ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERIA DE SISTEMAS

ANÁLISIS DE LA REGULACIÓN DEL RIESGO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN EN EL ÁMBITO FINANCIERO ECUATORIANO

TESIS PREVIA A LA OBTENCIÓN DEL GRADO DE MÁSTER (MSc) EN GESTION DE LAS COMUNICACIONES Y TECNOLOGIAS DE LA INFORMACIÓN

FRANKIE ERIKSON CATOTA QUINTANA

DIRECTOR: ENRIQUE MAFLA G. PhD

Quito, Junio 2010

DECLARACIÓN

Yo, Frankie Erikson Catota Quintana, declaro bajo juramento que la investigación aquí descrita es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

_____

Frankie Erikson Catota Quintana

AGRADECIMIENTO

Al Todopoderoso por sus generosas bendiciones, al Doctor Enrique Mafla Gallegos, por su valioso aporte, a la Escuela Politécnica Nacional por la formación ofrecida.

A mi madre y hermanas por su gran dedicación y atenciones, a mi padre y hermanos por sus oraciones y cariño.

DEDICATORIA

A mi madre Elsa María por su desprendido y gran cariño, a mi padre César Agusto por su ejemplo, a mis hermanas y hermanos.

Al Todopoderoso por ofrecerme fortaleza y aliento.

Al favor del Altísimo, favor, de quien me complacería imprimir su nombre.

CONTENIDO

INDICE DE FIGURAS

INDICE DE TABLAS

NDICE DE ANEXOS

RESUMEN

La investigación planteada en este documento realiza el análisis de la Resolución JB-2005-834, con el propósito de identificar el alineamiento que existe entre las exigencias de la Resolución y las mejores prácticas generalmente aceptadas para administrar Riesgos en las Tecnologías de la Información (RTI). A partir de este análisis se plantea una propuesta de mejoramiento. La Resolución JB-2005-834 fue emitida por la Junta Bancaria en Octubre del 2005, donde se emitieron instrucciones para la administración del Riesgo Operacional (RO) para regular a las instituciones financieras ecuatorianas. Dentro de esta regulación se incluyeron conceptos de administración RTI como un componente relevante de RO. Esta realidad plantea la necesidad de realizar un análisis para determinar el grado de alineación de estas directrices respecto a las mejores prácticas de RTI aceptadas, especialmente debido al grado de relevancia que TI tiene en el ámbito financiero ecuatoriano.

Para cumplir con el propósito planteado, esta investigación realiza un análisis comparativo del contenido de la Resolución respecto al marco de trabajo de COBIT 4.1 y el estándar ISO-IEC 27002:2005. El criterio de elección de estas referencias obedece al propósito de obtener en primera instancia una visión general de aspectos de Gobierno de RTI; y, luego una visión más particular de los aspectos de Seguridad de la Información mediante ISO-IEC 27002:2005. El análisis inicia identificando las debilidades y fortalezas de la Resolución y el grado de coincidencia es expresado a través de un índice de alineamiento. Finalmente, este índice y la fortaleza de las referencias (COBIT e ISO) son utilizadas como criterios de entrada para realizar la propuesta de mejoramiento, la cual considera la inclusión de objetivos de control requeridos para mejorar la administración de RTI.

ACRONIMOS

AZ /NZS	Australia/New Zealand Standard
CC	Calificación Cualitativa
COBIT	Control Objectives for Information and related Technology
CERT	Computer Emergency Response Team
CID	Confidencialidad, Integridad y Disponibilidad
COSO	Committee Of Sponsoring Organizations Of the Threadway Comission
EE	Efectividad y Eficiencia
IA	Indice de Alineamiento
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
IT	Tecnologías de la Información
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation
OLA	Operation Level Agreement
QMS	Quality Management System
RO	Riesgo Operacional
RTI	Riesgo en las Tecnologías de la Información
SLA	Service Level Agreement
SOX	Sarbanes-Oxley Act

CAPITULO 1

INTRODUCCION

El 20 de Octubre del año 2005, la Superintendencia de Bancos del Ecuador, a través de la Junta Bancaria emitió la Resolución JB-2005-834. Esta Resolución fue instituida con el propósito de entregar lineamientos de administración de Riesgo Operacional (RO) a las instituciones financieras públicas y privadas; para lo cual se fundamentó esencialmente en los lineamientos propuestos por el Comité de Basilea.[1] Este comité publicó en Junio del 2004 la propuesta "*Convergencia Internacional de Medidas y Normas de Capital*", más conocido como Basilea II. El propósito de esta propuesta consiste en la creación de una base para la regulación del capital y el riesgo operacional en las instituciones financieras, para de esta manera apoyar a la solidez y estabilidad del sistema bancario en general.

La Regulación JB-2005-834 considera como factores del Riesgo Operacional a los procesos institucionales, las personas y las Tecnologías de la Información (TI). Por consiguiente, la Resolución también ha incluido en su contenido los principios de administración de Riesgo en las Tecnologías de la Información (RTI). De esta manera, la Resolución se alinea con el planteamiento de Basilea II, el cual incluye el RTI como parte del Riesgo Operacional. Consecuentemente, las instituciones del sistema financiero están reguladas por un marco que dictamina las reglas que deben seguirse en la gestión de riesgos de TI.

La investigación planteada en este documento realiza el análisis de la Resolución JB-2005-834, con el propósito de identificar el alineamiento que existe entre las exigencias de la Resolución y las mejores prácticas generalmente aceptadas para administrar RTI. Para el efecto, esta investigación realiza un análisis comparativo del contenido de la Resolución respecto a estándares de gobierno y administración de riesgo de TI. De esta manera se identifican oportunidades de

[1] Comité de Basilea

mejoramiento que permiten plantear una actualización de la Resolución alineada con estándares especializados.

1.1 OBJETIVOS GENERAL Y ESPECÍFICOS

1.1.1 OBJETIVO GENERAL

Identificar las fortalezas y debilidades de la Regulación del Riesgo de las Tecnologías de la Información en el ámbito Financiero Ecuatoriano, la cual se encuentra incluida en la Resolución JB-2005-834; y proponer medidas de mejoramiento para las debilidades identificadas.

1.1.2 OBJETIVOS ESPECÍFICOS

- Identificar las fortalezas y debilidades en la Resolución de riesgo operacional financiero 2005-834 en lo relativo a la gestión de riesgo en las Tecnologías de la Información.
- Analizar la Resolución de riesgo operacional financiero JB-2005-834 respecto al marco de trabajo para el Gobierno de las Tecnologías de la Información COBIT 4.1.[2]
- Analizar la Resolución de riesgo operacional financiero JB-2005-834 respecto al estándar Código para la Práctica de la Gestión de Seguridad de la Información ISO-IEC 27002:2005.[3]
- Proponer medidas de mejoramiento para debilidades detectadas en base al análisis.

1.2 ALCANCE

La investigación contempla el análisis comparativo de la Regulación JB-2005-834 respecto a dos estándares o marcos de referencia relativos a la Administración del Riesgo de las Tecnologías de la Información. Estos son, el Marco de Trabajo de COBIT en su versión 4.1 y el Código para la Práctica de la Gestión de Seguridad

[2] Control Objectives for Information and related Technology, <www.isaca.org/cobit>.
[3] ISO, International Organization for Standardization
IEC, International Electrotechnical Commission

de la Información ISO-IEC 27002:2005. El procedimiento de comparación busca los Objetivos de Control de estas referencias en el contenido de la Resolución. A partir de este análisis se realiza una propuesta de mejoramiento que recomienda los Objetivos de Control mínimos que deberían ser considerados en una posible actualización de la Resolución JB-2005-834. Este análisis no cubre la implantación de la propuesta y tampoco considera otros tipos de riesgos comunes en el ámbito financiero, como por ejemplo: riesgo legal, de liquidez, de mercado, estratégico, ó de crédito.

1.3 ANTECEDENTES Y JUSTIFICACION

La ausencia de prácticas de administración de RTI expone a las instituciones financieras riesgos que afectan la consecución de sus objetivos organizacionales, su subsistencia e inclusive pueden incluir implicaciones sociales. En el Ecuador, el suceso financiero de 1999, año en el cual desaparecieron algunos bancos del sistema financiero, presenta un ejemplo de las consecuencias que puede ocasionar la ausencia de instancias de control en las instituciones financieras. En este caso los efectos tuvieron implicaciones económicas y sociales; pues, generaron inestabilidad y desconfianza en el sistema financiero ecuatoriano. Estas consecuencias exigen la existencia de un proceso de administración continua del riesgo, que permita mitigar, controlar, transferir, y en algunos casos de manera responsable aceptar cierta magnitud del mismo. Dentro de esta administración, RTI constituye un elemento esencial debido a la influencia de las TI en los procesos operacionales financieros.

Según la información disponible en el portal electrónico de la Superintendencia de Bancos, la Junta Bancaria empezó a incluir los principios de gestión de riesgo desde el año 2002. En este año se consideraron riesgos de liquidez y de mercado. Posteriormente en el año 2003 se publican principios para regular el riesgo de crédito. En el año 2004 en la Resolución JB-2004-63, se agrega el concepto de "*La Gestión Integral y Control de Riesgos*"; donde se dan instrucciones sobre la obligatoriedad de "*Establecer esquemas eficientes y efectivos de administración y control de todos los riesgos a los que se encuentran*

expuestas el desarrollo del negocio."[4] Finalmente, el 20 de Octubre del 2005 se emite la Resolución JB-2005-834, donde se incluye el concepto de Gestión de Riesgo Operativo, el cual tiene una equivalencia con la terminología de Riesgo Operacional utilizada en este documento. La Resolución JB-2005-834 es el objeto del análisis de esta investigación por contener principios de administración de Riesgo de TI. El hecho de que han transcurrido casi 5 años desde la emisión de esta Resolución hace presuponer posibles ausencias de control que requieren directrices de mejoramiento.

1.4 ESTRUCTURA DE LA JB-2005-834

El contenido de la Resolución JB-2005-834 está estructurada en 6 secciones y 24 artículos que definen exigencias sobre la administración de riesgo operacional y por consiguiente de RTI.

La sección I, *Ámbito, Definiciones y Alcance*, establece el alcance de aplicación de la Resolución, identifica de manera particular los tipos de entidades sujetos a esta regulación. Adicionalmente se define la terminología empleada.

La sección II, *Factores del Riesgo Operativo*, establece los elementos considerados como factores de riesgo, los cuales incluyen a los procesos, las personas y las Tecnologías de Información. Esta sección contiene la mayor parte de los principios de control aplicados a TI.

La sección III, *Administración del Riesgo Operativo*, donde se especifica la obligatoriedad del diseño de un proceso de administración de riesgo operativo que les permita "*Controlar identificar, medir, controlar/mitigar y monitorear sus exposiciones a este riesgo al que se encuentran expuestas en el desarrollo de sus negocios y operaciones*."[5]

---

[4] Junta Bancaria, Libro I, Normas Generales para la aplicación de la Ley General de Instituciones del Sistema Financiero, Titulo X. De la Gestión y Administración de Riesgos, 2004.
[5] Junta Bancaria, Libro I, Normas Generales para la aplicación de la Ley General de Instituciones del Sistema Financiero, Titulo X. De la Gestión y Administración de Riesgos, 2004.

La sección IV, *Continuidad del Negocio*, exige la implementación de planes de contingencia y continuidad operacional, donde se consideran riesgos por fallas en TI. La sección V, *Responsabilidades en la Administración del Riesgo Operativo*, define las responsabilidades respecto a RO del directorio de las instituciones controladas. La sección VI, *Disposiciones Generales*, establece el control de servicios provistos por terceros. Finalmente la sección VII, *Disposiciones y Transitorias*, establece plazos de entrega del diagnóstico y proyectos de implementación de las disposiciones.

1.5 ELECCION DE LOS ESTANDARES DE REFERENCIA

Desde hace dos décadas, varios marcos y estándares de referencia han emergido para ofrecer directrices sobre diversos aspectos relacionados con el control, el gobierno corporativo y la gestión de riesgos. Entre los más relevantes para el propósito de esta investigación se mencionan; el marco integrado de COSO,[6] el cual provee una referencia en, "*Aspectos organizacionales de gobernabilidad, ética de negocios, control interno, administración del riesgo empresarial, fraude y reporte financiero*."[7]. COBIT por su parte representa un marco de referencia para el gobierno y control de las Tecnologías de la Información, que según ISACA[8] se ajusta como soporte a COSO. Adicionalmente, el equipo de respuesta a emergencias computacionales CERT,[9] que pertenece a la universidad estadounidense "*Carnegie-Mellon University*", ha creado OCTAVE.[10] Este estándar propone un conjunto de herramientas, técnicas y métodos para la elaboración de una estrategia de evaluación y planificación estratégica de la seguridad de la información. Por otro lado, el Comité Técnico de Estándares de Australia y Nueva Zelanda desarrolló el estándar de Administración de Riesgos AZ/NZS 4360:1999,[11] el cual incorpora el establecimiento del contexto y la identificación, análisis, evaluación, tratamiento, comunicación y el monitoreo de los riesgos. Por último en esta lista, ISO e IEC proponen el Código para la

[6] COSO, Committee Of Sponsoring Organizations Of the Threadway Comission
[7] COSO. <http://www.coso.org>.
[8] ISACA, Information Systems Audit and Control Association.
[9] CERT, Computer Emergency Response Team.
[10] OCTAVE, Operationally Critical Threat, Asset, and Vulnerability Evaluation
[11] AZ /NZS, Australia/New Zealand Standard.

Práctica de la Gestión de Seguridad de la Información ISO-IEC 27002:2005, el cual tiene su origen en el estándar británico BS7799. Este estándar plantea una estructura de controles con un enfoque en seguridad de la información para precautelar las propiedades de la información.

La elección de los estándares se referencia para la investigación sigue los siguientes criterios:

- Propósito de análisis de esta investigación (RTI).
- Orientación de los estándares de referencia respecto a la administración de Riesgo de las Tecnologías de la Información.
- Reconocimiento a nivel internacional de los estándares de referencia.

En busca de referencias a nivel internacional, se puede citar las iniciativas estadounidenses respecto al control en el ámbito financiero. En el año 2002 el congreso de los Estadios Unidos promulgó la Ley SOX,[12] con el propósito de establecer controles en el ámbito financiero. Por consiguiente, una evidente necesidad que emergió es, cómo implementar los controles para cumplir esta ley. Las compañías estadounidenses han encontrado una respuesta en COSO y en Cobito. A pesar de que COSO nace como una iniciativa del sector privado, este también ha alcanzado reconocimiento en el sector de control, en particular en la entidad encargada de regular los mercados bursátiles en los Estados Unidos de América, la SEC,[13] la cual expresa su reconocimiento de COSO en su sitio web. De esta manera, COSO ha llegado a ser el marco de soporte en el cumplimiento de SOX. Sin embargo, COSO no proporciona detalles sobre el diseño y aplicación de controles de TI, por lo que las compañías utilizan COBIT como un complemento para COSO en lo que a TI se refiere. Esto, a pesar de que este no ha sido validado por alguna instancia del gobierno estadounidense.

COBIT es aceptado internacionalmente por organizaciones debido a que proporciona una aproximación metodológica al gobierno, a los procesos, y a los

[12] SOX, acta de los Estados Unidos Sarbanes Oxley
[13] SEC, Securities and Exchange Comision

controles de TI. Una referencia de ello es su adopción por instituciones financieras, gubernamentales, de tecnología, y de salud entre otros. Otra referencia es la compañía de investigación de tecnología Gartner, la cual afirma en base a estudios realizados que "*COBIT se alinea con las mejores prácticas de administración de IT e incrementa la posibilidad de que su uso resultará en una mejor administración del ambiente de IT y especialmente de la administración del riesgo*."[14]

En resumen, se ha elegido a COBIT por su aproximación a la Administración de Riesgos de TI, confirmada por su aceptación como "una extensión" de los objetivos de control de COSO para las Tecnologías de la Información; y, debido a la aceptación que ha recibido como una mejor práctica. COSO no ha sido considerado debido a su enfoque en la administración del riesgo empresarial, lo cual sale del alcance de esta investigación.

Los principios planteados en la Resolución consideran elementos de RTI relacionados con el gobierno y el control de TI, es decir qué se debe hacer, para lo cual ya tenemos a COBIT. Adicionalmente, la Resolución define requerimientos técnicos específicos de TI, es decir cómo se debe hacer. En este contexto, nos hace falta un estándar de más bajo nivel en cuanto a su enfoque de RTI, el cual defina controles a nivel técnico para complementar la comparación. Para el efecto, esta investigación propone el estándar ISO 27002:2005.

ISO 27002:2005 está enfocado en la administración de la Seguridad de la Información, según la cual existen tres fuentes de requerimientos de seguridad: la evaluación de riesgos, las leyes y regulaciones, y los requerimientos comerciales. En función de estos, ISO propone un conjunto de controles que deben ser evaluados para su implementación. La aceptación a nivel internacional de este estándar es indiscutible, el cual ha venido siendo adoptado por instituciones a nivel mundial desde el año 1995, e inclusive existe emisión de certificaciones a través de la norma ISO 27001.

---

[14] Simon Mingay, Gartner, www.gartner.com.

Este documento no contiene todos los detalles de ISO/IEC 27002:2005, el nombre de los dominios y controles se citan con propósitos académicos. Se recomienda adquirir una copia del documento original de ISO disponible en su sitio web.

En conclusión, COBIT nos ofrecerá una visión desde el punto de vista de gobierno, procesos y control de IT considerando componentes de RTI, mientras que ISO, de un modo complementario, ofrecerá una visión más técnica y cercana a la implementación de los lineamientos de administración de RTI.

1.6 METODOLOGÍA

El desarrollo del presente trabajo está estructurado en tres fases. Las dos primeras corresponden al análisis comparativo y la última a la propuesta.

- Análisis comparativo de la Resolución JB-2005-834 respecto a COBIT 4.1.
- Análisis comparativo de la Resolución JB-2005-834 respecto a ISO-IEC 27002:2005.
- Propuesta de Mejoramiento de la Resolución JB-2005-834.

Según lo ilustra la figura 1, el análisis comparativo considera como punto de inicio a COBIT. El criterio de elección obedece al propósito de obtener en primera instancia una visión general de aspectos de Gobierno de TI; y, luego una visión más particular de los aspectos de Seguridad de la Información mediante ISO-IEC 27002:2005.

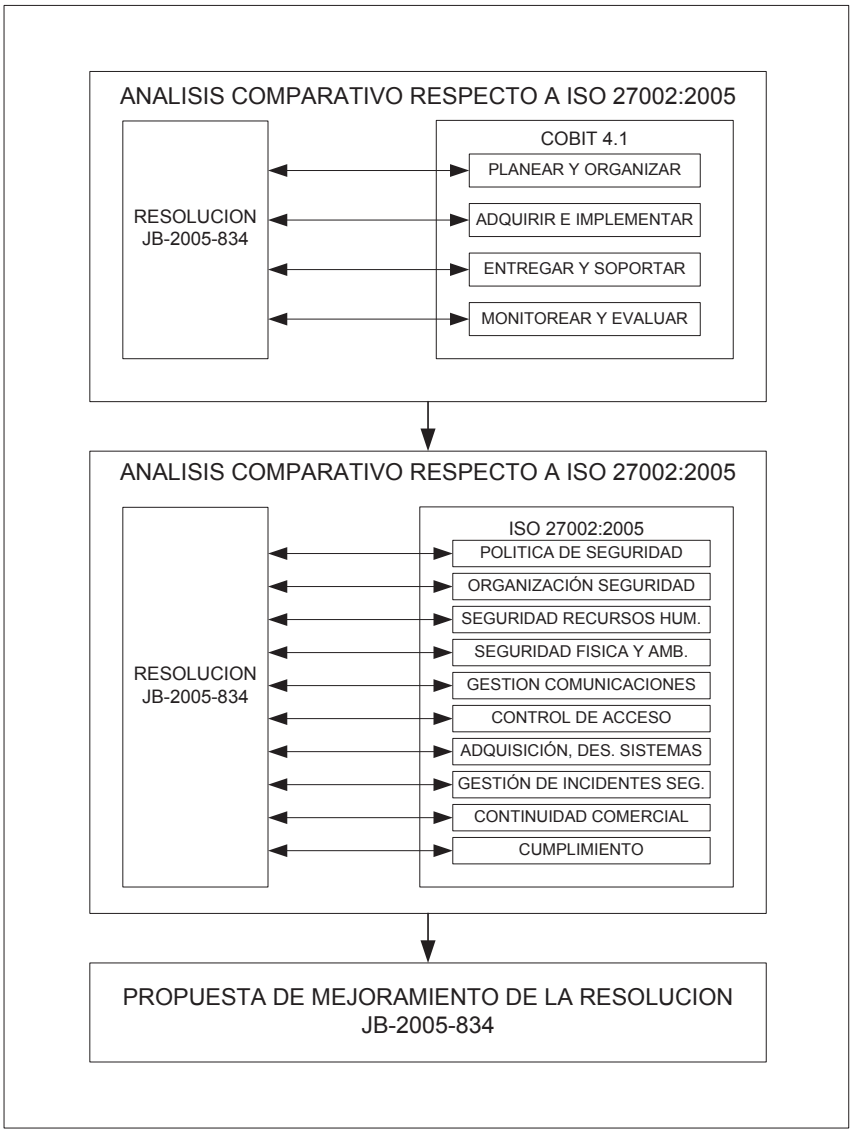

Figura 1. Metodología

1.6.1 ANÁLISIS DE LA RESOLUCIÓN JB-2005-834 RESPECTO A COBIT 4.1

Esta fase realiza el análisis comparativo de la Resolución JB-2005-834 respecto al marco de Gobierno para las Tecnologías de la Información de COBIT 4.1. El análisis comprende la comparación de la Resolución respecto a todos los dominios y objetivos de control de COBIT 4.1. Como resultado, se identificará las áreas de debilidad y fortaleza de la Resolución respecto a esta referencia, las cuales serán utilizadas como criterios de entrada para realizar la propuesta de mejoramiento.

1.6.2 ANÁLISIS DE LA RESOLUCIÓN JB-2005-834 RESPECTO A ISO-IEC 27002:2005

Esta fase realiza el análisis comparativo de la Resolución JB-2005-834 respecto al estándar denominado Código para la Práctica de la Gestión de Seguridad de la Información ISO-IEC 27002:2005. El análisis contempla la comparación de la Resolución respecto a todos los dominios, objetivos de control y controles de ISO-IEC 27002:2005. Como resultado, se identificará las áreas de debilidad y fortaleza de la Resolución respecto a esta segunda referencia, las cuales serán utilizadas como criterios adicionales para realizar la propuesta de mejoramiento.

1.6.3 PROPUESTA DE MEJORAMIENTO DE LA RESOLUCIÓN JB-2005-834

Esta fase define una propuesta de mejoramiento a la Resolución JB-2005-834. La propuesta considera la inclusión de objetivos de control ausentes en la Resolución conforme a dos criterios. El primero y más importante se refiere a las áreas de debilidad identificadas en las dos fases de análisis comparativo. El segundo se refiere a la fortaleza de los estándares según las áreas de debilidad para lo cual se analiza el enfoque que las dos referencias tienen respecto a la Administración de Riesgos de TI. La propuesta consistirá en un planteamiento de mejoramiento que considere los controles mínimos que deberían ser considerados en una actualización. Sin embargo, una segunda propuesta podría extraerse de los capítulos 2 y 3 de este documento al incorporar todos los controles COBIT e ISO ausentes en la Resolución JB-2005-834.

En resumen, el resultado del análisis que se rige a la metodología presentada, permitirá establecer el grado de alineamiento con el cual la Resolución JB-2005-834 está regulando el riesgo de TI en el ámbito financiero ecuatoriano, así como la propuesta de mejoramiento. Ahora que se conoce el tema de análisis y la metodología que describe como será abordado, el siguiente capítulo realizará el análisis comparativo respecto a COBIT.

CAPITULO 2
ANÁLISIS DE LA RESOLUCIÓN JB-2005-834 RESPECTO A COBIT 4.1

Este capítulo realiza el análisis comparativo de la Resolución JB-2005-834 respecto al marco de trabajo de COBIT en su versión 4.1, la cual fue liberada en Mayo de 2007. COBIT propone un marco de gobierno para las Tecnologías de la Información, el cual se basa en cinco áreas de enfoque que son: alineación estratégica, entrega de valor, administración de recursos, *administración de riesgos* y medición de desempeño. A pesar de que COBIT cubre un espectro más amplio que la gestión de riesgos, este marco ha sido considerado como una referencia para analizar la Resolución JB-2005-834 debido a que la gestión de riesgos no está aislada de los procesos de gobierno de TI. Por tanto, el análisis de este capítulo considerará todos los dominios y objetivos de control de COBIT 4.1.

El análisis comparativo permitirá detectar la brecha existente entre COBIT 4.1 y la Resolución JB-2005-834, la cual será expresada a través de un *Índice de Alineamiento* (IA) para cada objetivo de control de COBIT. Este índice es un número que puede variar entre cero y uno; y que expresa el grado de cumplimiento ó coincidencia que la Resolución JB-2005-834 tiene respecto a COBIT en cada uno de sus objetivos de control. Este índice permitirá identificar áreas susceptibles de mejora, las cuales serán abordadas en la propuesta de mejoramiento.

Este capítulo se encuentra estructurado en cinco secciones. La primera explica la estructura del marco de COBIT 4.1, necesaria para entender el procedimiento de comparación. La segunda identifica los criterios de información de COBIT requerido para identificar las maneras como la información puede ser expuesta al riesgo. La tercera explica la metodología de comparación. La cuarta sección realiza el análisis comparativo que estima el incide de alineamiento; y, finalmente la última sección realiza el análisis de los resultados donde se resume las áreas de fortaleza y debilidad.

2.1 ESTRUCTURA DE COBIT 4.1

COBIT se encuentra conformado por una estructura de cuatro dominios que agrupan 34 procesos de alto nivel, que a su vez dan lugar a 210 objetivos de control. Cada uno de estos objetivos guarda relación con las cinco *áreas de enfoque* del Gobierno de TI que incluye el alineamiento estratégico, la entrega de valor, la evaluación y gestión de riesgos, la gestión de recursos y la medición del desempeño.

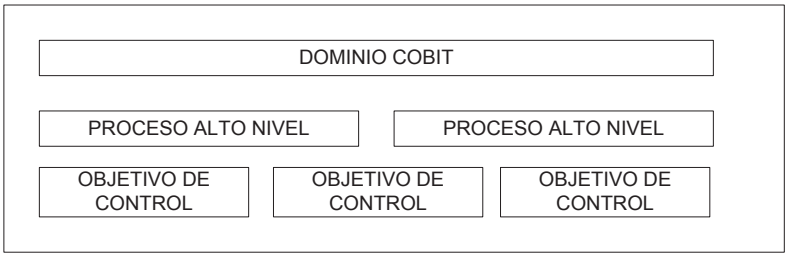

Figura 2. Estructura Marco COBIT

La estructura de la figura se aplica a cada uno de los cuatro dominios:

- Planear y Organizar
- Adquirir e Implementar
- Entregar y Soportar
- Monitorear y Evaluar

El análisis comparativo considera todos los procesos y los objetivos de control contenidos en estos dominios.

2.2 CRITERIOS DE LA INFORMACION DE COBIT 4.1

COBIT define los criterios de la información como requerimientos de la información por parte del negocio, los cuales incluyen conceptos de calidad, fiduciarios y de seguridad.

- La *efectividad* se refiere a la relevancia de la información para los procesos de negocio, a la oportunidad y consistencia de esta.

- La *eficiencia* se refiere a la optimización de uso de los recursos para generar la información de manera óptima.
- La *confidencialidad* se refiere a la protección de información sensitiva contra revelación no autorizada.
- La *integridad* se relaciona con la precisión y completitud de la información.
- La *disponibilidad* se refiere a que la información esté disponible cuando sea requerida por los procesos del negocio.
- El *cumplimiento*, tiene que ver con acatar aquellas leyes, reglamentos y acuerdos contractuales a los cuales está sujeto los procesos de negocios.
- La *confiabilidad*, se refiere a proporcionar la información apropiada para que la gerencia administre la entidad y ejerza sus responsabilidades fiduciarias y de gobierno.[15]

Los criterios de la información no tienen una relevancia uniforme en cada *proceso de alto nivel*. El Apéndice II de COBIT 4.1 en su sección "*COBIT Information Criteria*,"[16] especifica la importancia que cada *proceso de alto nivel* asigna a cada criterio de la información con la terminología de primario (P) y secundario (S); esto, dependiendo del grado de enfoque que un proceso ofrece a cada criterio. COBIT aclara que esto podría variar dependiendo de los usuarios y las metas de negocio particulares de una organización. Con el propósito de expresar gráficamente este concepto, vamos a realizar una aproximación matemática. Partiendo del Apéndice II de COBIT, asignaremos el valor de 1 para expresar la importancia primaria y 0.5 para expresar la importancia secundaria; el resultado se presenta en la siguiente figura y el detalle del cálculo en el Anexo A de este documento.

Según se observa en la figura 3, COBIT presenta un elevado enfoque en efectividad y eficiencia como consecuencia de su alineamiento al Gobierno de TI. En concordancia con lo expuesto, es lógico esperar un déficit relacionado con los criterios de la información en la Resolución JB-2005-834, ya que esta última tiene un enfoque en riesgo operacional.

[15] COBIT 4.1, pag. 10.
[16] El Apendice II de COBIT está incluido en el Anexo B de este documento

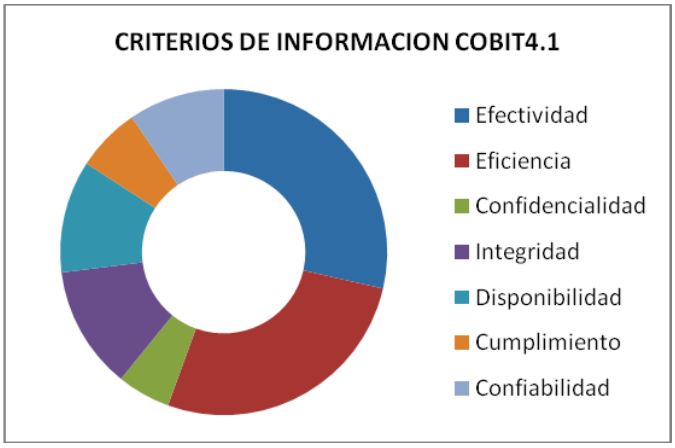

Figura 3. Criterios de la Información de COBIT 4.1

2.3 METODOLOGIA DEL ANÁLISIS COMPARATIVO

El análisis y cálculo de alineamiento se realizará mediante la identificación de la correspondencia entre los requerimientos planteados por COBIT y los enunciados de la Resolución JB-2005-834. El cálculo se fundamentará en un análisis del contenido de la Resolución JB-2005-834 respecto a COBIT, para luego ser representado en una estimación cuantitativa y cualitativa. La estimación cuantitativa se la conocerá como el Índice de Alineamiento (IA) y la estimación cualitativa como Calificación Cualitativa (CA).

2.3.1 DESRIPCION DEL PROCEDIMIENTO

La determinación del alineamiento de la Resolución JB-2005-834 para cada uno de los controles de COBIT se realiza mediante los siguientes pasos:

- Elección de un objetivo de control de COBIT.
- Identificación y documentación de requerimientos clave del objetivo de control. Estos requerimientos se refieren a los aspectos importantes del control.
- Búsqueda de los requerimientos clave en cada una de las secciones de la Resolución JB-2005-834. Esta búsqueda se realiza mediante dos métodos. El primero mediante lectura, análisis e interpretación de la Resolución JB-2005-834; y, el segundo mediante búsqueda electrónica múltiple con la asistencia de

un programa lector de formato PDF.[17] Generalmente los requerimientos clave se encuentran distribuidos en varias partes del documento, ya sea en un artículo o sub-artículo del mismo.

- Documentación de requerimientos clave del control así como los identificadores de artículo y sub-artículo con fines de referencia. Este detalle se encuentran en el Anexo K de este documento.
- Asignación cuantitativa al grado de alineamiento del objetivo de control en base a los criterios de valoración más adelante explicados.
- Asignación cualitativa al grado de alineamiento del objetivo de control en base a los criterios más adelante explicados.

2.3.2 ASIGNACION CUANTITATIVA

El valor del índice de alineamiento se obtiene a partir de la identificación de los requerimientos clave de cada objetivo de control en la Resolución JB-2005-834. Este valor se obtiene a partir de los siguientes criterios:

- Existirán cuatro posibles niveles expresados en términos numéricos: cero (0), (0.5), (0.75), y (1).
- Asignación (0): cuando los requerimientos clave del objetivo de control de COBIT no están contenidos en la Resolución JB-2005-834.
- Asignación (0.5); cuando aproximadamente la mitad de los requerimientos de COBIT se cumplen, ó cuando en la Resolución JB-2005-834 existe un enunciado general relativo al control, pero no se especifican detalles.
- Asignación (0.75); cuando los requerimientos de COBIT se cumplen sobre el 50% de las exigencias, pero no se encuentran completas.
- Asignación (1); cuando los requerimientos de COBIT se cumplen de manera exacta, aproximada al 100% ó se superan.

[17]PDF Portable Document Format

2.3.3 ASIGNACION CUALITATIVA

La asignación cualitativa se refiere a la calificación no numérica que describe el grado de alineamiento de cada objetivo de control de manera descriptiva; así:

- Asignación (N): (No considerado) cuando la asignación cuantitativa es cero (0).
- Asignación (P): (Parcialmente considerado) cuando la asignación cuantitativa es cero (0) ó (0.75).
- Asignación (C): (Completo) cuando la asignación cuantitativa es (1).

Como resultado, se obtendrá el parámetro CC (Calificación Cualitativa), el cual expresa el alineamiento en términos cualitativos.

En el análisis de correspondencia, las referencias numeradas de la Resolución JB-2005-834 (sección, artículo ó sub-artículo), así como la asignación cuantitativa y cualitativa para los 34 procesos y sus correspondientes objetivos de control, se encuentra en detalle en el Anexo K. A continuación se realiza el análisis para los cuatro dominios de COBIT y cada uno de sus procesos de alto nivel.

2.4 CORRESPONDENCIA ENTRE COBIT Y LA RESOLUCION JB-2005-834

2.4.1 DOMINIO PLANEAR Y ORGANIZAR (PO)

Este dominio considera diez procesos de alto nivel orientados a la planeación estratégica para direccionar los recursos de TI con los objetivos de negocio. Seguidamente se analiza el índice de alineamiento en la Resolución JB-2005-834 en cada uno de estos procesos.

2.4.1.1 PO1. Definir un Plan Estratégico de TI

Este proceso consta de seis objetivos de control, entre los objetivos considerados se encuentran: el alineamiento de los objetivos de TI con los de negocio, la identificación de procesos críticos y un plan funcional de TI. Sin embargo, no se ha considerado educación a ejecutivos sobre capacidades de TI actuales y futuras, no

se exige un análisis de la dependencia crítica que tienen las áreas de negocio de TI, así como tampoco se exige planes tácticos.

P01 Definir un Plan Estratégico		IA	CC
PO 1.1	Administración del Valor de TI	0.00	N
PO 1.2	Alineación de TI con el Negocio	0.75	P
PO 1.3	Evaluación del Desempeño y la Capacidad Actual	1.00	C
PO 1.4	Plan Estratégico de TI	1.00	C
PO 1.5	Planes Tácticos de TI	0.50	P
PO 1.6	Administración del Portafolio de TI	0.00	N
Número de Objetivos de Control Cubiertos		3.25	2C
Número de Objetivos de Control Requeridos		6	2P
Alineamiento R-JB-2005-834 respecto a COBIT 4.1		**0.54**	2N

Tabla 1. PO1 Definir un Plan Estratégico

Según el método explicado anteriormente, el índice de alineamiento es 0.54, mientras que la calificación cualitativa (CC) está expresada en términos de completitud; es decir, la Resolución considera PO1.3 y PO1.4 de manera completa, PO1.2 y PO1.5 de manera parcial, y PO1.1 y PO1.6 no están considerados. La calificación cualitativa se resume en las tres últimas celdas de la columna CC de esta manera:

- 2C: dos objetivos de control completamente considerados
- 2P: dos objetivos de control parcialmente considerados
- 2N: dos objetivos de control no considerados.

Todas las tablas subsiguientes en cada objetivo de control deben ser interpretadas de la misma manera.

2.4.1.2 PO2. Definir la Arquitectura de la Información

Respecto a la arquitectura de información se identifican dos fortalezas referidas a la clasificación de datos y a la integridad de la información. En contraste, no se ha considerado una estructura de datos corporativos mediante la cual se puedan tomar decisiones y tampoco se exige un diccionario de datos que incluya las reglas de sintaxis de datos de las instituciones financieras. El índice de alineamiento estimado es 0.5.

P02. Definir la Arquitectura de la Información		IA	CC
PO 2.1	Modelo de Arquitectura de Información Empresarial	0.0	N
PO 2.2	Diccionario de Datos Empresarial y Reglas de Sintaxis de Datos	0.0	N
PO 2.3	Esquema de Clasificación de Datos	1.0	C
PO 2.4	Administración de Integridad	1.0	C
Número de Objetivos de Control Cubiertos		2.00	2C
Número de Objetivos de Control Requeridos		4	0P
Alineamiento R-JB-2005-834 respecto a COBIT 4.1		**0.5**	2N

Tabla 2. PO2 Definir la Arquitectura de la Información

2.4.1.3 PO3. Determinar la Dirección Tecnológica

En el ámbito de este proceso, la Resolución realiza un énfasis en los temas regulatorios y normativos así como en el uso de estándares. La planeación de la dirección tecnológica no se encuentra totalmente definida como lo plantea COBIT; aunque si se menciona un plan funcional de TI, no se precisa detalles de lo que debe contener, como tampoco considera el análisis de las tecnologías existentes y emergentes como un apoyo a la planeación de TI. Por último, no se exige un consejo que oriente el diseño de la arquitectura de TI. El índice de alineamiento estimado es 0.5.

P03. Determinar la Dirección Tecnológica		IA	CC
PO 3.1	Planeación de la Dirección Tecnológica	0.75	P
PO 3.2	Plan de Infraestructura Tecnológica	0.25	P
PO 3.3	Monitoreo de Tendencias y Regulaciones Futuras	0.75	P
PO 3.4	Estándares Tecnológicos	0.75	P
PO 3.5	Consejo de Arquitectura de TI	0.00	N
Número de Objetivos de Control Cubiertos		2.50	0C
Número de Objetivos de Control Requeridos		5.00	4P
Alineamiento R-JB-2005-834 respecto a COBIT 4.1		**0.5**	1N

Tabla 3. PO3 Determinar la Dirección Tecnológica

2.4.1.4 PO4. Definir los Procesos, Organización y Relaciones de TI

Las exigencias de este proceso se han cubierto parcialmente; es decir siete de los quince objetivos de control se encuentran cubiertos casi en su totalidad. Dentro de estos se destaca la exigencia de planificación en base a un marco de trabajo de procesos, el establecimiento de roles y responsabilidades, la identificación de propiedad de datos y la segregación de funciones. En menor medida se aborda las exigencias de COBIT para el personal de TI.

Así también, existen varios objetivos de control que no son tratados, dejándose sin atención elementos fundamentales para el gobierno de TI que garantice una

dirección estratégica. En la Resolución no se establece la definición de un comité estratégico y un directivo de TI; como medida de compensación se exige un comité de administración integral de riesgos, el cual tiene un enfoque solamente en la administración de estos. Adicionalmente, no se establecen directrices sobre la estructura organizacional y la función de TI dentro de la misma, no se fomenta la comunicación del departamento de TI con las demás áreas de la empresa; por último, no se contemplan las directrices sobre aseguramiento de Calidad de TI. Según se expone en la tabla el índice de alineamiento estimado es 0.43.

P04. Definir los Procesos, Organización y Relaciones de TI		IA	CC
PO 4.1	Marco de Trabajo de Procesos de TI	1.00	C
PO 4.2	Comité Estratégico de TI	0.25	P
PO 4.3	Comité Directivo de TI	0.00	N
PO 4.4	Ubicación Organizacional de la Función de TI	0.00	N
PO 4.5	Estructura Organizacional	0.00	N
PO 4.6	Establecimiento de Roles y Responsabilidades	1.00	C
PO 4.7	Responsabilidad de Aseguramiento de Calidad de TI	0.25	P
PO 4.8	Responsabilidad sobre el Riesgo, la Seguridad y el Cumplimiento	1.00	C
PO 4.9	Propiedad de Datos y de Sistemas	0.75	P
PO 4.10	Supervisión	0.00	N
PO 4.11	Segregación de Funciones	1.00	C
PO 4.12	Personal de TI	0.75	P
PO 4.13	Personal Clave de TI	0.00	N
PO 3.14	Políticas y Procedimientos para Personal Contratado	0.50	P
PO 4.15	Relaciones	0.00	N
Número de Objetivos de Control Cubiertos		6.50	4C
Número de Objetivos de Control Requeridos		15	5P
Alineamiento R-JB-2005-834 respecto a COBIT 4.1		**0.43**	6N

Tabla 4. PO4 Definir los Procesos, Organización y Relaciones de TI

2.4.1.5 PO5. Administrar la Inversión en TI

El proceso de administración de la inversión financiera en TI no ha sido exigido en ningún aspecto. Es decir, no se establece un marco de trabajo para su administración, no se toma en cuenta la priorización de asignación de recursos para la operación, proyectos y mantenimiento en TI. Tampoco se plantea la medición del grado de retorno al portafolio empresarial por lo que no se puede tomar decisiones para optimizarlo. No se exige planificación de un presupuesto general de TI y presupuestos de programas individuales, y por tanto tampoco la revisión, refinamiento y aprobación de los mismos. La administración de costos que compare costo real y presupuestado se ha omitido, así como el monitoreo y reporte de desviaciones e impacto. En estas condiciones no se puede conocer el

grado de contribución de TI a resultados de negocio; evidentemente el índice de alineamiento es 0.

P05. Administrar la Inversión en TI		IA	CC
PO 5.1	Marco de Trabajo para la Administración Financiera	0.00	N
PO 5.2	Prioridades dentro del presupuesto de TI	0.00	N
PO 5.3	Proceso Presupuestal	0.00	N
PO 5.4	Administración de Costos de TI	0.00	N
PO 5.5	Administración de Beneficios	0.00	N
Número de Objetivos de Control Cubiertos		0.00	0C
Número de Objetivos de Control Requeridos por este Proceso		5	0P
Cumplimiento de R-JB-2005-834 respecto a COBIT 4.1		**0.0**	5N

Tabla 5. PO5 Administrar la Inversión en TI

2.4.1.6 PO6. Comunicar las Aspiraciones y la Dirección de la Gerencia

Las exigencias de este proceso referidas a riesgo corporativo, control interno de TI, y administración e implantación de políticas de TI se encuentran cubiertas. COBIT demanda un enfoque empresarial hacia los riesgos y control, la Resolución JB-2005-834 se refiere a este enfoque como administración integral de riesgos, y sobre este aspecto hace referencia al capítulo I de la Resolución JB-2004-63 “De la gestión integral y control de riesgos” del “TITULO X.- DE LA GESTION Y ADMINISTRACION DE RIESGOS”, donde se exponen exigencias de riesgo corporativo; entre ellos: riego de crédito, de mercado, operativo, de liquidez, legal, de tasa de interés, de tipo de cambio y de reputación; aquí se definen los preceptos para su administración y responsabilidades. En este ámbito no se menciona el control de la política de TI que se exige en el proceso PO6.

La administración e implantación de políticas de TI tienen un soporte amplio por parte de la Resolución JB-2005-834. Se exige su creación, difusión, comunicación y su implementación, así como también se demanda que los controles formen parte integral de las actividades regulares de la entidad.

Los aspectos ausentes se encuentran a nivel de las expectativas de la gerencia respecto a la entrega de valor sobre: inversiones en TI, apetito de riesgo, integridad y valores éticos. Por último, no se exige explícitamente comunicación de objetivos negocio y de TI a interesados y usuarios. Según se expone en la tabla, el índice de alineamiento estimado es 0.65.

P06. Comunicar las Aspiraciones y la Dirección de la Gerencia		IA	CC
PO 6.1	Ambiente de Políticas y de Control	0.25	P
PO 6.2	Riesgo Corporativo y Marco de Referencia de Control Interno de TI	1.00	C
PO 6.3	Administración de Políticas para TI	1.00	C
PO 6.4	Implantación de Políticas de TI	1.00	C
PO 6.5	Comunicación de los Objetivos y la Dirección de TI	0.00	N
Número de Objetivos de Control Cubiertos		3.25	3C
Número de Objetivos de Control Requeridos por este Proceso		5	1P
Cumplimiento de R-JB-2005-834 respecto a COBIT 4.1		**0.65**	1N

Tabla 6. PO6 Comunicar las Aspiraciones y la Dirección de la Gerencia

2.4.1.7 PO7. Administrar los Recursos Humanos de TI

Existe una amplia cobertura de casi todos los objetivos de control de este proceso, sin embargo la mayoría abarca solamente un contenido parcial de los planteamientos de COBIT. Entre los conceptos omitidos se encuentran: la ausencia de participación de la gerencia para garantizar que la institución cuenta con el recurso humano para alcanzar las metas de negocio, la definición de habilidades esenciales para TI, la supervisión de roles y responsabilidades; y, los métodos de compensación del personal. Adicional, no se menciona la dependencia sobre los individuos, su conciencia sobre la seguridad, ni se establecen procedimientos de investigación del personal. Finalmente, se aborda el proceso de terminación de trabajo, pero no se considera la reasignación de responsabilidades ni la eliminación de privilegios de acceso. Según se expone en la tabla, el índice de alineamiento estimado es del 0.53.

P07. Administrar los Recursos Humanos de TI		IA	CC
PO 7.1	Reclutamiento y Retención del Personal	0.75	P
PO 7.2	Competencias del Personal	0.75	P
PO 7.3	PO7.3 Asignación de Roles	0.25	P
PO 7.4	Entrenamiento del Personal de TI	0.75	P
PO 7.5	Dependencia Sobre los Individuos	0.00	N
PO 7.6	Procedimientos de Investigación del Personal	0.25	P
PO 7.7	Evaluación del Desempeño del Empleado	0.75	P
PO 7.8	Cambios y Terminación de Trabajo	0.75	P
Número de Objetivos de Control Cubiertos		4.25	0C
Número de Objetivos de Control Requeridos por este Proceso		8	7P
Cumplimiento de R-JB-2005-834 respecto a COBIT 4.1		**0.53**	1N

Tabla 7. P07 Administrar los Recursos Humanos de TI

2.4.1.8 PO8.Administrar la Calidad

El enfoque de calidad de la Resolución radica en exigencias generales sobre la calidad de los productos, servicios, materiales, equipos y la información sometida a migración. El objetivo de control mejor considerado por la Resolución en este proceso es el referido a "*PO 8.3 Estándares de Desarrollo y de Adquisición,*" para el cual la Resolución exige un proceso de adquisición y desarrollo que contenga una metodología para la administración y control de compra de software.

En los restantes objetivos de control, las exigencias de este proceso son ignorados en gran medida en la Resolución. No se menciona un Sistema de Administración de Calidad (QMS) y por tanto sus propiedades, requerimientos, beneficios y todos los procesos que lo soportan están ausentes. El índice de alineamiento estimado es del 0.17.

P08. Administrar la Calidad		**IA**	**CC**
PO 8.1	Sistema de Administración de Calidad	0.75	P
PO 8.2	Estándares y Prácticas de Calidad	0.25	P
PO 8.3	Estándares de Desarrollo y de Adquisición	0.00	N
PO 8.4	Enfoque en el Cliente de TI	0.00	N
PO 8.5	Mejora Continua	0.00	N
PO 8.6	Medición, Monitoreo y Revisión de la Calidad	0.00	N
Número de Objetivos de Control Cubiertos		1.00	0C
Número de Objetivos de Control Requeridos por este Proceso		6	2P
Cumplimiento de R-JB-2005-834 respecto a COBIT 4.1		**0.17**	4N

Tabla 8. PO8 Administrar la Calidad

2.4.1.9 PO9. Evaluar y Administrar los Riesgos de TI

En comparación con todos los procesos del dominio Planificación y Organización, este proceso guarda una relación más estricta y completa con el propósito de la Resolución JB-2005-834. Según el análisis realizado, la Resolución recoge cuatro de los seis controles del proceso de manera casi completa y deja sin consideración dos de los mismos.

COBIT exige establecer un marco de trabajo de *Administración de Riesgos* de TI alineado a la administración de riesgos de la organización. La Resolución asume que existe una evaluación de los riesgos en la institución debido a que esta es

exigida en el Libro I[18], Titulo X: “DE LA GESTION Y ADMINISTRACION DE RIESGOS”, Capítulo I “De la gestión integral y control de riesgos” donde se puntualiza sobre la existencia obligatoria de una administración integral de Riesgos.

La *Identificación de Eventos* que podrían provocar un impacto negativo en los negocios son considerados de manera amplia. Así, la Resolución JB-2005-834 contempla riesgos por fallas en las tecnologías de información, personas y procesos; como también temas legales y normativos. Adicionalmente, la Resolución JB-2005-834 adjunta el *Anexo No.1* con una matriz que contiene detalles sobre los tipos de eventos que deberían considerarse.

Sobre la *Evaluación de Riesgos*, COBIT establece la necesidad de evaluar la probabilidad y el impacto de los riesgos identificados mediante métodos cualitativos y cuantitativos. Al respecto la Resolución no especifica detalles sobre la valoración cuantitativa o cualitativa, se deja libertad para el uso de la metodología de cálculo de probabilidad y la determinación de la “Incidencia para la institución” de pérdidas esperadas (artículo 11). La Resolución es enfática en su artículo 5 al pedir “*Identificar, medir, controlar/mitigar y monitorear la exposición al riesgo*”. Con estas exigencias se cubre aproximadamente un 75% de los requerimientos de COBIT en relación a este objetivo de control.

En lo que se refiere a *Respuesta a los Riesgos,* COBIT exige eficiencia y eficacia de los controles de mitigación así como la implantación de estrategias para evitar el riesgo en términos de evitar, mitigar o aceptarlo. La Resolución en su artículo 10 por su parte, insta a que los directivos decidan si el riesgo se debe asumir, compartirlo, evitarlo o transferirlo, reduciendo sus consecuencias y efectos. Según se mencionó el artículo 5 cumple con estos criterios, por lo que prácticamente existe una coincidencia total entre los dos planteamientos.

---

[18] Normas Generales Para La Aplicación De La Ley General De Instituciones Del Sistema Financiero

En contraste a lo expuesto, no se han considerado el objetivo de control "*Establecimiento del Contexto del Riesgo",* por lo que se deja de lado la definición del marco de trabajo de evaluación de riesgos para garantizar resultados apropiados y los criterios contra los cuales se evalúan los riesgos.

Por último, el objetivo de control *"Mantenimiento y Monitoreo de un Plan de Acción de Riesgos"* se ha cubierto en una mínima parte. Es decir la priorización y planificación de repuesta a riesgos; así como sus costos, beneficios, monitoreo de desviaciones no se enfatizan. En referencia a este control, la Resolución en su artículo 10 enumera acciones, estrategias, políticas y otras iniciativas de respuesta. El índice de alineamiento estimado es del 0.67.

P09. Evaluar y Administrar los Riesgos de TI		**IA**	**CC**
PO 9.1	Marco de Trabajo de Administración de Riesgos	1.00	C
PO 9.2	Establecimiento del Contexto del Riesgo	0.00	N
PO 9.3	Identificación de Eventos	1.00	C
PO 9.4	Evaluación de Riesgos de TI	0.75	P
PO 9.5	Respuesta a los Riesgos	1.00	C
PO 9.6	Mantenimiento y Monitoreo de un Plan de Acción de Riesgos	0.25	P
Número de Objetivos de Control Cubiertos		4.00	3C
Número de Objetivos de Control Requeridos por este Proceso		6	2P
Cumplimiento de RJB-2005-834 respecto a COBIT 4.1		**0.67**	1N

Tabla 9. P09 Evaluar y Administrar los Riesgos de TI

2.4.1.10 PO10 Administrar Proyectos

Este objetivo de control establece lineamientos de administración de programas y proyectos de TI. Entre los que se destacan: la inversión en el proyecto, el control, el alineamiento, las metodologías, el alcance, la rendición de cuentas, la participación de los interesados, su relación con otros proyectos, el manejo de riesgos del proyecto, la calidad, los cambios la seguridad embebida, el desempeño y el proceso de cierre. La Resolución no contempla estos principios por lo que el índice de alineamiento es 0.

P10. Administrar Proyectos		IA	CC
PO 10.1	Marco de Trabajo para la Administración de Programas	0.00	N
PO 10.2	Marco de Trabajo para la Administración de Proyectos	0.00	N
PO 10.3	Enfoque de Administración de Proyectos	0.00	N
PO 10.4	Compromiso de los Interesados	0.00	N
PO 10.5	Declaración de Alcance del Proyecto	0.00	N
PO 10.6	Inicio de las Fases del Proyecto	0.00	N
PO 10.7	Plan Integrado del Proyecto	0.00	N
PO 10.8	Recursos del Proyecto	0.00	N
PO 10.9	Administración de Riesgos del Proyecto	0.00	N
PO 10.10	Plan de Calidad del Proyecto	0.00	N
PO 10.11	Control de Cambios del Proyecto	0.00	N
PO 10.12	Planeación del Proyecto y Métodos de Aseguramiento	0.00	N
PO 10.13	Medición del Desempeño, Reporte y Monitoreo del Proyecto	0.00	N
PO 10.14	Cierre del Proyecto	0.00	N
Número de Objetivos de Control Cubiertos		0.00	0C
Número de Objetivos de Control Requeridos por este Proceso		14	0P
Cumplimiento de R-JB-2005-834 respecto a COBIT 4.1		**0.00**	14N

Tabla 10. P010 Administrar Proyectos

De esta manera se han cubierto todos los objetivos de control que pertenecen al dominio Planear y Organizar (PO).

2.4.2 DOMINIO ADQUIRIR E IMPLEMENTAR (AI)

Este dominio considera siete procesos de alto nivel orientados a la ejecución de la estrategia de TI mediante identificación, desarrollo ó adquisición de de soluciones de IT para ser integradas a los procesos de negocio de una organización, en este caso financiera. Seguidamente se analiza el índice de alineamiento en la Resolución JB-2005-834 en cada uno de estos procesos.

2.4.2.1 AI1 Identificar Soluciones Automatizadas

Este objetivo de control busca que los requerimientos de negocio estén adecuadamente identificados y reflejados en los programas de inversión de TI. Además establece que: se realice el reporte de riesgos asociados con los requerimientos de negocio y diseño de soluciones, el estudio de factibilidad que permita implementar estos requerimientos, y por último que el patrocinador del negocio realice las funciones de aprobación y decisión sobre las soluciones y adquisiciones relacionadas. La Resolución no contempla estos principios por lo que el cumplimiento es 0.

AI1 Identificar Soluciones Automatizadas		IA	CC
AI1.1	Definición y Mantenimiento de los Requerimientos Técnicos y Funcionales del Negocio	0.00	N
AI1.2	Reporte de Análisis de Riesgos	0.00	N
AI1.3	Estudio de Factibilidad y Formulación de Cursos de Acción Alternativos	0.00	N
AI1.4	Requerimientos, Decisión de Factibilidad y Aprobación	0.00	N
Número de Objetivos de Control Cubiertos		0.00	0C
Número de Objetivos de Control Requeridos por este Proceso		4	0P
Cumplimiento de R-JB-2005-834 respecto a COBIT 4.1		**0.00**	4N

Tabla 11. AI1 Identificar Soluciones Automatizadas

2.4.2.2 AI2 Adquirir y Mantener Software Aplicativo

Este proceso se enfoca en el diseño de las aplicaciones, la inclusión de controles, requerimientos de seguridad y definiciones para su mantenimiento. La Resolución solamente cubre aspectos relativos al mantenimiento y cambios en las aplicaciones, dejando por fuera temas relacionados con el diseño, configuración, implantación y administración de requerimientos de las aplicaciones. Además, respecto a la seguridad mantiene un enfoque sobre la información, pero no se realiza énfasis sobre las aplicaciones o sistemas de software.

AI2. Adquirir y Mantener Software Aplicativo		IA	CC
AI2.1	Diseño de Alto Nivel	0.00	N
AI2.2	Diseño Detallado	0.00	N
AI2.3	Control y Posibilidad de Auditar las Aplicaciones	0.25	P
AI2.4	Seguridad y Disponibilidad de las Aplicaciones	0.25	P
AI2.5	Configuración e Implantación de Software Aplicativo Adquirido	0.00	N
AI2.6	Actualizaciones Importantes en Sistemas Existentes	0.75	P
AI2.7	Desarrollo de Software Aplicativo	0.50	P
AI2.8	Aseguramiento de la Calidad del Software	0.00	N
AI2.9	Administración de los Requerimientos de Aplicaciones	0.00	N
AI2.10	Mantenimiento de Software Aplicativo	1.00	C
Número de Objetivos de Control Cubiertos		2.75	1C
Número de Objetivos de Control Requeridos por este Proceso		10	4P
Cumplimiento de R-JB-2005-834 respecto a COBIT 4.1		**0.28**	5N

Tabla 12. AI2 Adquirir y Mantener Software Aplicativo

2.4.2.3 AI3 Adquirir y Mantener Infraestructura Tecnológica

La Resolución ha considerado dos de los cuatros controles exigidos, aunque lo hace de manera incompleta. El primero está referido a la "*Protección y Disponibilidad del Recurso de Infraestructura*", donde se exige que la tecnología de información garantice "*La captura, procesamiento, almacenamiento y transmisión de la información de manera oportuna y confiable*"[19] y agrega las propiedades de integridad y confidencialidad para la información. Esto no se lo

[19] Resolución JB-2005-834, Articulo 4, Numeral 4.3

hace para el hardware ni software de infraestructura. Por otro lado nunca la mención de control sobre la configuración de los sistemas y la auditabilidad solo se circunscribe a los sistemas de seguridad. Otro objetivo de control considerado parcialmente por la Resolución es "*Mantenimiento de la Infraestructura*", el cual exige un plan de mantenimiento, control de cambios y administración de parches; de estos solo se considera el primer requerimiento.

Los otros dos controles ignorados completamente son "*Plan de Adquisición de Infraestructura Tecnológica*", donde COBIT demanda garantizar la satisfacción de los requerimientos funcionales y técnicos del negocio; y, "*Ambiente de Prueba de Factibilidad*", donde se demanda un ambiente de desarrollo y pruebas de integración de aplicaciones e infraestructura, desempeño, migración entre ambientes, control de la versiones, datos y herramientas de prueba y seguridad. Si bien la Resolución exige en su numeral 4.3.6.3 "*Controles que permitan asegurar la adecuada administración de versiones de las aplicaciones puestas en producción*" estas se delimitan a las aplicaciones y no abarca la infraestructura de hardware y software.

AI3 Adquirir y Mantener Infraestructura Tecnológica		**IA**	**CC**
AI3.1	Plan de Adquisición de Infraestructura Tecnológica	0.25	P
AI3.2	Protección y Disponibilidad del Recurso de Infraestructura	0.75	P
AI3.3	Mantenimiento de la Infraestructura	0.50	P
AI3.4	Ambiente de Prueba de Factibilidad	0.00	N
Número de Objetivos de Control Cubiertos		1.50	0C
Número de Objetivos de Control Requeridos por este Proceso		4	3P
Cumplimiento de R-JB-2005-834 respecto a COBIT 4.1		**0.38**	1N

Tabla 13. AI3 Adquirir y Mantener Infraestructura Tecnológica

2.4.2.4 AI4 Facilitar la Operación y el Uso

Este proceso basa sus lineamientos en la operación de TI y los elementos requeridos para ejecutarla; es decir, los procedimientos, el entrenamiento de usuarios y técnicos; y, el conocimiento correspondiente por parte de la gerencia. En alineamiento con este proceso, la Resolución exige la presencia de una infraestructura tecnológica documentada así como el entrenamiento técnico y de los usuarios. El único control que no se aborda es la "*Transferencia de Conocimiento a la Gerencia del Negocio*".

AI4 Facilitar la Operación y el Uso		IA	CC
AI4.1	Plan para Soluciones de Operación	0.75	P
AI4.2	Transferencia de Conocimiento a la Gerencia del Negocio	0.00	N
AI4.3	Transferencia de Conocimiento a Usuarios Finales	0.75	P
AI4.4	Transferencia de Conocimiento al Personal de Operaciones y Soporte	1.00	C
Número de Objetivos de Control Cubiertos		2.50	1C
Número de Objetivos de Control Requeridos por este Proceso		4	2P
Cumplimiento de R-JB-2005-834 respecto a COBIT 4.1		**0.63**	1N

Tabla 14. AI4 Facilitar la Operación y el Uso

2.4.2.5 AI5 Adquirir Recursos de TI

La Resolución se muestra bastante fuerte en los objetivos de control relacionados con la administración de contratos con proveedores y a la selección de los mismos; cumpliéndose con casi todos los requerimientos planteados por COBIT. Sin embargo, en el "*Control de Adquisición*" solo se consideran las aplicaciones pero no la infraestructura de TI y tampoco hay mención de una estrategia de adquisición. De la misma manera no se menciona la búsqueda de los intereses de la organización durante la "*Adquisición de Recursos de TI.*"

AI5 Adquirir Recursos de TI		IA	CC
AI5.1	Control de Adquisición	0.25	P
AI5.2	Administración de Contratos con Proveedores	1.00	C
AI5.3	Selección de Proveedores	1.00	C
AI5.4	Adquisición de Recursos de TI	0.00	N
Número de Objetivos de Control Cubiertos		2.25	2C
Número de Objetivos de Control Requeridos por este Proceso		4	1P
Cumplimiento de R-JB-2005-834 respecto a COBIT 4.1		**0.56**	1N

Tabla 15. AI5 Adquirir Recursos de TI

2.4.2.6 AI6 Administrar Cambios

Existe un gran vacío en el cumplimiento de este proceso en la Resolución 834. Únicamente se considera un control con mayor énfasis, uno parcialmente y tres se omiten. De hecho el contenido de la Resolución 834 solamente cuenta con un punto (4.3.1.4) relacionado a este tema que dice: "*Un responsable de la información que se encargue principalmente de definir y autorizar de manera formal los accesos y cambios funcionales a las aplicaciones.*"[20] Esta exigencia no es suficiente para cubrir los cuatro objetivos de control que plantea COBIT para este proceso.

[20] Resolución No JB-2005-834, Artículo 4, Numeral, 4.3.1.4

AI6 Administrar Cambios		IA	CC
AI6.1	Estándares y Procedimientos para Cambios	0.75	P
AI6.2	Evaluación de Impacto, Priorización y Autorización	0.25	P
AI6.3	Cambios de Emergencia	0.00	N
AI6.4	Seguimiento y Reporte del Estatus de Cambio	0.00	N
AI6.5	Cierre y Documentación del Cambio	0.00	N
Número de Objetivos de Control Cubiertos		1.00	0C
Número de Objetivos de Control Requeridos por este Proceso		5	2P
Cumplimiento de R-JB-2005-834 respecto a COBIT 4.1		**0.20**	3N

Tabla 16. AI6 Administrar Cambios

2.4.2.7 AI7 Instalar y Acreditar Soluciones y Cambios

Similar a lo que ocurrió en el proceso inmediato anterior, es muy poco lo que la Resolución exige en este tema. Solamente un objetivo de control está considerado, el cual se refiere a la "*Conversión de Sistemas y Datos*". La Resolución es muy enfática al demandar un aseguramiento de la calidad de la información sometida a migración, de hecho exige las tres propiedades de seguridad para este proceso integridad, disponibilidad y confidencialidad.

AI7 Instalar y Acreditar Soluciones y Cambios		IA	CC
AI7.1	Entrenamiento	0.00	N
AI7.2	Plan de Prueba	0.00	N
AI7.3	Plan de Implantación	0.00	N
AI7.4	Ambiente de Prueba	0.00	N
AI7.5	Conversión de Sistemas y Datos	1.00	C
AI7.6	Pruebas de Cambios	0.00	N
AI7.7	Prueba de Aceptación Final.	0.00	N
AI7.8	Promoción a Producción	0.00	N
AI7.9	Revisión Posterior a la Implantación	0.00	N
Número de Objetivos de Control Cubiertos		1.00	1C
Número de Objetivos de Control Requeridos por este Proceso		9	0P
Cumplimiento de R-JB-2005-834 respecto a COBIT 4.1		**0.11**	8N

Tabla 17. AI7 Instalar y Acreditar Soluciones y Cambios

2.4.3 ENTREGAR Y SOPORTAR

Este dominio considera trece procesos de alto nivel orientados a la entrega de los servicios que incluye aspectos de seguridad, continuidad, soporte a usuarios, administración de datos y de instalaciones operacionales.

2.4.3.1 DS1 Definir y Administrar los Niveles de Servicio

La Resolución 834 exige en su numeral 20.2 la existencia de niveles mínimos de servicios, pero hace falta especificar detalles sobre la administración de SLA,[21] así

[21] SLA Service Level Agreement

como también mencionar acuerdos de operación OLA.[22] Debido a la ausencia de estos objetivos de control podría presentarse una falta de alineamiento entre los servicios de TI y los requerimientos de negocio.

DS1 Definir y Administrar los Niveles de Servicio		IA	CC
DS1.1	Marco de Trabajo de la Administración de los Niveles de Servicio	0.25	P
DS1.2	Definición de Servicios	0.00	N
DS1.3	Acuerdos de Niveles de Servicio	0.75	P
DS1.4	Acuerdos de Niveles de Operación	0.00	N
DS1.5	Monitoreo y Reporte del Cumplimento de los Niveles de Servicio	1.00	C
DS1.6	Revisión de los Acuerdos de Niveles de Servicio y de los Contratos	0.25	P
Número de Objetivos de Control Cubiertos		2.25	1C
Número de Objetivos de Control Requeridos por este Proceso		6	3P
Cumplimiento de R-JB-2005-834 respecto a COBIT 4.1		**0.38**	2N

Tabla 18. DS1 Definir y Administrar los Niveles de Servicio

2.4.3.2 DS2 Administrar los Servicios de Terceros

La Resolución 834 dedica varios puntos al control de la relación con terceros; sin embargo, se puede mejorar en la categorización de proveedores, documentación formal de roles y responsabilidades, metas, entregables, esperados, y credenciales de estos proveedores.

DS2 Administrar los Servicios de Terceros		IA	CC
DS2.1	Identificación de Todas las Relaciones con Proveedores	0.25	P
DS2.2	Gestión de Relaciones con Proveedores	0.50	P
DS2.3	Administración de Riesgos del Proveedor	1.00	C
DS2.4	Monitoreo del Desempeño del Proveedor	1.00	C
Número de Objetivos de Control Cubiertos		2.75	2C
Número de Objetivos de Control Requeridos por este Proceso		4	2P
Cumplimiento de R-JB-2005-834 respecto a COBIT 4.1		**0.69**	0N

Tabla 19. DS2 Administrar los Servicios de Terceros

2.4.3.3 DS3 Administrar el Desempeño y la Capacidad

La Resolución 834 no se exige planeación de la capacidad del desempeño, pero si se enfoca en el resultado de disponer sistemas Tecnología de información acorde a las operaciones del negocio y al volumen de transacciones. Sin embargo hay exigencias de COBIT muy específicas que no están cubiertas; por ejemplo, identificación de tendencias y redistribución de carga.

[22] OLA Operation Level Agreement

DS3 Administrar el Desempeño y la Capacidad		IA	CC
DS3.1	Planeación del Desempeño y la Capacidad	0.25	P
DS3.2	Capacidad y Desempeño Actual	0.75	P
DS3.3	Capacidad y Desempeño Futuros	0.75	P
DS3.4	Disponibilidad de Recursos de TI	0.50	P
DS3.5	Monitoreo y Reporte	0.75	P
Número de Objetivos de Control Cubiertos		3.00	0C
Número de Objetivos de Control Requeridos por este Proceso		5	5P
Cumplimiento de R-JB-2005-834 respecto a COBIT 4.1		**0.60**	0N

Tabla 20. DS3 Administrar el Desempeño y la Capacidad

2.4.3.4 DS4 Garantizar la Continuidad del Servicio

La Resolución 834 cubre satisfactoriamente casi todos los requerimientos de este objetivo de control, el cual es significativamente exigente. Existe un vacío relativamente muy leve en la coordinación de la post reanudación.

DS4 Garantizar la Continuidad del Servicio		IA	CC
DS4.1	Marco de Trabajo de Continuidad de TI	1.00	C
DS4.2	Planes de Continuidad de TI	1.00	C
DS4.3	Recursos Críticos de TI	0.75	P
DS4.4	Mantenimiento del Plan de Continuidad de TI	1.00	C
DS4.5	Pruebas del Plan de Continuidad de TI	1.00	C
DS4.6	Entrenamiento del Plan de Continuidad de TI	1.00	C
DS4.7	Distribución del Plan de Continuidad de TI	1.00	C
DS4.8	Recuperación y Reanudación de los Servicios de TI	1.00	C
DS4.9	Almacenamiento de Respaldos Fuera de las Instalaciones	1.00	C
DS4.10	Revisión Post Reanudación	0.50	P
Número de Objetivos de Control Cubiertos		9.25	8C
Número de Objetivos de Control Requeridos por este Proceso		10	2P
Cumplimiento de R-JB-2005-834 respecto a COBIT 4.1		**0.93**	0N

Tabla 21. DS4 Garantizar la Continuidad del Servicio

2.4.3.5 DS5 Garantizar la Seguridad de los Sistemas

La Resolución contempla la mayoría de los factores de administración de la seguridad planteada en este objetivo, pero lo hace de manera incompleta. Las áreas más débiles se encuentran en el uso de técnicas criptográficas y la seguridad en la red. Sobre la criptografía la única mención que se hace se refiere al procesamiento de transferencias y transacciones electrónicas sobre medios seguros que utilicen técnicas de encriptación, es decir solamente en el canal de comunicaciones. Mientras que respecto a la red se menciona administración y monitoreo sin especificar controles de filtrado, segmentación, detección o prevención de intrusos.

DS5 Garantizar la Seguridad de los Sistemas		IA	CC
DS5.1	Administración de la Seguridad de TI	0.75	P
DS5.2	Plan de Seguridad de TI	0.50	P
DS5.3	Administración de Identidad	0.75	P
DS5.4	Administración de Cuentas del Usuario	1.00	C
DS5.5	Pruebas, Vigilancia y Monitoreo de la Seguridad	0.50	P
DS5.6	Definición de Incidente de Seguridad	0.50	P
DS5.7	Protección de la Tecnología de Seguridad	0.50	P
DS5.8	Administración de Llaves Criptográficas	0.00	N
DS5.9	Prevención, Detección y Corrección de Software Malicioso	0.75	P
DS5.10	Seguridad de la Red	0.25	P
DS5.11	Intercambio de Datos Sensitivos	0.75	P
Número de Objetivos de Control Cubiertos		6.25	1C
Número de Objetivos de Control Requeridos por este Proceso		11	9P
Cumplimiento de R-JB-2005-834 respecto a COBIT 4.1		**0.57**	1N

Tabla 22. DS5 Garantizar la Seguridad de los Sistemas

Cumplimiento legal pudiera estar comprometido debido a falta de observación de regulaciones ambientales y los activos pudieran estar comprometidos por falta de vigilancia en áreas de carga.

2.4.3.6 DS6 Identificar y Asignar Costos

Este objetivo de control busca identificar y asignar costos para satisfacer los requerimientos del negocio de TI, el entendimiento de los costos de TI, el manejo transparente y el mejoramiento de la relación costo-eficiencia. La Resolución no contempla estos principios.

DS6 Identificar y Asignar Costos		IA	CC
DS6.1	Definición de Servicios	0.00	N
DS6.2	Contabilización de TI	0.00	N
DS6.3	Modelación de Costos y Cargos	0.00	N
DS6.4	Mantenimiento del Modelo de Costos	0.00	N
Número de Objetivos de Control Cubiertos		0.00	0C
Número de Objetivos de Control Requeridos		4	0P
Alineamiento R-JB-2005-834 respecto a COBIT 4.1		**0.00**	4N

Tabla 23. DS6 Identificar y Asignar Costos

2.4.3.7 DS7 Educar y Entrenar a los Usuarios

En este objetivo de control COBIT establece un plan de entrenamiento, el modo óptimo de impartición del mismo y la evaluación de los usuarios. La Resolución en este aspecto cubre la identificación de necesidades de entrenamiento y educación; y, además menciona el registro de participantes en los entrenamientos. No se hace referencia a los detalles del proceso de entrenamiento y se deja fuera de alcance el proceso de evaluación.

DS7 Educar y Entrenar a los Usuarios		IA	CC
DS7.1	Identificación de Necesidades de Entrenamiento y Educación	1.00	C
DS7.2	Impartición de Entrenamiento y Educación	0.25	P
DS7.3	Evaluación del Entrenamiento Recibido	0.00	N
Número de Objetivos de Control Cubiertos		1.25	1C
Número de Objetivos de Control Requeridos		3	1P
Alineamiento R-JB-2005-834 respecto a COBIT 4.1		**0.42**	1N

Tabla 24. DS7 Educar y Entrenar a los Usuarios

2.4.3.8 DS8 Administrar la Mesa de Servicio y los Incidentes

La Resolución no contempla en sus exigencias el concepto de Mesa de Servicios. El único concepto mencionado en este objetivo de control está referido a incidentes, para el cual, se exige políticas y procedimientos pero no se ofrecen detalles como escalamiento y cierre de incidentes.

DS8 Administrar la Mesa de Servicio y los Incidentes		IA	CC
DS8.1	Mesa de Servicios	0.00	N
DS8.2	Registro de Consultas de Clientes	0.00	N
DS8.3	Escalamiento de Incidentes	0.50	P
DS8.4	Cierre de Incidentes	0.00	N
DS8.5	Análisis de Tendencias	0.00	N
Número de Objetivos de Control Cubiertos		0.50	0C
Número de Objetivos de Control Requeridos		5	1P
Alineamiento R-JB-2005-834 respecto a COBIT 4.1		**0.10**	4N

Tabla 25. DS8 Administrar la Mesa de Servicio y los Incidentes

2.4.3.9 DS9 Administrar la Configuración

La Resolución no contempla el concepto de Gestión de la Configuración, únicamente y de manera aislada se menciona iniciativas de control sobre versiones de las aplicaciones en el numeral 4.3.6.3 "*Controles que permitan asegurar la adecuada administración de versiones de las aplicaciones puestas en producción*."

DS9 Administrar la Configuración		IA	CC
DS9.1	Repositorio y Línea Base de Configuración	0.75	P
DS9.2	Identificación y Mantenimiento de Elementos de Configuración	0.00	N
DS9.3	Revisión de Integridad de la Configuración	0.00	N
Número de Objetivos de Control Cubiertos		0.75	0C
Número de Objetivos de Control Requeridos		3	1P
Alineamiento R-JB-2005-834 respecto a COBIT 4.1		**0.25**	2N

Tabla 26. DS9 Administrar la Configuración

2.4.3.10 DS10 Administración de Problemas

El concepto de *problema* no existe en la Resolución; sin embargo, si hace referencia al término *fallas*, para el cual no se da una definición explícita en la sección de definiciones definidas en su artículo 2. Según la Real Academia Española existe una distinción entre *falla* y *problema*. Se define *falla* como un defecto material de una cosa que merma su resistencia, una falta, deficiencia, error ó un incumplimiento de una obligación; mientras que, se define *problema* como un conjunto de hechos o circunstancias que dificultan la consecución de algún fin. Por otro lado, según COBIT, *problema* es la causa subyacente desconocida de uno o más incidentes. Estos conceptos indican que estamos ante dos eventos que tienen cierta relación pero son diferentes conceptualmente.

Partiendo de esta diferencia y con la consideración de que una falla puede ser parte de un problema, la estimación es del 12.5 % ya que la Resolución si considera la identificación de fallas, lo que cumple parcialmente el control DS10.1. Los restantes objetivos de control no son considerados.

DS10 Administración de Problemas		IA	CC
DS10.1	Identificación y Clasificación de Problemas	0.50	P
DS10.2	Rastreo y Resolución de Problemas	0.00	N
DS10.3	Cierre de Problemas	0.00	N
DS10.4	Integración de las Administración de Cambios, Config. y Problemas	0.00	N
Número de Objetivos de Control Cubiertos		0.50	0C
Número de Objetivos de Control Requeridos		4	1P
Alineamiento R-JB-2005-834 respecto a COBIT 4.1		**0.13**	3N

Tabla 27. DS10 Administración de Problemas

2.4.3.11 DS11 Administración de Datos

Con el propósito de garantizar la calidad, oportunidad y disponibilidad de la información, este objetivo de control establece la administración de datos, lo que incluye la identificación de requerimientos de los datos, el establecimiento de procedimientos para administrar la librería de medios, el respaldo, la recuperación de datos y la eliminación apropiada de medios. La Resolución JB-2005-834 exige en el numeral 4.3.4.8 que existan "*Controles formales para proteger la información contenida en documentos; medios de almacenamiento u otros dispositivos*" así como también da reglas para el respaldo y restauración de información en su

numeral 4.3.5.2. No obstante, se deja sin mención y con poca atención respectivamente, los acuerdos de almacenamiento y los procedimientos de eliminación segura.

DS11 Administración de Datos		IA	CC
DS11.1	Requerimientos del Negocio para Administración de Datos	0.00	N
DS11.2	Acuerdos de Almacenamiento y Conservación	0.00	N
DS11.3	Sistema de Administración de Librerías de Medios	1.00	C
DS11.4	Eliminación	0.25	P
DS11.5	Respaldo y Restauración	1.00	C
DS11.6	Requerimientos de Seguridad para la Administración de Datos	0.75	P
Número de Objetivos de Control Cubiertos		3.00	2C
Número de Objetivos de Control Requeridos		6	2P
Alineamiento R-JB-2005-834 respecto a COBIT 4.1		**0.50**	2N

Tabla 28 DS11 Administración de Datos

La ausencia de estos objetivos de control permitiría la inconsistencia de datos, destrucción o pérdida de información inapropiadamente almacenada, y divulgación de información.

2.4.3.12 DS12 Administración del Ambiente Físico

La Resolución JB-2005-834 cubre la seguridad física en las instalaciones de procesamiento de información, el acceso físico en áreas protegidas. Esto con el fin de prevenir acceso de personal no autorizado y daños a los equipos de computación y a la información en ellos procesada, almacenada o distribuida. Se omite protección ambiental, seguridad física en áreas de envío y recepción, y además no se toma cuidado de la administración de instalaciones de equipos de comunicaciones y fluido eléctrico. Para este último elemento solamente se menciona la identificación de riesgos en la interrupción.

DS12 Administración del Ambiente Físico		IA	CC
DS12.1	Selección y Diseño del Centro de Datos	1.00	C
DS12.2	Medidas de Seguridad Física	0.00	N
DS12.3	Acceso Físico	1.00	C
DS12.4	Protección Contra Factores Ambientales	0.50	P
DS12.5	Administración de Instalaciones Físicas	0.25	P
Número de Objetivos de Control Cubiertos		2.75	2C
Número de Objetivos de Control Requeridos		5	2P
Alineamiento R-JB-2005-834 respecto a COBIT 4.1		**0.55**	1N

Tabla 29. DS12 Administración del Ambiente Físico

2.4.3.13 DS13 Administración de Operaciones

La Resolución JB-2005-834 contempla la existencia de procedimientos de operación, y el monitoreo de la Infraestructura de TI. Respecto a COBIT, se omite mencionar la organización de trabajos, tareas operativas y la eficiencia con la que se realizan; así como tampoco se citan actividades de mantenimiento de hardware. Sin un control de este tipo, existe la probabilidad de indisponibilidad de sistemas de hardware por falta de mantenimiento y respecto al rendimiento se podrían presentar tareas que no son eficientes.

DS13 Administración de Operaciones		IA	CC
DS13.1	Procedimientos e Instrucciones de Operación	1.00	C
DS13.2	Programación de Tareas	0.00	N
DS13.3	Monitoreo de la Infraestructura de TI	0.75	P
DS13.4	Documentos Sensitivos y Dispositivos de Salida	0.25	P
DS13.5	Mantenimiento Preventivo del Hardware	0.00	N
Número de Objetivos de Control Cubiertos		2.00	1C
Número de Objetivos de Control Requeridos		5	2P
Alineamiento R-JB-2005-834 respecto a COBIT 4.1		**0.40**	2N

Tabla 30. DS13 Administración de Operaciones

2.4.4 DOMINIO MONITOREAR Y EVALUAR EL DESEMPEÑO DE TI (ME)

Este dominio considera cuatro procesos de alto nivel orientados a la evaluación de la calidad y cumplimiento de requerimientos de control. Seguidamente se analiza el índice de alineamiento de la Resolución JB-2005-834 en cada uno de estos procesos.

2.4.4.1 ME1 Monitorear y Evaluar el Desempeño de TI

Este objetivo de control considera el monitoreo de la administración del desempeño de TI respecto a su apoyo al negocio y a las políticas. Este proceso incluye la definición de indicadores de desempeño, reportes de desempeño y detección de desviaciones. Es muy limitado lo que la Resolución JB-2005-834 considera al respecto, por lo que existiría la probabilidad de que las inversiones de TI no entreguen los resultados esperados, así como se podrían presentar falta de alineamiento, falta de control, dirección y eficacia de TI.

ME1 Monitorear y Evaluar el Desempeño de TI		IA	CC
ME1.1	Enfoque del Monitoreo	0.00	N
ME1.2	Definición y Recolección de Datos de Monitoreo	0.00	N
ME1.3	Método de Monitoreo	0.00	N
ME1.4	Evaluación del Desempeño	0.25	P
ME1.5	Reportes al Consejo Directivo y a Ejecutivos	0.25	P
ME1.6	Acciones Correctivas	0.00	N
Número de Objetivos de Control Cubiertos		0.50	0C
Número de Objetivos de Control Requeridos		6	2P
Alineamiento R-JB-2005-834 respecto a COBIT 4.1		**0.08**	4N

Tabla 31. ME1 Monitorear y Evaluar el Desempeño de TI

2.4.4.2 ME2 Monitorear y Evaluar el Control Interno

Existe exigencias de control interno Resolución JB-2005-834, aunque no se plantean temas complementarios relevantes como autoevaluación de controles o evaluación de los mismos por parte de terceros. Debido a esto, se podrían presentar controles débiles que no cumplen su función.

ME2 Monitorear y Evaluar el Control Interno		IA	CC
ME2.1	Monitoreo del Marco de Trabajo de Control Interno	1.00	C
ME2.2	Revisiones de Auditoría	1.00	C
ME2.3	Excepciones de Control	0.00	N
ME2.4	Control de Auto Evaluación	0.00	N
ME2.5	Aseguramiento del Control Interno	0.00	N
ME2.6	Control Interno para Terceros	0.50	P
ME2.7	Acciones Correctivas	1.00	C
Número de Objetivos de Control Cubiertos		3.50	3C
Número de Objetivos de Control Requeridos		7	1P
Alineamiento R-JB-2005-834 respecto a COBIT 4.1		**0.50**	3N

Tabla 32. ME2 Monitorear y Evaluar el Control Interno

2.4.4.3 ME3 Garantizar el Cumplimiento con Requerimientos Externos

A pesar que Resolución JB-2005-834 tiene un alto grado de enfoque en el cumplimiento, hay algunas omisiones respecto a procesos de reporte y optimización de su direccionamiento y comunicación. Esto deja la posibilidad a la existencia de políticas que no sean efectivas.

ME3 Garantizar el Cumplimiento con Requerimientos Externos		IA	CC
ME3.1	Identificar los Requerimientos de las Leyes, Regulaciones y Cumplimientos Contractuales	1.00	C
ME3.2	Optimizar la Respuesta a Requerimientos Externos	0.75	P
ME3.3	Evaluación del Cumplimiento con Requerimientos Externos	0.75	P
ME3.4	Aseguramiento Positivo del Cumplimiento	0.25	P
ME3.5	Reportes Integrados	1.00	C
Número de Objetivos de Control Cubiertos		3.75	2C
Número de Objetivos de Control Requeridos		5	3P
Alineamiento R-JB-2005-834 respecto a COBIT 4.1		**0.75**	0N

Tabla 33. ME3 Garantizar el Cumplimiento con Requerimientos Externos

2.4.4.4 ME4 Proporcionar Gobierno de TI

La Resolución JB-2005-834 no considera lo siguientes conceptos de gobierno: una estructura de gobierno de TI, entrega de valor, administración de los recursos y medición del desempeño. Por otro lado, hace menciones aisladas de alineamiento en varias secciones; donde, en general se exige un alineamiento hacia los objetivos organizacionales, define procesos de manera general para la gestión de recursos, pero no se hace énfasis en temas de inversión, asignación y alineamiento como propone COBIT. La Resolución también exige auditorías internas independientes, pero no se menciona a nivel externo.

El área de fortaleza en aspecto de gobierno se encuentra en la *administración de riesgos*, donde se cubre de manera total el aseguramiento de que el negocio y TI regularmente evalúe y reporte riesgos relacionados con TI y su impacto y que se definan las responsabilidades de administración de riesgos en la organización. Se considera parcialmente en definir el nivel de riesgo de TI aceptable, y que la posición de los riesgos de TI de la empresa sea transparente a los interesados. Sin embargo, no se precisa sobre las prácticas de administración de riesgos de TI para asegurar que el riesgo actual de TI no excede el riesgo aceptable.

ME4 Proporcionar Gobierno de TI		**IA**	**CC**
ME4.1	Establecimiento de un Marco de Gobierno de TI	0.00	N
ME4.2	Alineamiento Estratégico	0.25	P
ME4.3	Entrega de Valor	0.00	N
ME4.4	Administración de Recursos	0.00	N
ME4.5	Administración de Riesgos	0.75	P
ME4.6	Medición del Desempeño	0.00	N
ME4.7	Aseguramiento Independiente	0.25	P
Número de Objetivos de Control Cubiertos		1.25	0C
Número de Objetivos de Control Requeridos		7	3P
Alineamiento R-JB-2005-834 respecto a COBIT 4.1		**0.21**	4N

Tabla 34. ME4 Proporcionar Gobierno de TI

La ausencia de los objetivos de control ausentes permitiría que se realicen actividades de TI sin una adecuada administración que guie hacia el cumplimiento de los objetivos y estrategia de la empresa. Además, causaría una asignación de inversión en proyectos y programas que no aseguren el beneficio esperado, y por último, que ciertos individuos no conozcan riesgos de TI asociados a su rol y responsabilidad debido a la falta exigencias de transparencia.

2.5 ANÁLISIS DE RESULTADOS DE ALINEAMIENTO

En concordancia con la metodología explicada, a continuación se presenta el diagrama que esquematiza el índice de alineamiento de la Resolución JB-2005-834 respecto a COBIT 4.1., donde la circunferencia perimetral externa representa el valor máximo de los 34 procesos de COBIT y la figura interior representa el alineamiento que la Resolución ha logrado en cada uno de estos procesos.

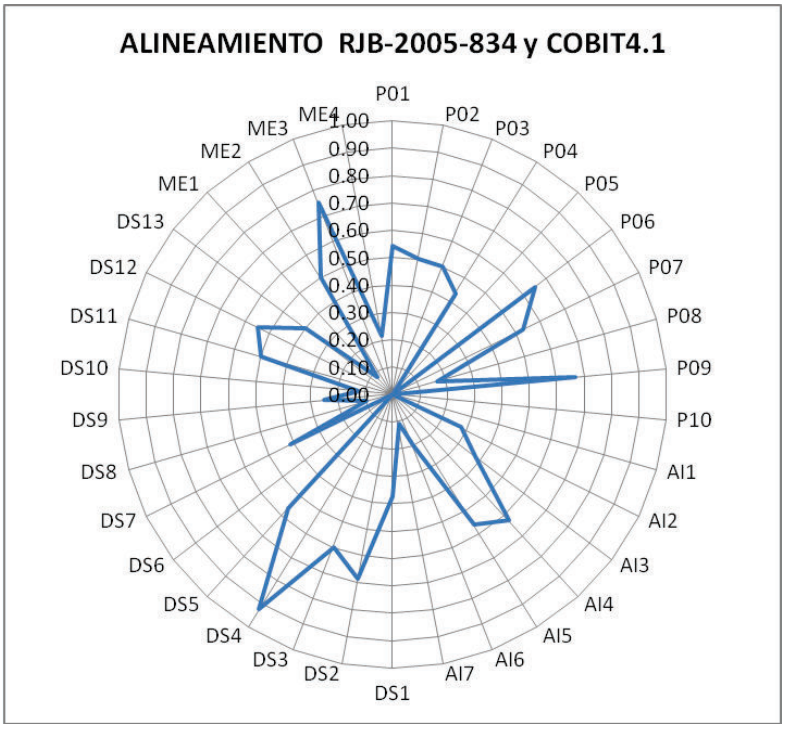

Figura 4. Alineamiento RJB-2005-834 y COBIT4.1

El índice de alineamiento general estimado es 0.38, lo que deja cierto vacío en los cuatro dominios del marco de referencia, así como también presenta áreas aisladas de fortaleza. Seguidamente se exponen las fortalezas y debilidades en cada uno de los dominios.

2.5.1 ALINEAMIENTO EN EL DOMINIO PLANEAR Y ORGANIZAR

El índice de alineamiento en este dominio es 0.4. Los procesos *con un índice de alineamiento mayor son Evaluar y Administrar los Riesgos de TI – (P09)*, *Comunicar las Aspiraciones y Dirección Gerencia (P06)* y *Definir un Plan Estratégico (P01)*. Este hecho identifica el perfil de alineamiento que tiene la

Resolución respecto a los procesos de negocios, así como también su enfoque en planificación; los cuales a pesar de ser puntos relativamente sobresalientes requieren un nivel de mejoramiento.

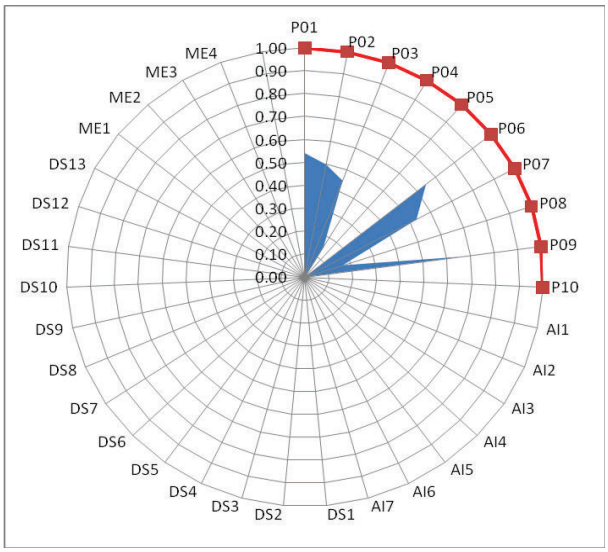

Figura 5. Alineamiento en el Dominio Planear y Organizar

Las áreas de extrema debilidad se encuentran en los procesos que exigen *Administrar la Inversión en TI - P05, Administrar Proyectos - P10,* y *Administrar la Calidad - P08.* Esto evidencia que el manejo de los recursos de inversión, la gestión de proyectos y la preocupación por la calidad no son una prioridad para la Resolución JB-2005-834.

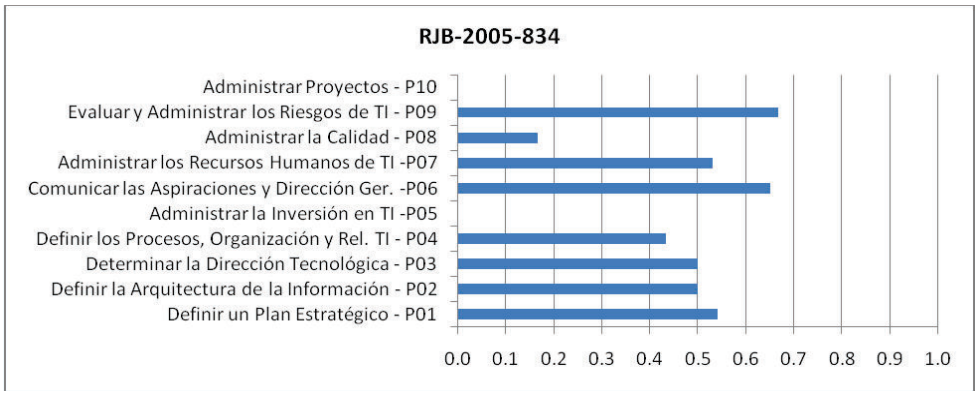

Figura 6. Alineamiento en los Procesos de Planear y Organizar

En general, el riesgo inherente como producto de la falta de alineamiento en este dominio reside en la ausencia de manejo estratégico y además el modo como se

administran los riesgos en las tecnologías de la información. El primero cubre la manera en que TI puede contribuir a la consecución de los objetivos del negocio. El segundo y más importante para nuestro análisis deja exposiciones a nivel de establecimiento del contexto del riesgo, mantenimiento y monitoreo de un plan de acción de riesgos y evaluación de riesgos de TI.

2.5.2 ALINEAMIENTO EN EL DOMINIO ADQUIRIR E IMPLEMENTAR

El índice de alineamiento en este dominio es 0.31. Las áreas de fortaleza relativa de este dominio se ubican en los proceso *Facilitar la Operación y el Uso (AI4)* y *Adquirir Recursos de TI (AI5).* La Resolución soporta la presencia de una infraestructura tecnológica documentada así como el entrenamiento técnico y de los usuarios. Además, la Resolución se muestra bastante fuerte en los objetivos de control relacionados con la administración de contratos con proveedores y a la selección de los mismos aunque se omiten la mención de una estrategia de adquisición.

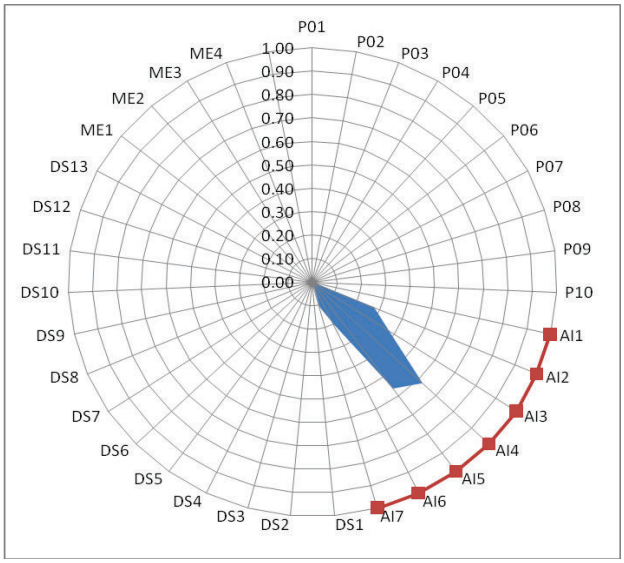

Figura 7. Alineamiento en el Dominio Adquirir e Implementar

El área de extrema debilidad se encuentra en el proceso de *Identificar Soluciones Automatizadas* (AI1), donde es necesario especificar definiciones de mantenimiento, análisis de riesgos, y estudios de factibilidad principalmente. Las áreas de debilidad representativa están en los procesos encargados de regular la

administración de cambios (AI6) y la adquisición y mantenimiento de software aplicativo (AI2) e infraestructura (AI3). Es necesario implantar mejoras en cambios emergentes, seguimiento de reportes de estos cambios y procedimientos de cierre. El proceso de mantenimiento de software requiere exigencias particulares en el diseño, configuración aseguramiento de la calidad y especificación de requerimientos. La adquisición de infraestructura requiere exigencias de planificación y mantenimiento.

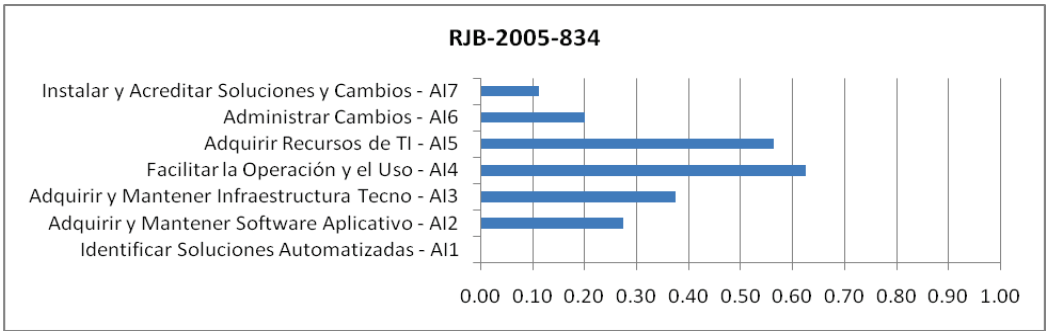

Figura 8. Alineamiento en los Procesos de Adquirir e Implementar

El riesgo inherente en este dominio reside en la falta de completitud de los procesos de control de cambios y mantenimiento de recursos de TI, lo que puede llegar a ser una causa raíz en la introducción de errores o incidentes en las Tecnologías de la Información.

2.5.3 ALINEAMIENTO EN EL DOMINIO ENTREGAR Y SOPORTAR

El índice de alineamiento en este dominio es 0.42, este es el valor más alto de los cuatro dominios de COBIT. El área de máximo cumplimiento se registra en proceso *Garantizar la Continuidad del Servicio (DS4),* de hecho este proceso tiene el mayor índice cumplimiento de los 34 procesos del marco. La Resolución cubre casi todos los objetivos de control planteados para continuidad, su contenido está fundamentado básicamente en los controles planteados por ISO 27002:2005 en el dominio relativo a la Gestión de Continuidad Comercial.

Las áreas de fortaleza mediana relativa se encuentran en los procesos *Administración de Servicios de Terceros (DS2), Administrar el Desempeño y la Capacidad (DS3), Garantizar la Seguridad de los Sistemas (DS5),* y

Administración del Ambiente Físico (DS12). No obstante, es necesario mejorar respectivamente en la identificación de las relaciones con los proveedores, planeación y desempeño de la capacidad de los recursos de IT, controles preventivos contra código malicioso, prácticas de encriptación y seguridad en redes.

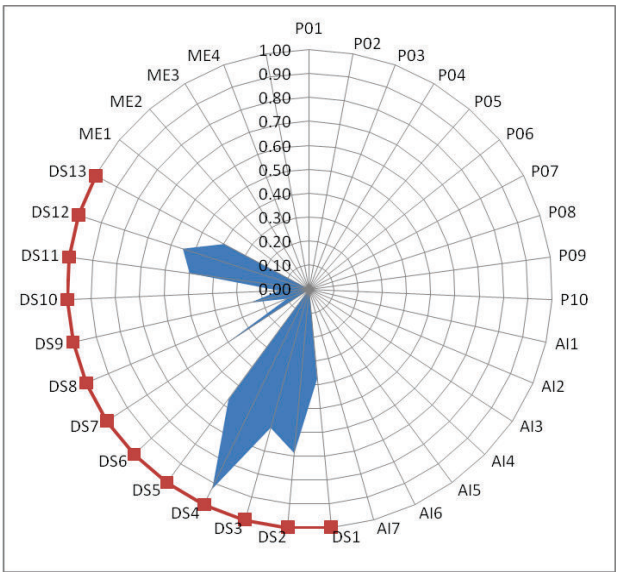

Figura 9. Alineamiento en el Dominio Entregar y Soportar

El área de extrema debilidad se encuentra en los procesos *Identificar y Asignar Costos (DS6), Administrar la Mesa de Servicio* y *los Incidentes (DS8)* y *Administración de Problemas (DS10).* No existen exigencias para la contabilización de TI ni modelación de costos. Se omiten los procesos de soporte a través de mesa de servicios, registro de consultas de clientes, cierre de Incidentes y análisis de tendencias. Otro elemento débil importante está es la *Administrar la Configuración (DS9)*, la Resolución menciona iniciativas de control sobre versiones de las aplicaciones pero no se precisan detalles propios de la gestión de la configuración.

El riesgo inherente en este dominio reside principalmente en la calidad y oportunidad con la que se entregan los servicios de soporte requeridos, la falta de alineamiento sobre la gestión de costos y la integridad de los elementos configurables de las Tecnologías de la Información.

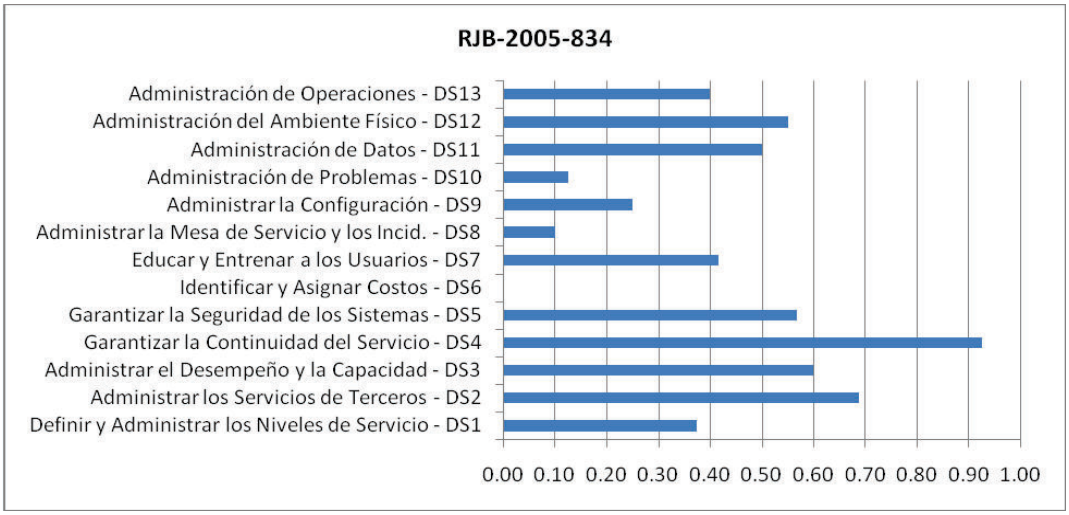

Figura 10. Alineamiento en los Procesos de Entregar y Soportar

2.5.4 ALINEAMIENTO EN EL DOMINIO MONITOREAR Y EVALUAR

El índice de alineamiento en este dominio es 0.39. Las áreas de fortaleza relativa de este dominio se ubican en los procesos *Monitorear y Evaluar el Control Interno (ME2)* y *Garantizar el Cumplimiento con Requerimientos Externos (ME3)*. Sin embargo, el control interno puede mejorarse en aspectos de autoevaluación y manejo de excepciones. El cumplimiento puede mejorar en aspectos de la optimización de respuesta y evaluaciones periódicas de cumplimiento con requerimientos externos.

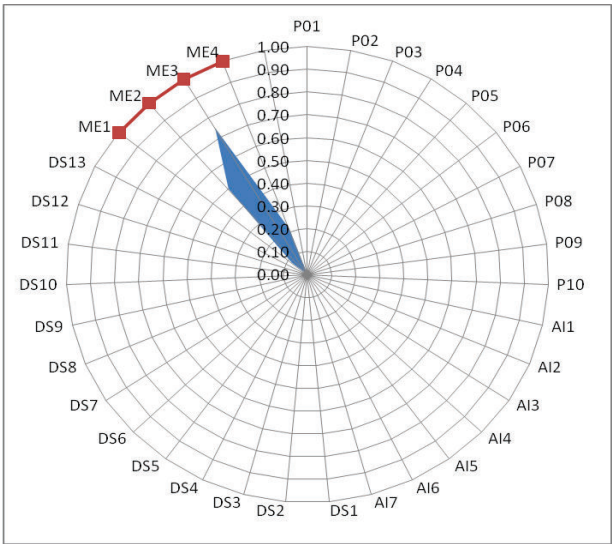

Figura 11. Alineamiento en el Dominio Monitorear y Evaluar

Las áreas de extrema debilidad se encuentran en los procesos *Monitorear y Evaluar el Desempeño de TI (ME1)* y *Proporcionar Gobierno de TI (ME4)*. La resolución no tiene un enfoque en monitoreo y evaluación del desempeño y las consideraciones que estos conllevan, como por ejemplo el reporte a niveles ejecutivos. En esta misma línea, la Resolución no considera estructuras de gobierno de TI que garanticen la entrega de valor de TI.

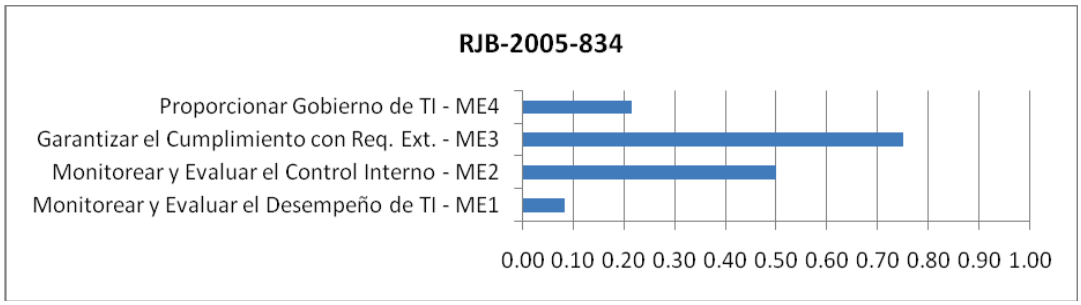

Figura 12. Alineamiento en los Procesos de Monitorear y Evaluar

El riesgo inherente en este dominio reside principalmente en la ejecución de actividades de TI sin una adecuada administración que guie hacia el cumplimiento de los objetivos y estrategia de la empresa. Además, una asignación de inversión en proyectos y programas que no aseguren el beneficio esperado.

2.5.5 ALINEAMIENTO RESPECTO A LOS CRITERIOS DE INFORMACIÓN DE COBIT 4.1

El alineamiento que tiene la Resolución JB-2005-834 respecto a COBIT en términos de los criterios de la información, se lo ha calculado en función del índice de cumplimiento identificado en cada uno de los 34 procesos de alto nivel de COBIT.

La línea que corresponde en el gráfico a COBIT 4.1 representa la relevancia que COBIT asigna a los criterios de información según se explico en la sección 2.2 de este capítulo. La línea de la figura que corresponde a Resolución JB-2005-834 representa la afectación que cada uno de los criterios de información ha sufrido al

ser multiplicado por el índice de alineamiento en cada proceso de alto nivel de COBIT. Los detalles del cálculo se encuentran en el Anexo D.

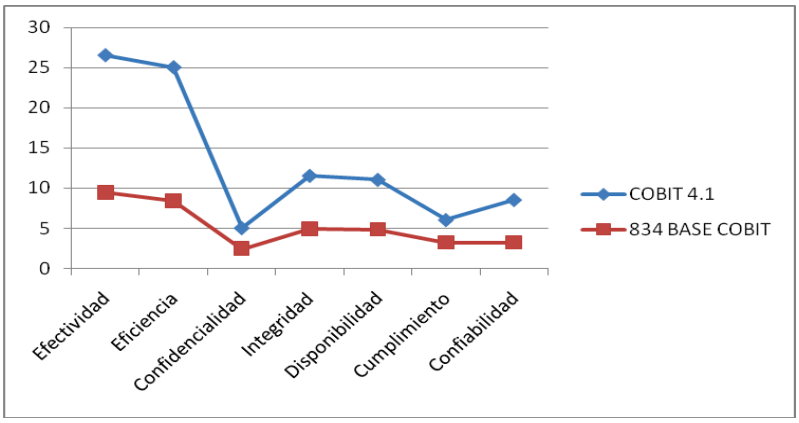

Figura 13. Alineamiento de JB-2005:834 respecto a COBIT4.1

Según se observa los criterios de información con un rango de menor cumplimiento en la Resolución JB-2005-834 son la *efectividad y la eficiencia*. Esto indica claramente que la Resolución no tiene un enfoque en temas de gobierno de TI, lo cual si bien soporta los procesos de IT no guarda una relación tan estricta con el riesgo de TI como lo hacen los criterios de confidencialidad, integridad, disponibilidad y en cierto grado el cumplimiento y la confiabilidad.

En conclusión, el análisis realizado muestra que la Resolución JB-2005-834 no representa un marco regulatorio para normar gobierno de las tecnologías de la información. La Resolución ha cubierto ciertas áreas del Riesgo en TI pero presenta debilidades notables en cuanto a su gestión. Como resultado, las propiedades de la información relativas a la administración de riesgos respecto a COBIT se encuentran comprometidas en este orden, *la integridad, la disponibilidad, la confiabilidad* y la confidencialidad.

En el siguiente capítulo se realizará el análisis con un estándar que tiene una estructura diferente pero con un enfoque muy alineado con la gestión de riesgos de las Tecnologías de la Información.

CAPITULO 3

ANÁLISIS COMPARATIVO RESPECTO A ISO 27002:2005

Este capítulo realizará el análisis de la Resolución JB-2005-834 respecto al estándar internacional conocido como Código para la Práctica de la Gestión de Seguridad de la Información ISO-IEC 27002:2005, publicado en Julio de 2005 como ISO 17799:2005 y renombrado en el año 2007 para formar parte de la serie ISO 27000. El estándar ISO 27002:2005 establece un enfoque orientado hacia la protección de la información como activo de una organización. Para el efecto, identifica las múltiples formas en que la información se presenta, el procesamiento al que esta se encuentra sujeta, las amenazas a las que se expone, entre otras. A este concepto de búsqueda de protección para la información, este estándar plantea el concepto de "Seguridad de la Información", que dice:"*Seguridad de la Información es la protección de la información de un rango amplio de amenazas para poder asegurar la continuidad del negocio, minimizar el riesgo comercial y maximizar el retorno de las inversiones y las oportunidades comerciales*."[23] Otra definición empleada para describir el mismo concepto es:"*Preservación de confidencialidad, integración y disponibilidad de la información.*"[24] Dado que el objeto de esta investigación es el riesgo de las Tecnologías de la Información, el estándar de ISO se ajusta debido a su enfoque en los criterios de la información.

El análisis comparativo permitirá detectar la brecha existente entre ISO-IEC 27002:2005 y la Resolución JB-2005-834, la cual será expresada a través de un Indice de Alineamiento (IA) para cada objetivo de control de ISO-IEC 27002:2005. Este índice tiene la misma definición expresada en el capitulo anterior, puede variar entre cero y uno y expresa el grado de coincidencia que la Resolución JB-2005-834 tiene respecto a ISO-IEC 27002:2005. Este índice permitirá identificar áreas susceptibles de mejora, las cuales serán abordadas en la propuesta de mejoramiento.

[23] ISO-IEC 27002:2005
[24] ISO-IEC 27002:2005

Este capítulo se encuentra estructurado en cinco secciones. La primera explica la estructura del marco de ISO-IEC 27002:2005, necesaria para entender el procedimiento de comparación. La segunda sección identifica los criterios de la información de ISO-IEC 27002:2005, requerido para determinar el enfoque de ISO respecto a estos criterios. La tercera explica la metodología de comparación o correspondencia. La cuarta sección realiza el análisis de correspondencia que identifica el incide de alineamiento. Finalmente la última sección realiza el análisis de los resultados de alineamiento donde se resume las áreas de fortaleza y debilidad.

3.1 ESTRUCTURA DE ISO 27002

El estándar ISO-IEC 27002:2005 se encuentra conformado por una estructura de once categorías, las cuales este documento las identificará como dominios. Estos dominios conforman 39 objetivos de control, que a su vez agrupan 133 controles. Cada uno de estos controles, según ISO, ha sido diseñado para satisfacer los requerimientos identificados por una evaluación del riesgo.

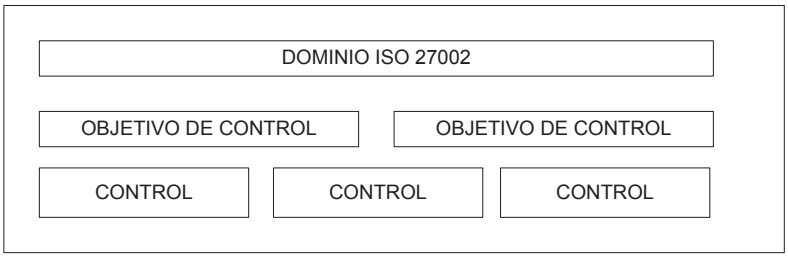

Figura 14. Estructura ISO-IEC 27002:2005

La estructura de la figura se aplica a cada uno de los once dominios y objetivos de control.

3.2 CRITERIOS DE INFORMACION DE ISO 27002:2005

Los criterios de información considerados de manera explícita por ISO para la gestión de la seguridad de la información son la confidencialidad, la integridad, la disponibilidad y el cumplimiento. Sin embargo, en mucha menor proporción considera la efectividad, la eficiencia y la confiabilidad.

ISO-IEC 27002:2005 no indica el grado de importancia que sus objetivos de control asigna a los criterios de información; así que hemos realizado una asignación de importancia primaria y secundaria, similarmente a lo que hace COBIT en su Apéndice II. Esta asignación se ha realizado en función de la definición y orientación a la protección de los activos de información de cada objetivo de control de ISO-IEC 27002:2005. Por tal motivo, esta estimación podría estar sujeta a cierto grado de subjetividad en la precisión, más no en la aproximación. Adicionalmente, hemos expresado la importancia primaria con 1 y la secundaria con 0.5 para completar la analogía realizada en la sección 2.2 del capítulo 2 para COBIT. El resultado se expone en la siguiente figura y el detalle en el Anexo F.

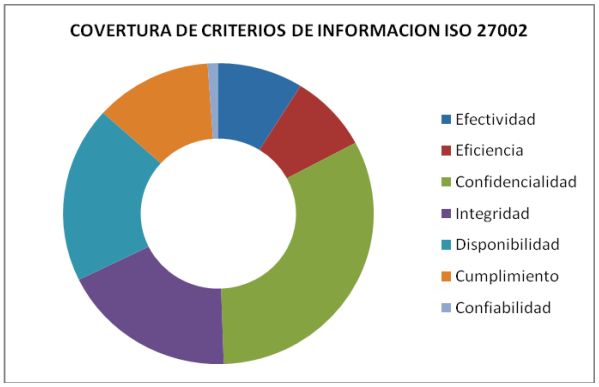

Figura 15. Estructura ISO 27002:2005

Según se observa, ISO 27002:2005 presenta un elevado enfoque en confidencialidad, integridad y disponibilidad como consecuencia de su alineamiento a la Seguridad de la Información.

3.3 METODOLOGIA DEL ANÁLISIS COMPARATIVO

El análisis y cálculo del alineamiento se realizará mediante la identificación de correspondencia entre los requerimientos planteados por los objetivos de control de ISO 27002 y los enunciados de la Resolución JB-2005-834. A cada uno de los objetivos de control se asignará un grado de cumplimiento. El cálculo se fundamentará en un análisis del contenido de la Resolución JB-2005-834 respecto

a ISO 27002, para luego ser representado en una estimación cuantitativa y cualitativa.

3.3.1 DESRIPCION DEL PROCEDIMIENTO

La determinación del nivel de coincidencia ó grado de cumplimiento para cada uno de los controles del estándar ISO 27002 se realiza mediante los siguientes pasos:

- Elección de un objetivo de control del estándar ISO 27002.
- Identificación y documentación de requerimientos (aspectos) clave del control del estándar ISO 27002. Estos requerimientos se refieren a los aspectos importantes del control.
- Búsqueda de estos requerimientos clave en cada una de las secciones de la Resolución JB-2005-834. Esta búsqueda se realiza mediante dos métodos. El primero mediante lectura, análisis e interpretación de la Resolución JB-2005-834; y, el segundo mediante búsqueda electrónica múltiple con la asistencia de un programa lector de formato PDF.
- Documentación de requerimientos clave del control así como los identificadores de artículo y sub-artículo con fines de referencia.
- Asignación cuantitativa al grado de cumplimiento de los de requerimientos clave del control en base a los criterios de valoración, más adelante explicados.
- Asignación cualitativa al grado de cumplimiento de cumplimiento de los de requerimientos clave del control en base a los criterios más adelante explicados.

3.3.2 ASIGNACION CUANTITATIVA

El valor del índice de alineamiento que un objetivo de control ISO 27002 alcanza en la Resolución JB-2005-834 se obtiene a partir del cumplimiento que cada uno de los requerimientos clave del control logra. Este valor se obtiene a partir de los siguientes criterios

- Existirán cuatro posibles niveles expresados en términos numéricos por: (0), (0.5), (0.75), y (1).

- Asignación (0): cuando los requerimientos del control del estándar de referencia ISO 27002 no se cumplen en la Resolución JB-2005-834.
- Asignación (0.5); cuando aproximadamente la mitad de los requerimientos de ISO 27002 se cumplen, ó cuando en la Resolución JB-2005-834 existe un enunciado general relativo al control, pero no se especifican detalles.
- Asignación (0.75); cuando se cumple el requerimiento más relevante y adicionalmente otros complementarios pero se omite uno o dos complementarios.
- Asignación (1); cuando los requerimientos del control del estándar de referencia ISO 27002 se cumplen de manera aproximada al 100%, ó exacta, ó se superan.
- Los resultados de este procedimiento se expresan en una tabla.

Como resultado se tendrá el índice de alineamiento de un *Control.* Para obtener el valor del índice de alineamiento de un *Objetivo de Control*, se calculará la media aritmética entre los valores de cada uno de los controles contemplados en este objetivo de control.

3.3.3 ASIGNACION CUALITATIVA

Eta asignación cualitativa se refiere a una calificación no numérica que describe el grado de cumplimiento de cada control expresado en una descripción del estado; así:

- Asignación (N): (No considerado) cuando la asignación cuantitativa es cero (0).
- Asignación (P): (Parcialmente considerado) cuando la asignación cuantitativa es cero (0) ó (0.75).
- Asignación (C): (Completo) cuando la asignación cuantitativa es (1).

Como resultado, se obtendrá el parámetro CC (Calificación Cualitativa), el cual expresará el cumplimiento en términos cualitativos.

3.3.4 EJEMPLO DE CÁLCULO

Para esquematizar lo expuesto en los numerales anteriores, a continuación se realiza el análisis del objetivo de control de ISO 27002 denominado “Política de seguridad de la información.”

DOMINIO 5: POLITICA DE SEGURIDAD OBJETIVO DE CONTROL 5.1: Política de Seguridad de la Información				
ISO 27002:2005		RESOLUCIÓN NO. JB-2005-834	CUMPLIMIENTO	
Control	**Control (requerimientos claves)**	**Aspectos Claves**	**IA**	**CC**
5.1.1 Documento de la política de seguridad de la información	**Aprobado por la gerencia**, y **publicado** y **comunicado** a todos los empleados y las partes externas relevantes	4.3.1.5 Políticas, procesos y procedimientos de TI....que garanticen.. control interno de eficacia, eficiencia y cumplimiento, debidamente **aprobados por el directorio** 4.3.4.1 Políticas y procedimientos de **seguridad de la información** que establezcan .. requisitos de cumplimiento, responsabilidades.. 4.3.1.6 **Difusión y comunicación** a todo el personal involucrado de las mencionadas políticas, procesos y procedimientos..	1.00	C
5.1.2 Revisión de la política de seguridad de la información	La política **revisada a intervalos** planeados o si ocurren cambios significativos para asegurar su continua idoneidad, eficiencia y efectividad.	No considerado	0.00	N

Tabla 35. Ejemplo de Cálculo del Índice de Alineamiento

En este caso, el *objetivo de control* tiene dos *controles*. En el primer *control* ISO pide la existencia de una política, su aprobación de alto nivel, su publicación y comunicación. Estos representan los *requerimientos del control*, los mismos que tienen una correspondencia exacta en la Resolución JB-2005-834 expresada en la tercera columna, por lo que la asignación cuantitativa es (1) y la cualitativa es (C). Adicionalmente, estos requerimientos están contenidos en diferentes secciones de la Resolución por lo que están identificadas con el numerador original de su documento para su ubicación. El segundo control no se encuentra considerado en el contenido de la Resolución JB-2005-834, por lo que la asignación cuantitativa es (0) y la cualitativa es (N).

De esta manera, aplicando la media aritmética se tiene que el índice de alineamiento del objetivo de control es 0.5.

3.4 CORRESPONDENCIA ENTRE LA RESOLUCION JB-2005-834 E ISO 27002

Esta sección realiza el análisis de cada uno de los controles, objetivos de control y por tanto los dominios de ISO 27002, para identificar la posible correspondencia con la Resolución JB-2005-834.

3.4.1 POLÍTICA DE SEGURIDAD

Este dominio considera un objetivo de control y dos controles orientados al alineamiento de la administración de IT con los objetivos de negocio. ISO exige la existencia de una política documentada, aprobada y publicada lo cual es cubierto por la Resolución JB-2005-834. Sin embargo, se descuida el control referido a la actualización de la misma y por tanto a su efectividad.

OBJETIVO DE CONTROL 5.1: Política de Seguridad de la Información		**IA**	**CC**
5.1.1	5.1.1 Documento de la política de seguridad de la información	1.00	C
5.1.2	5.1.2 Revisión de la política de seguridad de la información	0.00	N
Número de Objetivos de Control Considerados		1.00	**1C**
Número de Objetivos de Control Requeridos		2	**0P**
Cumplimiento R-JB-2005-834 respecto a ISO 27002		**0.50**	**1N**

Tabla 36. Política de Seguridad de la Información

Según el método explicado anteriormente, el índice de alineamiento es 0.5, mientras que la calificación cualitativa (CC) está expresada en términos de completitud. La información de la tabla indica que la Resolución considera el control 5.1.1 de manera completa, no existen controles considerados parcialmente y el control 5.1.2 no está considerado. La calificación cualitativa (CC) se resume en las tres últimas celdas de la columna CC de esta manera:

- 1C: un control completamente considerado
- 0P: cero controles parcialmente considerados
- 1N: un control no considerado.

Todas las tablas subsiguientes en cada objetivo de control deben ser interpretadas de la misma manera.

3.4.2 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

La organización de la seguridad busca el apoyo de los niveles directivos a la seguridad de la información para su implementación y cumplimiento efectivo. Además para que se guarde un alineamiento de la seguridad de la información con los objetivos de negocio. Con este propósito el estándar plantea dos objetivos de control, uno a nivel interno y otro para entidades externas a la organización, lo cual se cubre con 11 controles.

3.4.2.1 Organización Interna

A nivel interno, es muy poco lo que la Resolución JB-2005-834 contempla. De hecho, tan solo un control de los ocho exigidos es considerado completamente, el cual se refiera al compromiso de la gerencia para la seguridad de la información, que representa un buen punto de partida pero es insuficiente. Adicionalmente, dos controles se consideran medianamente, estos son la coordinación y la asignación de responsabilidades en materia de seguridad de la información. Se omiten aspectos como acuerdos de confidencialidad, contactos con autoridades, grupos de interés y revisión independiente de la seguridad. El índice de alineamiento es 0.34.

A.6.1	**Organización Interna**	**IA**	**CC**
A.6.1.1	Compromiso de la gerencia para la seguridad de la información	1.00	C
A.6.1.2	Coordinación de la seguridad de la información	0.50	P
A.6.1.3	Asignación de responsabilidades en materia de SI	0.50	P
A.6.1.4	Proceso de autorización para instalaciones de procesamiento de I.	0.00	N
A.6.1.5	Acuerdos de confidencialidad	0.50	P
A.6.1.6	Contrato con autoridades	0.00	N
A.6.1.7	Contacto con grupos de interes especial	0.25	P
A.6.1.8	Revisión independiente de la seguridad de la información	0.00	N
Número de Objetivos de Control Considerados		2.75	1C
Número de Objetivos de Control Requeridos		8	4P
Cumplimiento R-JB-2005-834 respecto a ISO 27002		**0.34**	3N

Tabla 37. Organización Interna

3.4.2.2 Entidades Externas

A nivel externo la Resolución ha tomado más previsiones. Se identifican riesgos relacionados a partes externas, como recursos y servicios provistos por terceros y contratos asociados; especialmente a la información crítica y a las instalaciones de

procesamiento de datos. Se puede mejorar respecto a la identificación temprana de necesidades de seguridad en los contratos.

D.6.2	Entidades Externas	IA	CC
D.6.2.1	Identificación de riesgos relacionados a partes externas	1.00	C
D.6.2.2	Direccionar la seguridad cuando se trata de clientes	0.50	P
D.6.2.3	Direccionar la seguridad en acuerdos de terceras partes	1.00	C
Número de Objetivos de Control Considerados		2.50	2C
Número de Objetivos de Control Requeridos		3	1P
Cumplimiento R-JB-2005-834 respecto a ISO 27002		**0.83**	0N

Tabla 38. Entidades Externas

El tener una visibilidad externa independiente de la seguridad es saludable para la corrección de controles que no funcionan apropiadamente, para la optimización de los mismos y para la implementación de controles omitidos. Se podría presentar una exposición de los activos debido a la falsa percepción interna de seguridad. Además a nivel externo se podrían omitir necesidades de seguridad que deberían constar en contratos con terceros.

3.4.3 GESTIÓN DE ACTIVOS

Se plantean dos objetivos de control, uno orientado a la responsabilidad de los activos y otro sobre la clasificación de la información.

3.4.3.1 Responsabilidad por los Activos

La Resolución JB-2005-834 exige un *procedimiento de clasificación y control de activos de tecnología de información*, donde se definen requerimientos que "*considere por lo menos el registro e identificación, así como los responsables de su uso y mantenimiento*" de activos.

D.7.1	Responsabilidad por los Activos	IA	CC
D.7.1.1	Inventario de Activos	1.00	C
D.7.1.2	Propiedad de los Activos	0.75	P
D.7.1.3	Uso Aceptable de los Activos	0.00	N
Número de Objetivos de Control Considerados		1.75	1C
Número de Objetivos de Control Requeridos		3	1P
Cumplimiento R-JB-2005-834 respecto a ISO 27002		**0.58**	1N

Tabla 39. Responsabilidad por los Activos

3.4.3.2 Clasificación de la Información

La Resolución deja sin mención directa a la propiedad de los activos, se omite el uso aceptable de los mismos, el etiquetado y el manejo de la información. Los requerimientos mínimos exigidos son limitados, dado que no se exige propietario de la información de manera directa. El rol "responsable de uso" no conocerá las obligaciones explícitas que tiene sobre la protección de la información. La efectividad de esta implementación dependerá de la iniciativa y habilidad de las instituciones financieras reguladas.

D.7.2	Clasificación de la información	IA	CC
D.7.2.1	Lineamientos de clasificación	1.00	C
D.7.2.2	Etiquetado y manejo de la información	0.00	N
Número de Objetivos de Control Considerados		1.00	1C
Número de Objetivos de Control Requeridos		2	0P
Cumplimiento R-JB-2005-834 respecto a ISO 27002		**0.50**	1N

Tabla 40. Clasificación de la información

Adicionalmente, la omisión del etiquetado de la información presenta oportunidades para que los usuarios expongan información confidencial de manera involuntaria por no conocer su clasificación.

3.4.4 SEGURIDAD DE LOS RECURSOS HUMANOS

ISO plantea objetivos de control para regular las tres instancias de la gestión de personal: el proceso de ingreso, la permanencia y la salida.

3.4.4.1 Antes del Empleo

La Resolución se preocupa de regular respecto a los roles y responsabilidades, el proceso de reclutamiento, pero no menciona chequeos de verificación de antecedentes de candidatos para empleo, contratistas y terceros.

A.8.1	Antes del Empleo	IA	CC
A.8.1.1	Roles y Responsabilidades	1.00	C
A.8.1.2	Investigacion de Antecedentes	0.25	P
A.8.1.3	Términos y Condiciones del empleo	0.75	P
Número de Objetivos de Control Considerados		2.00	1C
Número de Objetivos de Control Requeridos		3	2P
Cumplimiento R-JB-2005-834 respecto a ISO 27002		**0.67**	0N

Tabla 41. Antes del Empleo

3.4.4.2 Durante el Empleo

La Resolución menciona capacitación para el tema de operaciones de TI, pero no se especifica la capacitación en áreas de seguridad y tampoco se considera un proceso disciplinario para los empleados que han cometido un incumplimiento. La participación de la gerencia está ausente en este tema.

A.8.2	Durante el Empleo	IA	CC
A.8.2.1	Responsabilidades de la Gerencia	0.00	N
A.8.2.2	Capacitación y Educación en la seguridad de Inf.	0.00	N
A.8.2.3	Proceso Disciplinario	0.00	N
Número de Objetivos de Control Considerados		0.00	0C
Número de Objetivos de Control Requeridos		3	0P
Cumplimiento R-JB-2005-834 respecto a ISO 27002		**0.00**	3N

Tabla 42. Durante el Empleo

3.4.4.3 Terminación o Cambio de Empleo

Existen debilidades en cuando a que empleados, contratistas y terceras personas debieran devolver todos los activos de la organización, además la revocación de los derechos de acceso a los sistemas tampoco se ha establecido.

A.8.3	Terminación o Cambio De Empleo	IA	CC
A.8.3.1	Terminación de Responsabilidades	1.00	C
A.8.3.2	Devolución de Activos	0.50	P
A.8.3.3	Revocación de Derechos de Acceso	0.25	P
Número de Objetivos de Control Considerados		1.75	1C
Número de Objetivos de Control Requeridos		3	2P
Cumplimiento R-JB-2005-834 respecto a ISO 27002		**0.58**	0N

Tabla 43. Terminación o Cambio De Empleo

La falta de control posibilita la presencia de incidentes de seguridad debido al a la falta de concienciación en temas de seguridad y a la ausencia de un proceso disciplinario; adicionalmente, la falta de un aseguramiento de eliminación de accesos podrían permitir acceso no autorizado a la información.

3.4.5 SEGURIDAD FISICA Y AMBIENTAL

3.4.5.1 Areas Seguras

ISO exige que las áreas seguras debieran protegerse mediante controles de ingreso para asegurar que únicamente se permita el acceso al personal autorizado.

La Resolución no menciona seguridad en oficinas o habitaciones, así como tampoco se indican los lineamientos para trabajar en áreas seguras. La Resolución si se preocupa por las condiciones físicas y ambientales necesarias para garantizar el correcto funcionamiento del entorno de la infraestructura de TI.

A.9.1	Areas Seguras	IA	CC
A.9.1.1	Perímetro de Seguridad Física	1.00	C
A.9.1.2	Controles de Entrada Físicos	1.00	C
A.9.1.3	Seguridad de Oficinas, habitaciones y medios	0.00	N
A.9.1.4	Protección contra amenazas externas y ambientales	1.00	C
A.9.1.5	Trabajo en áreas seguras	0.00	N
A.9.1.6	Areas de Acceso Público, entrega y carga	0.00	N
Número de Objetivos de Control Considerados		3.00	3C
Número de Objetivos de Control Requeridos		6	0P
Cumplimiento R-JB-2005-834 respecto a ISO 27002		**0.50**	3N

Tabla 44. Aéreas Seguras

3.4.5.2 Seguridad del Equipo

Este objetivo de control busca evitar la pérdida, daño, robo o compromiso de los activos y la interrupción de las actividades de la organización.

A.9.2	Seguridad del Equipo	IA	CC
A.9.2.1	Ubicación y protección del equipo	1.00	C
A.9.2.2	Servicios Públicos	0.75	P
A.9.2.3	Seguridad del cableado	0.00	N
A.9.2.4	Mantenimiento del Equipo	1.00	C
A.9.2.5	Seguridad del Equipo fuera del local	1.00	C
A.9.2.6	Eliminación seguro o re-uso del equipo	0.00	N
A.9.2.7	Retiro de propiedad	0.00	N
Número de Objetivos de Control Considerados		3.75	3C
Número de Objetivos de Control Requeridos		7	1P
Cumplimiento R-JB-2005-834 respecto a ISO 27002		**0.54**	3N

Tabla 45. Seguridad del Equipo

La Resolución no menciona seguridad en el cableado, eliminación ó re-uso de equipos de manera segura, y tampoco se controla el retiro de equipos, información o software. La debilidad de este dominio reside en la posibilidad de exposición de equipos con información confidencial, falta de regulación del comportamiento de las personas en ambientes seguros, lo cual pueden dar lugar a incidentes de seguridad no detectados y exposición de áreas físicas a través de la cual se puede presentar acceso físico no autorizado.

3.4.6 GESTION DE COMUNICACIONES Y OPERACIONES

3.4.6.1 Procedimientos y Responsabilidades Operacionales

Este control es adecuadamente abordado respecto a la gestión de cambios, documentación de procedimientos y segregación de deberes. Únicamente se omite la separación de los ambientes de desarrollo, prueba y operación.

A.10.1	Operaciones y Responsabilidades Operativas	IA	CC
A.10.1.1	Documentación de los procedimientos operativos	1.00	C
A.10.1.2	Control de Cambios	1.00	C
A.10.1.3	Segregación de Deberes	1.00	C
A.10.1.4	Separación de los medios de desarrollo y operacionales	0.00	N
Número de Objetivos de Control Considerados		3.00	3C
Número de Objetivos de Control Requeridos		4	0P
Cumplimiento R-JB-2005-834 respecto a ISO 27002		**0.75**	1N

Tabla 46. Operaciones y Responsabilidades Operativas

La debilidad de este objetivo de control se basa en la posibilidad de cambios no autorizados, presencia de errores en y acceso no autorizado en los ambientes de operación.

3.4.6.2 Administración de Entrega de Servicios a Terceros

La Resolución direcciona el monitoreo y revisión de los servicios de terceros de acuerdo a lo que ISO propone en este control. La entrega del servicio requiere mayor atención en cuanto a controles de seguridad para terceros. Se omite el manejo de cambios en la provisión de servicios de terceros.

A.10.2	Administración De Entrega De Servicios a Terceros	IA	CC
A.10.2.1	Entrega del Servicio	0.75	P
A.10.2.2	Monitoreo y Revisión de los Servicios de Terceros	1.00	C
A.10.2.3	Administración de cambios en los servicios de terceros	0.00	N
Número de Objetivos de Control Considerados		1.75	1C
Número de Objetivos de Control Requeridos		3	1P
Cumplimiento R-JB-2005-834 respecto a ISO 27002		**0.58**	1N

Tabla 47. Operaciones y Responsabilidades Operativas

3.4.6.3 Planeación y Aceptación del Sistema

La Resolución presenta requerimientos en términos de minimizar riesgos potenciales de equipos de computación ante insuficiencia de los recursos. Es decir aborda la gestión de capacidad a nivel general. No establece criterios de aceptación de los sistemas de información nuevos, actualizaciones, no se

especifica la ejecución de pruebas de sistema durante el desarrollo y antes de su aceptación.

A.10.3	Planeación y Aprobación del Sistema	IA	CC
A.10.3.1	Gestión de Capacidad	0.75	P
A.10.3.2	Aceptación del Sistema	0.00	N
Número de Objetivos de Control Considerados		0.75	0C
Número de Objetivos de Control Requeridos		2	1P
Cumplimiento R-JB-2005-834 respecto a ISO 27002		**0.38**	1N

Tabla 48. Planeación y Aprobación del Sistema

3.4.6.4 Protección Contra Software Malicioso y Móvil

La Resolución exige la instalación y actualización periódica de aplicaciones de detección y desinfección de virus informáticos y demás software malicioso; no se considera controles de prevención y recuperación y tampoco se especifica la categoría de código móvil para su control.

A.10.4	Protección Contra Software Malicioso y Móvil	IA	CC
A.10.4.1	Controles contra Software Malicioso	0.75	P
A.10.4.2	Controles contra códigos móviles	0.50	P
Número de Objetivos de Control Considerados		1.25	0C
Número de Objetivos de Control Requeridos		2	2P
Cumplimiento R-JB-2005-834 respecto a ISO 27002		**0.63**	0N

Tabla 49. Protección Contra Software Malicioso y Móvil

3.4.6.5 Respaldo o Back-Up

La Resolución se ajusta a las consideraciones de ISO sobre los requerimientos para tomar copias de respaldo de la información. Este es uno de los dos objetivos de control con mayor alineamiento de los 39 contemplados por ISO 27002.

A.10.5	Respaldo (Back-Up)	IA	CC
A.10.5.1	Back-up o respaldo de la información	1.00	C
Número de Objetivos de Control Considerados		1.00	1C
Número de Objetivos de Control Requeridos		1	0P
Cumplimiento R-JB-2005-834 respecto a ISO 27002		**1.0**	0N

Tabla 50. Respaldo (Back-Up)

3.4.6.6 Gestión de seguridad de la red

ISO exige protección de la información, los sistemas y las aplicaciones cuando estas utilizan la red para lo cual enuncia la necesidad de controles de red y la inclusión de características de seguridad en los contratos con proveedores. Por su

parte, la Resolución exige una adecuada administración y monitoreo de las redes de datos, no se define que es adecuado por lo que las entidades reguladas podrían aplicar un libre criterio al respecto. ISO también emplea el término adecuado pero luego establece los lineamientos que definen este adjetivo.

A.10.6	Gestión de Seguridad de Redes	IA	CC
A.10.6.1	Controles de Red	0.25	P
A.10.6.2	Seguridad de los Servicios de Red	0.25	P
Número de Objetivos de Control Considerados		0.50	0C
Número de Objetivos de Control Requeridos		2	2P
Cumplimiento R-JB-2005-834 respecto a ISO 27002		**0.25**	0N

Tabla 51. Gestión de Seguridad de Redes

El riesgo está asociado con el acceso no autorizado a la información en tránsito por una red informática y a la afectación de las aplicaciones y servicios de red.

3.4.6.7 Gestión de Medios

La Resolución demanda un control sobre la gestión de los medios removibles y establecer los procedimientos para el manejo de información. Sin embargo, se descuida la protección de la documentación de los sistemas informáticos y no se dan lineamientos sobre la eliminación de medios de una manera segura.

A.10.7	Gestión de Medios	IA	CC
A.10.7.1	Gestión de los Medios Removibles	1.00	C
A.10.7.2	Eliminación de Medios	0.25	P
A.10.7.3	Procedimientos de Manejo de la Información	1.00	C
A.10.7.4	Seguridad en la documentacion del sistema	0.00	N
Número de Objetivos de Control Considerados		2.25	2C
Número de Objetivos de Control Requeridos		4	1P
Cumplimiento R-JB-2005-834 respecto a ISO 27002		**0.56**	1N

Tabla 52. Gestión de Medios

3.4.6.8 Intercambio de Información

En el contexto de este control, la Resolución exige lineamientos para el intercambio electrónico de información cuando menciona "*proteger la información contenida en documentos…. e intercambio electrónico de datos contra daño, robo, accesos*.. ,"[25] pero se omite los acuerdos de intercambio para proteger la información y medios físicos en tránsito. Además no se considera la protección de información sensitiva

[25] Resolución JB-2005-834 punto 4.3.4.8

en contratos o acuerdos cuando se llevan cabo interconexión de sistemas de información comercial.

A.10.8	Intercambio de Información	IA	CC
A.10.8.1	Políticas de cinterambio de información y procedimientos	1.00	C
A.10.8.2	Acuerdos de Intercambio	0.00	N
A.10.8.3	Medios físicos en tránsito	0.25	P
A.10.8.4	Correo Electrónico	1.00	C
A.10.8.5	Sistemas de Información Comercial.	0.00	N
Número de Objetivos de Control Considerados		2.25	2C
Número de Objetivos de Control Requeridos		5	1P
Cumplimiento R-JB-2005-834 respecto a ISO 27002		**0.45**	2N

Tabla 3.19 Intercambio de Información

3.4.6.9 Servicios de Comercio Electrónico

ISO establece que "*la información involucrada en el comercio electrónico que pasa a través de redes públicas debe protegerse*".[26] La resolución responde bastante bien a este primer lineamiento y exige que "*las instituciones controladas que ofrezcan los servicios de transferencias y transacciones electrónicas deberán contar con políticas y procedimientos de seguridad de la información que garanticen que las operaciones sólo pueden ser realizadas por personas debidamente autorizadas; que el canal de comunicaciones utilizado sea seguro, mediante técnicas de encriptación..*".[27] Sin embargo, ISO es más exigente y especifico en sus controles ya que recomienda adicionalmente control transmisión incompleta, control de routing equivocado, alteración no-autorizada del mensaje, divulgación no-autorizada, duplicación o repetición no-autorizada del mensaje, y por último control de la integridad de la información puesta en un sistema público.

A.10.9	Servicios de Comercio Electronico	IA	CC
A.10.9.1	Comercio electrónico	1.00	C
A.10.9.2	Transacciones en línea	0.50	P
A.10.9.3	Información pública disponible	0.50	P
Número de Objetivos de Control Considerados		2.00	1C
Número de Objetivos de Control Requeridos		3	2P
Cumplimiento R-JB-2005-834 respecto a ISO 27002		**0.67**	0N

Tabla 53. Servicios de Comercio Electrónico

[26] ISO 27002, A.10.9.1
[27] Resolución JB-2005-834 punto 4.3.4.12

3.4.6.10 Monitoreo

La Resolución cubre un gran espectro de los controles de este objetivo, lo cual incluye el registro de auditoría, el monitoreo del sistema de usuarios, los registros del administrador y operador y el registro de fallas. Se deja sin atención, la protección de de los registros mencionados y la sincronización de relojes.

A.10.10	Monitoreo	IA	CC
A.10.10.1	Registro de Auditoría	1.00	C
A.10.10.2	Monitoreo del Sistema de Usuarios	1.00	C
A.10.10.3	Protección de la Información del Registro	0.00	N
A.10.10.4	Registros del Administrador y Operador	1.00	C
A.10.10.5	Registro de Fallas	1.00	C
A.10.10.6	Sincronización de relojes	0.00	N
Número de Objetivos de Control Considerados		4.00	4C
Número de Objetivos de Control Requeridos		6	0P
Cumplimiento R-JB-2005-834 respecto a ISO 27002		**0.67**	2N

Tabla 54. Monitoreo

3.4.7 CONTROL DE ACCESO

3.4.7.1 Requerimientos del Negocio para el Control de Acceso

La Resolución no especifica una política relacionada con el control de acceso, pero se establecen directrices de referidas a seguridad lógica "*Seguridad en el uso del software, la protección de los datos, procesos y programas, así como la del acceso ordenado y autorizado de los usuarios a la información*."

A.11.1	Requerimientos de Negocio para el Control de Acceso	IA	CC
A.11.1.1	Política de control de acceso	0.25	P
Número de Objetivos de Control Considerados		0.25	0C
Número de Objetivos de Control Requeridos		1	1P
Cumplimiento R-JB-2005-834 respecto a ISO 27002		**0.25**	0N

Tabla 55. Requerimientos del Negocio para el Control de Acceso

3.4.7.2 Gestión de Acceso del Usuario

La Resolución contempla la restricción de privilegios y revisión de los derechos de acceso de la clave de usuario. En menor grado se consideran procedimientos formales para el registro, des-registro de los usuarios y para otorgar y revocar el acceso a los sistemas de información. No se encuentran especificaciones sobre gestión de claves secretas de usuario.

A.11.2	Gestión de Acceso del Usuario	IA	CC
A.11.2.1	Registro del Usuario	0.50	P
A.11.2.2	Gestión de Privilegios	1.00	C
A.11.2.3	Gestión de la Clave de Usuario	0.00	N
A.11.2.4	Revisión de los derechos de acceso de la clave de usuario	0.75	P
Número de Objetivos de Control Considerados		2.25	1C
Número de Objetivos de Control Requeridos		4	2P
Cumplimiento R-JB-2005-834 respecto a ISO 27002		**0.56**	1N

Tabla 56. Gestión de Acceso del Usuario

3.4.7.3 Responsabilidades del Usuario

La Resolución no considera los lineamientos que ISO propone este en objetivo de control. No se precisa las responsabilidades del usuario pero si se considera las responsabilidades de administración de riesgo. La ausencia de este control permite que el usuario ignore su responsabilidad en seguridad de la información.

A.11.3	Responsabilidades del Usuario	IA	CC
A.11.3.1	Uso de clave	0.00	N
A.11.3.2	Equipo de usuario desatenido	0.50	P
A.11.3.3	Política de pantalla y escritorio limpio	0.00	N
Número de Objetivos de Control Considerados		0.50	0C
Número de Objetivos de Control Requeridos		3	1P
Cumplimiento R-JB-2005-834 respecto a ISO 27002		**0.17**	2N

Tabla 57. Responsabilidades del Usuario

3.4.7.4 Control de Acceso a Redes

Existe un amplio vacio en casi la totalidad de los controles de acceso a la red. La Resolución se limita a citar en su numeral 4.3.4.6, "*Adecuados sistemas de control y autenticación para evitar accesos no autorizados, inclusive de terceros; y, ataques externos especialmente a la información crítica y a las instalaciones de procesamiento*". Sin embargo ISO es mucho más exigente al respecto y propone siete controles para responder a riesgos de este tipo, algunos de los cuales tienen un alto nivel de especialización.

A.11.4	Control de Acceso a Redes	IA	CC
A.11.4.1	Política sobre el uso de servicios de red	0.50	P
A.11.4.2	Autenticación del usuario para conexiones externas	1.00	C
A.11.4.3	Identificación del equipo en red	0.00	N
A.11.4.4	Protección del puerto de diagnóstico remoto	0.00	N
A.11.4.5	Segregación de redes	0.00	N
A.11.4.6	Control de conexión de redes	0.00	N
A.11.4.7	Control de routing de redes	0.00	N
Número de Objetivos de Control Considerados		1.50	1C
Número de Objetivos de Control Requeridos		7	1P
Cumplimiento R-JB-2005-834 respecto a ISO 27002		**0.21**	5N

Tabla 58. Control de Acceso a Redes

3.4.7.5 Control del Acceso al Sistema Operativo

El control de registro está considerado, mientras que la identificación y la gestión de claves no cubre totalmente las exigencias de ISO, estos son considerados de una manera muy general en el numeral 4.3.4.4, "*Un sistema de administración de las seguridades de acceso a la información, que defina las facultades y atributos de los usuarios, desde el registro, eliminación y modificación, pistas de auditoría; además de los controles necesarios que permitan verificar su cumplimiento,*" los tres controles restantes son ignorados.

A.11.5	Control del Acceso al Sistema Operativo	IA	CC
A.11.5.1	Procedimientos para un registro seguro	1.00	C
A.11.5.2	Identificación y autenticación del usuario	0.50	P
A.11.5.3	Sistema de gestión de claves	0.50	P
A.11.5.4	Uso de Utilidades del sistema	0.00	N
A.11.5.5	Sesión inactiva	0.00	N
A.11.5.6	Limitación del tiempo de conexión	0.00	N
Número de Objetivos de Control Considerados		2.00	1C
Número de Objetivos de Control Requeridos		6	2P
Cumplimiento R-JB-2005-834 respecto a ISO 27002		**0.33**	3N

Tabla 59. Control del Acceso al Sistema Operativo

3.4.7.6 Aplicación e Información del Control de Acceso

La restricción de acceso está contemplada en el mismo numeral de la Resolución citado en el objetivo de control anterior. No se exige ambientes aislados para sistemas sensibles.

A.11.6	Aplicación e Información del Control de Acceso	IA	CC
A.11.6.1	Restricción al acceso a la información	1.00	C
A.11.6.2	Aislamiento del sistema sensible	0.00	N
Número de Objetivos de Control Considerados		1.00	1C
Número de Objetivos de Control Requeridos		2	0P
Cumplimiento R-JB-2005-834 respecto a ISO 27002		**0.50**	1N

Tabla 60. Aplicación e Información del Control de Acceso

3.4.7.7 Computación Móvil y Tele-Trabajo

El control de las telecomunicaciones no es una fortaleza de la Resolución, se omiten los dos controles.

A.11.7	Computación Móvil y Tele-Trabajo	IA	CC
A.11.7.1	Computación móvil y comunicaciones	0.00	N
A.11.7.2	Tele-trabajo	0.00	N
Número de Objetivos de Control Considerados		0.00	0C
Número de Objetivos de Control Requeridos		2	0P
Cumplimiento R-JB-2005-834 respecto a ISO 27002		**0.0**	2N

Tabla 61. Computación Móvil y Tele-Trabajo

3.4.8 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

3.4.8.1 Requerimientos de Seguridad de los Sistemas

La Resolución no considera enunciados con requerimientos de controles de seguridad para sistemas de información nuevos, o las mejoras a los sistemas de información existentes.

A12.1	Requerimientos de Seguridad de los Sistemas	IA	CC
A.12.1.1	Análisis y especificación de requerimientos de seguridad	0.00	N
Número de Objetivos de Control Considerados		0.00	0C
Número de Objetivos de Control Requeridos		1	0P
Cumplimiento R-JB-2005-834 respecto a ISO 27002		**0.0**	1N

Tabla 62. Requerimientos de Seguridad de los Sistemas

3.4.8.2 Procesamiento Correcto en las Aplicaciones

La Resolución indica requerimientos generales relativos a este control en su numeral 4.3.4.3, “Los controles necesarios para asegurar la integridad, disponibilidad y confidencialidad de la información..,” pero no precisa el control del procesamiento correcto.

A12.2	Procesamiento Correcto en las Aplicaciones	IA	CC
A.12.2.1	Validación de datos de entrada	0.00	N
A.12.2.2	Control de procesamiento interno	0.00	N
A.12.2.3	Integridad del mensaje	0.50	P
A.12.2.4	Validación de los datos de salida	0.00	N
Número de Objetivos de Control Considerados		0.50	0C
Número de Objetivos de Control Requeridos		4	1P
Cumplimiento R-JB-2005-834 respecto a ISO 27002		**0.13**	3N

Tabla 63. Procesamiento Correcto en las Aplicaciones

3.4.8.3 Controles Criptográficos

La Resolución considera criptografía únicamente en el canal de comunicaciones, se omite la gestión de claves para dar soporte al uso de técnicas criptográficas en las instituciones controladas.

A12.3	Controles Criptográficos	IA	CC
A.12.3.1	Política sobre el uso de controles criptográficos	0.75	P
A.12.3.2	Gestión de claves	0.00	N
Número de Objetivos de Control Considerados		0.75	0C
Número de Objetivos de Control Requeridos		2	1P
Cumplimiento R-JB-2005-834 respecto a ISO 27002		**0.38**	1N

Tabla 64. Controles Criptográficos

3.4.8.4 Seguridad de los Archivos del Sistema

La Resolución considera la administración de versiones de las aplicaciones puestas en producción, pero no especifica sobre el tratamiento de datos de prueba ni restricciones del acceso al código fuente de programas.

A.12.4	Seguridad de los Archivos del Sistema	IA	CC
A.12.4.1	Control del software operacional	0.50	P
A.12.4.2	Protección de los datos de prueba del sistema	0.00	N
A.12.4.3	Control de acceso del código fuente del programa	0.00	N
Número de Objetivos de Control Considerados		0.50	0C
Número de Objetivos de Control Requeridos		3	1P
Cumplimiento R-JB-2005-834 respecto a ISO 27002		**0.17**	2N

Tabla 65. Seguridad de los Archivos del Sistema

3.4.8.5 Seguridad en los Procesos de Desarrollo y Soporte

La Resolución establece fuertes exigencias sobre la supervisión y monitoreo del desarrollo del software abastecido externamente, Además exige procedimientos de control de cambio, sin embargo se deja fuera de consideración la revisión técnica de la aplicación después de haberse realizado cambios en el sistema y el filtrado de información.

A.12.5	Seguridad en los Procesos de Desarrollo y Soporte	IA	CC
A.12.5.1	Procedimientos de control de cambio	1.00	C
A.12.5.2	Revisión técnica de la aplicación después de cambios en el sistema	0.00	N
A.12.5.3	Restricciones sobre los cambios en los paquetes de software	0.50	P
A.12.5.4	Filtración de Información	0.00	N
A.12.5.5	Desarrollo externo de software	1.00	C
Número de Objetivos de Control Considerados		2.50	2C
Número de Objetivos de Control Requeridos		5	1P
Cumplimiento R-JB-2005-834 respecto a ISO 27002		**0.50**	2N

Tabla 66. Seguridad en los Procesos de Desarrollo y Soporte

3.4.8.6 Gestión de Vulnerabilidad Técnica

La Resolución no exige un proceso de gestión de vulnerabilidades técnicas sobre los sistemas. En estas condiciones no se conocería la exposición de estas vulnerabilidades, por tanto no hay habría exigencia sobre las medidas de remediación.

A.12.6	Gestión de Vulnerabilidad Técnica	IA	CC
A.12.6.1	Control de vulnerabilidades técnicas	0.00	N
Número de Objetivos de Control Considerados		0.00	0C
Número de Objetivos de Control Requeridos		1	0P
Cumplimiento R-JB-2005-834 respecto a ISO 27002		**0.00**	1N

Tabla 67. Gestión de Vulnerabilidad Técnica

3.4.9 GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE INFORMACIÓN

3.4.9.1 Reporte de los Eventos y Debilidades de la Seguridad de la Información

La Resolución toma cuidado en la identificación de eventos de riesgo. En su artículo 9 se cubre: fraude, daños físicos, interrupciones, deficiencias en prácticas laborales y deficiencias legales. No se habla directamente del reporte, pero se exige que los niveles directivos estén enterados. Además, a pesar de que si se exige la comunicación de los incidentes relativos a la seguridad (numeral 4.3.4.1), ISO es más exigente y plantea obligaciones de este tipo sobre los usuarios empleados, contratistas y terceros.

A13.1	Reporte de los Eventos y Debilidades de la Seguridad de la Información	IA	CC
13.1.1	Reporte de eventos en la seguridad de la información	1.00	C
13.1.2	Reporte de las debilidades en la seguridad	0.50	P
Número de Objetivos de Control Considerados		1.50	1C
Número de Objetivos de Control Requeridos		2	1P
Cumplimiento R-JB-2005-834 respecto a ISO 27002		**0.75**	0N

Tabla 68. Reporte de los Eventos y Debilidades de la Seguridad

3.4.9.2 Gestión de los Incidentes y Mejoras en la Seguridad de la Información

En el numeral 4.3.2.1, la Resolución establece las responsabilidades y los procedimientos del directorio para asegurar respuestas a incidentes de TI. Esta sección se encuentra muy focalizada en eventos de riesgo operativo y se plantea su identificación para posteriormente tomar decisiones al respecto. Se establece la cuantificación de posibles pérdidas de eventos de seguridad, pero no se precisa el aprovechamiento de lecciones aprendidas y recolección de evidencia.

A13.2	Gestión de los Incidentes y Mejoras en la Seguridad de la Información	IA	CC
13.2.1	Responsabilidades y procedimientos	1.00	C
13.2.2	Aprender de los incidentes en la seguridad de la información	0.25	P
13.2.3	Recolección de evidencia	0.00	N
Número de Objetivos de Control Considerados		1.25	1C
Número de Objetivos de Control Requeridos		3	1P
Cumplimiento R-JB-2005-834 respecto a ISO 27002		0.42	1N

Tabla 69. Gestión de los Incidentes y Mejoras en la seguridad

3.4.10 GESTIÓN DE LA CONTINUIDAD COMERCIAL

Los artículos 15 y 16 de la Resolución cubren satisfactoriamente todos los requerimientos de este dominio de ISO 27002:2005. Se evidencia una coincidencia casi exacta en este ámbito con ISO 27002:2005. Este dominio representa la fortaleza más relevante de la Resolución.

A.14.1	**Seguridad de Información en la Gestión de la Continuidad Comercial**	**IA**	**CC**
A.14.1.1	Compromiso de la gerencia con la seguridad de la información	1.00	C
A.14.1.2	Continuidad comercial y evaluación del riesgo	1.00	C
A.14.1.3	Desarrollar en implementar planes de continuidad incluyendo seguridad de la información	1.00	C
A.14.1.4	Marco referencial para la planeación de la continuidad de información	1.00	C
A.14.1.5	Prueba, mantenimiento y re-evaluación de planes de continuidad comerciales	1.00	C
Número de Objetivos de Control Considerados		5.00	5C
Número de Objetivos de Control Requeridos		5	0P
Cumplimiento R-JB-2005-834 respecto a ISO 27002		**1.00**	0N

Tabla 70. Gestión de la Continuidad Comercial

3.4.11 CUMPLIMIENTO

3.4.11.1 Cumplimiento con Requisitos Legales

La Resolución satisface la identificación de la legislación aplicable. Respecto a los registros de datos, no se contempla el control de falsificación y destrucción en términos específicos. La protección de datos se indica a nivel general, no se menciona a la legislación como un motivante para su protección. Se omite la protección de derechos de propiedad intelectual, la prevención de uso inadecuado de los recursos de procesamiento y la regulación de controles criptográficos.

A.15.1	**Cumplimiento con Requisitos Legales**	**IA**	**CC**
A.15.1.1	Identificación de Legislación aplicable	1.00	C
A.15.1.2	Derechos de Propiedad Intelectual (IPR)	0.00	N
A.15.1.3	Protección de los registros de la organización	0.50	P
A.15.1.4	Protección de los datos y privacidad de información personal	0.50	P
A.15.1.5	Prevención de uso inadecuado de los recursos de procesamiento de información	0.00	N
A.15.1.6	Regulación de controles criptográficos	0.00	N
Número de Objetivos de Control Considerados		2.00	1C
Número de Objetivos de Control Requeridos		6	2P
Cumplimiento R-JB-2005-834 respecto a ISO 27002		**0.33**	3N

Tabla 71. Cumplimiento con Requisitos Legales

3.4.11.2 Cumplimiento con las Políticas Estándares y el Cumplimiento Técnico

En el artículo 4.3.1.4, la Resolución exige el monitoreo del cumplimiento de los controles establecidos, por lo que satisface las exigencias de verificación del cumplimiento técnico. Además de exige el cumplimiento de políticas y normas de seguridad, pero no se considera el apadrinamiento de los gerentes para la aplicación de estos.

A.15.2	Cumplimiento con las Políticas y Estándares de \Seguridad y el Cumplimiento Técnico	IA	CC
A.15.2.1	Cumplimiento de políticas y normas de seguridad	0.50	P
A.15.2.2	Verificación del cumplimiento técnico	1.00	C
Número de Objetivos de Control Considerados		1.50	1C
Número de Objetivos de Control Requeridos		2	1P
Cumplimiento R-JB-2005-834 respecto a ISO 27002		**0.75**	0N

Tabla 72. Cumplimiento Políticas y Estándares

3.4.11.3 Consideraciones de Auditoria de los Sistemas de Información

La Resolución considera la prevención de interrupciones referidas a varios eventos, pero no se menciona a las auditorias o chequeos internos como una posible causa o agente de interrupción. Se omite el control de acceso a las herramientas de auditoría de los sistemas de información.

A.15.3	Consideraciones de Auditoria de los Sistemas de Información	IA	CC
A.15.3.1	Controles de Auditoría de Sistemas de Información	0.50	P
A.15.3.2	Protección de las herramientas de auditoría de los sistemas	0.00	N
Número de Objetivos de Control Considerados		0.50	0C
Número de Objetivos de Control Requeridos		2	1P
Cumplimiento R-JB-2005-834 respecto a ISO 27002		**0.25**	1N

Tabla 73. Consideraciones de Auditoria de los Sistemas de Información

3.5 ANÁLISIS DE RESULTADOS DE ALINEAMIENTO

En concordancia con la metodología explicada, a continuación se presenta el diagrama que esquematiza el grado alineamiento de la Resolución JB-2005-834 respecto a ISO 27002:2005, donde la circunferencia perimetral externa representa los valores máximos de cada uno de los objetivos de control de ISO 27002:2005 y la figura interior representa el alcance que la Resolución ha logrado en cada uno de estos objetivos.

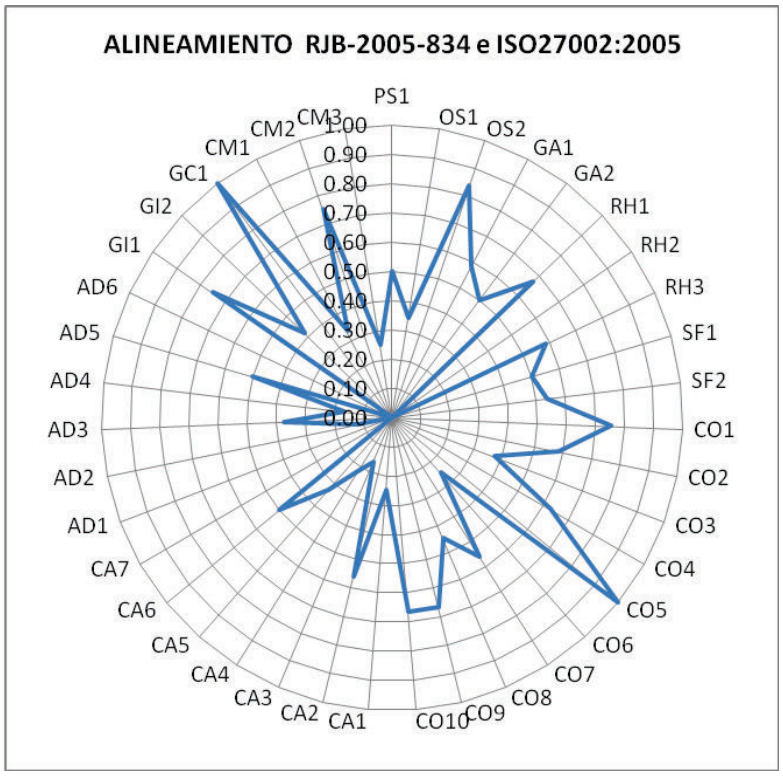

Figura 16. Alineamiento JB-2005-834 respecto a ISO 27002:2005

El índice de alineamiento general estimado es 0.42, lo que deja cierto vacío en los dominios del marco de referencia, así como también presenta áreas aisladas de fortaleza. Seguidamente se exponen las fortalezas y debilidades en la mayoría de los dominios.

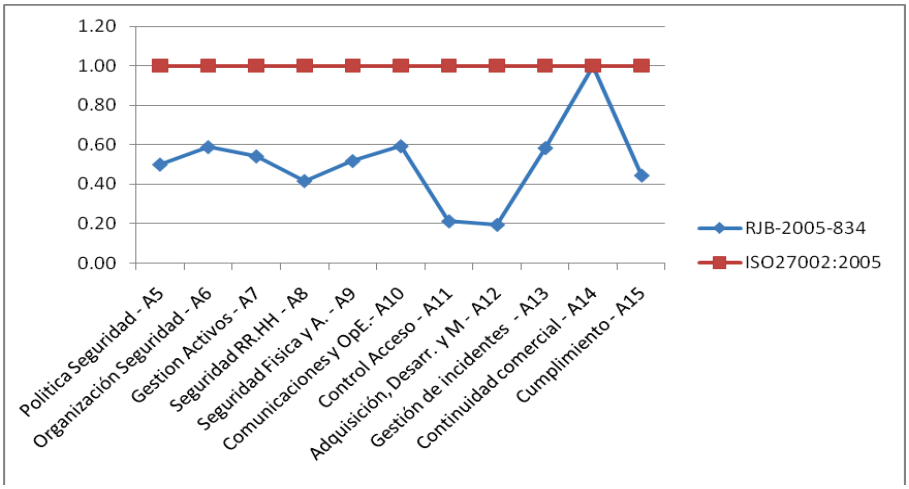

Figura 17. Alineamiento JB-2005-834 por Dominios ISO 27002:2005

Se evidencia que las areas de mayor debilidad se encuentran en los dominios A11 y A12. Los cuales presentan un vacio de control en la adquisición, desarrollo y mantenimiento de sistemas y en el control de acceso a estos sistemas. Por otro lado el punto más fuerte es la gestión de la continuidad comercial.

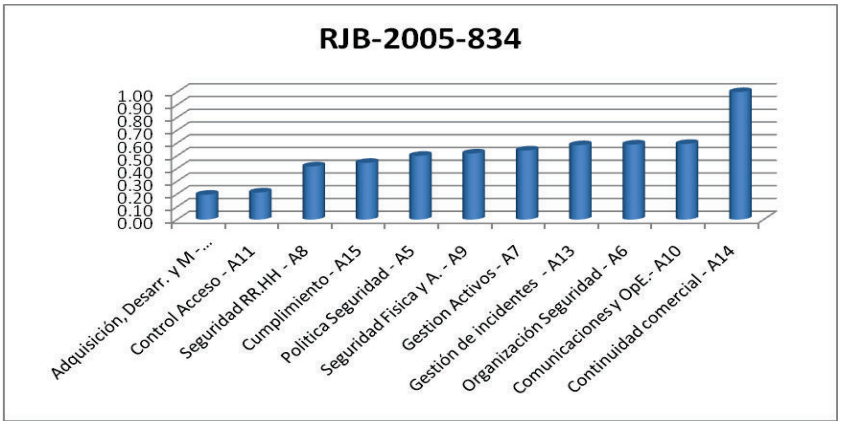

Figura 18. Fortalezas JB-2005-834 por Dominios ISO 27002:2005

3.5.1 ALINEAMIENTO RESPECTO A CRITERIOS DE LA INFORMACIÓN

Según el índice de cumplimiento de la Resolución JB-2005-834 respecto a que cada uno de los objetivos de control de ISO 27002:2005, se tiene que los criterios de información han sido afectados conforme lo muestra la siguiente figura.

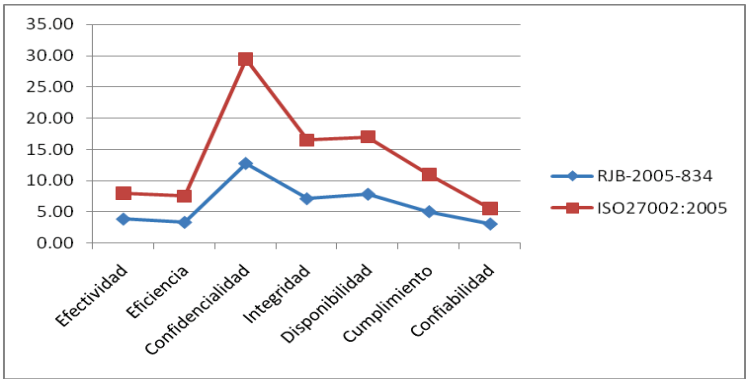

Figura 19. Alineamiento Respecto a Criterios de Información en ISO

La línea que corresponde a ISO 27002 representa la importancia que ISO ofrece a los criterios de información según se explico en la sección 3.2 de este capítulo. La línea que corresponde a la Resolución JB-2005-834 representa la afectación que cada uno de los criterios de información ha sufrido al ser multiplicado por el índice de alineamiento que cada objetivo de control obtuvo en la Resolución. El detalle del cálculo se encuentra en el Anexo H.

Según se observa los criterios de información con un rango de menor cumplimiento en la Resolución JB-2005-834 son la confidencialidad, integridad, disponibilidad, seguidas del cumplimiento. Esto indica claramente que la Resolución tiene debilidades importantes respecto a estos criterios.

3.5.2 ALINEAMIENTO EN EL DOMINIO POLITICA DE SEGURIDAD

El índice de alineamiento en este dominio es 0.5. Las áreas de fortaleza relativa de este dominio se ubican en la documentación de la política de seguridad de la información. El punto de debilidad se encuentra en la revisión de la política de seguridad de la información.

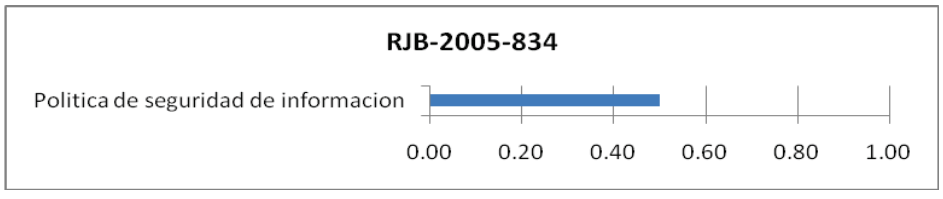

Figura 20. Alineamiento en el Dominio Política de Seguridad

3.5.3 ALINEAMIENTO EN EL DOMINIO ORGANIZACIÓN DE LA SEGURIDAD

El índice de alineamiento en este dominio es 0.59. Las áreas de fortaleza relativa de este dominio se ubican en la Identificación de riesgos relacionados a partes externas y en la seguridad en acuerdos de terceras partes. El punto de debilidad relativa se encuentra en la organización interna.

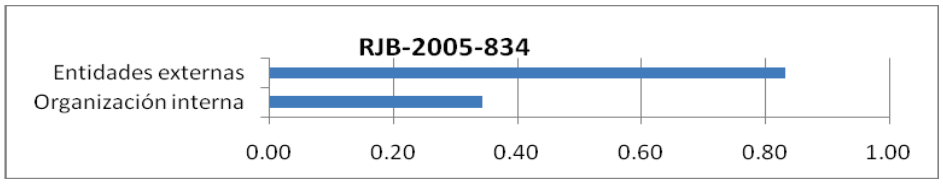

Figura 21. Alineamiento en el Dominio Organización de la Seguridad

3.5.4 ALINEAMIENTO EN EL DOMINIO GESTION DE ACTIVOS

El índice de alineamiento en este dominio es 0.54. Los controles tienen el similar nivel de cumplimiento que se puede calificar de medio. La debilidad relativa esta en el uso aceptable de los activos y en el etiquetado y manejo de la información.

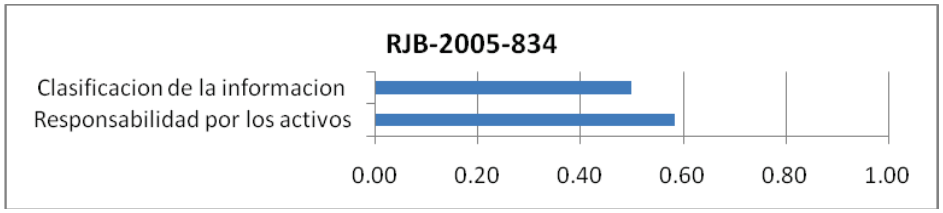

Figura 22. Alineamiento en el Dominio Gestión de Activos

3.5.5 ALINEAMIENTO EN EL DOMINIO SEGURIDAD DE LOS RECURSOS HUMANOS

El índice de alineamiento en este dominio es 0.42. Las áreas de fortaleza relativa de este dominio se ubican en la gestión del personal antes y en el cambio o terminación del empleo. El punto de debilidad se encuentra en la gestión durante el empleo.

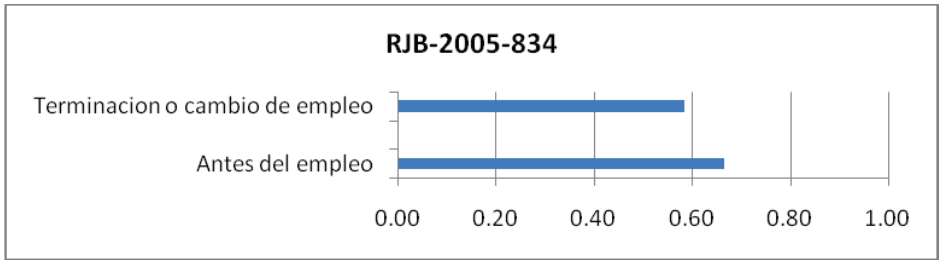

Figura 23. Alineamiento en el Dominio Seguridad de Recursos Humanos

3.5.6 ALINEAMIENTO EN EL DOMINIO SEGURIDAD FISICA Y AMBIENTAL

El índice de alineamiento en este dominio es 0.52. Los controles tienen el similar nivel de cumplimiento que se puede calificar de medio. Las áreas de fortaleza relativa de este dominio se ubican en el perímetro de seguridad física, controles de entrada físicos y protección contra amenazas externas y ambientales. Las áreas de debilidad están en la seguridad del cableado, trabajo en áreas seguras y re-uso de equipos principalmente.

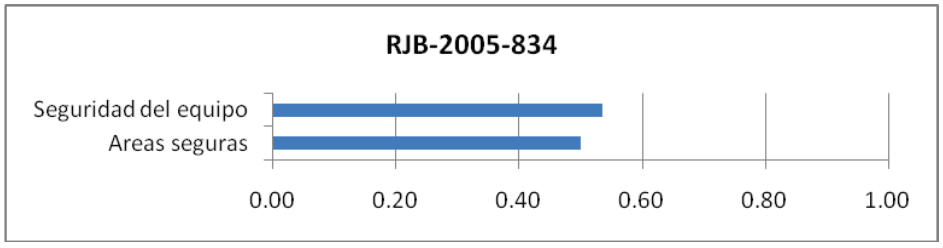

Figura 24. Alineamiento en el Dominio Seguridad Física y Ambiental

3.5.7 ALINEAMIENTO EN EL DOMINIO GESTION DE COMUNICACIONES Y OPERACIONES

El índice de alineamiento en este dominio es 0.59. Según se muestra en la figura, las áreas de fortaleza relativa de este dominio se ubican en los procedimientos de respaldo, operaciones y responsabilidades operativas; en menor proporción la gestión de servicios de comercio electrónico, monitoreo y protección contra software malicioso. El área de mayor debilidad está en la gestión de seguridad de redes.

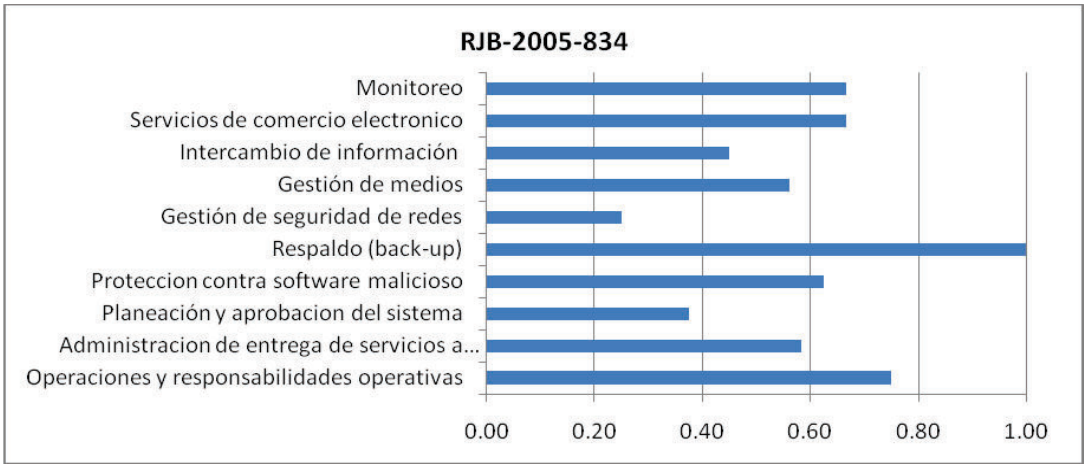

Figura 25. Alineamiento en el Dominio Gestión de Comunicaciones

3.5.8 ALINEAMIENTO EN EL DOMINIO CONTROL DE ACCESO

El índice de alineamiento en este dominio es 0.21, lo cual nos indica que es uno de los dos dominios de ISO con el cumplimiento más bajo. El punto de relativa fortaleza es gestión de acceso del usuario. Existen varias áreas de extrema debilidad, especialmente en la seguridad de las redes de telecomunicaciones, el proceso de acceso remoto y responsabilidades del usuario.

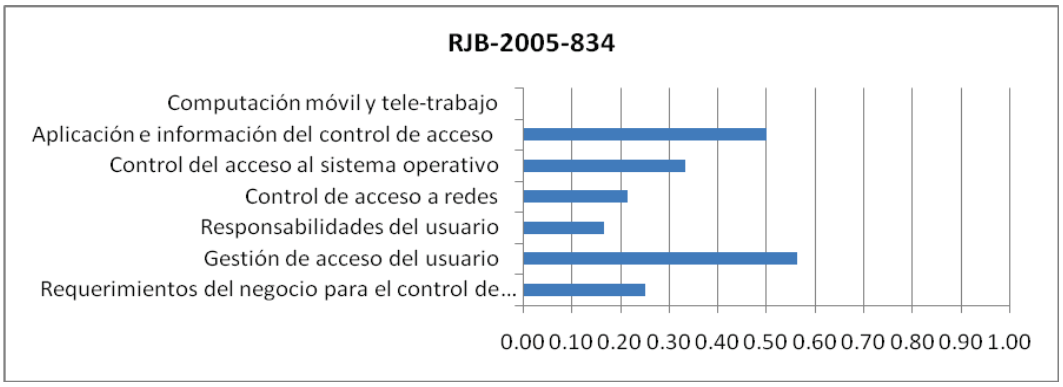

Figura 26. Alineamiento en el Dominio Control de Acceso

3.5.9 ALINEAMIENTO EN EL DOMINIO ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

El índice de alineamiento en este dominio es 0.19, dejando a este dominio como el punto más débil de los once dominios de ISO. Las áreas de mayor alineamiento están en la seguridad en los procesos de desarrollo y soporte. Las áreas de

debilidad extrema se encuentran en la falta de requerimientos de seguridad de los sistemas y la inexistencia de gestión de vulnerabilidad técnica.

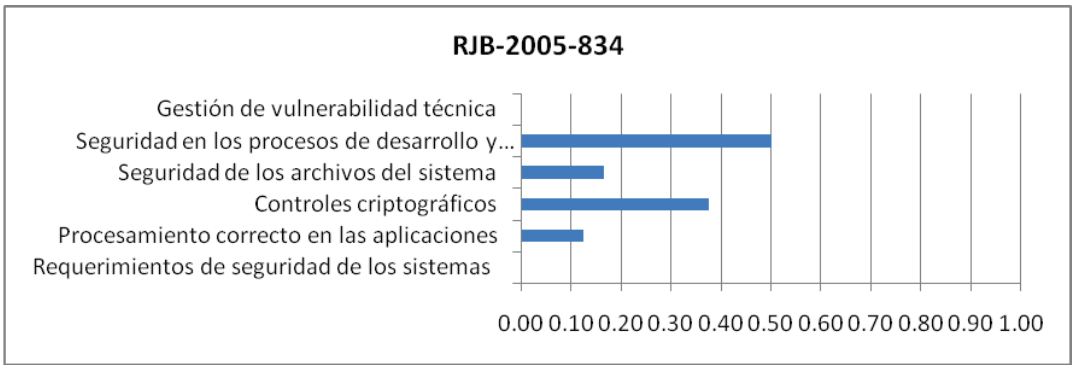

Figura 27. Alineamiento en el Dominio Adquisición, D. y M. de Sistemas

3.5.10 ALINEAMIENTO EN EL DOMINIO GESTIÓN DE INCIDENTES DE SEGURIDAD

El índice de alineamiento en este dominio es 0.58. Las áreas de fortaleza de este dominio se ubican en reporte de eventos y debilidades de seguridad. Las áreas de debilidad relativamente esta en el reporte de incidentes de seguridad y la implementación de mejoras.

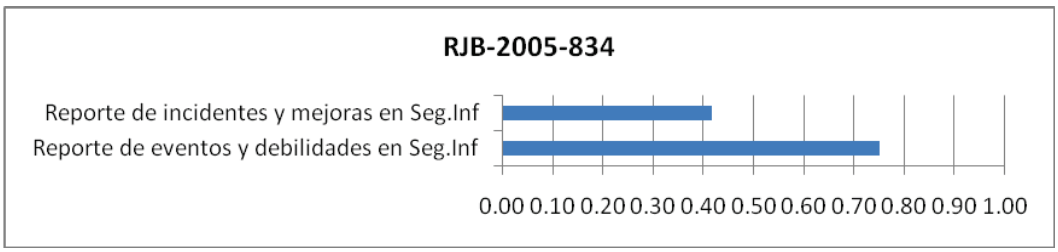

Figura 28. Alineamiento en el Dominio Gestión de Incidentes

3.5.11 ALINEAMIENTO EN EL DOMINIO GESTIÓN DE CONTINUIDAD COMERCIAL

El índice de alineamiento en este dominio es 1.0. Según se mencionó anteriormente existe una coincidencia exacta de las exigencias de ISO en este dominio, por lo tanto representa la fortaleza más relevante de la Resolución.

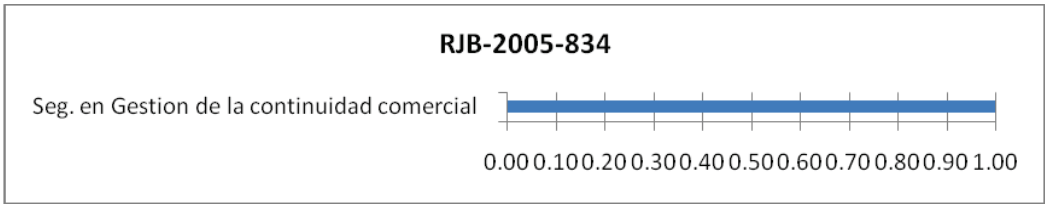

Figura 29. Alineamiento en el Dominio Gestión de Continuidad

3.5.12 ALINEAMIENTO EN EL DOMINIO CUMPLIMIENTO

El índice de alineamiento en este dominio es 0.44. Las áreas de fortaleza relativa de este dominio se ubican en el cumplimiento con las políticas y estándares de seguridad y el cumplimiento técnico. Las áreas de debilidad están en las consideraciones de auditoría de los sistemas de información y el cumplimiento de las exigencias de ISO para los requisitos legales.

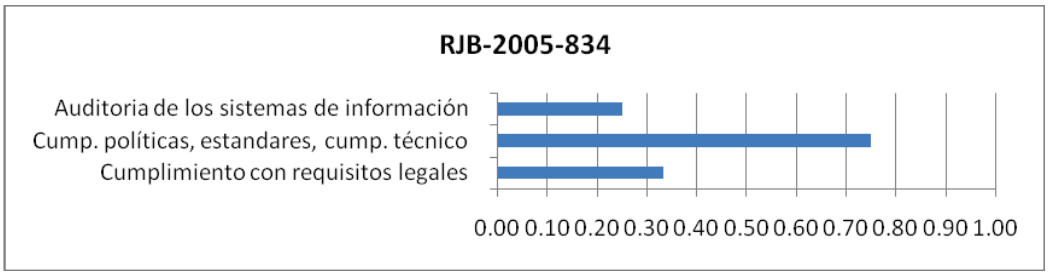

Figura 30. Alineamiento en el Dominio Cumplimiento

En conclusión, el análisis realizado muestra que la Resolución JB-2005-834 contiene varios elementos técnicos necesarios para administrar RTI, sin embargo existen varias generalizaciones que dan lugar a interpretaciones por parte de las entidades financieras reguladas y adicionalmente por la entidad de control. Esto se podría evidenciar en los procesos de auditoría que se deben practicar a las instituciones. Es notorio que ISO 27002 considera algunos controles elevadamente técnicos que no se van a encontrar en una Resolución bancaria, sin embargo el concepto de control relacionado con estos aspectos especializados debería estar presente en la mencionada regulación. Por otro lado, también hay controles que no son técnicos pero también están ausentes. Como resultado del análisis, se evidencia que las propiedades de la información relativas a la administración de

riesgos respecto a ISO 27002 se encuentran comprometidas en este orden; la confidencialidad, la disponibilidad, la integridad, y el cumplimiento.

De esta manera se ha concluido el análisis comparativo de la Resolución JB-2005-834 respecto a las dos referencias planteadas. En el próximo capítulo se abordará la propuesta de mejoramiento.

CAPITULO 4
PROPUESTA DE MEJORAMIENTO A LA RESOLUCIÓN JB-2005-834

Los capítulos anteriores realizaron el análisis comparativo de la Resolución JB-2005-834 respecto a COBIT 4.1 y respecto a ISO 27002:2005, donde se identificaron oportunidades de mejoramiento en el marco de regulación de las Tecnologías de la Información en el ámbito financiero ecuatoriano. Este capítulo presentará una propuesta de mejoramiento de la Resolución JB-2005-834 que incluirá principios de control que se han identificado como ausentes. Para el efecto, este capítulo toma criterios contenidos en las dos referencias ISO y COBIT dentro de un procedimiento metodológico. La propuesta considera dos factores, el primero contempla las áreas de debilidad de la Resolución JB-2005-834 expresadas en el índice de alineamiento respecto a los dos estándares. De esta manera, se conocerá en qué áreas se debería concentrar el mejoramiento. El segundo factor considera el enfoque de Administración de Riesgos que tiene tanto ISO y COBIT respecto a las Tecnologías de la Información. Esto proporcionará una visión de los controles importantes requeridos de manera *sine qua non* para establecer una propuesta efectiva.

4.1 ESTRATEGIA DE MEJORAMIENTO

La estrategia se enmarca en los factores mencionados, los cuales se explican a continuación.

4.1.1 AREAS DE DEBILIDAD DE RESOLUCIÓN JB-2005-834

La figura 4.1 muestra las áreas de concentración de debilidades respecto a COBIT 4.1 e ISO27002 expresadas en función de los criterios de la información, donde se aprecian dos puntos de vista diferentes. En primera instancia, COBIT presenta las debilidades de la Resolución en el área de gobierno, es decir *Efectividad y Eficiencia (EE)*, y después en *Confidencialidad, Integridad y Disponibilidad (CID).*

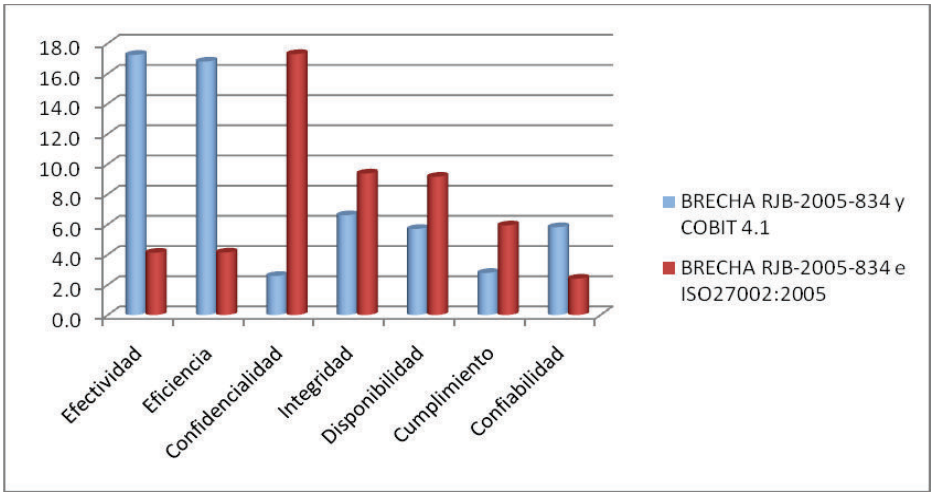

Figura 31. Brecha de RJB-2005-834 Respecto a Criterios de la Información

Por otro lado, el analisis basado en ISO dice que las áreas de debilidad se encuentra en CID. Es decir, COBIT le da la razón a ISO especialmente en las áreas de la integridad y disponibilidad, pero esto en segunda instancia ya que para COBIT la prioridad es EE, es decir efectividad y eficiencia.

Con fines exclusivamente visuales, la figura 4.2 muestra una suma simple de las brechas en ISO y COBIT, lo cual confirma que las debilidades encontradas en CID toman un protagonismo significativo después de EE.

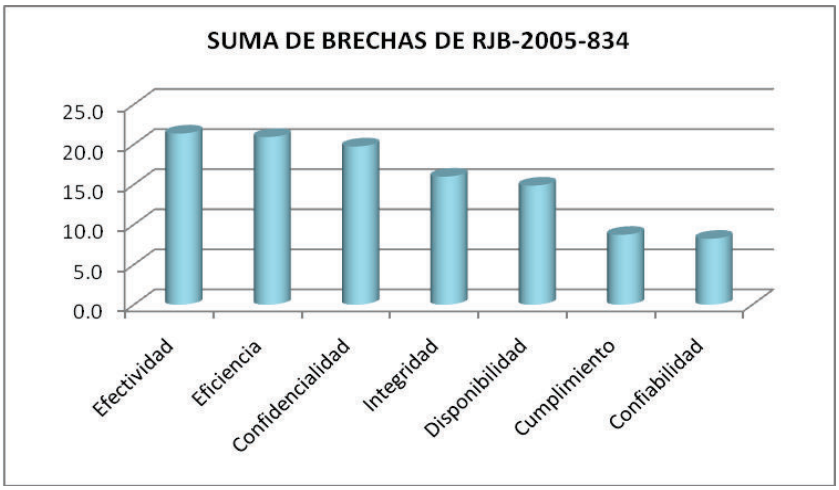

Figura 32. Suma de Brechas de RJB-2005-834

Para interpretar adecuadamente estos resultados, seguidamente recordaremos el enfoque que los estándares tienen respecto a los criterios de información y la administración del riesgo.

4.1.2 ADMINISTRACION DE RIESGO EN TI SEGÚN COBIT E ISO

COBIT presenta el estado de la Resolución JB-2005-834 desde una amplia perspectiva donde se incluyen conceptos de administración de riesgos, alineación estratégica, entrega de valor, administración de recursos, y medición de desempeño. Según se expresa en el capítulo 2, la *Administración de Riesgos* es una de las cinco *áreas de Gobierno de TI* y está contemplada transversalmente en los cuatro dominios de COBIT. Esto se evidencia en la sección *IT Governance Focus Areas – Risk Management* de la tabla contenida en el Apéndice II del Marco de Trabajo de COBIT.[28] En esta se especifica que la administración de riesgos está contemplada en 26 de los 34 procesos del marco de trabajo. De estos 26 procesos, 11 son considerados como primarios y 15 secundarios, esto dependiendo de su enfoque hacia el riesgo.

Adicionalmente, y según se especifica en el capítulo 2, COBIT también tiene un *proceso de alto nivel* denominado "*Evaluación y Administración de Riesgos de TI*" que viene a ser una especificación más particular del concepto de gestión de riesgos. Según este, los criterios de información primarios para el proceso de gestión de riesgos son: la Integridad, Disponibilidad y Confiabilidad*;* dejando como secundarios los criterios de Efectividad, Eficiencia, Cumplimiento y Confiabilidad.[29]

Por otro lado, ISO27002 basa su enfoque en la Gestión de la Seguridad de la Información, por lo que es necesario citar que dice ISO al respecto, "*Seguridad de la información es la preservación de confidencialidad, integridad y disponibilidad de la información; además, también puede involucrar otras propiedades como autenticidad, responsabilidad, y el no repudio.*"[30] En esta definición, ISO expresa

[28] Apendice II COBIT 4.1, IT Governance Focus Areas, Incluido en el Anexo B de este documento.
[29] Apendice II COBIT 4.1, IT Governance Focus Areas.
[30] ISO 27002:2005

seguridad en términos de criterios de información, dando relevancia a Confidencialidad, Integridad y Disponibilidad.

Si se compara el enfoque de COBIT e ISO, ambos coinciden en que CID son los criterios más importantes para la Administración de Riesgos de TI y para la Seguridad de la Información. Este análisis, proporciona un direccionamiento de hacia donde deberían estar orientados los esfuerzos de mejoramiento de la Resolución JB-2005-834, es claro que CID debe constar como una prioridad en el programa de mejoramiento que propone este capítulo.

Dentro de este contexto, el siguiente gráfico muestra la fortaleza de los dos estándares en cada uno de los criterios de información.

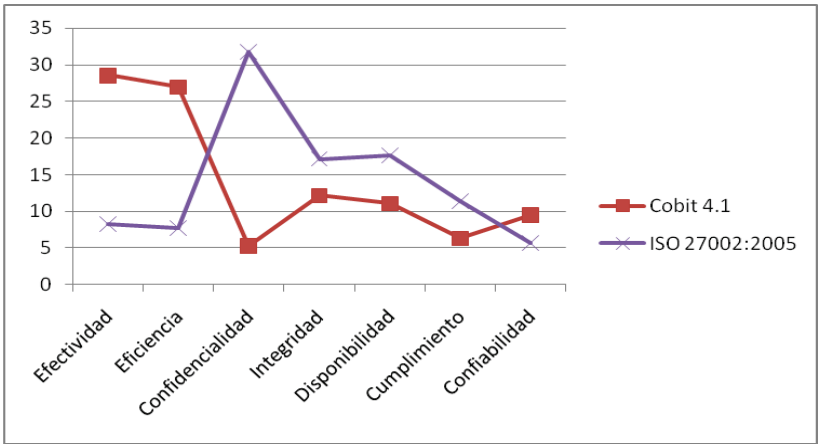

Figura 33. COBIT e ISO respecto a Criterios de la Información

Este gráfico se ha obtenido calculando la importancia que los dos estándares asignan a los criterios de información y expresando este concepto en términos porcentuales. El detalle se lo ha descrito en la sección 2.2 del capítulo 2 para COBIT 4,1 y sección 3.2 del capítulo 3 para ISO 27002.

El gráfico evidencia la fortaleza de ISO 27002 en los criterios de la información CID y la fortaleza de COBIT en los criterios EE. Por otro lado, las debilidades más representativas en la Resolución JB-2005-834 están en CID. Por consiguiente, la propuesta de mejoramiento de la Resolución JB-2005-834 inicia con la identificación de las oportunidades de mejora respecto a ISO 27002.

4.2 PROPUESTA DE MEJORAMIENTO RESPECTO A ISO 27002:2005

Un proceso de gestión de riesgo de las tecnologías de la información en el ámbito financiero, debería evaluar la inclusión de todos los lineamientos que ISO presenta para la gestión de seguridad de la información. Esto debido a la alta dependencia que mantienen las instituciones financieras de las TI en sus actividades operacionales.

Debido a la orientación de ISO hacia CID, la propuesta de mejoramiento recibe un alto soporte de ISO 27002:2005. Una solución relativamente sencilla de expresar sería “Hay que implementar ISO 27002”, lo cual no se aleja de la realidad; y, si una institución decide alinearse a este objetivo, seguramente va a administrar el riesgo de TI en base a principios sólidos. Sin embargo, con el propósito de plantear una propuesta alternativa, se ha realizado un análisis de los controles en que la Resolución JB-2005-834 puede mejorar para incrementar su efectividad de una manera equilibrada en cuanto a las fortalezas del estándar respecto a las debilidades de la Resolución.

El criterio para elegir los objetivos de controles de ISO que formarán parte de la propuesta se basa en los siguientes principios:

- Índice de alineamiento (IA)
- Índice de relevancia (IR)
- Esfuerzo relativo de implementación (ER)

El *índice de alineamiento* (IA) es uno de los criterios más importantes que nos ha dejado el análisis de los dos capítulos anteriores ya que especifican donde están las áreas de debilidad y por tanto las oportunidades de mejoramiento en la Resolución JB-2005-834. La propuesta de mejoramiento considera la inclusión de los objetivos de control que obtuvieron un índice de alineamiento menor e igual 0.5,

lo cual incluye objetivos de control con extrema debilidad y objetivos omitidos por la Resolución.

El *Índice de Relevancia (IR)* se refiere a la estimación cuantitativa del grado de importancia o relevancia que ISO asigna a cada uno de sus objetivos de control únicamente respecto a los criterios de información: confidencialidad, integridad y disponibilidad. Para el efecto, se utiliza la misma información que se empleó para graficar la importancia que ISO ofrece a los siete criterios de la información que se describe en la sección 3.2 de este documento, y que se detalla en los Anexos E e I.

En resumen, el índice de relevancia es un valor numérico entre cero y uno que expresa el grado de importancia que un objetivo de control de ISO 27002:2005 tiene respecto a CID. Se lo obtiene calculado la media aritmética del grado de importancia que un objetivo de control tiene en confidencialidad, integridad y disponibilidad.

ID	Objetivo de Control	Confiden Cialidad	Integri dad	Disponi bilidad	Indice de Relevancia
A.10.6	Gestión de seguridad de redes	1	1	1	1.00
A.10.3	Planeación y aprobacion del sistema		1	1	0.67
A.6.2	Entidades externas	1			0.33

Tabla 4.1 Cálculo del Incide de Relevancia

De acuerdo al ejemplo que muestra la tabla 4.1, los dos primeros objetivos de control serán incluidos en la propuesta debido a que su índice es mayor a 0.5. Este índice no es un elemento tomado de bibliografía alguna y se lo utiliza en este documento únicamente con el propósito mencionado.

El *Esfuerzo Relativo de Implementación (ER)* se refiere al esfuerzo operacional de implementar un objetivo de control ISO 27002 y está expresado únicamente en términos cualitativos (alto, medio y bajo); esto en base a la observación y experiencia del autor de este documento. Un objetivo de control es incluido en la propuesta cuando el esfuerzo es bajo ó medio. Por ejemplo; la Resolución JB-2005-834 no contempla exigencias de manera completa para los controles en el área de recursos humanos, esto es, antes del empleo y posterior al empleo. La implantación

de estos requieren un esfuerzo medio dependiendo del tamaño de la organización, lo cual comprende la inclusión y ejecución de políticas organizacionales respectivas. El criterio de esfuerzo relativo únicamente se ha aplicado a estos dos objetivos de control relacionado con recursos humanos. Por lo que no se realizará una calificación a los demás criterios ya que no es necesario debido a su consideración en los criterios anteriores.

Ciertos criterios podrían estar sujetos a cierto grado de subjetividad, y además podrían responder a varias consideraciones; como por ejemplo: capacidad económica y estructural de las instituciones financieras, plazos de implementación, estado de madurez actual de las instituciones, entre otros factores. De hecho COBIT también especifica en su documentación que puede existir cierto grado de subjetividad al asignar la importancia a los criterios de información, por lo que estos planteamientos deben ser tomados como una aproximación.

Como consecuencia de la aplicación de los tres criterios explicados, la siguiente figura presenta de manera esquemática la propuesta de mejoramiento para la Resolución JB-2005-834. El detalle se lo puede encontrar en el Anexo H.

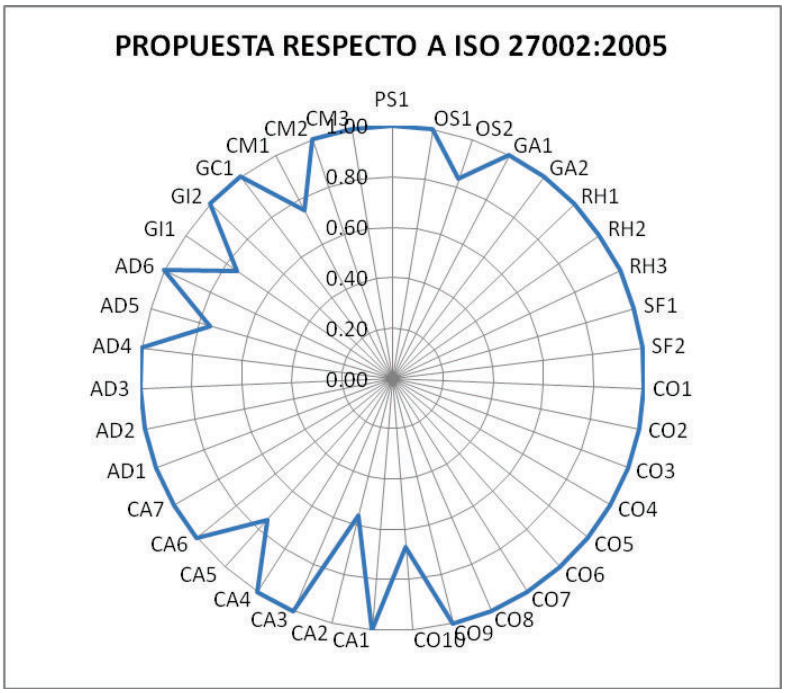

Figura 34. Propuesta de Mejoramiento Respecto a ISO 27002:2005

La interpretación de la figura presenta las modificaciones que deberían introducirse en la Resolución, la cual debería incluir enunciados que incluyan el concepto de control en los ámbitos siguientes.

4.2.1 POLITICA DE SEGURIDAD

- Actualización periódica de la política de seguridad.

4.2.2 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

- Uso aceptable de los activos.
- Etiquetado y manejo de la información.
- Ser más específico respecto a la propiedad de los activos.

4.2.3 SEGURIDAD DE LOS RECURSOS HUMANOS

- Investigación de antecedentes de candidatos para empleo.
- Establecer sus responsabilidades y las de la organización para la seguridad de la información en los términos y condiciones del empleo.
- Establecimiento de responsabilidades de la gerencia respecto a la aplicación de políticas de seguridad.
- Capacitación y educación en la seguridad de Información y establecimiento de un proceso disciplinario por incumplimiento de las políticas de seguridad.
- Control sobre la revocación de derechos de acceso y énfasis en la devolución de activos.

4.2.4 SEGURIDAD FISICA Y AMBIENTAL

- Seguridad en oficinas, habitaciones y medios; control del trabajo en áreas seguras, áreas de acceso público, entrega y carga.
- Seguridad del cableado eléctrico y de telecomunicaciones, eliminación segura, re-uso de equipos y retiro de propiedad.

4.2.5 GESTION DE COMUNICACIONES Y OPERACIONES

- Aceptación de los sistemas y énfasis sobre un plan para la gestión de capacidad.
- Ser más específico en la implementación de controles contra código malicioso ya que el uso de adjetivos como “adecuado” para el control, deja mucha libertad de interpretación. Además, se debería citar controles para código móvil.
- Controles de red y seguridad de los servicios de red.
- Procedimientos formales para eliminación de medios y seguridad en la documentación de los sistemas de TI.
- Incluir requerimientos o características de seguridad de la información en los contratos.
- Protección de la Información de registros para evitar la alteración y el acceso no autorizado e implementar la sincronización de relojes.

4.2.6 CONTROL DE ACCESO

- Establecer, documentar y revisar la política de control de acceso.
- Control en la asignación de claves secretas a través de un proceso formal y hacer énfasis en el registro y des-registro del usuario.
- Uso de clave, política de pantalla y escritorio limpio; además ser más específico respecto a controles para equipo de usuario desatendidos.
- Control de acceso a redes, donde se incluya identificación del equipo en red, protección de puertos de diagnóstico remoto, segregación de redes, control de conexión de redes y enrutamiento.
- Control sobre las utilidades del sistema, sesión inactiva y limitación del tiempo de conexión.
- Ser más específicos sobre la restricción de acceso a la información y el aislamiento de sistema sensibles.
- Control en computación móvil, comunicaciones y tele-trabajo.
- El control de acceso a redes, este objetivo de control requiere especial atención ya que es uno de los puntos más débiles.

4.2.7 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

- Análisis y especificación de requerimientos de seguridad en sistemas de TI.
- Control en el procesamiento, validación de datos de entrada y salida.
- Gestión de claves y ser más específico en la política sobre el uso de controles criptográficos.
- Control del software operativo, protección de los datos de prueba del sistema, y control de acceso del código fuente de programas.
- Revisión técnica de la aplicación después de cambios en el sistema y filtro u ocultamiento de información.
- Control de vulnerabilidades técnicas.

4.2.8 GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE INFORMACIÓN

- Aprendizaje de los incidentes de seguridad y recolección de evidencia.

4.2.9 CUMPLIMIENTO

- Derechos de Propiedad Intelectual, prevención de uso inadecuado de los recursos de procesamiento de información, regulación de controles criptográficos. Además, ser más específico respecto a la protección de los registros de la organización.

Según se menciona, es conveniente realizar una modificación sobre enunciados que actualmente son muy generales por términos más específicos en algunas áreas de control de ISO, con ello se lograría un incremento significativo en el alineamiento de la Resolución respecto a ISO 27002. De esta manera el auditor que va a controlar el cumplimiento en las instituciones financieras, no tendrá que acudir a su discreción para determinar si una institución cumple o no con un determinado requerimiento. El capítulo 3 representa una guía para el mejoramiento en este sentido.

4.3 PROPUESTA DE MEJORAMIENTO RESPECTO A COBIT 4.1

La propuesta define los elementos de control que deberían abordarse con alta prioridad en una actualización al marco de control sobre la administración de riesgo en las Tecnologías de la Información contenida en la Resolución JB-2005-834.

Respecto a la perspectiva de COBIT, la propuesta se concentra en la inclusión de los *procesos de* alto nivel que tienen una relación enfocada directamente con la administración de riesgos según COBIT. El Apéndice II de COBIT 4.1, especifica la lista de estos procesos, así como la importancia primaria y secundaria de estos dentro el proceso de administración de riesgos. De este modo, se conforma un grupo de 26 procesos de alto nivel que permitirán ofrecer un direccionamiento gerencial al proceso de gestión de riesgos en las Tecnologías de la Información.

Con la inclusión de los controles mencionados, los criterios EE y Confiabilidad estarán mejor soportados aunque no cubiertos totalmente, ya que no es el objetivo de la versión de esta propuesta en particular.

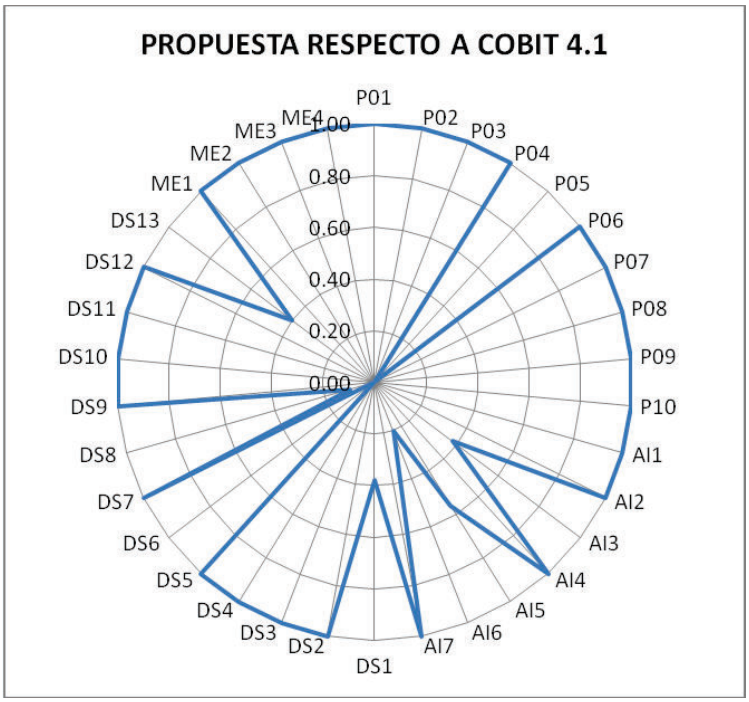

Figura 35. Figura 4.5 Propuesta de Mejoramiento respecto a COBIT 4.1

La interpretación de la figura muestra las modificaciones que deberían introducirse en la Resolución, la cual debería contener enunciados que incluyan conceptos de control en los siguientes ámbitos.

4.3.1 MEJORAMIENTO EN LA PLANIFICACION Y ORGANIZACIÓN

Esta área de mejoramiento cubre las oportunidades que existen en las estrategias y las tácticas para mejorar a la contribución de logro de los objetivos del negocio en función de la administración de riesgo. Par el efecto es necesario que en unos casos se implemente y en otros se mejore la implantación de los siguientes objetivos de control, según se detalla en el Anexo K.

- La administración del valor de TI, alineación de TI con el negocio, los planes tácticos de TI, y la administración del portafolio de TI.
- Definición de un modelo de arquitectura de Información corporativa y su correspondiente diccionario de datos.
- Definición de un plan de Infraestructura Tecnológica, un consejo de arquitectura de TI y establecer un monitoreo de tendencias de regulaciones y tecnologías emergentes.
- Definición de un comité estratégico de TI, comité directivo de TI, ubicación organizacional de la función de TI, estructura organizacional, responsabilidad de aseguramiento de calidad de TI, garantizar el ejercicio de roles y responsabilidades, dependencia del personal clave de TI y mejorar el enlace, comunicación entre TI y otras instancias fuera de TI, como lo son consejo directivo, ejecutivos, y otras unidades de negocio. Adicionalmente, ser más específicos respecto a la propiedad de datos y de sistemas.
- Mejorar la comunicación de las expectativas de la gerencia mediante un ambiente de políticas y de control, y la comunicación de los objetivos de negocio y de TI a los interesados.
- La administración de la calidad se puede mejorar respecto a estándares y prácticas de calidad, estándares de desarrollo y de adquisición, enfoque en el cliente de TI, mejora continua, medición, monitoreo y revisión de la calidad.

- La evaluación y administración de riesgos de TI requiere que se implemente el establecimiento del contexto del riesgo, un mantenimiento y monitoreo de un plan de acción de riesgos y se mejore en menor dimensión en cuanto a evaluación de riesgos de TI, esto conforme lo explica COBIT en el objetivo de control P09. Ver Anexo K.

4.3.2 MEJORAMIENTO EN LA ADQUISICION E IMPLEMENTACION

De la misma manera que en el anterior numeral, se requiere que la implantación de los siguientes objetivos de control y el mejoramiento de otros. Se sugiere revisar los detalles en el capítulo 2 y el Anexo K.

- Implantación completa de un proceso para identificar soluciones automatizadas, que incluya la definición y mantenimiento de requerimientos técnicos y funcionales del negocio; el reporte de análisis de riesgos, estudio de factibilidad y formulación de cursos de acción alternativos, requerimientos, decisión de factibilidad y aprobación.
- Mejoramiento de la adquisición y mantenimiento del software aplicativo, su diseño detallado, control y posibilidad de auditar las aplicaciones, seguridad y disponibilidad de las aplicaciones, configuración e implantación de software aplicativo adquirido, desarrollo de software aplicativo, aseguramiento de la calidad del software y administración de los requerimientos de aplicaciones.
- Transferencia de conocimiento de aprobaciones relacionadas con seguridad a la gerencia del negocio.
- Entrenamiento en operación de los sistemas de TI, definición de planes de prueba, de implantación, ambientes de prueba, pruebas de cambios, pruebas de aceptación final, promoción a producción y revisión posterior a la implantación.

4.3.3 MEJORAMIENTO EN LA ENTREGA Y SOPORTE

Para lograr un mejoramiento en los niveles de servicio y alineación de los servicios de TI respecto a los requerimientos de negocio, se debería considerar los siguientes objetivos de control conforme lo precisa el capitulo 2 y el Anexo K.

- Identificación de todas las relaciones con proveedores, gestión de estas relaciones y la calidad de las mismas, esto en lo que se refiere a la administrar los servicios de terceros.
- Planeación del desempeño, la capacidad y disponibilidad de recursos de TI.
- Definir controles para la seguridad de la red. Mejorar la planificación de seguridad de TI, pruebas, vigilancia y monitoreo de la seguridad, así como la definición de incidente de seguridad.
- Impartición de entrenamiento y educación, así como la evaluación del entrenamiento recibido.
- Identificación y mantenimiento de elementos de configuración y revisión de la integridad de la configuración.
- Rastreo y resolución de problemas, cierre de problemas, integración de las administraciones de cambios, y gestión de la configuración y problemas
- Requerimientos del negocio para administración de datos, acuerdos de almacenamiento, conservación, y eliminación segura.
- Medidas de seguridad física, administración de instalaciones físicas y protección contra factores ambientales

4.3.4 MEJORAMIENTO EN EL MONITOREO Y EVALUACION

La entrega de los servicios y soporte requiere incluir la implantación y mejoramiento de los siguientes objetivos de control según se detalla en el Anexo K.

- Enfoque del monitoreo, definición y recolección de datos, método de monitoreo, evaluación del desempeño, reportes al consejo directivo y a ejecutivos, así como las acciones correctivas.
- Excepciones de control, auto evaluación, aseguramiento del control interno, control interno para terceros y acciones correctivas.
- Aseguramiento positivo del cumplimiento.

Según se ha indicado, sería oportuno realizar una modificación sobre enunciados que actualmente son muy generales por términos más específicos en algunas

áreas de control de COBIT, algunos procesos no existen en la Resolución por lo que requieren una implantación total. El capítulo 2 representa una guía para el mejoramiento en este sentido.

Una propuesta de actualización a la Resolución 834 debería considerar los dos estándares de referencia. Ahora, evidentemente los dos estándares tienen un área de intersección común; es decir que los controles de ISO tienen un alineamiento con los procesos planteados por COBIT. Por lo que el implementar mejoras utilizando ISO implica un mejoramiento directo en algunos procesos de COBIT. El Instituto de Governanza de las Tecnologías de la Información en su publicación "*Mapping of ISO/IEC 17799:2005 with COBIT 4.0*", ubica esta área de intersección en los siguientes procesos PO04, PO05, PO06, PO07, PO09, DS4, DS5, DS11, DS12, ME2 y ME3, estos lineamientos se los podría considerar como aplicables a nuestro análisis ya que no existe una diferencia sustancial en la estructura de COBIT 4.0 respecto a su versión 4.1

4.4 CONSIDERACION FINAL

De esta manera se ha expuesto en este capítulo una alternativa de mejoramiento, la cual se concentra en aspectos exclusivos de la administración de riesgo desde el punto de vista de dos referencias ampliamente aceptadas en los procesos de gestión de las Tecnologías de la Información.

Una segunda alternativa sería sin duda el cumplimiento de todos los objetivos de control de ISO y todos los procesos de alto nivel de COBIT 4.1; lo cual podría lograrse agregando a la Resolución todos aquellos conceptos omitidos en los dos estándares y que se detallan en el capítulo dos y tres de este documento. De este modo, este documento de manera global en su estructura propone los principios de mejoramiento útiles para dos alternativas; la primera enfocada en Riegos de TI y la segunda considerando la inclusión de todos los procesos de COBIT y objetivos de control de ISO 27002.

El proceso de gestión de riesgos en las Tecnologías de la Información, al igual que otros tipos de riesgos corporativos, es un reto para las organizaciones financieras, las cuales requiere procedimientos de administración y metodologías complejas de estimación. La legislación ecuatoriana en un intento por regular la gestión de riesgo operacional ha entregado en la Resolución JB-2005-834 un direccionamiento para administrar el riesgo de TI. Sin embargo, según se ha expuesto en este documento en conformidad con dos estándares aceptados, existen evidentes oportunidades de mejoramiento que deberían ser direccionadas. Especialmente después de que ha transcurrido casi cinco años desde su emisión original, y adicionalmente debido a que las entidades financieras necesitan desarrollar sus actividades en un ambiente cada vez más competitivo, ofreciendo estabilidad a la confianza de sus clientes, del gobierno ecuatoriano y en general de la sociedad.

CAPITULO 5

CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

- La Resolución JB-2005-834 establece un marco inicial de regulación del Riesgo de TI, la cual en el año 2005 ofreció los primeros lineamientos a las instituciones financieras ecuatorianas en su reto de administrar este riesgo. Sin embargo, se ha encontrado que bajo la luz de las referencias que ofrecen las mejores prácticas relativas, existen varias áreas que requieren un mejoramiento con el propósito de lograr una administración más efectiva de RTI. Los riesgos empresariales y de TI están sujetos a constantes cambios, y las instituciones requieren adaptarse a estos cambios. De hecho el estándar de ISO 27002 y el marco de referencia COBIT, están continuamente cambiando en la búsqueda de un mejoramiento continuo a través de investigación y lecciones aprendidas. Esta realidad plantea la necesidad de una actualización a la Resolución JB-2005-834 para adaptarla al contexto dinámico de RTI.

- Las áreas de debilidad absoluta (índice de alineamiento de cero) de la Resolución JB-2005-834 respecto a COBIT 4.1 se encuentran en dos procesos relativos al gobierno de TI, en uno de soporte de TI, y en cinco procesos administración de riesgos de TI. Respecto al gobierno de TI, la Resolución no realiza consideraciones de administración de las inversiones de TI ni administración de costos. En cuanto al soporte no se contempla la administración de la mesa de servicios. Finalmente respecto a la administración de riesgo, no se contempla, administración de proyectos, administración de problemas, automatización de soluciones, acreditación de cambios, y el desempeño de TI. En menor grado, pero en un estado comprometido se encuentra el concepto de calidad, la cual no figura como una preocupación de la Resolución JB-2005-834.

- Las áreas de debilidad más representativas (índice de alineamiento de cero o cercano a cero) de la Resolución JB-2005-834 respecto a ISO 27002 se encuentran en la gestión del control de acceso y en el mantenimiento y desarrollo de sistemas. El control de acceso presenta cuatro objetivos de control extremadamente débiles, los cuales incluyen el acceso a la red, las responsabilidades del usuario, el acceso remoto, y el control de acceso para requerimientos de negocio. El mantenimiento y desarrollo tiene el mismo grado de debilidad que incluyen ausencia de control en los requerimientos de seguridad en los sistemas, vulnerabilidad técnica, seguridad en los archivos de sistema y procesamiento correcto. Por último, un elemento relativamente débil que pertenece a las comunicaciones y operaciones es la gestión de seguridad en redes informáticas, para la cual la Resolución JB-2005-834 se limita a exigir una “adecuada” administración y monitoreo, dejando sin definir el adjetivo adecuado.

- Las áreas de debilidad de la Resolución JB-2005-834 respecto a al marco de COBIT y al estándar de ISO, exponen la posibilidad de que las auditorías realizadas a las instituciones financieras para evaluar el cumplimiento, puedan dejar vacios de control en áreas importantes de la administración de riesgo de TI. Algunas exigencias de la resolución son muy generales y da lugar a la interpretación personal de los auditores de la Superintendencia de Bancos cuando se realice un control de cumplimiento en las instituciones reguladas. Por lo que la efectividad de las auditorías dependerían del grado de experiencia y preparación del auditor. Al existir un marco de regulación que considere objetivos de control estándares, esta ambigüedad podría ser eliminada.

- Las áreas de fortaleza más sobresalientes de la Resolución JB-2005-834 respecto a COBIT se encuentran en los procesos de continuidad del servicio y el cumplimiento con requerimientos externos. Especialmente el primero es el punto más relevante encontrado en la Resolución respecto a su especificación, enfoque y propósito. Respecto a ISO 27002 las fortalezas sobresalientes se

encuentran en el reporte de incidentes y eventos, gestión de respaldo, continuidad de negocio y a la identificación de riesgos con entidades externas. COBIT e ISO coinciden en estos dos últimos puntos. Es evidente que la creación de la Resolución JB-2005-834 consideró muy seriamente el concepto de continuidad comercial.

- La propuesta de mejoramiento considera dos dimensiones, una alineada con los conceptos de gobierno, la cual aborda RTI alineado con una visión empresarial y la segunda que permite llegar al entendimiento técnico de RTI. Así, COBIT a través de los 26 procesos incluidos en la propuesta, entrega un aporte en las áreas eficiencia, efectividad y en cierto grado en CID. Por su parte ISO a través de sus 39 objetivos de control conforme lo plantea la propuesta, entrega un soporte notable en confidencialidad, integridad y disponibilidad. De esta manera se ha realizado un planteamiento de mejora que contempla principios de administración de riesgo y de seguridad de la información, los cuales en su conjunto ofrecen un mejoramiento integral.

5.2 RECOMENDACIONES

- La Superintendencia de Bancos debería realizar una actualización de la Resolución JB-2005-834 considerando una adición de objetivos de control de RTI propuestos por referencias generalmente aceptadas. Esta recomendación está sustentada en el análisis comparativo que expone las debilidades encontradas en RTI respecto al marco y estándar de referencia. Esta investigación propone una alternativa considerando ISO y COBIT, la cual propone el mejoramiento en base a los objetivos de control mínimos requeridos para establecer un grado de mejora focalizado en principios de administración de RTI. De este modo, se plantearía una alternativa de regulación que debería ser discutida con las entidades reguladas para establecer alcances y plazos de planificación e implementación.

- Una actualización de la Resolución JB-2005-834 debería considerar el propósito enfocado en la administración de RTI. La elección de estándares o marcos de referencia con un alcance diferente podrían desviar este propósito. En particular, la aceptación que tiene COBIT en la comunidad de TI se fundamenta en el aporte que este marco ofrece al gobierno y control de TI. Según se ha presentado en este documento, el gobierno de TI tiene un espectro de cobertura más amplio que el riesgo de TI. La inclusión de todo el marco de COBIT en una regulación como la Resolución JB-2005-834 implicaría que las autoridades de regulación estarían influyendo en la manera en que las instituciones financieras generan valor mediante la eficiencia y efectividad de los procesos de TI.

- La regulación de RTI en las instituciones financieras ecuatorianas debería exigir la implementación de los principios de control planteados en el estándar ISO 27002:2005. Esto no necesariamente implica la implantación de todos los controles de ISO 27002:2005; pero si contempla el análisis de la aplicabilidad de cada uno de estos y la decisión de incluirlos o no, en base a una evaluación de riesgo. Según se analiza en el capítulo 4, ISO 27002:2005 ofrece un soporte completamente enfocado en la administración de RTI. Una implementación de este estándar dentro de un Sistema de Gestión de Seguridad Corporativo representa la base sobre la cual las instituciones pueden establecer un proceso de administración de RTI maduro, el cual puede ser complementado con principios gobierno de TI que permitan integrar RTI al soporte de la misión de las instituciones financieras.

- La Superintendencia de Bancos debería evaluar si debe mantener el concepto de RTI como parte del Riesgo Operacional ó definirlo como un tipo de riesgo independiente. En el ámbito financiero ecuatoriano, RTI está considerado como parte del Riesgo Operacional debido a la influencia de Basilea II sobre la Resolución JB-2005-834. Sin embargo, hay otros tipos de riesgos que pueden contener un componente de TI. Un ejemplo es el riesgo estratégico, el cual que puede tener un componente de TI al ser un habilitante clave para nuevas iniciativas de negocio.

REFERENCIAS BIBLIOGRÁFICAS

[1] ISACA, Information Systems Audit and Control Association, “The Risk IT Framework,” Diciembre, 2009.

[2] IT Governance Institute, COBIT 4.1, “Control Objectives for Information and related Technology,” Mayo 2007.

[3] IT Governance Institute, “IT Control Objectives for Basel II: The Importance of Governance and Risk Management for Compliance,” 2007.

[4] Comité de Supervisión Bancaria de Basilea, “Convergencia Internacional de Medidas y Normas de Capital,” Junio 2004.

ISACA, Information Systems Audit and Control Association, “The Risk IT Framework,” December 2009.

[5] Ministerio de Comunicaciones, Republica de Colombia, “Modelo de Seguridad de la Información para la Estrategia de Gobierno en Línea,” Septiembre, 2008.

[6] Superintendencia de Bancos y Seguros del Ecuador, “Libro I.- Normas Generales para la aplicación de la Ley General de Instituciones del Sistema Financiero, Titulo X.- De la Gestión y Administración de Riesgos, Capítulo V.- De la Gestión del Riesgo Operativo, Resolución No JB-2005-834,” Octubre, 2005.

[7] Superintendencia de Bancos y Seguros del Ecuador, “Libro I.- Normas Generales para la aplicación de la Ley General de Instituciones del Sistema Financiero, Titulo X.- De la Gestión y Administración de Riesgos, Capitulo I.- De la Gestión Integral y Control de Riesgos, Resolución No JB-2004-631,” Enero, 2004.

[8] Basel Committee on Banking Supervision, “Practicas sanas para la Administración y Supervisión del Riesgo Operacional,” Febrero, 2003.

[9] ISO, International Organization for Standardization, ISO-IEC 27002, “Tecnología de la Información – Técnicas de Seguridad – Código para la práctica de la Gestión de la Seguridad de la Información,” Julio, 2007.

[10] NIST, National Institute of Standards and Technology, Gary Stoneburner, Alice Goguen, y Alexis Feringa, “Risk Management Guide for Information Technology Systems”, Julio 2002.

ANEXO A

IMPORTANCIA DE LOS CRITERIOS DE INFORMACION EN COBIT 4.1

	OBJETIVO DE CONTROL	ID	Efectividad	Eficiencia	Confidencialidad	Integridad	Disponibilidad	Cumplimiento	Confiabilidad
Planear y Organizar	Definir un Plan Estratégico	P01	1	0.5					
	Definir la Arquitectura de la Información.	P02	0.5	1	0.5	1			
	Determinar la Dirección Tecnológica.	P03	1	1					
	Definir los Procesos, Organización y Relaciones de TI.	P04	1	1					
	Administrar la Inversión en TI.	P05	1	1					0.5
	Comunicar las Aspiraciones y la Dirección de la Gerencia	P06	1					0.5	
	Administrar los Recursos Humanos de TI.	P07	1	1					
	Administrar la Calidad.	P08	1	1		0.5			0.5
	Evaluar y Administrar los Riesgos de TI	P09	0.5	0.5	1	1	1	0.5	0.5
	Administrar Proyectos.	P10	1	1					
Adquirir e Implementar	Identificar Soluciones Automatizadas	AI1	1	0.5					
	Adquirir y Mantener Software Aplicativo	AI2	1	1		0.5			0.5
	Adquirir y Mantener Infraestructura Tecnológica	AI3	0.5	1		0.5	0.5		
	Facilitar la Operación y el Uso	AI4	1	1		0.5	0.5	0.5	0.5
	Adquirir Recursos de TI	AI5	0.5	1				0.5	
	Administrar Cambios	AI6	1	1		1	1		0.5
	Instalar y Acreditar Soluciones y Cambios	AI7	1	0.5		0.5	0.5		
Entregar y Soportar	Definir y Administrar los Niveles de Servicio	DS1	1	1	0.5	0.5	0.5	0.5	0.5
	Administrar los Servicios de Terceros	DS2	1	1	0.5	0.5	0.5	0.5	0.5
	Administrar el Desempeño y la Capacidad	DS3	1	1			0.5		
	Garantizar la Continuidad del Servicio	DS4	1	0.5			1		
	Garantizar la Seguridad de los Sistemas	DS5			1	1	0.5	0.5	0.5
	Identificar y Asignar Costos	DS6		1					1
	Educar y Entrenar a los Usuarios	DS7	1	0.5					
	Administrar la Mesa de Servicio y los Incidentes	DS8	1	1					
	Administrar la Configuración	DS9	1	0.5			0.5		0.5
	Administración de Problemas	DS10	1	1			0.5		
	Administración de Datos	DS11				1			1
	Administración del Ambiente Físico	DS12				1	1		
	Administración de Operaciones	DS13	1	1		0.5	0.5		
Monitorear y Evaluar	Monitorear y Evaluar el Desempeño de TI	ME1	1	1	0.5	0.5	0.5	0.5	0.5
	Monitorear y Evaluar el Control Interno	ME2	1	1	0.5	0.5	0.5	0.5	0.5
	Garantizar el Cumplimiento con Requerimientos Externos	ME3						1	0.5
	Proporcionar Gobierno de TI	ME4	1	1	0.5	0.5	0.5	0.5	0.5

1: Importancia Primaria (P) *
0: Importancia Secundaria (S) *

* Información tomada del Apéndice II de COBIT 4.1, el cual se incluye en el Anexo B de este documento.

ANEXO B

APENDICE II DE COBIT 4.1.[31]

Apendice II – Mapeo de Procesos de TI a las Areas Focales de Gobierno TI, COSO, Recursos de TI de CobiT y Criterios de Información de CobiT

		Áreas de enfoque de Gobierno TI					COSO					Recursos TI de CobiT				Criterios de Información de CobiT						
	IMPORTANCIA	Alineación estratégica	Entrega de valor	Administración de	Administración de	Medición del desempeño	Entorno de Control	Evaluación de riesgos	Actividades de control	Información y	Monitoreo	Aplicación	Información	Infraestructura	Personas	Efectividad	Eficiencia	Confidencialidad	Integridad	Disponibilidad	Cumplimiento	Confiabilidad
Planear y Organizar																						
PO1 Definir un plan estratégico de TI	A	P		S	S			P		S	S					P	S					
PO2 Definir la arquitectura de la información	B	P	S	P	S				P	P						S	P	S	P			
PO3 Determinar la dirección tecnológica	M	S	S	P	S			S	P	S						P	P					
PO4 Definir los procesos, organización y relaciones de TI	B	S		P	P		P			S	S					P	P					S
PO5 Administrar la inversión en TI	M	S	P	S		S		S	P							P	P					
PO6 Comunicar las aspiraciones y la dirección de la gerencia	M	P			P		P			P						P					S	
PO7 Administrar recursos humanos de TI	B	P		P	S	S	P			S						P	P					
PO8 Administrar la calidad	M	P	S		S		P		P	S	P					P	P		S			S
PO9 Evaluar y administrar los riesgos de TI	A	P			P			P								S	S	P	P	P	S	S
PO10 Administrar proyectos	A	P	S	S	S	S	S	S	P		S					P	P					
Adquirir e Implementar																						
AI1 Identificar soluciones automatizadas	M	P	P	S	S				P							P	S					
AI2 Adquirir y mantener software aplicativo	M	P	P		S				P							P	P		S			S
AI3 Adquirir y mantener infraestructura tecnológica	B			P					P							S	P		S	S		
AI4 Facilitar la operación y el uso	B	S	P	S	S				P	S						P	P		S	S	S	S
AI5 Adquirir recursos de TI	M		S	P					P							S	P				S	
AI6 Administrar cambios	A		P	S				S	P		S					P	P		P	P		S
AI7 Instalar y acreditar soluciones y cambios	M	S	P	S	S	S			P	S	S					P	S		S	S		
Entregar y Dar Soporte																						
DS1 Definir y administrar los niveles de servicio	M	P	P	P		P	S		P	S	S					P	P	S	S	S	S	S
DS2 Administrar los servicios de terceros	B		P	S	P	S	P	S	P		S					P	P	S	S	S	S	S
DS3 Administrar el desempeño y la capacidad	B	S	S	P	S	S			P		S					P	P			S		
DS4 Garantizar la continuidad del servicio	M	S	P	S	P	S	S		P	S						P	S			P		
DS5 Garantizar la seguridad de los sistemas	A				P				P	S	S							P	P	S	S	S
DS6 Identificar y asignar costos	B		S	P		S			P								P					P
DS7 Educar y entrenar a los usuarios	B	S	P	S	S		P			S						P	S					
DS8 Administrar la mesa de servicio y los incidentes	B		P			S	S			P	P					P	P					
DS9 Administrar la configuración	M		P	P	S				P							P	S			S		S
DS10 Administrar los problemas	M		P		S	S			P	S	S					P	P			S		
DS11 Administrar los datos	A		P	P	P				P										P			P
DS12 Administrar el ambiente físico	B			S	P			S	P											P	P	
DS13 Administrar las operaciones	B			P					P	S						P	P		S	S		
Monitorear y Evaluar																						
ME1 Monitorear y evaluar el desempeño de TI	A	S	S	S	S	P				S	P					P	P	S	S	S	S	S
ME2 Monitorear y evaluar el control interno	M		P		P						P					P	P	S	S	S	S	S
ME3 Garantizar el cumplimiento regulatorio	A	P			P				P	S	S										P	S
ME4 Proporcionar gobierno de TI	A	P	P	P	P	P	P	S		S	P					P	P	S	S	S	S	S

(P=Primario, S=Secondario).

[31] Fuente: COBIT 4.1, IT Governance Institute ITGT, www.itgi.org, 2007. Los derechos de autor de esta información le pertenecen al IT Governance Institute.

ANEXO C

INDICE DE ALINEAMIENTO DE LA RESOLUCION JB-2005-834 RESPECTO A COBIT 4.1

	OBJETIVO DE CONTROL	ID	ALINEAMIENTO RJB-2005-834 y COBIT4.1
Planear y Organizar	Definir un Plan Estratégico	P01	0.54
	Definir la Arquitectura de la Información.	P02	0.50
	Determinar la Dirección Tecnológica.	P03	0.50
	Definir los Procesos, Organización y Relaciones de TI	P04	0.43
	P05. Administrar la Inversión en TI.	P05	0.00
	Comunicar las Aspiraciones y la Dirección de la Gerencia	P06	0.65
	Administrar los Recursos Humanos de TI.	P07	0.53
	Administrar la Calidad.	P08	0.17
	P09. Evaluar y Administrar los Riesgos de TI	P09	0.67
	Administrar Proyectos.	P10	0.00
Adquirir e Implementar	Identificar Soluciones Automatizadas	AI1	0.00
	Adquirir y Mantener Software Aplicativo	AI2	0.28
	Adquirir y Mantener Infraestructura Tecnológica	AI3	0.38
	Facilitar la Operación y el Uso	AI4	0.63
	Adquirir Recursos de TI	AI5	0.56
	Administrar Cambios	AI6	0.20
	Instalar y Acreditar Soluciones y Cambios	AI7	0.11
Entregar y Soportar	Definir y Administrar los Niveles de Servicio	DS1	0.38
	Administrar los Servicios de Terceros	DS2	0.69
	Administrar el Desempeño y la Capacidad	DS3	0.60
	Garantizar la Continuidad del Servicio	DS4	0.93
	Garantizar la Seguridad de los Sistemas	DS5	0.57
	Identificar y Asignar Costos	DS6	0.00
	Educar y Entrenar a los Usuarios	DS7	0.42
	Administrar la Mesa de Servicio y los Incidentes	DS8	0.10
	Administrar la Configuración	DS9	0.25
	Administración de Problemas	DS10	0.13
	Administración de Datos	DS11	0.50
	Administración del Ambiente Físico	DS12	0.55
	Administración de Operaciones	DS13	0.40
Monitorear y Evaluar	Monitorear y Evaluar el Desempeño de TI	ME1	0.08
	Monitorear y Evaluar el Control Interno	ME2	0.50
	Garantizar el Cumplimiento con Requerimientos Externos	ME3	0.75
	Proporcionar Gobierno de TI	ME4	0.21

ANEXO D

ALINEAMIENTO DE CRITERIOS DE LA INFORMACION EN LA RESOLUCION JB-2005-834 RESPECTO A COBIT 4.1

DOMINIO	ID	INDICE DE ALINEAMIENTO	R834 -Efectividad	COBIT-Efectividad	R834-Eficiencia	COBIT-Eficiencia	R834-Confidencialidad	COBIT-Confidencialidad	R834-Integridad	COBIT-Integridad	R834-Disponibilidad	COBIT-Disponibilidad	R834-Cumplimiento	COBIT-Cumplimiento	R834-Confiabilidad	COBIT- Confiabilidad
Planear y Organizar	P01	0.54	0.5	1	0.3	0.5	0		0		0		0		0	
	P02	0.50	0.3	0.5	0.5	1	0.3	0.5	0.5	1	0		0		0	
	P03	0.50	0.5	1	0.5	1	0		0		0		0		0	
	P04	0.43	0.4	1	0.4	1	0		0		0		0		0	
	P05	0.00	0.0	1	0	1	0		0		0		0		0	0.5
	P06	0.65	0.7	1	0		0		0		0		0.3	0.5	0	
	P07	0.53	0.5	1	0.5	1	0		0		0		0		0	
	P08	0.17	0.2	1	0.2	1	0		0.1	0.5	0		0		0.1	0.5
	P09	0.67	0.3	0.5	0.3	0.5	0.7	1	0.7	1	0.7	1	0.3	0.5	0.3	0.5
	P10	0.00	0.0	1	0	1	0		0		0		0		0	
Adquirir e Implementar	AI1	0.00	0.0	1	0	0.5	0		0		0		0		0	
	AI2	0.28	0.3	1	0.3	1	0		0.1	0.5	0		0		0.1	0.5
	AI3	0.38	0.2	0.5	0.4	1	0		0.2	0.5	0.2	0.5	0		0	
	AI4	0.63	0.6	1	0.6	1	0		0.3	0.5	0.3	0.5	0.3	0.5	0.3	0.5
	AI5	0.56	0.3	0.5	0.6	1	0		0		0		0.3	0.5	0	
	AI6	0.2	0.2	1	0.2	1	0		0.2	1	0.2	1	0		0.1	0.5
	AI7	0.11	0.1	1	0.1	0.5	0		0.1	0.5	0.1	0.5	0		0	
Entregar y Soportar	DS1	0.38	0.4	1	0.4	1	0.2	0.5	0.2	0.5	0.2	0.5	0.2	0.5	0.2	0.5
	DS2	0.69	0.7	1	0.7	1	0.3	0.5	0.3	0.5	0.3	0.5	0.3	0.5	0.3	0.5
	DS3	0.60	0.6	1	0.6	1	0		0		0.3	0.5	0		0	
	DS4	0.93	0.9	1	0.5	0.5	0		0		0.9	1	0		0	
	DS5	0.57	0.0		0		0.6	1	0.6	1	0.3	0.5	0.3	0.5	0.3	0.5
	DS6	0.00	0.0		0	1	0		0		0		0		0	1
	DS7	0.42	0.4	1	0.2	0.5	0		0		0		0		0	
	DS8	0.10	0.1	1	0.1	1	0		0		0		0		0	
	DS9	0.25	0.3	1	0.1	0.5	0		0		0.1	0.5	0		0.1	0.5
	DS10	0.13	0.1	1	0.1	1	0		0		0.1	0.5	0		0	
	DS11	0.50	0.0		0		0		0.5	1	0		0		0.5	1
	DS12	0.55	0.0		0		0		0.6	1	0.6	1	0		0	
	DS13	0.40	0.4	1	0.4	1	0		0.2	0.5	0.2	0.5	0		0	
Monitorear y Evaluar	ME1	0.08	0.1	1	0.1	1	0	0.5	0	0.5	0	0.5	0	0.5	0	0.5
	ME2	0.50	0.5	1	0.5	1	0.3	0.5	0.3	0.5	0.3	0.5	0.3	0.5	0.3	0.5
	ME3	0.75	0.0		0		0		0		0		0.8	1	0.4	0.5
	ME4	0.21	0.2	1	0.2	1	0.1	0.5	0.1	0.5	0.1	0.5	0.1	0.5	0.1	0.5

ANEXO E

PROPUESTA DE MEJORAMIENTO RESPECTO A COBIT 4.1

	OBJETIVO DE CONTROL	ID.O.C.	IMPORTANCIA DEL PROCESO EN RTI	IA PROPUESTO PARA COBIT 4.1
Planear y Organizar	Definir un Plan Estratégico	P01	S	1.00
	Definir la Arquitectura de la Información.	P02	S	1.00
	Determinar la Dirección Tecnológica.	P03	S	1.00
	Definir los Procesos, Organización y Relaciones de TI.	P04	P	1.00
	P05. Administrar la Inversión en TI.	P05		0.00
	Comunicar las Aspiraciones y la Dirección de la Gerencia	P06	P	1.00
	Administrar los Recursos Humanos de TI.	P07	S	1.00
	Administrar la Calidad.	P08	S	1.00
	P09. Evaluar y Administrar los Riesgos de TI	P09	P	1.00
	Administrar Proyectos.	P10	S	1.00
Adquirir e Implementar	Identificar Soluciones Automatizadas	AI1	S	1.00
	Adquirir y Mantener Software Aplicativo	AI2	S	1.00
	Adquirir y Mantener Infraestructura Tecnológica	AI3		0.38
	Facilitar la Operación y el Uso	AI4	S	1.00
	Adquirir Recursos de TI	AI5		0.56
	Administrar Cambios	AI6		0.20
	Instalar y Acreditar Soluciones y Cambios	AI7	S	1.00
Entregar y Soportar	Definir y Administrar los Niveles de Servicio	DS1		0.38
	Administrar los Servicios de Terceros	DS2	P	1.00
	Administrar el Desempeño y la Capacidad	DS3	S	1.00
	Garantizar la Continuidad del Servicio	DS4	P	1.00
	Garantizar la Seguridad de los Sistemas	DS5	P	1.00
	Identificar y Asignar Costos	DS6		0.00
	Educar y Entrenar a los Usuarios	DS7	S	1.00
	Administrar la Mesa de Servicio y los Incidentes	DS8		0.10
	Administrar la Configuración	DS9	S	1.00
	Administración de Problemas	DS10	S	1.00
	Administración de Datos	DS11	P	1.00
	Administración del Ambiente Físico	DS12	P	1.00
	Administración de Operaciones	DS13		0.40
Monitorear y Evaluar	Monitorear y Evaluar el Desempeño de TI	ME1	S	1.00
	Monitorear y Evaluar el Control Interno	ME2	P	1.00
	Garantizar el Cumplimiento con Requerimientos Externos	ME3	P	1.00
	Proporcionar Gobierno de TI	ME4	P	1.00

P: Importancia Primaria del proceso respecto a la Administración de RTI.
S: Importancia Secundaria del proceso respecto a la Administración de RTI.
IA: Índice de Alineamiento

ANEXO F

IMPORTANCIA DE LOS CRITERIOS DE INFORMACION EN ISO 27002:2005

	OBJETIVO DE CONTROL	ID	Efectividad	Eficiencia	Confidencialidad	Integridad	Disponibilidad	Cumplimiento	Confiabilidad
A5	**Politica de seguridad**								
A.5.1	Politica de seguridad de informacion	PS1	1	0.5					
A.6	**Organización de la seguridad de la informacion**								
A.6.1	Organización interna	OS1	1	0.5	1		1	0.5	1
A.6.2	Entidades externas	OS2			1			0.5	1
A.7	**Gestion de activos**								
A.7.1	Responsabilidad por los activos	GA1		1	1		1		
A.7.2	Clasificacion de la informacion	GA2			1			1	
A.8	**Seguridad de los recursos humanos**								
A.8.1	Antes del empleo	RH1			1			1	
A.8.2	Durante el empleo	RH2	1					1	
A.8.3	Terminacion o cambio de empleo	RH3		1	1			1	
A9	**Seguridad fisica y ambiental**								
A.9.1	Areas seguras	SF1			1	0.5	0.5		
A.9.2	Seguridad del equipo	SF2			1	0.5	0.5		
A.10	**Gestion de comunicaciones y operaciones**								
A.10.1	Operaciones y responsabilidades operativas	CO1			0.5	1	0.5		
A.10.2	Administracion de entrega de servicios a terceros	CO2	0.5			1	1		0.5
A.10.3	Planeación y aprobacion del sistema	CO3				1	1		
A.10.4	Proteccion contra software malicioso	CO4		0.5	1	0.5	1		
A.10.5	Respaldo (back-up)	CO5	0.5		1	1	1		
A.10.6	Gestión de seguridad de redes	CO6			1	1	1	0.5	
A.10.7	Gestión de medios	CO7			1	1	1		
A.10.8	Intercambio de información	CO8			1			0.5	
A.10.9	Servicios de comercio electronico	CO9			0.5	1		0.5	
A.10.10	Monitoreo	CO10						1	
A11	**Control de acceso**								
A.11.1	Requerimientos del negocio para el control de acceso	CA1			1	0.5	0.5		
A.11.2	Gestión de acceso del usuario	CA2	0.5		1				
A.11.3	Responsabilidades del usuario	CA3			1				
A.11.4	Control de acceso a redes	CA4			1	0.5			
A.11.5	Control del acceso al sistema operativo	CA5			1				
A.11.6	Aplicación e información del control de acceso	CA6			1				
A.11.7	Computación móvil y tele-trabajo	CA7	1		1	0.5			

1: Importancia Primaria (P) *
0: Importancia Secundaria (S) *

* Información estimada por el autor de este documento en base a la descripción de cada uno de los objetivos de control detallada en el estándar ISO 27002:2005.

Continuación del Anexo F.

	OBJETIVO DE CONTROL	ID	Efectividad	Eficiencia	Confidencialidad	Integridad	Disponibilidad	Cumplimiento	Confiabilidad
A12	**Adquisición, desarrollo y mantenimiento de sistemas**								
A12.1	Requerimientos de seguridad de los sistemas	AD1		1	1	0.5	0.5		
A12.2	Procesamiento correcto en las aplicaciones	AD2		1		1	1		
A12.3	Controles criptográficos	AD3			1	1			
A.12.4	Seguridad de los archivos del sistema	AD4			1	0.5	0.5		0.5
A.12.5	Seguridad en los procesos de desarrollo y soporte	AD5			1	1	1		0.5
A.12.6	Gestión de vulnerabilidad técnica	AD6			1	1	1		
A.13	**Gestión de incidentes en la seguridad de información**								
A.13.1	Reporte de eventos y debilidades en la seguridad de información	GI1	0.5		1			0.5	
A.13.2	Reporte de incidentes y mejoras en la seguridad de informacion	GI2	0.5		1	1	0	1	
A14	**Gestión de continuidad comercial**								
A.14.1	Aspectos de la seguridad de informacion de la gestion de la continuidad comercial	GC1	1	1			1		1
A15	**Cumplimiento**								
A.15.1	Cumplimiento con requisitos legales	CM1		1	1		0.5	1	0.5
A.15.2	Cumplimiento con las políticas y estandares de seguridad y el cumplimiento tecnico	CM2	0.5		0.5	0.5	0.5	1	
A.15.3	Consideraciones de auditoria de los sistemas de información	CM3			1		1	1	0.5

ANEXO G

INDICE DE DE LA RESOLUCION JB-2005-834 RESPECTO A ISO 27002:2005

	OBJETIVO DE CONTROL	ID	ALINEAMIENTO RJB-2005-834 e ISO27002:2005
A5	**Politica de seguridad**		
A.5.1	Politica de seguridad de informacion	PS1	0.50
A.6	**Organización de la seguridad de la informacion**		
A.6.1	Organización interna	OS1	0.34
A.6.2	Entidades externas	OS2	0.83
A.7	**Gestion de activos**		
A.7.1	Responsabilidad por los activos	GA1	0.58
A.7.2	Clasificacion de la informacion	GA2	0.50
A.8	**Seguridad de los recursos humanos**		
A.8.1	Antes del empleo	RH1	0.67
A.8.2	Durante el empleo	RH2	0.00
A.8.3	Terminacion o cambio de empleo	RH3	0.58
A9	**Seguridad fisica y ambiental**		
A.9.1	Areas seguras	SF1	0.50
A.9.2	Seguridad del equipo	SF2	0.54
A.10	**Gestion de comunicaciones y operaciones**		
A.10.1	Operaciones y responsabilidades operativas	CO1	0.75
A.10.2	Administracion de entrega de servicios a terceros	CO2	0.58
A.10.3	Planeación y aprobacion del sistema	CO3	0.38
A.10.4	Proteccion contra software malicioso	CO4	0.63
A.10.5	Respaldo (back-up)	CO5	1.00
A.10.6	Gestión de seguridad de redes	CO6	0.25
A.10.7	Gestión de medios	CO7	0.56
A.10.8	Intercambio de información	CO8	0.45
A.10.9	Servicios de comercio electronico	CO9	0.67
A.10.10	Monitoreo	CO10	0.67
A11	**Control de acceso**		
A.11.1	Requerimientos del negocio para el control de acceso	CA1	0.25
A.11.2	Gestión de acceso del usuario	CA2	0.56
A.11.3	Responsabilidades del usuario	CA3	0.17
A.11.4	Control de acceso a redes	CA4	0.21
A.11.5	Control del acceso al sistema operativo	CA5	0.33
A.11.6	Aplicación e información del control de acceso	CA6	0.50
A.11.7	Computación móvil y tele-trabajo	CA7	0.00

Continuación del Anexo G.

	OBJETIVO DE CONTROL	ID	ALINEAMIENTO RJB-2005-834 e ISO27002:2005
A12	**Adquisición, desarrollo y mantenimiento de sistemas**		
A12.1	Requerimientos de seguridad de los sistemas	AD1	0.00
A12.2	Procesamiento correcto en las aplicaciones	AD2	0.13
A12.3	Controles criptográficos	AD3	0.38
A.12.4	Seguridad de los archivos del sistema	AD4	0.17
A.12.5	Seguridad en los procesos de desarrollo y soporte	AD5	0.50
A.12.6	Gestión de vulnerabilidad técnica	AD6	0.00
A.13	**Gestión de incidentes en la seguridad de información**		
A.13.1	Reporte de eventos y debilidades en la seguridad de información	GI1	0.75
A.13.2	Reporte de incidentes y mejoras en la seguridad de informacion	GI2	0.42
A14	**Gestión de continuidad comercial**		
A.14.1	Aspectos de la seguridad de informacion de la gestion de la continuidad comercial	GC1	1.00
A15	**Cumplimiento**		
A.15.1	Cumplimiento con requisitos legales	CM1	0.33
A.15.2	Cumplimiento con las políticas y estandares de seguridad y el cumplimiento tecnico	CM2	0.75
A.15.3	Consideraciones de auditoria de los sistemas de información	CM3	0.25

ANEXO H

ALINEAMIENTO DE CRITERIOS DE LA INFORMACION EN LA RESOLUCION JB-2005-834 RESPECTO A ISO 27002:2005

ID	ALINEAMIENTO ISO27002 - R834	R834 -Efectividad		ISO-Efectividad		R834-Eficiencia		ISO-Eficiencia		R834-Confidencialidad		ISO-Confidencialidad		R834-Integridad		ISO-Integridad		R834-Disponibilidad		ISO-Disponibilidad		R834-Cumplimiento		ISO-Cumplimiento		R834-Confiabilidad		ISO- Confiabilidad	
PS1	0.50	0.50	1			0.25	0.5			0				0				0				0				0			
		0.00				0				0				0				0				0				0			
OS1	0.34	0.34	1			0.17	0.5			0.34	1			0				0.34	1			0.2	0.5			0.3	1		
OS2	0.83	0.00				0				0.83	1			0				0				0.4	0.5			0.8	1		
		0.00				0				0				0				0				0				0			
GA1	0.58	0.00				0.58	1			0.58	1			0				0.58	1			0				0			
GA2	0.50	0.00				0				0.5	1			0				0				0.5	1			0			
		0.00				0				0				0				0				0				0			
RH1	0.67	0.00				0				0.67	1			0				0				0.7	1			0			
RH2	0.00	0.00	1			0				0				0				0				0	1			0			
RH3	0.58	0.00				0.58	1			0.58	1			0				0				0.6	1			0			
		0.00				0				0				0				0				0				0			
SF1	0.50	0.00				0				0.5	1			0.25	0.5			0.25	0.5			0				0			
SF2	0.54	0.00				0				0.54	1			0.27	0.5			0.27	0.5			0				0			
		0.00				0				0				0				0				0				0			
CO1	0.75	0.00				0				0.38	0.5			0.75	1			0.38	0.5			0				0			
CO2	0.58	0.29	0.5			0				0				0.58	1			0.58	1			0				0.3	0.5		
CO3	0.38	0.00				0				0				0.38	1			0.38	1			0				0			
CO4	0.63	0.00				0.31	0.5			0.63	1			0.31	0.5			0.63	1			0				0			
CO5	1.00	0.50	0.5			0				1	1			1	1			1	1			0				0			
CO6	0.25	0.00				0				0.25	1			0.25	1			0.25	1			0.1	0.5			0			
CO7	0.56	0.00				0				0.56	1			0.56	1			0.56	1			0				0			
CO8	0.45	0.00				0				0.45	1			0				0				0.2	0.5			0			
CO9	0.67	0.00				0				0.33	0.5			0.67	1			0				0.3	0.5			0			
CO10	0.67	0.00				0				0				0				0				0.7	1			0			
		0.00				0				0				0				0				0				0			
CA1	0.25	0.00				0				0.25	1			0.13	0.5			0.13	0.5			0				0			
CA2	0.56	0.28	0.5			0				0.56	1			0				0				0				0			
CA3	0.17	0.00				0				0.17	1			0				0				0				0			
CA4	0.21	0.00				0				0.21	1			0.11	0.5			0				0				0			
CA5	0.33	0.00				0				0.33	1			0				0				0				0			
CA6	0.50	0.00				0				0.5	1			0				0				0				0			
CA7	0.00	0.00	1			0				0	1			0	0.5			0				0				0			

Continuación del Anexo H.

ID	ALINEAMIENTO ISO27002 - R834	R834 -Efectividad		ISO-Efectividad		R834-Eficiencia		ISO-Eficiencia		R834-Confidencialidad		ISO-Confidencialidad		R834-Integridad		ISO-Integridad		R834-Disponibilidad		ISO-Disponibilidad		R834-Cumplimiento		ISO-Cumplimiento		R834-Confiabilidad		ISO- Confiabilidad	
		0.00				0				0				0				0				0				0			
AD1	0.00	0.00				0		1		0		1		0		0.5		0		0.5		0				0			
AD2	0.13	0.00				0.13		1		0				0.13		1		0.13		1		0				0			
AD3	0.38	0.00				0				0.38		1		0.38		1		0				0				0			
AD4	0.17	0.00				0				0.17		1		0.08		0.5		0.08		0.5		0				0.1		0.5	
AD5	0.50	0.00				0				0.5		1		0.5		1		0.5		1		0				0.3		0.5	
AD6	0.00	0.00				0				0		1		0		1		0		1		0				0			
		0.00				0				0				0				0				0				0			
GI1	0.75	0.38		0.5		0				0.75		1		0				0				0.4		0.5		0			
GI2	0.42	0.21		0.5		0				0.42		1		0.42		1		0		0		0.4		1		0			
		0.00				0				0				0				0				0				0			
GC1	1	1.00		1		1		1		0				0				1		1		0				1		1	
		0.00				0				0				0				0				0				0			
CM1	0.33	0.00				0.33		1		0.33		1		0				0.17		0.5		0.3		1		0.2		0.5	
CM2	0.75	0.38		0.5		0				0.38		0.5		0.38		0.5		0.38		0.5		0				0			
CM3	0.25	0.00				0				0.25		1		0				0.25		1		0.3		1		0.1		0.5	

ANEXO I

ALINEAMIENTO DE CRITERIOS DE LA INFORMACION EN LA RESOLUCION JB-2005-834 RESPECTO A ISO 27002:2005

No	OBJETIVO DE CONTROL	ID	Confidencialidad	Integridad	Disponibilidad	Indice de Relevancia CID
A5	**Politica de seguridad**					
A.5.1	Politica de seguridad de informacion	PS1				0.00
A.6	**Organización de la seguridad de la informacion**					
A.6.1	Organización interna	OS1	1		1	0.67
A.6.2	Entidades externas	OS2	1			0.33
A.7	**Gestion de activos**					
A.7.1	Responsabilidad por los activos	GA1			1	0.33
A.7.2	Clasificacion de la informacion	GA2	1			0.33
A.8	**Seguridad de los recursos humanos**					
A.8.1	Antes del empleo	RH1	1			0.33
A.8.2	Durante el empleo	RH2				0.00
A.8.3	Terminacion o cambio de empleo	RH3	1			0.33
A9	**Seguridad fisica y ambiental**					
A.9.1	Areas seguras	SF1	1	0.5	0.5	0.67
A.9.2	Seguridad del equipo	SF2	1	0.5	0.5	0.67
A.10	**Gestion de comunicaciones y operaciones**					
A.10.1	Operaciones y responsabilidades operativas	CO1	0.5	1	0.5	0.67
A.10.2	Administracion de entrega de servicios a terceros	CO2		1	1	0.67
A.10.3	Planeación y aprobacion del sistema	CO3		1	1	0.67
A.10.4	Proteccion contra software malicioso	CO4	1	0.5	1	0.83
A.10.5	Respaldo (back-up)	CO5	1	1	1	1.00
A.10.6	Gestión de seguridad de redes	CO6	1	1	1	1.00
A.10.7	Gestión de medios	CO7	1	1	1	1.00
A.10.8	Intercambio de información	CO8	1			0.33
A.10.9	Servicios de comercio electronico	CO9	0.5	1		0.50
A.10.10	Monitoreo	CO10				0.00
A11	**Control de acceso**					
A.11.1	Requerimientos del negocio para el control de acceso	CA1	1	0.5	0.5	0.67
A.11.2	Gestión de acceso del usuario	CA2	1			0.33
A.11.3	Responsabilidades del usuario	CA3	1			0.33
A.11.4	Control de acceso a redes	CA4	1	0.5		0.50
A.11.5	Control del acceso al sistema operativo	CA5	1			0.33
A.11.6	Aplicación e información del control de acceso	CA6	1			0.33
A.11.7	Computación móvil y tele-trabajo	CA7	1	0.5		0.50

Continuación del Anexo I.

No	OBJETIVO DE CONTROL	ID	Confidencialidad	Integridad	Disponibilidad	Indice de Relevancia CID
A12	**Adquisición, desarrollo y mantenimiento de sistemas**					
A12.1	Requerimientos de seguridad de los sistemas	AD1	1	0.5	0.5	0.67
A12.2	Procesamiento correcto en las aplicaciones	AD2		1	1	0.67
A12.3	Controles criptográficos	AD3	1	1		0.67
A.12.4	Seguridad de los archivos del sistema	AD4	1	0.5	0.5	0.67
A.12.5	Seguridad en los procesos de desarrollo y soporte	AD5	1	1	1	1.00
A.12.6	Gestión de vulnerabilidad técnica	AD6	1	1	1	1.00
A.13	**Gestión de incidentes en la seguridad de información**					
A.13.1	Reporte de eventos y debilidades en la seguridad de información	GI1	1			0.33
A.13.2	Reporte de incidentes y mejoras en la seguridad de informacion	GI2	1	1	0	0.67
A14	**Gestión de continuidad comercial**					
A.14.1	Aspectos de la seguridad de informacion de la gestion de la continuidad comercial	GC1			1	0.33
A15	**Cumplimiento**					
A.15.1	Cumplimiento con requisitos legales	CM1	1		0.5	0.50
A.15.2	Cumplimiento con las políticas y estandares de seguridad y el cumplimiento tecnico	CM2	0.5	0.5	0.5	0.50
A.15.3	Consideraciones de auditoria de los sistemas de información	CM3	1		1	0.67

ANEXO J

PROPUESTA DE MEJORAMIENTO RESPECTO A ISO 27002:2005

DOM	OBJETIVO DE CONTROL	ID	ALINEAMIENTO RJB-2005-834 e ISO27002	PROPUESTA RESPECTO ISO27002	JUSTIFICACION
A.5.1	Politica de seguridad de informacion	PS1	0.50	1.00	IA Medio
A.6.1	Organización interna	OS1	0.34	1.00	IA Bajo / IR Alto
A.6.2	Entidades externas	OS2	0.83	0.83	Permanece
A.7.1	Responsabilidad por los activos	GA1	0.58	1.00	IR Alto
A.7.2	Clasificacion de la informacion	GA2	0.50	1.00	IA Medio
A.8.1	Antes del empleo	RH1	0.67	1.00	Esfuerzo Bajo
A.8.2	Durante el empleo	RH2	0.00	1.00	IA Bajo
A.8.3	Terminacion o cambio de empleo	RH3	0.58	1.00	Esfuerzo bajo
A.9.1	Areas seguras	SF1	0.50	1.00	IR Alto
A.9.2	Seguridad del equipo	SF2	0.54	1.00	IR Alto
A.10.1	Operaciones y responsabilidades operativas	CO1	0.75	1.00	IR Alto
A.10.2	Administracion de entrega de servicios a terceros	CO2	0.58	1.00	IR Alto
A.10.3	Planeación y aprobacion del sistema	CO3	0.38	1.00	IA Bajo / IR Alto
A.10.4	Proteccion contra software malicioso	CO4	0.63	1.00	IR Alto
A.10.5	Respaldo (back-up)	CO5	1.00	1.00	IR Alto
A.10.6	Gestión de seguridad de redes	CO6	0.25	1.00	IA Bajo / IR Alto
A.10.7	Gestión de medios	CO7	0.56	1.00	IR Alto
A.10.8	Intercambio de información	CO8	0.45	1.00	IA Bajo
A.10.9	Servicios de comercio electronico	CO9	0.67	1.00	IR Alto
A.10.10	Monitoreo	CO10	0.67	0.67	Permanece
A.11.1	Requerimientos del negocio para el control de acceso	CA1	0.25	1.00	IA Bajo / IR Alto
A.11.2	Gestión de acceso del usuario	CA2	0.56	0.56	Permanece
A.11.3	Responsabilidades del usuario	CA3	0.17	1.00	IA Bajo
A.11.4	Control de acceso a redes	CA4	0.21	1.00	IA Bajo / IR Alto
A.11.5	Control del acceso al sistema operativo	CA5	0.33	0.75	IA Bajo
A.11.6	Aplicación e información del control de acceso	CA6	0.50	1.00	IR Medio
A.11.7	Computación móvil y tele-trabajo	CA7	0.00	1.00	IA Bajo / IR Alto
A12.1	Requerimientos de seguridad de los sistemas	AD1	0.00	1.00	IA Bajo / IR Alto
A12.2	Procesamiento correcto en las aplicaciones	AD2	0.13	1.00	IA Bajo / IR Alto
A12.3	Controles criptográficos	AD3	0.38	1.00	IA Bajo / IR Alto
A.12.4	Seguridad de los archivos del sistema	AD4	0.17	1.00	IA Bajo / IR Alto
A.12.5	Seguridad en los procesos de desarrollo y soporte	AD5	0.50	0.75	IR Alto
A.12.6	Gestión de vulnerabilidad técnica	AD6	0.00	1.00	IA Bajo / IR Alto
A.13.1	Reporte de eventos y debilidades en la seguridad	GI1	0.75	0.75	Permanece
A.13.2	Reporte de incidentes y mejoras en la seguridad de informacion	GI2	0.42	1.00	IA Bajo / IR Alto
A.14.1	Continuidad comercial	GC1	1.00	1.00	Alineamiento completo
A.15.1	Cumplimiento con requisitos legales	CM1	0.33	0.75	IA Bajo / IR Alto
A.15.2	Cumplimiento con las políticas y estandares Seg.	CM2	0.75	1.00	IR Alto
A.15.3	Consideraciones de auditoria de los sistemas	CM3	0.25	1.00	IA Bajo / IR Alto

ANEXO K

K1. ESTIMACION DEL ALINEAMIENTO EN PO1

El Anexo K en este documento contiene únicamente el registro de 4 procesos de COBIT. El detalle completo se encuentra en medio óptico (CD) en el archivo electrónico "Anexo K- Regulacion de RTI en el Ambito Financiero Ecuatoriano.xls"

P01 Definir un Plan Estratégico					
ID	**OBJETIVO DE CONTROL**	**ELEMENTOS CLAVE EN COBIT**	**RESOLUCIÓN JB-2005-834**	**IA**	**CC**
PO 1.1	Administración del Valor de TI	Caso de negocio Asignación de fondos Realización de beneficios Evaluación del caso de negocio	No considerado	0.00	N
PO 1.2	Alineación de TI con el Negocio	Alineación con la estrategia de negocio Participación bidireccional y recíproca en la planificación de la estrategia	Administración de TI 4.3.1.2 Plan funcional y operativo Art 15.2 Identificación procesos críticos	0.75	P
PO 1.3	Evaluación del Desempeño y la Capacidad Actual	Linea de base del desempeño actual Valoración de la contribución de los negocios, funcionalidad, estabilidad, complejidad, costos, fortalezas y debilidades.	4.1 Definición de procesos 4.1.3 Procesos habilitantes, de soporte o apoyo 4.3.4 Administración de seguridad 4.3.4.11 Desempeño del sistema de administración de la seguridad	1.00	C
PO 1.4	Plan Estratégico de TI	Definición de metas de TI Contribución a los objetivos de la empresa, financiación, fuente y estrategia de adquisición. Requerimientos legales o regulatorios	4.3.1.2 Plan funcional y operativo Alineación estratégica Actividades de corto plazo para el logro de objetivos 9.5 Cumplimiento legal y normativo	1.00	C
PO 1.5	Planes Tácticos de TI	Iniciativas IT Requerimientos de recursos Monitoreo y administración del logro de objetivos.	4.3.1.2 Plan funcional y operativo Planes tácticos no mencionados Falta monitoreo de uso de recursos y logro de beneficios	0.50	P
PO 1.6	Administración del Portafolio de TI	Programas de inversión de TI Definición, priorización y administración de programas (proyectos). Clarificación de resultados y alcance del esfuerzo. Asignación de rendición de cuentas. Asignación de recursos y financiación.	No considerado	0.00	N
Número de Objetivos de Control Cubiertos				3.25	2C
Número de Objetivos de Control Requeridos				6	2P
Cumplimiento R-JB-2005-834 respecto a COBIT 4.1				**0.54**	2N

C: Alineamiento Completo
P: Alineamiento Parcial
N: Control No considerado

IA: Índice de Alineamiento
CC: Calificación Cualitativa

K2. ESTIMACION DEL ALINEAMIENTO EN PO2

P02. Definir la Arquitectura de la Información					
ID	**OBJETIVO DE CONTROL**	**ELEMENTOS CLAVE EN COBIT**	**RESOLUCIÓN JB-2005-834**	**IA**	**CC**
PO 2.1	Modelo de Arquitectura de Información Empresarial	Análisis de las decisiones de apoyo Modelo de arquitectura de información mantenido. Modelo de datos corporativos	No se considera Se exige BDD con información relativa al riesgo.	0.0	N
PO 2.2	Diccionario de Datos Empresarial y Reglas de Sintaxis de Datos	Diccionario de datos corporativos Entendimiento comun de los datos	No se considera	0.0	N
PO 2.3	Esquema de Clasificación de Datos	Clases de información Propietarios Retención Reglas de acceso Niveles de seguridad para cada clase de información	Está expresado en terminos generales con ciertos detalles aunque no con todos. 4.3.2.2 Procedimiento de clasificación y control de activos de TI. Art.11 Registrar, ordenar, clasificar, disponer información de RO. 4.3.1.4 Responsabilidad de Información.	1.0	C
PO 2.4	Administración de Integridad	Integridad y consistencia de datos	4.3.3.1. Requerimientos contractuales que soporten integrifad información 4.3.4.3 Controles de integridad de la información administrada 4.3.6.4 Controles de integridad de la información sujeta a migración	1.0	C
Número de Objetivos de Control Cubiertos				2.00	2C
Número de Objetivos de Control Requeridos				4	0P
Cumplimiento R-JB-2005-834 respecto a COBIT 4.1				**0.50**	2N

K3. ESTIMACION DEL ALINEAMIENTO EN PO3

P03. Determinar la Dirección Tecnológica					
ID	**OBJETIVO DE CONTROL**	**ELEMENTOS CLAVE EN COBIT**	**RESOLUCIÓN JB-2005-834**	**IA**	**CC**
PO 3.1	Planeación de la Dirección Tecnológica	Analizar recnologías existentes y emergentes Habilitación de la estrategia de TI Arquitectura de sistemas Dirección tecnológica Estrategias de migración Contingencia de componentes de infrestructura	No se considera análisis de nuevas tecnologías 4.3 Tecnología de información 4.3.1.2 Plan funcional de tecnología de información 4.3.6.4 Estrategia de migración 4.3 Tecnología de información 4.4 Eventos externos ART 10, 15 y 16. (planes de contingencia)	0.75	N
PO 3.2	Plan de Infraestructura Tecnológica	Plan de infraestructura tecnológica Dirección de la adquisición Economía de escala Interoperatividad de plataformas	4.3.1.2 Plan funcional de tecnología de información	0.25	P
PO 3.3	Monitoreo de Tendencias y Regulaciones Futuras	Sector de negocios, industria, tecnología, infraestructura, tendencias legales y regulatorias.	No se menciona tendencias tecnológicas ART.9 Exposición al riesgo legal y normativo 9.5 Cumplimiento legal y normativo	0.75	N
PO 3.4	Estándares Tecnológicos	Foro tecnológico Estándares y lineamientos para productos	Foro no considerado 4.3.1.5 Políticas, Procesos y Procedimientos	0.75	N
PO 3.5	Consejo de Arquitectura de TI	Lineamientos y estándares de arquitectura de tecnología.	No considerado	0.00	P
Número de Objetivos de Control Cubiertos				2.50	3N
Número de Objetivos de Control Requeridos				5.00	2P
Cumplimiento R-JB-2005-834 respecto a COBIT 4.1				**0.50**	0C

K4. ESTIMACION DEL ALINEAMIENTO EN PO4

ID	OBJETIVO DE CONTROL	ELEMENTOS CLAVE EN COBIT	RESOLUCIÓN JB-2005-834	IA	CC
PO 4.1	Marco de Trabajo de Procesos de TI	Ejecución del plan estratégico de TI Medición del desempeño, mejoras y cumplimiento. Integración con Calidad y Control Interno	4.3.1.2 Plan funcional y operativo 4.1.3 Procesos habilitantes, de soporte o apoyo a Procesos productivos, fundamentales u operativos	1.00	C
PO 4.2	Comité Estratégico de TI	Nivel de consejo Gobierno de TI adecuado Asesoría sobre dirección estratégica	ART.18 Comité de administración integral de Riesgos.	0.25	P
PO 4.3	Comité Directivo de TI	Prioridades de programas de inversión de TI alineadas a estrategia y prioridades de negocio. Seguimiento a proyectos, SLAs	No considerado	0.00	N
PO 4.4	Ubicación Organizacional de la Función de TI	Importancia de TI en la empresa Linea de reporte del CIO	No considerado	0.00	N
PO 4.5	Estructura Organizacional	Estructura conforme a las necesidades de negocio. Revisar periódicamente la estructura, satisfacer objetivos y cambios.	No considerado Se exige que existan procesos relacionados	0.00	N
PO 4.6	Establecimiento de Roles y Responsabilidades	Definición y comunicación Rendición de cuentas	4.2.2. Los procesos de permanencia SECCIÓN V.- RESPONSABILIDADES EN LA ADMINISTRACIÓN DEL RO	1.00	C
PO 4.7	Responsabilidad de Aseguramiento de Calidad de TI	Asignar la función de QA Proporcionar sistemas de QA Tamaño del grupo QA	4.1.2. Procesos productivos, fundamentales u operativo Practicamente ausente	0.25	P
PO 4.8	Responsabilidad sobre el Riesgo, la Seguridad y el Cumplimiento	Responsabilidad de los riesgos de TI Nivel superior apropiado Roles críticos para administrar los riesgos de TI Responsabilidad específica de la seguridad de la información Seguridad física Apetito de riesgo de TI	ART.17. Responsabilidades de la administración del RO ART.18. Responsabilidades del comité de administración integral de riesgos ART.19. Responsabilidades de la unidad de riesgos. ART.9 Perfil de riesgos de la institución. ART.10 Decisión sobre tratamiento del riesgo: asumir, compartir, evitar, transferir..	1.00	C
PO 4.9	Propiedad de Datos y de Sistemas	Procedimientos y herramientas para enfrentar responsabilidades de propiedad de datos y sistemas de información. Decisiones sobre la clasificación de la información	4.3.1.4. Responsabilidad de Información 4.3.2.2. Procedimiento de clasificación y control de activos de TI No mencionan herramientas	0.75	P
PO 4.10	Supervisión	Garantizar el ejercicio de roles y responsabilidades. Evaluación de la suficiente autoridad y recursos para ejecución de roles y responsabilidades Revisión de indicadores clave de desemp.	No considerado	0.00	N
PO 4.11	Segregación de Funciones	Reducir la posibilidad de que un solo individuo afecte un proceso crítico La gerencia asegura que el personal realice sólo las tareas autorizadas a su rol	4.3.4.5. Segregación de funciones	1.00	C
PO 4.12	Personal de TI	Número suficiente de recursos Cambios en negocios, operaciones y TI	4.2 Personas 19.2 Monitorear y evaluar los cambios significativos y la exposición a riesgos	0.75	P
PO 4.13	Personal Clave de TI	Evitar dependencia	No considerado	0.00	N
PO 3.14	Políticas y Procedimientos Personal Contr.	Asegurar cumplimiento de políticas	4.2.2. Los procesos de permanencia	0.50	P
PO 4.15	Relaciones	Enlace, comunicación entre TI y otros fuera de TI (ejecutivos, unidades de negocio..)	No considerado	0.00	N
Número de Objetivos de Control Cubiertos				6.50	4C
Número de Objetivos de Control Requeridos				15	5P
Cumplimiento R-JB-2005-834 respecto a COBIT 4.1				**0.43**	6N

ANEXO L

L1. ESTIMACION DEL ALINEAMIENTO EN GA1 (D.7.1)

El Anexo L en este documento contiene únicamente el registro de 4 objetivos de control de ISO 27002. El detalle completo se encuentra en medio óptico (CD) en el archivo electrónico “Anexo L- Regulacion de RTI en el Ambito Financiero Ecuatoriano.xls”

Responsabilidad por los Activos					
D.7.1	**Responsabilidad por los Activos**	**CONTROLES**	**RESOLUCIÓN NO. JB-2005-834**	**IA**	**CC**
D.7.1.1	Inventario de Activos	Se debieran identificar todos los activos y se debiera elaborar y mantener un inventario de todos los activos importantes.	4.3.2.2 Un procedimiento de clasificación y control de activos de tecnología de información, que considere por lo menos, su registro e identificación, así como los responsables de su uso y mantenimiento, especialmente de los más importantes;	1.00	C
D.7.1.2	Propiedad de los Activos	Toda la información y los activos asociados con los medios de procesamiento de información debieran ser propiedad de una parte designada de la organización.	4.3.3.1 Requerimientos contractuales convenidos que definan la propiedad de la información y de las aplicaciones; y, la responsabilidad de la empresa proveedora de la tecnología 4.3.2.2 Un procedimiento de clasificación y control de activos de tecnología de información, que considere por lo menos, su registro e identificación, así como los responsables de su uso y mantenimiento..	0.75	P
D.7.1.3	Uso Aceptable de los Activos	Se debieran identificar, documentar e implementar reglas para el uso aceptable de la información y los activos asociados con los medios del procesamiento de la información	No considerado	0.00	N
Número de Objetivos de Control ConsiderDdos				1.75	1C
Número de Objetivos de Control Requeridos				3	1P
Cumplimiento R-JB-2005-834 respecto D ISO 27002				**0.58**	1N

L2. ESTIMACION DEL ALINEAMIENTO EN GA1 (D.7.2)

Clasificación de la información					
D.7.2		**CONTROLES**	**RESOLUCIÓN NO. JB-2005-834**	**CN**	**CC**
D.7.2.1	Lineamientos de clasificación	Definir y documentar los roles y responsabilidades de la seguridad de los empleados, contratistas y terceros en concordancia con la política de seguridad de la información de la organización	4.3.2.2 Un procedimiento de clasificación y control de activos de tecnología de información, que considere por lo menos, su registro e identificación, así como los responsables de su uso y mantenimiento, especialmente de los más importantes;	1.00	C
D.7.2.2	Etiquetado y manejo de la información	Desarrollar e implementar un conjunto de procedimientos para el etiquetado y manejo de la información en concordancia con el esquema de clasificación	No considerado	0.00	N
Número de Objetivos de Control ConsiderDdos				1.00	1C
Número de Objetivos de Control Requeridos				2	0P
Cumplimiento R-JB-2005-834 respecto D ISO 27002				**0.50**	1N

GLOSARIO DE TÉRMINOS

Actualización: Proceso consistente en reemplazar un sistema de uso actual por otro del mismo género y fabricante pero de distinta versión.

Activo: Datos, infraestructura, hardware, software, personal y su experiencia e información.

Análisis de Riesgo: Proceso mediante el cual se identifican las amenazas y las vulnerabilidades en una organización, se valora su impacto y la probabilidad de que ocurran.

Control: se define como las políticas, procedimientos, prácticas e infraestructuras organizativas, diseñadas para garantizar razonablemente, que los objetivos de negocio se llevarán a cabo, y que las incidencias no deseadas se pueden prevenir o detectar y corregir. (COSO 1992).

Datos personales: Son aquellos datos o información de carácter personal o íntimo, que son materia de protección en virtud de esta ley.

Fiduciario: dicho de un negocio o de un contrato: Basado principalmente en la confianza entre las partes.

Normas. Indican requisitos técnicos específicos, cubren detalles como, por ejemplo, los pasos a seguir para lograr alguna implementación, los conceptos del diseño de los sistemas, las especificaciones de las interfaces del software, los algoritmos y otros.

Objetivo de control de TI: se define como el propósito o resultado que se desea alcanzar, mediante la implantación de procedimientos de control para una actividad de TI específica.

Política de Seguridad: Las políticas representan declaraciones instruccionales de más alto nivel que las normas, aunque ambas son de obligatorio cumplimiento. Las políticas están diseñadas para durar hasta cinco años, mientras que las normas sólo unos pocos.

Procedimientos: Dictan los pasos operativos específicos o los métodos manuales que los trabajadores deben emplear para lograr un objetivo dado.

Riesgo: Es la posibilidad de sufrir algún daño o pérdida.

Riesgo Operacional ó Riesgo operativo: se define como el riesgo de pérdida debido a la inadecuación o a fallos de los procesos, el personal y los sistemas internos o bien a causa de acontecimientos externos. Esta definición incluye el riesgo legal90, pero excluye el riesgo estratégico y el de reputación.

Sistemas Informáticos: Es todo dispositivo físico o lógico utilizado para crear, generar, enviar, recibir, procesar, comunicar o almacenar, de cualquier forma, mensajes de datos.

Sistema de información: Es todo dispositivo físico o lógico utilizado para crear, generar, enviar, recibir, procesar, comunicar o almacenar, de cualquier forma, mensajes de datos.

Sistema operacional: es un programa o conjunto de programas cuya función es la de administrar los recursos del sistema (Procesador, memoria, sistema de archivos, etc.).

Sarbanes-Oxley Act: es una ley de Estados Unidos publicada el 30 de julio de 2002, también conocida como el Acta de Reforma de la Contabilidad Pública de Empresas y de Protección al Inversionista ó SOX. Tiene el propósito de monitorear a las empresas que cotizan en bolsa, evitando que las acciones de las mismas sean alteradas de manera dudosa y por tanto evitar fraudes y riesgo de bancarrota.