ESCUELA POLITÉCNICA DEL EJÉRCITO

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

METODOLOGÍA DE EVALUACIÓN DEL RIESGO TECNOLÓGICO EN LAS INSTITUCIONES DEL SISTEMA FINANCIERO ECUATORIANO, UTILIZANDO COBIT 4.1

Previa a la obtención del Título de:

INGENIERO EN SISTEMAS E INFORMÁTICA

POR: KATALINA DEL ROCÍO CORONEL HOYOS

SANGOLQUÍ, OCTUBRE DE 2008

CERTIFICACIÓN

Certifico que el presente trabajo fue realizado en su totalidad por la Sra. KATALINA DEL ROCÍO CORONEL HOYOS, como requerimiento parcial a la obtención del título de INGENIERO EN SISTEMAS E INFORMÁTICA.

_____
Fecha

_____
ING. EDGAR HERMOSA

DEDICATORIA

A mi esposo e hijos, que han sido mi constante apoyo, fuente de renovadas fuerzas, y por quienes todo esfuerzo vale la pena; a mi padre cuyo respaldo y ejemplo han sido fundamentales en mi formación no solo académica sino también ética y moral; y a mi madre, a quien le hubiese llenado de satisfacción este nuevo logro.

Katalina Coronel Hoyos

AGRADECIMIENTOS

A mi Dios, que ha sabido guiarme y germinar en mí el conocimiento y el tiempo necesario para dar curso a este trabajo, a mi esposo por su tenacidad y soporte en cada dilema surgido, a mis compañeros matemáticos y financieros que me dieron luces y opiniones oportunas en las definiciones planteadas, a Iván Velasteguí, Margarita Marín y todas las personas que me apoyaron en la implementación del plan piloto, y a mi director y codirectora de tesis, que con paciencia supieron darle forma a mis ideas.

Katalina Coronel Hoyos

METODOLOGÍA DE EVALUACIÓN DEL RIESGO TECNOLÓGICO PARA LAS INSTITUCIONES DEL SISTEMA FINANCIERO ECUATORIANO, UTILIZANDO COBIT 4.1

ÍNDICE DE CONTENIDOS

LISTADO DE FIGURAS Y TABLAS

METODOLOGÍA DE EVALUACIÓN DEL RIESGO TECNOLÓGICO PARA LAS INSTITUCIONES DEL SISTEMA FINANCIERO ECUATORIANO, UTILIZANDO COBIT 4.1

RESUMEN

La presente metodología es una propuesta de evaluación del riesgo tecnológico para las instituciones financieras controladas por la Superintendencia de Bancos y Seguros del Ecuador, utilizando una de las mejores prácticas en administración de la tecnología de información como lo es Cobit 4.1.

Una de las motivaciones que llevaron al desarrollo de este proyecto fue la de proveer una herramienta para que las instituciones financieras puedan realizar un auto-diagnóstico de su plataforma de tecnología de información para dar cumplimiento a lo dispuesto en la normativa de gestión de riesgo operativo en el factor de tecnología de información, cuyo plazo establece como límite el 31 de octubre del 2009 para las cooperativas y mutualistas, y el 31 de octubre del 2008 para el resto de instituciones financieras.

Por ello, la metodología de evaluación del riesgo tecnológico planteada incluye entre sus actividades la homologación de los objetivos de control de Cobit 4.1 a los requerimientos normativos del factor de tecnología de información establecidos en la norma de gestión de riesgo operativo vigente, para dar un

mayor peso en la calificación de riesgo obtenida, a aquellos procesos que son requeridos por la norma.

Adicionalmente, se utilizan los modelos de madurez, los conductores de valor, los conductores de riesgo, las pruebas de diseño de controles de Cobit 4.1, y la valoración del impacto en el negocio, para la evaluación de los procesos de tecnología de información. Con las calificaciones obtenidas se elabora un mapa de riesgo tecnológico ajustable al riesgo institucional que se ha concebido como la mayor o menor dependencia que tiene una empresa con respecto a su tecnología o automatización de los procesos de negocio.

Finalmente, se sugiere una estructura de elaboración de informe de evaluación que considere la utilización de los modelos de madurez para realizar las recomendaciones que permitan mitigar los riesgos detectados, lo que permitirá a la institución financiera ir madurando progresivamente sus procesos de tecnología de información hacia la consecución de un buen gobierno de TI.

CAPÍTULO 1: ANTECEDENTES Y JUSTIFICACIÓN

1.1 - Introducción

En un tiempo relativamente corto, las instituciones que se dedican al negocio bancario y financiero han ido evolucionando su tecnología de información, desde sistemas de información manuales hasta complejos sistemas expertos, predictivos y hasta basados en inteligencia artificial y redes neuronales, para dar soporte a sus procesos organizacionales contables, financieros, de mercadeo, de cartera, etc. y mejorar y optimizar las tomas de decisiones.

Sin embargo, las nuevas tendencias y mejores prácticas internacionales han cambiado el enfoque de la administración financiera tradicional hacia la administración basada en riesgos, haciendo que las plataformas tecnológicas se tengan que complementar con nuevas herramientas que faciliten la identificación, medición, control y monitoreo de los riesgos a los que las instituciones financieras se encuentran expuestas en la actualidad, con la finalidad de reducir la probabilidad de incurrir en pérdidas debido a riesgos, y de maximizar la solvencia y rentabilidad que permita proteger los intereses de sus clientes, sus accionistas y demás partes interesadas.

Es así que la normativa expedida por la Superintendencia de Bancos y Seguros del Ecuador, establece lineamientos mínimos prudenciales en torno al riesgo operativo, en el que considera a las personas, procesos, tecnología de

información y eventos externos como factores que deben ser administrados adecuadamente.

Concomitantemente, el IT Governance Institute (ITGI, por sus siglas en inglés) se estableció en 1998 para evolucionar el pensamiento y los estándares internacionales respecto a la dirección y control de la tecnología de información de una empresa. Un gobierno de TI efectivo, ayuda a garantizar que la tecnología de información soporte las metas del negocio, optimice la inversión del negocio en TI, y administre de forma adecuada los riesgos y oportunidades asociados a la TI, es decir, va de la mano con el objetivo de la normativa creada para la administración del riesgo operativo en lo referente a tecnología de información.

El ITGI diseñó y creó los Objetivos de Control para la Información y la Tecnología relacionada, denominados COBIT®, los cuales brindan buenas prácticas a través de un marco de trabajo de dominios y procesos, que integra varios estándares y mejores prácticas internacionales bajo un esquema estructurado y ordenado en la forma natural en que ocurren los procesos en la tecnología de información.

El presente trabajo pretende contribuir con una metodología que permita evaluar el nivel de cumplimiento normativo y de las metas del Gobierno de TI en las instituciones que integran el sistema financiero ecuatoriano, permitiéndoles aprovechar el marco de trabajo de control de COBIT versión 4.1 y su medición de logros, alineándose con las mejores prácticas y estándares internacionales que este marco de trabajo integra a nivel mundial.

De esta manera, espero aportar a la sociedad en forma positiva, para el crecimiento constante del país, con los conocimientos adquiridos en la carrera de Ingeniería en Sistemas, en la experiencia laboral y los que han permitido desarrollar el presente trabajo de tesis, y estimular a los futuros colegas a colaborar de similar manera con los sectores productivos que sostienen la economía de nuestra Patria.

1.2 - Antecedentes

En los años 70, el crecimiento de mercados financieros internacionales y el flujo de dinero entre países realzaron la falta de una supervisión bancaria efectiva a un nivel internacional. Las autoridades de supervisión bancaria básicamente regulaban bancos domésticos y las actividades domésticas de bancos internacionales, mientras que las actividades internacionales de estos bancos no eran siempre supervisadas de cerca. El colapso en 1974 del Bankhaus Herstatt en Alemania y del Franklin National Bank en Estados Unidos exhortó a los gobernantes de 10 bancos centrales a crear el Comité de Basilea para Supervisión Bancaria.

El Banco de Pagos Internacionales (BIS por sus siglas en inglés: Bank for International Settlements) es la institución financiera internacional más antigua del mundo y sigue siendo el centro principal para la cooperación de bancos centrales internacionales y la búsqueda de la estabilidad financiera y monetaria. Además,

da soporte al trabajo de los comités y organizaciones basados en Basilea, siendo un enlace de distribución de información estadística bancaria, de seguridades, tipos de cambio y mercados derivados.

En 1988 el Comité de Basilea emitió el Acuerdo de Capital de Basilea, introduciendo un marco de trabajo que se convirtió en un estándar globalmente aceptado. La mayoría de países en el mundo, incluido el Ecuador, adoptaron las recomendaciones emitidas por el BIS en el Acuerdo de 1988.

Una revisión de este Acuerdo de Capital en el 2004, conocido como Basilea II, incluyó en sus estándares el riesgo operativo. Tales estándares, que se están implementando a nivel mundial desde finales del año 2006, apuntan a lograr una mejor y más transparente medición de varios riesgos a los que se enfrentan las instituciones financieras, limitando la posibilidad de contagio en caso de una crisis y fortaleciendo la infraestructura financiera global.

Concomitantemente con la emisión de dichas prácticas bancarias internacionales, el 20 de octubre del 2005 la Superintendencia de Bancos y Seguros del Ecuador (SBS) emitió la resolución No. JB-2005-834, en la que establece estándares mínimos prudenciales con el afán de propender a que las instituciones del sistema financiero cuenten con un sistema de administración del riesgo operativo que les permita identificar, medir, controlar / mitigar y monitorear los riesgos de manera que se fortalezca su seguridad y solidez, en orden a proteger los intereses del público.

Posteriormente la SBS, mediante la circular No. SBS-INIF-DNR-SRO-2006-1539 del 4 de abril del 2006, solicita a las instituciones financieras bajo su control que se dé cumplimiento a la resolución No. JB-2005-834 en lo referente a obtener un diagnóstico mediante un proceso de autoevaluación que refleje su situación actual en cada uno de los factores de la administración del riesgo operativo que son: personas, procesos, tecnología de información y eventos externos.

Debido a que la gestión del riesgo operativo es relativamente nueva, la mayoría de instituciones financieras, especialmente las que cuentan con menos recursos, no disponen de una metodología lógica, flexible y adaptada a las mejores prácticas internacionales, que les permita, no solo realizar el proceso de autoevaluación del grado de cumplimiento que ha tenido su avance en la implementación de la normativa vigente respecto al factor de tecnología de información de la administración del riesgo operativo, sino que además dicho cumplimiento regulatorio vaya de la mano con las adopción de prácticas de control de tecnología de información generalmente aceptadas.

Internacionalmente, el marco de trabajo de COBIT y todos los productos y publicaciones relacionados que emitió el ITGI, guía a las organizaciones en la implementación de un adecuado gobierno de TI que garantice el cumplimiento de los objetivos del negocio por medio del valor agregado que debe brindar la tecnología de información, la administración de los riesgos y recursos y la medición del desempeño. Además integra estándares internacionales generalmente aceptados como COSO, ITIL, ISO 9001, ISO 27002, AS/NZ 4360:

2004, etc., que lo convierten en un marco de trabajo completo y alineado con las mejores prácticas relativas a la tecnología de información.

El presente trabajo se orienta a buscar una solución para esta falencia, adoptando para ello las mejores prácticas que el marco de trabajo de COBIT 4.1 puede aportar en ese tema.

1.3 - Descripción de la situación actual

En la actualidad, las empresas desarrolladoras de software y las instituciones que generan sus propios sistemas han implementado desde básicos hasta avanzados sistemas informáticos que les permiten manejar la información financiera, contable, de clientes, de mercadeo, estadística, etc., pero carecen de herramientas que les permitan fortalecer procesos importantes de la tecnología de información como son: la planificación estratégica, relaciones con proveedores, seguridades, etc.

Además, las soluciones informáticas que en la actualidad pretenden facilitar los procesos de la administración integral de riesgos no contemplan la evaluación del grado de cumplimiento de las disposiciones legales emitidas en torno al riesgo tecnológico, ni brindan las métricas necesarias que permitan determinar el grado de madurez que cada organización ha alcanzado en torno a este tema.

Previo a emitir la resolución que establece los estándares mínimos prudenciales para la administración del riesgo operativo, la Superintendencia de

Bancos y Seguros consideró necesario que las instituciones financieras que están bajo su control respondan algunas preguntas a través de una encuesta que fue publicada el 11 de marzo del 2004, cuyos resultados evidenciaron la situación en la que se encontraban dichas instituciones respecto a la administración de este riesgo y de manera específica respecto a la tecnología de información.

La encuesta se dirigió a todas las entidades privadas y públicas del sistema financiero controladas por la SBS en aquel entonces, que sumaban:

- 24 bancos
- 33 cooperativas
- 11 sociedades financieras
- 6 mutualistas
- 7 entidades públicas

De los resultados obtenidos en la encuesta se concluyó que el manejo del riesgo operativo en cuanto a tecnología de información en las instituciones controladas por la SBS no tenía una dirección adecuada en todos los casos, por lo que el organismo de supervisión emitió la normativa que da los lineamientos básicos de control para prevenir que las instituciones bajo su vigilancia incurran en pérdidas por fallas en las personas, procesos, sistemas de información y eventos externos.

La resolución que rige la gestión de riesgo operativo estipula que dicha norma es aplicable a las instituciones financieras públicas y privadas, al Banco

Central del Ecuador, a las compañías de arrendamiento mercantil, a las compañías emisoras y administradoras de tarjetas de crédito y a las corporaciones de desarrollo de mercado secundario de hipotecas, cuyo control compete a la Superintendencia de Bancos y Seguros.

La cantidad de instituciones financieras controladas por la Superintendencia de Bancos y Seguros que deben dar cumplimiento a la norma de gestión de riesgo operativo, y específicamente en los temas relacionados con el factor de tecnología de información, se resume por tipo de institución en la tabla que se presenta a continuación:

Tabla 1.1: Número de instituciones controladas por la SBS

TIPOS DE INSTITUCIONES	No.
Instituciones Financieras Públicas	7
Bancos Privados Nacionales	24
Bancos Privados Extranjeros	2
Bancos Off Shore	3
Sociedades Financieras	10
Mutualistas	5
Cooperativas de Ahorro y Crédito	39
Emisora y Administradora de tarjetas de crédito	1
Compañía de titularización	1
Banco Central del Ecuador	1
TOTAL	**93**

Sin embargo, en el tema de tecnología de información, las mismas directrices podrían ser aplicables también a las instituciones que conforman el sistema de seguros privados y públicos, y en general, a cualquier empresa que desee evaluar el grado de avance que ha tenido su gestión en la reducción de pérdidas ocasionadas por fallas en sus sistemas y tecnología de información.

Actualmente, en el mercado de software existen herramientas financieras que incluyen módulos de administración de riesgos que consideran entre ellos el riesgo operativo; sin embargo la funcionalidad de dichos módulos se orientan a generar una base de datos de eventos de riesgo que facilita el posterior cálculo de pérdidas esperadas por los factores de riesgo que se hayan registrado en la base de datos, entre los que se presentan los riesgos relacionados con la tecnología de información y a partir de ellas determinar los niveles aceptables, marginales y altos de los factores de riesgo operativo evaluados, y otros indicadores de pérdida operacional y desempeño.

Otros tipos de software se enfocan puntualmente en el tema de seguridades físicas o informáticas tales como ataques de sistemas maliciosos, virus, spam, intrusión, seguridad de aplicaciones, etc., pero no ven a los procesos de tecnología de información como un todo dentro del área de Sistemas de las empresas, ya que la seguridad es solamente uno de ellos.

Por supuesto, existe una innumerable cantidad de empresas consultoras que guían a las empresas hacia una adecuada administración del riesgo operativo y sugieren metodologías que ayudan a identificar, controlar y monitorear dicho riesgo, basándose en las recomendaciones que ha efectuado Basilea II sobre el tema, la cual prevé a futuro el cálculo de patrimonio técnico y provisiones de acuerdo con el riesgo operativo de cada institución financiera.

Penosamente, se ha podido constatar en las publicaciones que se pueden obtener de Internet, que existen instituciones que han desarrollado planes y

proyectos de implementación del riesgo operativo en los que no se considera el riesgo tecnológico como un factor del riesgo operativo, y las actividades a desarrollar incluyen únicamente las personas, procesos y eventos externos, pese a que las disposiciones legales emitidas por la Superintendencia de Bancos y Seguros en torno a este tema sí lo hacen.

Hace falta entonces crear una cultura informática en la sociedad que conlleve a administrar el riesgo tecnológico de una manera integrada y paralela con los procesos de negocio de las empresas, que coadyuven a optimizar su gestión y faciliten el logro de las metas trazadas en beneficio de sus propietarios, funcionarios y clientes.

1.4 - Objetivos

Objetivo general

Desarrollar una metodología de evaluación del riesgo tecnológico para las instituciones financieras controladas por la Superintendencia de Bancos y Seguros del Ecuador, utilizando el marco de trabajo de Cobit 4.1.

Objetivos específicos

- ✓ Elaborar una metodología que permita obtener un valor cuantificable del grado de cumplimiento de cada uno de los aspectos asociados a la tecnología de información, requeridos por la norma de gestión del riesgo operativo.

- ✓ Determinar los requerimientos normativos de tecnología de información para las instituciones que están bajo el control de la Superintendencia de Bancos y Seguros, y establecer los objetivos de control de COBIT 4.1 que los satisfacen.

- ✓ Establecer el grado de madurez actual y objetivo de cada proceso de tecnología de información, de acuerdo con los modelos de madurez de COBIT.

- ✓ Desarrollar un soporte informático en Excel que facilite la aplicación de la presente metodología en los cálculos que se requiera realizar.

- ✓ Probar la eficiencia de la metodología obtenida y validar los resultados esperados, mediante la aplicación de este estudio en la evaluación del riesgo tecnológico de una institución controlada por la Superintendencia de Bancos y Seguros.

1.5 - Alcance

A diferencia de un proyecto de implementación de gobierno de TI en una organización, el presente trabajo se orienta a facilitar una herramienta de auto – diagnóstico del riesgo tecnológico, que permita a las instituciones que conforman el sistema financiero ecuatoriano, dar cumplimiento a lo dispuesto por la normativa de gestión del riesgo operativo en el factor de tecnología de información, emitida por la Superintendencia de Bancos y Seguros en la resolución No. JB-2005-834 del 20 de octubre del 2005, en cuya sección II "Factores del riesgo operativo", artículo 1, numeral 1.3 "Tecnología de

información", establece la obligatoriedad de que las instituciones bajo su control cuenten con políticas, procesos y procedimientos que aseguren una adecuada planificación y administración de la tecnología de información.

En este sentido, el alcance del presente proyecto se limita a considerar la evaluación del cumplimiento de los requerimientos normativos que se enmarcan dentro de lo dispuesto en la resolución No. JB-2005-834 emitida por la Superintendencia de Bancos y Seguros, y que se refieren a:

1. Planeación y estrategia de la tecnología de información
2. Cumplimiento de requerimientos operativos de la entidad
3. Relaciones con terceros
4. Administración de seguridad
5. Continuidad de las operaciones
6. Adquisición, desarrollo, implementación y mantenimiento de aplicaciones
7. Políticas y procedimientos que permitan la adecuada administración, monitoreo y documentación de las bases de datos, redes de datos, software de base y hardware

La metodología a desarrollar pretende obtener una serie de pasos que permitan a una institución financiera determinar el nivel de cumplimiento de la norma de gestión de riesgo operativo en el factor de tecnología de información, para cada uno de los procesos de tecnología de información de COBIT 4.1 que satisfacen dichos requerimientos normativos. A partir de dicho nivel de

cumplimiento, la entidad financiera podrá determinar un plan de acción a seguir para fortalecer aquellos procesos que resulten con un nivel de cumplimiento deficiente o que no satisfagan sus expectativas.

Además, para la evaluación del cumplimiento de los requerimientos normativos anotados anteriormente, se considerarán los 34 objetivos de control de Cobit 4.1 y se identificará a aquellos que los satisfacen, permitiendo que los que no estén referidos en la norma, también sean evaluados por la institución para conocer el nivel de riesgo global en todos sus procesos de tecnología de información.

Cabe aclarar que el presente proyecto de ningún modo pretende obtener una metodología de implementación de gobierno de tecnología de información, ya que Cobit brinda un mapa de ruta genérico para realizar dicha implementación en su documento "*IT Governance Implementation Guide: Using Cobit and Val IT, 2nd Edition*". Únicamente aspira a brindar una serie de pasos que permitan, de una manera lógica, ordenada y flexible, obtener el grado de cumplimiento de las regulaciones normativas, y como herramienta, utilizar Cobit 4.1 para conocer los objetivos de control en los que la institución deberá reforzar sus procedimientos tecnológicos, acogiéndose a las mejores prácticas internacionales.

Esto permitirá a la institución que utilice la metodología que se va a desarrollar en este proyecto, ir más allá del simple cumplimiento normativo, pues conocerá los objetivos de control que facilitarán el impulso de su tecnología de información hacia el buen gobierno corporativo.

1.6 - Términos y condiciones de uso

Los términos y condiciones de uso de los productos del ITGI establecen que algunos de los materiales que se pueden descargar electrónicamente de la página web de ISACA pueden ser utilizados únicamente con propósitos personales, informativos y no comerciales, y se debe mantener todos los derechos reservados de copyright incluidos en los materiales.

Los materiales, o cualquier parte de ellos, no pueden ser copiados, reproducidos o redistribuidos sin el permiso escrito y expreso del ITGI y de ISACA. La reproducción de secciones elegidas de Cobit para uso interno y no comercial o académico está permitida y debe incluir todas las atribuciones de la fuente del material utilizado.

El producto obtenido del desarrollo del presente proyecto puede ser utilizado con fines académicos. Incluye contenido de *COBIT 4.1*, el cual es utilizado con autorización del IT Governance Institute (ITGI). ©1996-2007 IT Governance Institute. Todos los derechos reservados.

También incluye contenido del *IT Assurance Guide Using COBIT*®, el cual es utilizado con autorización del IT Governance Institute (ITGI). ©1996-2007 IT Governance Institute. Todos los derechos reservados.

Dichas autorizaciones se han efectuado para las versiones en español e inglés, por lo que se incluyen los créditos en el lenguaje original:

CAPÍTULO 2: MARCO TEÓRICO DE REFERENCIA

2.1 - El Comité de Basilea

El Banco de Pagos Internacionales (BIS por sus siglas en inglés - Bank for International Settlements) es una organización internacional que promueve el desarrollo monetario internacional y cooperación financiera y sirve como un banco para bancos centrales.

El BIS realiza su mandato siendo:

- Un foro para promover la discusión y análisis de políticas entre bancos centrales y dentro de la comunidad financiera internacional.
- Un centro para la investigación económica y monetaria.
- Una contraparte primordial para bancos centrales en sus transacciones financieras.
- Agente o representante legal en conexión con operaciones financieras internacionales.

Su oficina matriz está en Basilea, Suiza, y hay dos oficinas de representación: en la Región Administrativa Especial Hong Kong de la República de China y en la Ciudad de México. Establecida el 17 de mayo de 1930, el BIS es la organización financiera internacional más antigua del mundo.

Las investigaciones económicas, monetarias, financieras y legales del BIS dan soporte a las reuniones y actividades de los comités basados en Basilea, los cuales están localizados en el BIS y son:

- El Comité de Basilea para la Supervisión Bancaria
- El Comité para el Sistema Financiero Global
- El Comité del Sistema de Pagos y Acuerdos
- El Comité de Mercados, y
- El Comité Irving Fisher para Estadísticas de Bancos Centrales

El Comité de Basilea para la Supervisión Bancaria constituye un foro para la cooperación permanente en materia de supervisión bancaria. Su objetivo es ampliar la comprensión de temas clave de supervisión y mejorar la calidad de la supervisión bancaria alrededor del mundo, por medio del intercambio de información de temas, propuestas y técnicas de supervisión nacionales, con la intención de promover la comprensión común.

Al mismo tiempo, el Comité de Basilea utiliza esta comprensión común para desarrollar guías y estándares de supervisión en áreas donde se consideran necesarios. Con esta consideración, el Comité de Basilea es mejor conocido por sus estándares internacionales en adecuación de capital, los Principios Básicos para una Supervisión Bancaria Efectiva, y el Acuerdo de supervisión bancaria internacional.

Los miembros del Comité de Basilea provienen de Bélgica, Canadá, Francia, Alemania, Italia, Japón, Luxemburgo, Holanda, España, Suecia, Suiza, el Reino Unido y los Estados Unidos. El Comité de Basilea exhorta al contacto y la cooperación entre sus miembros y otras autoridades de supervisión bancaria, por lo que, tanto los documentos publicados como los no publicados, circulan hacia los supervisores de todo el mundo, proveyendo guías en materia de supervisión bancaria.

Los esfuerzos del Comité de Basilea para la Supervisión Bancaria para revisar los estándares que rigen la adecuación de capital de bancos activos internacionalmente alcanzaron un nivel trascendental con la publicación del texto del Acuerdo Basilea II en junio del 2004, en el que se incluyeron lineamientos para la gestión del riesgo operativo. En noviembre del 2005, el Comité emitió una versión actualizada del Acuerdo revisado, incorporando el conjunto de guías formales adicionales del documento "La aplicación de Basilea II a las actividades de negociación y el tratamiento de los efectos de doble pérdida", de julio del 2005.

El Acuerdo de Basilea II emitido por el Comité describe técnicas más comprensibles para la adecuación de capital en la que las autoridades de supervisión están trabajando para implementar a través de la elaboración de reglas domésticas y la adopción de procedimientos. Basilea II busca mejorar las reglas existentes alineando los requerimientos regulatorios de capital hacia los riesgos inherentes que los bancos enfrentan.

Además, el Acuerdo de Basilea II está orientado a promover una propuesta más progresiva de la supervisión de capital, que exhorta a los bancos a identificar los riesgos que pueden enfrentar, ahora y en el futuro, y a desarrollar o mejorar su habilidad para administrar esos riesgos. Como resultado, está orientado a ser más flexible y capaz de evolucionar con los avances de los mercados y las prácticas de administración de riesgos.

El 4 de julio del 2006, el Comité emitió una versión comprensible del Acuerdo de Basilea II. Únicamente como material conveniente para los lectores, este documento comprensible es una compilación del Acuerdo de Basilea II de junio del 2004, los elementos del Acuerdo de 1988, la Enmienda al Acuerdo de Capital para incorporar riesgos de mercado del 2006, y el documento de julio del 2005 mencionado anteriormente. En esta compilación no se han introducido nuevos elementos.

2.2- Superintendencia de Bancos y Seguros

En 1927, bajo inspiración de la Misión Kemmerer (1925 - 1927), llamada así porque la presidió el doctor Edwin Walter Kemmerer, se produjo en el país una verdadera transformación en el ramo bancario y financiero al expedir la Ley Orgánica de Bancos, la Ley Orgánica del Banco Hipotecario (Banco Nacional de Fomento) y la Ley Orgánica del Banco Central, que afianzaron el sistema financiero del país, así como otras leyes que regularon el manejo de la Hacienda Pública.

Desde entonces, se estableció la supervisión de las operaciones bancarias mediante la creación de la SUPERINTENDENCIA DE BANCOS el día 6 de Septiembre de 1927.

La Superintendencia de Bancos y Seguros es un organismo técnico, con autonomía administrativa, económica y financiera, cuyo objetivo principal es vigilar y controlar con transparencia y eficacia a las instituciones de los sistemas financiero, de seguro privado y de seguridad social, a fin de que las actividades económicas y los servicios que prestan se sujeten a la ley y atiendan al interés general. Asimismo, busca contribuir a la profundización del mercado a través del acceso de los usuarios a los servicios financieros, como aporte al desarrollo económico y social del país.

En su estructura orgánico funcional, cuenta con órganos de apoyo especializado entre los que se encuentra la Dirección Nacional de Riesgos, la cual tiene entre sus funciones generar políticas de supervisión y metodologías de evaluación del riesgo y apoyar a las unidades de supervisión en la aplicación de dichas metodologías en las instituciones controladas por la Superintendencia de Bancos y Seguros.

Uno de los procesos asignados a la Dirección Nacional de Riesgos es la evaluación del Riesgo Operacional de los sistemas financiero, de seguro privado y de seguridad social, que se realiza en una de sus subdirecciones: la Subdirección de Riesgos Operacionales.

Las funciones de esta subdirección son, entre otras, las siguientes:

- Elaborar estudios sobre la identificación y exposición a riesgos operacionales
- Elaborar metodologías para la evaluación de los riesgos operacionales
- Elaborar proyectos de norma para mejorar la administración y control de riesgos operacionales
- Apoyar a las unidades de supervisión en la aplicación de las metodologías
- Participar en los procesos de supervisión in situ

Para el cumplimiento de sus funciones, la Subdirección de Riesgos Operacionales debe considerar los riesgos tecnológicos de las entidades controladas por la Superintendencia de Bancos y Seguros. Como se puede advertir, el presente trabajo también podría coadyuvar al cumplimiento de algunas de las funciones que debe cumplir la Subdirección de Riesgos Operacionales de la Superintendencia de Bancos y Seguros, especialmente en el desarrollo de metodologías para la evaluación de los riesgos operacionales y su aplicación en las instituciones controladas.

2.3- Base legal de la gestión del riesgo operativo

Existen diferentes normas legales, metodologías y mejores prácticas internacionales que se han adoptado en los últimos años para la administración

orientada a riesgos en las instituciones financieras, tendientes a minimizar la posibilidad de que se produzca un hecho generador de pérdidas que afecten el valor económico de la organización, en pro de proteger los intereses de sus accionistas, funcionarios, clientes y proveedores.

En el tema normativo, por un lado se encuentran los lineamientos emitidos por el Comité de Basilea para la Supervisión Bancaria, los cuales han sido desarrollados para un ámbito internacional pero no constituyen una exigencia legal para las instituciones financieras del Ecuador, sino que más bien representan las mejores prácticas financieras y bancarias para conseguir una adecuada administración y supervisión bancaria. Por otro lado, la Codificación de Resoluciones de la Superintendencia de Bancos y Seguros y de la Junta Bancaria constituye un compendio de disposiciones legales que tienen el carácter de obligatorio en cuanto a su cumplimiento por parte de las entidades que conforman los sistemas financieros, de seguros privados y de seguridad privada a nivel nacional.

Con respecto al Nuevo Acuerdo de Capital de Basilea (Basilea II), su primer pilar, que se refiere a los requerimientos mínimos de capital, propone cambiar la definición de activos ponderados por su nivel de riesgo en el Nuevo Acuerdo a través de dos elementos principales: (1) modificaciones sustanciales en el tratamiento del riesgo de crédito con respecto al Acuerdo vigente; y (2) la introducción de un tratamiento explícito para el riesgo operativo, lo cual resultará en una medición de dicho riesgo que afectará el coeficiente de capital del banco, y

sugiere tres opciones distintas para el cálculo del riesgo operativo, a aplicar según la naturaleza, tamaño y complejidad de cada institución financiera.

El Comité de Basilea considera que el riesgo operativo es un factor de gran importancia para los bancos, los cuales deben mantener el capital necesario para protegerse de posibles pérdidas causadas por estos riesgos. En el marco de Basilea II, el riesgo operativo se define como:

"el riesgo de que se produzcan pérdidas como resultado de procesos, personal o sistemas internos inadecuados o defectuosos, o bien a consecuencia de acontecimientos externos."

El riesgo operativo constituye otro ámbito para el que el Comité ha articulado un nuevo método de capital regulador. Al igual que ocurre con el riesgo de crédito, el Comité se apoya en el desarrollo por parte de los bancos de técnicas de evaluación internas e intenta incentivar a los bancos para que mejoren dichas técnicas, y en términos más generales, también su gestión del riesgo operativo con el tiempo. En relación a este tema, se indica textualmente:

"Las técnicas aplicadas al riesgo operativo continúan evolucionando rápidamente, aunque lo cierto es que no se prevé que en un futuro cercano alcancen la precisión con la que se pueden cuantificar los riesgos de mercado y de crédito. Dicha situación ha obstaculizado en cierto modo la incorporación de una medida destinada al riesgo operativo dentro del primer pilar del Nuevo Acuerdo.

No obstante, el Comité es de la opinión de que dicha incorporación es vital para asegurar la existencia de incentivos contundentes para que los bancos continúen desarrollando sistemas de medición y gestión del riesgo operativo y para cerciorarse de que mantienen niveles de capital suficiente para hacer frente a dichos riesgos.

Lo cierto es que si no se hubiera establecido un requerimiento de capital mínimo para el riesgo operativo en el Nuevo Acuerdo, se habrían mermado esos incentivos, lo que hubiera resultado en una reducción de los recursos con los que cuenta la banca para afrontar el riesgo operativo."

Entre tanto, la Codificación de Resoluciones de la Superintendencia de Bancos y Seguros y de la Junta Bancaria en su título VII “De los activos y de los límites de crédito”, subtítulo VI “De la gestión y administración de riesgos”, capítulo I “De la gestión integral y control de riesgos”, establece la normativa que rige la Administración integral de riesgos, en la que exige a las instituciones del sistema financiero establecer esquemas eficientes y efectivos de administración y control de todos los riesgos a los que se encuentran expuestas en el desarrollo de su negocio conforme su objeto social, ya que considera a la Administración integral de riesgos parte de la estrategia institucional y del proceso de toma de decisiones.

En este contexto, dicha norma define algunos de los riesgos a los que están expuestas las instituciones que se encuentran bajo su control, entre los cuales establece la siguiente definición para el Riesgo Operativo:

*"**Riesgo operativo.-** Es la posibilidad de que se produzcan pérdidas debido a eventos originados en fallas o insuficiencia de procesos, personas, sistemas internos, tecnología, y en la presencia de eventos externos imprevistos. Incluye el riesgo legal pero excluye los riesgos sistémico y de reputación.*

Agrupa una variedad de riesgos relacionados con deficiencias de control interno; sistemas, procesos y procedimientos inadecuados; errores humanos y fraudes; fallas en los sistemas informáticos; ocurrencia de eventos externos o internos adversos, es decir, aquellos que afectan la capacidad de la institución para responder por sus compromisos de manera oportuna, o comprometen sus intereses"

Adicionalmente, el primer párrafo del artículo 5 de la sección II "Administración de riesgos" del mismo capítulo, señala:

*"**ARTICULO 5.-** Todos los niveles de la organización, dentro de sus competencias, harán seguimiento sistemático de las exposiciones de riesgo y de los resultados de las acciones adoptadas, lo cual significa un monitoreo permanente a través de un sistema de información para cada tipo de riesgo, preparado para satisfacer las necesidades particulares de la institución."*

Como se puede advertir, las instituciones financieras requieren implementar sistemas de información que les permita realizar el control de sus riesgos y que establezcan los mecanismos para elaborar e intercambiar información oportuna, segura, confiable, fidedigna, interna y externa.

Como una regulación más específica, en el capítulo V "De la gestión del riesgo operativo" de la misma base legal, se establece que los factores del riesgo operativo que se deben administrar adecuadamente para minimizar la posibilidad de sufrir pérdidas debido a este riesgo, son: los procesos, las personas, la tecnología de información (riesgo tecnológico) y los eventos externos.

De esta necesidad de cumplimiento regulatorio, y más que todo, de la necesidad de implementar un adecuado gobierno de tecnología de información en las organizaciones, nace la iniciativa de llevar a cabo el presente proyecto que pretende servir de soporte para la administración del riesgo tecnológico en las instituciones del sistema financiero ecuatoriano.

2.4 - Marco de trabajo de Cobit

Una parte integral del Gobierno Corporativo es el Gobierno de TI, que de acuerdo con el ITGI, consiste en el liderazgo, estructuras organizacionales y

procesos que aseguran que la tecnología de información de la empresa soportará y complementará las estrategias y objetivos de la empresa. Cobit establece que la responsabilidad del gobierno de TI es de la alta dirección y de los directivos, es decir que su implementación se debe dar a todo nivel dentro de una organización, y no solo en el área de Tecnología de Información de las empresas.

Para contar con la información que una institución necesita para lograr sus objetivos, los recursos de tecnología de información deben ser administrados por un conjunto de procesos. Para ello, la alta dirección requiere objetivos de control que definan la meta de implantar políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para garantizar que se alcancen los objetivos del negocio y se prevengan o se detecten y corrijan los eventos no deseados, buscando continuamente información oportuna y condensada para tomar decisiones difíciles respecto a riesgos y controles, de manera rápida y exitosa.

El marco de trabajo de COBIT 4.1, que brinda las directrices gerenciales para el control de la tecnología de información, tiene su base en referencias internacionales como COSO, ITIL, normas ISO 9001 de calidad e ISO 27002 de gestión de seguridad de la información, PMBOK para administración de proyectos, etc., y se elaboró con la colaboración de expertos de universidades, gobiernos y de la profesión de gobierno, aseguramiento, control y seguridad de TI.

Los objetivos de control de Cobit fueron elaborados por el Instituto de Gobierno de Tecnología de Información (ITGI - IT Governance Institute) en 1996, y a partir de entonces fue evolucionando con la creación de las Guías de auditoría

en 1998 y la emisión de su versión 3 en el año 2000, en la que ya incluye indicadores, directrices gerenciales, prácticas de control y el modelo de madurez para sus objetivos de control. Cobit 4.0 eleva la responsabilidad de la tecnología de información hacia la alta gerencia, por lo que le da otro enfoque a sus objetivos de control, reduce su número y define roles y responsabilidades a través de la matriz RACI. Su versión más reciente es la 4.1, que aún no ha sido traducida al castellano, fue creada en el 2007 y es una versión mejorada de su anterior.

CobiT™ es en realidad un acrónimo formado por las siglas derivadas de *Control Objectives for Information and Related Technology* (objetivos de control para la información y las tecnologías relacionadas). Su misión es investigar, desarrollar, publicar y promover un marco de trabajo de control de gobierno de TI autorizado y actualizado, internacionalmente aceptado y adoptado para el uso cotidiano de las empresas, gerentes de negocios, profesionales de TI y de Aseguramiento.

Dado que Cobit 4.1 agrupa un conjunto de estándares y mejores prácticas internacionales en sus procesos, la implementación del gobierno de TI en una institución que ha adoptado alguno de esos estándares, como ISO 9001, ISO 27002, ITIL, AS/NZ 4360, PMBOK, etc., se facilita aún más por el lenguaje común que se maneja en el desarrollo de un proyecto de esta naturaleza. Sin embargo, en una institución que no ha adoptado aún ninguno de esos estándares, la implementación del gobierno de TI resulta igualmente factible y mejora notablemente la capacidad de manejo de procesos organizacionales debido a sus indicadores de medición de logros.

A más de ser un marco de trabajo, Cobit tiene un conjunto de herramientas de soporte que permite a los directivos de una institución disminuir la brecha entre los requerimientos de control, la evolución tecnológica y los riesgos del negocio. Además facilita un desarrollo claro de las políticas y buenas prácticas para el control de la tecnología de información en las organizaciones, enfatiza el cumplimiento regulatorio, y ayuda a las instituciones a incrementar el valor agregado que se obtiene de la tecnología de información y su alineamiento con los objetivos organizacionales.

Cobit 4.1 toma como punto de inicio del ciclo de la información a los objetivos del negocio, a los cuales deben alinearse los objetivos o metas de TI para poder satisfacer los requerimientos de negocio. Los requerimientos de negocio, en términos de criterios de información, son siete y se agrupan de la siguiente manera:

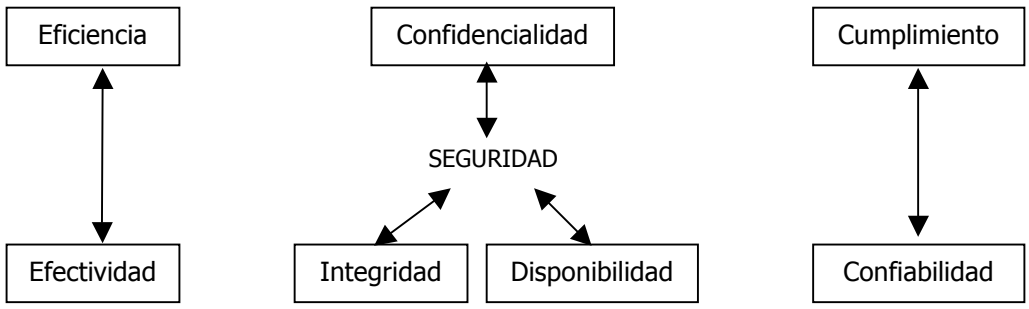


Figura 2.1: Criterios de información

Cobit establece las siguientes definiciones para estos 7 criterios de información:

Efectividad: tiene que ver con que la información sea relevante y pertinente a los procesos del negocio, y se proporcione de una manera oportuna, correcta, consistente y utilizable.

Eficiencia: consiste en que la información sea generada optimizando los recursos (más productivo y económico).

Confidencialidad: se refiere a la protección de información sensitiva contra revelación no autorizada.

Integridad: está relacionada con la precisión y completitud de la información, así como con su validez de acuerdo a los valores y expectativas del negocio.

Disponibilidad: se refiere a que la información esté disponible cuando sea requerida por los procesos del negocio en cualquier momento. También concierne con la protección de los recursos y las capacidades necesarias asociadas.

Cumplimiento: tiene que ver con acatar aquellas leyes, reglamentos y acuerdos contractuales a los cuales está sujeto el proceso de negocios, es decir, criterios de negocios impuestos externamente, así como políticas internas.

Confiabilidad: significa proporcionar la información apropiada para que la gerencia administre la entidad y ejercite sus responsabilidades fiduciarias y de gobierno.

Las metas de tecnología de información son 28 y deben alinearse a los objetivos del negocio para satisfacer sus requerimientos. Estas metas de tecnología de información se logran mediante la ejecución de 34 procesos de tecnología de información que se denominan también objetivos de control de alto nivel, que a su vez se desglosan en 218 actividades u objetivos de control detallados. Los 34 objetivos de control están agrupados en 4 dominios que se realizan de forma lógica, secuencial o "natural" en el área tecnológica, y son:

Planificar y organizar (10 objetivos de control o procesos de TI)

PO1 Definir un plan estratégico de TI

PO2 Definir la arquitectura de la información

PO3 Determinar la dirección tecnológica

PO4 Definir los procesos, organización y relaciones de TI

PO5 Administrar la inversión en TI

PO6 Comunicar las aspiraciones y la dirección de la gerencia

PO7 Administrar recursos humanos de TI

PO8 Administrar la calidad

PO9 Evaluar y administrar los riesgos de TI

PO10 Administrar proyectos

Adquirir e implementar (7 objetivos de control o procesos de TI)

AI1 Identificar soluciones automatizadas

AI2 Adquirir y mantener software aplicativo

AI3 Adquirir y mantener infraestructura tecnológica

AI4 Facilitar la operación y el uso

AI5 Adquirir recursos de TI

AI6 Administrar cambios

AI7 Instalar y acreditar soluciones y cambios

Entregar y dar soporte (13 objetivos de control o procesos de TI)

DS1 Definir y administrar los niveles de servicio

DS2 Administrar los servicios de terceros

DS3 Administrar el desempeño y la capacidad

DS4 Garantizar la continuidad del servicio

DS5 Garantizar la seguridad de los sistemas

DS6 Identificar y asignar costos

DS7 Educar y entrenar a los usuarios

DS8 Administrar la mesa de servicio y los incidentes

DS9 Administrar la configuración

DS10 Administrar los problemas

DS11 Administrar los datos

DS12 Administrar el ambiente físico

DS13 Administrar las operaciones

Monitorear y evaluar (4 objetivos de control o procesos de TI)

ME1 Monitorear y evaluar el desempeño de TI

ME2 Monitorear y evaluar el control interno

ME3 Garantizar el cumplimiento regulatorio

ME4 Proporcionar gobierno de TI

La ejecución de estos procesos en una forma estructurada y lógica en el área de tecnología de información, permiten implementar el gobierno de TI en una forma más comprensible y clara y aseguran una administración integrada y estructurada al definir roles, responsabilidades, prácticas de control y métricas para la evaluación de su desempeño y los logros obtenidos en cada uno de los procesos.

Para alcanzar las metas de tecnología de información, Cobit 4.1 especifica que los **recursos de información** requeridos en toda organización son 4:

1. **Aplicaciones:** Este concepto se entiende como los sistemas de información (aplicaciones) que integran tanto procedimientos manuales como procedimientos programados (basados en tecnología) y que dan soporte a procesos de negocio.
2. **Información:** incluye a los objetos de información en su sentido más amplio, considerando información interna y externa, estructurada y no estructurada, gráficas, sonidos, etc.
3. **Infraestructura:** Incluye hardware (equipos), sistemas operativos, sistemas de administración de bases de datos, de redes y de telecomunicaciones, multimedia, etc., e instalaciones.
4. **Recurso humano:** Este concepto incluye habilidades, conciencia y productividad del personal para planear, adquirir, prestar servicios, proporcionar soporte y monitorear los sistemas y servicios de información.

Uno o más de cada uno de estos recursos de información serán requeridos en cada uno de los objetivos de control de alto nivel para lograr su cumplimiento. La alta dirección deberá seleccionar los objetivos de control que son aplicables a su institución, balancear el costo de inversión para su implementación versus el riesgo de no ejecutarlos, y decidir qué prácticas de control se implementarán y cómo, para cada objetivo de control de alto nivel.

Para cada uno de los 34 procesos, el documento de Cobit 4.1 dispone de las siguientes herramientas:

- Objetivo de control de alto nivel / Proceso de tecnología de información
- Descripción del proceso
- Requerimientos del negocio / criterios de información que soporta
- Prácticas clave para alcanzar el objetivo de control
- Indicadores de medición
- Dominios del Gobierno de TI relacionados con el proceso
- Recursos de TI relacionados
- Actividades del proceso
- Directrices gerenciales (entradas y salidas del proceso)
- Matriz RACI (Responsible, Accountable, Consulted and Informed)
- Metas y métricas (KGI y KPI)
- Modelo de madurez

En el documento Cobit 4.1 se pueden encontrar todas las herramientas mencionadas anteriormente para cada proceso. En el presente trabajo se hará

referencia principalmente a las actividades y a los modelos de madurez de cada proceso, por lo que a continuación se los describe:

Actividades del proceso

Como en todo proceso organizacional, los procesos de tecnología de información se desagregan en actividades conducentes a lograr el objetivo de control establecido. Cobit denomina "objetivos de control de alto nivel" a cada uno de los procesos de tecnología de información, y "objetivos de control detallados" a cada una de sus actividades, y las orienta a obtener un gobierno de tecnología de información efectivo que se consigue además con la evaluación de los riesgos que deben ser administrados en cada proceso.

Los objetivos de control detallados, o actividades del proceso se encuentran en la segunda página de cada proceso de tecnología de información.

Modelos de madurez

Los modelos de madurez de Cobit son una derivación del modelo de madurez que el Instituto de Ingeniería de Software (SEI por sus siglas en inglés) definió para la madurez de la capacidad de desarrollo de software. Cobit provee un modelo de madurez específico para cada uno de sus 34 procesos de tecnología de información, en cada uno de los cuales establece la siguiente escala:

0 - Inexistente

1 - Ad hoc, inicial

2 - Repetible pero intuitivo

3 - Definido

4 - Administrado y medido

5 - Optimizado

Esta herramienta le permite a una empresa realizar comparaciones e identificar:

a) El desempeño actual de la empresa - donde la empresa está hoy en día
b) El estado actual de la industria - la comparación
c) El objetivo de la empresa para mejorar - donde la empresa quiere estar
d) El camino a recorrer entre la situación actual y la objetivo

La ventaja de un modelo de madurez es que es relativamente fácil para que la alta administración se ubique en la escala y aprecie lo que involucra mejorar el desempeño actual. La escala incluye el cero debido a que es muy posible que un proceso no exista. La escala de 0 a 5 está basada en una escala de madurez simple que indica cómo un proceso evoluciona desde una capacidad no existente hasta una capacidad optimizada.

Sin embargo, la capacidad de administración de un proceso no es lo mismo que el desempeño de un proceso. La capacidad requerida, determinada por las metas del negocio y la tecnología de información, puede no necesitar ser aplicada al mismo nivel en todo el ambiente de tecnología de información, sino solo a un

número limitado de sistemas o unidades. La medición del desempeño es esencial para determinar el desempeño actual de la empresa que tienen sus procesos de tecnología de información.

Los modelos de madurez están construidos empezando desde el modelo cualitativo genérico de Cobit, al cual los principios de los siguientes atributos son adicionados de una manera creciente a través de los niveles de la escala:

• Conciencia y comunicación

• Políticas, planes y procedimientos

• Herramientas y automatización

• Habilidades y experiencia

• Responsabilidad y rendición de cuentas

• Establecimiento de objetivos y medición

Guías de auditoría

Además del marco de trabajo de Cobit 4.1, el ITGI ha elaborado las guías de auditoría que en la versión 4.1 pasaron a ser las "Guías de aseguramiento de tecnología de información usando Cobit", que se encuentran en el documento "IT Assurance Guide Using Cobit", del cual se han extraído las pruebas de diseño de controles, los conductores de valor y los conductores de riesgo de los controles genéricos de procesos.

Los controles genéricos de procesos de Cobit han sido diseñados para ser aplicados a cualquier proceso, pero especialmente en la ejecución de sus 34 procesos de tecnología de información, y son los siguientes:

Controles genéricos de Procesos

PC1 Objetivos y metas del Proceso

PC2 Propietario del Proceso

PC3 Repetitividad del Proceso

PC4 Roles y Responsabilidades

PC5 Políticas, Planes y Procedimientos

PC6 Mejoramiento del Desempeño del Proceso

Dependiendo de la madurez con que una institución maneje sus procesos de tecnología de información, la implementación del gobierno de TI puede llevar hasta dos años para completar su ciclo completo, por lo que el presente trabajo se limitará a evaluar la condición actual y la deseada para la tecnología de información de una institución del sistema financiero, considerando para ello los controles genéricos de procesos y los modelos de madurez de Cobit 4.1.

Los conductores de valor proveen ejemplos de los beneficios para el negocio que pueden resultar de un buen control, mientras que los conductores de riesgo proveen ejemplos de los riesgos que se puede necesitar evitar o mitigar. Para quienes realizan aseguramiento e implementan gobierno de tecnología de información, los conductores de valor y de riesgo les proveen los argumentos para implementar controles y sustanciar el impacto de no implementarlos.

En el documento “IT Assurance Guide Using Cobit” también se encuentran los pasos de aseguramiento para probar el diseño de controles para cada objetivo de control específico basado en sus prácticas de control, los cuales fueron utilizados para obtener las características propias de cada uno de los controles genéricos de procesos mencionados anteriormente.

2.5 - Modelos para diagnóstico

Existen varios modelos para diagnosticar la situación de una institución o de un área específica, sin embargo para los fines de esta metodología se emplearán básicamente dos: los análisis FODA y OPEDEPO.

Análisis FODA

El FODA es un método de análisis participativo que permite conocer la situación real de empresas, instituciones y cualquier tipo de organización, y ayuda en la determinación de políticas para mantener las fortalezas, atacar las debilidades convirtiéndolas en oportunidades y las oportunidades en fortalezas, así como direccionar estrategias para que las amenazas no lleguen a concretarse o si llegan a hacerlo, minimizar su impacto.

El Análisis de la Situación que se logra a través del FODA permite el análisis sistémico, ya que las diversas variables se entrelazan dentro del Principio

de Paretto (causa/efecto), obligando a tener una visión sistémica de la empresa para comprender la situación, incluso interrelacionando su funcionamiento con su entorno nacional e internacional.

Pese a que el FODA parece ser un método sencillo y directo, se puede tropezar con algunos problemas, como el grado de objetividad empleado. Hay que tener cuidado de no caer en irrealidades y plantear con toda objetividad, e incluso frialdad, las oportunidades y fortalezas para que sean reales. Además, el grupo que realice el análisis debe estar consciente de que demasiado optimismo puede llevarlo a ignorar riesgos y enfrentar situaciones de peligro, la mayoría de las veces innecesarias, por no considerarlas en el FODA.

El silencio y la no intervención nunca deben ser tomados como signos aprobatorios dentro de las dinámicas conducentes a obtener un FODA. Debe partirse siempre del principio de que “donde todos piensan igual nadie piensa”, ya que el FODA exige criticidad, objetividad, participación, claridad de pensamiento, capacidad sintética y analítica, y capacidad para ver panoramas globales.

También un grupo muy cohesionado que intente realizar este análisis, puede caer en una conducta grupal de explicar y justificar cualquier cosa, perdiendo capacidad analítica y por lo tanto corriendo el riesgo de obtener un FODA irreal. Además hay que abstenerse de basarse en opiniones para realizar este análisis, pues para trabajar con objetividad se deben considerar únicamente situaciones reales.

Existen otros factores que pueden afectar al grupo de análisis a llegar a un correcto diagnóstico utilizando el método FODA, tales como el temor a decir las cosas, el sentimentalismo por el trabajo propio, diferentes percepciones de la realidad debido a la posición jerárquica en la empresa, un desequilibrio en el número de participantes de diferentes áreas que puede llevar a conflicto, etc., pero en general se debe plantear la máxima objetividad y análisis crítico que conduzcan a obtener un diagnóstico real que a final de cuentas será en beneficio de la institución.

Análisis OPEDEPO

OPEDEPO PF es un acrónimo para oportunidades, peligros, debilidades y potencialidades, fundamentales en la planeación. Al análisis OPEDEPO también se lo conoce como análisis FORD, el cual viene de las primeras letras de Fortalezas, Oportunidades, Riesgos y Debilidades, que son equivalentes. El análisis de estos factores es un paso crítico en la planeación estratégica ya que permite descubrir las oportunidades y los peligros futuros para elaborar planes, ya sea para explotar dichos factores o para evitarlos. El examinar correctamente oportunidades y peligros futuros de una empresa, y relacionarlo en un estudio imparcial con las potencialidades y debilidades de la misma representa una enorme ventaja ya que se toma en cuenta no solo la situación actual sino también su proyección.

Para realizarlo, se procede de manera muy similar al análisis FODA, es decir, primero se piensa en los factores internos de la empresa, que son aquellos

en los que se puede intervenir para modificarlos o reforzarlos, y que corresponden a las debilidades y potencialidades. Después se medita sobre los factores externos o del entorno, que son sobre los que no se puede actuar pero que interactúan con la empresa.

De esta forma, se obtienen cuatro listas que representan un análisis autocrítico que permitirá determinar los riesgos que afectan el logro de los objetivos y cumplimiento de la misión si no se actúa oportunamente, y los factores que pueden ser aprovechados si se toman las medidas adecuadas. Para complementar este análisis, se puede incorporar de manera muy clara y precisa las características fundamentales del segmento de mercado en que se desenvuelven las operaciones de la empresa y su competitividad, y la relación de los principales problemas de la diaria operatividad que afectan y comprometen el logro de los objetivos.

Es importante listar todos estos aspectos considerando solamente aquellos que son principales, sin repetir ni redundar, en forma concreta y eficaz; ello permitirá identificar las acciones a tomar en cada uno de los objetivos o proyectos empresariales y determinar medidas cuantitativas de su logro que permitan verificar su cumplimiento en cantidad y tiempo.

2.6 - Análisis de riesgos

El análisis de los riesgos a los que estaría sujeta la tecnología de información de una institución, si ésta no cumple con los objetivos de control de

tecnología de información que le permite cumplir con los requerimientos normativos de la gestión del riesgo operativo, determina la implicación de varios aspectos, pero principalmente de los dos siguientes:

De cumplimiento

Como se dijo anteriormente, la norma expedida por la Superintendencia de Bancos y Seguros en materia de la administración integral de riesgos, y específicamente para la gestión del riesgo operativo, establece la obligatoriedad de que las instituciones bajo su control cuenten con políticas, procesos y procedimientos que aseguren una adecuada planificación y administración de la tecnología de información.

El incumplimiento de las disposiciones normativas mencionadas podrá ser sancionado de conformidad con lo establecido en el capítulo I “Normas para la aplicación de sanciones pecuniarias”, del título XVI "De las sanciones y de los recursos en sede administrativa" de la Codificación de Resoluciones de la Superintendencia de Bancos y Seguros y la Junta Bancaria.

Bajo este enfoque, los 21 objetivos de control de Cobit 4.1 que satisfacen los requerimientos normativos de riesgo operativo, son de aplicación obligatoria para todas las instituciones que conforman el sistema financiero, y su incumplimiento puede conllevar a la institución a sanciones económicas que pueden resultar significativas dependiendo de la gravedad de la situación.

De mercado

Más allá del cumplimiento normativo, la aplicación de las mejores prácticas internacionales para la administración de la tecnología de información y de los riesgos tecnológicos a los que está expuesta una institución financiera le permitirán, en el mediano y largo plazo, mejorar su eficiencia y efectividad y ser más competitiva en el entorno de los negocios financieros y bancarios, logrando cada vez mejores oportunidades de obtener un incremento en el retorno de su inversión. Esto es aplicable, tanto a las instituciones que conforman el sistema financiero nacional, como a las empresas del sector productivo, y de forma inversa, también se puede advertir que la no aplicación de dichas prácticas de administración de la tecnología de información y sus riesgos, puede resultar en la pérdida de imagen, reputación o mercado empresarial, lo que a su vez podría derivar en un riesgo de mercado o liquidez.

Bajo este enfoque, la implementación de los 34 objetivos de control o procesos de tecnología de información de Cobit 4.1 resulta conveniente para todas las instituciones financieras, por lo que su selección y nivel de madurez a implementar deberá basarse en el apetito de riesgo de cada institución y la comparación con sus similares en mercados similares.

CAPÍTULO 3: DESARROLLO DE LA METODOLOGÍA

3.1 - Introducción

La metodología propuesta consta de cinco etapas que comprenden los pasos macro a seguir para el desarrollo del proyecto, y son:

- Etapa A: Comprensión y aprobación del proyecto
- Etapa B: Evaluación de la situación actual
- Etapa C: Identificación del grado de madurez de los procesos de TI
- Etapa D: Obtención del mapa de riesgo tecnológico
- Etapa E: Elaboración del informe de evaluación

La etapa B considera la utilización de los controles generales de procesos aplicados a todos los procesos de tecnología de información en forma de características que corresponden a los conductores de valor, conductores de riesgo y pruebas de diseño de controles que ofrecen las Guías de Auditoría de Cobit.

La etapa C ha sido adaptada de los pasos de la metodología de implementación del gobierno de tecnología de información de Cobit, en la cual se utilizan los modelos de madurez para identificar los niveles alcanzados y los esperados para cada proceso de tecnología de información. Para la metodología propuesta, se ha efectuado una adición para incluir la valoración del impacto de cada proceso de tecnología de información en los procesos del negocio, lo cual

permite dar un mayor peso a aquellos que presenten una mayor importancia en la organización.

En este capítulo se definen los objetivos de cada etapa y los responsables, entregables, técnicas o herramientas a utilizar y el tiempo máximo requerido para realizar cada una de sus actividades, y se describe cada uno de los pasos que deben llevarse a cabo dentro de cada etapa, especialmente en cuanto a las herramientas creadas para facilitar la aplicación de la metodología propuesta.

Cabe anotar que el tiempo máximo requerido para cada etapa consta de dos partes: el tiempo efectivo que se necesita para desarrollar en sí dicha actividad, y el tiempo con holgura, que usualmente va a ser mucho mayor al tiempo efectivo debido a que en la holgura se estiman tiempos “muertos” o de espera que pueden ocurrir por la falta de disponibilidad del personal involucrado, lo cual se debe tomar en cuenta especialmente en las fechas de cierre de mes en que la institución evaluada debe realizar operaciones y reportes que demandan mayor tiempo.

Dependiendo de la actividad, el tiempo con holgura también obedece a que si el personal involucrado no conoce a fondo la herramienta o técnica con la que se va a desarrollar la actividad, puede ser necesario un tiempo adicional para investigarla. Una vez que la institución conoce el tiempo efectivo requerido para cada actividad, puede determinar la cantidad de recursos humanos y de tiempo empleado diariamente para su consecución.

Producto final de la aplicación de la metodología propuesta es la obtención del mapa de riesgo tecnológico y el informe de evaluación, que permitirán conocer la situación de la institución en cuanto a los controles aplicados a sus procesos de tecnología de información, su madurez, impacto, riesgos relevantes y las acciones de mejora que permitirán mitigar los riesgos a los que actualmente se encuentra expuesta la plataforma tecnológica de la institución evaluada.

Paralelamente al desarrollo de la presente metodología, se elaboró un soporte informático en Excel que facilita el desarrollo de las actividades de las diferentes etapas mencionadas, desde la homologación del requerimiento normativo a los procesos de tecnología de información, hasta las operaciones de cálculo que se requiere realizar para obtener la calificación de riesgo de los ejes X e Y del mapa de riesgo tecnológico. Dicho libro en Excel se adjunta a este documento como un anexo en CD, y su utilización se explica conforme se avanza en la descripción de las actividades a realizar para la evaluación del riesgo tecnológico.

Las recomendaciones efectuadas en el informe de evaluación también consideran la utilización de los modelos de madurez de Cobit, de modo que su cumplimiento llevará a la entidad al logro de sus objetivos en cuanto a la madurez de procesos, estableciendo de este modo un mecanismo natural, lógico y escalable de mejoramiento continuo, aplicando estándares y mejores prácticas en tecnología de información, permitiendo a la institución evaluada ir más allá del cumplimiento normativo para llegar a establecer un buen gobierno de TI.

3.2 - Etapa A: Comprensión y aprobación del proyecto

Objetivo: Caracterizar el proyecto y asignarle recursos humanos, de tiempo y financieros.

Entregable: Carta de compromiso de la alta gerencia y aprobación de la planificación y los recursos asignados.

Esta etapa es indispensable para la correcta ejecución del proyecto pues logra el compromiso de la alta gerencia y la asignación de los recursos necesarios para las etapas subsiguientes.

La comprensión de la importancia que tiene la tecnología de información para dar soporte a los procesos de negocio es básica para el involucramiento de toda la organización en la definición de sus requerimientos y el consecuente logro del retorno de la inversión efectuada. Si no existe dicha comprensión, vanos serán los esfuerzos que se empleen en tecnología de información pues sus objetivos no estarán necesariamente alineados con los propósitos y objetivos empresariales.

Para tener una comprensión y estimación clara de los riesgos asociados a la tecnología de información de una institución es necesario partir del análisis del riesgo inherente de la entidad a ser evaluada, ya que de allí se derivarán los aspectos que pueden contribuir o afectar el desempeño general de la plataforma de tecnología de información y sus riesgos asociados.

Tabla 3.1: Actividades de la etapa A, Comprensión y aprobación del proyecto

ACTIVIDADES	RESPONSABLES	ENTREGABLES	TÉCNICA / HERRAMIENTA	TIEMPO MÁXIMO	
				EFECTIVO	CON HOLGURA
A.1. Aprobación de la Gerencia para dar inicio al proyecto.	Gerencia General o de TI	Carta de aprobación para la ejecución del proyecto en la institución	Reunión y solicitud formal con explicación general del proyecto	2 horas	1 semana
A.2. Planificación del proyecto y propuesta de conformación del equipo de trabajo.	Gerencia de Tecnología de Información	Cronograma y conformación del equipo de proyecto con sus roles y responsabilidades	Diagramas de Gantt	2 horas	1 semana
A.3. Presentación y aprobación de la planificación y recursos requeridos por el proyecto.	Comité de Tecnología de Información	Acta de reunión del Comité aprobando la planificación propuesta y los recursos asignados	Exposición de objetivos, alcance y planificación del proyecto	1 hora	1 semana
A.4. Caracterización del proyecto	Gerencia de Tecnología de Información	Caracterización del proyecto	Revisión del plan estratégico y operativo de TI	2 horas	1 semana
A.5. Homologación de los procesos de TI con la norma de riesgo operativo vigente	Gerencia de TI, Auditoría informática o Gerencia de Riesgos	Procesos de Cobit 4.1 requeridos por la norma de riesgo operativo vigente	Tablas de asociación entre los requerimientos normativos y los procesos de TI	4 horas	3 semanas

Actividad A.1: Aprobación de la Gerencia para dar inicio al proyecto

Para dar inicio al proyecto, es necesario que la Gerencia General. o la Gerencia de Tecnología de Información en el caso de que la institución posea una estructura organizacional grande, conozca en términos generales el alcance del proyecto, determine la utilidad de contar con una evaluación del riesgo tecnológico en la institución y apruebe por escrito el desarrollo de las actividades subsiguientes.

Para ello, se deberá mantener una reunión inicial de trabajo con el Gerente General, o Gerente de Tecnología de Información, para explicarle de modo global la necesidad de contar con una metodología para evaluar el riesgo tecnológico en

una institución, el alcance que tendrá la misma, y los productos que se esperan obtener como resultado de su aplicación. Una vez comprendidos los aspectos expuestos, es necesario formalizar el pedido al Gerente mediante una solicitud por escrito que abarque los temas acordados, y a la cual se dará contestación para contar con el sustento necesario para dar inicio al proyecto.

Actividad A.2: Planificación del proyecto y propuesta de conformación del equipo de trabajo

Una vez aprobada la ejecución del proyecto, el Gerente deberá coordinar con el área de tecnología de información la disponibilidad del personal que colaborará en la aplicación de la metodología propuesta. Es deseable que el personal seleccionado para conformar el equipo de proyecto cuente con un conocimiento general tanto de la situación actual de la tecnología de información de la institución como del nivel de soporte que la misma brinda actualmente al resto de áreas o departamentos.

El Gerente de Tecnología de Información o similar, deberá coordinar la planificación del proyecto, la cual incluirá la elaboración de un cronograma mediante un diagrama de Gantt que permita visualizar cada una de las actividades que se llevarán a cabo en el resto de etapas de la metodología junto con sus recursos asignados, y facilitar el seguimiento o revisión del estado de su ejecución. La metodología propuesta ofrece un cronograma base de actividades elaborado en MS Project, con la lista de actividades y los tiempos para cada una de las etapas.

Para los recursos humanos involucrados, se deberá describir los roles y responsabilidades que tendrá cada persona en las actividades a desarrollar, que permitan garantizar que existirá objetividad e imparcialidad en el diagnóstico y evaluación a realizar. Para ello, es conveniente la participación de un auditor informático o un oficial de seguridad de la institución para garantizar la validez de la colaboración del personal asignado y sus roles y responsabilidades asociados, y asegurar una conveniente segregación de sus funciones, ya que al tratarse de una metodología de evaluación del riesgo tecnológico, el personal de Sistemas podría presentar un conflicto de intereses.

En el caso de no contar con un auditor informático o un oficial de seguridad en la entidad, se puede considerar la participación del auditor interno que más conocimiento tenga sobre tecnología de información.

Actividad A.3: Presentación y aprobación de la planificación y recursos requeridos por el proyecto

Esta actividad requiere de la participación de un Comité de Tecnología de Información o similar, que es quien define la dirección tecnológica de la institución y coordina su implementación y funcionamiento en toda la organización. Este Comité deberá estar conformado por el Gerente General y los altos ejecutivos de todas las áreas de negocio, financieras, de tecnología y riesgos, y en forma opcional, de Auditoría Interna.

De no existir un Comité de Tecnología de Información formalmente estructurado y con sus funciones y responsabilidades aprobadas por el directorio o el organismo que haga sus veces, se deberá proponer la conformación de uno funcional para la ejecución del proyecto.

Una vez planificado el proyecto, con el cronograma y los roles y responsabilidades del personal asignado, se deberá presentar dicha propuesta al Comité de Tecnología de Información, para hacerle conocer además los objetivos, alcance y productos del proyecto a ejecutar para obtener sus comentarios y aprobación.

De esta actividad deberá obtenerse una carta de compromiso o acta de aprobación de la alta gerencia, representada por el Comité de Tecnología de Información, para que la ejecución del proyecto tenga la formalidad necesaria para disponer de los recursos necesarios.

La importancia de la ejecución de esta actividad radica en la necesidad de que la alta gerencia conozca y comprenda la importancia que tiene la tecnología de información en el soporte de los procesos de negocio, por lo que su responsabilidad es corporativa y no solo del área de Sistemas.

Además, mediante la ejecución de esta actividad, el Comité conocerá las ventajas que conlleva el contar con el mapa de riesgo tecnológico y el informe de evaluación que se obtendrán como producto de la aplicación de la presente metodología de evaluación del riesgo tecnológico, los mismos que, a la vez que le

permitirán a la institución dar cumplimiento a un requerimiento normativo de un organismo de control, le facilitará la orientación de esfuerzos para mejorar su plataforma tecnológica.

Actividad A.4: Caracterización del proyecto

Para documentar el proyecto, se deberá elaborar la Caracterización del mismo, la cual recogerá la planificación y recursos humanos aprobados por el Comité de Tecnología de Información e incluirá los siguientes temas:

- Nombre del proyecto
- Informático responsable
- Usuarios responsables y áreas a las que pertenecen
- Roles y responsabilidades del recurso humano asignado
- Cronograma de trabajo
- Determinación del modelo para diagnóstico (Análisis FODA u OPEDEPO)
- Descripción general del riesgo inherente institucional
- Restricciones o consideraciones a tomar en cuenta en la realización del proyecto, tanto de la parte tecnológica como de la parte funcional

Cabe aclarar que la caracterización del proyecto no contendrá el análisis de la situación actual de la entidad sino únicamente el modelo de diagnóstico que se utilizará para el efecto, el cual puede ser un análisis FODA u OPEDEPO, y que se llevará a cabo en la siguiente etapa de esta metodología.

Actividad A.5: Homologación de los procesos de TI con la norma de riesgo operativo vigente

Uno de los riesgos que se mencionaron en el capítulo anterior sobre la no ejecución de todos los procesos de tecnología de información era el legal. La normativa que rige la gestión del riesgo operativo en el factor de tecnología de información requiere la ejecución de algunos procesos de TI que deben realizarse en forma obligatoria en las instituciones controladas por la Superintendencia de Bancos y Seguros, por lo que la metodología propuesta sugiere efectuar una homologación entre dicha normativa y los procesos de tecnología de información de Cobit 4.1 para asignar un peso mayor a aquellos requeridos por las regulaciones legales.

Esta homologación de los procesos de Cobit frente a las normas vigentes de la Superintendencia de Bancos y Seguros podría tomar un tiempo adicional para la entidad evaluada, sin embargo la metodología propuesta ya presenta una homologación inicial para las normas que se encuentran vigentes a la fecha de elaboración del presente trabajo de tesis, por lo que en la aplicación de la presente metodología solo haría falta realizar una actualización en el caso de que dichas normas hayan variado a la fecha de inicio del proyecto.

Dicha actualización será responsabilidad de la gerencia del área de tecnología de información, con la participación (deseable) de un auditor informático o gerente de riesgos que conozca las normas citadas y su relación con los objetivos de control de Cobit 4.1.

Para realizar la asociación entre cada requerimiento normativo y los procesos de tecnología de información, se enumeró de 1 a 32 cada uno de los requerimientos normativos y se revisó las actividades de cada objetivo de control de Cobit 4.1 que los satisfacen, encontrando que en algunos casos el requerimiento normativo es muy general en sus términos, por lo que su cumplimiento es cubierto por ciertas actividades de un proceso de tecnología de información y se completa con las actividades de otro.

En otros casos, el cumplimiento se da con la aplicación parcial de un proceso de tecnología de información y en otros con la aplicación completa de todas sus actividades.

Sin embargo, para que el presente proyecto brinde un mayor aporte en la evaluación del riesgo tecnológico, en la homologación efectuada se ha considerado la aplicación completa del proceso o procesos de tecnología de información que satisfagan cada requerimiento normativo.

A continuación se presentan las tablas en las que se especifica la asociación realizada entre los requerimientos normativos y objetivos de control de Cobit 4.1, con las consideraciones anotadas anteriormente, y manteniendo los numerales de la normativa en la que es requerido cada uno de ellos en la base legal para su fácil identificación en la misma:

Tabla 3.2: Soporte de TI a requerimientos de operación de la entidad

No.	Requerimiento normativo	Objetivo de control de Cobit	
1	1.3.1.1 El apoyo y compromiso formal del directorio u organismo que haga sus veces y la alta gerencia;	PO4	Definir los procesos, organización y relaciones de TI
2	1.3.1.2 Un plan funcional de tecnología de información alineado con el plan estratégico institucional; y, un plan operativo que establezca las actividades a ejecutar en el corto plazo (un año), de manera que se asegure el logro de los objetivos institucionales propuestos;	PO1	Definir un plan estratégico de TI
3	1.3.1.3 Tecnología de información acorde a las operaciones del negocio y al volumen de transacciones, monitoreada y proyectada según las necesidades y crecimiento de la institución;	PO3	Determinar la dirección tecnológica
4	1.3.1.4 Un responsable de la información que se encargue principalmente de definir y autorizar de manera formal los accesos y cambios funcionales a las aplicaciones y monitorear el cumplimiento de los controles establecidos;	PO4	Definir los procesos, organización y relaciones de TI
5	1.3.1.5 Políticas, procesos y procedimientos de tecnología de información definidos bajo estándares de general aceptación que garanticen la ejecución de los criterios de control interno de eficacia, eficiencia y cumplimiento, debidamente aprobados por el directorio u organismo que haga sus veces, alineados a los objetivos y actividades de la institución;	PO6	Comunicar las aspiraciones y la dirección de la gerencia
6	1.3.1.6 Difusión y comunicación a todo el personal involucrado de las mencionadas políticas, procesos y procedimientos, de tal forma que se asegure su implementación; y,	PO6	Comunicar las aspiraciones y la dirección de la gerencia
7	1.3.1.7 Capacitación y entrenamiento técnico al personal del área de tecnología de información y de los usuarios de la misma.	DS7	Educar y entrenar a los usuarios
		PO7	Administrar recursos humanos de TI

Tabla 3.3: Operaciones de TI acordes a requerimientos de la entidad

No.	Requerimiento normativo	Objetivo de control de Cobit	
8	1.3.2.1 Manuales o reglamentos internos, debidamente aprobados por el directorio u organismo que haga sus veces, que establezcan como mínimo las responsabilidades y procedimientos para la operación, el uso de las instalaciones de procesamiento de información y respuestas a incidentes de tecnología de información;	DS13	Administrar las operaciones
9	1.3.2.2 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;	DS9	Administrar la configuración

Tabla 3.4: Recursos y servicios provistos por terceros y monitoreados

No.	Requerimiento normativo	Objetivo de control de Cobit	
10	1.3.3.1 Requerimientos contractuales convenidos que definan la propiedad de la información y de las aplicaciones; y, la responsabilidad de la empresa proveedora de la tecnología en caso de ser vulnerables sus sistemas, a fin de mantener la integridad, disponibilidad y confidencialidad de la información; y,	DS2	Administrar los servicios de terceros
11	1.3.3.2 Requerimientos contractuales convenidos que establezcan que las aplicaciones sean parametrizables, que exista una transferencia del conocimiento y que se entregue documentación técnica y de usuario, a fin de reducir la dependencia de las instituciones controladas con proveedores externos y los eventos de riesgo operativo que esto origina.	AI5	Adquirir recursos de TI

Tabla 3.5: Administración de seguridad de la información

No.	Requerimiento normativo	Objetivo de control de Cobit	
12	1.3.4.1 Políticas y procedimientos de seguridad de la información que establezcan sus objetivos, importancia, normas, principios, requisitos de cumplimiento, responsabilidades y comunicación de los incidentes relativos a la seguridad; considerando los aspectos legales, así como las consecuencias de violación de estas políticas;	DS5	Garantizar la seguridad de los sistemas
13	1.3.4.2 La identificación de los requerimientos de seguridad relacionados con la tecnología de información, considerando principalmente: la evaluación de los riesgos que enfrenta la institución; los requisitos legales, normativos, reglamentarios y contractuales; y, el conjunto específico de principios, objetivos y condiciones para el procesamiento de la información que respalda sus operaciones;	DS5	Garantizar la seguridad de los sistemas
14	1.3.4.3 Los controles necesarios para asegurar la integridad, disponibilidad y confidencialidad de la información administrada;	DS11	Administrar los datos
15	1.3.4.4 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 en todos los ambientes de procesamiento;	DS5	Garantizar la seguridad de los sistemas
16	1.3.4.5 Niveles de autorización de accesos y ejecución de las funciones de procesamiento de las aplicaciones, formalmente establecidos, que garanticen una adecuada segregación de funciones y reduzcan el riesgo de error o fraude;	DS5	Garantizar la seguridad de los sistemas
		PO4	Definir los procesos, organización y relación TI
17	1.3.4.6 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;	DS5	Garantizar la seguridad de los sistemas
18	1.3.4.7 Controles adecuados para detectar y evitar la instalación de software no autorizado o sin la respectiva licencia, así como instalar y actualizar periódicamente aplicaciones de detección y desinfección de virus informáticos y demás software maliciosos;	DS5	Garantizar la seguridad de los sistemas
19	1.3.4.8 Controles formales para proteger la información contenida en documentos; medios de almacenamiento u otros dispositivos externos; el uso e intercambio electrónico de datos contra daño, robo, accesos, utilización o divulgación no autorizada de información para fines contrarios a los intereses de la entidad, por parte de todo su personal y de sus proveedores;	DS13	Administrar las operaciones
		DS5	Garantizar la seguridad de los sistemas
20	1.3.4.9 Instalaciones de procesamiento de información crítica en áreas protegidas con los suficientes controles que eviten el acceso de personal no autorizado y daños a los equipos de computación y a la información en ellos procesada, almacenada o distribuida;	DS12	Administrar el ambiente físico
21	1.3.4.10 Las condiciones físicas y ambientales necesarias para garantizar el correcto funcionamiento del entorno de la infraestructura de tecnología de información;	DS12	Administrar el ambiente físico
22	1.3.4.11 Un plan para evaluar el desempeño del sistema de administración de la seguridad de la información, que permita tomar acciones orientadas a mejorarlo; y,	DS5	Garantizar la seguridad de los sistemas
23	1.3.4.12 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 de información; que existan mecanismos alternos que garanticen la continuidad del servicio ofrecido; y, que aseguren la existencia de pistas de auditoría.	DS5	Garantizar la seguridad de los sistemas

Tabla 3.6: Administración de la continuidad de operaciones

No.	Requerimiento normativo	Objetivo de control de Cobit	
24	1.3.5.1 Controles para minimizar riesgos potenciales de sus equipos de computación ante eventos imprevistos, tales como: fallas, daños o insuficiencia de los recursos de tecnología de información; robo; incendio; humo; inundaciones; polvo; interrupciones en el fluido eléctrico, desastres naturales; entre otros;	AI3	Adquirir y mantener infraestructura tecnológica
		DS12	Administrar el ambiente físico
25	1.3.5.2 Políticas y procedimientos de respaldo de información periódicos, que aseguren al menos que la información crítica pueda ser recuperada en caso de falla de la tecnología de información o con posterioridad a un evento inesperado;	DS4	Garantizar la continuidad del servicio
26	1.3.5.3 Mantener los sistemas de comunicación y redundancia de los mismos que permitan garantizar la continuidad de sus servicios; y,	DS4	Garantizar la continuidad del servicio
27	1.3.5.4 Información de respaldo y procedimientos de restauración en una ubicación remota, a una distancia adecuada que garantice su disponibilidad ante eventos de desastre en el centro principal de procesamiento.	DS4	Garantizar la continuidad del servicio

Tabla 3.7: Administración de la adquisición de aplicaciones

No.	Requerimiento normativo	Objetivo de control de Cobit	
28	1.3.6.1 Una metodología que permita la adecuada administración y control del proceso de compra de software y del ciclo de vida de desarrollo y mantenimiento de aplicaciones, con la aceptación de los usuarios involucrados;	PO8	Administrar la calidad
29	1.3.6.2 Documentación técnica y de usuario permanentemente actualizada de las aplicaciones de la institución;	AI4	Facilitar la operación y el uso
		AI6	Administrar cambios
30	1.3.6.3 Controles que permitan asegurar la adecuada administración de versiones de las aplicaciones puestas en producción; y,	AI6	Administrar cambios
31	1.3.6.4 Controles que permitan asegurar que la calidad de la información sometida a migración, cumple con las características de integridad, disponibilidad y confidencialidad.	PO3	Determinar la dirección tecnológica
		AI7	Instalar y acreditar soluciones y cambios

Tabla 3.8: Administración de la infraestructura tecnológica

No.	Requerimiento normativo	Objetivo de control de Cobit	
32	Contar con políticas y procedimientos que permitan la adecuada administración, monitoreo y documentación de las bases de datos, redes de datos, software de base y hardware.	DS3	Administrar el desempeño y la capacidad

Como se puede apreciar, algunos requerimientos normativos se cumplen con la aplicación de dos objetivos de control o procesos de tecnología de información de Cobit 4.1, generalmente correspondiendo a diferentes dominios.

El siguiente resumen muestra los objetivos de control referenciados en su relación con los requerimientos normativos de riesgo tecnológico numerados del 1 al 32, presentada en las tablas anteriores:

Tabla 3.9: Objetivos de control de Cobit 4.1 referenciados por la normativa

Objetivos de control de Cobit 4.1		Selección	No. Requerimiento
P L A N E A R Y O R G A N I Z A R			
PO1	Definir un plan estratégico de TI	SI	2
PO2	Definir la arquitectura de la información	NO	
PO3	Determinar la dirección tecnológica	SI	3, 31
PO4	Definir los procesos, organización y relaciones de TI	SI	1, 4, 16
PO5	Administrar la inversión en TI	NO	
PO6	Comunicar las aspiraciones y la dirección de la gerencia	SI	5, 6
PO7	Administrar recursos humanos de TI	SI	7
PO8	Administrar la calidad	SI	28
PO9	Evaluar y administrar los riesgos de TI	SI	13
PO10	Administrar proyectos	NO	
A D Q U I R I R E I M P L A N T A R			
AI1	Identificar soluciones automatizadas	NO	
AI2	Adquirir y mantener software aplicativo	NO	
AI3	Adquirir y mantener infraestructura tecnológica	SI	24
AI4	Facilitar la operación y el uso	SI	29
AI5	Adquirir recursos de TI	SI	11
AI6	Administrar cambios	SI	29, 30
AI7	Instalar y acreditar soluciones y cambios	SI	31
E N TREGAR Y D A R S OPORTE			
DS1	Definir y administrar los niveles de servicio	NO	
DS2	Administrar los servicios de terceros	SI	10
DS3	Administrar el desempeño y la capacidad	SI	32
DS4	Garantizar la continuidad del servicio	SI	25, 26, 27
DS5	Garantizar la seguridad de los sistemas	SI	12, 13, 15-19, 22, 23
DS6	Identificar y asignar costos	NO	
DS7	Educar y entrenar a los usuarios	SI	7
DS8	Administrar la mesa de servicio y los incidentes	NO	
DS9	Administrar la configuración	SI	9
DS10	Administrar los problemas	NO	
DS11	Administrar los datos	SI	14
DS12	Administrar el ambiente físico	SI	20, 21, 24
DS13	Administrar las operaciones	SI	8, 19
M O N I T O R E A R Y E V A L U A R			
ME1	Monitorear y evaluar el desempeño de TI	NO	
ME2	Monitorear y evaluar el control interno	NO	
ME3	Garantizar el cumplimiento regulatorio	NO	
ME4	Proporcionar gobierno de TI	NO	
	TOTAL OBJETIVOS DE COBIT 4.1:	**21**	

3.2- Etapa B: Evaluación de la situación actual

Objetivo: Identificar el nivel de riesgo y la criticidad de los procesos de tecnología de información de la entidad evaluada.

Entregables: Diagnóstico y puntaje de riesgo general de los controles genéricos aplicados a los procesos de tecnología de información.

Responsable: Equipo de proyecto designado.

En esta etapa se obtiene un diagnóstico de la situación actual utilizando el modelo seleccionado en la caracterización del proyecto, y una valoración de los controles genéricos de Cobit que se están aplicando a cada proceso de tecnología de información en la institución evaluada, y que sirve para posteriormente establecer una calificación de riesgo general para todos los procesos.

La ventaja de aplicar esta etapa en el desarrollo de la metodología propuesta es que la calificación de riesgo obtenida para todos los procesos considera tanto los controles aplicados a cada proceso de tecnología de información como el aspecto normativo que rige la administración del riesgo operativo en el factor de tecnología de información, pues aquellos que constituyan un requerimiento de la Superintendencia de Bancos y Seguros para las instituciones del sistema financiero tendrán un mayor peso en la calificación general a obtener.

Por otro lado, el diagnóstico obtenido servirá de insumo para la siguiente etapa, en la que se define el nivel de madurez de cada proceso de TI, y para elaborar el informe final con los resultados obtenidos en la aplicación de la presente metodología de evaluación.

Tabla 3.10: Actividades de la etapa B, Evaluación de la situación actual

ACTIVIDADES	ENTREGABLES	TÉCNICA / HERRAMIENTA	TIEMPO MÁXIMO	
			EFECTIVO	CON HOLGURA
B.1. Aplicación del modelo de diagnóstico.	Diagnóstico de la situación actual de la tecnología de información	Modelo de diagnóstico especificado en la caracterización del proyecto	2 horas	1 semana
B.2. Evaluación de los controles genéricos aplicados en cada proceso de tecnología de información.	Puntaje de controles aplicados a cada proceso de TI	Matriz de controles genéricos aplicados a los procesos de TI	20 horas	3 semanas
B.3. Aplicación de la homologación de los procesos de TI con la norma de riesgo operativo vigente.	Matriz de controles genéricos con los pesos relativos asignados a los procesos de Cobit 4.1	Fórmulas de cálculo de los pesos relativos respecto al requerimiento o no de la norma para cada proceso.	1 día	1 día
B.4. Obtención de una calificación de riesgo general inicial de los procesos de tecnología de información.	- Puntaje de riesgo general de los procesos de TI - Identificación inicial de procesos en estado crítico	Fórmula de cálculo del puntaje de riesgo general	1 día	1 día

Actividad B.1: Aplicación del modelo de diagnóstico

Para obtener el diagnóstico de la situación actual de la tecnología de información, se deberá utilizar el modelo definido en la caracterización del proyecto, el mismo que podrá ser el Análisis FODA o el OPEDEPO, según se adapte a la institución evaluada.

La explicación de cada uno de estos modelos de diagnóstico se encuentra detallada en el capítulo 2 – Marco teórico de referencia, los cuales además indican el formato que se deberá adoptar para la entrega de los resultados

obtenidos. El diagnóstico obtenido deberá tomarse en cuenta en las posteriores actividades en que se evalúa la situación actual de los procesos de tecnología de información y sus niveles de madurez, en la siguiente etapa, para que exista congruencia en la evaluación.

Actividad B.2: Evaluación de los controles genéricos aplicados en cada proceso de tecnología de información

Los 34 procesos de tecnología de información de Cobit 4.1 han sido diseñados y orientados a soportar las metas de tecnología de información que satisfacen los objetivos de negocio de las empresas. El hecho de no contar o de cumplir parcialmente con algunos de dichos procesos de tecnología de información conlleva diferentes riesgos tecnológicos que deben ser analizados en cada institución para determinar su criticidad e impacto en el negocio y poder establecer un plan de acción que permita mitigar las consecuencias de la ocurrencia de dichos riesgos.

Para facilitar dicho análisis, y llevarlo a cabo de un modo general y uniforme, se ha tomado como referencia los controles genéricos de procesos, o pasos de aseguramiento generales, para los procesos de tecnología de información de Cobit 4.1 que provee el documento "IT Assurance Guide Using Cobit" en su apéndice I "Process Control" y que se presentan a continuación:

PC1 Metas y objetivos del proceso

PC2 Propiedad del proceso

PC3 Repetitividad del proceso

PC4 Roles y responsabilidades

PC5 Políticas, planes y procedimientos

PC6 Mejoramiento del desempeño del proceso

La evaluación resultante de la aplicación de estos controles en cada uno de los 34 procesos de tecnología de información de Cobit 4.1 permitirá a la institución financiera determinar en cuáles de ellos hay más debilidades que se requiere corregir para prevenir situaciones no deseadas en el futuro.

Además de estos controles de procesos, el documento "IT Assurance Guide Using Cobit" provee unos conductores de valor y conductores de riesgo que permiten determinar las condiciones favorables o desfavorables para la consecución de las actividades que conforman los 34 procesos de tecnología de información; también sugiere una serie de pasos a seguir para probar el diseño de los controles que se deben aplicar a las actividades de cada proceso y evaluar la validez de su implementación. Estos tres mecanismos de evaluación que provee el documento mencionado se pueden aplicar en forma individual a cada actividad que conforma los 34 procesos de tecnología de información, y son diferentes para cada una de ellas; como dichos mecanismos también están disponibles para los controles de proceso genéricos mencionados anteriormente, se vio la conveniencia de analizar los tres mecanismos anotados y traducirlos a atributos o características específicas de los controles que deben cumplir todos los procesos Cobit, obteniendo las 24 que se indican a continuación:

Tabla 3.11: Características de los controles genéricos de procesos

Controles genéricos de procesos	Características específicas	
PC1: Metas y objetivos	1	Define y comunica metas y objetivos específicos, medibles, ejecutables, realísticos, orientados a resultados y con fechas límite
	2	Alineado con los objetivos del negocio
	3	Medido por métricas adecuadas
PC2: Propiedad	4	Existe un propietario con suficiente autoridad para cumplir roles y responsabilidades
	5	Roles y responsabilidades definidos, entendidos y aceptados
	6	La responsabilidad incluye: diseño, interacción, rendición de cuentas, medición del desempeño
PC3: Repetitividad	7	La repetitividad del proceso es un objetivo de la Administración
	8	Si el proceso es crítico, provee evidencia para revisión por parte de la Administración
	9	Se aplicaron buenas prácticas y estándares internacionales en su definición
	10	Las partes interesadas integran y son coherentes con el proceso
	11	La secuencia de sus actividades es lógica, flexible y escalable
PC4: Roles y responsabilidades	12	Las actividades clave y entregables están definidos y documentados
	13	Roles y responsabilidades no ambiguos, asignados y comunicados
	14	Roles y responsabilidades para ejecución efectiva, eficiente y documentada de actividades
	15	Está asignada la rendición de cuentas de resultados y entregables
PC5: Políticas, planes y procedimientos	16	Existen, están comunicadas, son conocidas y aplicadas
	17	Su administración incluye documentar, revisar, mantener, comunicar, y usar para capacitar
	18	Hay responsabilidad por su administración y se revisa su correcto cumplimiento periódicamente
	19	Son accesibles, correctas, entendidas y actualizadas
PC6: Mejoramiento del desempeño	20	Existen métricas que permiten percibir los resultados y desempeño del proceso con un esfuerzo limitado
	21	El diseño de las métricas permite medir la utilización de recursos, calidad de resultados y tiempos
	22	Existen procedimientos para definir marcas a cumplir en las metas del proceso y conductores de desempeño
	23	Se comparan las medidas actuales con las marcas de los logros a cumplir y se toman acciones de mejora
	24	Las métricas, marcas y métodos están alineados con el monitoreo del desempeño general de TI

Estas 24 características específicas de los controles genéricos han sido obtenidas, como se indicó anteriormente, de un análisis de las pruebas de diseño de controles, conductores de valor y conductores de riesgo que provee el documento "IT Assurance Guide Using Cobit" para los controles de proceso genéricos, considerando y seleccionando aquellos que dan el mayor valor agregado que se puede aportar al análisis de riesgos de los procesos de tecnología de información.

Estos controles genéricos y sus características específicas han sido trasladados a una hoja de cálculo en un modo matricial en el que las columnas de la matriz corresponden a los controles y las filas corresponden a los 34 procesos de tecnología de información de Cobit. En las intersecciones de esta matriz se colocarán las letras S o N para indicar "Sí" o "No" como respuesta a la evaluación del cumplimiento de dicha característica del control en el proceso de tecnología de información correspondiente. La estrictez de la presente metodología obliga a que si alguna de las características evaluadas es cumplida por la entidad solamente en forma parcial, la respuesta debe ser “No”.

Como resultado de este análisis se obtendrá una columna con el número de cumplimientos de cada proceso de tecnología de información, el mismo que se obtiene mediante la suma de un peso asignado a la letra consignada en cada celda, de la siguiente manera:

(S)í = 1

(N)o = 0

Si un proceso de tecnología de información presenta cumplimiento en todos los controles especificados en la tabla 3.9, obtendrá un valor de 24 y le corresponderá un porcentaje de 100% en el cumplimiento, mientras que si obtiene un valor menor se calculará el porcentaje correspondiente.

Para esta evaluación, además se fijará un porcentaje mínimo de criticidad o umbral de riesgo por debajo del cual los procesos de tecnología de información

deberán ser considerados críticos en la institución y por lo tanto constituyen los procesos a ser reforzados (ver tabla 3.12). El cálculo de dicho porcentaje se explica más adelante en la actividad B.4.

Tabla 3.12: Ejemplo de evaluación de controles genéricos

CONTROLES GENÉRICOS DE LOS PROCESOS DE TECNOLOGÍA DE COBIT 4.1			100%	Requerido			
			20%	No requerido			
			58.33%	Umbral de riesgo			
Dominios y procesos de tecnología de Cobit 4.1			Resultado por proceso	%	Requerido por norma de gestión del riesgo operativo	Peso absoluto	Valor Relativo
PLANEAR Y ORGANIZAR	PO1	Definir un plan estratégico de TI	24	100.00%	SI	3.70%	3.704%
	PO2	Definir la arquitectura de la información	20	83.33%	NO	1.11%	0.926%
	PO3	Determinar la dirección tecnológica	7	29.17%	SI	3.70%	1.080%
	PO4	Definir los procesos, organización y relaciones de TI	14	58.33%	SI	3.70%	2.160%
	PO5	Administrar la inversión en TI	0	0.00%	NO	1.11%	0.000%
	PO6	Comunicar las aspiraciones y la dirección de la gerencia	19	79.17%	SI	3.70%	2.932%
	PO7	Administrar recursos humanos de TI	22	91.67%	SI	3.70%	3.395%
	PO8	Administrar la calidad	0	0.00%	SI	3.70%	0.000%
	PO9	Evaluar y administrar los riesgos de TI	14	58.33%	SI	3.70%	2.160%
	PO10	Administrar proyectos	17	70.83%	NO	1.11%	0.787%
ADQUIRIR E IMPLANTAR	AI1	Identificar soluciones automatizadas	18	75.00%	NO	1.11%	0.833%
	AI2	Adquirir y mantener software aplicativo	19	79.17%	SI	3.70%	2.932%
	AI3	Adquirir y mantener infraestructura tecnológica	14	58.33%	SI	3.70%	2.160%
	AI4	Facilitar la operación y el uso	14	58.33%	SI	3.70%	2.160%
	AI5	Adquirir recursos de TI	23	95.83%	SI	3.70%	3.549%
	AI6	Administrar cambios	17	70.83%	SI	3.70%	2.623%
	AI7	Instalar y acreditar soluciones y cambios	19	79.17%	SI	3.70%	2.932%
ENTREGAR Y DAR SOPORTE	DS1	Definir y administrar los niveles de servicio	23	95.83%	NO	1.11%	1.065%
	DS2	Administrar los servicios de terceros	23	95.83%	SI	3.70%	3.549%
	DS3	Administrar el desempeño y la capacidad	15	62.50%	SI	3.70%	2.315%
	DS4	Garantizar la continuidad del servicio	18	75.00%	SI	3.70%	2.778%
	DS5	Garantizar la seguridad de los sistemas	16	66.67%	SI	3.70%	2.469%
	DS6	Identificar y asignar costos	0	0.00%	NO	1.11%	0.000%
	DS7	Educar y entrenar a los usuarios	10	41.67%	SI	3.70%	1.543%
	DS8	Administrar la mesa de servicio y los incidentes	15	62.50%	NO	1.11%	0.694%
	DS9	Administrar la configuración	16	66.67%	SI	3.70%	2.469%
	DS10	Administrar los problemas	12	50.00%	NO	1.11%	0.556%
	DS11	Administrar los datos	14	58.33%	SI	3.70%	2.160%
	DS12	Administrar el ambiente físico	19	79.17%	SI	3.70%	2.932%
	DS13	Administrar las operaciones	23	95.83%	SI	3.70%	3.549%
MONITOREAR Y EVALUAR	ME1	Monitorear y evaluar el desempeño de TI	0	0.00%	SI	3.70%	0.000%
	ME2	Monitorear y evaluar el control interno	11	45.83%	NO	1.11%	0.509%
	ME3	Garantizar el cumplimiento regulatorio	20	83.33%	SI	3.70%	3.086%
	ME4	Proporcionar gobierno de TI	15	62.50%	NO	1.11%	0.694%
		Calificación de riesgo general inicial:	**65.10%**				

Esta actividad puede ser realizada en forma paralela con las actividades de la etapa C, para hacer un análisis integral de cada uno de los procesos y

optimizar el tiempo empleado en la revisión de la documentación que sirve de soporte para la determinación de cada evaluación, tanto de los controles genéricos como de las condiciones determinadas en el modelo de madurez de Cobit y su impacto en el negocio.

Esta forma de trabajo además hará más fiables los resultados finales ya que habrá congruencia entre el porcentaje de controles aplicados a cada proceso y su respectivo nivel de madurez.

Actividad B.3: Aplicación de la homologación de los procesos de TI con la norma de riesgo operativo vigente

Para esta actividad, la hoja de cálculo en la que consta la matriz de controles provee fórmulas para ubicar en cada proceso evaluado, el requerimiento de la norma de gestión de riesgo operativo bajo las palabras “SI” o “NO”, de acuerdo con la actualización de la homologación de cada proceso de Cobit 4.1 con la mencionada norma, efectuada en la actividad A.5.

A partir del indicativo del requerimiento de la norma de gestión de riesgo operativo, la matriz de controles calcula los pesos relativos de cada proceso (ver tabla 3.10) con una distribución inicial de 80/20, acogiendo como válido el Principio de Paretto para este caso bajo la premisa de que las instituciones financieras cumplen el 80% de las regulaciones en sus procesos de tecnología de información y el 20% de controles restantes lo aplican en procesos no requeridos por la norma.

De esta forma, si el proceso es requerido por la norma se asignará el 100% de los puntos adicionales al puntaje obtenido, mientras que si el proceso no es requerido por la norma se asignará únicamente el 20% de los puntos adicionales.

Para el cálculo de los pesos absolutos de cada proceso se ha dividido el 100% que debe ser el resultado final de su suma, entre el número de respuestas afirmativas y negativas. Ya que las respuestas negativas "NO" son un porcentaje de las respuestas positivas "SI", se aplica la siguiente fórmula para el cálculo de los pesos absolutos de aquellos procesos que *sí* son requeridos por la norma de riesgo operativo:

$$\frac{100\%}{\text{Número de "SÍ" + (Número de "NO" * \% participación)}}$$

La siguiente fórmula se aplica para el cálculo de los pesos absolutos de aquellos procesos que *no* son requeridos por la norma de riesgo operativo:

Peso absoluto de "SI" * % participación de "NO"

Los valores o pesos relativos se calculan multiplicando el peso absoluto obtenido mediante las fórmulas anotadas, por el porcentaje de aplicación de controles genéricos obtenido por cada proceso evaluado.

Los valores porcentuales de participación según cada proceso sea requerido o no por la normativa, están parametrizados en la matriz de controles

bajo la relación 100% - 20%; sin embargo, estos valores deben ser aprobados por el Comité de Tecnología de Información cuando se hayan completado las etapas B y C de la metodología, por lo que los pesos relativos de los procesos podrían variar durante la ejecución de la actividad D.3.

De existir dicha variación, la misma se reflejará automáticamente en la matriz de controles debido a que sus fórmulas de cálculo están en función de las participaciones que se aprueben posteriormente.

Actividad B.4: Obtención de una calificación de riesgo general inicial de los procesos de tecnología de información

La calificación de riesgo general inicial de los procesos de tecnología de información se obtiene automáticamente a partir de las fórmulas ya integradas en la matriz de controles genéricos llenada en la actividad B.2, y se calcula mediante la suma de los pesos relativos previamente calculados para cada proceso en la actividad B.3.

La calificación de riesgo general obtenida en esta etapa (ver tabla 3.12), se la considera todavía “inicial” debido a que en la etapa D el Comité de Tecnología de Información podría aprobar valores diferentes para la participación del factor normativo dentro de la calificación final; sin embargo, proporciona una idea bastante aproximada del nivel de riesgo que presentan actualmente los procesos de tecnología de información de la entidad analizada en su conjunto, debido a la aplicación o falta de controles en dichos procesos.

Adicionalmente, la matriz de controles provista en Excel contiene una homologación entre los 24 controles genéricos evaluados y el modelo de madurez de control interno que presenta la versión 4.1 de Cobit, obteniendo valores porcentuales para los niveles 3, 4 y 5, que son los niveles aceptables para las instituciones financieras, y cuyos porcentajes representarían el nivel de criticidad o umbral de riesgo aceptado por la institución evaluada. Para el nivel 3, la homologación arrojó un valor de 58.33% que sería el valor mínimo a cumplir por una institución para considerar una aplicación adecuada de controles, pero sujeto a un apetito de riesgo mayor que para el nivel 4, cuya homologación arrojó un valor de 79.17%. El nivel 5 requiere un cumplimiento del 100% de los controles, por lo que presenta la mayor exigencia.

La hoja de cálculo provista para esta actividad tiene fijado como parámetro inicial el valor de homologación al nivel de madurez 3, es decir, el 58.33%, pero el Comité de Tecnología de Información podría aprobar un valor diferente, siempre mayor, durante la ejecución de la actividad D.3. Para facilitar el análisis de los puntajes obtenidos por cada proceso de tecnología de información, la hoja de cálculo presentará en color rojo los porcentajes de cumplimiento de los procesos evaluados que se encuentren por debajo del parámetro definido como nivel de criticidad o umbral de riesgo (ver tabla 3.12).

3.3 - Etapa C: Identificación del grado de madurez de los procesos de tecnología de información

Objetivo: Identificar el grado de madurez de los procesos de tecnología de información y su objetivo de mejoramiento mediato.

Entregable: Niveles de madurez actual y objetivo, e impacto en el negocio de cada proceso de tecnología de información.

Responsable: Equipo de proyecto designado.

En esta etapa se ha aplicado el mismo mecanismo utilizado por la fase "Prever la solución" de la metodología de implementación del gobierno de tecnología de información, contenida en el documento "IT Governance Implementation Guide Using COBIT® and Val IT™, 2nd Edition", en la que se utilizan los modelos de madurez para determinar la situación actual y la objetivo de cada proceso de tecnología de información, y la brecha existente entre las dos, y que en la presente metodología propuesta se realiza en las actividades C.1 y C.2.

Adicionalmente a estas dos actividades, la presente metodología establece la valoración del impacto que tiene cada proceso de tecnología de información en el negocio, para incluir un aspecto cualitativo que permita diferenciar en cada institución, la mayor o menor importancia que tiene cada uno de ellos en la plataforma tecnológica organizacional, y obtener un análisis final más real de la entidad.

Tabla 3.13: Actividades de la etapa C, Identificación del grado de madurez de los procesos de tecnología de información

ACTIVIDADES	ENTREGABLES	TÉCNICA / HERRAMIENTA	TIEMPO MÁXIMO	
			EFECTIVO	CON HOLGURA
C.1. Evaluación del nivel de madurez actual de cada proceso de tecnología de información.	Nivel de madurez actual de cada proceso de TI	Modelos de madurez de Cobit 4.1, plantilla en Excel	10 horas	1.5 semanas
C.2. Determinación del nivel de madurez objetivo de cada proceso de tecnología de información.	Nivel de madurez objetivo de cada proceso de TI y su brecha con el nivel actual	Modelos de madurez de Cobit 4.1, plantilla en Excel	6 horas	1 semana
C.3. Valoración del impacto de cada proceso de tecnología de información en el negocio.	Impacto de cada proceso de TI en el negocio	Plantilla en Excel	3 horas	1 semana

Actividades C.1 y C.2: Determinación de los niveles de madurez actual y objetivo de cada proceso de tecnología de información

Tal como se indicó en la actividad B.2, estas dos actividades podrían ser realizadas paralelamente con la evaluación de los controles de los procesos de tecnología de información para aprovechar el análisis que se hace de la documentación de soporte de cada proceso.

Para el desarrollo de estas actividades se requerirá utilizar los Modelos de madurez que ofrece el marco de trabajo de COBIT® 4.1 para cada uno de los procesos de tecnología de información. Debido a que estos modelos de madurez contienen gran cantidad de información, no han podido ser incluidos como un anexo de este documento, sino que se los debe utilizar directamente desde su fuente original. También es válido utilizar los modelos de madurez de la versión 4.0 de Cobit, que se encuentra disponible en español, ya que son los mismos que los de la versión 4.1, de la cual solo se ha publicado la versión en inglés.

Para su aplicación, hay que tomar en cuenta que para decidir qué nivel de madurez ha alcanzado un determinado proceso, se deben cumplir todas las condiciones que se indica en los niveles anteriores. Si una de las condiciones de un determinado nivel no se ha cumplido en el proceso analizado, entonces se ha alcanzado el nivel anterior.

Si no existe conciencia de que un proceso de tecnología de información debe existir en la entidad, entonces el nivel de madurez alcanzado será el nivel cero y ello deberá guardar relación con el porcentaje de cumplimiento de los controles evaluados en la actividad B.2, que se calificará también con cero.

Por supuesto, el nivel ideal a alcanzar como situación objetivo para cada proceso será el 5, sin embargo la brecha entre la situación actual y la objetivo puede ser muy grande y consecuentemente los esfuerzos a realizar para llegar al nivel 5 pueden ser demasiados, tornándose en un objetivo inalcanzable en el tiempo previsto y con los recursos disponibles.

Por ello, es conveniente que se vaya definiendo niveles objetivo razonables de acuerdo a la disponibilidad de recursos y factibilidad de implementación, tomando en cuenta además el nivel que ha alcanzado el segmento de instituciones similares en el mercado, como referencia (benchmark).

Los procesos que presentan un nivel de madurez de cero se mantendrán debido a que se considera que los 34 procesos de tecnología de información u objetivos de control de Cobit 4.1 son importantes de ejecutar en cada institución,

puesto que sus dominios representan el círculo de calidad de Demming que incluye: planear, hacer, evaluar y actuar. Más aún son importantes en una institución financiera, en la que sus procesos de negocio tienen gran dependencia de los procesos de tecnología de información.

Para la determinación del nivel de madurez objetivo, se deberá comparar el nivel de madurez actual frente a las metas y objetivos propuestos en el plan estratégico de tecnología de información, de modo que se obtengan resultados alineados con los objetivos de negocio. Si dicho plan estratégico contiene metas y objetivos demasiado generales, debe anotarse este hecho como una debilidad en el informe de resultados.

Los niveles de madurez actual y objetivo con las causas por las que se determinó cada nivel, deberán anotarse en la hoja electrónica cuyo formato se puede visualizar en el tabla 3.14, la misma que contiene todos los procesos a evaluar y las columnas para ubicar los niveles alcanzados.

Se incluye una columna que permite calcular la brecha existente entre los dos niveles establecidos y una adicional para elegir el impacto que tiene dicho proceso de tecnología de información en el negocio, que servirá para realizar la actividad C.3.

La última columna contiene una fórmula de verificación que permitirá garantizar que existe coherencia entre el porcentaje de cumplimiento de los

controles aplicados a un proceso y el nivel de madurez actual, y entre el nivel de madurez actual y el objetivo.

Las reglas a seguir para este verificador son las siguientes:

- El nivel de madurez objetivo no puede ser menor al actual (brecha negativa)

- Si el porcentaje de cumplimiento de controles del proceso está por debajo del nivel de criticidad, el nivel de madurez actual no puede ser mayor a 3.

- Si el porcentaje de cumplimiento de controles del proceso está por debajo del 20% del total, el nivel de madurez no puede ser mayor o igual a 2.

- Si el porcentaje de cumplimiento de controles del proceso está por encima del nivel de criticidad, el nivel de madurez actual no puede ser menor o igual a 1.

En caso de que se incurra en uno de los casos mencionados, la columna de verificación de la hoja Excel presentará una “X” en color rojo (ver tabla 3.14), la cual desaparecerá cuando se corrijan los valores que revelan la inconsistencia.

Tales inconsistencias deberán ser anotadas para reflejarlas en el informe de observaciones.

Tabla 3.14: Ejemplo de identificación del grado de madurez

Dominios y procesos de tecnología de Cobit 4.1			Nivel actual	Causa	Nivel objetivo	Causa	Brecha	Impacto			Verifica
								A	M	B	
PLANEAR Y ORGANIZAR	PO1	Definir un plan estratégico de TI	3	Causa 1	3	Causa A	0	X			✔
	PO2	Definir la arquitectura de la información	2	Causa 2	3	Causa B	1			X	✔
	PO3	Determinar la dirección tecnológica	1	Causa 3	3	Causa C	2			X	✔
	PO4	Definir los procesos, organización y relaciones de TI	2	Causa 4	3	Causa D	1	X			✔
	PO5	Administrar la inversión en TI	0	:	3	:	3		X		✔
	PO6	Comunicar las aspiraciones y la dirección de la gerencia	2	:	3	:	1	X			✔
	PO7	Administrar recursos humanos de TI	2		2		0		X		✔
	PO8	Administrar la calidad	0		2		2		X		✔
	PO9	Evaluar y administrar los riesgos de TI	1		4		3	X			✔
	PO10	Administrar proyectos	0		2		2	X			✘
ADQUIRIR E IMPLANTAR	AI1	Identificar soluciones automatizadas	3		4		1	X			✔
	AI2	Adquirir y mantener software aplicativo	3		4		1	X			✔
	AI3	Adquirir y mantener infraestructura tecnológica	3		5		2	X			✔
	AI4	Facilitar la operación y el uso	2		3		1			X	✔
	AI5	Adquirir recursos de TI	1		5		4		X		✘
	AI6	Administrar cambios	3		4		1		X		✔
	AI7	Instalar y acreditar soluciones y cambios	2		3		1	X			✔
ENTREGAR Y DAR SOPORTE	DS1	Definir y administrar los niveles de servicio	2		3		1		X		✔
	DS2	Administrar los servicios de terceros	3		4		1	X			✔
	DS3	Administrar el desempeño y la capacidad	1		4		3	X			✘
	DS4	Garantizar la continuidad del servicio	2		4		2	X			✔
	DS5	Garantizar la seguridad de los sistemas	3		4		1	X			✔
	DS6	Identificar y asignar costos	1		1		0			X	✔
	DS7	Educar y entrenar a los usuarios	2		3		1		X		✔
	DS8	Administrar la mesa de servicio y los incidentes	2		4		2			X	✔
	DS9	Administrar la configuración	2		3		1	X			✔
	DS10	Administrar los problemas	2		4		2		X		✔
	DS11	Administrar los datos	2		4		2	X			✔
	DS12	Administrar el ambiente físico	3		5		2	X			✔
	DS13	Administrar las operaciones	1		4		3	X			✘
MONIT. Y EVAL.	ME1	Monitorear y evaluar el desempeño de TI	1		2		1		X		✔
	ME2	Monitorear y evaluar el control interno	2		3		1	X			✔
	ME3	Garantizar el cumplimiento regulatorio	3		4		1	X			✔
	ME4	Proporcionar gobierno de TI	2	Causa n	3	Causa Z	1		X		✔

Actividad C.3: Valoración del impacto de cada proceso de tecnología de información en el negocio

Los valores posibles a elegir para el impacto de cada proceso de tecnología de información en los procesos de negocio son: bajo, medio y alto. Para su determinación, hay que considerar factores tales como: criticidad en cuanto a la frecuencia de realización, afectación a la continuidad de las operaciones de la institución, costos operativos asociados con dicho proceso, entrega de valor para otros procesos, dependencia para la toma de decisiones, y otros que determine la institución como elementales dependiendo de la naturaleza del proceso.

La valoración del impacto de un proceso en el negocio permite a la metodología propuesta incluir una variable cualitativa de la importancia de cada proceso, de modo que el nivel de riesgo final obtenido para cada uno de ellos sea más real para la institución evaluada. El impacto será graficado posteriormente en el mapa de riesgo tecnológico, por lo que es importante que su determinación sea lo más objetiva posible pues de ello dependerá que un proceso se encuentre en un nivel de riesgo no significativo, bajo, medio, alto o crítico.

Al finalizar la ejecución de estas tres actividades (C.1, C.2 y C.3), en la hoja electrónica provista se podrá visualizar un cuadro de resumen del número de procesos (ver tabla 3.15) que se encuentran en cada nivel de madurez y el tipo de impacto para el negocio; estos datos brindarán un panorama general de los esfuerzos a realizar para llegar a las metas fijadas y permitirán realizar un análisis

del estado de madurez de los procesos, que podrá alimentar también el informe de observaciones.

Tabla 3.15: Ejemplo de conteo de procesos por nivel de madurez e impacto

MADUREZ		Actual	Objetivo	IMPACTO	#
0	No existente	3	0	Alto	19
1	Inicial, ad/hoc, desorganizado	7	1	Medio	10
2	Repetible pero intuitivo; sigue un patrón regular	15	4	Bajo	5
3	Definido; documentado y comunicado	9	13		
4	Administrado y medido	0	13		
5	Optimizado; automatizado	0	3		
	TOTAL:	34	34		34

3.4 - Etapa D: Obtención del mapa de riesgo tecnológico

Objetivo: Obtener un mapa de riesgo tecnológico que indique el riesgo alcanzado por cada proceso de tecnología de información.

Entregable: Mapa de evaluación de la tecnología de información.

La ejecución de las etapas B y C de la metodología propuesta han permitido obtener algunas variables para cada proceso de tecnología de información, que incluyen:

- Porcentaje de aplicación de controles en cada proceso
- Indicativo de que el proceso esté o no requerido por la normativa vigente
- Calificación de riesgo general inicial de la aplicación de controles a los procesos
- Nivel de madurez actual de cada proceso
- Nivel de madurez objetivo de cada proceso
- Brecha del nivel de madurez de cada proceso

- Impacto de cada proceso de tecnología de información en los procesos del negocio

Estas variables dan una medida de las evaluaciones realizadas a los procesos de tecnología de información de una institución, las cuales por sí mismas ya brindan un indicativo para reforzar aquellos procesos que se hayan determinado como críticos para el desenvolvimiento de las operaciones de la entidad.

Sin embargo, una consolidación de dichas variables puede ser realizada empleando una de las herramientas que ha tenido mayor éxito en la administración de riesgos a nivel mundial, que son los mapas de riesgo.

Para el tema que nos ocupa, se considerará la elaboración de un mapa de riesgo tecnológico que permita conocer el nivel de riesgo alcanzado por cada uno de los procesos de tecnología de información evaluado, y una calificación de riesgo tecnológico de cada dominio de Cobit 4.1 que constituya una guía en cuanto a la identificación del grupo de procesos que se encuentra más débil o más fuerte con respecto a la calificación alcanzada por cada uno de sus procesos de tecnología de información.

Otro factor que se ha incluido en la elaboración del mapa de riesgo tecnológico es el riesgo institucional. Este factor permitirá ubicar a cada institución en uno de los tres segmentos de riesgo que se graficará en el eje de las Y, mientras que el eje de las X contendrá la calificación de riesgo alcanzada

por cada uno de los procesos de tecnología de información, obtenida de la ejecución de las etapas anteriores de la metodología.

Se han analizado diferentes variables para seleccionar aquella que pueda representar adecuadamente el riesgo institucional, que han ido desde la concentración de los depósitos de los 100 mayores clientes, la solvencia patrimonial, la participación de los activos y pasivos con respecto al subsistema al que pertenece cada institución, indicadores de eficiencia microeconómica, y otros datos financieros que finalmente no han logrado describir el riesgo institucional que se pretende plasmar en la presente metodología, debido a que el riesgo tecnológico no depende, como se ha visto en la experiencia laboral, de indicadores financieros o económicos, sino de la gestión en sí de la tecnología de la información y de la dependencia tecnológica que tiene cada institución del total de sus transacciones operativas.

Por ello, el eje Y del mapa de evaluación del riesgo tecnológico estará representado por el riesgo institucional en términos de la mayor o menor automatización que tenga cada entidad, independientemente de su tamaño, solvencia o tipo de institución de que se trate.

El hecho de considerar el riesgo institucional para la obtención del mapa de riesgo tecnológico presenta la ventaja de que los riesgos asociados a cada uno de sus procesos se ajustarán en función de la mayor o menor dependencia que tenga la institución en la tecnología de información, por lo que las

recomendaciones o acciones sugeridas de mejora también variarán en ese sentido.

Para el equipo de proyecto, las actividades a desarrollar en esta etapa son básicamente de recolección de información, ya que el mapa de riesgo tecnológico con sus fórmulas de cálculo y gráficos ya está provisto por la presente metodología en una hoja electrónica en Excel.

De esta manera, la ejecución de las etapas anteriores servirá para alimentar los datos requeridos para ubicar el riesgo alcanzado por cada proceso de tecnología de información en el mapa de evaluación.

Tabla 3.16: Actividades de la etapa D, Obtención del mapa de riesgo tecnológico

ACTIVIDADES	ENTREGABLES	TÉCNICA / HERRAMIENTA	TIEMPO MÁXIMO	
			EFECTIVO	CON HOLGURA
D.1. Elaboración de un cuadro de evaluación de cada proceso de tecnología de información.	Cuadro de evaluación de los procesos de tecnología de información (eje X del mapa)	Aplicación de fórmulas	1 minuto	1 minuto
D.2. Cálculo del riesgo institucional.	Segmento del riesgo institucional (eje Y del mapa)	Entrevistas a jefes departamentales	2 horas	3 días
D.3. Revisión y aprobación de pesos de factores de la calificación final.	Porcentajes de participación de cada factor de calificación	Reunión del Comité de Tecnología de Información	30 minutos	3 días
D.4. Obtención del mapa de riesgo tecnológico.	Mapa de evaluación del riesgo tecnológico	Aplicación de fórmulas	1 minuto	1 minuto
D.5. Aprobación de las etapas B, C y D.	Acta de aprobación de las etapas B, C y D, por parte del Comité de Tecnología de Información	Revisión de los entregables de las etapas B, C y D	30 minutos	3 días

Actividad D.1: Elaboración de un cuadro de evaluación de cada proceso de tecnología de información

El cuadro de evaluación de cada proceso de tecnología de información se encuentra listo para su utilización en la hoja electrónica provista por esta metodología. A continuación se describen los cálculos que se efectúan en ella:

Para la obtención de una calificación de riesgo para cada proceso de tecnología de información se han identificado cuatro factores: el porcentaje de cumplimiento de los controles genéricos, el requerimiento por la norma, el estado de madurez y la brecha de madurez.

Tomando nuevamente como base el Principio de Paretto, se ha considerado una participación del 80% para los factores que representan el cumplimiento de controles genéricos y el 20% para los factores que representan la madurez de cada proceso. Dentro de estos dos grupos, igualmente se ha considerado una participación 80/20 para cada factor, según se resume en la siguiente tabla:

Tabla 3.17: Participación absoluta y relativa de los factores de calificación

Factor evaluado	Participación total	Participación relativa	Participación absoluta
Cumplimiento de controles genéricos:	80%	80%	64.00%
Requerido por norma:		20%	16.00%
Estado de madurez:	20%	80%	16.00%
Brecha de madurez:		20%	4.00%
TOTAL	100.00%		100.00%

El puntaje de la aplicación de los controles genéricos corresponde al obtenido en la ejecución de la actividad B.3. El valor máximo a obtener en este factor constituye el 64.00% del puntaje total del proceso.

El puntaje del requerimiento por norma tendrá un puntaje de cero (0) cuando la aplicación de controles genéricos también tenga cero, en caso contrario tendrá un puntaje de 16 si dicho proceso de tecnología de información está requerido por la norma de riesgo operativo, y de su 20% si no lo está, es decir, 3.20 puntos.

El puntaje del estado de madurez se obtiene del nivel actual de madurez que se ha definido en la actividad C.1 de esta metodología multiplicado por 0.20 ya que son 5 niveles de madurez y se les ha dado un puntaje de 20% por cada uno. Luego se obtiene el 16% de dicho valor, con lo cual se consigue una participación de hasta 16 puntos en el puntaje total del proceso.

El puntaje de la brecha de madurez se obtiene multiplicando la brecha por 0.20 y restándolo de 1 para obtener el puntaje positivo de la brecha (0 es bueno y 5 es malo). Luego se obtiene el 4% de dicho valor, con lo cual se consigue una participación que corresponde al 25% del estado de madurez (factor anterior), y que representa el 4% del puntaje total del proceso. Este puntaje se adquiere únicamente cuando la brecha es 0, 1 ó 2, pues se considera que una brecha mayor no es un aspecto positivo para la calificación del proceso.

Tanto para el factor correspondiente al estado de madurez actual como para la brecha, se asigna un puntaje de cero si el factor de cumplimiento de controles genéricos también es igual a cero.

Para cada proceso de tecnología de información, se efectúa la suma de los puntajes obtenidos en cada factor evaluado y se lo resta de 1 para obtener el porcentaje de riesgo; luego, en base a la siguiente tabla, se calcula la calificación de riesgo que se graficará en el eje X del mapa de riesgo tecnológico y que va de 1 a 9:

Tabla 3.18: Asignación de calificaciones de acuerdo a percentiles

Banda superior (percentiles)	Calificación de riesgo (Eje "X")
11%	1
22%	2
33%	3
44%	4
56%	5
67%	6
78%	7
89%	8
100%	9

Con la calificación de riesgo del eje "X", ya se cuenta con la información necesaria para preparar el cuadro de resumen de calificación por proceso que servirá de base para elaborar el mapa de riesgo tecnológico. Un ejemplo de este resumen se encuentra en la tabla 3.19.

Tabla 3.19: Resumen de calificación por proceso con datos de ejemplo

Dominios y procesos de tecnología de Cobit 4.1			Puntaje cumplim. de controles	Puntaje factor normativo	Puntaje estado de madurez	Puntaje brecha de madurez	TOTAL	Riesgo alcanzado	Calif. de riesgo "X"
PLANEAR Y ORGANIZAR	PO1	Definir un plan estratégico de TI	64.00	16.00	9.60	4.00	93.60	6.40%	1
	PO2	Definir la arquitectura de la información	53.33	3.20	6.40	3.20	66.13	33.87%	4
	PO3	Determinar la dirección tecnológica	18.67	16.00	3.20	2.40	40.27	59.73%	6
	PO4	Definir los procesos, organización y relaciones de TI	37.33	16.00	6.40	3.20	62.93	37.07%	4
	PO5	Administrar la inversión en TI	-	-	-	-	-	100.00%	9
	PO6	Comunicar las aspiraciones y la dirección de la gerencia	50.67	16.00	6.40	3.20	76.27	23.73%	3
	PO7	Administrar recursos humanos de TI	58.67	16.00	6.40	4.00	85.07	14.93%	2
	PO8	Administrar la calidad	-	-	-	-	-	100.00%	9
	PO9	Evaluar y administrar los riesgos de TI	37.33	16.00	3.20	-	56.53	43.47%	4
	PO10	Administrar proyectos	45.33	3.20	-	2.40	50.93	49.07%	5
ADQUIRIR E IMPLANTAR	AI1	Identificar soluciones automatizadas	48.00	3.20	9.60	3.20	64.00	36.00%	4
	AI2	Adquirir y mantener software aplicativo	50.67	16.00	9.60	3.20	79.47	20.53%	2
	AI3	Adquirir y mantener infraestructura tecnológica	37.33	16.00	9.60	2.40	65.33	34.67%	4
	AI4	Facilitar la operación y el uso	37.33	16.00	6.40	3.20	62.93	37.07%	4
	AI5	Adquirir recursos de TI	61.33	16.00	3.20	-	80.53	19.47%	2
	AI6	Administrar cambios	45.33	16.00	9.60	3.20	74.13	25.87%	3
	AI7	Instalar y acreditar soluciones y cambios	50.67	16.00	6.40	3.20	76.27	23.73%	3
ENTREGAR Y DAR SOPORTE	DS1	Definir y administrar los niveles de servicio	61.33	3.20	6.40	3.20	74.13	25.87%	3
	DS2	Administrar los servicios de terceros	61.33	16.00	9.60	3.20	90.13	9.87%	1
	DS3	Administrar el desempeño y la capacidad	40.00	16.00	3.20	-	59.20	40.80%	4
	DS4	Garantizar la continuidad del servicio	48.00	16.00	6.40	2.40	72.80	27.20%	3
	DS5	Garantizar la seguridad de los sistemas	42.67	16.00	9.60	3.20	71.47	28.53%	3
	DS6	Identificar y asignar costos	-	-	-	-	-	100.00%	9
	DS7	Educar y entrenar a los usuarios	26.67	16.00	6.40	3.20	52.27	47.73%	5
	DS8	Administrar la mesa de servicio y los incidentes	40.00	3.20	6.40	2.40	52.00	48.00%	5
	DS9	Administrar la configuración	42.67	16.00	6.40	3.20	68.27	31.73%	3
	DS10	Administrar los problemas	32.00	3.20	6.40	2.40	44.00	56.00%	6
	DS11	Administrar los datos	37.33	16.00	6.40	2.40	62.13	37.87%	4
	DS12	Administrar el ambiente físico	50.67	16.00	9.60	2.40	78.67	21.33%	2
	DS13	Administrar las operaciones	61.33	16.00	3.20	-	80.53	19.47%	2
MONITOREAR Y EVALUAR	ME1	Monitorear y evaluar el desempeño de TI	-	-	-	-	-	100.00%	9
	ME2	Monitorear y evaluar el control interno	29.33	3.20	6.40	3.20	42.13	57.87%	6
	ME3	Garantizar el cumplimiento regulatorio	53.33	16.00	9.60	3.20	82.13	17.87%	2
	ME4	Proporcionar gobierno de TI	40.00	3.20	6.40	3.20	52.80	47.20%	5
		PARTICIPACIÓN ABSOLUTA:	**64.00%**	**16.00%**	**16.00%**	**4.00%**	100.00%		
		PUNTAJE MÁXIMO:	64.00	16.00	16.00	4.00	100.00		
		MÌNIMO SOBRE CERO:	2.67	**3.20**	3.20	2.40	11.47		

Adicionalmente, para contar con información consolidada por cada dominio de Cobit, se suma la calificación de riesgo “X” de todos los procesos de tecnología

de información que conforman cada dominio, y se lo divide para el total máximo a alcanzar como riesgo para dicho dominio, lo que da como resultado un porcentaje de riesgo que se asocia a una calificación de acuerdo con los percentiles de la tabla 3.14. Para los datos de ejemplo de la tabla 3.19, se ha realizado el cálculo de las calificaciones por dominio de Cobit, que se puede ver en la tabla 3.20.

Tabla 3.20: Ejemplo de calificaciones por dominio de Cobit

RIESGO POR DOMINIO DE COBIT 4.1	Calif. de riesgo "X"	Número de procesos	Máximo a alcanzar	% alcanzado	Calificación del dominio
PLANEAR Y ORGANIZAR	46	10	90	51.11%	5
ADQUIRIR E IMPLANTAR	22	7	63	34.92%	4
ENTREGAR Y DAR SOPORTE	49	13	117	41.88%	4
MONITOREAR Y EVALUAR	22	4	36	61.11%	6

Una vez que se cuenta con la calificación por cada dominio de Cobit, se obtiene la calificación general de la institución sumando el producto del número de procesos y la calificación de cada dominio, y esta suma se divide entre 34 que es el número total de procesos de tecnología de información. Para los datos de ejemplo mostrados en la tabla 3.16, el resultado de este cálculo es de 4.53, que trasladado a un nivel de riesgo nos da un riesgo “medio”.

Las escalas utilizadas para determinar los niveles de riesgo se muestran en la tabla 3.21, y fueron elaboradas utilizando la fórmula de longitud de clases: (valor máximo – valor mínimo) / número de clases = (9 – 1) / 5 = 1.6.

Tabla 3.21: Escalas de nivel de riesgo

Escalas		Nivel de riesgo
Desde	**Hasta**	
1	2.6	No significativo
2.6	4.2	Bajo
4.2	5.8	Medio
5.8	7.4	Alto
7.4	9	Crítico

Como se puede ver, al finalizar esta actividad se cuenta con tres tipos de datos: la calificación de riesgo de cada proceso, la calificación de riesgo de cada dominio de Cobit, y la calificación de riesgo general de la institución, los cuales pueden servir para elaborar gráficos comparativos si se cuenta con datos de varias instituciones o de la misma institución en fechas diferentes que permitan visualizar su evolución en el tiempo.

Actividad D.2: Cálculo del riesgo institucional

El eje "Y" del mapa de evaluación del riesgo tecnológico está representado por el riesgo institucional, el mismo que, como se explicó anteriormente, está en función de la mayor o menor dependencia que tiene la institución frente a la tecnología de información y se establece mediante la relación existente entre el número de procesos, operaciones o transacciones mensuales automatizadas frente al total, incluyendo las operaciones o procesos que se ejecutan manualmente.

Debido a que la presente metodología está orientada a las instituciones del sistema financiero ecuatoriano, por la experiencia laboral se considera que ninguna de ellas tiene una automatización menor al 60% de su total de procesos de negocio, por lo que el rango de 60% a 100% se ha dividido en tres segmentos a efectos de reflejarlos en el eje "Y" del mapa de riesgo tecnológico. Estos tres segmentos se obtuvieron calculando 3 percentiles entre 60% y 100% que

representan al riesgo institucional “bajo” en el segmento 1, al riesgo institucional “medio” en el segmento 2 y al riesgo institucional “alto” en el segmento 3.

El valor calculado como riesgo institucional será asociado automáticamente a uno de dichos tres segmentos en el mapa de riesgo tecnológico. Para la determinación del número de procesos u operaciones automatizadas frente al total, es importante que la institución tenga al menos inventariados, si no relevados, sus procesos de negocio, y se conozca el grado de automatización que tiene cada uno de ellos. Si no existe dicho inventario de procesos, el cálculo puede efectuarse considerando el inventario de áreas o departamentos de negocio y determinando su grado de automatización y su frecuencia, es decir, el número de operaciones que se realiza en cada una de ellas en forma mensual. Un ejemplo de los datos a ingresar para este cálculo se puede visualizar en la tabla 3.22.

Tabla 3.22: Ejemplo de cálculo del riesgo institucional

RIESGO INSTITUCIONAL (EJE "Y")		
	Desde	**Hasta**
Riesgo institucional bajo:	60.00%	73.33%
Riesgo institucional medio:	73.34%	87.67%
Riesgo institucional alto:	87.68%	100.00%
	Frecuencia	**% automatización**
Proceso / área 1	1,500.00	90.00%
Proceso / área 2	2,000.00	50.00%
Proceso / área 3	10.00	84.00%
Proceso / área 4	850.00	85.00%
Proceso / área 5	3,000.00	75.00%
Proceso / área 6		
Proceso / área 7		
Proceso / área 8		
Proceso / área 9		
Proceso / área 10		
TOTAL FRECUENCIA:	7,360.00	
PORCENTAJE DE AUTOMATIZACIÓN DE LA ENTIDAD:		72.43%
Riesgo institucional bajo, segmento:		1

Para el ejemplo anotado, el riesgo institucional se encuentra dentro del segmento 1. Cada uno de los tres segmentos que se ubican en el eje "Y" del mapa, se subdividen en tres secciones que corresponden al impacto que tiene cada proceso de tecnología de información en el negocio, dando como resultado 9 cuadrantes en el eje "Y", al igual que en el eje "X". Para el caso del ejemplo, las calificaciones de riesgo (eje "X") obtenidas por cada uno de los procesos de TI se ubicarán en las tres secciones del segmento 1 según el impacto que tenga cada uno de ellos: alto, medio o bajo. Esta asignación también se hará automáticamente mediante las fórmulas ingresadas en la hoja electrónica que contiene el mapa de evaluación del riesgo tecnológico.

Nótese que al ir subiendo de segmento en el eje "Y", las mismas calificaciones de riesgo del eje "X" producen un efecto de exigencia mayor en cuanto al nivel de riesgo alcanzado, por lo que una calificación de riesgo de 9 que en el segmento 1 representa un nivel de riesgo "medio", representaría un nivel de riesgo "crítico" si la misma estuviese en el segmento 3.

Actividad D.3: Revisión y aprobación de pesos de factores de la calificación final

En esta actividad el Comité de Tecnología de Información deberá revisar y aprobar los pesos o porcentajes de participación que tendrá cada uno de los factores que intervienen en la obtención de la calificación de riesgo final.

Los pesos o porcentajes de participación a revisar y aprobar son aquellos que se explicaron en la actividad D.1, que se resumen al final de la tabla 3.19 y cuyo fragmento se presenta en la tabla 3.23. Pese a la sencillez que aparenta tener esta actividad de revisión y aprobación, la misma es de suma importancia pues de ella depende la forma en que se varíen o no los pesos relativos asociados a cada proceso de tecnología de información en la matriz de evaluación de controles (actividad B.3), y por consiguiente, la calificación de riesgo general inicial de dichos procesos, que luego de esta actividad se convertirá en la definitiva.

Así mismo, un cambio en los porcentajes de participación de cada uno de los factores que intervienen en la calificación final hará variar las calificaciones de riesgo por proceso, por dominio y general de la institución.

Tabla 3.23: Participación de factores de calificación a aprobar

	Puntaje cumplim. de controles	Puntaje factor normativo	Puntaje estado de madurez	Puntaje brecha de madurez	Puntaje total
PARTICIPACIÓN ABSOLUTA:	**64.00%**	**16.00%**	**16.00%**	**4.00%**	100.00%
PUNTAJE MÁXIMO:	64.00	16.00	16.00	4.00	100.00
MÌNIMO SOBRE CERO:	2.67	**3.20**	3.20	2.40	11.47

Solo aquellos valores remarcados en negrilla en la tabla 3.23 podrán ser modificados por el Comité de Tecnología de Información.

Cada proceso de tecnología de información se califica sobre 100 puntos. La participación en valores porcentuales está traducida a un puntaje en números reales en la línea titulada “puntaje máximo”, y su total debe sumar 100 puntos;

estos valores no pueden ser modificados en la hoja electrónica sino que se actualizarán en forma automática mediante las fórmulas que contienen sus celdas, las cuales corresponden a la multiplicación de 100 por el porcentaje de participación absoluta (fila 1) de cada columna.

En el caso de que el Comité de Tecnología de Información decida hacer variaciones sobre los porcentajes de participación absoluta, deberá considerar la restricción de que la suma de los cuatro factores deben sumar 100%; si dicho total es diferente a 100%, la hoja de cálculo mostrará el valor en color rojo hasta que se corrijan los porcentajes ingresados.

La fila titulada “Mínimo sobre cero” muestra los valores que adquirirá un proceso en el caso de que se le esté aplicando al menos un control genérico y tenga un nivel de madurez mínimo de 1. En esta fila (3), la segunda columna es la única que el Comité de Tecnología de Información podría variar, y corresponde al valor que se asignará al proceso en el caso de que no esté requerido por la norma de riesgo operativo.

El valor de 3.2 corresponde al 20% del 16%, que es el puntaje a obtener en el caso de que el proceso sí esté requerido por la norma. Si se hace un cambio a este valor, la hoja de cálculo determinará la relación entre ambos valores (16% y el nuevo valor) y aplicará dicho porcentaje a los pesos relativos asignados a cada proceso en la matriz de evaluación de controles genéricos, haciendo variar la calificación de riesgo inicial de cada proceso, que se obtuvo en la actividad B.3.

Adicionalmente, el Comité de Tecnología de Información deberá aprobar el nivel de criticidad o umbral de riesgo que inicialmente se encuentra fijado en 58.33% y que se explicó en la actividad B.4.

Esto corresponderá al apetito de riesgo institucional y a la disponibilidad de recursos con que la entidad cuente para poner a buen resguardo los procesos de tecnología de información que resulten críticos por encontrarse por debajo del cumplimiento mínimo fijado por el umbral de riesgo.

Una vez aprobados los porcentajes indicados, el Comité de Tecnología de Información deberá suscribir un acta para formalizar la actividad y así evitar que en lo posterior se realicen modificaciones no autorizadas a los datos aprobados. A partir de este momento, ya se puede obtener el mapa de riesgo tecnológico que se explica en la siguiente sección.

Actividad D.4: Obtención del mapa de riesgo tecnológico

Como se ha explicado anteriormente, el mapa de riesgo tecnológico consta de 9 cuadrantes en el eje “X” y 9 cuadrantes en el eje “Y”, dando un total de 81 cuadrantes que se los ha distribuido en cinco niveles de riesgo identificados con diferentes colores para representar el riesgo alcanzado por cada proceso de tecnología de información, los mismos que se describen en la tabla 3.24.

Tabla 3.24: Niveles de riesgo y colores asociados

NIVEL DE RIESGO	DESCRIPCIÓN	COLOR
Riesgo no significativo	La probabilidad de ocurrencia de un evento de riesgo es casi inexistente, y de ocurrir, no generará una pérdida económica o impacto en el negocio.	Blanco
Riesgo bajo	Existe una probabilidad baja de ocurrencia de un evento de riesgo que puede ocasionar una pérdida económica asumible por la entidad y con una afectación no perceptible en los procesos de negocio.	Verde
Riesgo medio	La probabilidad de ocurrencia de un evento de riesgo es real, pero su impacto en el negocio o las pérdidas ocasionadas pueden ser manejados por la entidad en el mediano plazo, sin llegar a tener interrupciones significativas en los servicios informáticos.	Amarillo
Riesgo alto	La recuperación de un evento de riesgo en la entidad es costosa y puede ocasionar la interrupción de los servicios informáticos por un tiempo significativo para el negocio.	Anaranjado
Riesgo crítico	Existe una inminente probabilidad de ocurrencia de un riesgo con las consecuentes pérdidas económicas e impactos que desestabilizarán las operaciones de negocio.	Rojo

Durante la investigación de la elaboración de mapas de riesgo en los ámbitos tecnológico y financiero, se pudo determinar que la asociación entre los niveles de riesgo y los cuadrantes del mapa la realizan conjuntamente el propietario de cada proceso evaluado y un auditor informático, quienes se basan en la probabilidad de ocurrencia de un riesgo y el impacto para el negocio, y por lo general utilizan la función Multiplicación para definir rangos en dicha asociación.

Esta forma de distribución de los niveles de riesgo puede producir resultados subjetivos en el mapa de riesgos, por lo que en la presente metodología los cinco niveles de riesgo definidos en la tabla 3.24 se han ubicado en los 81 cuadrantes del mapa mediante una distribución de frecuencias de la función Suma.

Para utilizar la función Suma, se sumaron los valores de los ejes X e Y para cada uno de los cuadrantes, obteniendo un valor mínimo de 2 y un máximo de 18, que generaron una longitud de clase de 3.20 para 5 clases, tal como se muestra en la tabla 3.25.

Tabla 3.25: Clases y distribución de frecuencias de la función Suma

Longitud de clase:		3.20	Frecuencia absoluta	Frec. absol. acumulada	Frecuencia relativa	Frec. relat. acumulada
Mínimo	**Máximo**	**Clase**				
2	5.20	1	10	10	12.35%	12.35%
5.21	8.41	2	18	28	22.22%	34.57%
8.42	11.62	3	25	53	30.86%	65.43%
11.63	14.83	4	18	71	22.22%	87.65%
14.84	18.04	5	10	81	12.35%	100.00%

Asociando los valores de cada cuadrante del mapa a las 5 clases de la tabla 3.25, se obtuvo la siguiente distribución de niveles de riesgo:

Tabla 3.26: Mapa con niveles de riesgo distribuidos con la función Suma

9	10	11	12	13	14	15	16	17	18
8	9	10	11	12	13	14	15	16	17
7	8	9	10	11	12	13	14	15	16
6	7	8	9	10	11	12	13	14	15
5	6	7	8	9	10	11	12	13	14
4	5	6	7	8	9	10	11	12	13
3	4	5	6	7	8	9	10	11	12
2	3	4	5	6	7	8	9	10	11
1	2	3	4	5	6	7	8	9	10
	1	2	3	4	5	6	7	8	9

El mismo procedimiento se aplicó a la función MULTIPLICACIÓN para comparar los resultados con los de la función SUMA y determinar cuál de las dos se adapta mejor a los niveles de riesgo esperados, obteniendo la siguiente distribución:

Tabla 3.27: Clases y distribución de frecuencias de la función Multiplicación

9	9	18	27	36	45	54	63	72	81
8	8	16	24	32	40	48	56	64	72
7	7	14	21	28	35	42	49	56	63
6	6	12	18	24	30	36	42	48	54
5	5	10	15	20	25	30	35	40	45
4	4	8	12	16	20	24	28	32	36
3	3	6	9	12	15	18	21	24	27
2	2	4	6	8	10	12	14	16	18
1	1	2	3	4	5	6	7	8	9
	1	2	3	4	5	6	7	8	9

Al representar las funciones Suma y Multiplicación en una curva de distribución de frecuencias de los niveles de riesgo del mapa, se obtuvo las figuras 3.1 y 3.2 que se muestran a continuación:

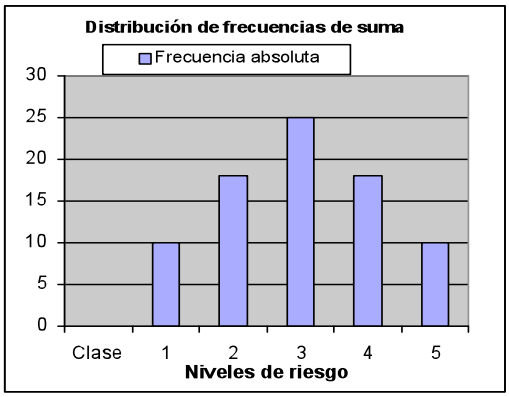


Figura 3.1: Gráfico de la función Suma

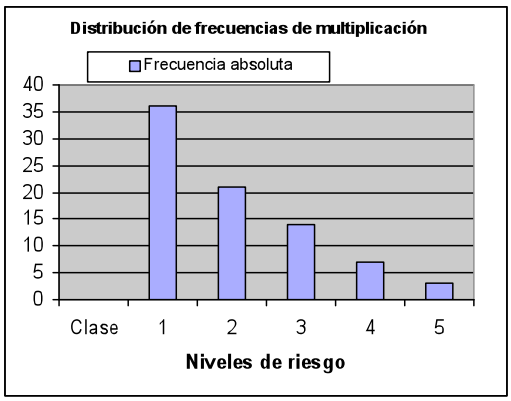


Figura 3.2: Gráfico de la función Multiplicación

Como se puede apreciar, la función Multiplicación presenta una distribución de frecuencias con un sesgo pronunciado hacia el nivel de riesgo “no significativo” y una mínima frecuencia para el riesgo “crítico”, mientras que la función Suma presenta una distribución de curva normal que proporciona una clasificación más equitativa de los niveles de riesgo, por lo que se adoptó la misma para el mapa de riesgo tecnológico de esta metodología.

Tanto para el eje X como para el eje Y, se considera que a mayor valor, mayor riesgo, por lo que al aplicar los cálculos descritos y asociarlos a los colores que los representan, los niveles de riesgo distribuidos en los cuadrantes del mapa quedan como se muestra en la tabla 3.26. En la figura 3.3 se muestra un mapa de riesgos con datos de ejemplo, y los colores asociados a cada nivel de riesgo.

A partir del cuadro de resumen de la calificación mostrado en la tabla 3.19, se utilizan fórmulas para búsqueda, extracción y unión de textos en Excel para colocar en cada uno de los cuadrantes del mapa las siglas que emplea la versión 4.1 de Cobit para sus procesos. Para ello se considera el segmento de riesgo institucional, la calificación de riesgo obtenida, y el impacto definidos para cada proceso de tecnología de información.

MAPA DE EVALUACIÓN DEL RIESGO TECNOLÓGICO

ENTIDAD:

FECHA DE CORTE:

RIESGO INSTITUCIONAL		Impacto									
	100%	Alto									
		Medio									
		Bajo									
	87.7%	Alto									
		Medio									
		Bajo									
	73.3%	Alto	PO1 DS2	AI2 DS12 DS13 ME3	PO6 AI7 DS4 DS5 DS9	PO4 PO9 AI1 AI3 DS3 DS11	PO10	ME2			
		Medio		PO7 AI5	AI6 DS1		DS7 DS10 ME4				PO5 PO8 ME1
		Bajo			PO2	AI4	DS8	PO3			DS6
	60%	0	1	2	3	4	5	6	7	8	9

CALIFICACIÓN DE RIESGO ALCANZADA POR CADA PROCESO DE TI

No significativo | Bajo | Medio | Alto | Crítico

Figura 3.3: Mapa de evaluación del riesgo tecnológico con datos de ejemplo

Los usuarios de la presente metodología en realidad solo tendrán que limitarse a realizar un análisis de los datos presentados en el mapa de evaluación del riesgo tecnológico, ya que como se ha explicado anteriormente, la hoja electrónica que se provee con este documento, contiene todas las fórmulas y datos requeridos para su generación, los cuales provienen de la ejecución de las actividades anteriores.

Actividad D.5: Aprobación de las etapas B, C y D

Una vez obtenido el mapa de riesgo tecnológico, es necesario formalizar las actividades desarrolladas en las etapas B, C y D mediante la revisión y aprobación por parte del Comité de Tecnología de Información de los entregables derivados de cada una de las actividades que las conforman.

Cabe indicar que en esta etapa dicha revisión y aprobación es aún más importante puesto que en la siguiente etapa se elaborará el informe de los resultados obtenidos que se encuentran reflejados en el mapa de evaluación del riesgo tecnológico, por lo que si ameritase hacer alguna corrección o actualización de datos, es en este momento en que se lo debe realizar.

Una vez obtenida la conformidad por parte del Comité de Tecnología de Información, se deberá elaborar un acta con los comentarios y correctivos que hayan surgido del análisis de los datos obtenidos hasta esta etapa, lo cual garantizará que la responsabilidad de todas las actividades hasta aquí desarrolladas son de dicho Comité y no solo del equipo de proyecto asignado.

3.5 - Etapa E: Elaboración del informe de evaluación

Objetivo: Elaborar el informe final con los resultados de la aplicación de la metodología propuesta.

Entregable: Informe de evaluación del riesgo tecnológico dirigido al Comité de Tecnología de Información.

Responsable: Asesor o auditor informático del proyecto.

Tiempo máximo: Dos semanas.

Por tratarse de un documento que comunica a la alta gerencia los resultados de la aplicación de la metodología propuesta, el informe debe ser redactado de modo objetivo, claro, preciso, verificable, suficiente y no ambiguo, y debe contener como mínimo los siguientes aspectos:

- **Título:** "Informe de evaluación del riesgo tecnológico"

- **Nombre de la institución evaluada**

- **Fecha de inicio del proyecto**

- **Alcance:** Mencionar los 34 procesos de tecnología de información de Cobit 4.1, sobre los cuales se ha efectuado un diagnóstico, una evaluación de los controles genéricos aplicados, una valoración de su requerimiento legal, la

determinación del grado de madurez alcanzado y esperado y la especificación de su impacto en el negocio.

- **Restricciones del alcance:** situaciones que impidieron realizar determinadas actividades de acuerdo con la planificación efectuada.

- **Resultados:** Deben recolectarse los entregables de las etapas A, B, C y D y exponerse los resultados relacionando las temáticas anotadas en el Alcance: Diagnóstico, análisis de la deficiente aplicación de controles a los procesos críticos y su influencia en la calificación final, un resumen de la calificación de riesgo obtenida por cada proceso de tecnología de información, el mapa de riesgo tecnológico, y el gráfico de la curva de distribución del conteo de procesos de acuerdo a la calificación obtenida.

Estos aspectos permitirán analizar de modo macro la situación actual del riesgo tecnológico. Adicionalmente se deberá detallar las observaciones y recomendaciones de los procesos que se encuentren en una situación de riesgo relevante para la institución.

La relevancia se debe establecer considerando las siguientes condiciones:

- El proceso se encuentra en un nivel de riesgo crítico, alto o medio. Se excluyen los procesos que se encuentran en los niveles inferiores.
- El proceso no es requerido por la norma de riesgo operativo pero se encuentra por debajo del umbral de riesgo del nivel de madurez 3.

- El proceso sí es requerido por la norma de riesgo operativo y se encuentra por debajo del umbral de riesgo del nivel inmediato superior al definido por la entidad, es decir, los asociados a los niveles de madurez 4 ó 5 según corresponda.

Las observaciones deberán indicar el riesgo que se deriva de la situación de riesgo del proceso. Para la elaboración de las recomendaciones, se debe tomar en cuenta las mejores prácticas definidas por Cobit en los modelos de madurez, que permitan alcanzar el nivel de madurez objetivo definido para cada proceso de tecnología de información.

- **Plan de acción:** para obtener resultados concretos, es deseable el establecer un calendario con fechas máximas de ejecución de las recomendaciones efectuadas, que permitan hacer un seguimiento posterior de su cumplimiento.

- **Conclusión:** se deberá realizar un resumen gerencial sobre los aspectos que tengan mayor relevancia en la calificación obtenida y las sugerencias que permitan mitigar los riesgos tecnológicos encontrados, así como las posibles consecuencias de su no aplicación a mediano y largo plazo. Esta conclusión debe estar contenida en un máximo de una página.

- **Lugar, fecha y firma:** el informe debe ser elaborado y firmado por el auditor informático o asesor del proyecto, y remitido al Comité de

Tecnología de Información para su conocimiento y seguimiento de las acciones de mejora para verificar su cumplimiento.

3.6- Soporte de la herramienta informática

Como se ha ido explicando a lo largo de este capítulo, el libro Excel que se ha desarrollado para dar soporte a la metodología propuesta, facilita el registro de las actividades realizadas y los cálculos matemáticos requeridos. Este libro está dividido en las siguientes hojas de cálculo:

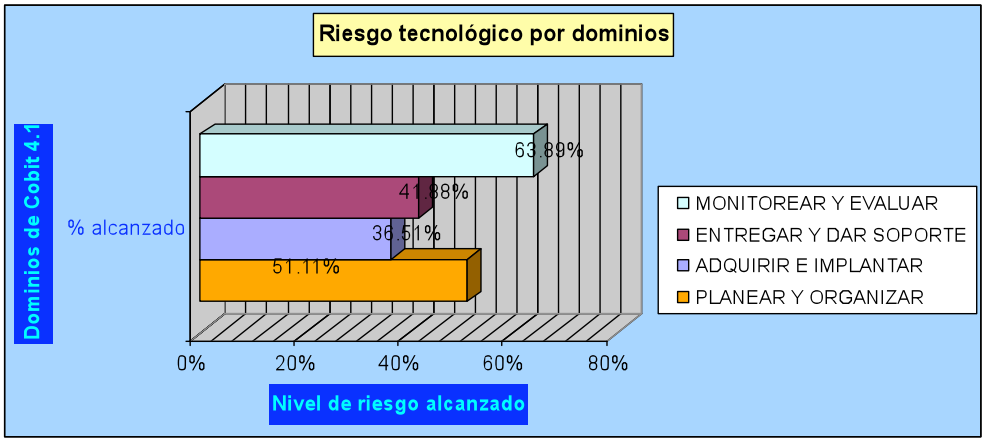
- **Objetivos de Cobit 4.1**: Contiene los nombres de los dominios y procesos de tecnología de información de Cobit, en inglés y su equivalente en español. El resto de hojas de cálculo siempre harán referencia a estos nombres para su uso.
- **Homologación**: En esta hoja se encuentran numerados los 32 requerimientos de la norma que rige el riesgo operativo hasta la fecha de elaboración de la presente metodología, y su homologación hacia los 34 procesos de tecnología de información de Cobit 4.1, con las actividades que satisfacen dichos requerimientos normativos. Esta estructura se encuentra reflejada en las tablas 3.2 a 3.8 de este documento.
- **Seleccionados x norma**: Por medio de fórmulas, esta hoja realiza el conteo del número de procesos de tecnología de información homologados a la norma de riesgo operativo realizado en la hoja de cálculo anterior. Su contenido puede ser visualizado en la tabla 3.9.

- **Controles genéricos**: Corresponde a la matriz a que se hace referencia en la actividad B.2 “Evaluación de los controles genéricos aplicados en cada proceso de tecnología de información”, con todas sus fórmulas y parámetros que están ligados a las demás hojas de cálculo que los requieren. Además contiene el resumen de calificación por control genérico que debe ser incorporado en el informe de evaluación.
- **Madurez**: En esta hoja se registra el grado de madurez actual y objetivo de cada proceso de tecnología de información, así como su impacto en el negocio, que corresponden a las actividades C.1, C.2 y C.3 de la etapa C. Un ejemplo de su contenido se muestra en las tablas 3.14 y 3.15.
- **Calif x proceso**: Corresponde a la actividad D.1 “Elaboración de un cuadro de evaluación de cada proceso de tecnología de información”, que sirve de obtener la calificación de riesgo o eje “X” del mapa de riesgo tecnológico, y cuyo contenido se muestra en la tabla 3.19. Además contiene el resumen de calificación por dominio de Cobit que se calcula automáticamente, las escalas de nivel de riesgo utilizados y la plantilla que sirve para realizar el cálculo del riesgo institucional, que se muestran en las tablas 3.20, 3.21 y 3.22.
- **Resumen**: Esta hoja corresponde a un resumen ejecutivo de la evaluación del riesgo tecnológico efectuada, en la que se anotan los resultados de cada etapa realizada, la calificación del dominio, el nivel de riesgo alcanzado y la relevancia que tiene cada proceso de tecnología de información para determinar su inclusión como una observación en el informe de evaluación. Un fragmento de dicho resumen se encuentra en la tabla 4.7. Además contiene el gráfico de la distribución del número de

procesos por cada calificación de riesgo que va de 1 a 9, y que facilita diagnosticar el estado de la plataforma tecnológica evaluada, tal como se indica en la figura 4.2

- **Mapa**: Esta es la última hoja del libro Excel y contiene el gráfico del mapa de riesgo tecnológico junto a todas las fórmulas que extraen datos de las demás hojas de cálculo para mostrar los riesgos asociados a cada proceso de tecnología de información. Además contiene un gráfico del riesgo de cada dominio de Cobit, un ejemplo del cual se muestra a continuación:

Tabla 3.28: Gráfico del riesgo tecnológico por dominios de Cobit



CAPÍTULO 4: IMPLEMENTACIÓN DEL PLAN PILOTO

4.1 - Características del plan piloto

La realización del plan piloto de la metodología de evaluación del riesgo tecnológico tuvo como objetivo validar los resultados obtenidos en la aplicación de cada una de las etapas y actividades propuestas en una plataforma de tecnología real, de modo que se puedan efectuar correctivos o mejoras para su optimización.

La institución financiera que colaboró con el proyecto tiene una baja participación en cuanto a depósitos del público, dentro de su segmento de mercado, y sin embargo cuenta con una plataforma tecnológica que da soporte a todos los procesos de negocio y atiende a 3 agencias en la ciudad de Quito. Cuenta con un sistema informático transaccional integrado que ha venido funcionando desde hace poco más de 3 años, y ha efectuado una importante inversión en cuanto a equipos e infraestructura de soporte y mantenimiento.

Parte del personal del área de Sistemas y de Auditoría Interna ha participado en cursos de fundamentos de Cobit e implementación del gobierno de tecnología de información, y el Comité de Sistemas decidió adoptar dicho estándar para sus procesos de TI desde inicios del año 2008, por lo que el lenguaje utilizado por la presente metodología les fue completamente familiar, y facilitó la comprensión de las actividades a desarrollar en cada una de las etapas, agilitando además de manera importante el tiempo de ejecución de las mismas.

Por razones de confidencialidad de la información no se revela el nombre de la institución financiera evaluada, e intencionalmente se ha omitido en los entregables de cada etapa los nombres de las personas que participaron en el proyecto y algunas características que podrían permitir la identificación de la institución financiera en la que se desarrolló el plan piloto.

4.2 - Desarrollo de actividades

A continuación se describe los resultados obtenidos en cada una de las etapas de la metodología aplicada:

Etapa A: Comprensión y aprobación del proyecto

Para la realización de esta etapa, se realizó una reunión con el Gerente General y Jefe de Sistemas para explicarles el alcance y beneficios de la aplicación de la presente metodología, y obtener la carta de aprobación requerida por la actividad A.1.

Una vez que el Gerente General aprobó la ejecución del proyecto, se elaboró una presentación que fue expuesta en una reunión de Comité de Sistemas, en la cual se aclararon los puntos a cubrir en el desarrollo del proyecto, los recursos humanos requeridos, actividades y plazos, y sobre todo los resultados esperados al final de la aplicación de la metodología. En dicha reunión participaron el Gerente General, Auditora Interna, Jefe de Sistemas, Jefe de la Unidad de Riesgos, y un representante de la alta gerencia.

Previo a convocar al Comité de Sistemas se elaboró una propuesta de roles y responsabilidades para cada una de las actividades a desarrollar, y un cronograma tentativo para establecer la duración de cada etapa.

Estos dos documentos fueron presentados al Comité y aprobados en su totalidad, por lo que inmediatamente se iniciaron las actividades correspondientes a la caracterización del proyecto y la revisión de la homologación de los procesos de tecnología de información de Cobit 4.1 a la norma de riesgo operativo vigente.

A continuación se presenta el texto de la caracterización del proyecto, que es el entregable de la actividad A.4.

CARACTERIZACIÓN DEL PROYECTO

1. **NOMBRE DEL PROYECTO.-** Validación de la metodología de evaluación del riesgo tecnológico utilizando COBIT 4.1.
2. **FECHA DE INICIO DEL PROYECTO:** 9 de junio del 2008.
3. **INFORMÁTICO RESPONSABLE.-** Jefe de Sistemas.
4. **USUARIOS RESPONSABLES Y ÁREAS A LAS QUE PERTENECEN:**

   Auditora Interna: Auditoría Interna

   Jefe de Riesgos: Unidad de Riesgos
5. **ROLES Y RESPONSABILIDADES DEL PERSONAL ASIGNADO:**

   Para la planificación del proyecto se ha asignado personal de la institución que, a más de ser responsables por la parte informática y por la parte usuaria,

participarán en las diferentes actividades de la evaluación del riesgo tecnológico, y cuyos roles y responsabilidades se describen a continuación:

- **COMITÉ DE SISTEMAS**

  Rol: Aprobar y dar seguimiento al proyecto

  Responsabilidad: Es el responsable por toda la ejecución del proyecto

- **JEFE DE SISTEMAS**

  Rol: Ejecutar el proyecto

  Responsabilidad: Será responsable de garantizar que la evaluación de los procesos de tecnología sea objetiva y se cuente con la documentación de respaldo pertinente en cada caso, para su rendición de cuentas al Comité de Sistemas.

- **JEFE DE RIESGOS**

  Rol: Monitorear el cumplimiento normativo en lo relativo al riesgo tecnológico

  Responsabilidad: Deberá participar en la actualización del análisis FODA de la tecnología de información y la identificación de sus riesgos asociados, garantizando que la misma sea efectiva para determinar las acciones de mejora tendientes a mitigar el riesgo operativo en el factor de tecnología de información, de acuerdo a la normativa vigente.

- **ASESORA**

  Rol: Asesorar en la ejecución del proyecto

  Responsabilidad: Guiar y diagnosticar el nivel de riesgo tecnológico que presenta la institución, y garantizar la correcta aplicación de la metodología utilizada para su evaluación.

- **AUDITORA**

  Rol: Evaluar controles informáticos

  Responsabilidad: Participar en la evaluación de los controles genéricos de los procesos de tecnología de la información, para garantizar objetividad en la misma.

6. CRONOGRAMA DE TRABAJO

A continuación se detalla el cronograma de trabajo empleado en el proyecto:

Tabla 4.1: Cronograma de trabajo del plan piloto

Actividad	Duración	Comienzo	Fin
METODOLOGÍA DE EVALUACIÓN DEL RIESGO TECNOLÓGICO	**33**	**09/Jun/2008**	**16/Jul/2008**
ETAPA A	**9**	**09/Jun/2008**	**18/Jun/2008**
A.1. Aprobación de la Gerencia para dar inicio al proyecto	2	09/Jun/2008	10/Jun/2008
Reunión con el Gerente General y entrega de solicitud	1	09/Jun/2008	09/Jun/2008
Obtención de la carta de aprobación	1	10/Jun/2008	10/Jun/2008
A.2. Planificación y conformación del equipo del proyecto	3	11/Jun/2008	13/Jun/2008
Elaboración del cronograma	2	11/Jun/2008	12/Jun/2008
Definición de roles y responsabilidades	1	13/Jun/2008	13/Jun/2008
A.3. Presentación y aprobación de la planificación y recursos	2	16/Jun/2008	17/Jun/2008
Elaboración de diapositivas	1	16/Jun/2008	16/Jun/2008
Reunión y aprobación del Comité de Sistemas	1	17/Jun/2008	17/Jun/2008
A.4 Caracterización del proyecto	0.5	18/Jun/2008	18/Jun/2008
A.5. Homologación de procesos de TI con norma de RO vigente	1.5	18/Jun/2008	19/Jun/2008
ETAPA B	**14.5**	**20/Jun/2008**	**10/Jul/2008**
B.1. Aplicación del modelo de diagnóstico	1	20/Jun/2008	20/Jun/2008
Actualizar Análisis FODA	1	20/Jun/2008	20/Jun/2008
Revisión del plan estratégico y operativo	1	20/Jun/2008	20/Jun/2008
B.2. Evaluación de controles genéricos aplicados en cada proceso de TI	12.5	23/Jun/2008	09/Jul/2008
B.3. Aplicación de homologación de procesos de TI	0.5	09/Jul/2008	09/Jul/2008
B.4. Obtención de una calificación de riesgo general de los procesos de TI	0.5	10/Jul/2008	10/Jul/2008
ETAPA C	**12**	**24/Jun/2008**	**09/Jul/2008**
C.1. Evaluación del nivel de madurez actual de cada proceso de TI	12	24/Jun/2008	09/Jul/2008
C.2. Determinación del nivel de madurez objetivo de cada proceso de TI	12	24/Jun/2008	09/Jul/2008
C.3. Valoración del impacto de cada proceso de TI en el negocio	12	24/Jun/2008	09/Jul/2008
ETAPA D	**2.5**	**09/Jul/2008**	**11/Jul/2008**
D.1. Elaboración de un cuadro de evaluación de cada proceso de TI	0.5	10/Jul/2008	10/Jul/2008
D.2. Cálculo del riesgo institucional	0.5	09/Jul/2008	11/Jul/2008
D.3. Revisión y aprobación de pesos de factores de la calificación final	0.5	11/Jul/2008	11/Jul/2008
D.4. Obtención del mapa de riesgo tecnológico	0.5	11/Jul/2008	11/Jul/2008
D.5. Aprobación de las etapas B, C y D	0.5	11/Jul/2008	11/Jul/2008
ETAPA E	**3**	**14/Jul/2008**	**16/Jul/2008**
Elaboración del informe de evaluación	3	14/Jul/2008	16/Jul/2008

7. DETERMINACIÓN DEL MODELO PARA EL DIAGNÓSTICO

Se ha determinado factible utilizar el modelo de análisis FODA para la elaboración del diagnóstico de la plataforma de tecnología de información en la institución, debido a que se ha venido utilizando dicho modelo en el plan estratégico institucional, y se ajusta a los requerimientos de la entidad.

Además, como parte del diagnóstico de la situación actual, se ha determinado necesario identificar los riesgos tecnológicos a los que está expuesta la plataforma de tecnología de información de la institución, por lo que se incluirán en el informe del análisis de la situación actual a efectuar en la segunda etapa de la metodología.

8. DESCRIPCIÓN GENERAL DEL RIESGO INHERENTE INSTITUCIONAL

- El recurso humano en la institución es nuevo en su mayoría, con pocas excepciones.
- Existe un alto porcentaje de rotación en el personal de la entidad debido a errores operativos detectados recientemente.
- La plataforma tecnológica que da soporte a los procesos de negocio ha requerido una alta inversión económica y su capacidad contratada es mayor a la capacidad instalada.
- Los servicios de comunicaciones, provisión de software y operación del sistema transaccional se encuentran tercerizados.

- El Comité de Sistemas ha aprobado la adopción de Cobit como una de las mejores prácticas en tecnología de información a aplicar en la entidad, el cual se encuentra en proceso de implementación desde inicios del presente año.

9. RESTRICCIONES O CONSIDERACIONES PARA LA REALIZACIÓN DEL PROYECTO.

- En la planificación del proyecto se han considerado las fechas de inicio y fin de cada actividad asignando un estimado de 2 horas diarias a su ejecución, sin embargo, debido a que en el área de Sistemas hay un número limitado de funcionarios, el involucramiento del Jefe de Sistemas en el proyecto estaría limitado al tiempo que disponga fuera de la realización de sus actividades diarias y de control, lo que podría eventualmente prolongar el desarrollo y consecuentemente la obtención de los resultados esperados.
- No se puede involucrar en el proyecto a los jefes de Negocios o de Operaciones debido a que es personal nuevo que no conoce a profundidad la institución y/o los servicios que presta el Departamento de Sistemas.
- Las propuestas de mejora que se planteen como resultado de este proyecto, estarían limitadas en su aplicación por la disponibilidad de recursos económicos, por lo que posiblemente se tendrían que incluir en la planificación operativa del próximo ejercicio económico.

ACTUALIZACIÓN DE LA HOMOLOGACIÓN DE PROCESOS

Durante el proceso de revisión de la homologación propuesta, se trabajó con la versión 4.0 en español de Cobit para aclarar algunos de los conceptos utilizados, ya que aún no se cuenta con una publicación oficial en español de la versión 4.1. Luego de la revisión, los cambios efectuados a la propuesta original fueron mínimos, y son los que se detallan a continuación:

- El requerimiento normativo No. 1 "1.3.1.1 El apoyo y compromiso formal del directorio u organismo que haga sus veces y la alta gerencia", se había homologado al proceso PO4 "Definir los procesos, organización y relaciones de TI" de Cobit con la ejecución de las actividades PO4.6 y PO4.10; por sugerencia de las jefaturas de Sistemas y la Unidad de Riesgos se añadieron las actividades PO4.2 y PO4.3.

- El requerimiento normativo No. 28 "1.3.6.1 Una metodología que permita la adecuada administración y control del proceso de compra de software y del ciclo de vida de desarrollo y mantenimiento de aplicaciones, con la aceptación de los usuarios involucrados", se había homologado al proceso PO8 "Administrar la calidad", con la aplicación específica de la actividad PO8.3. La sugerencia en este caso fue añadir el proceso AI2 "Adquirir y mantener software aplicativo".

- El requerimiento normativo No. 32 "Contar con políticas y procedimientos que permitan la adecuada administración, monitoreo y documentación de las bases de datos, redes de datos, software de base y

hardware" se había homologado al proceso DS3 "Administrar el desempeño y la capacidad". En este caso la sugerencia fue incrementar los procesos ME1 "Monitorear y evaluar el desempeño de TI" y ME3 "Garantizar el cumplimiento regulatorio", este último pese a que no es requerido explícitamente en la norma de riesgo operativo, pero es deber de toda institución financiera cumplir con todas las disposiciones legales emitidas por el organismo de control.

Con estas actualizaciones, la homologación queda como sigue:

Tabla 4.2: Homologación actualizada de procesos del plan piloto

		Selección	Referencia
PLANEAR Y ORGANIZAR			
PO1	Definir un plan estratégico de TI	SI	2
PO2	Definir la arquitectura de la información	NO	
PO3	Determinar la dirección tecnológica	SI	3, 31
PO4	Definir los procesos, organización y relaciones de TI	SI	1, 4, 16
PO5	Administrar la inversión en TI	NO	
PO6	Comunicar las aspiraciones y la dirección de la gerencia	SI	5, 6
PO7	Administrar recursos humanos de TI	SI	7
PO8	Administrar la calidad	SI	28
PO9	Evaluar y administrar los riesgos de TI	SI	13
PO10	Administrar proyectos	NO	
ADQUIRIR E IMPLANTAR			
AI1	Identificar soluciones automatizadas	NO	
AI2	Adquirir y mantener software aplicativo	SI	28
AI3	Adquirir y mantener infraestructura tecnológica	SI	24
AI4	Facilitar la operación y el uso	SI	29
AI5	Adquirir recursos de TI	SI	11
AI6	Administrar cambios	SI	29, 30
AI7	Instalar y acreditar soluciones y cambios	SI	31
ENTREGAR Y DAR SOPORTE			
DS1	Definir y administrar los niveles de servicio	NO	
DS2	Administrar los servicios de terceros	SI	10
DS3	Administrar el desempeño y la capacidad	SI	32
DS4	Garantizar la continuidad del servicio	SI	25, 26, 27
DS5	Garantizar la seguridad de los sistemas	SI	12, 13, 15-19, 22, 23
DS6	Identificar y asignar costos	NO	
DS7	Educar y entrenar a los usuarios	SI	7
DS8	Administrar la mesa de servicio y los incidentes	NO	
DS9	Administrar la configuración	SI	9
DS10	Administrar los problemas	NO	
DS11	Administrar los datos	SI	14
DS12	Administrar el ambiente físico	SI	20, 21, 24
DS13	Administrar las operaciones	SI	8, 19
MONITOREAR Y EVALUAR			
ME1	Monitorear y evaluar el desempeño de TI	SI	32
ME2	Monitorear y evaluar el control interno	NO	
ME3	Garantizar el cumplimiento regulatorio	SI	32
ME4	Proporcionar gobierno de TI	NO	
TOTAL OBJETIVOS DE COBIT 4.1 REQUERIDOS POR NORMA:		**24**	

Etapa B: Evaluación de la situación actual

Para la evaluación de la situación actual se utilizó como base el análisis FODA constante en el Plan Estratégico de TI 2006 - 2008, complementando la información con la matriz de identificación de riesgos tecnológicos delineados por la jefatura de la Unidad de Riesgos para la elaboración del plan de contingencias de tecnología de información. El análisis FODA actualizado se presenta a continuación.

Oportunidades

- Existe una tecnología débil en el segmento de mercado institucional
- Nueva tecnología está disponible en el mercado
- Credibilidad fuerte en el segmento de mercado institucional
- Importante demanda de servicios financieros
- Proveedor con buen posicionamiento en el mercado

Amenazas

- Políticas cambiantes en las entidades controladoras
- Cambios en las políticas del gobierno
- Alta competencia en productos y servicios
- Avance tecnológico del mercado es mayor al institucional
- Ataques informáticos

- Exigencias de normativa de riesgos tecnológico no aplicable a la entidad
- Costos adicionales por requerimientos de control

Fortalezas

- Software financiero transaccional sólido y completo
- Recurso humano calificado y con experiencia
- Tecnología adecuada en LAN y WAN
- Crecimiento tecnológico disponible
- Rápida respuesta al cambio
- Disponibilidad de ambiente Intranet
- Hardware actualizado y adecuadamente administrado
- Alta inversión en tecnología de información
- Apoyo gerencial a la tecnología
- Adecuada estructura física del área
- Hay conciencia de la necesidad de utilización de estándares y mejores prácticas para la administración de la tecnología de información

Debilidades

- No se cuenta con los códigos fuente del sistema transaccional
- Dependencia tecnológica del software financiero por parte de los usuarios
- No existe un área de desarrollo
- Falta de evaluación de los controles en aplicativos
- Excedente de servicios financieros (sistema subutilizado)

- Falta de un programa de capacitación continua para el personal de TI
- Inadecuada transferencia de conocimientos en la rotación de personal

En la evaluación de los controles genéricos aplicados en cada proceso de tecnología de información participó también Auditoría Interna, lo que permitió garantizar objetividad en los datos ingresados como respuesta a la evaluación. El puntaje de riesgo general obtenido en la matriz de evaluación de controles genéricos, la cual incluye la aplicación de la homologación de los procesos de tecnología de información con la norma de riesgo operativo vigente, fue de 65.85%.

El umbral de riesgo para la institución fue fijado en 58.33% debido a que es el porcentaje que corresponde a una homologación de los controles genéricos evaluados a un nivel de madurez 3 de un modelo de control interno, mientras que un nivel 4 establecía un umbral de riesgo del 79.17%, el cual exigía la aplicación de mayores controles y por tanto mayores costos a la institución. En vista de que este valor depende del apetito de riesgo que tenga la institución, el Comité de Sistemas optó por adoptar el porcentaje que representa el nivel de madurez 3.

Con dicho umbral de riesgo fijado, se registraron 7 procesos en estado crítico de controles debido a que sus porcentajes de aplicación o cumplimiento de controles se encuentran por debajo del mismo, y son aquellos cuyo porcentaje se encuentra sombreado en la tabla 4.3.

Tabla 4.3: Matriz de controles genéricos evaluados en el plan piloto

CONTROLES GENERALES DE LOS PROCESOS DE TECNOLOGÍA DE COBIT 4.1			100%	Requerido			
			30%	No requerido			
			58.33%	Umbral de riesgo			
Dominios y procesos de tecnología de Cobit 4.1			Resultado por proceso	% cumplimiento	Requerido por la norma de gestión riesgo operativo	Peso	Valor relativo
PLANEAR Y ORGANIZAR	PO1	Definir un plan estratégico de TI	22	91.67%	SI	3.70%	3.395%
	PO2	Definir la arquitectura de la información	18	75.00%	NO	1.11%	0.833%
	PO3	Determinar la dirección tecnológica	7	29.17%	SI	3.70%	1.080%
	PO4	Definir los procesos, organización y relaciones de TI	15	62.50%	SI	3.70%	2.315%
	PO5	Administrar la inversión en TI	19	79.17%	NO	1.11%	0.880%
	PO6	Comunicar las aspiraciones y la dirección de la gerencia	18	75.00%	SI	3.70%	2.778%
	PO7	Administrar recursos humanos de TI	23	95.83%	SI	3.70%	3.549%
	PO8	Administrar la calidad	0	0.00%	SI	3.70%	0.000%
	PO9	Evaluar y administrar los riesgos de TI	15	62.50%	SI	3.70%	2.315%
	PO10	Administrar proyectos	17	70.83%	NO	1.11%	0.787%
ADQUIRIR E IMPLANTAR	AI1	Identificar soluciones automatizadas	16	66.67%	NO	1.11%	0.741%
	AI2	Adquirir y mantener software aplicativo	19	79.17%	SI	3.70%	2.932%
	AI3	Adquirir y mantener infraestructura tecnológica	15	62.50%	SI	3.70%	2.315%
	AI4	Facilitar la operación y el uso	15	62.50%	SI	3.70%	2.315%
	AI5	Adquirir recursos de TI	23	95.83%	SI	3.70%	3.549%
	AI6	Administrar cambios	18	75.00%	SI	3.70%	2.778%
	AI7	Instalar y acreditar soluciones y cambios	17	70.83%	SI	3.70%	2.623%
ENTREGAR Y DAR SOPORTE	DS1	Definir y administrar los niveles de servicio	23	95.83%	NO	1.11%	1.065%
	DS2	Administrar los servicios de terceros	23	95.83%	SI	3.70%	3.549%
	DS3	Administrar el desempeño y la capacidad	14	58.33%	SI	3.70%	2.160%
	DS4	Garantizar la continuidad del servicio	19	79.17%	SI	3.70%	2.932%
	DS5	Garantizar la seguridad de los sistemas	15	62.50%	SI	3.70%	2.315%
	DS6	Identificar y asignar costos	0	0.00%	NO	1.11%	0.000%
	DS7	Educar y entrenar a los usuarios	11	45.83%	SI	3.70%	1.698%
	DS8	Administrar la mesa de servicio y los incidentes	16	66.67%	NO	1.11%	0.741%
	DS9	Administrar la configuración	17	70.83%	SI	3.70%	2.623%
	DS10	Administrar los problemas	14	58.33%	NO	1.11%	0.648%
	DS11	Administrar los datos	15	62.50%	SI	3.70%	2.315%
	DS12	Administrar el ambiente físico	19	79.17%	SI	3.70%	2.932%
	DS13	Administrar las operaciones	23	95.83%	SI	3.70%	3.549%
MONIT Y EVAL.	ME1	Monitorear y evaluar el desempeño de TI	0	0.00%	SI	3.70%	0.000%
	ME2	Monitorear y evaluar el control interno	13	54.17%	NO	1.11%	0.602%
	ME3	Garantizar el cumplimiento regulatorio	19	79.17%	SI	3.70%	2.932%
	ME4	Proporcionar gobierno de TI	13	54.17%	NO	1.11%	0.602%
		Calificación general inicial:	**65.85%**				

Los demás procesos que tienen un puntaje mayor al umbral de riesgo definido, no se consideran críticos pero de igual manera se debe analizar su nivel de riesgo alcanzado y la calificación general de la institución.

Etapa C: Identificación del grado de madurez de los procesos de TI

La identificación del grado de madurez de los procesos se efectuó utilizando los modelos de madurez de Cobit 4.0 puesto que están en español y, de acuerdo a la revisión previa efectuada, coinciden con la versión en inglés de Cobit 4.1.

La plantilla en la que se ingresó el nivel de madurez actual y el objetivo de cada proceso de tecnología de información incluyó la descripción de la causa por la que se considera que cada proceso de TI está ubicado en el nivel de madurez indicado (ver tabla 4.4), con el fin de documentar el proceso de revisión presente y que sirva como referencia para procesos de revisión futuros.

Tabla 4.4: Definición de niveles de madurez e impacto en el negocio

Dominios y procesos de tecnología de Cobit 4.1			Niv. actual	Causa	Niv. objet.	Causa	Brecha	Impacto			Verificador
								A	M	B	
PLANEAR Y ORGANIZAR	PO1	Definir un plan estratégico de TI	3	No se realiza reingeniería de procesos	4	Para mejorar los procesos usando la TI	1	X			✔
	PO2	Definir la arquitectura de la información	3	No hay métodos y técnicas formales, la herramienta automática aún no funciona	3	Aún no se va a utilizar herramientas automatizadas integradas	0			X	✔
	PO3	Determinar la dirección tecnológica	1	No hay técnicas o estándares para planificar componentes de TI	3	Contar con un plan de infraestructura definido	2			X	✔
	PO4	Definir los procesos, organización y relaciones de TI	2	Falta formalizar relaciones con áreas usuarias de TI	3	Contar con descripción de funciones de terceros relacionadas con TI	1	X			✔
	PO5	Administrar la inversión en TI	2	No existen políticas formales para inversión de TI	3	La gerencia debe implementar políticas para elaboración del presupuesto	1		X		✔
	PO6	Comunicar las aspiraciones y la dirección de la gerencia	2	No existe concientización de las políticas y estándares	4	Se crearán un mecanismos para concientizar sobre las políticas y estándares y su evaluación	2	X			✔
	PO7	Administrar recursos humanos de TI	2	Está formalizado el proceso de selección y capacitación	2	Por la infraestructura de la entidad	0		X		✔
	PO8	Administrar la calidad	0	No existe proceso de administración de calidad	2	Establecer un programa para evaluar la calidad de los procesos de TI	2		X		✔
	PO9	Evaluar y administrar los riesgos de TI	2	No existe una metodología específica para identificar el riesgo	3	Determinar una metodología formal para administrar el riesgo	1	X			✔
	PO10	Administrar proyectos	2	No existe un sistema de administración de calidad ni un área de proyectos	2	Recursos limitados y no poder conformar el área de proyectos, aunque sí se administran	0	X			✔

ADQUIRIR E IMPLANTAR	AI1	Identificar soluciones automatizadas	4	Si maneja metodología de requerimientos	4	No aplica una mejora continua de la metodología	0	X			✔
	AI2	Adquirir y mantener software aplicativo	3	No existe metodología formal para la etapa de pruebas	4	Realizar la metodología de pruebas para esta etapa	1	X			✔
	AI3	Adquirir y mantener infraestructura tecnológica	3	Optimización de costos	5	Optimizar costos	2	X			✔
	AI4	Facilitar la operación y el uso	2	Por no existir plan de capacitación	3	Tener un plan formal de capacitación	1			X	✔
	AI5	Adquirir recursos de TI	5	Está optimizado	5	Está optimizado	0		X		✔
	AI6	Administrar cambios	3	No existe procedimiento de administración de la calidad	4	Realizar proceso de administración de la calidad	1		X		✔
	AI7	Instalar y acreditar soluciones y cambios	2	No hay metodología formal para pruebas y migración	3	Formalizar la metodología de pruebas	1	X			✔
ENTREGAR Y DAR SOPORTE	DS1	Definir y administrar los niveles de servicio	3	Sí existe administración de niveles de servicio	3	Es suficiente para la estructura de la entidad	0		X		✔
	DS2	Administrar los servicios de terceros	3	Por no existir KPI ni KGI	4	Evaluar los controles de KPI y KGI	1	X			✔
	DS3	Administrar el desempeño y la capacidad	2	No hay una herramienta de monitoreo integrada	4	Implementar una herramienta de monitoreo de recursos de la red	2	X			✔
	DS4	Garantizar la continuidad del servicio	3	Falta capacitación en escalamiento de los incidentes	4	Se implementará capacitación para manejo del plan de contingencia	1	X			✔
	DS5	Garantizar la seguridad de los sistemas	2	No existen funciones completas del oficial de seguridad	4	Capacitación en seguridad y establecer funciones formales de oficial de seguridad	2	X			✔
	DS6	Identificar y asignar costos	1	No existe asignación de costos, solo un presupuesto	1	No aplica al tamaño de la institución	0			X	✔
	DS7	Educar y entrenar a los usuarios	2	Falta capacitación continua	3	Se implementará con RRHH un entrenamiento continuo a los usuarios	1		X		✔
	DS8	Administrar la mesa de servicio y los incidentes	3	Implementar KPI, KGI	4	implementar indicadores de evaluación de la mesa de servicio	1			X	✔
	DS9	Administrar la configuración	3	Administración compartida y en otros es del proveedor esta bajo contrato la configuración	3	Administración compartida y en otros es del proveedor esta bajo contrato la configuración	0	X			✔
	DS10	Administrar los problemas	2	Se está concluyendo herramienta centralizada	4	Implementar KPI y KGI	2		X		✔
	DS11	Administrar los datos	2	Falta el procedimiento para desechos de datos	3	Elaborar procedimientos para desechos de datos	1	X			✔
	DS12	Administrar el ambiente físico	3	Se tiene las normas de seguridad establecidas	4	Determinar los KPI y KPG	1	X			✔
	DS13	Administrar las operaciones	3	Cumple con los procesos de automatización	4	Informes de causa y efecto	1	X			✔
MONITOREAR Y EVALUAR	ME1	Monitorear y evaluar el desempeño de TI	0	No existe el proceso	1	Iniciar con monitoreo	1		X		✔
	ME2	Monitorear y evaluar el control interno	1	Auditoría Interna y externas como parte de la auditoría financiera	3	Establecer procedimientos de control interno	2	X			✔
	ME3	Garantizar el cumplimiento regulatorio	2	La capacitación es informal	3	Exista capacitación en las leyes y regulaciones	1	X			✔
	ME4	Proporcionar gobierno de TI	2	No existe un gobierno de TI Corporativo el Comité de Sistemas es aprobador	3	El Comité de Sistemas debe involucrarse en el gobierno de TI	1		X		✔
		Promedio general	**2.3**		**3.3**		**1.0**				

Paralelamente a estas dos actividades, se valoró el impacto de cada proceso de tecnología de información en el negocio, considerando los aspectos indicados en el manual de la metodología, tales como continuidad del negocio, nivel de inversión institucional en cada proceso, volumen de transacciones y complejidad del proceso.

El grado de madurez objetivo determinado para cada proceso de tecnología de información, sirvió para efectuar las recomendaciones tendientes a mitigar los riesgos tecnológicos considerados relevantes para la entidad, y que constan en el informe de evaluación que se elabora en la etapa E de esta metodología. Para el efecto, también se utilizaron los modelos de madurez de Cobit, adaptándolos a la realidad de la entidad en cada caso particular, pero manteniendo como base las mejores prácticas establecidas por dicho marco de trabajo.

Etapa D: Obtención del mapa de riesgo tecnológico

El cuadro resumen de la evaluación de los procesos de tecnología de información se generó automáticamente en una hoja en Excel, ya que las fórmulas que lo componen traen de las etapas anteriores los valores y puntajes alcanzados en la evaluación de controles genéricos y la identificación del grado de madurez.

Sin embargo, los porcentajes de participación de cada factor evaluado en la calificación final de cada proceso de tecnología de información tuvieron que ser previamente revisados y aprobados por el Comité de Sistemas de la institución para que tuvieran formalidad en su aplicación.

Para el cálculo del riesgo institucional, la entidad no cuenta con un levantamiento de procesos previo que permita determinar el número de procesos automatizados frente al número total de procesos, por lo que la determinación de dicha variable se efectuó considerando el número de operaciones diarias en cada una de las áreas de la institución y un estimado porcentual de la automatización que se tiene en cada una de ellas, valores que fueron estimados por los jefes de las áreas correspondientes mediante entrevistas personales.

El valor al que se llegó mediante dicho cálculo fue al 84.85% (ver tabla 4.5), que corresponde al segmento de riesgo institucional medio (2).

Tabla 4.5: Cálculo del riesgo institucional del plan piloto

	Frecuencia	% automatización
Tesorería	47.00	80.00%
Inversiones	12.00	90.00%
Recepción	15.00	80.00%
Cajas	62.00	100.00%
Operaciones	200.00	80.00%
Crédito	180.00	90.00%
Contabilidad	36.00	70.00%
RRHH	5.00	60.00%
TOTAL FRECUENCIA:	557.00	
PORCENTAJE DE AUTOMATIZACIÓN DE LA ENTIDAD:		84.85%
Riesgo institucional medio, segmento:		**2**

Una vez calculado el riesgo institucional, se obtuvo el mapa de riesgo tecnológico (ver figura 4.1), el cual fue aprobado por el Comité de Sistemas.

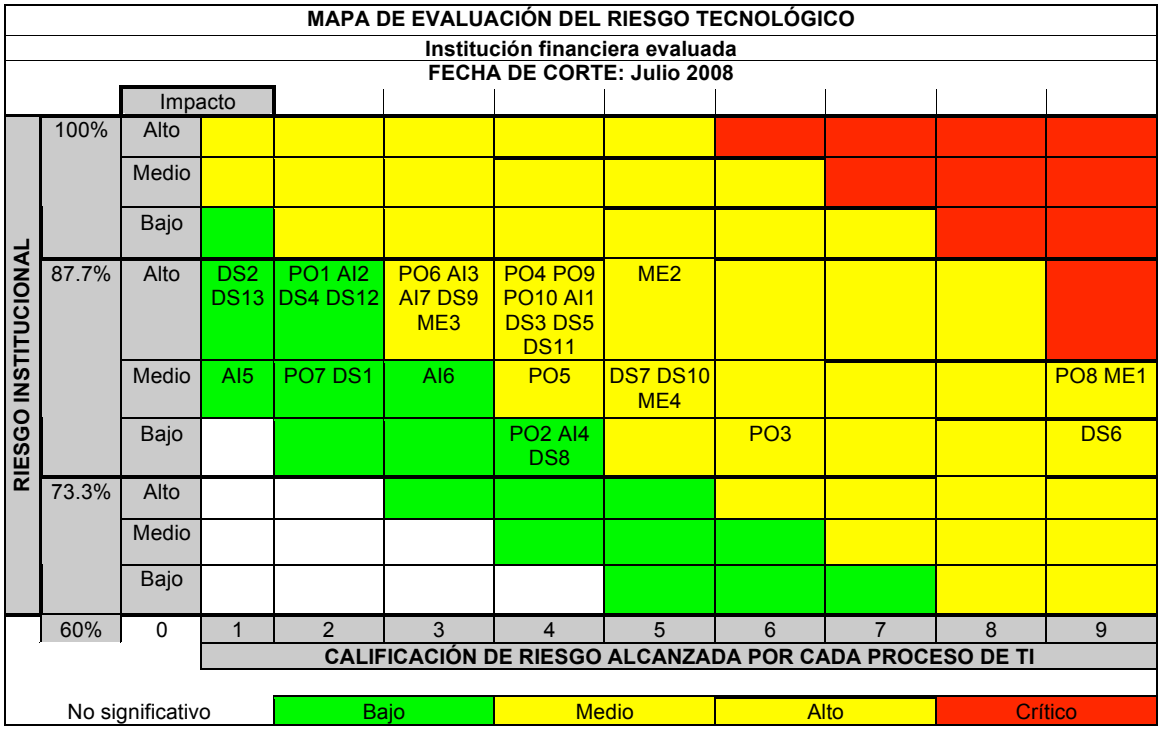


Figura 4.1: Mapa de evaluación del riesgo tecnológico del plan piloto

Etapa E: Elaboración del informe de evaluación

Para la elaboración del informe de evaluación fue necesario realizar cuadros de resumen que permitan analizar la información recolectada hasta la presente etapa, e incluso un gráfico con la curva de distribución de las calificaciones de riesgo alcanzadas por cada uno de los procesos de tecnología de información evaluados, los cuales también se incluyeron dentro del informe. A continuación se presenta el texto del informe, del cual se ha eliminado el análisis FODA y las condiciones del riesgo inherente que corresponden al análisis de la situación actual que ya fueron expuestos en la etapa B, y la homologación de procesos que se presentó en la etapa A de este capítulo.

Institución financiera evaluada

FECHA DE INICIO DEL PROYECTO: 9 de junio del 2008.

ALCANCE

La evaluación del riesgo tecnológico se realizó sobre los 34 procesos de tecnología de información definidos por la versión 4.1 de Cobit, agrupados en sus 4 dominios.

Sobre estos procesos, se han efectuado las siguientes actividades:

- Homologación a su requerimiento legal, con la norma de riesgo operativo vigente
- Evaluación de los controles genéricos aplicados
- Identificación del grado de madurez alcanzado y el esperado
- Determinación de su impacto en el negocio

Derivado de la aplicación de las citadas actividades, se obtuvo el mapa de riesgo tecnológico, que se expone más adelante en la sección de resultados.

RESTRICCIONES

No se presentaron restricciones al alcance, únicamente se tuvo limitaciones en cuanto al tiempo disponible del equipo de proyecto por cuanto en la semana del 30 de junio tuvieron que atender procesos propios de cierre de mes y de fin de semestre, que prolongaron la terminación del proyecto.

RESULTADOS

1. Homologación de los procesos de tecnología de información de Cobit 4.1 a la norma de riesgo operativo vigente en el factor de tecnología de información

El resultado de esta actividad se resume en la tabla 4.2.

2. Evaluación de los controles genéricos, niveles de madurez e impacto en el negocio

La evaluación de los controles genéricos que se aplican a los procesos de tecnología de información dio como resultado una calificación general de controles del 65.85%, el cual se encuentra por encima del umbral de riesgo definido por el Comité de Sistemas en el 58.33%, por lo que en términos generales se puede concluir que los controles que se aplican a la plataforma tecnológica de la institución caen dentro del margen de riesgo asumido por la entidad. Se puede notar que la mayor deficiencia se encuentra en el mejoramiento del desempeño, puesto que la institución no ha previsto la necesidad de contar con un sistema de administración de la calidad y tampoco existe un proceso de monitoreo del desempeño general institucional.

En menor grado, también presenta deficiencias la formalización de políticas, planes y procedimientos, ya que existen manuales de procedimientos para la mayoría de procesos de tecnología de información, pero no se han definido,

formalizado y difundido las políticas que deben regir dichos procedimientos, o en algunos casos las mismas se encuentran incorporadas en forma tácita dentro del manual de procedimientos. Estos dos grandes grupos de controles son los que en gran medida afectan a la puntuación general de los procesos de tecnología de información.

Tabla 4.6: Resumen de los controles evaluados en el plan piloto

CONTROLES GENÉRICOS EVALUADOS			Procesos que aplican	%	Prom.
Metas y objetivos	1	Define y comunica metas y objetivos específicos, medibles, ejecutables, realísticos, orientados a resultados y con fechas límite	29	85.29%	82.35%
	2	Alineado con los objetivos del negocio	30	88.24%	
	3	Medido por métricas adecuadas	25	73.53%	
Propiedad	4	Existe un propietario con suficiente autoridad para cumplir roles y responsabilidades	31	91.18%	89.22%
	5	Roles y responsabilidades definidos, entendidos y aceptados	30	88.24%	
	6	La responsabilidad incluye: diseño, interacción, rendición de cuentas, medición del desempeño	30	88.24%	
Repetitividad	7	La repetitividad del proceso es un objetivo de la Administración	29	85.29%	82.94%
	8	Si el proceso es crítico, provee evidencia para revisión por parte de la Administración	30	88.24%	
	9	Se aplicaron buenas prácticas y estándares internacionales en su definición	23	67.65%	
	10	Las partes interesadas integran y son coherentes con el proceso	29	85.29%	
	11	La secuencia de sus actividades es lógica, flexible y escalable	30	88.24%	
Roles y responsabilidades	12	Las actividades clave y entregables están definidos y documentados	29	85.29%	80.88%
	13	Roles y responsabilidades no ambiguos, asignados y comunicados	29	85.29%	
	14	Roles y responsabilidades para ejecución efectiva, eficiente y documentada de actividades	26	76.47%	
	15	Está asignada la rendición de cuentas de resultados y entregables	26	76.47%	
Políticas, planes y procedimientos	16	Existen, están comunicadas, son conocidas y aplicadas	16	47.06%	46.32%
	17	Su administración incluye documentar, revisar, mantener, comunicar, y usar para capacitar	17	50.00%	
	18	Hay responsabilidad por su administración y se revisa su correcto cumplimiento periódicamente	15	44.12%	
	19	Son accesibles, correctas, entendidas y actualizadas	15	44.12%	
Mejoramiento del desempeño	20	Existen métricas que permiten percibir los resultados y desempeño del proceso con un esfuerzo limitado	13	38.24%	24.71%
	21	El diseño de las métricas permite medir la utilización de recursos, calidad de resultados y tiempos	9	26.47%	
	22	Existen procedimientos para definir marcas a cumplir en las metas del proceso y conductores de desempeño	10	29.41%	
	23	Se comparan las medidas actuales con las marcas de los logros a cumplir y se toman acciones de mejora	10	29.41%	
	24	Las métricas, marcas y métodos están alineados con el monitoreo del desempeño general de TI	0	0.00%	

En la evaluación del riesgo tecnológico se utilizó una escala de 5 categorías para los niveles de riesgo, los cuales tienen la distribución mostrada en la tabla 3.21 para la calificación de riesgo que va de 1 a 9.

Tabla 4.7: Resumen de los controles evaluados en el plan piloto

			Evaluación de controles genéricos			Madurez		Eje "Y"	Eje "X"	
Procesos de tecnología de información			# Controles	%	Req. por norma	Actual	Objetivo	Impacto	Calif. de riesgo	Calif. del dominio
PLANEAR Y ORGANIZAR	PO1	Definir un plan estratégico de TI	22	91.67%	SI	3	4	Alto	2	5
	PO2	Definir la arquitectura de la información	18	75.00%	NO	3	3	Bajo	4	
	PO3	Determinar la dirección tecnológica	7	29.17%	SI	1	3	Bajo	6	
	PO4	Definir los procesos, organización y relaciones de TI	15	62.50%	SI	2	3	Alto	4	
	PO5	Administrar la inversión en TI	19	79.17%	NO	2	3	Medio	4	
	PO6	Comunicar las aspiraciones y la dirección de la gerencia	18	75.00%	SI	2	4	Alto	3	
	PO7	Administrar RRHH de TI	23	95.83%	SI	2	2	Medio	2	
	PO8	Administrar la calidad	0	0.00%	SI	0	2	Medio	9	
	PO9	Evaluar y admin. los riesgos de TI	15	62.50%	SI	2	3	Alto	4	
	PO10	Administrar proyectos	17	70.83%	NO	2	2	Alto	4	
ADQUIRIR E IMPLANTAR	AI1	Identificar soluciones automatizadas	16	66.67%	NO	4	4	Alto	4	3
	AI2	Adquirir y mantener software aplicativo	19	79.17%	SI	3	4	Alto	2	
	AI3	Adquirir y mantener infraestructura tecnológica	15	62.50%	SI	3	5	Alto	3	
	AI4	Facilitar la operación y el uso	15	62.50%	SI	2	3	Bajo	4	
	AI5	Adquirir recursos de TI	23	95.83%	SI	5	5	Medio	1	
	AI6	Administrar cambios	18	75.00%	SI	3	4	Medio	3	
	AI7	Instalar y acreditar soluciones y cambios	17	70.83%	SI	2	3	Alto	3	
ENTREGAR Y DAR SOPORTE	DS1	Definir y administrar los niveles de servicio	23	95.83%	NO	3	3	Medio	2	4
	DS2	Administrar los servicios de terceros	23	95.83%	SI	3	4	Alto	1	
	DS3	Administrar el desempeño y la capacidad	14	58.33%	SI	2	4	Alto	4	
	DS4	Garantizar la continuidad del servicio	19	79.17%	SI	3	4	Alto	2	
	DS5	Garantizar la seguridad de los sistemas	15	62.50%	SI	2	4	Alto	4	
	DS6	Identificar y asignar costos	0	0.00%	NO	1	1	Bajo	9	
	DS7	Educar y entrenar a los usuarios	11	45.83%	SI	2	3	Medio	5	
	DS8	Administrar la mesa de servicio y los incidentes	16	66.67%	NO	3	4	Bajo	4	
	DS9	Administrar la configuración	17	70.83%	SI	3	3	Alto	3	
	DS10	Administrar los problemas	14	58.33%	NO	2	4	Medio	5	
	DS11	Administrar los datos	15	62.50%	SI	2	3	Alto	4	
	DS12	Administrar el ambiente físico	19	79.17%	SI	3	4	Alto	2	
	DS13	Administrar las operaciones	23	95.83%	SI	3	4	Alto	1	
MONIT. Y EVAL.	ME1	Monitorear y evaluar el desempeño de TI	0	0.00%	SI	0	1	Medio	9	6
	ME2	Monitorear y evaluar el control interno	13	54.17%	NO	1	3	Alto	5	
	ME3	Garantizar el cumplimiento regulatorio	19	79.17%	SI	2	3	Alto	3	
	ME4	Proporcionar gobierno de TI	13	54.17%	NO	2	3	Medio	5	
		Calificación general de controles:		65.85%		Calificación de riesgo de la institución:				4.32
						Nivel de riesgo:				Medio

La tabla 4.7 muestra el puntaje obtenido por cada proceso de tecnología de información en cuanto a los controles aplicados y su requerimiento legal, el impacto de cada proceso en el negocio, y los niveles de madurez actual y objetivo determinados por la Jefatura de Sistemas, que fueron identificados considerando el nivel de inversión institucional en cada proceso, su

complejidad, volumen de transacciones o dependencia para la continuidad de operaciones, y la disponibilidad de recursos para alcanzar el nivel de madurez deseado.

Los puntajes obtenidos en los factores mencionados dan como resultado una calificación de riesgo individual que, consolidada por cada uno de los dominios dan una calificación de riesgo general de la institución de 4.32, que se homologa a un nivel de riesgo institucional “medio”:

Para la elaboración del mapa de riesgo tecnológico se utilizó en el eje “X” la calificación de riesgo obtenida por cada proceso de tecnología de información, que va de 1 a 9, mientras que en el eje “Y” se utilizó el riesgo institucional, dividido en 3 segmentos de riesgo. Para efectos de la presente evaluación, se consideró que el riesgo institucional está dado por la mayor o menor dependencia de la institución hacia la tecnología, bajo el supuesto de que ninguna institución financiera controlada por la Superintendencia de Bancos y Seguros tiene una automatización menor al 60%.

Para el caso de la institución evaluada, el porcentaje de automatización o dependencia institucional hacia la tecnología de información, se determinó en 84.85%, lo cual ubica a la institución en el segmento de riesgo “2” del mapa de riesgo tecnológico. Al ubicar las calificaciones de riesgo obtenidas por cada uno de los procesos de tecnología de información en dicho segmento, los niveles de riesgo de la entidad evaluada quedan como se muestra en el mapa de riesgo tecnológico de la figura 4.1.

Como se puede ver en el mapa de riesgo, no existen procesos de tecnología de información en el nivel de riesgo crítico, únicamente hay 3 procesos en el nivel de riesgo alto, 18 procesos en el nivel de riesgo medio y 13 procesos en el nivel de riesgo bajo, lo que van en concordancia con el puntaje de calificación de riesgo institucional mostrado en el cuadro anterior.

El número de procesos evaluados, de acuerdo con la calificación de riesgo alcanzada, se muestra gráficamente de la siguiente manera:

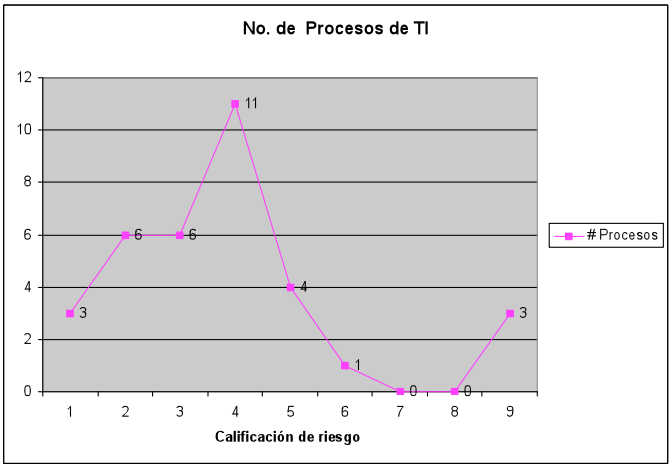


Figura 4.2: Curva de distribución de niveles de riesgo en el plan piloto

Hallazgos relevantes

A continuación se detalla el análisis efectuado a cada uno de los procesos de tecnología de información cuya situación es relevante para la institución, y que constituyen aquellos procesos que se encuentran dentro de los niveles de

riesgo medio y alto y cuya calificación de controles genéricos está por debajo del umbral de riesgo base, dependiendo de si están o no requeridos por la norma de riesgo operativo.

Las observaciones se encuentran agrupadas por el nivel de riesgo alcanzado por los procesos, y las recomendaciones han sido efectuadas considerando el nivel de madurez objetivo definido por la institución, y los aspectos que permitirían mitigar los riesgos tecnológicos a los que se encuentran expuestos actualmente cada uno de los procesos de tecnología de información, en base a las mejores prácticas sugeridas por Cobit 4.1.

Procesos en riesgo alto

- **PO8 Administrar la calidad**

  La institución no cuenta con un sistema de administración de calidad que identifique de forma estándar, formal y continua los requerimientos de calidad para sus procesos clave, y las políticas, criterios y métodos para definir, detectar, corregir y prevenir inconformidades respecto a los requerimientos del negocio. La administración de la calidad es esencial para asegurar que la tecnología de información está entregando valor al negocio, y un mejoramiento continuo y transparente a las partes interesadas de la institución.

  Recomendación:

  Establecer un programa para definir y monitorear actividades de administración de la calidad dentro del área de Sistemas, tanto en sus

proyectos como en sus procesos. Esto permitirá a la entidad llegar a un nivel de madurez 2, desde el cual se deberá partir para establecer un ciclo de mejoramiento continuo.

Plan de acción:

Incluir un proyecto de administración de calidad en el plan operativo del 2009.

- **DS6 Identificar y asignar costos**

  Debido al tamaño de la institución, no existe un sistema de asignación de costos de tecnología de información, ya que esto requiere una medición precisa de sus costos y el acuerdo con los usuarios para su asignación, que permita a la entidad tomar decisiones considerando el uso de los servicios de tecnología de información. Este proceso incrementaría los costos operacionales de la institución, por lo que la decisión de su implementación deberá basarse en un análisis costo – beneficio.

  Recomendación:

  Se recomienda llegar a un nivel de madurez mínimo de 1 con el fin de que haya al menos un entendimiento general de costos de los servicios de información entregados a los usuarios y llegar a monitorear mediante la función de mesa de servicio que se está automatizando actualmente, los costos que por la provisión de servicios informáticos han sido asignados a cada área de la institución. Esto permitirá evaluar el retorno de la inversión en tecnología de información respecto al costo de los servicios que ofrecen los proveedores actuales. Al respecto, además se deberá analizar la factibilidad

de elaborar un adendum al contrato mantenido con Macosa, cuyo valor es importante para la institución, de forma que se optimice la rentabilidad por servicios informáticos.

Plan de acción:

Incluir un proyecto de identificación y asignación de costos general en el plan operativo del 2009, basado en la función de mesa de servicio automatizada y elaborar el adendum sugerido hasta diciembre 2008.

- **ME1 Monitorear y evaluar el desempeño de TI**

  El monitoreo y evaluación del desempeño no existe ni en el área de Sistemas ni en el resto de áreas de la institución. Una administración efectiva del desempeño de la tecnología de información requiere de un proceso de monitoreo, que incluya la definición de indicadores relevantes de desempeño, reportes sistemáticos y periódicos de desempeño y la toma de acciones al detectar desviaciones, sin embargo no se ha implementado un proceso de auditoría informática que permita llevar a cabo estas actividades. El monitoreo es necesario para asegurar que se hacen las cosas correctas y están en línea con el conjunto de políticas y procedimientos institucionales El no contar con este proceso puede afectar la transparencia y entendimiento de los costos, beneficios, estrategia, políticas y niveles de servicio de la tecnología de información de acuerdo con los requerimientos del gobierno corporativo.

  Recomendación:

Debido a que este proceso demanda esfuerzos conjuntos en toda la institución, y que los recursos para lograrlo pueden estar limitados por el tamaño de la entidad, se recomienda tomar las acciones necesarias para llegar a un nivel de madurez de al menos 1, el cual requiere que la alta gerencia reconozca la necesidad de recolectar información necesaria para el monitoreo de procesos, caso por caso, de acuerdo con las necesidades específicas de cada proyecto y proceso de tecnología de información, y con dicha información iniciar un proceso periódico de auditoría informática.

Además, deben establecerse medidas financieras básicas para TI, para lo cual se recomienda utilizar una de las mejores prácticas en tecnología de información.

Plan de acción:

Incluir un proyecto de recolección de información para el monitoreo de cada proceso de TI en el plan operativo del 2009, y dar inicio a las auditorías informáticas periódicas como parte del plan anual de auditoría interna.

Procesos en riesgo medio

- **PO3 Determinar la dirección tecnológica**

  La plataforma tecnológica que da soporte a los procesos de negocio se mantiene y actualiza frente a las demandas de la estrategia empresarial, pero

no existe un proceso de planificación de la infraestructura tecnológica ni un plan que establezca y administre expectativas realistas y claras de lo que la tecnología puede ofrecer en términos de productos, servicios y mecanismos de aplicación. Esto impide garantizar que en el mediano y largo plazo la entidad contará con sistemas aplicativos estándar, bien integrados, rentables y estables, así como recursos y capacidades que satisfagan requerimientos de negocio actuales y futuros.

Recomendación:

Elaborar, aprobar, difundir y aplicar políticas y procedimientos que guíen un proceso de planificación de la infraestructura tecnológica alineado con el plan estratégico de TI. El Comité de Sistemas deberá definir metas y objetivos con respecto al uso de la tecnología en el mediano y largo plazo, basándose en riesgos y la estrategia organizacional, y considerando el desarrollo de planes y productos futuros. La responsabilidad y roles acerca de la administración del plan deberá estar claramente definida en el manual de funciones.

Plan de acción:

Incluir un proyecto de planificación de la infraestructura tecnológica en el plan operativo del 2009.

- **PO4 Definir los procesos, organización y relaciones de TI**

  Pese a que se han definido niveles de servicio adecuados con los proveedores de software y comunicaciones, y que existen procedimientos definidos para los diferentes procesos de tecnología de información, no se ha formalizado las

relaciones del área de Sistemas con los usuarios internos de la entidad. Hace falta definir roles y responsabilidades, niveles de servicio, políticas y métricas de mejoramiento del desempeño desde y hacia los usuarios internos a fin de garantizar agilidad en respuesta a la estrategia de negocios, cumplir los requerimientos de gobierno corporativo y proveer puntos de contacto definidos y competentes en la relación.

Recomendación:

Revisar y definir roles y responsabilidades para los usuarios internos del área de Sistemas, incluido el Comité de Sistemas y Auditoría Interna, y definir el ambiente de control interno para los usuarios dentro de las políticas. Las funciones a ser ejecutadas por el personal de Sistemas así como por terceros debe estar claramente definida, así como los requerimientos de conocimientos y experiencia relacionados con tecnología de información, garantizando siempre una adecuada segregación de funciones.

Plan de acción:

El Jefe de Sistemas deberá dar cumplimiento a la recomendación efectuada, para lo cual trabajará conjuntamente con Auditoría Interna y la Unidad de Riesgos. La aprobación por parte del Comité de Sistemas se realizará hasta diciembre del 2008, y los documentos elaborados se publicarán en la Intranet inmediatamente después.

- **PO6 Comunicar las aspiraciones y la dirección de la gerencia**

Este proceso cuenta con una definición de metas y objetivos, propiedad, repetitividad, roles y responsabilidades, y políticas y procedimientos, sin embargo dichas políticas y procedimientos no se actualizan periódicamente ni han sido utilizadas para capacitar al personal nuevo que ingresa a la institución, lo que podría afectar a la provisión de información precisa y periódica de los servicios actuales y futuros de tecnología de información y sus riesgos y responsabilidades asociados.

Recomendación:

Establecer una política de comunicación, asignación de recursos y mantenimiento de las políticas de control interno en línea con cambios significativos, así como un ambiente de control de información positivo y proactivo. Las políticas, procedimientos y estándares definidos deben mantenerse y comunicarse, formando un componente de buenas prácticas internas, y deben permitir realizar la verificación de su cumplimiento. Toda esta documentación deberá implementarse en el Manual de Políticas y Procedimientos de Sistemas.

Plan de acción:

Incluir en el plan operativo del 2009 la elaboración del Manual de Políticas y Procedimientos de Sistemas, de acuerdo con la recomendación efectuada.

- **PO9 Evaluar y administrar los riesgos de TI**

  La debilidad en la evaluación y administración de los riesgos de TI se encuentra en la falta de definición formal de los roles y responsabilidades

sobre el mismo, pues actualmente una parte lo ejecuta el Jefe de Sistemas, otra parte el Jefe de Riesgos y otra parte los proveedores de software y comunicaciones, pero dichas funciones no han sido formalizadas en el manual orgánico funcional, lo que dificulta el análisis y comunicación de riesgos tecnológicos y su impacto potencial en las metas y procesos de negocio, e impide realizar un seguimiento de su ejecución y que ésta sea efectiva, eficiente y documentada para la rendición de cuentas de resultados y entregables . Además, no existe una metodología formal para la identificación de riesgos tecnológicos por lo que su administración se realiza de manera intuitiva y se podría dar una evaluación incompleta de los mismos.

Hecho subsecuente:

Durante la visita a la entidad, se adoptó el estándar australiano – neozelandés AS/NZ 4360:1999 para la administración de riesgos, el mismo que se está aplicando para este proceso y para el mejoramiento del plan de contingencias de la entidad, pero aún no se ha aprobado formalmente su uso.

Recomendación:

Formalizar en las políticas de administración de riesgos la definición de cuándo y cómo realizar las evaluaciones de riesgos, en base al estándar recientemente adoptado, y garantizando que todos los riesgos claves sean identificados; documentar el proceso de administración de riesgos y hacerlo disponible para todo el personal involucrado.

Elaborar las descripciones de puestos para las responsabilidades de administración de riesgos, incluyendo la rendición de cuentas y los entregables.

Plan de acción:

Los jefes de las áreas de Sistemas y Riesgos deberán presentar una propuesta para dar cumplimiento a la recomendación efectuada hasta diciembre del 2008, para someterlo a revisión y aprobación del Comité de Sistemas hasta enero del 2009. El Jefe de Recursos Humanos deberá elaborar las descripciones de puestos conjuntamente con Auditoría interna para definir las responsabilidades de la administración de riesgos, hasta enero del 2009.

- **AI3 Adquirir y mantener infraestructura tecnológica**

  Pese a que éste es uno de los procesos mejor administrados en la entidad, existe una falta de definición y segregación de políticas y procedimientos, ya que en la generalidad de casos se confunden estos dos términos y por ello al momento existe un manual de procedimientos pero las políticas que los deberían regir no están formalizadas, lo que podría dar lugar a la aplicación de procedimientos inadecuados o no alineados con las políticas establecidas. Adicionalmente, uno de los objetivos del Departamento de Sistemas es la optimización de costos para alcanzar el nivel esperado de escalamiento, flexibilidad e integración, lo cual todavía no se ha conseguido.

Recomendación:

Elaborar, formalizar, difundir, aplicar y verificar periódicamente el cumplimiento de las políticas para la adquisición y mantenimiento de la infraestructura tecnológica, las cuales deberán enmarcarse dentro de un proceso preventivo y en línea con las aplicaciones críticas del negocio y con la arquitectura de la tecnología. Para alcanzar el objetivo del área de Sistemas de optimizar los costos, se recomienda además adoptar buenas prácticas respecto a las soluciones de tecnología, y mantener un proceso de investigación y actualización para conocer las últimas plataformas desarrolladas y herramientas de administración, que permitan reducir costos al racionalizar y estandarizar los componentes de la infraestructura. Las políticas deberán considerar además el mejoramiento del desempeño, incluyendo y siendo consistentes con los procesos de los proveedores externos de la entidad.

Plan de acción:

Implementar las políticas hasta diciembre del 2008, y una vez aprobadas por el Comité de Sistemas, difundirlas y aplicarlas en los proyectos que se incluirán en el plan operativo del 2009.

- **AI7 Instalar y acreditar soluciones y cambios**

  La debilidad de este proceso se encuentra en que no se cuenta con una metodología formal para la realización de pruebas previas a la puesta en producción de los aplicativos, ni para un posible proceso de migración hacia una nueva plataforma, lo cual podría darse al finalizar el contrato actual con la empresa proveedora.

Dada la dependencia existente entre la entidad y el proveedor del software, es de vital importancia contar con la metodología citada para evitar posibles interrupciones en los servicios que presta la entidad a sus clientes o la incursión en costos elevados debidos a una deficiente planificación.

Recomendación:

Elaborar, formalizar, difundir y verificar periódicamente la aplicación de una metodología del ciclo de vida de sistemas que incluya los procesos de instalación, migración, conversión, aceptación y acreditación de datos y sistemas, que consideren el entrenamiento y la planeación e implementación de pruebas, tanto individuales como integradas y de usuario antes de su puesta en producción. Para el efecto se analizará la factibilidad de adoptar buenas prácticas o estándares internacionales.

Plan de acción:

Incluir la elaboración de una metodología del ciclo de vida de sistemas como un proyecto a ejecutar en el primer semestre del plan operativo del 2009.

- **DS3 Administrar el desempeño y la capacidad**

  La entidad realiza la evaluación del desempeño tomando como métricas los niveles de servicio establecidos en los contratos con los proveedores de software y comunicaciones, y utilizando algunas herramientas aisladas para el monitoreo de equipos y enlaces; sin embargo, se desconoce la metodología, políticas y procedimientos que utilizan los proveedores para administrar su propio desempeño y la capacidad de los equipos utilizados para brindar los

servicios tercerizados a la entidad, generando incertidumbre acerca de la eficiencia y eficacia con que son administrados y de la garantía de que los niveles de servicio se mantengan en el tiempo y en situaciones de carga pico y peor escenario.

Recomendación:

Definir en el ciclo de vida de sistemas los requerimientos de desempeño y capacidad y modelar sus pronósticos por medio de un proceso definido. Implementar estadísticas de desempeño para los reportes y publicar los niveles de servicio a los usuarios y clientes, y solicitar la implementación de estas recomendaciones en el proceso de administración de desempeño y capacidad de los proveedores de servicios.

Plan de acción:

Incluir un proyecto de identificación y asignación de costos general en el plan operativo del 2009.

- **DS5 Garantizar la seguridad de los sistemas**

  Por ser una institución pequeña, no existe un oficial de seguridades que desempeñe todas las funciones requeridas para garantizar la seguridad de los sistemas, sino que las mismas son realizadas por diferentes áreas, sin que se haya llegado a formalizar las responsabilidades para una ejecución efectiva, eficiente y documentada de actividades, y se asigne la rendición de cuentas de resultados y entregables.

Recomendación:

Formalizar en el manual de funciones las responsabilidades sobre la seguridad de TI, y establecer las políticas y procedimientos necesarios para administrarlas e implementarlas de forma clara, considerando la realización regular de un análisis de impacto y de riesgos de seguridad, y la ejecución de pruebas utilizando procesos estándares y formales que lleven a mejorar los niveles de seguridad. Para el efecto, se recomienda utilizar mejores prácticas internacionales que además promuevan la conciencia de la seguridad en toda la organización a través de programas de capacitación. Los reportes de seguridad deben estar ligados con los objetivos del negocio y la capacitación sobre seguridad de TI debe ser planeada y administrada de manera que responda a las necesidades del negocio y a los perfiles de riesgo de seguridad.

Además, para cumplir el objetivo institucional de llegar a un nivel 4 de madurez en este proceso, es necesario que los responsables de la auditoría y la administración de la seguridad busquen la certificación en seguridad y se definan indicadores de gestión y cumplimiento.

Plan de acción:

Elaborar un cronograma para la ejecución de todas las actividades recomendadas a partir de octubre del 2008 y hasta el primer semestre del 2009.

- **DS7 Educar y entrenar a los usuarios**

  La institución no cuenta con un programa de capacitación continua ni con políticas y procedimientos que estandaricen el proceso de educación y entrenamiento a los usuarios, tanto de actualización como de inducción a la institución, en temas relativos a la tecnología de información, de manera que se pueda incrementar el uso efectivo y eficiente de los aplicativos y soluciones tecnológicas por medio de la reducción de errores, y la productividad y el cumplimiento de los controles clave, tales como las medidas de seguridad de usuario. Estas debilidades provocan una alta dependencia institucional hacia el personal de Sistemas, quienes han llegado a dominar aspectos del negocio que deberían ser definidos y administrados por los usuarios.

  Recomendación:

  Institucionalizar y comunicar programas de entrenamiento y educación, identificando y documentando las necesidades de cada área, con procesos estandarizados y documentados que cuenten con presupuestos, recursos, instructores e instalaciones.

  Dichos programas deben incluir clases formales sobre conducta ética y sobre conciencia y prácticas de seguridad en los sistemas, y deben ser monitoreados y evaluados.

  Plan de acción:

Elaborar hasta diciembre 2008 las políticas y procedimientos necesarias para dar cumplimiento a las recomendaciones indicadas, y aplicarlas y verificar su cumplimiento a partir del plan operativo del 2009.

- **DS9 Administrar la configuración**

  Pese a que existen algunas métricas que permiten percibir el desempeño del proceso y la utilización de recursos, éstas se encuentran definidas en los contratos de tercerización de servicios para su monitoreo diario antes del pago mensual, pero no están regidas por políticas y procedimientos que permitan monitorear periódicamente la configuración de los equipos administrados por los proveedores externos.

  Esta deficiencia hace vulnerable la disponibilidad de los sistemas, la productividad y la solución de incidentes y problemas de tecnología de información, que podrían ocasionar una interrupción de los servicios que brinda la entidad a sus clientes.

  Recomendación:

  Elaborar, aprobar, difundir al personal involucrado y verificar la aplicación de políticas y procedimientos de administración de la configuración de los equipos locales y el monitoreo periódico de la configuración de equipos administrados por los proveedores externos, que incluyan procesos estandarizados y documentados. Se deben utilizar herramientas similares de administración de configuración entre plataformas y se debe analizar la factibilidad de mantener

un proceso de actualización continua para el personal técnico de la entidad en las plataformas de equipos utilizados por los proveedores externos.

Plan de acción:

Elaborar y aprobar las políticas hasta diciembre del 2008 e incluir el resto de actividades recomendadas en el plan operativo del 2009.

- **DS10 Administrar los problemas**

  No está asignada la rendición de cuentas de resultados y entregables, ni se han definido políticas, planes, procedimientos o métricas para percibir los resultados y desempeño del proceso, lo que impide garantizar la satisfacción de los usuarios finales con los servicios recibidos, y puede conducir a duplicar esfuerzos y mantener defectos en la prestación de los servicios y las soluciones. La herramienta automatizada para la función de mesa de servicio ha sido concebida para la administración de incidentes, por lo que no tiene la funcionalidad de identificación y seguimiento de problemas.

  Recomendación:

  Elaborar, aprobar, comunicar y aplicar políticas y procedimientos para administración de problemas con alcance a toda la institución, en las que las responsabilidades y la propiedad de los problemas estén claramente establecidas, y se defina la identificación, registro y reporte de los problemas para iniciar su solución. Además se deberá implementar un procedimiento periódico de revisión para evaluar su efectividad. La administración de problemas deberá estar integrada con los procesos interrelacionados, tales

como administración de incidentes, de cambios, y de configuración, y deberá contar con indicadores de logro y de desempeño. La herramienta automatizada para la función de mesa de servicio deberá incluir la identificación, reporte y seguimiento de los problemas para facilitar esta tarea.

Plan de acción:

Modificar la herramienta automatizada con la recomendación efectuada hasta noviembre del 2008, y dar cumplimiento al resto de recomendaciones hasta junio del 2009.

- **DS11 Administrar los datos**

  No existen políticas que permitan garantizar una efectiva administración de datos, la librería de medios, respaldos y recuperación de datos y la eliminación apropiada de medios, lo que podría afectar a la calidad, oportunidad y disponibilidad de la información del negocio.

  Recomendación:

  Elaborar, aprobar, difundir y aplicar políticas y procedimientos que reflejen el entendimiento y la necesidad de la administración de datos, tanto dentro de TI como a lo largo de toda la organización, considerando la utilización de algunas herramientas para respaldos / recuperación y desecho de equipo. Su responsabilidad debe estar establecida en el manual de funciones, siendo los propietarios de los datos los responsables de controlar la integridad y la seguridad. Además se deberán definir métricas básicas de desempeño, de preferencia con la utilización de estándares y mejores prácticas.

Plan de acción:

Elaborar, aprobar y difundir las políticas hasta diciembre del 2008, y verificar su cumplimiento en el plan operativo del 2009.

- **ME2 Monitorear y evaluar el control interno**

  La entidad no cuenta con un programa de control interno efectivo para TI, que incluya el monitoreo y el reporte de las excepciones de control, resultados de auto-evaluaciones y revisiones por parte de terceros, excepto por las supervisiones efectuadas en las auditorías financieras, lo que no garantiza seguridad respecto a las operaciones eficientes y efectivas y el cumplimiento de las leyes y regulaciones aplicables. Esto se evidencia por la falta de metas y objetivos estratégicos, políticas, planes, procedimientos y métricas de mejoramiento del desempeño que permitan proteger el logro de los objetivos de tecnología de información.

Recomendación:

La Gerencia General deberá apoyar e institucionalizar el monitoreo del control interno como una estrategia del Plan Estratégico Institucional, y por medio del desarrollo de políticas y procedimientos para evaluar y reportar las actividades de monitoreo, así como un programa de educación y entrenamiento para el monitoreo del control interno. Además se deberá definir un proceso periódico para auto-evaluaciones y revisiones de aseguramiento del control interno, con roles definidos para los responsables de la administración del negocio y de TI, y la utilización de herramientas. Las políticas deben considerar también el

manejo y mitigación de riesgos específicos de procesos de tecnología de información, derivados de las auto-evaluaciones.

Plan de acción:

Dar cumplimiento a la recomendación expuesta hasta diciembre del 2008, con alcance al área de Sistemas, y hasta junio del 2009 para el resto de áreas de la institución.

- **ME4 Proporcionar gobierno de TI**

  No existe una integración adecuada del gobierno de tecnología de información con los objetivos de gobierno corporativo de la entidad, ya que en la actualidad el Comité de Sistemas es únicamente aprobador y no emite directrices sobre los requerimientos de gobierno de TI. Esto se evidencia por la falta de roles y responsabilidades definidos, la revisión periódica del cumplimiento de políticas y procedimientos de Sistemas, y la definición de métricas que permitan percibir los resultados y desempeño del proceso.

  Recomendación:

  La Gerencia General y el Comité de Administración deben reconocer la importancia y la necesidad de un gobierno de TI, y elaborar un conjunto de indicadores base en los que se definan y documenten los resultados. El Comité de Sistemas deberá estandarizar los procedimientos para gobierno de TI, difundirlos para establecer un programa de entrenamiento en su aplicación e identificar herramientas que apoyen a la supervisión del gobierno de TI.

Plan de acción:

Dar cumplimiento a la recomendación hasta marzo del 2009.

CONCLUSIÓN DEL INFORME

Desde la auditoría informática efectuada por parte de la Superintendencia de Bancos y Seguros en abril del 2007, la institución ha disminuido su riesgo tecnológico de un nivel alto a un nivel medio. El riesgo tecnológico que presenta actualmente la entidad se debe principalmente a la inexistencia de controles de mejoramiento del desempeño y a la falta de formalización y aplicación de políticas que rijan cada uno de los procesos de tecnología de información.

En la presente evaluación, los procesos de TI se han ubicado principalmente en los niveles de riesgo bajo y medio, pero la falta de definición de políticas y la inexistencia de los procesos de administración de la calidad, la identificación y asignación de costos, y el monitoreo y evaluación del desempeño de TI, podrían ocasionar a largo plazo una débil gestión de la tecnología de información y por ende, una baja productividad organizacional, por lo que es preciso que las acciones de mejora sugeridas se lleven a cabo durante los próximos 12 meses.

Un factor decisivo en el mejoramiento de la calificación obtenida en la presente visita, con respecto a la anterior, es la adopción del marco de trabajo Cobit que ha efectuado la institución, como una de las mejores prácticas en la administración de la plataforma tecnológica, la cual, si es aplicada en forma consistente en los

procesos relevantes de la entidad, conjuntamente con otros estándares y buenas prácticas internacionales, permitirá mitigar los posibles riesgos actuales y futuros a los que se encuentren expuestos los procesos de tecnología de información, por lo que se recomienda la capacitación y la investigación continua de dichos temas, lo que permitirá a la entidad ir más allá del cumplimiento regulatorio y orientarse hacia un buen gobierno de tecnología de información.

Una vez concluido, el informe fue conocido por la jefatura de Sistemas y posteriormente se realizó una nueva reunión con el Comité de Sistemas para comunicarles los análisis efectuados y las recomendaciones y acciones de mejora sugeridas para mitigar los riesgos tecnológicos a los que se encuentran expuestos los procesos de tecnología de información relevantes para la institución.

CAPÍTULO 5: CONCLUSIONES Y RECOMENDACIONES

5.1 - Conclusiones

a) Las etapas y actividades planteadas para la metodología de evaluación del riesgo tecnológico, permitieron alcanzar los objetivos propuestos al inicio del proyecto y que son:
   - Obtener un valor cuantificable del grado de cumplimiento en cada uno de los aspectos asociados a la tecnología de información requeridos para la administración del riesgo operativo,
   - Establecer los objetivos de control de COBIT 4.1 que satisfacen los requerimientos normativos de tecnología de información,
   - Reflejar en el mapa de riesgo tecnológico las mediciones de madurez e importancia de los procesos de tecnología de información; y,
   - Validar la consistencia y efectividad de la metodología por medio de la implementación de un plan piloto en una institución financiera controlada por la Superintendencia de Bancos y Seguros.

b) El plan piloto en el que se aplicó la metodología propuesta para la evaluación del riesgo tecnológico, permitió determinar que de su aplicación se obtienen resultados consistentes con la realidad de la institución evaluada, utilizando una de las mejores prácticas en administración de la tecnología de información, como lo es el marco de trabajo de Cobit.

c) El conocimiento previo que el equipo de proyecto debe tener sobre el marco de trabajo de Cobit, limita pero no impide la ejecución de la metodología propuesta, ya que al no contar con dicho conocimiento, se deberá emplear mayor tiempo en el entendimiento de cada proceso de tecnología de información que se va a evaluar.

d) Por tratarse de una metodología de evaluación del riesgo tecnológico que permite realizar un autodiagnóstico en las instituciones del sistema financiero ecuatoriano, el grado de honestidad y objetividad durante la evaluación es importante para obtener resultados consistentes y confiables. Por ello es necesario que cada etapa de evaluación sea realizada conjuntamente por personas que pertenezcan a diferentes áreas de la institución evaluada, o involucrar a Auditoría Interna en todas ellas.

e) La determinación del grado de madurez actual y objetivo para cada proceso de tecnología de información permiten obtener resultados más ajustados respecto de la situación real de una institución financiera, además de que permiten orientar las recomendaciones del informe de evaluación a la consecución de los objetivos planteados en cada proceso en forma gradual. Sin embargo, el mayor peso en la calificación obtenida está dada por la aplicación de controles, debido a que éstos permiten mitigar los riesgos a los que podría estar expuesto un proceso.

f) Desde el punto de vista de ITIL, una de las buenas prácticas de tecnología de información, la presente metodología incorpora el modelo de mejora continua del servicio, que establece la visión (cumplimiento normativo), la evaluación de la situación actual (etapa B y nivel de madurez actual), el planteamiento de objetivos (nivel de madurez objetivo), el método para alcanzar los objetivos (recomendaciones), y las mediciones y métricas para evaluar la consecución (mapa de riesgo tecnológico).

5.2 - Recomendaciones

a) Se recomienda realizar más pruebas con instituciones en las que el nivel de automatización o dependencia de la tecnología sea baja y alta, pues el plan piloto se efectuó únicamente en una institución con un nivel de automatización medio, así como más evaluaciones en diferentes períodos de tiempo para segmentos de mercado homogéneos, lo que permitirá evidenciar debilidades comunes que puedan ser resueltas con la unión de esfuerzos conjuntos y de esa manera minimizar costos operativos en la implementación de soluciones informáticas o prevenir situaciones no deseadas en el futuro.

b) En la planificación del proyecto se sugiere considerar los tiempos de holgura especificados para cada actividad con respecto a su tiempo efectivo, de modo que se pueda ajustar los recursos humanos y de

tiempo empleados para culminar el proyecto en un plazo adecuado. No se recomienda extender los plazos de holgura fijados puesto que las condiciones de la plataforma tecnológica evaluada podrían variar en ese lapso, dando lugar a una duplicación de esfuerzos.

c) La presente metodología es perfectible en la medida en que las instituciones que deseen aplicarla tengan un mayor apetito de exigibilidad durante la evaluación; de ser ése el caso, se recomienda utilizar parámetros más estrictos de evaluación tales como un umbral de riesgo más alto o la utilización de un impacto alto para la mayoría de procesos de tecnología de información, con lo que se logrará maximizar el riesgo al que se encuentra expuesta la plataforma tecnológica de la entidad a evaluar.

d) La metodología puede ser aún más ajustada a la realidad de las instituciones evaluadas asignando pesos por importancia a los 24 controles genéricos que se evalúan en cada proceso de tecnología de información. Se recomienda que dichos pesos sean asignados por el organismo de control o un ente independiente para que las evaluaciones realizadas sean homogéneas en cada tipo de institución.

e) Debido a que el plazo para dar cumplimiento a la norma que rige la administración del riesgo operativo vence en octubre del 2008 para bancos, sociedades financieras, compañías de arrendamiento mercantil, compañías emisoras y administradoras de tarjetas de crédito,

corporaciones de desarrollo de mercado secundario de hipotecas, e instituciones financieras públicas, y en octubre del 2009 para cooperativas y mutualistas, se recomienda difundir y aplicar la presente metodología de evaluación del riesgo tecnológico para cumplir con dicho requerimiento del organismo de control.

f) Una herramienta que es de total actualidad y aplicabilidad en las empresas no solo financieras sino de cualquier naturaleza, es la Administración de Riesgos, la misma que ha servido de base para la presente metodología y por ello se recomienda que sea incorporada en el pénsum académico de la carrera de Ingeniería de Sistemas e Informática de la ESPE.

BIBLIOGRAFÍA

Internet

- www.google.com.ec, Google Ecuador
- www.bis.org, Bank for International Settlements
- www.superban.gov.ec, Superintendencia de Bancos y Seguros
- www.finanware.com/riesgo_operativo.htm, Finanware - A business intelligence solution
- www.objectrisk.com/riesgooperacional.htm, ObjectRisk OP - Riesgo operacional
- http://secretosenred.com/articles/2217/1/DISENANDO-LA-ESTRATEGIA-EMPRESARIAL/Paacutegina1.html
- www.rincondelvago.com - monografía de Luis Gonzalo Omar Molina, Planeamiento estratégico.
- http://www.mitecnologico.com/Main/AnalisisDeRiesgos

Documentos

- Comité de Supervisión Bancaria de Basilea (2004), Presentación del Nuevo Acuerdo de Capital de Basilea.
- Codificación de resoluciones de la Superintendencia de Bancos y Seguros y de la Junta Bancaria.
- Rodrigo Mora Guzmán, Taller de Riesgo Operativo - Basilea II.

- Superintendencia de Bancos y Seguros (2004), Resultados de la encuesta sobre Riesgo Operativo.
- Lucio Molina Focazzio (2007), COBIT - Un marco de Referencia en Controles para TI.
- IT Governance Institute (2005), COBIT® 4.0, Rolling Meadows, USA.
- IT Governance Institute (2007), COBIT® 4.1, Rolling Meadows, USA.
- IT Governance Institute (2007), IT Governance Using COBIT® and Val IT™: Student book, 2nd Edition, Rolling Meadows, USA.
- IT Governance Institute (2007), IT Governance Implementation Guide Using COBIT® and Val IT™, 2nd Edition, Rolling Meadows, USA.
- IT Governance Institute (2007), IT Assurance Guide Using COBIT®, Rolling Meadows, USA.
- E. Fowler Newton, Tratado de Auditoría, tomo II, capítulo XXV.

BIOGRAFÍA

Katalina del Rocío Coronel Hoyos

Datos Generales

Lugar y fecha de nacimiento: Quito, 17 de junio de 1970.

Domicilio: Jumandi Oe2-454 y Av. Jipijapa, Ciudadela Atahualpa
Tel. (593) 2 - 2617 315

Trabajo: Auditor informático, Superintendencia de Bancos y Seguros
Av. 12 de octubre 1561 y Madrid
Tel. (593) 2 - 2547 642 / 2231 613

E-mail: katysan33@yahoo.com

Estudios cursados

Primaria: ***Escuela Femenina "Espejo"***
1976 - 1982

Secundaria: ***Colegio Experimental "24 de mayo"***
Título: Bachiller en ciencias, especialización Químico Biológicas
1982 - 1988

Superior: ***Escuela Politécnica del Ejército***
Título: Analista de Sistemas
Junio - 1994

Escuela Politécnica del Ejército
Egresada de la carrera de Ingeniería en Sistemas e Informática
Agosto - 2001.

Inglés: ***British Council***
Nivel pre-intermedio, julio 1998
Escuela Politécnica del Ejército
Cuarto nivel, marzo 2002
Universidad de Michigan
Advanced Diploma, 2003
The International Bénédict Schools of Languages
Suficiencia y Proficiencia, junio 2003

HOJA DE LEGALIZACIÓN DE FIRMAS

ELABORADA POR

_____
Katalina Coronel Hoyos

COORDINADOR DE LA CARRERA

_____
Ing. Ramiro Delgado

Lugar y fecha: _____

HOMOLOGACIÓN ENTRE REQUERIMIENTOS NORMATIVOS Y OBJETIVOS DE CONTROL DE COBIT 4.1

No.	Requerimiento normativo	Objetivo de control de Cobit	
1	1.3.1.1 El apoyo y compromiso formal del directorio u organismo que haga sus veces y la alta gerencia;	PO4	Definir los procesos, organización y relaciones de TI
2	1.3.1.2 Un plan funcional de tecnología de información alineado con el plan estratégico institucional; y, un plan operativo que establezca las actividades a ejecutar en el corto plazo (un año), de manera que se asegure el logro de los objetivos institucionales propuestos;	PO1	Definir un plan estratégico de TI
3	1.3.1.3 Tecnología de información acorde a las operaciones del negocio y al volumen de transacciones, monitoreada y proyectada según las necesidades y crecimiento de la institución;	PO3	Determinar la dirección tecnológica
4	1.3.1.4 Un responsable de la información que se encargue principalmente de definir y autorizar de manera formal los accesos y cambios funcionales a las aplicaciones y monitorear el cumplimiento de los controles establecidos;	PO4	Definir los procesos, organización y relaciones de TI
5	1.3.1.5 Políticas, procesos y procedimientos de tecnología de información definidos bajo estándares de general aceptación que garanticen la ejecución de los criterios de control interno de eficacia, eficiencia y cumplimiento, debidamente aprobados por el directorio u organismo que haga sus veces, alineados a los objetivos y actividades de la institución;	PO6	Comunicar las aspiraciones y la dirección de la gerencia
6	1.3.1.6 Difusión y comunicación a todo el personal involucrado de las mencionadas políticas, procesos y procedimientos, de tal forma que se asegure su implementación; y,	PO6	Comunicar las aspiraciones y la dirección de la gerencia
7	1.3.1.7 Capacitación y entrenamiento técnico al personal del área de tecnología de información y de los usuarios de la misma.	DS7	Educar y entrenar a los usuarios
		PO7	Administrar recursos humanos de TI
	Requerimiento normativo	**Objetivo de control de Cobit**	
8	1.3.2.1 Manuales o reglamentos internos, debidamente aprobados por el directorio u organismo que haga sus veces, que establezcan como mínimo las responsabilidades y procedimientos para la operación, el uso de las instalaciones de procesamiento de información y respuestas a incidentes de tecnología de información;	DS13	Administrar las operaciones
9	1.3.2.2 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;	DS9	Administrar la configuración
	Requerimiento normativo	**Objetivo de control de Cobit**	
10	1.3.3.1 Requerimientos contractuales convenidos que definan la propiedad de la información y de las aplicaciones; y, la responsabilidad de la empresa proveedora de la tecnología en caso de ser vulnerables sus sistemas, a fin de mantener la integridad, disponibilidad y confidencialidad de la información; y,	DS2	Administrar los servicios de terceros

11	1.3.3.2 Requerimientos contractuales convenidos que establezcan que las aplicaciones sean parametrizables, que exista una transferencia del conocimiento y que se entregue documentación técnica y de usuario, a fin de reducir la dependencia de las instituciones controladas con proveedores externos y los eventos de riesgo operativo que esto origina.	AI5	Adquirir recursos de TI
	Requerimiento normativo	**Objetivo de control de Cobit**	
12	1.3.4.1 Políticas y procedimientos de seguridad de la información que establezcan sus objetivos, importancia, normas, principios, requisitos de cumplimiento, responsabilidades y comunicación de los incidentes relativos a la seguridad; considerando los aspectos legales, así como las consecuencias de violación de estas políticas;	DS5	Garantizar la seguridad de los sistemas
13	1.3.4.2 La identificación de los requerimientos de seguridad relacionados con la tecnología de información, considerando principalmente: la evaluación de los riesgos que enfrenta la institución; los	DS5	Garantizar la seguridad de los sistemas
		PO9	Evaluar y administrar los riesgos de TI
14	1.3.4.3 Los controles necesarios para asegurar la integridad, disponibilidad y confidencialidad de la información administrada;	DS11	Administrar los datos
15	1.3.4.4 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 en todos los ambientes de procesamiento;	DS5	Garantizar la seguridad de los sistemas
16	1.3.4.5 Niveles de autorización de accesos y ejecución de las funciones de procesamiento de las aplicaciones, formalmente establecidos, que garanticen una adecuada segregación de funciones y reduzcan el riesgo de error o fraude;	DS5	Garantizar la seguridad de los sistemas
		PO4	Definir los procesos, organización y relaciones de TI
17	1.3.4.6 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;	DS5	Garantizar la seguridad de los sistemas
18	1.3.4.7 Controles adecuados para detectar y evitar la instalación de software no autorizado o sin la respectiva licencia, así como instalar y actualizar periódicamente aplicaciones de detección y desinfección de virus informáticos y demás software maliciosos;	DS5	Garantizar la seguridad de los sistemas
19	1.3.4.8 Controles formales para proteger la información contenida en documentos; medios de almacenamiento u otros dispositivos externos; el uso e intercambio electrónico de datos contra daño, robo, accesos, utilización o divulgación no autorizada de información para fines contrarios a los intereses de la entidad, por parte de todo su personal y de sus proveedores;	DS13	Administrar las operaciones
		DS5	Garantizar la seguridad de los sistemas
20	1.3.4.9 Instalaciones de procesamiento de información crítica en áreas protegidas con los suficientes controles que eviten el acceso de personal no autorizado y daños a los equipos de computación y a la información en ellos procesada, almacenada o distribuida;	DS12	Administrar el ambiente físico
21	1.3.4.10 Las condiciones físicas y ambientales necesarias para garantizar el correcto funcionamiento del entorno de la infraestructura de tecnología de información;	DS12	Administrar el ambiente físico
22	1.3.4.11 Un plan para evaluar el desempeño del sistema de administración de la seguridad de la información, que permita tomar acciones orientadas a mejorarlo; y,	DS5	Garantizar la seguridad de los sistemas

23	1.3.4.12 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 de información; que existan mecanismos alternos que garanticen la continuidad del servicio ofrecido; y, que aseguren la existencia de pistas de auditoría.	DS5	Garantizar la seguridad de los sistemas
	Requerimiento normativo	**Objetivo de control de Cobit**	
24	1.3.5.1 Controles para minimizar riesgos potenciales de sus equipos de computación ante eventos imprevistos, tales como: fallas, daños o insuficiencia de los recursos de tecnología de información; robo; incendio; humo; inundaciones; polvo; interrupciones en el fluido eléctrico, desastres naturales; entre otros;	AI3	Adquirir y mantener infraestructura tecnológica
		DS12	Administrar el ambiente físico
25	1.3.5.2 Políticas y procedimientos de respaldo de información periódicos, que aseguren al menos que la información crítica pueda ser recuperada en caso de falla de la tecnología de información o con posterioridad a un evento inesperado;	DS4	Garantizar la continuidad del servicio
26	1.3.5.3 Mantener los sistemas de comunicación y redundancia de los mismos que permitan garantizar la continuidad de sus servicios; y,	DS4	Garantizar la continuidad del servicio
27	1.3.5.4 Información de respaldo y procedimientos de restauración en una ubicación remota, a una distancia adecuada que garantice su disponibilidad ante eventos de desastre en el centro principal de procesamiento.	DS4	Garantizar la continuidad del servicio
	Requerimiento normativo	**Objetivo de control de Cobit**	
28	1.3.6.1 Una metodología que permita la adecuada administración y control del proceso de compra de	PO8	Administrar la calidad
29	1.3.6.2 Documentación técnica y de usuario permanentemente actualizada de las aplicaciones de la institución;	AI4	Facilitar la operación y el uso
		AI6	Administrar cambios
30	1.3.6.3 Controles que permitan asegurar la adecuada administración de versiones de las aplicaciones puestas en producción; y,	AI6	Administrar cambios
31	1.3.6.4 Controles que permitan asegurar que la calidad de la información sometida a migración, cumple con las características de integridad, disponibilidad y confidencialidad.	PO3	Determinar la dirección tecnológica
		AI7	Instalar y acreditar soluciones y cambios
	Requerimiento normativo	**Objetivo de control de Cobit**	
32	Contar con políticas y procedimientos que permitan la adecuada administración, monitoreo y documentación de las bases de datos, redes de datos, software de base y hardware.	DS3	Administrar el desempeño y la capacidad

Actividades
PO4.6, PO4.10
PO1.4, PO1.5
PO4.9
PO6.1, PO6.3, PO6.4
PO6.5
DS7.1, DS7.2, DS7.3
PO7.4
Actividades
DS13.1
DS9.1
Actividades
DS2.1, DS2.2, DS2.3, DS2.4

AI5.2, AI5.4, AI5.5
Actividades
DS5.2
DS5.1, DS5.6
DS11.1-6
DS5.4
DS5.3
PO4.11
DS5.3
DS5.9
DS13.4
DS5.11
DS12.3
DS12.1, DS12.2, DS12.4
DS5.5

DS5.11
Actividades
AI3.2
DS12.2, DS12.4
DS4.3, DS4.9
DS4.2
DS4.8
Actividades
PO8.3
AI4.1
AI6.5
AI6.1, AI6.4
PO3.1
AI7.5
Actividades
DS3.1, DS3.2, DS3.5

Metodología de evaluación del riesgo tecnológico, utilizando Cobit 4.1

Presentación del proyecto

ANTECEDENTES

- En el 2004, Basilea II incluyó en sus estándares el riesgo operativo
- El 20 de octubre del 2005 la SBS emitió la resolución No. JB-2005-834
- El 4 de abril del 2006 se emite la circular No. SBS-INIF-DNR-SRO-2006-1539
- En el año 2007, el ITGI emite la versión 4.1 de Cobit, que brinda directrices gerenciales para el control de la TI

OBJETIVOS

- Desarrollar una metodología para cuantificar el grado de cumplimiento normativo en cada uno de los procesos de tecnología de información, como parte de la administración del riesgo operativo
- Utilizar una de las mejores prácticas en TI para diagnosticar el riesgo tecnológico en las entidades controladas por la SBS
- Validar la metodología desarrollada mediante la implantación de un plan piloto

ALCANCE (1)

Instituciones financieras

NORMA DE RIESGO OPERATIVO - TI

1. Planeación y estrategia de la tecnología de información
2. Cumplimiento de requerimientos operativos de la entidad
3. Relaciones con terceros
4. Administración de seguridad
5. Continuidad de las operaciones
6. Adquisición, desarrollo, implementación y mantenimiento de aplicaciones
7. Políticas y procedimientos de administración de la infraestructura de tecnología de información

COBIT 4.1

PO - Planear y organizar
AI - Adquirir e implementar
DS - Entregar y dar soporte
ME - Monitorear y evaluar

ALCANCE (2)

MAPA DE EVALUACIÓN DEL RIESGO TECNOLÓGICO

ENTIDAD:

FECHA DE CORTE:

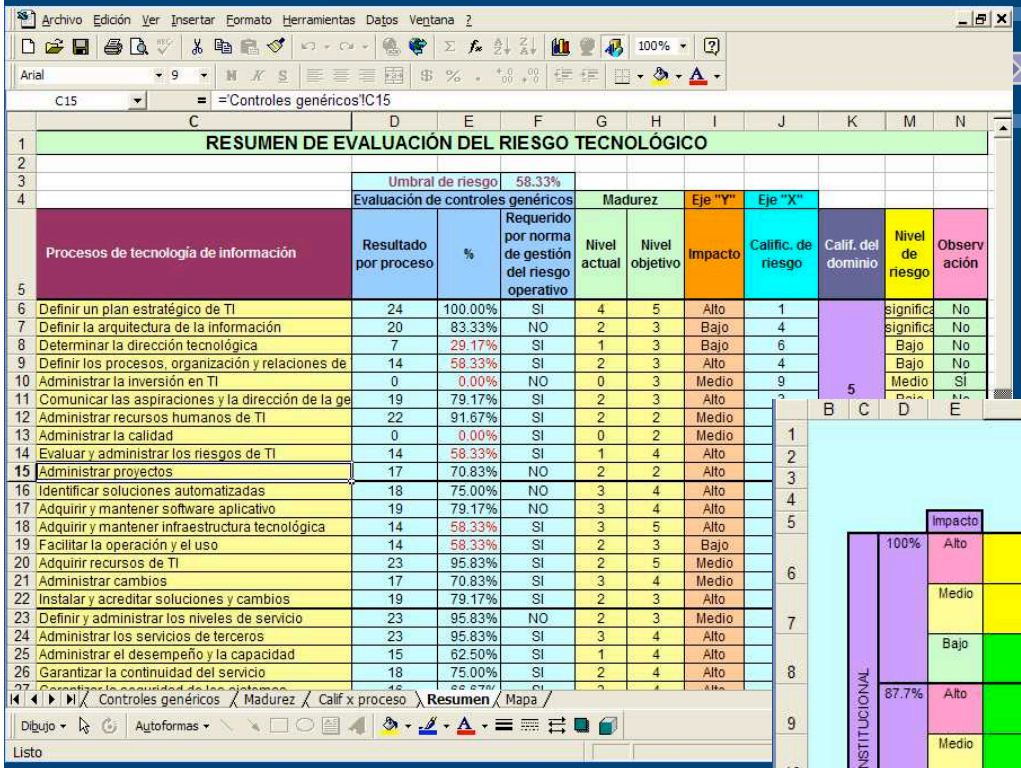
RIESGO INSTITUCIONAL		Impacto									
	100%	Alto									
		Medio									
		Bajo									
	80%	Alto	AI4							ME1	PO9
		Medio		PO3 AI3 DS7 DS12	AI7		PO2	PO6	DS10	PO10 DS6	
		Bajo	PO1 AI5 AI6 DS9 DS13	PO4 PO8 DS2 DS4 DS5 DS11			DS1	PO5 PO7	DS3	DS8 ME2 ME3 ME4	AI1 AI2
	60%	Alto									
		Medio									
		Bajo									
		0	1	2	3	4	5	6	7	8	9
			NIVEL DE RIESGO ALCANZADO POR CADA PROCESO DE TECNOLOGÍA DE INFORMACIÓN								

ALCANCE (3)

INFORME DE EVALUACIÓN

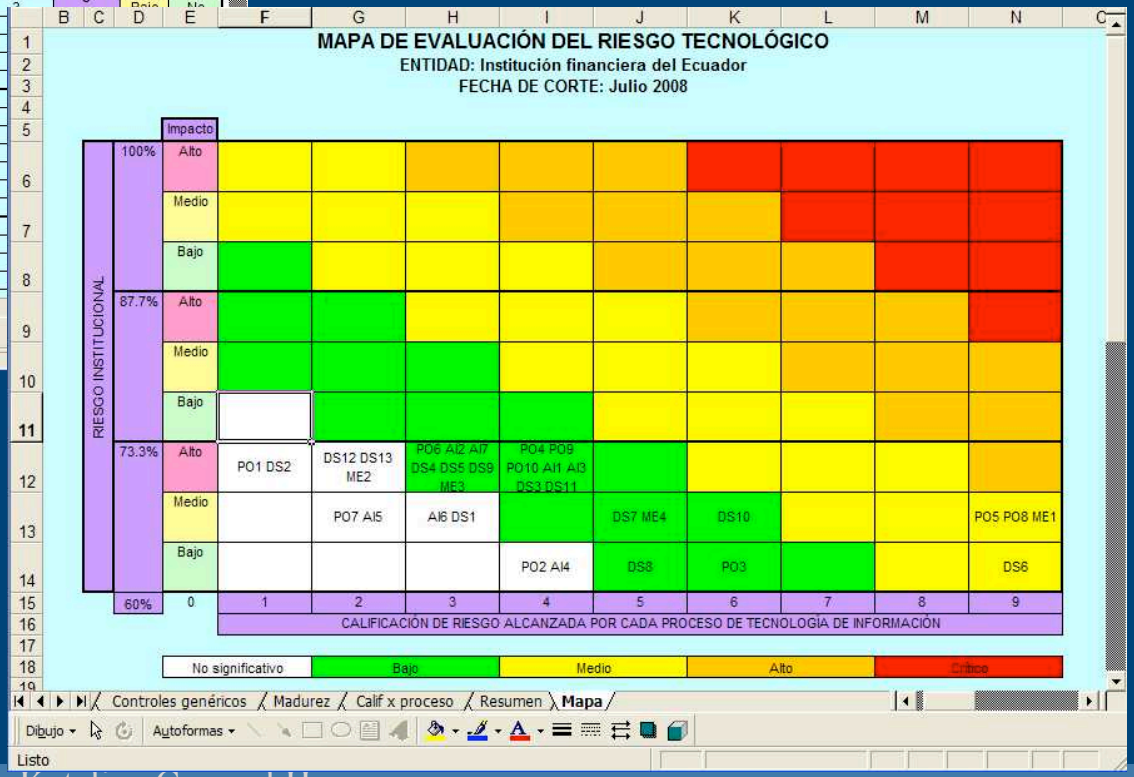
- Hallazgos
- Recomendaciones
- Plan de acción

ALCANCE (4)



RESUMEN DE EVALUACIÓN DEL RIESGO TECNOLÓGICO

Procesos de tecnología de información	Resultado por proceso	%	Requerido por norma de gestión del riesgo operativo	Nivel actual	Nivel objetivo	Impacto	Calific. de riesgo	Calif. del dominio	Nivel de riesgo	Observación
	Umbral de riesgo	58.33%								
	Evaluación de controles genéricos			Madurez		Eje "Y"	Eje "X"			
Definir un plan estratégico de TI	24	100.00%	SI	4	5	Alto	1		significa	No
Definir la arquitectura de la información	20	83.33%	NO	2	3	Bajo	4		significa	No
Determinar la dirección tecnológica	7	29.17%	SI	1	3	Bajo	6		Bajo	No
Definir los procesos, organización y relaciones de	14	58.33%	SI	2	3	Alto	4		Bajo	No
Administrar la inversión en TI	0	0.00%	NO	0	3	Medio	9	5	Medio	SI
Comunicar las aspiraciones y la dirección de la ge	19	79.17%	SI	2	3	Alto				
Administrar recursos humanos de TI	22	91.67%	SI	2	2	Medio				
Administrar la calidad	0	0.00%	SI	0	2	Medio				
Evaluar y administrar los riesgos de TI	14	58.33%	SI	1	4	Alto				
Administrar proyectos	17	70.83%	NO	2	2	Alto				
Identificar soluciones automatizadas	18	75.00%	NO	3	4	Alto				
Adquirir y mantener software aplicativo	19	79.17%	NO	3	4	Alto				
Adquirir y mantener infraestructura tecnológica	14	58.33%	SI	3	5	Alto				
Facilitar la operación y el uso	14	58.33%	SI	2	3	Bajo				
Adquirir recursos de TI	23	95.83%	SI	2	5	Medio				
Administrar cambios	17	70.83%	SI	3	4	Medio				
Instalar y acreditar soluciones y cambios	19	79.17%	SI	2	3	Alto				
Definir y administrar los niveles de servicio	23	95.83%	NO	2	3	Medio				
Administrar los servicios de terceros	23	95.83%	SI	3	4	Alto				
Administrar el desempeño y la capacidad	15	62.50%	SI	1	4	Alto				
Garantizar la continuidad del servicio	18	75.00%	SI	2	4	Alto				



MAPA DE EVALUACIÓN DEL RIESGO TECNOLÓGICO

ENTIDAD: Institución financiera del Ecuador

FECHA DE CORTE: Julio 2008

RIESGO INSTITUCIONAL		Impacto	1	2	3	4	5	6	7	8	9
	100%	Alto									
		Medio									
		Bajo									
	87.7%	Alto									
		Medio									
		Bajo									
	73.3%	Alto	PO1 DS2	DS12 DS13 ME2	PO6 AI2 AI7 DS4 DS5 DS9 ME3	PO4 PO9 PO10 AI1 AI3 DS3 DS11					
		Medio		PO7 AI5	AI6 DS1		DS7 ME4	DS10			PO5 PO8 ME1
		Bajo				PO2 AI4	DS8	PO3			DS6
	60%	0									

CALIFICACIÓN DE RIESGO ALCANZADA POR CADA PROCESO DE TECNOLOGÍA DE INFORMACIÓN

No significativo	Bajo	Medio	Alto	Crítico

COBIT

- Acrónimo de *Control Objectives for Information and Related Technology* - objetivos de control para la información y las tecnologías relacionadas
- Su misión es investigar, desarrollar, publicar y promover un marco de trabajo de control de gobierno de TI autorizado y actualizado, internacionalmente aceptado y adoptado para el uso cotidiano de las empresas, gerentes de negocios, profesionales de TI y de Aseguramiento.
- Agrupa un conjunto de estándares y mejores prácticas internacionales en sus procesos, tales como ISO 9001, ISO 27002, ITIL, AS/NZ 4360, PMBOK, etc.

APLICACIÓN DE COBIT (1)

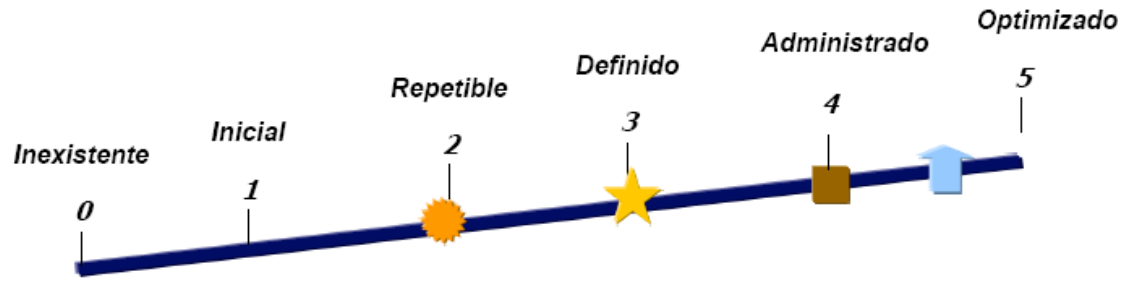
PROCESOS DE TECNOLOGÍA DE INFORMACIÓN DE COBIT 4.1	
PLANEAR Y ORGANIZAR	**ENTREGAR Y DAR SOPORTE**
PO1 Definir un plan estratégico de TI	DS1 Definir y administrar los niveles de servicio
PO2 Definir la arquitectura de la información	DS2 Administrar los servicios de terceros
PO3 Determinar la dirección tecnológica	DS3 Administrar el desempeño y la capacidad
PO4 Definir los procesos, organización y relaciones de TI	DS4 Garantizar la continuidad del servicio
PO5 Administrar la inversión en TI	DS5 Garantizar la seguridad de los sistemas
PO6 Comunicar las aspiraciones y la dirección de la gerencia	DS6 Identificar y asignar costos
PO7 Administrar recursos humanos de TI	DS7 Educar y entrenar a los usuarios
PO8 Administrar la calidad	DS8 Administrar la mesa de servicio y los incidentes
PO9 Evaluar y administrar los riesgos de TI	DS9 Administrar la configuración
PO10 Administrar proyectos	DS10 Administrar los problemas
ADQUIRIR E IMPLANTAR	DS11 Administrar los datos
AI1 Identificar soluciones automatizadas	DS12 Administrar el ambiente físico
AI2 Adquirir y mantener software aplicativo	DS13 Administrar las operaciones
AI3 Adquirir y mantener infraestructura tecnológica	**MONITOREAR Y EVALUAR**
AI4 Facilitar la operación y el uso	ME1 Monitorear y evaluar el desempeño de TI
AI5 Adquirir recursos de TI	ME2 Monitorear y evaluar el control interno
AI6 Administrar cambios	ME3 Garantizar el cumplimiento regulatorio
AI7 Instalar y acreditar soluciones y cambios	ME4 Proporcionar gobierno de TI

APLICACIÓN DE COBIT (2)

Controles Generales sobre los Procesos

- PC1 Objetivos y metas del Proceso
- PC2 Propietario del Proceso
- PC3 Repetitibilidad del Proceso
- PC4 Roles y Responsabilidades
- PC5 Politicas, Planes y Procedimientos
- PC6 Mejoramiento del Desempeño del Pro

Modelo de Madurez de Control para los Procesos de TI



SIMBOLOS UTILIZADOS

- Estado Actual de la Empresa
- Estándares Internacionales
- Mejores Prácticas de la Industria
- Estrategia corporativa

CLASIFICACIONES UTILIZADAS

0 Inexistente	No se aplica ningún proceso de gestión
1 Inicial	Los procesos se aplican según la ocasión y de manera desorganizada
2 Repetible	Los procesos siguen un patrón regular
3 Definido	Los procesos son documentados y comunicados
4 Administrado	Los procesos son monitoreados y medidos
5 Optimizado	Se siguen y se automatizan las mejores prácticas

APLICACIÓN DE COBIT (3)

APPENDIX I—PROCESS CONTROL (PC)

PROCESS ASSURANCE STEPS

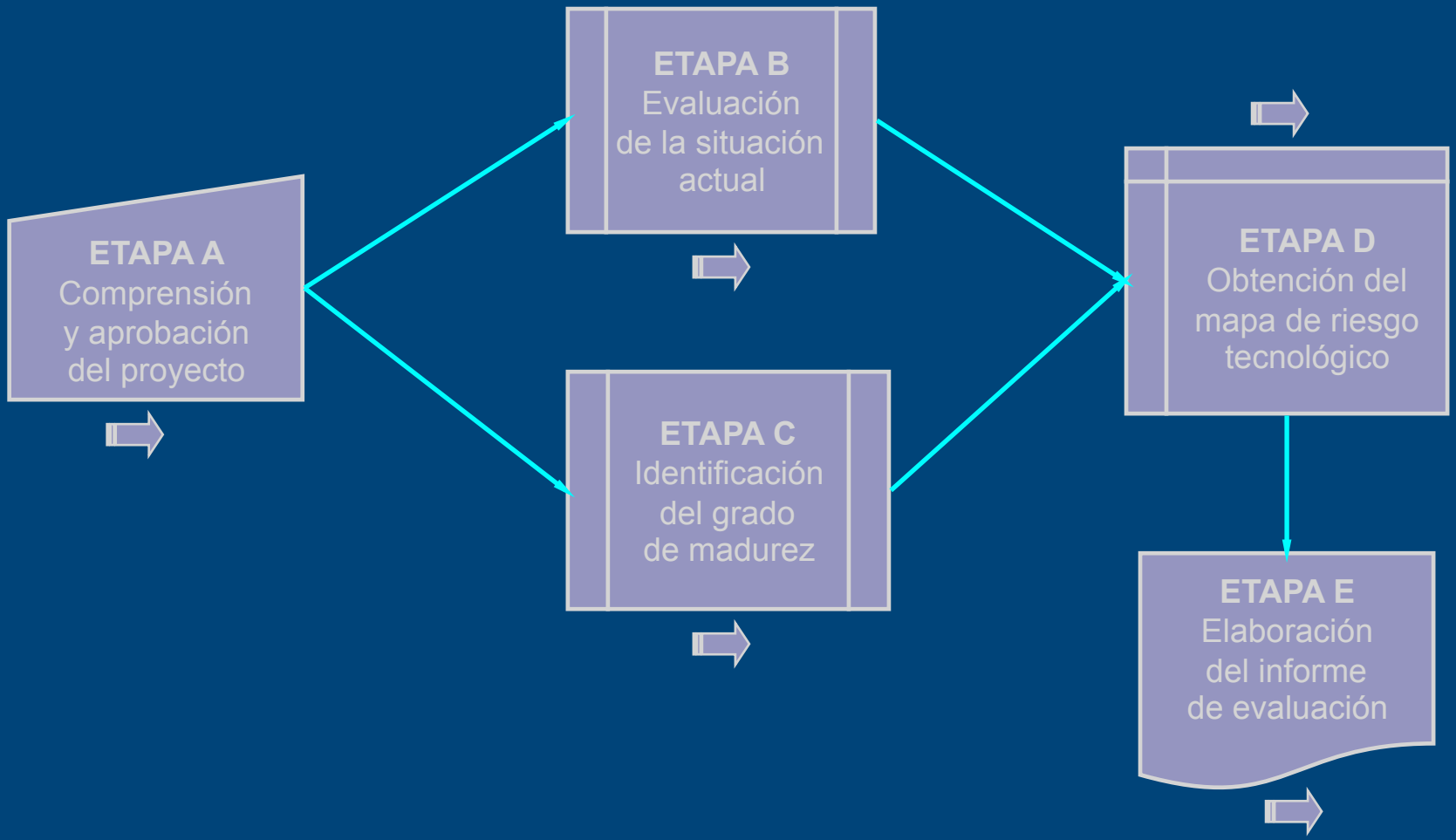
PC1 Process Goals and Objectives

Control Objective	Value Drivers	Risk Drivers
Define and communicate specific, measurable, actionable, realistic, results-oriented and timely (SMARRT) process goals and objectives for the effective execution of each IT process. Ensure that they are linked to the business goals and supported by suitable metrics.	• Key processes measured efficiently and effectively • Processes in line with business objectives	• Process effectiveness difficult to measure • Business objectives not supported by processes

Test the Control Design

- Ensure that a formal process exists for communicating goals and objectives and that, when updated, such communication is repeated.
- Enquire whether and confirm that process goals and objectives have been defined. Verify that process stakeholders understand these goals.
- Enquire whether and confirm that the IT process goals link back to business goals.
- Confirm through interviews with process stakeholders that the IT process goals are SMARRT.
- Enquire whether and confirm that outputs and associated quality targets are defined for each IT process.
- Walk through the process design with selected process stakeholders and verify whether the process is understood and likely to achieve its objectives.

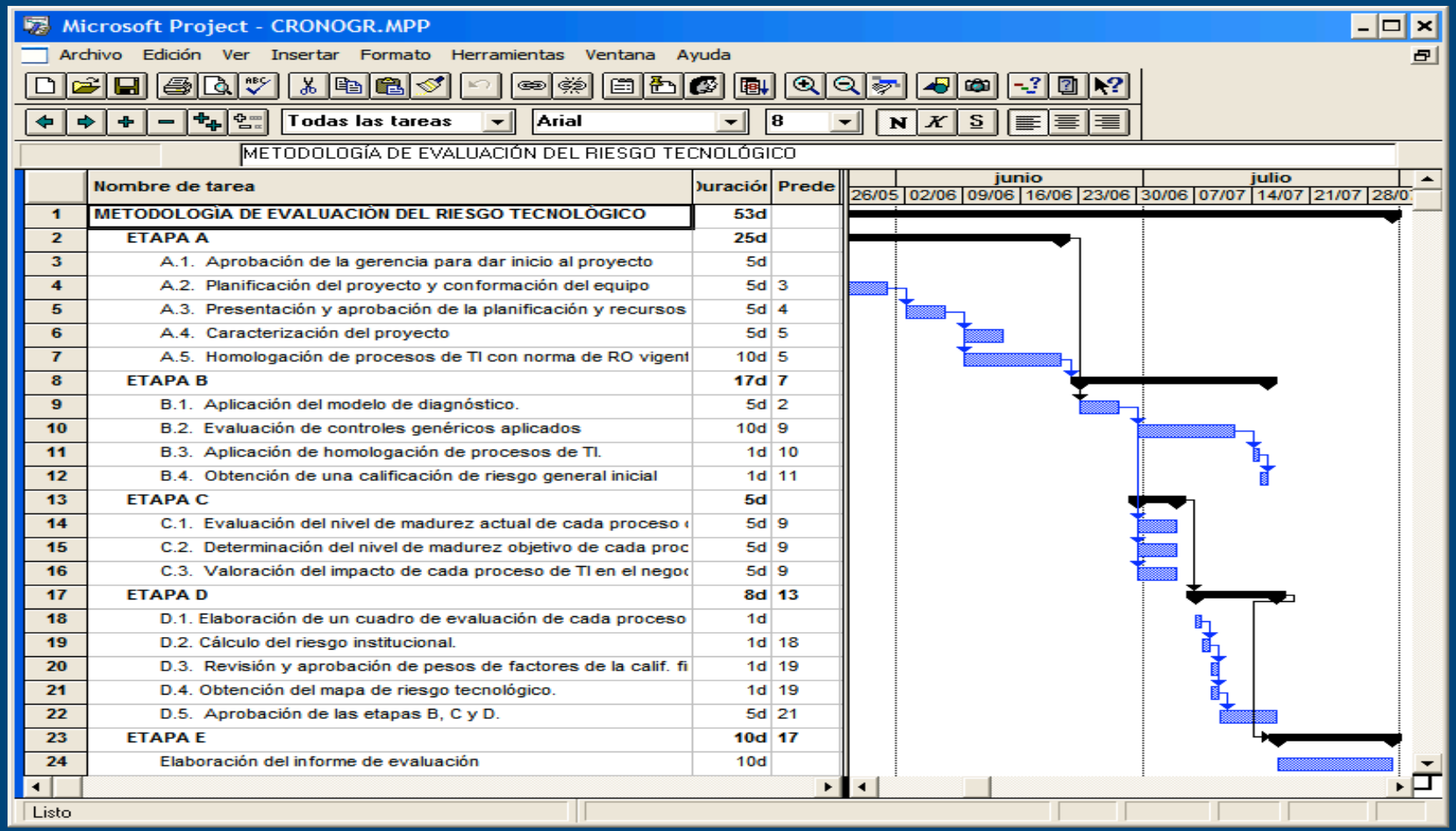
ETAPAS DE LA METODOLOGÍA



Etapa A: Comprensión y aprobación del proyecto

ACTIVIDADES	RESPONSABLES	ENTREGABLES	TÉCNICA / HERRAMIENTA	TIEMPO MÁXIMO	
				EFECTIVO	CON HOLGURA
A.1. Aprobación de la Gerencia para dar inicio al proyecto.	Gerencia General o de TI	Carta de aprobación para la ejecución del proyecto en la institución	Reunión y solicitud formal con explicación general del proyecto	2 horas	1 semana
A.2. Planificación del proyecto y propuesta de conformación del equipo de trabajo.	Gerencia de Tecnología de Información	Cronograma y conformación del equipo de proyecto con sus roles y responsabilidades	Diagramas de Gantt	2 horas	1 semana
A.3. Presentación y aprobación de la planificación y recursos requeridos por el proyecto.	Comité de Tecnología de Información	Acta de reunión del Comité aprobando la planificación propuesta y los recursos asignados	Exposición de objetivos, alcance y planificación del proyecto	1 hora	1 semana
A.4. Caracterización del proyecto	Gerencia de Tecnología de Información	Caracterización del proyecto	Revisión del plan estratégico y operativo de TI	2 horas	1 semana
A.5. Homologación de los procesos de TI con la norma de riesgo operativo vigente	Gerencia de TI, Auditoría informática o Gerencia de Riesgos	Procesos de Cobit 4.1 requeridos por la norma de riesgo operativo vigente	Tablas de asociación entre los requerimientos normativos y los procesos de TI	4 horas	3 semanas

Actividad A.2: Planificación del proyecto



	Nombre de tarea	Duración	Prede
1	METODOLOGÌA DE EVALUACIÒN DEL RIESGO TECNOLÒGICO	53d	
2	ETAPA A	25d	
3	A.1. Aprobación de la gerencia para dar inicio al proyecto	5d	
4	A.2. Planificación del proyecto y conformación del equipo	5d	3
5	A.3. Presentación y aprobación de la planificación y recursos	5d	4
6	A.4. Caracterización del proyecto	5d	5
7	A.5. Homologación de procesos de TI con norma de RO vigent	10d	5
8	ETAPA B	17d	7
9	B.1. Aplicación del modelo de diagnóstico.	5d	2
10	B.2. Evaluación de controles genéricos aplicados	10d	9
11	B.3. Aplicación de homologación de procesos de TI.	1d	10
12	B.4. Obtención de una calificación de riesgo general inicial	1d	11
13	ETAPA C	5d	
14	C.1. Evaluación del nivel de madurez actual de cada proceso (	5d	9
15	C.2. Determinación del nivel de madurez objetivo de cada proc	5d	9
16	C.3. Valoración del impacto de cada proceso de TI en el negoc	5d	9
17	ETAPA D	8d	13
18	D.1. Elaboración de un cuadro de evaluación de cada proceso	1d	
19	D.2. Cálculo del riesgo institucional.	1d	18
20	D.3. Revisión y aprobación de pesos de factores de la calif. fi	1d	19
21	D.4. Obtención del mapa de riesgo tecnológico.	1d	19
22	D.5. Aprobación de las etapas B, C y D.	5d	21
23	ETAPA E	10d	17
24	Elaboración del informe de evaluación	10d	

Actividad A.4: Caracterización del proyecto

* Nombre del proyecto
* Informático responsable
* Usuarios responsables y áreas a las que pertenecen
* Roles y responsabilidades del recurso humano asignado
* Cronograma de trabajo
* Determinación del modelo para diagnóstico
* Descripción general del riesgo inherente institucional
* Restricciones o consideraciones a tomar en cuenta en la realización del proyecto, tanto de la parte tecnológica como de la parte funcional

Actividad A.5: Homologación de procesos de TI a la norma de riesgo operativo

PLANEAR Y ORGANIZAR			ENTREGAR Y DAR SOPORTE		
PO1	Definir un plan estratégico de TI	SI	DS1	Definir y administrar los niveles de servicio	NO
PO2	Definir la arquitectura de la información	NO	DS2	Administrar los servicios de terceros	SI
PO3	Determinar la dirección tecnológica	SI	DS3	Administrar el desempeño y la capacidad	SI
PO4	Definir los procesos, organización y relaciones de TI	SI	DS4	Garantizar la continuidad del servicio	SI
PO5	Administrar la inversión en TI	NO	DS5	Garantizar la seguridad de los sistemas	SI
PO6	Comunicar las aspiraciones y la dirección de la gerencia	SI	DS6	Identificar y asignar costos	NO
PO7	Administrar recursos humanos de TI	SI	DS7	Educar y entrenar a los usuarios	SI
PO8	Administrar la calidad	SI	DS8	Administrar la mesa de servicio y los incidentes	NO
PO9	Evaluar y administrar los riesgos de TI	SI	DS9	Administrar la configuración	SI
PO10	Administrar proyectos	NO	DS10	Administrar los problemas	NO
ADQUIRIR E IMPLANTAR			DS11	Administrar los datos	SI
AI1	Identificar soluciones automatizadas	NO	DS12	Administrar el ambiente físico	SI
AI2	Adquirir y mantener software aplicativo	NO	DS13	Administrar las operaciones	SI
AI3	Adquirir y mantener infraestructura tecnológica	SI	MONITOREAR Y EVALUAR		
AI4	Facilitar la operación y el uso	SI	ME1	Monitorear y evaluar el desempeño de TI	NO
AI5	Adquirir recursos de TI	SI	ME2	Monitorear y evaluar el control interno	NO
AI6	Administrar cambios	SI	ME3	Garantizar el cumplimiento regulatorio	NO
AI7	Instalar y acreditar soluciones y cambios	SI	ME4	Proporcionar gobierno de TI	NO
TOTAL OBJETIVOS DE COBIT 4.1 REQUERIDOS POR NORMA:					21

Etapa B: Evaluación de la situación actual

ACTIVIDADES	ENTREGABLES	TÉCNICA / HERRAMIENTA	TIEMPO MÁXIMO	
			EFECTIVO	CON HOLGURA
B.1. Aplicación del modelo de diagnóstico.	Diagnóstico de la situación actual de la tecnología de información	Modelo de diagnóstico especificado en la caracterización del proyecto	2 horas	1 semana
B.2. Evaluación de los controles genéricos aplicados en cada proceso de tecnología de información.	Puntaje de controles aplicados a cada proceso de TI	Matriz de controles genéricos aplicados a los procesos de TI	20 horas	3 semanas
B.3. Aplicación de la homologación de los procesos de TI con la norma de riesgo operativo vigente.	Matriz de controles genéricos con los pesos relativos asignados a los procesos de Cobit 4.1	Fórmulas de cálculo de los pesos relativos respecto al requerimiento o no de la norma para cada proceso.	1 día	1 día
B.4. Obtención de una calificación de riesgo general inicial de los procesos de tecnología de información.	- Puntaje de riesgo general de los procesos de TI - Identificación inicial de procesos en estado crítico	Fórmula de cálculo del puntaje de riesgo general	1 día	1 día

Actividad B.1: Aplicación del modelo de diagnóstico

Oportunidades

- Existe una tecnología débil en el sector cooperativo
- Tecnología disponible en el mercado
- Credibilidad fuerte en el sistema cooperativo
- Importante demanda de servicios financieros
- Proveedor con posicionamiento del mercado

Fortalezas

- Software financiero transaccional sólido y completo
- Recurso humano calificado y con experiencia
- Tecnología adecuada en LAN y WAN
- Crecimiento tecnológico disponible
- Rápida respuesta al cambio
- Disponibilidad de ambiente Intranet
- Hardware actualizado y adecuadamente administrado
- Alta inversión en tecnología de información
- Apoyo gerencial a la tecnología
- Adecuada estructura física del área
- Hay conciencia de la necesidad de utilización de estándares y mejores prácticas para la administración de TI

Amenazas

- Políticas cambiantes en las entidades controladoras
- Cambios en las políticas del gobierno
- Alta competencia en productos y servicios
- Avance tecnológico del mercado es mayor al institucional
- Ataques informáticos
- Exigencias de normativa de riesgo tecnológico no aplicable a la entidad
- Costos adicionales por requerimientos de control

Debilidades

- No se cuenta con los códigos fuente del sistema transaccional
- Dependencia tecnológica del software financiero por parte de los usuarios
- No existe un área de desarrollo
- Falta de evaluación de los controles tecnológicos
- Excedente de servicios financieros (sistema subutilizado)
- Falta de un programa de capacitación continua para el personal de TI
- Inadecuada transferencia de conocimientos al rotar personal

Actividad B.2: Evaluación de controles genéricos

Controles genéricos de procesos	Características específicas	
PC1: Metas y objetivos	1	Define y comunica metas y objetivos específicos, medibles, ejecutables, realísticos, orientados a resultados y con fechas límite
	2	Alineado con los objetivos del negocio
	3	Medido por métricas adecuadas
PC2: Propiedad	4	Existe un propietario con suficiente autoridad para cumplir roles y responsabilidades
	5	Roles y responsabilidades definidos, entendidos y aceptados
	6	La responsabilidad incluye: diseño, interacción, rendición de cuentas, medición del desempeño
PC3: Repetitividad	7	La repetitividad del proceso es un objetivo de la Administración
	8	Si el proceso es crítico, provee evidencia para revisión por parte de la Administración
	9	Se aplicaron buenas prácticas y estándares internacionales en su definición
	10	Las partes interesadas integran y son coherentes con el proceso
	11	La secuencia de sus actividades es lógica, flexible y escalable
PC4: Roles y responsabilidades	12	Las actividades clave y entregables están definidos y documentados
	13	Roles y responsabilidades no ambiguos, asignados y comunicados
	14	Roles y responsabilidades para ejecución efectiva, eficiente y documentada de actividades
	15	Está asignada la rendición de cuentas de resultados y entregables
PC5: Políticas, planes y procedimientos	16	Existen, están comunicadas, son conocidas y aplicadas
	17	Su administración incluye documentar, revisar, mantener, comunicar, y usar para capacitar
	18	Hay responsabilidad por su administración y se revisa su correcto cumplimiento periódicamente
	19	Son accesibles, correctas, entendidas y actualizadas
PC6: Mejoramiento del desempeño	20	Existen métricas que permiten percibir los resultados y desempeño del proceso con un esfuerzo limitado
	21	El diseño de las métricas permite medir la utilización de recursos, calidad de resultados y tiempos
	22	Existen procedimientos para definir marcas a cumplir en las metas del proceso y conductores de desempeño
	23	Se comparan las medidas actuales con las marcas de los logros a cumplir y se toman acciones de mejora
	24	Las métricas, marcas y métodos están alineados con el monitoreo del desempeño general de TI

Actividad B.3: Aplicación de la homologación

Cálculo de los pesos absolutos:

- **SÍ:** $\frac{100\%}{\text{Número de “SI” + (Número de “NO” * \%Participación)}}$
- **NO:** Peso de “SI” * %Participación del “NO”

Cálculo de los pesos relativos:

Peso absoluto * %Aplicación de controles genéricos

Actividad B.4: Calificación de riesgo general inicial (1)

Calificación de riesgo general inicial

$$\frac{\Sigma \text{ pesos relativos}}{\%} \qquad \frac{}{100\%}$$

Nivel de madurez 3

Nivel de madurez 4

Nivel de madurez 5

Actividad B.4: Calificación de riesgo general inicial (2)

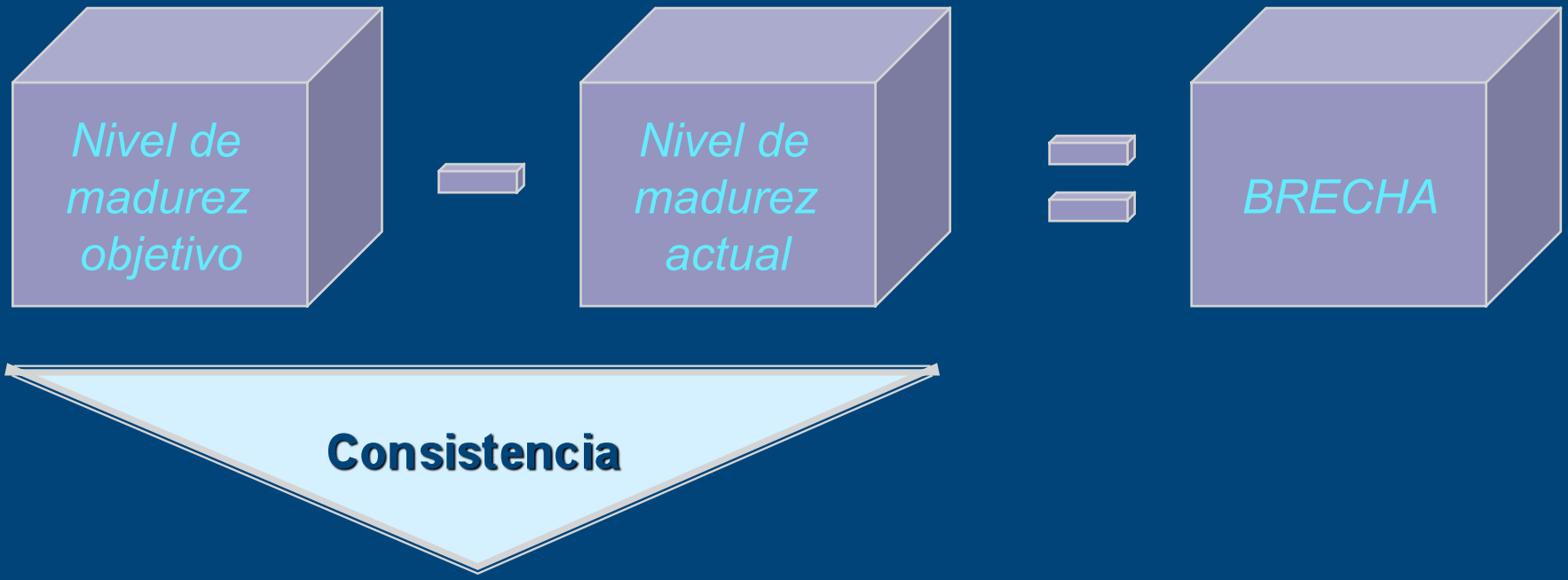
		CONTROLES GENÉRICOS EVALUADOS	Nivel de madurez 3	Nivel de madurez 4	Nivel de madurez 5
Metas y objetivos	1	Define y comunica metas y objetivos específicos, medibles, ejecutables, realísticos, orientados a resultados y con fechas límite	S	S	S
	2	Alineado con los objetivos del negocio	S	S	S
	3	Medido por métricas adecuadas	S	S	S
Propiedad	4	Existe un propietario con suficiente autoridad para cumplir roles y responsabilidades	S	S	S
	5	Roles y responsabilidades definidos, entendidos y aceptados	S	S	S
	6	La responsabilidad incluye: diseño, interacción, rendición de cuentas, medición del desempeño		S	S
Repetitividad	7	La repetitividad del proceso es un objetivo de la Administración	S	S	S
	8	Si el proceso es crítico, provee evidencia para revisión por parte de la Administración	S	S	S
	9	Se aplicaron buenas prácticas y estándares internacionales en su definición			S
	10	Las partes interesadas integran y son coherentes con el proceso		S	S
	11	La secuencia de sus actividades es lógica, flexible y escalable	S	S	S
Roles y responsabilidades	12	Las actividades clave y entregables están definidos y documentados	S	S	S
	13	Roles y responsabilidades no ambiguos, asignados y comunicados	S	S	S
	14	Roles y responsabilidades para ejecución efectiva, eficiente y documentada de actividades	S	S	S
	15	Está asignada la rendición de cuentas de resultados y entregables		S	S
Políticas, planes y procedimientos	16	Existen, están comunicadas, son conocidas y aplicadas	S	S	S
	17	Su administración incluye documentar, revisar, mantener, comunicar, y usar para capacitar	S	S	S
	18	Hay responsabilidad por su administración y se revisa su correcto cumplimiento periódicamente	S	S	S
	19	Son accesibles, correctas, entendidas y actualizadas		S	S
Mejoramiento del desempeño	20	Existen métricas que permiten percibir los resultados y desempeño del proceso con un esfuerzo limitado		S	S
	21	El diseño de las métricas permite medir la utilización de recursos, calidad de resultados y tiempos			S
	22	Existen procedimientos para definir marcas a cumplir en las metas del proceso y conductores de desempeño			S
	23	Se comparan las medidas actuales con las marcas de los logros a cumplir y se toman acciones de mejora			S
	24	Las métricas, marcas y métodos están alineados con el monitoreo del desempeño general de TI			S
		Total procesos:	14	19	24
		Porcentaje del total:	58.33%	79.17%	100.00%

mínimo

Etapa C: Identificación del grado de madurez de los procesos de TI

ACTIVIDADES	ENTREGABLES	TÉCNICA / HERRAMIENTA	TIEMPO MÁXIMO	
			EFECTIVO	CON HOLGURA
C.1. Evaluación del nivel de madurez actual de cada proceso de tecnología de información.	Nivel de madurez actual de cada proceso de TI	Modelos de madurez de Cobit 4.1, plantilla en Excel	10 horas	1.5 semanas
C.2. Determinación del nivel de madurez objetivo de cada proceso de tecnología de información.	Nivel de madurez objetivo de cada proceso de TI y su brecha con el nivel actual	Modelos de madurez de Cobit 4.1, plantilla en Excel	6 horas	1 semana
C.3. Valoración del impacto de cada proceso de tecnología de información en el negocio.	Impacto de cada proceso de TI en el negocio	Plantilla en Excel	3 horas	1 semana

Actividades C.1 y C.2: Determinación del nivel de madurez actual y objetivo



Actividad C.3: Valoración del impacto de los procesos de TI en el negocio

- Criticidad por frecuencia de realización
- Afectación a la continuidad de las operaciones de la institución
- Costos operativos asociados
- Entrega de valor para otros procesos
- Dependencia para la toma de decisiones
- Etc.

Alto

Medio

Bajo

Etapa D: Obtención del mapa de riesgo tecnológico

ACTIVIDADES	ENTREGABLES	TÉCNICA / HERRAMIENTA	TIEMPO MÁXIMO	
			EFECTIVO	CON HOLGURA
D.1. Elaboración de un cuadro de evaluación de cada proceso de tecnología de información.	Cuadro de evaluación de los procesos de tecnología de información (eje X del mapa)	Aplicación de fórmulas	1 minuto	1 minuto
D.2. Cálculo del riesgo institucional.	Segmento del riesgo institucional (eje Y del mapa)	Entrevistas a jefes departamentales	2 horas	3 días
D.3. Revisión y aprobación de pesos de factores de la calificación final.	Porcentajes de participación de cada factor de calificación	Reunión del Comité de Tecnología de Información	30 minutos	3 días
D.4. Obtención del mapa de riesgo tecnológico.	Mapa de evaluación del riesgo tecnológico	Aplicación de fórmulas	1 minuto	1 minuto
D.5. Aprobación de las etapas B, C y D.	Acta de aprobación de las etapas B, C y D, por parte del Comité de Tecnología de Información	Revisión de los entregables de las etapas B, C y D	30 minutos	3 días

Actividad D.1: Elaboración de un cuadro de evaluación (1)

Factor evaluado	Participación total	Participación relativa	Participación absoluta
Cumplimiento de controles genéricos:	80%	80%	64.00%
Requerido por norma:		20%	16.00%
Estado de madurez:	20%	80%	16.00%
Brecha de madurez:		20%	4.00%
TOTAL	**100%**		**100%**

Factor evaluado	Proceso A	Proceso B	Proceso C
Cumplimiento de controles genéricos:	61.33%	22.43%	0.00%
Requerido por norma:	16.00%	3.20%	0.00%
Estado de madurez:	9.60%	3.20%	0.00%
Brecha de madurez:	4.00%	2.40%	0.00%
TOTAL:	**90.93%**	**31.23%**	**0.00%**
Riesgo alcanzado	**9.07%**	**68.77%**	**100.00%**
Calificación de riesgo (Eje X)	**1**	**7**	**9**

Banda superior	Calificación de riesgo
11%	1
22%	2
33%	3
44%	4
56%	5
67%	6
78%	7
89%	8
100%	9

Actividad D.1: Elaboración de un cuadro de evaluación (2)

Dominios de Cobit 4.1	Calif. de riesgo "X"	Número de procesos	Máximo a alcanzar	% alcanzado	Calificación del dominio
Planear y organizar	46	10	90	51.11%	5
Adquirir e implantar	22	7	63	34.92%	4
Entregar y dar soporte	49	13	117	41.88%	4
Monitorear y evaluar	22	4	36	61.11%	6

Calificación de riesgo general
4.53
Nivel de riesgo general
Medio

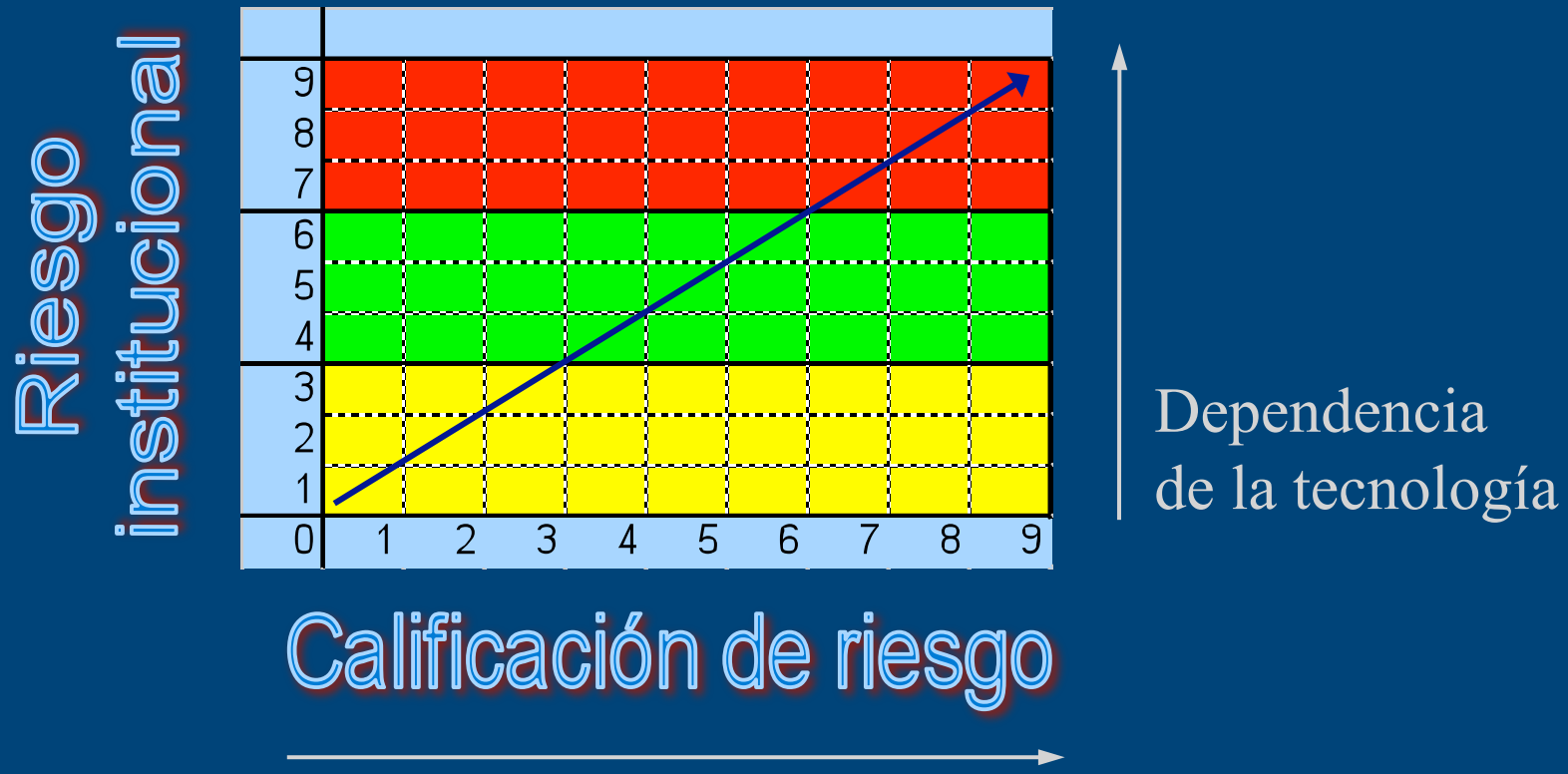
Escalas:		Nivel de riesgo
1	2.6	No significativo
2.6	4.2	Bajo
4.2	5.8	Medio
5.8	7.4	Alto
7.4	9	Crítico

Actividad D.2: Cálculo del riesgo institucional (1)

RIESGO INSTITUCIONAL (EJE "Y")		
	Desde	Hasta
Riesgo institucional bajo:	60.00%	73.33%
Riesgo institucional medio:	73.34%	87.67%
Riesgo institucional alto:	87.68%	100.00%

	Frecuencia	% automatiz
Proceso / área 1	1,500.00	90.00%
Proceso / área 2	2,000.00	50.00%
Proceso / área 3	10.00	84.00%
Proceso / área 4	850.00	85.00%
Proceso / área 5	3,000.00	75.00%
Proceso / área 6		
Proceso / área 7		
Proceso / área 8		
Proceso / área 9		
Proceso / área 10		
Proceso / área 11		
Proceso / área 12		
Proceso / área 13		
Proceso / área 14		
Proceso / área 15		
TOTAL FRECUENCIA:	7,360.00	
PORCENTAJE DE AUTOMATIZACIÓN DE LA ENTIDA		72.43%
Riesgo institucional bajo, segmento:		1

Actividad D.2: Cálculo del riesgo institucional (2)



Actividad D.3: Revisión y aprobación de pesos

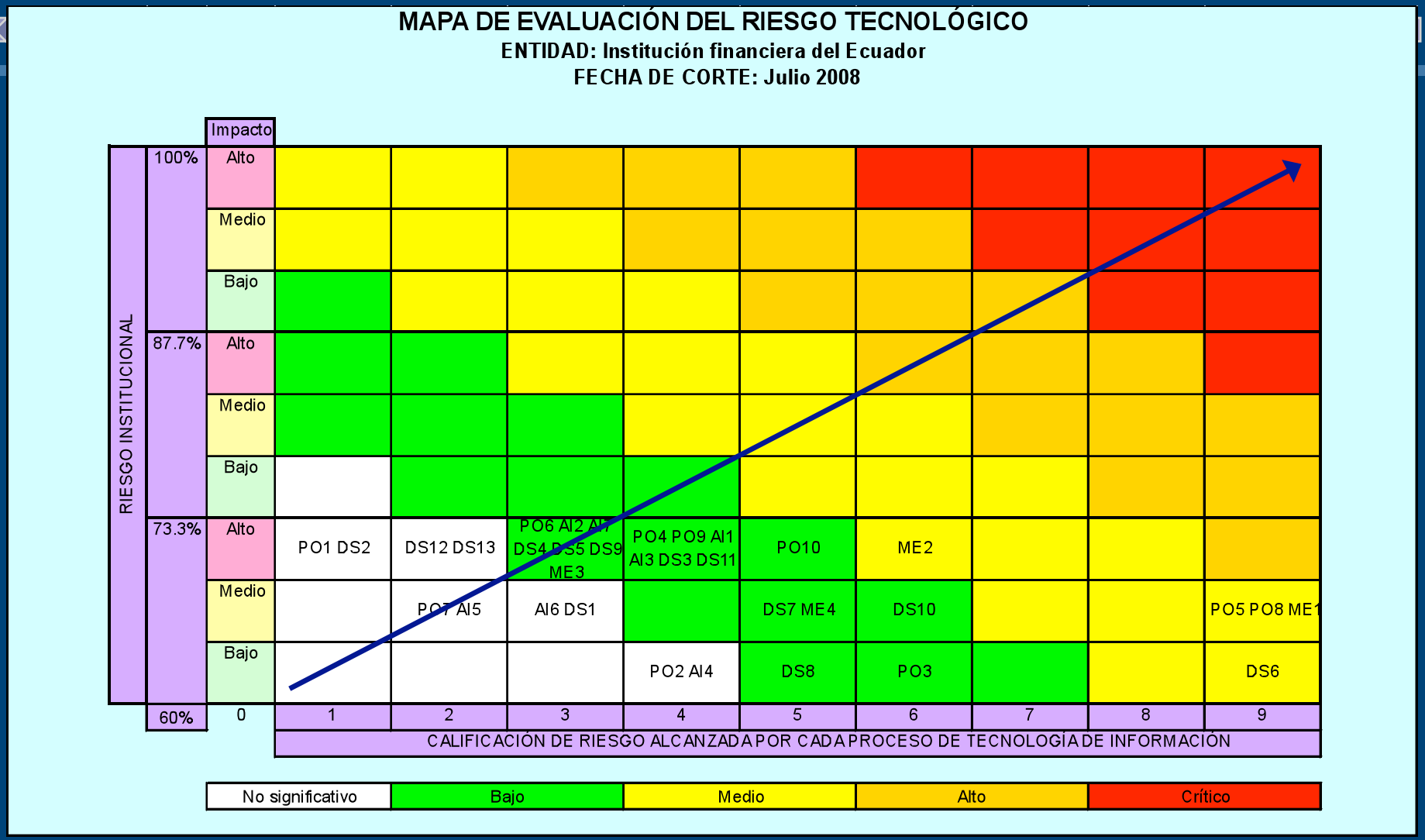
- Factores de calificación de procesos de TI

Puntajes:	Aplicación de controles	Factor normativo	Estado de madurez	Brecha de madurez	Puntaje total
PARTICIPACIÓN ABSOLUTA:	**64.00%**	**16.00%**	**16.00%**	**4.00%**	100.00%
PUNTAJE MÁXIMO:	64.00	16.00	16.00	4.00	100.00
MÌNIMO SOBRE CERO:	2.67	**3.20**	3.20	2.40	11.47

- Umbral de riesgo

Nivel de madurez 3	Nivel de madurez 4	Nivel de madurez 5
58.33%	**79.17%**	**100.00%**

Actividad D.4: Obtención del mapa de riesgo tecnológico



Etapa E: Elaboración del informe de evaluación (1)

- Título
- Nombre de la institución evaluada
- Fecha de inicio del proyecto
- Alcance
- Restricciones del alcance
- Resultados (hallazgos y recomendaciones)
- Plan de acción
- Conclusión
- Lugar, fecha y firma

Etapa E: Elaboración del informe de evaluación (2)

ALCANCE

- Análisis de la situación actual
- Homologación de los procesos de TI a la norma de riesgo operativo vigente
- Evaluación de los controles genéricos aplicados
- Identificación del grado de madurez alcanzado y el esperado
- Determinación del impacto de los procesos de TI en el negocio

Etapa E: Elaboración del informe de evaluación (3)

RESULTADOS

- Exponer los resultados relacionados con las temáticas anotadas en el Alcance:
  - Diagnóstico, análisis de la aplicación de controles a los procesos críticos y su influencia en la calificación final, un resumen de la calificación de riesgo obtenida por cada proceso de TI, el mapa de riesgo tecnológico, y el gráfico de la curva de distribución del conteo de procesos de acuerdo a la calificación obtenida.
- Detallar las observaciones y recomendaciones de los procesos que se encuentren en una situación de riesgo relevante para la institución:
  - El proceso se encuentra en un nivel de riesgo crítico, alto o medio. Se excluyen los procesos que se encuentran en los niveles inferiores.
  - El proceso no es requerido por la norma de riesgo operativo pero se encuentra por debajo del umbral de riesgo del nivel de madurez 3.
  - El proceso sí es requerido por la norma de riesgo operativo y se encuentra por debajo del umbral de riesgo del nivel inmediato superior al definido por la entidad, es decir, los asociados a los niveles de madurez 4 ó 5 según corresponda.
- Las observaciones deberán indicar el riesgo asociado a la situación de riesgo del proceso.
- Las recomendaciones se basarán en los modelos de madurez de Cobit.

Etapa E: Elaboración del informe de evaluación (4)

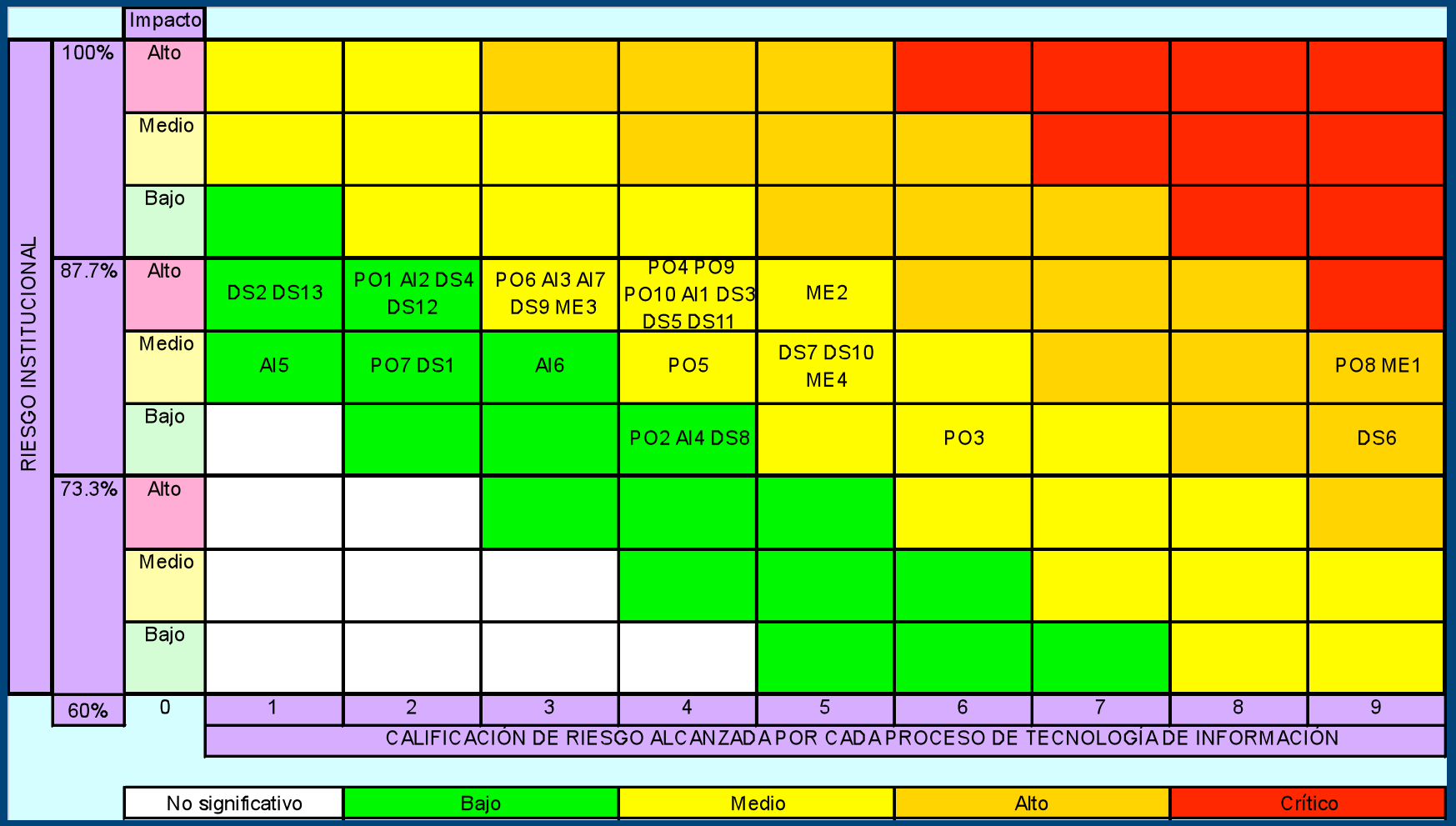
PLAN DE ACCIÓN

Para obtener resultados concretos, es deseable el establecer un calendario con fechas máximas de ejecución de las recomendaciones efectuadas, que permitan hacer un seguimiento posterior de su cumplimiento

CONCLUSIÓN

Resumen gerencial sobre los aspectos que tengan mayor relevancia en la calificación obtenida y las sugerencias que permitan mitigar los riesgos tecnológicos encontrados, así como las posibles consecuencias de su no aplicación a mediano y largo plazo. Esta conclusión debe estar contenida en un máximo de una página

PLAN PILOTO


Impacto
RIESGO INSTITUCIONAL
100%
87.7%
73.3%
60%
Alto
Medio
Bajo
Alto
Medio
Bajo
Alto
Medio
Bajo
0
DS2 DS13
PO1 AI2 DS4 DS12
PO6 AI3 AI7 DS9 ME3
PO4 PO9 PO10 AI1 DS3 DS5 DS11
ME2
AI5
PO7 DS1
AI6
PO5
DS7 DS10 ME4
PO8 ME1
PO2 AI4 DS8
PO3
DS6
1
2
3
4
5
6
7
8
9
CALIFICACIÓN DE RIESGO ALCANZADA POR CADA PROCESO DE TECNOLOGÍA DE INFORMACIÓN
No significativo
Bajo
Medio
Alto
Crítico

CONCLUSIONES (1)

- Se alcanzaron los objetivos propuestos al inicio del proyecto
- El plan piloto permitió determinar que se obtienen resultados consistentes con la realidad de la institución evaluada, utilizando una de las mejores prácticas en administración de TI
- El conocimiento previo que el equipo de proyecto debe tener sobre el marco de trabajo de Cobit, limita pero no impide la ejecución de la metodología propuesta.
- Por tratarse de una metodología que permite realizar un autodiagnóstico, el grado de honestidad y objetividad durante la evaluación es importante para obtener resultados consistentes y confiables.

CONCLUSIONES (2)

- La determinación del grado de madurez actual y objetivo para cada proceso de tecnología de información permiten obtener resultados más ajustados respecto de la situación real de una institución financiera, además de que permiten orientar las recomendaciones del informe de evaluación a la consecución de los objetivos planteados en cada proceso en forma gradual. Sin embargo, el mayor peso en la calificación obtenida está dada por la aplicación de controles, debido a que éstos permiten mitigar los riesgos a los que podría estar expuesto un proceso.

- Desde el punto de vista de ITIL, la presente metodología incorpora el modelo de mejora continua del servicio, que establece la visión (cumplimiento normativo), la evaluación de la situación actual (etapa B y nivel de madurez actual), el planteamiento de objetivos (nivel de madurez objetivo), el método para alcanzar los objetivos (recomendaciones), y las mediciones y métricas para evaluar la consecución (mapa de riesgo tecnológico).

RECOMENDACIONES (1)

- Para validar la aplicabilidad de la presente metodología en diferentes tamaños de instituciones, se recomienda realizar más pruebas con instituciones en las que el nivel de automatización o dependencia de la tecnología sea baja y alta, así como diferentes períodos de tiempo para segmentos de mercado homogéneos.

- En la planificación del proyecto se sugiere considerar los tiempos de holgura especificados para cada actividad con respecto a su tiempo efectivo, de modo que se pueda ajustar los recursos humanos y de tiempo empleados para culminar el proyecto en un plazo adecuado. No se recomienda extender los plazos de holgura fijados puesto que las condiciones de la plataforma tecnológica evaluada podrían variar en ese lapso, dando lugar a una duplicación de esfuerzos.

- La presente metodología es perfectible según el apetito de exigibilidad de la entidad; de ser ése el caso, se recomienda utilizar parámetros más estrictos de evaluación tales como un umbral de riesgo más alto o la utilización de un impacto alto para la mayoría de procesos de tecnología de información, con lo que se logrará maximizar el riesgo al que se encuentra expuesta la plataforma tecnológica de la entidad a evaluar.

RECOMENDACIONES (2)

- La metodología puede ser aún más ajustada a la realidad de las instituciones evaluadas asignando pesos por importancia a los 24 controles genéricos que se evalúan en cada proceso de tecnología de información. Se recomienda que dichos pesos sean asignados por el organismo de control o un ente independiente para que las evaluaciones realizadas sean homogéneas en cada tipo de institución.

- Debido a que el plazo para dar cumplimiento a la norma que rige la administración del riesgo operativo vence en octubre del 2008, y en octubre del 2009, se recomienda difundir y aplicar la presente metodología de evaluación del riesgo tecnológico para cumplir con dicho requerimiento del organismo de control.

- Una herramienta que es de total actualidad y aplicabilidad en las empresas no solo financieras sino de cualquier naturaleza, es la Administración de Riesgos, la misma que ha servido de base para la presente metodología y por ello se recomienda que sea incorporada en el pénsum académico de la carrera de Ingeniería de Sistemas e Informática de la ESPE.

Metodología de evaluación del riesgo tecnológico, utilizando Cobit 4.1

GRACIAS