautas***

- Elaboración de Informes

#### ***Base Normativa***

- Libro I.- Normas generales para la aplicación de la ley general de instituciones del sistema financiero; Título X.- De la gestión y administración de riesgos; Capítulo V.- De la gestión del riesgo operativo, emitido por la Superintendencia de Bancos y Seguros de la República del Ecuador.

#### ***Participantes***

Continúa 

- 
- Jefe Auditor

***Acción a seguir***

- Redactar de manera clara y concisa sobre el nivel de avance efectuado durante el seguimiento y su nivel de cumplimiento en base a los resultados de la ejecución
- Destacar los procesos cuyo nivel de avance es bajo que permita priorizarlos de acuerdo al nivel de riesgo obtenido.
- Destacar los procesos cuyo nivel de avance y su implementación
- Evaluar logros y resultados durante el proceso de seguimiento
- Informar a los responsables para que ellos respondan por los retrasos

## **5 CAPITULO V**

### **5.1 CONCLUSIONES Y RECOMENDACIONES.**

#### **Conclusiones:**

Como resultado final del desarrollo de la presente tesis se ha llegado a las siguientes conclusiones las mismas que se mencionan a continuación:

- 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.
- Se debe considerar que no necesariamente las tecnologías de información en una Institución Financiera, como es la banca pública, por si solas garantizan la seguridad de la información, por lo que es importante que cuenten con una adecuada gestión del riesgo tecnológico y que las mismas sean supervisadas y revisadas periódicamente a través de auditorías basadas en riesgos a las Tecnologías de Información.
- Para el cumplimiento de normativas, estándares, resoluciones y metodologías enfocados a las auditorías 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.
- Para el desarrollo de la guía se consideró los estándares y mejores prácticas de TI para la gestión de riesgo y control interno, como son: MAGERIT, ISO-27005, COBIT, Risk IT y COSO ERM.
- 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.

**Recomendaciones:**

En base a las conclusiones que son el resultado del trabajo realizado, a continuación se presentan una serie de recomendaciones que se consideran relevantes para el trabajo de Auditoría referente a Riesgos de TI, dichas recomendaciones

pueden contribuir o mejorar los proceso de auditoría en la Banca Pública dependiendo del interés que el auditor deba prestarle.

- Para llevar a cabo la ejecución de un Plan de Auditoría, con base a lineamientos de las Normas y Control Interno establecidos por la Súper Intendencia de Bancos y Seguros y la Contraloría General del estado, se sugiere considerar la guía y actividades indicadas en este trabajo y documentos propuesto producto de nuestra investigación, los mismos que se fundamentan en los estándares y mejores prácticas de TI.
- Se sugiere a los auditores internos de la banca pública promover en realizar auditorías de TI basada en la evaluación de 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.
- Con la finalidad de mejorar la profesión de Auditoría se recomienda que aquellos profesionales que se desempeñan como auditores internos en la banca pública, deberían contar con un documento que les guie u oriente en la realización de la planeación, ejecución y seguimiento para auditorías de TI basada en riesgos, por lo que se ha visto necesario contar con un documento que pueda servir de base para llevar a cabo las auditorías y así poder alertar a

la entidad auditada posibles riesgos o vulnerabilidades a las que pueden estar expuesta.

- Finalmente se sugiere que los auditores tomen conciencia de la importancia que es 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.

## 6 BIBLIOGRAFÍA

- Consejo de Auditoría Interna General de Gobierno. (Marzo de 2008). *Consejo de Auditoría Interna General de Gobierno*. Obtenido de Consejo de Auditoría Interna General de Gobierno: [www.auditoriainternadegobierno.cl/index.php/menu/ShowFile/id/21](http://www.auditoriainternadegobierno.cl/index.php/menu/ShowFile/id/21)
- COSO. (Septiembre de 2004). *Committee of Sponsoring Organizations of the Treadway Commission*. Recuperado el Agosto de 2013, de Committee of Sponsoring Organizations of the Treadway Commission: <http://www.coso.org>
- International Standards Organization. (15 de 06 de 2008). *International Standards Organization, First Edition*. Obtenido de <http://www.iso.org>
- ISACA. (2007). *Information Systems Audit and Control Association, 4.1*. Recuperado el Julio de 2013, de Information Systems Audit and Control Association: <http://www.isaca.org>
- ISACA. (2009). *Information Systems Audit and Control Association*. Recuperado el Julio de 2013, de Information Systems Audit and Control Association: <http://www.isaca.org>
- ISACA. (2010). *Manual de Preparación al Examen CISA*. Illinois, Estados Unidos.
- ISACA. (s.f.). *Information Systems Audit and Control Association*. Obtenido de Information Systems Audit and Control Association: <https://www.isaca.org/About-ISACA/History/Espanol/Documents/ISACA-Code-of-Ethics-Spanish.pdf>
- Ministerio de Hacienda y Administraciones Públicas. (Octubre de 2012). Recuperado el Junio de 2013, de <http://administracionelectronica.gob.es>: <http://administracionelectronica.gob.es>
- Registro Oficial de la República del Ecuador. (2009). *Normas de Control Interno para las Entidades, Organismos del Sector Público y personas jurídicas de Derecho Privado que dispongan de Recursos Públicos*. Quito: Registro Oficial.
- Superintendencia de Bancos y Seguros. (21 de Enero de 2010). RESOLUCIÓN No. JB-2010-1549. Quito, Pichincha, Ecuador.

## GLOSARIO

- Riesgo: posibilidad de que se produzca un Impacto determinado en un Activo, en un Dominio o en toda la Organización.
- Amenaza: Es un evento que puede desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.
- Vulnerabilidad: posibilidad de ocurrencia de la materialización de una amenaza sobre un Activo.
- Disponibilidad: Los recursos de información sean accesibles, cuando estos sean necesarios.
- Impacto: consecuencia de la materialización de una amenaza.
- Normas: Las normas son documentos técnico-legales que contienen especificaciones técnicas de aplicación voluntaria, están basados en los resultados de la experiencia y el desarrollo tecnológico, son aprobados por un organismo nacional, regional o internacional de normalización reconocido.
- Estándar: Son acuerdos (normas) documentados que contienen especificaciones técnicas u otros criterios precisos para ser usados consistentemente como reglas, guías, o definiciones de características, para asegurar que los materiales productos, procesos y servicios se ajusten a su propósito.
- Control Interno: El control interno será responsabilidad de cada institución del Estado y de las personas jurídicas de derecho privado que dispongan de recursos públicos y tendrá como finalidad crear las condiciones para el ejercicio del control.

- COBIT: Se enfoca en qué se requiere para lograr una administración y un control adecuado de TI, y se posiciona en un nivel alto. COBIT ha sido alineado y armonizado con otros estándares y mejores prácticas más detallados de TI.
- COSO (y marcos de trabajo compatibles similares) es generalmente aceptado como el marco de trabajo de control interno para las empresas.
- ISACA (Asociación para el Control y Auditoría de Sistemas de Información): Organización Global que establece las pautas para los profesionales del gobierno, control, seguridad y auditoría de información.