PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR
FACULTAD DE INGENIERÍA
MAESTRIA EN GERENCIA DE TECNOLOGÍAS DE LA INFORMACIÓN

TESIS PREVIA A LA OBTENCIÓN DEL TÍTULO

TEMA:

METODOLOGÍA DE EVALUACIÓN DEL GOBIERNO, RIESGOS Y CUMPLIMIENTO DE LA TECNOLOGÍA DE INFORMACIÓN EN INSTITUCIONES DEL SISTEMA FINANCIERO ECUATORIANO

AUTORA:
Ing. Katalina Coronel

DIRECTORA:
Ing. Irina Verkovitch, MSc.

REVISORES:
Ing. Javier Cóndor
Ing. Alberto Pazmiño

Quito – Ecuador, agosto 2013

DEDICATORIA

Dedico este trabajo a mis hijos y mi esposo, quienes han sabido brindarme la energía, el apoyo y el ánimo necesarios para seguir adelante, y por quienes todo esfuerzo vale la pena.
Sin ellos, no sería lo mismo.

AGRADECIMIENTO

Quiero expresar mi más profundo agradecimiento, primero a Dios por quien todo es y existe, y luego a todos los profesores de la Maestría en Gerencia de Tecnologías de la Información de la Pontificia Universidad Católica del Ecuador, por los conocimientos y experiencias compartidos, principalmente al ingeniero Oswaldo Espinosa por su paciencia y respaldo constante durante la carrera, a mis profesores revisores, por su apoyo y guía enriquecedores, y de manera muy especial a la ingeniera Irina Verkovitch, quien me dio el impulso y esperanza necesarios para lograr esta meta, sin los cuales, no estaría ahora escribiendo estas líneas.

Agradezco también a mi familia y amigos, quienes con su preocupación y ánimo me dieron el aliento para continuar hasta el final. A todos: gracias de corazón.

TABLA DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN EJECUTIVO

Para el desarrollo de esta metodología, se analizaron los elementos que provee COBIT 5, incluyendo procesos, catalizadores y herramientas, con el fin de determinar aquellos que influyen más directamente en la evaluación del Gobierno de TI, y se estableció su forma de evaluarlos; luego se introdujo el factor de Cumplimiento, a través de la identificación de los requerimientos normativos de la Superintendencia de Bancos y Seguros que coinciden con los procesos y catalizadores de COBIT 5, por lo cual su implementación se vuelve obligatoria para las instituciones financieras.

A continuación se desarrolló la propuesta metodológica para elaborar una matriz de riesgos en la que se presente una visión gerencial de la situación en que se encuentran los elementos que contribuyen con el Gobierno, Riesgos y Cumplimiento de TI, la cual se complementa con un procedimiento de priorización de iniciativas de mejora, con sus correspondientes metas, métricas e indicadores, que permitirán realizar la medición continua de los resultados, y conocer el avance de los logros obtenidos.

PALABRAS CLAVE: Gobierno, Riesgos y Cumplimiento de TI
Aplicación de COBIT 5 en instituciones financieras
Matriz de riesgos de tecnología de información
Gobierno y Riesgo de TI en instituciones financieras
Cumplimiento de TI en instituciones financieras ecuatorianas

INTRODUCCIÓN

La constante y veloz evolución de la tecnología de la información y las comunicaciones en el mundo de hoy, ha significado grandes avances en todos los ámbitos del quehacer humano, desde las ciencias astronómicas hasta la educación y la salud, en los rincones más remotos de la Tierra. Sin embargo, acompañando a este gran avance tecnológico, cada día aparecen riesgos y retos que es necesario gestionar adecuadamente para que, lo que parece ser una solución, no se convierta en un problema.

Uno de los sectores que ha ido de la mano con este avance tecnológico es el de la banca y las finanzas, en procura de emplear cada vez más canales y recursos tecnológicos para llegar hasta los clientes más alejados con la prestación de mayores beneficios financieros. No obstante, este sector también ha sido vulnerado por actividades maliciosas, delitos informáticos, fraude, estafa, lavado de activos, entre otros, en los que han sido víctimas tanto las instituciones financieras como sus clientes.

Una de las herramientas que constituye un factor de éxito para la prevención de pérdidas no esperadas en todo tipo de organizaciones es la gestión de riesgos, a través de la cual se puede identificar las amenazas y/o vulnerabilidades actuales para darles el tratamiento adecuado y minimizar el impacto de una eventual pérdida. Como parte de las mejores prácticas que hoy existen en el mundo, la gestión de Riesgos se enmarca dentro de un concepto aún mayor, que constituye el Gobierno Corporativo, los Riesgos y el Cumplimiento (GRC), cuyas directrices y objetivos se complementan entre sí, y ponen en relieve la importancia del Gobierno de la Tecnología de Información (TI).

Estudios en diversas industrias han demostrado que existen varias ventajas en la implementación de un buen Gobierno Corporativo de TI, tales como la mejora en el retorno de las inversiones, mejor imagen y reputación, mayor satisfacción de los clientes en la obtención de productos y servicios, mayor creación de valor para las partes interesadas de las organizaciones, entre otros.

En este contexto, el conocimiento y aplicación de herramientas que permitan diagnosticar el riesgo existente en la gestión tecnológica y conocer las áreas en las que deben enfocarse los esfuerzos es fundamental para la optimización del Gobierno Corporativo y de TI de las organizaciones. En el caso de las instituciones financieras, la Superintendencia de Bancos y Seguros ha emitido diversas normas de control para su funcionamiento, entre las cuales están las de Gestión de Riesgo Operativo y de Seguridades Mínimas, que establecen políticas y procedimientos necesarios para

garantizar que los riesgos y seguridad de la información y de los procesos, personas, establecimientos y dispositivos electrónicos estén adecuadamente gestionados.

El Instituto de Gobierno de TI (ITGI por su siglas en inglés) creó los Objetivos de Control para la Información y la Tecnología relacionada, denominados COBIT®, en cuya versión 5 brinda buenas prácticas a través de un marco de trabajo orientado 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, todo lo cual constituye la base para generar un Gobierno de TI efectivo.

Con el propósito de contar con una herramienta gerencial que facilite la evaluación de la gestión tecnológica, y brinde directrices prácticas para el establecimiento de un buen Gobierno de TI, se ha desarrollado esta metodología, de la mano de las buenas prácticas internacionales que sugiere el marco de trabajo COBIT 5, con lo cual se promueve el buen Gobierno Corporativo, la Gestión de Riesgos y el Cumplimiento normativo de TI en las instituciones financieras del Ecuador.

En el Capítulo 1, se realiza una breve descripción del marco de trabajo COBIT 5, se exponen en forma resumida los requerimientos que efectúa la Superintendencia de Bancos y Seguros (SBS) en sus normas para la gestión del riesgo operativo y las seguridades, se explica la metodología para elaborar matrices de riesgos, y se resumen los requerimientos del estándar ISO/IEC 27005 “Gestión de Riesgos de Seguridad de la Información”, parte de los cuales son considerados en las normas de la SBS.

En el Capítulo 2, se determinan y se seleccionan los elementos de COBIT 5 que influyen más directamente en la evaluación del Gobierno, Riesgos y Cumplimiento de TI.

En el Capítulo 3, se realiza un mapeo entre los procesos y prácticas clave de COBIT 5, frente a los requerimientos de las normas de la SBS y el estándar ISO/IEC 27005, con el fin de diferenciar los procesos de COBIT 5 que son de cumplimiento obligatorio para las instituciones financieras. Además se diseñó una encuesta que permite conocer el nivel de aplicación de estas buenas prácticas en las instituciones financieras, así como su impacto en cada organización.

En el Capítulo 4, se presenta la matriz de riesgos en la que se plasma la evaluación de todos los elementos que tienen mayor influencia en el sistema de Gobierno, Riesgos y Cumplimiento de TI, así como las medidas que se pueden adoptar para su mejoramiento, con las métricas sugeridas para la medición continua de los elementos evaluados.

Finalmente, en el Capítulo 5, se presentan las conclusiones de este trabajo y las recomendaciones para la aplicación de la metodología presentada.

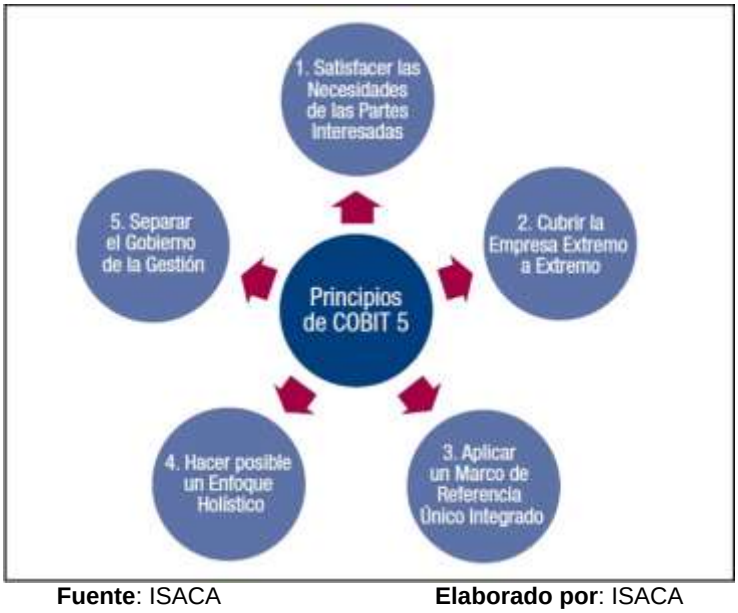
CAPÍTULO 1 - MARCO TEÓRICO

1.1. Gobierno de TI según el marco de referencia de COBIT 5

La Asociación de Control y Auditoría de Sistemas de Información (ISACA por sus siglas en inglés) es un proveedor líder de conocimiento[1], certificaciones, comunidades, y educación en sistemas de información, aseguramiento y seguridad, gobierno corporativo y gestión de Tecnología de Información (TI), y riesgo relacionados con TI y cumplimiento, la cual ha desarrollado varios marcos de trabajo que constituyen mejores prácticas en tecnología de información a nivel mundial, entre ellos los Objetivos de Control para la Información y la Tecnología relacionada (COBIT por sus siglas en inglés).

Con la versión 5 de COBIT, ISACA provee un marco de trabajo integral[2] que ayuda a las empresas a alcanzar sus objetivos para el gobierno y la gestión de las TI corporativas; es decir, las ayuda a crear el valor óptimo desde TI, manteniendo equilibrio entre la generación de beneficios y la optimización de los niveles de riesgo y el uso de recursos. COBIT 5 se basa en los siguientes cinco principios claves:

Figura 1: Principios de COBIT 5



Fuente: ISACA **Elaborado por**: ISACA

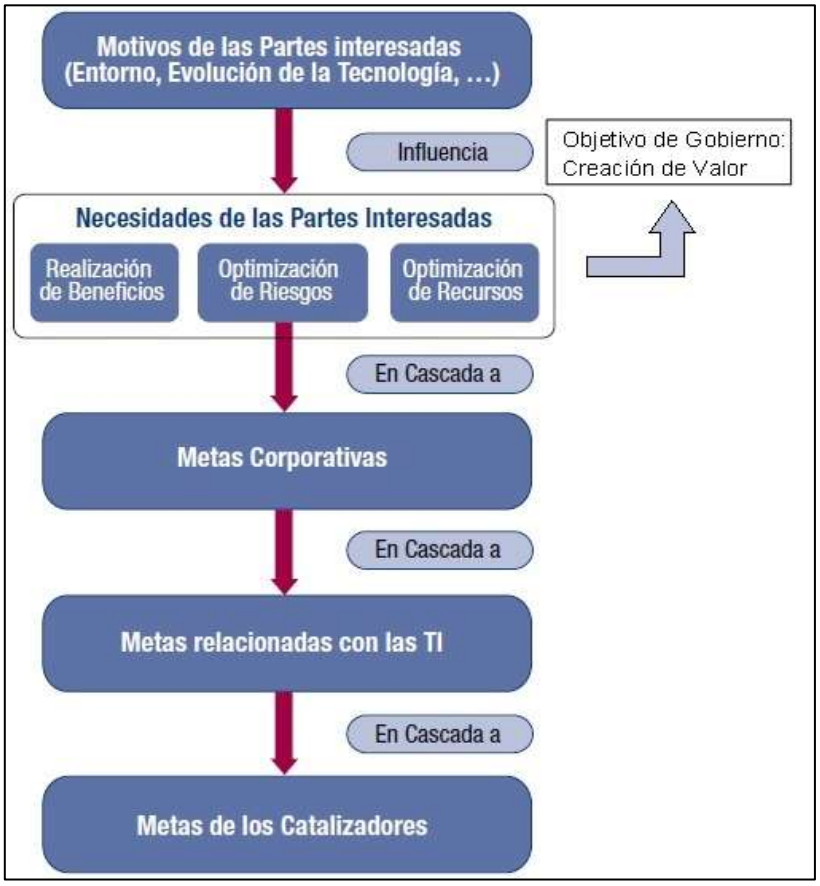
Según el primer principio de COBIT 5, "Satisfacer las Necesidades de la Partes Interesadas", las empresas existen para crear valor para sus interesados, por lo que cualquier empresa "*tendrá la creación de valor como un objetivo de Gobierno. Creación*

[1] ISACA, *COBIT 5 Un Marco de Negocio para el Gobierno y la Gestión de la empresa*, USA, ISACA, 2012. Pág. 2.
[2] Ibídem, pág. 13.

de valor significa conseguir beneficios a un coste óptimo de los recursos mientras se optimiza el riesgo" [3].

Con este enfoque, determina que las necesidades de las partes interesadas deben transformarse en una estrategia corporativa factible, creando una cascada de metas descendente, desde las metas corporativas hacia las metas relacionadas con las TI y las metas específicas habilitantes o catalizadoras. Este concepto se visualiza en las figuras 3 y 4 del marco de trabajo de COBIT 5, parte de las cuales se muestra a continuación:

Figura 2: Cascada de metas de COBIT 5



Fuente: ISACA **Elaborado por**: Katalina Coronel Hoyos

En su segundo principio, "Cubrir la Empresa Extremo a Extremo", COBIT 5 define un enfoque de gobierno y su relación con la gestión, que se forma por los siguientes componentes clave:

[3] Ibídem, pág. 17.

Figura 3: Gobierno y Gestión en COBIT 5

Fuente: ISACA **Elaborado por**: ISACA

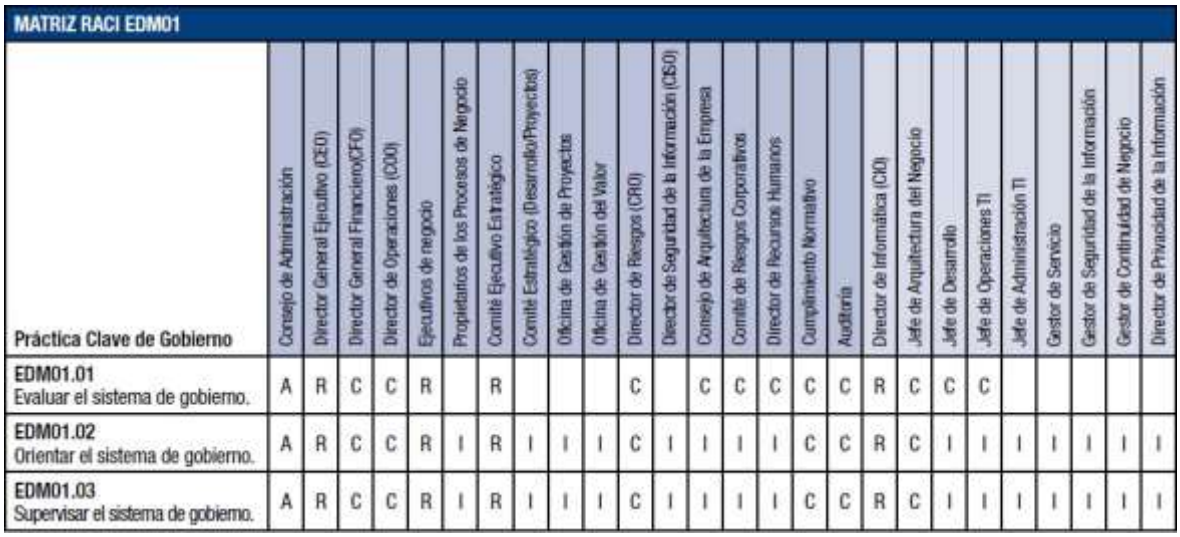
En este sistema, los catalizadores de gobierno son los recursos organizativos para el gobierno, tales como marcos de referencia, principios, estructuras, procesos y prácticas, a través de los que, o hacia los que, las acciones son dirigidas y los objetivos pueden ser alcanzados. Los catalizadores también incluyen los recursos corporativos, como capacidades de servicios, personas e información. Una falta de recursos o catalizadores puede afectar a la capacidad de la empresa de crear valor[4].

En cuanto al alcance, el gobierno puede ser aplicado a toda la empresa, a una entidad, a un activo tangible o intangible, entre otros. Es posible definir diferentes vistas de la empresa a la que se aplica el gobierno, y es esencial definir bien este alcance del sistema de gobierno. Un último elemento son los roles, actividades y relaciones de gobierno, que definen quién está involucrado en el gobierno, como se involucran, lo que hacen y cómo interactúan, dentro del alcance de cualquier sistema de gobierno.

Este segundo principio también se refleja en la Matriz RACI, cuyas siglas se refieren a los roles que tienen los diferentes actores en una empresa: “R”, define al Responsable de ejecutar la actividad, “A” es a quien se rinde cuentas de su ejecución, “C” es a quien se Consulta para obtener insumos para la actividad, e “I” es a quien se Informa; estos roles no solamente se refieren a la función de TI, sino que abarca a todo el negocio, tal como se puede ver en el siguiente ejemplo:

[4] Ibídem, pág. 24.

Figura 4: Ejemplo de Matriz RACI



MATRIZ RACI EDM01																										
Práctica Clave de Gobierno	Consejo de Administración	Director General Ejecutivo (CEO)	Director General Financiero(CFO)	Director de Operaciones (COO)	Ejecutivos de negocio	Propietarios de los Procesos de Negocio	Comité Ejecutivo Estratégico	Comité Estratégico (Desarrollo/Proyectos)	Oficina de Gestión de Proyectos	Oficina de Gestión del Valor	Director de Riesgos (CRO)	Director de Seguridad de la Información (CISO)	Consejo de Arquitectura de la Empresa	Comité de Riesgos Corporativos	Director de Recursos Humanos	Cumplimiento Normativo	Auditoría	Director de Informática (CIO)	Jefe de Arquitectura del Negocio	Jefe de Desarrollo	Jefe de Operaciones TI	Jefe de Administración TI	Gestor de Servicio	Gestor de Seguridad de la Información	Gestor de Continuidad de Negocio	Director de Privacidad de la Información
EDM01.01 Evaluar el sistema de gobierno.	A	R	C	C	R		R				C		C	C	C	C	C	R	C	C	C					
EDM01.02 Orientar el sistema de gobierno.	A	R	C	C	R	I	R	I	I	I	C	I	I	I	I	C	C	R	C	I	I	I	I	I	I	I
EDM01.03 Supervisar el sistema de gobierno.	A	R	C	C	R	I	R	I	I	I	C	I	I	I	I	C	C	R	C	I	I	I	I	I	I	I

Fuente: ISACA **Elaborado por**: ISACA

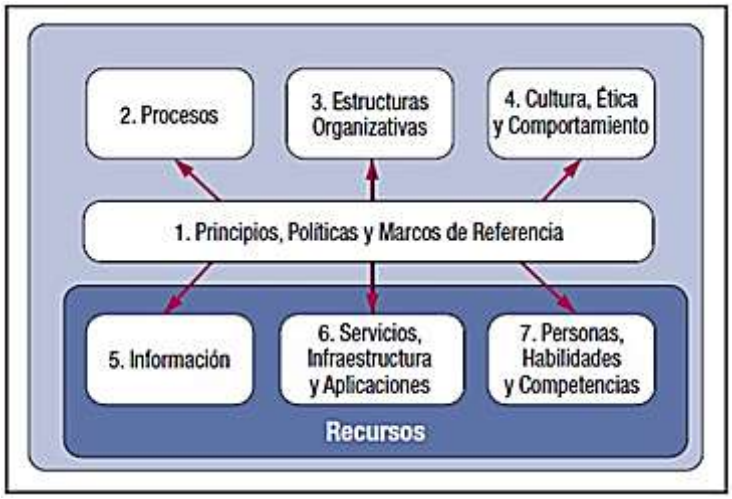
El principio 3, “Aplicar un marco de trabajo único integrado”, se refiere a la amplitud de normas y estándares sobre las que se ha basado el desarrollo de COBIT 5 y la elaboración de su marco de referencia, lo cual le permite alinearse con prácticas y estándares relevantes de alto nivel que constituyen guías para el gobierno y la gestión de la tecnología empresarial, tales como: COSO, COSO ERM, ISO/IEC 9000, ISO/IEC 31000, ISO/IEC 38500, ITIL, ISO/IEC 27000 series, TOGAF, PMBOK/PRINCE2, CMMI, King III, entre otras.

En el principio 4, “Hacer posible un enfoque holístico”, COBIT 5 se enfoca en “c*ubrir completamente las responsabilidades funcionales de TI y del negocio, y todos los aspectos que llevan a la gestión y el gobierno eficaz de las TI de la empresa, tales como estructuras organizativas, políticas y cultura, además de los procesos*”[5].

Para ello, se han desarrollado los “Catalizadores” como factores que influyen de manera general sobre el logro de los objetivos de la organización, y están divididos en las siete categorías que se muestran en la siguiente figura y cuya descripción se detalla a continuación:

[5] Ibídem, pág. 15.

Figura 5: Catalizadores Corporativos COBIT 5



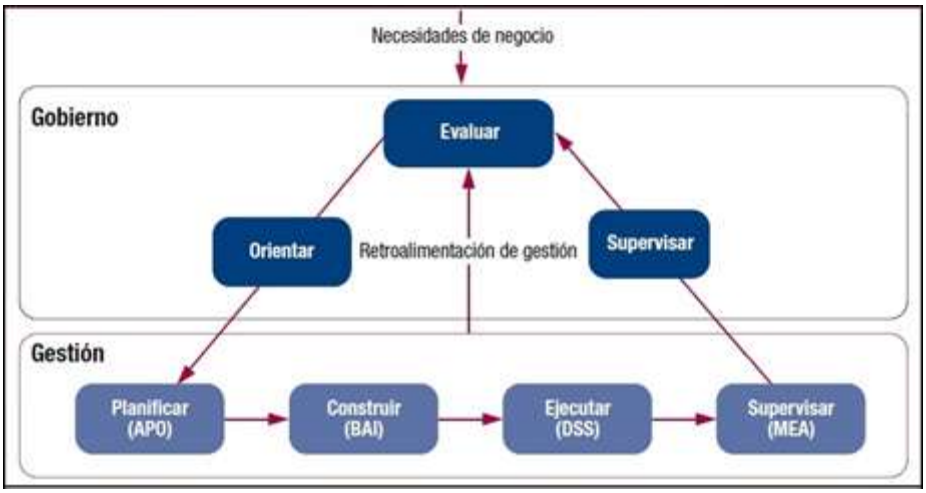
Fuente: ISACA **Elaborado por**: ISACA

1. **Principios, políticas y marcos de referencia:** vehículo para traducir el comportamiento deseado en guías prácticas para la gestión del día a día.
2. **Los procesos:** conjunto organizado de prácticas y actividades para alcanzar objetivos y producir resultados que soporten metas relacionadas con TI.
3. **Las estructuras organizativas:** las entidades de toma de decisiones clave en una organización.
4. **La Cultura, ética y comportamiento** de los individuos y de la empresa son muy a menudo subestimados como factor de éxito en el gobierno y gestión.
5. **La información:** incluye toda la información producida y utilizada, la cual es necesaria para mantener la organización funcionando y bien gobernada, pero a nivel operativo, a menudo es el producto clave de la empresa en sí misma.
6. **Los servicios, infraestructuras y aplicaciones:** incluyen la infraestructura, tecnología y aplicaciones que proporcionan a la empresa, servicios y tecnologías de procesamiento de la información.
7. **Las personas, habilidades y competencias:** están relacionadas con las personas y son necesarias para poder completar de manera satisfactoria todas las actividades y para la correcta toma de decisiones y de acciones correctivas. [6]

En el quinto principio, “Separar el Gobierno de la Gestión”, COBIT 5 hace una clara diferenciación entre las actividades de gobierno y de gestión, que se refleja en los dominios del modelo de referencia de procesos, tal como se muestra en la siguiente figura:

[6] Ibídem, pág. 27.

Figura 6: Dominios del modelo de referencia de procesos



Fuente: ISACA **Elaborado por**: ISACA

En este esquema, los conceptos de Gobierno y Gestión son definidos por COBIT 5 de la siguiente manera:

> *El Gobierno asegura que se evalúan las necesidades, condiciones y opciones de las partes interesadas para determinar que se alcanzan las metas corporativas equilibradas y acordadas; estableciendo la dirección a través de la priorización y la toma de decisiones; y midiendo el rendimiento y el cumplimiento respecto a la dirección y metas acordadas.*
>
> *En muchas corporaciones, el gobierno global es responsabilidad del comité de dirección bajo el liderazgo del presidente. Algunas responsabilidades de gobierno específicas se pueden delegar en estructuras organizativas especiales al nivel apropiado, particularmente en las corporaciones más grandes y complejas.*
>
> *La gestión planifica, construye, ejecuta y controla actividades alineadas con la dirección establecida por el cuerpo de gobierno para alcanzar las metas empresariales. En muchas empresas, la gestión es responsabilidad de la dirección ejecutiva bajo el liderazgo del Director General Ejecutivo (CEO)*[7]*.*

El modelo de referencia de procesos de COBIT 5 divide los procesos de gobierno y de gestión de la TI empresarial en dos dominios principales de procesos:

• Gobierno: Contiene cinco procesos de gobierno; dentro de cada proceso se definen prácticas de evaluación, orientación y supervisión (EDM).

• Gestión: Contiene cuatro dominios, para las áreas de responsabilidad de planificar, construir, ejecutar y supervisar (*Plan, Build, Run and Monitor - PBRM*). Los

[7] Ibídem, pág. 14.

nombres de estos dominios han sido elegidos de acuerdo a estas designaciones de áreas principales, pero contienen más verbos para describirlos:

– Alinear, Planificar y Organizar (*Align, Plan and Organise*, *APO*)

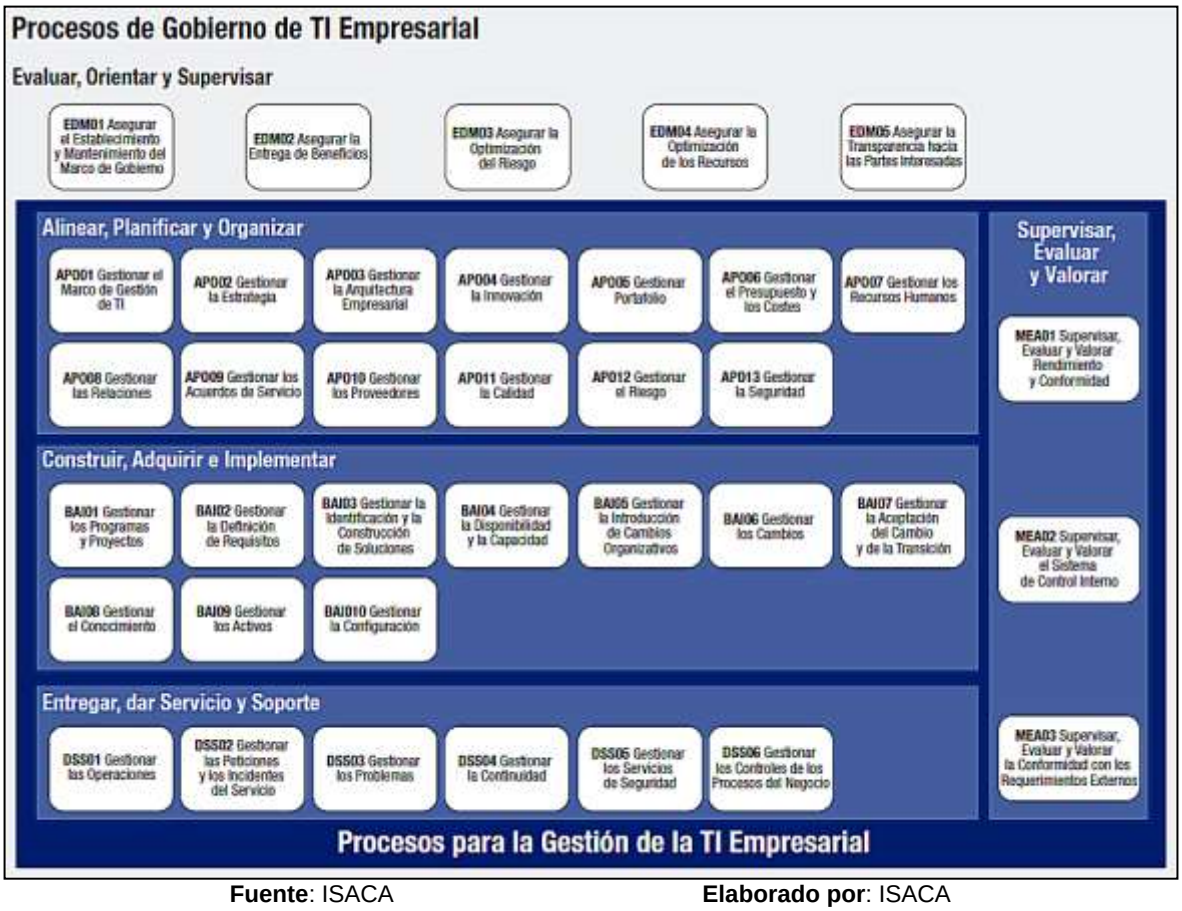
– Construir, Adquirir e Implementar (*Build, Acquire and Implement*, *BAI*)

– Entregar, dar Servicio y Soporte (*Deliver, Service and Support*, *DSS*)

– Supervisar, Evaluar y Valorar (*Monitor, Evaluate and Assess*, *MEA*) [8]

La siguiente figura muestra los 5 procesos de gobierno y 32 de gestión de COBIT 5:

Figura 7: Modelo de Referencia de Procesos de COBIT 5



Fuente: ISACA **Elaborado por**: ISACA

Para evaluar los procesos, el conjunto de productos de COBIT 5 incluye un modelo de capacidad de procesos, basado en la norma internacionalmente reconocida ISO / IEC 15504 de Ingeniería de Software-Evaluación de Procesos[9]. En este modelo, existen 6 niveles de capacidad que puede alcanzar un proceso:

[8] Ibídem, pág. 32.
[9] Ibídem, pág. 41.

0. Proceso incompleto: El proceso no está implementado o no alcanza su propósito. A este nivel, hay muy poca o ninguna evidencia de ningún logro sistemático del propósito del proceso.

1. Proceso ejecutado (1 atributo): El proceso alcanza su propósito.

2. Proceso gestionado (2 atributos): El proceso está ya implementado de forma gestionada (planificado, supervisado y ajustado) y los resultados de su ejecución están establecidos, controlados y mantenidos apropiadamente.

3. Proceso establecido (2 atributos): El proceso gestionado está ahora implementado usando un proceso definido que es capaz de alcanzar sus resultados de proceso.

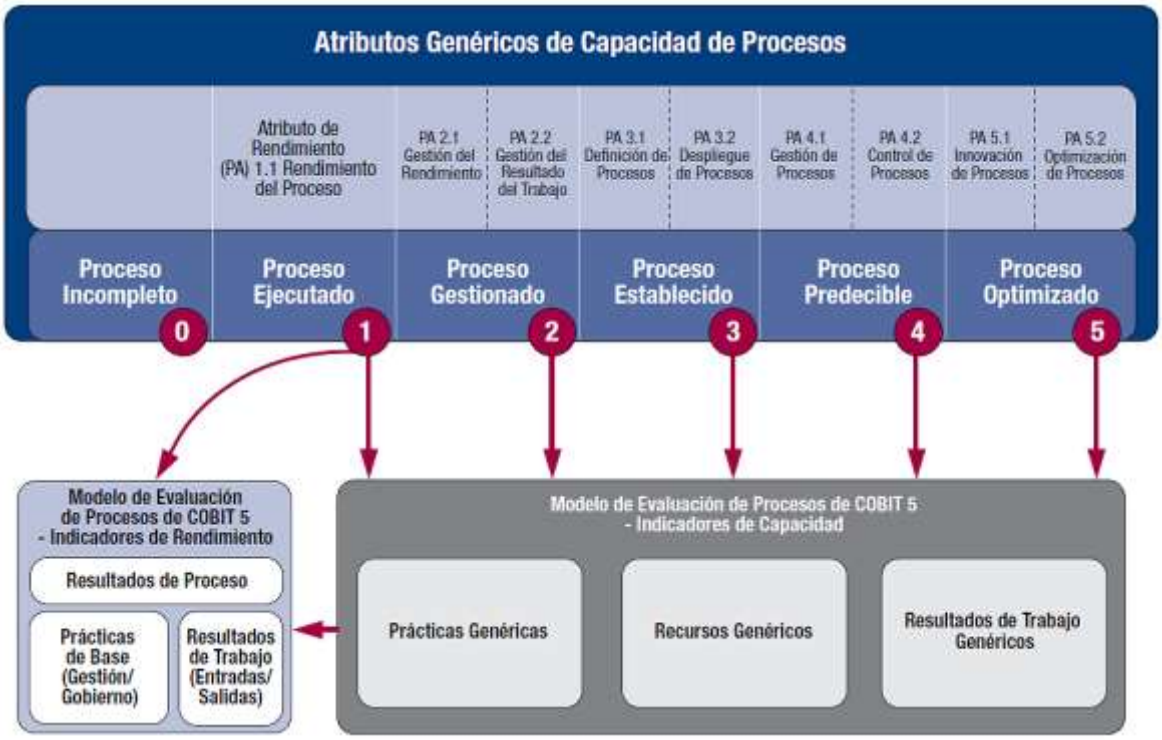
4. Proceso predecible (2 atributos): El proceso establecido ahora se ejecuta dentro de límites definidos para alcanzar sus resultados de proceso.

5. Proceso optimizado (2 atributos) – El proceso predecible es mejorado de forma continua para cumplir con metas empresariales presentes y futuras[10].

Cada nivel de capacidad puede ser alcanzado sólo cuando el nivel inferior se ha alcanzado por completo. Por ejemplo, un nivel 3 de capacidad de proceso (establecido) requiere que los atributos de definición y despliegue del proceso se hayan alcanzado ampliamente, sobre la consecución completa de los atributos del nivel 2 de madurez de procesos (proceso gestionado). El resumen de este modelo se muestra en la siguiente figura:

[10] Ibídem, pág. 42.

Figura 8: Resumen del Modelo de Capacidad de Procesos de COBIT 5



Fuente: ISACA **Elaborado por**: ISACA

Para evaluar si un proceso alcanza sus objetivos (nivel de capacidad 1), se debe seguir los siguientes pasos:

1. Revisar los resultados del proceso tal y como se describen para cada proceso en sus descripciones detalladas, y usar las escalas y ratios de la ISO/IEC 15504 para asignar un ratio para el grado en el que cada objetivo es alcanzado. Esta escala consiste en los siguientes ratios:

Tabla 1: Escalas y ratios de la norma ISO/IEC 15504

Nivel	Descripción	Logro
N (No alcanzado)	Hay poca o ninguna evidencia de los logros del atributo en la evaluación del proceso.	0 a 15%
P (Logrado parcialmente)	Hay una cierta evidencia de un enfoque y un logro del atributo en la evaluación del proceso. Algunos aspectos de la realización del atributo pueden ser impredecibles.	>15% a 50%
L (logrado en gran medida)	Hay evidencia de un enfoque sistemático para el logro significativo del atributo evaluado. Alguna debilidad relacionada con este atributo puede existir en el proceso.	>50% a 85%
F (Totalmente logrado)	Hay evidencia de un enfoque completo y sistemático, y la plena realización, del atributo definido en el proceso de evaluación. No hay debilidades significativas en relación a este atributo.	>85% a 100%

Fuente: ISACA **Elaborado por**: Katalina Coronel Hoyos

2. Las prácticas del proceso (de gobierno o de gestión) pueden ser evaluadas usando la misma escala de puntuación.

3. Para afinar la evaluación, los productos del trabajo pueden ser considerados para determinar el grado al que un atributo de evaluación específico ha sido alcanzado[11].

Otro de los productos de la familia COBIT 5 es su Guía de Implantación[12], que está basada en la publicación titulada "*Implementación de COBIT 5*", en la cual se describe cómo implementar la gestión de las TI de la empresa basada en COBIT 5, dentro de su ciclo de vida de la mejora continua y cómo crear el entorno adecuado, los catalizadores necesarios, puntos de fallo típicos y eventos desencadenantes para la implementación, cuyas principales fases son las siguientes:

1. Comienza con el reconocimiento y aceptación de la necesidad de una iniciativa de implementación o mejora. Identifica los puntos débiles actuales y desencadena y crea el ánimo de cambio a un nivel de dirección ejecutiva.
2. Se evalúa el estado actual y se identifican los problemas y deficiencias mediante la revisión de capacidad. Se concentra en definir el alcance de la iniciativa de implementación o mejora, empleando la cascada de metas de COBIT: empresariales - TI - procesos, considerando los procesos clave en los que focalizarse.
3. Se establece un objetivo de mejora, seguido de un análisis más detallado aprovechando las directrices de COBIT para identificar diferencias y posibles soluciones. Algunas soluciones pueden ser beneficios inmediatos (quick wins) y otras actividades pueden ser más desafiantes y de largo plazo. La prioridad deberían ser aquellas iniciativas que son más fáciles de conseguir y aquellas que podrían proporcionar los mayores beneficios.
4. La fase 4 planifica soluciones prácticas mediante la definición de proyectos apoyados por casos de negocios justificados. Además, se desarrolla un plan de cambios para la implementación. Un caso de negocio bien desarrollado ayuda a asegurar que se identifican y supervisan los beneficios del proyecto.
5. Las soluciones propuestas son implementadas en prácticas día a día. Se pueden definir mediciones y establecer la supervisión empleando las metas y métricas de COBIT para asegurar que se consigue y mantiene la alineación con el negocio y que el rendimiento puede ser medido.

[11] Ibídem, pág. 45.
[12] Ibídem, pág. 35.

6. Se focaliza en la operación sostenible de los nuevos o mejorados catalizadores y de la supervisión de la consecución de los beneficios esperados.
7. Durante la fase 7, se revisa el éxito global de la iniciativa, se identifican requisitos adicionales para el gobierno o la gestión de la TI empresarial y se refuerza la necesidad de mejora continua**.**

Como se puede apreciar de todos los elementos presentados, el marco de referencia de COBIT 5 proporciona varias herramientas que se pueden adaptar y utilizar para evaluar, dirigir y monitorear el Gobierno de TI, así como para contar con referencias para el desarrollo e implementación de buenas prácticas aceptadas internacionalmente, que contribuyen con el logro de los objetivos de TI y corporativos, de manera holística e integral, por lo que ha sido elegido como base para el desarrollo de la presente metodología.

1.2. Normas de Gestión del Riesgo Operativo y de Medidas de Seguridad de la Superintendencia de Bancos y Seguros

1.2.1. Norma de Gestión del Riesgo Operativo

Mediante resolución No. JB-2005-834 de 20 de octubre de 2005, la Superintendencia de Bancos y Seguros (SBS) emitió la norma “De la Gestión del Riesgo Operativo”, que fue incorporada en el Título X, Capítulo V de la Codificación de Resoluciones de la Superintendencia de Bancos y Seguros y de la Junta Bancaria (CRSBSYJB), y es de aplicación obligatoria para las instituciones financieras públicas y privadas, el Banco Central del Ecuador, las compañías de arrendamiento mercantil, las compañías emisoras y administradoras de tarjetas de crédito y las corporaciones de desarrollo de mercado secundario de hipotecas.

Posteriormente, esta norma fue modificada mediante resoluciones No. JB-2008-1202 de 23 de octubre del 2008, JB-2009-1491 de 26 de octubre del 2009, JB-2011-1851 de 11 de enero del 2011, JB-2011-1983 de 26 de agosto del 2011, y JB-2012-2148 de 26 de abril del 2012, las mismas que igualmente se fueron actualizando en el Título X y Capítulo V de la CRSBSYJB.

En esta base legal, el riesgo operativo se define como la posibilidad de que se ocasionen pérdidas financieras por eventos derivados de fallas o insuficiencias en los

procesos, personas, tecnología de información y por eventos externos, los cuales constituyen los Factores del riesgo operativo[13].

Dentro del factor de Tecnología de Información, se requiere que las instituciones controladas cuenten con la tecnología de información que garantice la captura, procesamiento, almacenamiento y transmisión de la información de manera oportuna y confiable; evite interrupciones del negocio y logre que la información, inclusive aquella bajo la modalidad de servicios provistos por terceros, sea íntegra, confidencial y esté disponible para una apropiada toma de decisiones.

De acuerdo con esta norma, para considerar la existencia de un apropiado ambiente de gestión de riesgo operativo en lo relativo al factor de tecnología de información, las instituciones controladas por la SBS deben definir formalmente políticas, procesos y procedimientos que aseguren una adecuada planificación y administración de la tecnología de información[14].

Dichas políticas, procesos y procedimientos deben referirse a:

1. **Administración de la tecnología de información**: debe dar un soporte adecuado a los requerimientos de operación actuales y futuros de la entidad.
2. **Operaciones de tecnología de información**: controles para que las operaciones satisfagan los requerimientos de la entidad.
3. **Recursos y servicios provistos por terceros**: para garantizar que los recursos y servicios provistos por terceros, se administren con base en responsabilidades claramente definidas y estén sometidas a un monitoreo de su eficiencia y efectividad.
4. **Sistema de administración de seguridad**: con el fin de garantizar que el mismo satisfaga las necesidades de la entidad para salvaguardar la información contra el uso, revelación y modificación no autorizados, así como daños y pérdidas.
5. **Continuidad de las operaciones**: para contar con controles que permitan mitigar el riesgo de presentarse interrupciones en la operación del negocio.
6. **Adquisición, desarrollo, implementación y mantenimiento de las aplicaciones**: buscan satisfacer las necesidades y objetivos del negocio, con un proceso controlado adecuadamente.

[13] Superintendencia de Bancos y Seguros, *Codificación de Resoluciones de la Superintendencia de Bancos y Seguros y de la Junta Bancaria*, Ecuador, SBS, 2005. Título X, Capítulo V, pág. 252.
[14] Ibídem, pág. 255.

7. **Infraestructura tecnológica**: que sea administrada, monitoreada y documentada de forma adecuada, en lo relativo a bases de datos, redes de datos, software de base y hardware.
8. **Medidas de seguridad en canales electrónicos**: su objetivo es garantizar que las transacciones realizadas a través de canales electrónicos cuenten con los controles, medidas y elementos de seguridad para evitar el cometimiento de eventos fraudulentos y garantizar la seguridad y calidad de la información de los usuarios así como los bienes de los clientes a cargo de las instituciones controladas.
9. **Cajeros automáticos**: se busca garantizar la seguridad en las transacciones realizadas a través de los cajeros automáticos.
10. **Puntos de venta**: su fin es garantizar la seguridad en las transacciones realizadas a través de los dispositivos de puntos de venta (POS por sus siglas en inglés) y PIN Pad (teclados móviles para el ingreso de las claves de los clientes).
11. **Banca electrónica**: las instituciones que ofrecen servicios a través de este canal electrónico deben contar con controles para garantizar la seguridad en las transacciones realizadas mediante banca electrónica (Internet).
12. **Banca móvil**: Las instituciones del sistema financiero que presten servicios a través de banca móvil (celular) deben sujetarse en lo que corresponda, a las medidas de seguridad requeridas para canales electrónicos y banca electrónica.
13. **Sistemas de audio respuestas** (IVR por las siglas en inglés, de *Interactive Voice Response*): Las instituciones del sistema financiero que presten servicios a través de IVR (telefónico) deben sujetarse en lo que corresponda, a las medidas de seguridad requeridas para canales electrónicos y banca electrónica.
14. **Corresponsales no bancarios**: Las instituciones del sistema financiero que presten servicios a través de corresponsales no bancarios (tiendas, comercios autorizados) deben sujetarse en lo que corresponda, a las medidas de seguridad requeridas para canales electrónicos, puntos de venta y banca electrónica[15].

Los controles identificados en esta normativa de la SBS serán utilizados en el Capítulo 3 para realizar un mapeo de estos requerimientos frente a los procesos y prácticas clave de COBIT 5, con el fin de determinar las exigencias normativas existentes para las instituciones financieras ecuatorianas respecto de la tecnología de información, y evaluar con ellas el factor de Cumplimiento de TI, que es parte del objeto de esta metodología.

[15] Ibídem, págs. 255 a 265.1

1.2.2. Norma sobre Medidas de Seguridad

Como una normativa complementaria a la de Gestión del Riesgo Operativo, la Superintendencia de Bancos y Seguros del Ecuador emitió la resolución No. JB-2011-1851 el 11 de enero del 2011, con la que se incorporó la sección VIII "De las medidas de seguridad" en el Título II, Capítulo I de la Codificación de Resoluciones de la Superintendencia de Bancos y Seguros y de la Junta Bancaria (CRSBSYJB).

Posteriormente, esta norma fue actualizada mediante las resoluciones No. JB-2011-1895 de 15-marzo-2011, JB-2011-1921 de 19-abril-2011, JB-2011-1923 de 26-abril-2011, JB-2012-2090 de 17-enero-2012, JB-2012-2148 de 26-abril-2012 y JB-2012-2352 de 23-octubre-2012, las mismas que igualmente fueron incorporadas oportunamente en la CRSBSYJB.

Con esta norma[16], la Superintendencia de Bancos y Seguros (SBS) requirió de forma obligatoria a todas las instituciones financieras ecuatorianas, la adopción de medidas de seguridad mínimas relacionadas con:

- **Establecimientos**: se requiere la instalación y funcionamiento de dispositivos, mecanismos y equipos, con el objeto de contar con la protección requerida en los establecimientos, para clientes, empleados, público y patrimonio, estableciendo parámetros de acuerdo a la ubicación del establecimiento.
- **Manuales y políticas de seguridad y protección**: su fin es definir ciertos aspectos fundamentales para garantizar la seguridad de las instituciones, en particular de sus empleados y usuarios, establecimientos, bienes y patrimonio, así como para el resguardo en el transporte de efectivo y valores.
- **Personal de seguridad**: con el objeto de contar con empleados debidamente formados y capacitados para supervisar y custodiar las instalaciones de la entidad en su interior o exterior al momento de apertura del establecimiento, durante el horario normal y diferido de atención al público y hasta tanto se encuentren empleados laborando.
- **Bóvedas y cajas fuertes**: Las bóvedas, cajas fuertes y sus áreas conexas en que se deposite efectivo y valores deben contar con elementos y sistemas que proporcionen una adecuada seguridad y protección, así como cumplir con estándares internacionales en su construcción.

[16] Superintendencia de Bancos y Seguros, *Codificación de Resoluciones de la Superintendencia de Bancos y Seguros y de la Junta Bancaria*, Ecuador, SBS, 2011. Título II, Capítulo I, Sección VIII, pág. 61.6

- **Sistemas de alarma de robo e incendio**: se realizan requerimientos sobre los sistemas de alarma contra robo e incendio con que deben contar todas las instalaciones de las entidades financieras, especialmente los relacionados con la verificación de su operatividad, monitoreo y planes de respuesta.
- **Sistemas de vídeo vigilancia** (cámaras): se realizan requerimientos sobre los sistemas de cámaras fijas y movibles de circuito cerrado de televisión con que deben contar las instalaciones de las entidades financieras, especialmente los relacionados con su monitoreo, cobertura y almacenamiento de imágenes.
- **Inhibidores de señal celular**: se refiere a normas y procedimientos estrictos que las instituciones financieras deben establecer para regular o prohibir, el uso de telefonía celular y cualquier otro mecanismo de comunicación desde el interior de sus instalaciones.
- **Cajeros automáticos**: se requieren controles y medidas de seguridad que los cajeros automáticos de las instituciones financieras deben cumplir.
- **Transporte de fondos y valores**: se refiere a medidas de seguridad mínimas que se deben aplicar para el transporte de especies monetarias y valores, vinculados con las actividades de las instituciones financieras.
- **Seguro contra fraudes generados a través de la tecnología**: se requiere contratar anualmente este seguro, con coberturas que aseguren a la entidad contra fraudes generados a través de su tecnología de la información, sistemas telemáticos, electrónicos o similares, ante varios riesgos.

De las medidas de seguridad anteriormente detalladas, se puede observar que existen varios requerimientos relacionados con la seguridad de la información y la tecnología de información, las mismas que se utilizarán en el Capítulo 3 para realizar un mapeo de estos requerimientos normativos frente a los procesos y prácticas clave de COBIT 5 y de la norma ISO/IEC 27005, con el fin de determinar exigencias normativas adicionales para las instituciones financieras ecuatorianas respecto de la tecnología de información, y evaluar con ellas el factor de Cumplimiento de TI, que es parte del objeto de esta metodología.

1.3. Metodologías de generación de Matrices de Riesgo

De manera general, el riesgo se define como la probabilidad de que ocurra un evento no deseado, mismo que puede generar pérdidas o efectos adversos. La Gestión de Riesgos tiene como finalidad minimizar la probabilidad de ocurrencia del evento adverso,

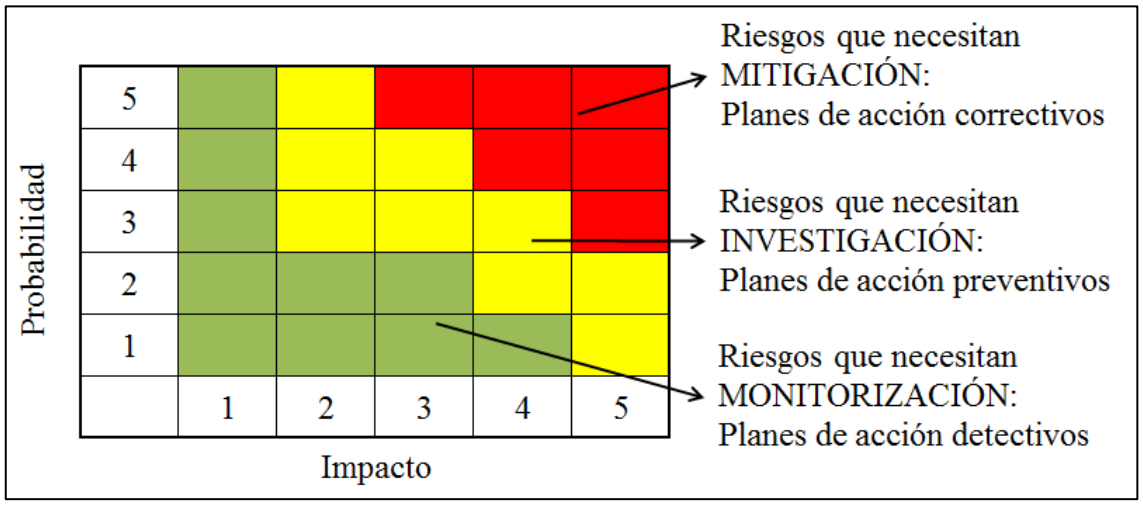
a través de la identificación, medición, tratamiento, monitoreo y control de los riesgos, y se aplica a diferentes tipos de riesgos, tales como los laborales, financieros, operativos, tecnológicos, de lavado de activos, entre otros.

Debido a que los riesgos pueden ser de diversa índole y magnitud, es necesario tratarlos y gestionarlos de manera ordenada y sistemática, enfocándose mayormente en los riesgos de nivel más alto, lo cual además permite una utilización eficiente de los recursos disponibles.

Para ello, se puede construir una matriz de riesgos, en la que se representen la probabilidad de ocurrencia de los riesgos por un lado, y por otro la gravedad o severidad de sus consecuencias (impacto o costos).

La combinación de la probabilidad y el impacto determina el nivel de riesgo de un evento, el cual se puede identificar con un color distintivo, tal como se observa en el siguiente ejemplo[17]:

Figura 9: Ejemplo de Matriz de Riesgos



Fuente: Beltrán Marta **Elaborado por**: Katalina Coronel Hoyos

En este ejemplo los riesgos se clasifican según su probabilidad: muy baja (1), baja (2), media (3), alta (4) o muy alta (5). En cuanto al impacto, se ha medido en costos con una escala que cuantifica si este impacto es: menor de 1,000 euros (1), entre 1,000 y 10,000 (2), entre 10,000 y 100,000 (3), entre 100,000 y 1'000,000 (4) o mayor (5).

Adicionalmente, la probabilidad puede ser potencial o histórica, es decir, si el evento ha ocurrido alguna vez se mide el período transcurrido entre cada evento (frecuencia), mientras que si es potencial, se estima la frecuencia de su posible ocurrencia.

[17] Beltrán Marta. "Matriz de riesgos". Internet. http://redindustria.blogspot.com/2010/05/matriz-de-riesgos.html. Acceso: 1-abr-2013.

Específicamente en el caso del factor "Tecnología de información" que señala la norma de Gestión del Riesgo Operativo de la Superintendencia de Bancos y Seguros, la ocurrencia de un evento adverso en una institución financiera tendrá un nivel de impacto acorde con el nivel de dependencia que tengan sus procesos respecto de la tecnología de información. Por ejemplo, una institución financiera que tenga un nivel bajo de automatización de sus procesos operativos, tendrá un bajo impacto ante la ocurrencia de un evento de riesgo tecnológico. En cambio en un Banco grande, en el que el 95% de sus procesos estén automatizados, será mayor el universo de posibles riesgos, así como su probabilidad de ocurrencia y su nivel de impacto.

Cabe anotar que la política de Gestión de riesgos a aplicarse dentro de una institución dependerá de su apetito de riesgo, y se reflejará en el umbral de riesgo que defina la instancia de gobierno en su matriz de riesgos. Una institución con un alto apetito de riesgo tendrá políticas menos conservadoras que otra cuyo apetito de riesgo sea bajo.

La importancia de construir una matriz de riesgos se basa en que permite tomar acciones correctivas y aplicar controles mitigantes de los riesgos identificados y medidos, con el fin de prevenir la generación de pérdidas, que pueden ser reputacionales, de imagen, operativas, entre otras, y que generalmente derivan en pérdidas económicas.

Respecto al Gobierno de Tecnología de Información, la matriz o mapa de riesgos permitirá identificar el nivel de riesgo que presentan los elementos de gobierno de TI, con el fin de definir las medidas a aplicar para su mejora continua en una institución.

1.4. Requerimientos del Estándar ISO/IEC 27005 "Gestión de Riesgos de Seguridad de la Información"

El estándar internacional ISO/IEC 27005 "*Information technology – Security techniques – Information security risk management*"[18] provee una guía para la gestión de riesgos en seguridad de la información en una organización, soportando en particular los requerimientos de un sistema de gestión de seguridad de información (ISMS por sus siglas en inglés) y los conceptos generales especificados en el estándar ISO/IEC 27001. Es aplicable a todos los tipos de organizaciones, sean comerciales, gubernamentales o sin fines de lucro, que pretenden gestionar los riesgos que pudieran comprometer la seguridad de su información.

Este estándar no constituye una metodología específica para la gestión del riesgo en seguridad de la información, ya que cada organización debe definirla según el alcance de su ISMS, el contexto de su administración de riesgos, o el sector de su industria.

[18] ISO/IEC 2008, *INTERNATIONAL STANDARD ISO/IEC 27005,* Suiza, 2008.

Este estándar contiene la descripción del proceso de gestión de riesgos de seguridad de la información y sus actividades. Estas actividades se refieren a las siguientes:

- Establecimiento del contexto
- Evaluación del riesgo
- Tratamiento del riesgo
- Aceptación del riesgo
- Comunicación del riesgo
- Monitoreo y revisión del riesgo

Cada una de estas actividades de gestión de riesgos está estructurada como sigue:

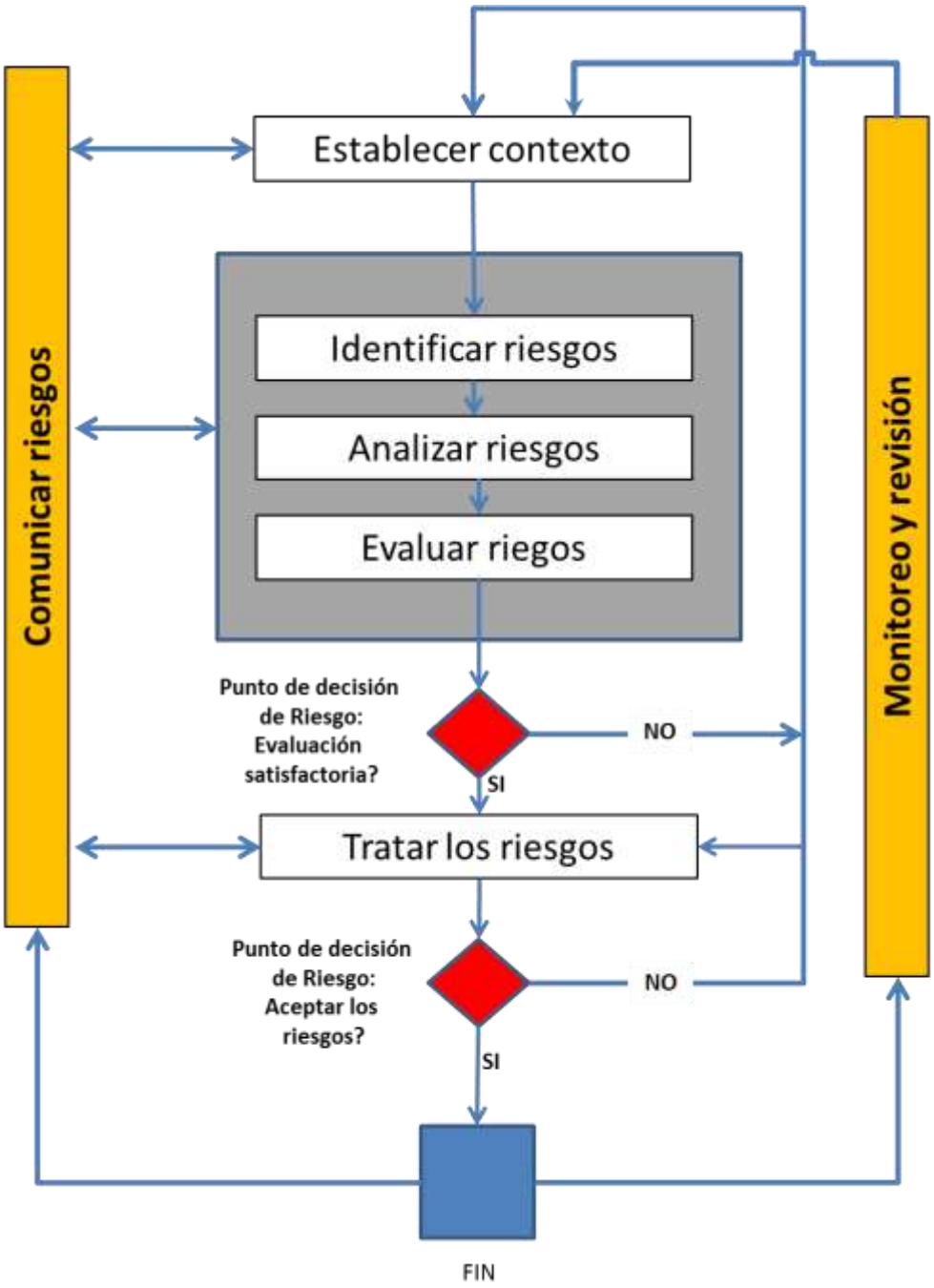
- Entrada: identifica cualquier información requerida para ejecutar la actividad
- Acción: Describe la actividad
- Guía de Implementación: provee una guía para ejecutar la acción.
- Salida: identifica cualquier información generada después de ejecutar la actividad.

Un enfoque sistemático para gestionar los riesgos de seguridad de la información es necesario para identificar las necesidades organizacionales relativas a seguridad de la información y crear un efectivo ISMS. Este enfoque debe ser ajustable al ambiente y recursos de la organización y debe estar alineado con el esquema de gestión de riesgos general de la empresa.

Para este estándar, los esfuerzos en seguridad de la información deben direccionar los riesgos de forma efectiva y oportuna donde y cuando sean necesarios. La gestión de riesgos de seguridad de la información debe ser un proceso continuo, debe ser parte integral de todas las actividades de gestión de seguridad de la información de una organización, como parte de sus procesos de negocio, y debe ser aplicada tanto a la implementación como a la operación diaria de un ISMS.

El esquema del proceso de gestión de riesgos de seguridad de la información en este estándar es el siguiente:

Figura 10: Proceso de gestión de riesgos de seguridad de la información



Fuente: ISO/IEC 2008 **Elaborado por**: Katalina Coronel Hoyos

Varios de los requisitos de este estándar están incorporados en las normas de la Superintendencia de Bancos y Seguros, por lo que en el Capítulo 3 se realizará una homologación o mapeo entre estos documentos normativos.

CAPÍTULO 2 - ANÁLISIS DE LOS ELEMENTOS DE COBIT 5 QUE PERMITAN DETERMINAR EL NIVEL DE RIESGO DEL GOBIERNO DE TI

Tal como se indicó en el numeral 1.1 del Capítulo 1, el enfoque principal de COBIT 5 se basa en el Gobierno de la tecnología de información empresarial, asegurando la alineación, realización de beneficios, optimización de riesgos y optimización de recursos hacia los objetivos empresariales y la satisfacción de necesidades de todas las partes interesadas.

Para enfocar aún más la evaluación en el gobierno, riesgos y cumplimiento de TI, dejando aparte posibles elementos más operativos, se ha analizado y seleccionado, de entre todos los elementos que provee COBIT 5, aquellos que tienen mayor influencia en la consecución de un buen Gobierno Corporativo.

Entre los elementos de COBIT 5 destacan los procesos y los catalizadores, con los cuales se conforma el sistema de gobierno al cual se orienta este marco de trabajo, por lo que en las siguientes secciones se efectúa el análisis de los mismos para la selección de aquellos más significativos que permitan realizar una posterior evaluación en una matriz de riesgos, en la que se refleje la situación de una institución financiera con respecto al sistema de Gobierno, Riesgos y Cumplimiento de TI.

2.1. Análisis y selección de procesos de COBIT 5 relacionados con el Gobierno de TI

Para la selección de los procesos de COBIT 5 que apoyan más directamente al gobierno de TI, se determinaron los siguientes criterios, que permitirán filtrar aquellos más relevantes con respecto al Gobierno de TI:

1. Que el proceso esté en el dominio de gobierno EDM Evaluar, Dirigir y Monitorear.
2. Que el proceso mantenga alineación “total” con los objetivos de gobierno.
3. Que el proceso provea información de insumo para alguno de los procesos del dominio de gobierno EDM.
4. Se analizaron los procesos que, a criterio de la revista Journal de ISACA, volumen 1, 2013, constituyen procesos de gobierno en COBIT 5.

Aplicando el criterio 1, los procesos EDM01, EDM02, EDM03, EDM04 y EDM05 quedarían seleccionados directamente para este análisis.

Para el análisis del criterio 2, relativo a la alineación “total” con los objetivos de gobierno, se examinaron las 17 metas u objetivos de negocio que COBIT 5 provee en su

cascada de metas[19], y su relación principal (P) o secundaria (S) con los objetivos de gobierno: realización de beneficios, optimización de riesgos y optimización de recursos, lo cual se muestra en la siguiente tabla[20]:

Tabla 2: Objetivos o metas corporativas de COBIT 5

Dimensión del CMI	Meta Corporativa	Relación con los Objetivos de Gobierno		
		Realización de Beneficios	Optimización de Riesgos	Optimización de Recursos
Financiera	1. Valor para las partes interesadas de las Inversiones de Negocio	P		S
	2. Cartera de productos y servicios competitivos	P	P	S
	3. Riesgos de negocio gestionados (salvaguarda de activos)		P	S
	4. Cumplimiento de leyes y regulaciones externas		P	
	5. Transparencia financiera	P	S	S
Cliente	6. Cultura de servicio orientada al cliente	P		S
	7. Continuidad y disponibilidad del servicio de negocio		P	
	8. Respuestas ágiles a un entorno de negocio cambiante	P		S
	9. Toma estratégica de Decisiones basada en Información	P	P	P
	10. Optimización de costes de entrega del servicio	P		P
Interna	11. Optimización de la funcionalidad de los procesos de negocio	P		P
	12. Optimización de los costes de los procesos de negocio	P		P
	13. Programas gestionados de cambio en el negocio	P	P	S
	14. Productividad operacional y de los empleados	P		P
	15. Cumplimiento con las políticas internas		P	
Aprendizaje y Crecimiento	16. Personas preparadas y motivadas	S	P	P
	17. Cultura de innovación de producto y negocio	P		

Fuente: ISACA **Elaborado por**: ISACA

Cabe anotar que, debido a una ambigüedad derivada de la traducción de la versión en inglés de COBIT 5 a su versión en castellano, tanto en las propias publicaciones de la familia de productos COBIT 5 en castellano, como en este documento, se utilizan indistintamente las palabras “meta” u “objetivo” para referirse a los objetivos señalados por COBIT 5[21].

Utilizando el mapeo provisto por COBIT 5 que se observa en la Tabla 2, se asignó un puntaje de 5 puntos a las relaciones soportadas de manera principal (P), y 1 punto a las relaciones soportadas de manera secundaria (S), para determinar aquellas metas de negocio que aportan de manera más importante a los 3 objetivos de gobierno. Los valores de 5 y 1 fueron elegidos por tener una distancia prudencial entre ellos, que facilita la identificación de una relación más importante (P) de una de menor importancia (S).

[19] ISACA, *COBIT 5 Un Marco de Negocio para el Gobierno y la Gestión de la empresa*, USA, ISACA, 2012. Pág. 19.
[20] ISACA, *COBIT 5 Procesos Catalizadores*, USA, ISACA, 2012. Pág. 14.
[21] En ciertas publicaciones de COBIT 5 se traduce la palabra “*Goal*” como “meta”, y en otras como “objetivo”.

Como se puede observar en la Tabla 2, los objetivos de negocio 2, 5, 9, 13 y 16 son los que dan soporte a los 3 objetivos de gobierno, por lo que al asignar puntos a su relación Principal o Secundaria, se obtuvieron los siguientes resultados:

Tabla 3: Objetivos de negocio que más aportan a los Objetivos de Gobierno

		OBJETIVOS DE GOBIERNO			
	OBJETIVOS DE NEGOCIO DE COBIT 5	Realización de beneficios	Optimización de riesgos	Optimización de recursos	TOTAL
1	Valor de los interesados de las inversiones del negocio				
2	**Portafolio de productos y servicios competitivos**	5	5	1	11
3	Riesgos del negocio administrados (protección de activos)				
4	Cumplimiento con leyes externas y regulaciones				
5	**Transparencia financiera**	5	1	1	7
6	Cultura de servicio orientada al cliente				
7	Continuidad y Disponibilidad de los servicios del negocio				
8	Respuestas ágiles a un ambiente de negocio cambiante				
9	**Toma de decisiones estratégica basada en información**	5	5	5	15
10	Optimización de los costos de entrega de servicios				
11	Optimización de la funcionalidad de los procesos de negocio				
12	Optimización de los costos de los procesos de negocio				
13	**Programas de cambio de negocio gestionados**	5	5	1	11
14	Productividad operacional y del personal				
15	Cumplimiento con políticas internas				
16	**Gente hábil y motivada**	1	5	5	11
17	Cultura de innovación de productos y del negocio				

Fuente: ISACA **Elaborado por**: Katalina Coronel Hoyos

Tal como se explicó en el Capítulo 1 (ver figura 2), los objetivos de negocio provistos por COBIT 5 tienen su soporte en objetivos relacionados con TI hacia los cuales se derivan en cascada; a su vez, los objetivos o metas de TI se derivan en cascada hacia los 37 procesos del modelo de referencia de procesos de COBIT 5, de la siguiente manera:

Figura 11: Cascada de metas hacia procesos de COBIT 5

Fuente: ISACA **Elaborado por**: Katalina Coronel Hoyos

En el ejercicio realizado en la Tabla 3, se descartó el objetivo de negocio 5, debido a que su puntaje es significativamente menor al máximo obtenido (15). Los restantes objetivos o metas de negocio 2, 9, 13 y 16 fueron mapeados hacia las metas u objetivos de TI, pero tomando en cuenta únicamente las relaciones de soporte principal (P), con el objetivo de filtrar aquellas que tienen mayor influencia en las metas de negocio seleccionadas. Para realizar este ejercicio, se utilizó el mapeo que provee COBIT 5 entre las 17 metas de negocio y las 17 metas de TI, que se muestran en el anexo A, y entre las 17 metas de TI y los 37 procesos de TI, que consta en el anexo B.

Aplicando el mapeo entre las metas de negocio y las metas de TI, quedaron seleccionadas las metas de TI 1, 3, 5, 7, 9, 12, 13, 14, 16 y 17, las cuales a su vez fueron mapeadas hacia los procesos de TI, obteniendo un puntaje de alineación máximo de 25 y mínimo de 3, por lo que se seleccionaron únicamente aquellos con un valor igual o superior al 80% de 25, es decir, de 20 puntos en adelante, más los 5 procesos del dominio de gobierno EDM que cumplen el criterio 1, quedando los siguientes:

Tabla 4: Mapeo Objetivos de TI seleccionados con Procesos de TI

	OBJETIVOS DE TI																
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
	Alineación entre TI y la estrategia de negocio	Cumplimiento y soporte de TI para el cumplimiento con leyes y regulac. externas	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	Administración de los riesgos del negocio relacionados con TI	Realización de beneficios del portafolio de inversiones y servicios habilitados por TI	Transparencia de costos, beneficios y riesgos de TI	Entrega de servicios de TI en línea con los requerimientos del negocio	Adecuado uso de aplicaciones, información y soluciones de tecnología	Agilidad de TI	Seguridad de información, infraestructura de procesamiento y aplicaciones	Optimización de activos, recursos y capacidades de TI	[illegible] de la integración de aplicaciones y tecnología dentro de [illegible]	Entrega de programas que generan beneficios, en tiempo, presupuesto y calidad	Disponibilidad de información confiable y útil para la toma de decisiones	Cumplimiento de TI con políticas internas	Personal de negocio y de TI competente y motivado	Conocimiento, pericia e iniciativas para la innovación del negocio
PROCESOS DE TI	**1**	**0**	**1**	**0**	**1**	**0**	**1**	**0**	**1**	**0**	**0**	**1**	**1**	**1**	**0**	**1**	**1**

Evaluar, Dirigir y Monitorear	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	**Puntaje**
EDM01 Asegurar el establecimiento y mantenimiento de un marco de trabajo de Gobierno	5		5		1		5		1			1	1	1		1	1	22
EDM02 Asegurar la entrega de beneficios	5		1		5		5					1	1	1		1	5	25
EDM03 Asegurar la optimización de riesgos	1		1				1						1	1		1	1	7
EDM04 Asegurar la	1		1		1		1		5				1			5	1	16

optimización de recursos																		
EDM05 Asegurar la transparencia de los interesados	1		5				5						1	1			1	14
Alinear, Planear y Organizar	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	
APO01 Gestionar el marco de trabajo de Administración de TI	5		1				1		5			1	1	1		5	5	25
APO02 Gestionar la Estrategia	5		1		1		5		1			1	1	1		1	5	22
APO03 Gestionar la Arquitectura Empresarial	5		1		1		1		5			1		1			1	16
APO04 Gestionar la Innovación	1				5				5			1		1			5	18
APO05 Gestionar el Portafolio	5		1		5		1		1				5				1	19
APO06 Gestionar el Presupuesto y los Costos	1		1		5		1						1					9
APO07 Gestionar los Recursos Humanos	5		1				1		1				5			5	5	23
APO08 Gestionar las Relaciones	5		1		1		5					5	1			1	5	24
APO09 Gestionar los Acuerdos de Servicios	1				1		5		1				1	5				14
APO10 Gestionar los Proveedores					1		5		5				1	1			1	14
APO11 Gestionar la Calidad	1				5		5		1				5	1		1	1	20
APO12 Gestionar los Riesgos							1		1				5	1		1	1	10
APO13 Gestionar la Seguridad							1							5				6
Construir, Adquirir y Operar	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	
BAI01 Gestionar Programas y Proyectos	5		1		5		1						5			1	1	19
BAI02 Gestionar la Definición de Requerimientos	5		1		1		5		1			5	1	1			1	21
BAI03 Gestionar la Identificación y Construcción de Soluciones	1				1		5					1	1	1			1	11
BAI04 Gestionar la Disponibilidad y Capacidad					1		5		1				1	5			1	14
BAI05 Gestionar la Habilitación del Cambio Organizacional	1		1		1		1		1			1	5				5	16
BAI06 Gestionar los Cambios			1		1		5		1			1	1	1			1	12
BAI07 Gestionar la Aceptación y Transición del Cambio					1		1		1			5	1	1			1	11
BAI08 Gestionar el Conocimiento	1				1		1		5					1		1	5	15
BAI09 Gestionar los Activos							1		1					1				3
BAI10 Gestionar la Configuración									1					5				6

Entregar Servicio y Soporte	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	
DSS01 Gestionar las Operaciones					1		5		1					1		1	1	10
DSS02 Gestionar las Solicitudes de Servicio e Incidentes							5							1			1	7
DSS03 Gestionar los Problemas					1		5		1			1		5			1	14
DSS04 Gestionar la Continuidad	1				1		5		1			1		5		1	1	16
DSS05 Gestionar los Servicios de Seguridad	1						1					1		1				4
DSS06 Gestionar los Controles de Procesos del Negocio							5					1		1		1	1	9
Monitorear, Evaluar y Valorar	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	
MEA01 Monitorear, Evaluar y Valorar el Desempeño y Conformidad	1		1		1		5		1				1	1		1	1	13
MEA02 Monitorear, Evaluar y Valorar el Sistema de Control Interno							1							1			1	3
MEA03 Monitorear, Evaluar y Valorar el Cumplimiento con Requerimientos Externos					1		1										1	3

Fuente: ISACA
Elaborado por: Katalina Coronel Hoyos

MÁXIMO	25
MÍNIMO	3
PROMEDIO	14

En resumen, los procesos que han sido seleccionados con este procedimiento bajo el criterio 2, relacionado con la alineación a los objetivos de Gobierno, más los procesos del dominio EDM Evaluar, Dirigir y Monitorear del criterio 1, son los siguientes:

Tabla 5: Procesos de TI seleccionados aplicando criterios 1 y 2

PROCESOS DE TI	OBJETIVOS DE TI																	
Evaluar, Dirigir y Monitorear	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	PUNTAJE
EDM01 Asegurar el establecimiento y mantenimiento de un marco de trabajo de Gobierno	5		5		1		5		1			1	1	1		1	1	22
EDM02 Asegurar la entrega de beneficios	5		1		5		5					1	1	1		1	5	25
EDM03 Asegurar la optimización de riesgos	1		1				1						1	1		1	1	7
EDM04 Asegurar la optimización de recursos	1		1		1		1		5				1			5	1	16
EDM05 Asegurar la transparencia de los interesados	1		5				5						1	1			1	14
Alinear, Planear y Organizar	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	
APO01 Gestionar el marco de trabajo de Administración de TI	5		1				1		5			1	1	1		5	5	25
APO02 Gestionar la Estrategia	5		1		1		5		1			1	1	1		1	5	22
APO07 Gestionar los Recursos Humanos	5		1				1		1				5			5	5	23
APO08 Gestionar las Relaciones	5		1		1		5					5	1			1	5	24
APO11 Gestionar la Calidad	1				5		5		1				5	1		1	1	20
Construir, Adquirir y Operar	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	
BAI02 Gestionar la Definición de Requerimientos	5		1		1		5		1			5	1	1			1	21
Entregar Servicio y Soporte	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	
Monitorear, Evaluar y Valorar	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	

Fuente: ISACA **Elaborado por**: Katalina Coronel Hoyos

Se puede observar la consistencia de los resultados obtenidos, ya que de los 4 dominios de Gestión o Administración, el de “Alinear, Planear y Organizar” es el que más soporte brinda al Gobierno de TI, mientras que los restantes son más operativos. Debido a ello, sus procesos APO01, APO02, APO07, APO08, APO11, así como el proceso BAI02 del dominio Construir, Adquirir y Operar, serán sumados a los 5 procesos del dominio EDM Evaluar, Dirigir y Monitorear, para ser seleccionados como parte de los elementos que servirán para evaluar el Gobierno, Riesgos y Cumplimiento de TI.

Para analizar el cumplimiento del criterio 3, que se refiere a que el proceso provea insumos para alguno de los procesos del dominio de Gobierno EDM Evaluar, Dirigir y Monitorear, se tomaron las prácticas clave de los 5 procesos del dominio de gobierno EDM (ver figuras 6 y 7) y se filtraron las entradas que utiliza cada una de ellas para generar sus salidas, así como los procesos de los dominios de Gestión que generan la información de dichas entradas para cada práctica clave de los procesos del dominio de Gobierno, resultando lo siguiente:

Tabla 6: Procesos de Gestión que generan entradas para los procesos de Gobierno

	Procesos del Dominio EDM Evaluar, Dirigir y Monitorear, con sus prácticas clave	**Procesos que generan Entradas para los procesos de Gobierno**
EDM01	Asegurar el establecimiento y mantenimiento de un marco de trabajo de Gobierno	
	EDM01.01 Evaluar el sistema de gobierno.	MEA03
	EDM01.02 Orientar el sistema de gobierno.	No tiene
	EDM01.03 Supervisar el sistema de gobierno.	MEA01, MEA0, MEA03
EDM02	Asegurar la entrega de beneficios	
	EDM02.01 Evaluar la optimización del valor.	APO02, APO05, BAI01
	EDM02.02 Orientar la optimización del valor.	No tiene
	EDM02.03 Supervisar la optimización del valor.	APO05
EDM03	Asegurar la optimización de riesgos	
	EDM03.01 Evaluar la gestión de riesgos.	APO12
	EDM03.02 Orientar la gestión de riesgos.	APO12
	EDM03.03 Supervisar la gestión de riesgos.	APO12
EDM04	Asegurar la optimización de recursos	
	EDM04.01 Evaluar la gestión de recursos.	APO02, APO07, APO10
	EDM04.02 Orientar la gestión de recursos.	No tiene
	EDM04.03 Supervisar la gestión de recursos.	No tiene
EDM05	Asegurar la transparencia de los interesados	
	EDM05.01 Evaluar los requisitos de elaboración de informes de las partes interesadas.	EDM02, EDM03, EDM04, MEA02
	EDM05.02 Orientar la comunicación con las partes interesadas y la elaboración de informes.	APO12
	EDM05.03 Supervisar la comunicación con las partes interesadas.	MEA02

Fuente: ISACA **Elaborado por**: Katalina Coronel Hoyos

Como se puede observar en la Tabla 6, los procesos de Gestión identificados como los generadores de información de entrada para los procesos del dominio de Gobierno son: APO02, APO05, APO07, APO10, APO12, BAI01, MEA01, MEA02 y MEA03. Esta condición que caracteriza a estos procesos, como proveedores de insumos para los procesos del dominio de Gobierno, pone de manifiesto su importancia, ya que una falla o insuficiencia en los mismos afectará a la ejecución de los procesos de Gobierno, razón por la que serán incluidos en la lista de procesos seleccionados que permitirán evaluar el Gobierno, Riesgos y Cumplimiento de TI, que es el objeto de esta metodología.

Por último, para el análisis del criterio 4, referente a los procesos que según la revista *Journal*, de ISACA, constituyen procesos de Gobierno[22], y considerando que ISACA es también la autora de COBIT 5, se examinaron los procesos que dicha revista señala como procesos de gobierno en COBIT 5, que son:

APO03 Administrar la arquitectura empresarial
APO04 Administrar la innovación
APO05 Administrar el portafolio
APO06 Administrar el presupuesto y los costos
APO08 Administrar las relaciones
APO13 Administrar la seguridad
BAI05 Administrar la habilitación del cambio organizacional
BAI08 Administrar el conocimiento
BAI09 Administrar los activos
DSS05 Administrar los servicios de seguridad
DSS06 Administrar los controles de procesos de negocio

En la revisión posterior de este artículo de la revista *Journal* en su versión web, se ha encontrado un comentario de que la afirmación de que éstos son procesos de gobierno en COBIT 5 es un error, ya que los mismos corresponden a los dominios de Administración. Sin embargo, tratándose de procesos que ha sido actualizados o nuevos respecto de la versión anterior de COBIT, y con el propósito de conocer si alguno de ellos presenta un alineamiento importante hacia los objetivos de TI que justifique incorporarlo entre los procesos seleccionados para la evaluación del Gobierno, Riesgos y Cumplimiento de TI, se analizó el puntaje obtenido por cada uno de ellos en el ejercicio de alineamiento que se practicó en la tabla 4.

[22] Larry Marks, "Governance Implementation – COBIT 5 and ISO", Journal, Volumen 1, 2013, ISACA, USA.

De este análisis, se concluyó que aquellos procesos que presentaron un puntaje de alineamiento superior al 60% del máximo obtenido por el resto de procesos, es decir 15 puntos o más, podrían ser considerados en la lista de procesos a ser seleccionados, mientras que los procesos con un puntaje menor fueron descartados bajo la perspectiva de que son procesos más operativos que de dirección, por lo que su ejecución no influye de manera importante en el sistema de gobierno.

Reuniendo todos estos elementos y resultados obtenidos, los procesos que quedarían seleccionados como los que más apoyan al gobierno de TI en COBIT 5, según los 4 criterios analizados, son los 22 siguientes:

Tabla 7: Procesos seleccionados para evaluar el Gobierno, Riesgos y Cumplimiento de TI

	Gobierno
	Evaluar, Dirigir and Monitorear
EDM01	Asegurar el establecimiento y mantenimiento de un marco de trabajo de Gobierno
EDM02	Asegurar la entrega de beneficios
EDM03	Asegurar la optimización de riesgos
EDM04	Asegurar la optimización de recursos
EDM05	Asegurar la transparencia de los interesados
	Administración
	Alinear, Planear y Organizar
APO01	Administrar el marco de trabajo de Administración de TI
APO02	Administrar la Estrategia
APO03	Administrar la Arquitectura Empresarial
APO04	Administrar la Innovación
APO05	Administrar el Portafolio
APO07	Administrar los Recursos Humanos
APO08	Administrar las Relaciones
APO10	Administrar los Proveedores
APO11	Administrar la Calidad
APO12	Administrar los Riesgos
	Construir, Adquirir y Operar
BAI01	Administrar Programas y Proyectos
BAI02	Administrar la Definición de Requerimientos
BAI05	Administrar la Habilitación del Cambio Organizacional
BAI08	Administrar el Conocimiento
	Entregar Servicio y Soporte
	Monitorear, Evaluar y Valorar
MEA01	Monitorear, Evaluar y Valorar el Desempeño y Conformidad
MEA02	Monitorear, Evaluar y Valorar el Sistema de Control Interno
MEA03	Monitorear, Evaluar y Valorar el Cumplimiento con Requerimientos Externos

Fuente: ISACA **Elaborado por**: Katalina Coronel Hoyos

Estos 22 procesos de COBIT 5, sumados a los elementos que se seleccionen en la siguiente sección, constituirán la base para realizar la evaluación del Gobierno, Riesgos y Cumplimiento de TI en una institución financiera, misma que se reflejará en la Matriz de Riesgos a elaborar en el Capítulo 4, como parte de esta metodología.

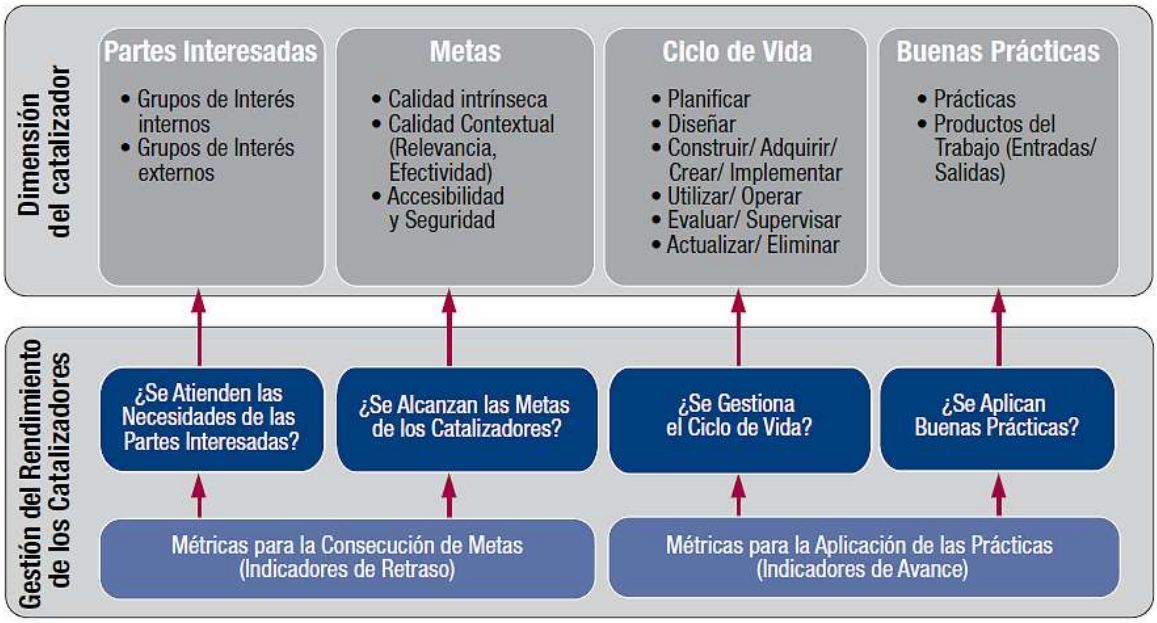
2.2. Estudio y selección de los habilitantes de COBIT 5 y sus dimensiones

Según se manifestó en el marco conceptual, los habilitantes o catalizadores de gobierno[23] son los recursos organizativos para el gobierno, tales como marcos de referencia, principios, estructuras, procesos y prácticas, a través de los que o hacia los que las acciones son dirigidas y los objetivos pueden ser alcanzados. Una falta de recursos o catalizadores puede afectar a la capacidad de la empresa de crear valor para sus interesados.

Debido a que los catalizadores o habilitantes están interconectados entre sí[24], es decir que cada habilitante necesita del resultado de otros habilitantes para ser completamente efectivo, una deficiencia en el desempeño de uno de ellos afectará a otro u otros, por lo que es necesario seleccionar a los 7 habilitantes para realizar una evaluación integral del Gobierno, Riesgos y Cumplimiento de TI.

Para este efecto, se utilizarán las dimensiones de los catalizadores, que existen de manera específica para cada uno de ellos, y cuyo modelo genérico es el que se muestra a continuación[25]:

Figura 12: Modelo genérico de los Catalizadores de COBIT 5



Fuente: ISACA **Elaborado por**: ISACA

[23] ISACA, *COBIT 5 Un Marco de Negocio para el Gobierno y la Gestión de la empresa*, USA, ISACA, 2012. Pág. 24.
[24] Ibídem, pág. 27.
[25] Ibídem, pág. 28.

Entre las herramientas que COBIT 5 provee para la implementación de un adecuado Gobierno corporativo de TI, no existe ninguna que oriente la forma de evaluar cada una de las dimensiones de los catalizadores (grupos de interés, metas, ciclo de vida y buenas prácticas), más allá de lo que se puede observar en la figura 12.

Con el objetivo de contar con una metodología clara y concreta para evaluar cada una de las dimensiones de los catalizadores, se elaboraron los cuestionarios que constan en el anexo C, los mismos que permitirán obtener una puntuación de la situación actual de cada uno de los catalizadores en la organización, lo cual a su vez servirá de línea base para priorizar y planificar iniciativas de mejora para cada uno de ellos.

Las preguntas que se han incluido en dichos cuestionarios han sido desarrolladas en base a la descripción detallada[26] que provee COBIT 5 para cada dimensión de los catalizadores, lo que asegura consistencia en la evaluación de todos los componentes analizados, así como el criterio técnico de la autora, el mismo que ha sido desarrollado en los varios años que tiene de experiencia en el campo de la Auditoría Informática en las instituciones financieras ecuatorianas.

Durante el desarrollo de los aspectos a ser evaluados en cada una de las dimensiones, se identificó la necesidad de establecer pesos que permitan obtener una calificación final que recoja la relevancia que tiene cada dimensión dentro del catalizador evaluado, ya que su correcta implementación o su falla afectará en mayor o menor medida a los objetivos del catalizador, dependiendo del impacto que en ellos tenga cada dimensión.

De esta manera, se determinó que las dimensiones “Grupos de interés” y “Metas”, impactan en menor medida en los objetivos de los catalizadores, mientras que las dimensiones “Ciclo de vida” y “Buenas prácticas” contribuyen en mayor medida al logro de los resultados esperados, ya que impactan en el diseño mismo del catalizador.

Por ejemplo, en el caso del catalizador “Principios, políticas y marcos de referencia”, es importante contar con metas como una forma de medición de los resultados de su aplicación; sin embargo, si en el ciclo de vida no está contemplada una etapa de evaluación de resultados, no se desarrollará tal actividad y por lo tanto no se podrán realizar mejoras, aunque las metas estén propuestas y formalizadas. Igualmente, si en la dimensión de Grupos de interés están identificadas las necesidades de todas las partes interesadas tanto internas como externas, pero no se aplica un ciclo de vida adecuado y apegado a buenas prácticas, no se lograrán los resultados que esperan esas partes interesadas.

[26] Ibídem, pág. 65

Con este enfoque, para el cálculo del puntaje total de cada catalizador se asignó un peso del 40% a las dimensiones “Grupos de interés” y “Metas”, por tratarse de indicadores de retraso (ver figura 12), y el 60% restante a las dimensiones “Ciclo de vida” y “Buenas prácticas”, por tratarse de indicadores de avance, con lo cual se suma un total de 100% en el puntaje.

El concepto de indicadores de retraso se refiere a que son aspectos cuya evaluación es posterior a la implementación del catalizador, y nos indica el retraso o las debilidades que se han presentado en su implementación; mientras que el concepto de indicadores de avance se refiere a los aspectos que nos indican durante la implementación, si se están logrando los resultados esperados para poder realizar oportunamente los correctivos que sean necesarios y que nos conduzcan al logro de los objetivos.

El peso asignado a los indicadores de retroceso y de avance se lo dividió a su vez en pesos individuales para cada una de las dimensiones, según la importancia de los aspectos a ser evaluados en cada dimensión, su grado de dificultad en la implementación, o su condición de ser requerimientos mínimos con que debería contar una institución financiera en el Ecuador.

De esta manera, se obtuvo la siguiente distribución de pesos, que servirá para calcular el puntaje total del catalizador a través de un promedio ponderado de las calificaciones de sus dimensiones:

Tabla 8: Pesos asignados a las dimensiones de los catalizadores

DIMENSIONES / CATALIZADORES	Grupos de interés	Metas	Ciclo de vida	Buenas prácticas
1. Principios, políticas y marcos de referencia	25%	15%	20%	40%
2. Procesos	20%	20%	25%	35%
3. Estructuras organizativas	15%	25%	30%	30%
4. Cultura, ética y comportamiento	15%	25%	20%	40%
5. Información	15%	25%	40%	20%
6. Servicios, Infraestructura y Aplicaciones	15%	25%	35%	25%
7. Personas, habilidades y competencias	15%	25%	35%	25%

Fuente: ISACA **Elaborado por**: Katalina Coronel Hoyos

Para calificar cada uno de los aspectos que constan en los cuestionarios de evaluación de los 7 catalizadores adjuntos en el anexo C, se sugiere utilizar valores porcentuales discretos, que sean múltiplos de 5, en un rango de valores entre 0% y 100%, tal como se muestra en el siguiente ejemplo genérico:

Tabla 9: Ejemplo de evaluación de un catalizador

Catalizador ABC		
Dimensión	**Aspectos a evaluar**	**Puntuación**
Grupos de interés	Aspecto 1	100
	Aspecto 2	25
15%	**PROMEDIO:**	**62.5**
Metas	Aspecto 3	85
	Aspecto 4	100
25%	**PROMEDIO:**	**92.50**
Ciclo de vida	Aspecto 5	85
	Aspecto 6	85
35%	**PROMEDIO:**	**85.00**
Buenas prácticas	Aspecto 7	50
	Aspecto 8	25
25%	**PROMEDIO:**	**37.50**
	PUNTAJE TOTAL:	**71.63**

Fuente: Tesis[27] **Elaborado por**: Katalina Coronel Hoyos

Una vez que se tiene la puntuación de cada aspecto evaluado, se calcula un promedio simple de todos los valores de una misma dimensión para obtener su promedio. Para calcular el puntaje total de la evaluación del catalizador, se multiplica el peso de cada dimensión por el promedio obtenido de todos sus aspectos evaluados, y al final se suman los 4 valores de las 4 dimensiones, con lo cual se consigue un promedio ponderado que se registra como “Puntaje total” del Catalizador.

Este mismo mecanismo debe ser aplicado para llenar los cuestionarios elaborados para cada uno de los catalizadores, cuyos puntajes totales se utilizarán en el Capítulo 4 para elaborar la matriz de riesgos resultante de la evaluación del Gobierno, Riesgos y Cumplimiento de TI, con todos los elementos seleccionados en este capítulo.

2.3. Estudio y selección de los elementos del modelo de evaluación de procesos de COBIT 5

Tal como se señaló en el Capítulo 1, la familia de productos de COBIT 5 incluye un modelo de evaluación de la capacidad de procesos, basado en la norma internacional ISO / IEC 15504 de Ingeniería de Software-Evaluación de Procesos. Este modelo permite evaluar el desempeño de cualquiera de los procesos del dominio de Gobierno (EDM Evaluar, Dirigir y Monitorear) o de los dominios de Gestión (ver figuras 6 y 7), a partir del cual se pueden identificar las posibles áreas de mejora.

[27] Ver la tabla 8.

Con el propósito de determinar otros elementos adicionales a los procesos y catalizadores seleccionados, que puedan contribuir con la evaluación del Gobierno, Riesgos y Cumplimiento de TI en las instituciones financieras ecuatorianas, se ha analizado el modelo de evaluación de capacidad de procesos de COBIT 5, mismo que cuenta con 6 niveles de capacidad que puede alcanzar un proceso, en cada uno de los cuales se determina si el proceso tiene los siguientes atributos:

Tabla 10: Niveles de capacidad de los procesos

NIVEL DE CAPACIDAD	ATRIBUTOS A ALCANZAR
0. **Proceso incompleto**: El proceso no está implementado o no alcanza su propósito. A este nivel, hay muy poca o ninguna evidencia de ningún logro sistemático del propósito del proceso.	
1. **Proceso ejecutado** (1 atributo): El proceso alcanza su propósito.	PA 1.1 Rendimiento del Proceso
2. **Proceso gestionado** (2 atributos): El proceso está ya implementado de forma gestionada (planificado, supervisado y ajustado) y los resultados de su ejecución están establecidos, controlados y mantenidos apropiadamente.	PA 2.1 Gestión del Rendimiento PA 2.2 Gestión del Resultado del trabajo
3. **Proceso establecido** (2 atributos): El proceso gestionado está ahora implementado usando un proceso definido que es capaz de alcanzar sus resultados de proceso.	PA 3.1 Definición de Procesos PA 3.2 Despliegue de Procesos
4. **Proceso predecible** (2 atributos): El proceso establecido ahora se ejecuta dentro de límites definidos para alcanzar sus resultados de proceso.	PA 4.1 Gestión de Procesos PA 4.2 Control de Procesos
5. **Proceso optimizado** (2 atributos) – El proceso predecible es mejorado de forma continua para cumplir con metas empresariales presentes y futuras.	PA 5.1 Innovación de Procesos PA 5.2 Optimización de Procesos

Fuente: ISACA **Elaborado por**: Katalina Coronel Hoyos

La evaluación que se efectúa con el modelo de capacidad de los procesos de COBIT 5 distingue diferentes procedimientos para evaluar el nivel 1 de capacidad y los niveles superiores.

El nivel 1 de capacidad de procesos describe si un proceso alcanza su objetivo establecido, y por lo tanto es un nivel muy importante a alcanzar, no solamente como la base para hacer alcanzables los niveles de capacidad superiores, sino que el nivel 1 requiere que el atributo de rendimiento sea alcanzado totalmente, lo que significa que el proceso se ejecuta con éxito y la organización obtiene los resultados esperados. Posterior a esto, los niveles de capacidad superiores añaden diferentes atributos al proceso. En este esquema de evaluación, alcanzar un nivel 1 de capacidad, incluso en una escala de 5, es un logro importante para la organización[28].

[28] Ibídem, pág. 43.

Para la evaluación de los niveles de capacidad superiores a 1 se evalúan prácticas genéricas y productos del trabajo genéricos para todos los procesos, mientras que para la evaluación del nivel 1 se evalúan las metas de cada proceso, sus prácticas clave de gobierno específicas y sus entradas y salidas, definidas en el modelo de referencia de procesos de COBIT 5.

Para analizar si un proceso alcanza el nivel de capacidad 1, es necesario utilizar los siguientes indicadores que establece el modelo de capacidad de procesos de COBIT 5[29]:

1. Indicadores de atributo de capacidad del proceso. Para el nivel 1, solo existe 1 indicador genérico de capacidad (PA 1.1) y mide la extensión hasta la cual se alcanza el propósito (metas u objetivos) del proceso. De acuerdo con los ratios establecidos por la norma ISO / IEC 15504, se debe alcanzar un ratio "F" (full o totalmente logrado) para cumplir con el nivel de capacidad establecido, tal como se observa en la siguiente tabla[30]:

Tabla 11: Criterios de evaluación de desempeño de un proceso

Resultado del Logro Total del atributo	Prácticas base (BPs)	Productos de trabajo (WPs)
El proceso alcanza sus metas definidas	BP 1.1.1 Alcanza las metas del proceso. Hay evidencia de que la intención de las prácticas base está siendo ejecutada.	Los productos de trabajo son producidos y proveen evidencia de las metas del proceso, como está definido en la sección 3.0.

Fuente: ISACA **Elaborado por**: Katalina Coronel Hoyos

2. Indicadores de desempeño del proceso. Los constituyen las prácticas base (prácticas clave) y los productos de trabajo (entradas y salidas) de cada proceso, según el modelo de referencia de procesos de COBIT 5, sobre los cuales debe existir evidencia de cumplimiento total (ratio "F").

Debido a la importancia relevante que se observa en que un proceso alcance el nivel 1 de capacidad, mientras que el resto de niveles toman esta base para añadir diferentes atributos al proceso, para efectos de evaluar el Gobierno, Riesgos y Cumplimiento de TI se utilizará únicamente la evaluación del nivel de capacidad 1 de cada proceso, la misma que será parte de la evaluación de los procesos seleccionados.

Con este componente se completa la selección de los elementos de COBIT 5 a ser evaluados, los mismos que se resumen en la siguiente tabla:

[29] ISACA, *Process Assessment Model (PAM): Using COBIT 5*, USA, ISACA, 2013. Pág. 14.
[30] Ibídem, pág. 115.

Tabla 12: Elementos de COBIT 5 seleccionados

22 Procesos de COBIT 5			CAPACIDAD			
1	EDM01	Asegurar el establecimiento y mantenimiento de un marco de trabajo de Gobierno	Atributo de capacidad del proceso	Prácticas base	Productos de trabajo	Evaluación de catalizador
2	EDM02	Asegurar la entrega de beneficios				
3	EDM03	Asegurar la optimización de riesgos				
4	EDM04	Asegurar la optimización de recursos				
5	EDM05	Asegurar la transparencia de los interesados				
6	APO01	Administrar el marco de trabajo de Administración de TI				
7	APO02	Administrar la Estrategia				
8	APO03	Administrar la Arquitectura Empresarial				
9	APO04	Administrar la Innovación				
10	APO05	Administrar el Portafolio				
11	APO07	Administrar los Recursos Humanos				
12	APO08	Administrar las Relaciones				
13	APO10	Administrar los Proveedores				
14	APO11	Administrar la Calidad				
15	APO12	Administrar los Riesgos				
16	BAI01	Administrar Programas y Proyectos				
17	BAI02	Administrar la Definición de Requerimientos				
18	BAI05	Administrar la Habilitación del Cambio Organizacional				
19	BAI08	Administrar el Conocimiento				
20	MEA01	Monitorear, Evaluar y Valorar el Desempeño y Conformidad				
21	MEA02	Monitorear, Evaluar y Valorar el Sistema de Control Interno				
22	MEA03	Monitorear, Evaluar y Valorar el Cumplimiento con Requerimientos Externos				
7 CATALIZADORES			DIMENSIONES			
1		Principios, políticas y marcos de referencia	Grupos de interés	Metas	Ciclo de vida	Buenas prácticas
2		Procesos				
3		Estructuras organizativas				
4		Cultura, ética y comportamiento				
5		Información				
6		Servicios, infraestructuras y aplicaciones				
7		Personas, habilidades y competencias				

Fuente: Tesis[31] **Elaborado por**: Katalina Coronel Hoyos

Como se puede apreciar en la tabla anterior, se han seleccionado 22 procesos con su evaluación de atributos de capacidad, prácticas clave y productos de trabajo; los 7 catalizadores, y la evaluación de sus 4 dimensiones. Estos elementos serán trasladados

[31] Ver las tablas 7, 8 y 11.

a una matriz de riesgos en el Capítulo 4, en la que se reflejará la situación del Gobierno, Riesgos y Cumplimiento de TI con todos estos componentes.

2.4. Determinación de las variables y escala de los niveles de riesgo a utilizar en la calificación de los elementos seleccionados

En los numerales previos de este capítulo se analizaron los elementos de COBIT 5 que inciden de manera más significativa en el Gobierno de TI, y se seleccionaron:

- 22 procesos del modelo de referencia de procesos
- 7 cuestionarios para evaluar las 4 dimensiones de los 7 catalizadores
- Evaluación del nivel 1 de capacidad de los procesos, con 3 indicadores: atributo de capacidad del proceso (metas), prácticas clave y productos del trabajo

De acuerdo con esta selección, se deberán evaluar los 22 procesos seleccionados y los 7 catalizadores de COBIT 5. Debido a que los procesos también constituyen 1 de los 7 catalizadores de COBIT 5, para la evaluación de los procesos se considerará un puntaje que reúna las calificaciones parciales obtenidas tanto en el modelo de capacidad de procesos, como la evaluación de cada proceso desde el punto de vista de catalizador. Los puntajes obtenidos para estos elementos se deberán registrar en la siguiente matriz:

Tabla 13: Matriz de evaluación de los elementos seleccionados

No.		Gobierno / Evaluar, Dirigir and Monitorear	Atributo de capacidad del proceso	Prácticas base	Productos de trabajo	Evaluación de catalizador	Promedio
1	EDM01	Asegurar el establecimiento y mantenimiento de un marco de trabajo de Gobierno					
2	EDM02	Asegurar la entrega de beneficios					
3	EDM03	Asegurar la optimización de riesgos					
4	EDM04	Asegurar la optimización de recursos					
5	EDM05	Asegurar la transparencia de los interesados					
		Administración					
		Alinear, Planear y Organizar					
6	APO01	Administrar el marco de trabajo de Administración de TI					
7	APO02	Administrar la Estrategia					
8	APO03	Administrar la Arquitectura Empresarial					
9	APO04	Administrar la Innovación					
10	APO05	Administrar el Portafolio					
11	APO07	Administrar los Recursos Humanos					
12	APO08	Administrar las Relaciones					
13	APO10	Administrar los Proveedores					
14	APO11	Administrar la Calidad					
15	APO12	Administrar los Riesgos					
		Construir, Adquirir y Operar					
16	BAI01	Administrar Programas y Proyectos					
17	BAI02	Administrar la Definición de Requerimientos					
18	BAI05	Administrar la Habilitación del Cambio Organizacional					
19	BAI08	Administrar el Conocimiento					
		Entregar Servicio y Soporte					
		Monitorear, Evaluar y Valorar					
20	MEA01	Monitorear, Evaluar y Valorar el Desempeño y Conformidad					
21	MEA02	Monitorear, Evaluar y Valorar el Sistema de Control Interno					
22	MEA03	Monitorear, Evaluar y Valorar el Cumplimiento con Requerimientos Externos					
		Catalizadores	**Grupos de interés**	**Metas**	**Ciclo de vida**	**Buenas prácticas**	**Promedio**
23	CAT1	Principios, políticas y marcos de referencia					
24	CAT2	Procesos					
25	CAT3	Estructuras organizativas					
26	CAT4	Cultura, ética y comportamiento					
27	CAT5	Información					
28	CAT6	Servicios, infraestructuras y aplicaciones					
29	CAT7	Personas, habilidades y competencias					

Fuente: Tesis[32] **Elaborado por**: Katalina Coronel Hoyos

En esta matriz, para la evaluación del atributo de capacidad del proceso, se determinará si el proceso cumple con las metas establecidas por COBIT 5 en su marco de referencia de procesos, con valores porcentuales correspondientes a los deciles: 0%, 10%, 20%, 30%, 40%, 50%, 60%, 70%, 80%, 90% y 100% para cada meta, y luego se obtiene un promedio simple, el cual se registrará en esta matriz.

Una evaluación similar sobre 100% se realizará para determinar el cumplimiento de las prácticas base de cada proceso, y posteriormente se obtendrá un promedio simple para registrarlo en esta matriz en la columna “Prácticas base” de cada proceso.

En cuanto a los productos de trabajo se procederá de manera similar: por cada práctica base se identificará el número de productos de trabajo (salidas) que se generan efectivamente, frente al total de productos de trabajo sugeridos por COBIT 5 para dicha práctica, y luego se obtiene un promedio simple de todas las prácticas base del proceso, para ubicarlo en esta matriz.

[32] Ver la tabla 12.

Para la evaluación de los 7 catalizadores, los cuestionarios desarrollados en el anexo C permitirán definir un valor porcentual para cada una de sus dimensiones, obteniendo al final un promedio ponderado para determinar el Puntaje Total del catalizador. En el caso de los 22 procesos seleccionados, se deberá llenar el cuestionario correspondiente al catalizador "Procesos" para cada uno de ellos, y su puntaje se registrará en esta matriz bajo la columna "Evaluación de catalizador".

Una vez que se cuenta con los 4 puntajes requeridos en esta matriz para cada proceso, se obtiene un promedio simple para obtener un puntaje total para cada proceso. Posteriormente, será necesario homologar el puntaje obtenido por cada uno de los procesos, con los ratios del modelo de evaluación de capacidad de procesos, los cuales permitirán determinar el nivel de logro alcanzado por el proceso.

Este mismo ratio puede ser utilizado en la evaluación del resto de catalizadores, haciendo una homologación del puntaje alcanzado en cada una de sus dimensiones con la escala de 0% a 100% hacia los ratios N, P, L, F, lo que reflejará a su vez la gestión de su rendimiento en los indicadores de avance y de retraso.

Para graficar el ratio obtenido en cada elemento evaluado, se puede asociar un color según el nivel de logro, tal como se muestra a continuación:

Tabla 14: Ratios del modelo de evaluación de capacidad de procesos

PUNTAJE	RATIO	COLOR
0 a 15%	**N** (No alcanzado)	Rojo
>15% a 50%	**P** (Logrado parcialmente)	Naranja
>50% a 85%	**L** (logrado en gran medida)	Amarillo
>85% a 100%	**F** (Totalmente logrado)	Verde

Fuente: Tesis[33] **Elaborado por**: Katalina Coronel Hoyos

Como se puede apreciar, los colores verde, amarillo, naranja y rojo, permiten identificar el nivel de riesgo en el logro de los resultados de un elemento evaluado. A mayor logro, menor será el riesgo, ya que se están obteniendo los resultados esperados, tanto en los procesos como en los catalizadores de COBIT 5, los cuales tienen un enfoque holístico respecto del negocio. Si no se obtienen los resultados esperados, entonces se pone en riesgo el logro de los objetivos institucionales y por ende, la creación de valor que busca toda organización para cada una de sus partes interesadas, lo cual es parte fundamental del Gobierno Corporativo.

La determinación del riesgo en el logro de los objetivos, permite enfocar de manera eficiente los esfuerzos y el uso de los recursos para gestionar adecuadamente los riesgos

[33] Ver la tabla 1.

al priorizar las iniciativas de mejora. La cultura de gestión de riesgos constituye el segundo elemento dentro del esquema GRC que se pretende evaluar con este trabajo, tanto dentro de los procesos de Optimización y Gestión de Riesgos, como en el habilitante de Cultura, ética y comportamiento.

Para obtener una calificación total del Gobierno, Riesgos y Cumplimiento de TI a partir del puntaje de los 29 elementos evaluados, se puede determinar pesos para cada uno de estos elementos, ya que no todos tienen la misma influencia y por lo tanto la calificación total no podría ser calculada con un promedio simple.

Para este efecto, en el siguiente capítulo se realizará el mapeo de los procesos de COBIT 5 frente a las normas de la Superintendencia de Bancos y Seguros sobre Gestión del Riesgo Operativo y de Seguridades Mínimas, y su relación con la norma ISO/IEC 27005. Este mapeo con las normas de la SBS permite afianzar el factor de Cumplimiento en la evaluación, ya que determinan el nivel de implementación de controles adecuados en los procesos relacionados con la tecnología de la información, que son exigibles a través de regulaciones externas.

CAPÍTULO 3 - ANÁLISIS COMPARATIVO DE LOS REQUERIMIENTOS DE COBIT 5, LA NORMATIVA DE LA SBS Y EL ESTÁNDAR ISO/IEC 27005

Con el fin de incluir en la evaluación de este trabajo el factor de Cumplimiento, se analizó cuáles de los elementos de COBIT 5 seleccionados en el Capítulo 2 constituyen una obligación de cumplimiento para las instituciones financieras ecuatorianas, al estar requeridos por la normativa de la Superintendencia de Bancos y Seguros (SBS), así como por el estándar internacional ISO/IEC 27005. Para este efecto, se realizó el mapeo entre ellos, con el fin de asignarles un peso diferenciado en la evaluación del Gobierno, Riesgos y Cumplimiento de TI a aquellos puntos comunes encontrados, que constituyen elementos de cumplimiento obligatorio.

3.1. Mapeo de los requerimientos de la norma de Gestión del Riesgo Operativo de la SBS y las prácticas clave de COBIT 5

Como se explicó en la sección 1.2 del Capítulo 1, la norma de Gestión del Riesgo Operativo incluye requerimientos sobre Procesos, Personas y Tecnología de Información para las instituciones financieras, razón por la cual se incorporó en esta metodología el mapeo entre los requerimientos de la norma de Gestión del Riesgo Operativo de la SBS, y los procesos y prácticas clave de COBIT 5. En el mapeo realizado con esta norma se realizaron 106 comparaciones, las cuales se pueden visualizar de manera completa en el anexo D.

En la realización de este ejercicio, se observó que la mayor cantidad de requerimientos normativos se enfocan principalmente en controles de seguridad de la información (44), gestión de proveedores (11), continuidad del negocio (10) y gestión de recursos humanos (9), de cuyo total existe una coincidencia con 11 de los procesos de COBIT 5 que fueron seleccionados en el Capítulo 2 (ver la tabla 12) para la evaluación del Gobierno, Riesgos y Cumplimiento de TI en una institución financiera, y son los siguientes:

Tabla 15: Procesos seleccionados coincidentes con la norma de Gestión del Riesgo Operativo

EDM01	Asegurar el establecimiento y mantenimiento de un marco de trabajo de Gobierno
EDM03	Asegurar la optimización de riesgos
APO01	Administrar el marco de trabajo de Administración de TI
APO02	Administrar la Estrategia
APO07	Administrar los Recursos Humanos
APO10	Administrar los Proveedores

APO12	Administrar los Riesgos
BAI02	Administrar la Definición de Requerimientos
BAI05	Administrar la Habilitación del Cambio Organizacional
MEA01	Monitorear, Evaluar y Valorar el Desempeño y Conformidad
MEA03	Monitorear, Evaluar y Valorar el Cumplimiento con Requerimientos Externos

Fuente: Tesis[34] **Elaborado por**: Katalina Coronel Hoyos

Al ser estos 11 procesos requeridos por la norma de Gestión del Riesgo Operativo de forma obligatoria para las instituciones financieras, su incumplimiento o una débil implementación de los mismos generarán más riesgos a las entidades, por lo que en la evaluación del Gobierno, Riesgos y Cumplimiento de TI se les asignará un peso diferenciado para el cálculo del puntaje total por proceso, el cual se determinará en la sección 3.4 del Capítulo 3.

3.2. Mapeo de los requerimientos de la norma de Medidas de Seguridad de la SBS frente a las prácticas clave de COBIT 5 y el estándar ISO/IEC 27005

En el ejercicio de mapeo de la norma de seguridades mínimas de la SBS, cuyo contenido se encuentra en el anexo E, se determinó la existencia de controles puntuales y específicos que deben implementar las instituciones financieras en sus políticas y procedimientos, personal, bóvedas y cajas fuertes, instalaciones, cajeros automáticos, y transporte de valores. De esta norma, se realizaron 62 comparaciones con los procesos y prácticas clave de COBIT 5, entre los cuales destacan la gestión de controles de procesos de negocio (29), administración de operaciones (11), y administración de seguridades (13).

De estos procesos, los que coinciden con los seleccionados para la evaluación del Gobierno, Riesgos y Cumplimiento de TI en una institución financiera, son los 5 siguientes, de los cuales 4 coinciden con los mapeados en la norma de Riesgo Operativo:

Tabla 16: Procesos seleccionados coincidentes con la norma de Medidas de Seguridad

		Riesgo Operativo	Medidas de Seguridad
APO07	Administrar los Recursos Humanos	X	X
APO10	Administrar los Proveedores	X	X
BAI05	Administrar la Habilitación del Cambio Organizacional		X
BAI08	Administrar el Conocimiento	X	X
MEA03	Monitorear, Evaluar y Valorar el Cumplimiento con Requerimientos Externos	X	X

Fuente: Tesis[35] **Elaborado por**: Katalina Coronel Hoyos

[34] Ver la tabla 12 y el anexo D.

De los mapeos efectuados con las dos normativas de la SBS, se puede apreciar que la implementación de los 12 procesos mapeados con COBIT 5, genera obligación regulatoria para las instituciones financieras, y su incumplimiento puede acarrear sanciones y multas, además de problemas operativos o de gobierno al interior de la organización. Al mismo tiempo, estos 12 procesos constituyen buenas prácticas internacionales cuya adecuada implementación permitirá mitigar posibles riesgos y principalmente, contribuir al logro de los objetivos de negocio.

Por esta razón, estos procesos no pueden tener el mismo tratamiento dentro del esquema de evaluación del Gobierno, Riesgos y Cumplimiento de TI, sino que se les debe asignar un peso diferente para obtener su puntuación total, que refleje esta condición de presentar un riesgo mayor para las instituciones.

Con el propósito de complementar el análisis de cumplimiento normativo exigible para las instituciones financieras, se realizó el mapeo con la norma ISO/IEC 27005 (ver anexo F), cuyos resultados revelan que las actividades de dicha norma que son requeridas en la norma de seguridades mínimas de la SBS son las siguientes, junto con el proceso de COBIT 5 equivalente:

Tabla 17: Mapeo de la norma ISO/IEC 27005 con COBIT 5

Cod.	Actividad Norma ISO 27005	Proceso	Práctica clave COBIT 5
7.22	Criterios básicos - Criterios de evaluación del riesgo	**EDM03**	EDM03.02 Orientar la gestión de riesgos.
7.23	Criterios básicos - Criterios de aceptación del riesgo	**EDM03**	EDM03.02 Orientar la gestión de riesgos.
8.2.1.3	Identificación de amenazas	**APO12**	APO12.01 Recopilar datos.
8.2.1.4	Identificación de controles existentes	**APO12**	APO12.02 Analizar el riesgo.
8.2.1.5	Identificación de vulnerabilidades	**APO12**	APO12.02 Analizar el riesgo.
9.1	Descripción general del tratamiento de riesgos	**APO12**	APO12.05 Definir un portafolio de acciones para la gestión de riesgos.
9.2	Reducción del riesgo	**APO12**	APO12.06 Responder al riesgo.
9.5	Transferencia del riesgo	**APO12**	APO12.06 Responder al riesgo.

Fuente: ISO/IEC 2008 e ISACA **Elaborado por**: Katalina Coronel Hoyos

Los procesos de COBIT 5 que son requeridos en la norma ISO/IEC 27005 “Gestión de riesgos de seguridad de la información” son aquellos relacionados con la Gestión de riesgos: el proceso de gobierno EDM03 “Asegurar la optimización de riesgos” y el proceso del dominio de gestión APO12 “Administrar los riesgos”. Estos 2 procesos ya fueron incluidos en la lista de elementos de COBIT 5 seleccionados en el Capítulo 2 para la evaluación del Gobierno, Riesgos y Cumplimiento de TI, por lo que no existe mayor

[35] Ver la tabla 15 y el anexo E.

aporte de la norma ISO/IEC 27005 al desarrollo de esta metodología. En este sentido, no se considera necesario asignar un puntaje diferente a estos dos procesos por el hecho de estar mapeados con la norma internacional.

3.3. Diseño y aplicación de encuestas a varias instituciones financieras sobre sus debilidades en el Gobierno de TI

Con el fin de conocer la generalidad de debilidades existentes en las instituciones financieras respecto de los 29 elementos seleccionados para la evaluación del Gobierno, Riesgos y Cumplimiento de TI, se diseñó el cuestionario que se encuentra en el anexo G, basado en las metas de los 22 procesos y los 7 catalizadores de COBIT 5 que fueron seleccionados en el Capítulo 2.

Para el desarrollo de las preguntas, se revisó la redacción de las metas de los procesos establecidas por COBIT 5 en su modelo de referencia de procesos, y se las puso en formato de afirmación como una buena práctica, seleccionando aquellas que describen de la manera más clara posible el objetivo de cada proceso.

En cuanto al nivel de aplicación de cada buena práctica, no se utilizó la escala de 0 a 5 del nivel de madurez de la versión 4.1 de COBIT, ya que podría confundirse el objetivo del cuestionario con una evaluación de la madurez de los procesos; en su lugar se adoptó en una escala de 0 a 7, basada en el modelo establecido en el artículo "IT Governance and Business-IT Alignment in SMEs"[36], de la Revista Journal, considerando para ello las siguientes descripciones:

0 La administración no está consciente de esta buena práctica
1 La administración está consciente pero no tiene voluntad para implementarla
2 La voluntad para implementar la buena práctica existe, pero no se ha planificado
3 Se ha planificado e iniciado la implementación
4 La implementación está avanzando conforme se planificó
5 La buena práctica está implementada y se reciben los beneficios esperados
6 Se miden los resultados para conocer desviaciones y se las gestiona
7 Su ejecución está optimizada, de forma sistematizada

Además de las preguntas de evaluación, se introdujeron variables demográficas para conocer el tipo de bienes o servicios que ofrece la organización, y su tamaño medido en

[36] Steven De Haes, Rogier Haest, Wim Van Grembergen, "IT Governance and Business-IT Alignment in SMEs", Journal, Volumen 6, 2010, ISACA, USA

activos. Se incluyó la variable de "impacto" que tiene cada elemento en el negocio, lo cual permite identificar las mayores o menores consecuencias que tenga una falla o una implementación inadecuada de dicho elemento, en el negocio.

Los resultados de la aplicación de este cuestionario servirán, por una parte, para determinar la validez de las preguntas respecto de los elementos que se busca evaluar, y por otro lado, pueden ser útiles como insumo para la identificación del impacto de cada elemento evaluado, sea éste alto, medio o bajo en el negocio, que a su vez definirá su nivel de riesgo en la matriz de evaluación[37].

En las respuestas obtenidas al llenar el cuestionario, es importante notar que la selección del nivel de aplicación de las buenas prácticas no siempre corresponde a la realidad de la institución evaluada, ya que las respuestas serán influidas por el tipo de involucramiento en la organización que tiene la persona que llena el cuestionario. Por ejemplo, dentro de una institución, se podrá obtener diferentes resultados dependiendo si el cuestionario es llenado por el Jefe de Sistemas, por un delegado de un área de negocio, o por el Auditor Interno.

Para mitigar posibles inconsistencias de este tipo, es importante conseguir que los cuestionarios sean llenados por al menos 2 personas de áreas diferentes de una misma institución, con el fin de validar los resultados por comparación cruzada. En este caso, el resultado a considerar válido debe ser aquel que presente la menor evaluación, pues se la considera en general más conservadora.

3.4. Definición de los pesos a asignar a los elementos de COBIT 5 que viabilizan el cumplimiento regulatorio de la SBS

De acuerdo con el mapeo realizado en los numerales anteriores, de los 22 procesos seleccionados para la evaluación, 12 constituyen requerimientos normativos de la Superintendencia de Bancos y Seguros (SBS), por lo que su incumplimiento generará mayor riesgo a la institución, así como posibles sanciones y multas que ello pueda acarrear. En cuanto a los catalizadores a ser evaluados, 6 de los 7 catalizadores de COBIT 5 son requeridos en diferentes normativas de la SBS, por lo que una implementación inadecuada o deficiente en los mismos también ocasionará un incumplimiento normativo, así como un menor desempeño organizacional.

A continuación se muestra un listado de las normas de la Codificación de Resoluciones de la Superintendencia de Bancos y Seguros y de la Junta Bancaria (CRSBSYJB), que en su libro 1 referencia o realiza requerimientos directos sobre cada

[37] Ver Capítulo 4, sección 4.1.

uno de los catalizadores de COBIT 5, aunque pueden existir más requerimientos en otras normativas particulares de la SBS que en esta tesis no se mencionan:

Tabla 18: Requerimientos de la CRSBSYJB relacionados con los catalizadores

CATALIZADOR	NORMATIVA PRINCIPAL DE SBS QUE LO REFERENCIA
1. Principios, políticas y marcos de referencia	Gestión Integral de Riesgos, Gestión del riesgo operativo, Del Control Interno, Principios de un Buen Gobierno Corporativo, Prevención de Lavado de Activos, entre otras.
2. Procesos	Gestión del riesgo operativo
3. Estructuras organizativas	
4. Cultura, ética y comportamiento	Prevención de Lavado de Activos, Principios de un Buen Gobierno Corporativo
5. Información	De la información y publicidad, De la Contabilidad, Medidas mínimas de seguridad (Apertura de oficinas), Transparencia y Derechos del usuario financiero
6. Servicios, infraestructuras y aplicaciones	Gestión del riesgo operativo
7. Personas, habilidades y competencias	Gestión del riesgo operativo, Del Control Interno, Del Gobierno y de la Administración

Fuente: Codificación de Resoluciones de la SBS y de la Junta Bancaria

Elaborado por: Katalina Coronel Hoyos

Debido las exigencias normativas que se presentan en 18 de los 29 elementos a evaluar, se ha visto necesario realizar una diferenciación en el peso a ser asignado a cada elemento antes de ser ubicado en la matriz de riesgo, ya que una asignación del puntaje total por igual a todos los elementos evaluados, impedirá reflejar la exigencia adicional existente en dichos elementos.

Para este efecto, se plantea la premisa de que el 80% de los procesos de tecnología y catalizadores de gobierno de una institución financiera ecuatoriana cumplen apenas con un 20% de los requerimientos normativos vigentes, mientras que el 20% de ellos los cumplen en un 80%.

Para aplicar esta premisa en la asignación de pesos de la evaluación de procesos y catalizadores, se considera necesario restar un 20% al puntaje obtenido en la evaluación de cada elemento seleccionado, siempre y cuando el elemento sea requerido en la normativa de la SBS, caso contrario se toma la totalidad del puntaje. Un ejemplo de esta aplicación se muestra en la siguiente tabla:

Tabla 19: Mecanismo de asignación de pesos a elementos requeridos en normativa

No.	Gobierno	Evaluar, Dirigir and Monitorear	Promedio	Req. Normativo	Puntaje
1	EDM01	Asegurar el establecimiento y mantenimiento de un marco de trabajo de Gobierno	74%	SI	59%
2	EDM02	Asegurar la entrega de beneficios	85%		85%

Fuente: Tesis[38] **Elaborado por**: Katalina Coronel Hoyos

Al reducir un 20% de su promedio para obtener el puntaje total, se logra que los elementos requeridos por la normativa de la SBS presenten un mayor riesgo en la matriz de riesgos, y ello obligue a la institución financiera a realizar una revisión más detallada de su cumplimiento normativo. La introducción de este cálculo en la tabla 13, origina la siguiente tabla:

Tabla 20: Matriz de evaluación de elementos seleccionados

	Gobierno	Atributo de capacidad del proceso	Prácticas base	Productos de trabajo	Evaluación de catalizador	Promedio	Req. Normativo	Puntaje
	Evaluar, Dirigir and Monitorear							
EDM01	Asegurar el establecimiento y mantenimiento de un marco de trabajo de Gobierno						SI	
EDM02	Asegurar la entrega de beneficios							
EDM03	Asegurar la optimización de riesgos						SI	
EDM04	Asegurar la optimización de recursos							
EDM05	Asegurar la transparencia de los interesados							
	Administración							
	Alinear, Planear y Organizar							
APO01	Administrar el marco de trabajo de Administración de TI						SI	
APO02	Administrar la Estrategia						SI	
APO03	Administrar la Arquitectura Empresarial							
APO04	Administrar la Innovación							
APO05	Administrar el Portafolio							
APO07	Administrar los Recursos Humanos						SI	
APO08	Administrar las Relaciones							
APO10	Administrar los Proveedores						SI	
APO11	Administrar la Calidad							
APO12	Administrar los Riesgos						SI	
	Construir, Adquirir y Operar							
BAI01	Administrar Programas y Proyectos							
BAI02	Administrar la Definición de Requerimientos						SI	
BAI05	Administrar la Habilitación del Cambio Organizacional						SI	
BAI08	Administrar el Conocimiento						SI	
	Entregar Servicio y Soporte							
	Monitorear, Evaluar y Valorar							
MEA01	Monitorear, Evaluar y Valorar el Desempeño y Conformidad						SI	
MEA02	Monitorear, Evaluar y Valorar el Sistema de Control Interno							
MEA03	Monitorear, Evaluar y Valorar el Cumplimiento con Requerimientos Externos						SI	
	Catalizadores	**Grupos de interés**	**Metas**	**Ciclo de vida**	**Buenas prácticas**	**Promedio**	**Req. Normativo**	**Puntaje**
CAT1	Principios, políticas y marcos de referencia						SI	
CAT2	Procesos						SI	
CAT3	Estructuras organizativas							
CAT4	Cultura, ética y comportamiento						SI	
CAT5	Información						SI	
CAT6	Servicios, infraestructuras y aplicaciones						SI	
CAT7	Personas, habilidades y competencias						SI	

Fuente: Tesis[39] **Elaborado por**: Katalina Coronel Hoyos

Con esta diferenciación de pesos, se visibiliza en esta metodología el factor de Cumplimiento, que complementa la evaluación conjunta del Gobierno y Riesgos de TI en una institución financiera ecuatoriana.

[38] Ver la tabla 13.
[39] Ver la tabla 13.

CAPÍTULO 4 - GENERACIÓN DE LA MATRIZ DE RIESGOS DE GOBIERNO DE TI Y MEDIDAS A ADOPTAR

Como se dijo en el capítulo anterior, la identificación y gestión de riesgos es una herramienta sumamente útil para conocer las áreas en las que no se están logrando los resultados esperados, para priorizar las iniciativas de mejora, y por tanto, para enfocar de manera más eficiente los esfuerzos y el uso de los recursos hacia el logro de los objetivos institucionales. Por ello, es importante determinar las áreas en las que se presentan las mayores debilidades del esquema de Gobierno de TI para poder identificar su causa y la forma de solventarlas de la manera más eficiente.

En esta metodología se ha desarrollado una matriz que permite visualizar de forma ejecutiva, cada uno de los aspectos más relevantes del Gobierno de TI y su estado de riesgo, desde el punto de vista del logro de los objetivos, con el fin de orientar los esfuerzos hacia su mejora continua, basándose para ello en las mejores prácticas sugeridas por el marco de trabajo de COBIT 5.

4.1. Desarrollo de la Matriz de Riesgos calórica con los elementos evaluados y su nivel de riesgo

La matriz que se ha diseñado para mostrar los resultados de la evaluación de los 29 elementos seleccionados, responde a una típica matriz de riesgos en la que, en un eje se muestra la probabilidad de ocurrencia de los eventos, y en otro se muestra el impacto o costos de sus consecuencias.

Con los resultados obtenidos en los Capítulos 2 y 3 de esta metodología[40], se cuenta con una calificación o puntaje porcentual de los 29 elementos seleccionados, la cual representa el porcentaje de logro de los resultados esperados para cada uno de los elementos en la organización.

Si se obtiene la diferencia entre 100% y la calificación obtenida en la tabla 20, tendremos un porcentaje que representa las debilidades existentes, lo cual para efectos de graficarlo en la matriz de riesgos, podría ser homologado a la probabilidad de ocurrencia del riesgo, ya que a mayores debilidades presentadas, mayor es la probabilidad de falla o error.

La medición de la probabilidad de ocurrencia del riesgo, o nivel de riesgo, se representa en el eje “X” de la matriz, utilizando una división por percentiles que se numeran del 1 al 9, así:

[40] Ver la tabla 20.

Tabla 21: Niveles de riesgo considerados en el eje X

Límite superior	11%	22%	33%	44%	56%	67%	78%	89%	100%
Nivel	1	2	3	4	5	6	7	8	9

Fuente: Tesis **Elaborado por**: Katalina Coronel Hoyos

En cuanto al impacto que debe representarse en el eje Y, es claro que no todos los elementos seleccionados tienen el mismo nivel de impacto en el negocio, es decir que la falla en uno de ellos puede provocar mayores o menores consecuencias en el negocio, en función de la baja, media o alta dependencia o apalancamiento que brinde dicho elemento de TI a la organización. Debido a que este nivel de impacto varía en cada empresa, su valor debe ser consultado al momento de realizar la encuesta aplicada en la sección 3.3 del Capítulo 3, tomando el máximo valor identificado de entre todas las respuestas dadas a un mismo elemento, ya que para cada elemento se establecieron de 1 a 3 preguntas.

Adicionalmente, el impacto no depende solamente de las consecuencias que la falla en uno de los elementos provoque en el negocio, sino también del tamaño de la empresa analizada, ya que los problemas que ocurran en una institución financiera generarán un riesgo sistémico que podría afectar a terceros, en mayor o menor magnitud, dependiendo de la cantidad de deudores, proveedores, acreedores o socios que tenga la organización, lo cual generalmente está asociado al total de Activos de sus estados financieros.

Para determinar un rango adecuado de valores de Activos de los estados financieros en los que se podría segmentar el impacto, se han analizado los ranking de bancos privados, cooperativas de ahorro y crédito, mutualistas para la vivienda, sociedades financieras, instituciones financieras públicas y tarjetas de crédito, que están publicados en los boletines financieros de la página web de la Superintendencia de Bancos y Seguros[41].

Cabe aclarar que en este análisis se incluyeron únicamente a las cooperativas de ahorro y crédito que estuvieron controladas por la SBS hasta diciembre 2012, por su mayor tamaño respecto de las demás cooperativas que ahora están controladas por la Superintendencia de Economía Popular y Solidaria, y por tener una mayor exigencia en cuanto a los controles a aplicar en su tecnología de información.

De acuerdo con estos boletines, los valores mínimos y máximos de activos en miles de dólares por cada tipo de institución con corte al 31 de diciembre de 2012, fueron los siguientes:

[41] Superintendencia de Bancos y Seguros. Estadísticas – "Boletines mensuales" por tipo de institución, con corte al 31-dic-2012. Internet. www.sbs.gob.ec Acceso: 15-junio-2013

Tabla 22: Valores mínimos y máximos de Activos por tipo de institución al 31-dic-2012

TIPO INSTITUCIÓN	No. INST.	MÍNIMO	MÁXIMO	% MIN/MAX
Bancos	26	10,915.03	8,092,708.41	0.13%
Cooperativas	39	8,357.87	539,691.04	1.55%
Soc. Financieras	10	2,403.99	1,299,082.53	0.19%
Financieras Públicas	4	267,692.46	2,599,120.89	10.30%
Mutualistas	4	12,213.28	411,961.83	2.96%
Tarjetas Crédito	2	81,188.32	245,164.25	33.12%

Fuente: SBS **Elaborado por**: Katalina Coronel Hoyos

Como se puede observar, la dispersión existente en los activos financieros dentro de un mismo tipo de institución en general es bastante amplia, por lo que conviene hacer la segmentación por rangos de valores, indistintamente del tipo de institución. De esta manera, se obtuvieron las siguientes frecuencias y distribuciones:

Figura 13: Rangos de activos de instituciones financieras

Fuente: SBS **Elaborado por**: Katalina Coronel Hoyos

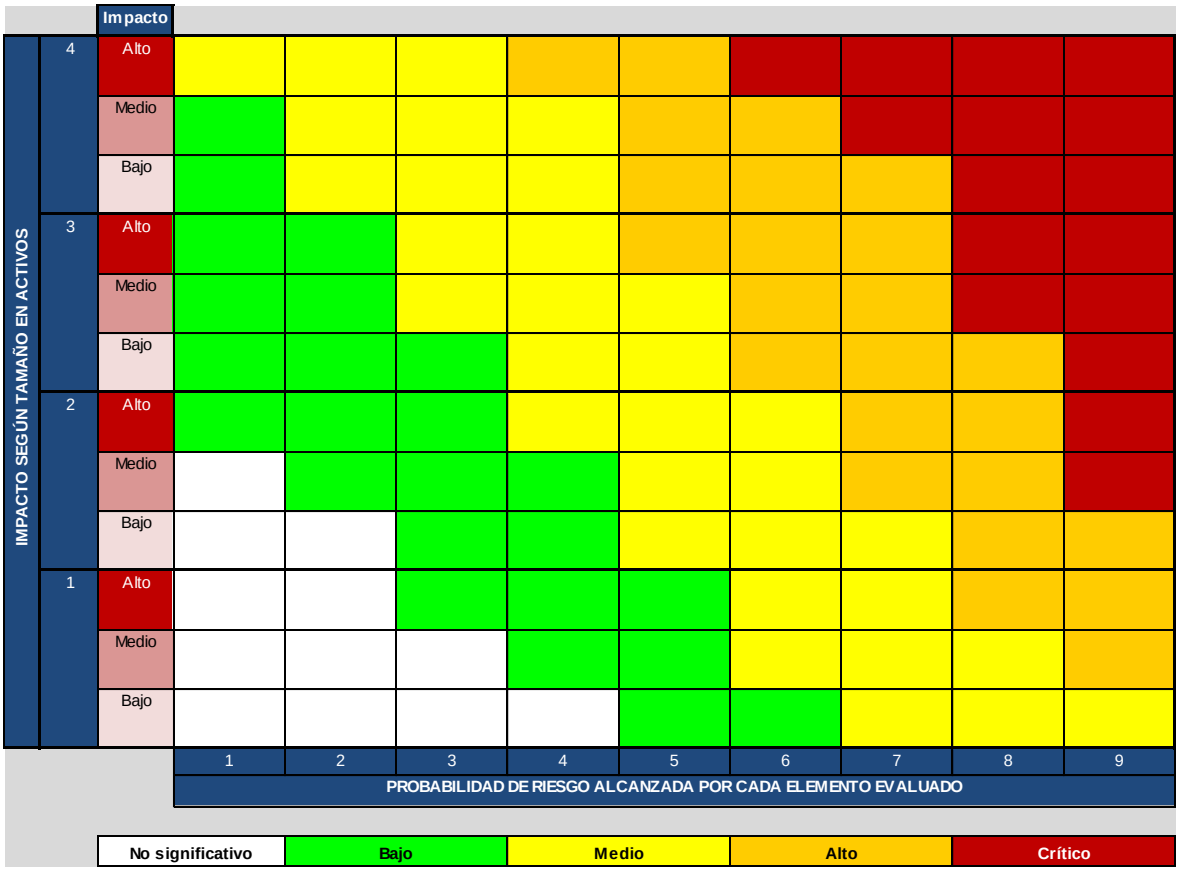
Para determinar los rangos de distribución de la figura anterior, se obtuvieron las diferencias entre cada institución financiera y la subsiguiente, en orden ascendente de activos, observando los valores en los que se podían apreciar "saltos" significativos dentro de la serie. Los valores detallados por institución se pueden ver en el anexo H.

De los grupos que se identificó que presentaban diferencias importantes entre ellos, se descartaron aquellos cuyo valor no era significativo dentro del rango, y también los que agrupaban a pocas instituciones, ya que el número de grupos será utilizado para identificar el número de segmentos que se graficará en la matriz de riesgos, por lo que lo ideal es contar con un número de 3 a 4 grupos.

De esta forma, se agruparon en el primer rango a 28 instituciones que tienen activos por hasta US$45.000.000, las cuales presentan características similares en cuanto a cobertura geográfica y número de socios o clientes; en un segundo rango se agruparon a 23 instituciones que presentaron activos por hasta US$131.000.000, y en los últimos rangos las restantes 34 instituciones financieras, que son las más grandes y por tanto requieren una mayor exigencia en cuanto a los controles que se deben aplicar en su Gobierno Corporativo, Gestión de Riesgos y Cumplimiento normativo de TI.

Una vez que se han definido los rangos de valores para el eje “X” (probabilidad de ocurrencia de riesgos) y para el eje “Y” (impacto de acuerdo al tamaño de los activos y a la importancia de cada elemento en el negocio) de la matriz de riesgos, se puede graficar la misma de la siguiente manera:

Figura 14: Matriz de riesgos de los elementos evaluados



Fuente: Katalina Coronel Hoyos **Elaborado por**: Katalina Coronel Hoyos

Para ubicar un elemento evaluado en esta matriz, se deberá obtener primero su probabilidad de riesgo, restando de 100% la calificación obtenida en su evaluación, y homologando dicho valor al percentil correspondiente, siendo el 1 un nivel no significativo de riesgo, y el 9 un riesgo crítico, tal como se anotó en la tabla 21.

Una vez determinado el valor del eje “X” de la matriz de riesgo (probabilidad), se debe determinar el valor en el eje “Y” (impacto), que está en función de los 4 rangos que se habían identificado para el tamaño de los activos de cada institución financiera, considerando los siguientes límites:

Tabla 23: Rangos de activos de instituciones financieras

RANGO	MÍNIMO	MÁXIMO
1	$0	$45.000.000
2	$45.000.001	$131.000.000
3	$131.000.001	$500.000.000
4	$500.000.001	>$500.000.001

Fuente: Tesis[42] **Elaborado por**: Katalina Coronel Hoyos

Por ejemplo, si una institución tiene US$86.000.000 de activos, se encuentra en el rango 2, y por tanto los valores de su evaluación deberán colocarse en el segmento 2 de la matriz de riesgos, tomando en cuenta para ello el nivel de impacto (alto, medio o bajo) de cada elemento evaluado respecto al negocio:

Figura 15: Ejemplo de selección del segmento en la matriz de riesgos

Fuente: Katalina Coronel Hoyos **Elaborado por**: Katalina Coronel Hoyos

Dependiendo del cuadrante en el que sea ubicada la evaluación de cada elemento, le corresponderá un color que representa su nivel de riesgo, según las siguientes equivalencias:

Tabla 24: Equivalencia de colores con el nivel de riesgo

COLOR	RIESGO
Blanco	No significativo
Verde	Bajo
Amarillo	Medio
Naranja	Alto
Rojo	Crítico

Fuente: Katalina Coronel H. **Elaborado por**: Katalina Coronel H.

[42] Ver el anexo H.

Al final de la evaluación, esta matriz contendrá la ubicación de todos los elementos seleccionados en alguno de los niveles de riesgo, lo cual permitirá que se cuente con una visión ejecutiva del estado general de los procesos y catalizadores que conforman el sistema de Gobierno, Riesgos y Cumplimiento de TI en la organización, que la guiarán hacia la adopción de medidas de mejora.

4.2. Establecimiento de las medidas a adoptar para el mejoramiento del Gobierno de TI según el nivel de riesgo obtenido

Una vez que se ha completado la matriz de riesgos con la evaluación de todos los elementos seleccionados, se facilita la identificación de los elementos que están siendo manejados de forma adecuada, así como aquellos que requieren fortalecerse. Ello permitirá priorizar los esfuerzos de mejoramiento de acuerdo con el impacto de cada elemento en el negocio, así como con la disponibilidad de los recursos y adecuación de capacidades requeridas en el corto, mediano y largo plazo.

El **primer paso** a seguir para el mejoramiento del Gobierno de TI es reconocer la necesidad de mejorar, lo cual se logra a través de identificar los puntos débiles actuales y desencadenar y crear el ánimo de cambio a un nivel de dirección ejecutiva. Este paso constituye la primera fase que COBIT 5 recomienda aplicar, dentro del ciclo de vida de su Guía de Implantación[43].

Una vez lograda la necesidad de cambio en la alta gerencia, se deberá continuar con la **fase 2** de la guía de implantación de COBIT 5, la cual se cubre aplicando los siguientes lineamientos:

1. Seleccionar todos aquellos procesos y catalizadores que se encuentren en riesgo crítico y alto para la organización, dentro de la matriz de riesgos.

2. Si el apetito de riesgo de la institución es medio o bajo, en la selección de elementos a mejorar se deberá incluir también a aquellos que se encuentren en riesgo medio, cuyo desempeño tenga un impacto medio o alto para la organización.

[43] ISACA, *COBIT 5 Un Marco de Negocio para el Gobierno y la Gestión de la empresa*, USA, ISACA, 2012. Pág. 38.

3. Para cada elemento seleccionado a ser mejorado, determinar las áreas en las que se obtuvo un puntaje bajo. Para ello, se deben analizar las variables que se calificaron durante la evaluación de cada elemento, y que constan en la siguiente tabla:

Tabla 25: Aspectos a ser evaluados en cada variable calificada

TIPO DE ELEMENTO	VARIABLE CALIFICADA	ASPECTOS EVALUADOS
PROCESO	Atributo de capacidad	Cumplimiento de metas del proceso[44]
	Prácticas base	Ejecución de las prácticas base sugeridas por COBIT 5 en su marco de referencia de procesos
	Productos de trabajo	Generación de las salidas establecidas en el marco de referencia de procesos de COBIT 5 para cada práctica clave
	Evaluación de catalizador	Puntaje total obtenido en el cuestionario "2. Procesos", para evaluación de catalizadores
CATALIZADOR	Grupos de interés	Identificación de necesidades de los grupos de interés Internos y externos
	Metas	Existencia de metas y métricas para monitoreo del desempeño
	Ciclo de vida	Existencia y aplicación de procedimientos adecuados en cada etapa del ciclo de vida
	Buenas prácticas	Aplicación de buenas prácticas en el ciclo de vida del catalizador

Fuente: Tesis[45] **Elaborado por**: Katalina Coronel Hoyos

4. Dependiendo de la variable que haya presentado un puntaje bajo, establecer la iniciativa de mejora en los aspectos evaluados correspondientes. En el caso de la evaluación de catalizador para un proceso, se deberá analizar la dimensión o variable calificada que obtuvo el puntaje más bajo en el cuestionario para identificar los aspectos en los que se debe realizar la mejora.

En la **fase 3**, se deben establecer las prioridades para los objetivos de mejora identificados, iniciando por aquellas iniciativas que son más fáciles de conseguir y que podrían proporcionar mayores beneficios (quick wins), ya que son las que generarán en un corto plazo la sensación de logro en el personal y promoverán un mejor ambiente para el resto de iniciativas.

[44] ISACA, *COBIT 5 Procesos Catalizadores*, USA, ISACA, 2012. Pág. 19.
[45] Ver la tabla 20.

Aquellas que son más retadoras y por lo tanto de mayor plazo, también deben contar con una prioridad de ejecución, en función de su impacto para el negocio y de los recursos requeridos.

En los casos que aplique, se debe justificar debidamente la razón por la que no se ejecutará alguna de las iniciativas de mejora y dejar constancia de forma manifiesta de la aceptación del riesgo de no hacerlo, por parte de la alta gerencia. Un aspecto importante a considerar es que la iniciativa de mejora debe estar alineada a la estrategia del negocio e identificarse claramente los objetivos de TI y de negocio a los que apoya.

En la **fase 4** se debe planificar, en base a las prioridades establecidas, la ejecución de las iniciativas de mejora, elaborando casos de negocio para cada una de ellas que especifiquen el patrocinador, beneficios a obtener, partes interesadas, tareas críticas e hitos, roles clave, responsabilidades, recursos necesarios, costos e inversiones previstos, plan de gestión de riesgos, cambios organizacionales requeridos, mecanismos de monitoreo y supervisión de la obtención de beneficios, y quién y cómo generará y usará las métricas.

En esta planificación también se debe desarrollar un plan de cambios para la implementación, que permita administrar de forma justificada y formalizada los cambios que las partes interesadas hayan solicitado, así como su análisis de impacto y la aprobación final antes de su ejecución.

En la **fase 5** se implementan las iniciativas de mejora de acuerdo con la planificación establecida, y se realiza el monitoreo para constatar la obtención de los beneficios esperados y gestionar posibles desviaciones que pudieran darse respecto del plan. El éxito de esta fase requiere el apoyo, involucramiento y compromiso de la alta gerencia así como la propiedad de las partes interesadas, tanto de TI como del negocio.

La **fase 6** se centra en la operación sostenible de los beneficios obtenidos con las iniciativas implementadas, y la **fase 7** en la identificación de posibles mejoras adicionales o correcciones que deban ser hechas para garantizar una mejora continua.

Se debe poner especial atención a aquellos procesos o catalizadores que son requeridos por la normativa de la Superintendencia de Bancos y Seguros, con el fin de asegurar que cumplen con todos los requerimientos regulatorios, y que su nivel de implementación y desempeño no generará sanciones u observaciones de parte del organismo de control.

Es importante además, establecer mecanismos que aseguren que se conocen oportunamente, se implementan y se gestionan los nuevos requerimientos normativos que pudieran presentarse en el futuro y que deban ser aplicados a los procesos o catalizadores del sistema de Gobierno de TI.

4.3. Definición de métricas a utilizar para garantizar la mejora continua en el Gobierno de TI

Si bien COBIT 5 sugiere métricas para cada meta de los procesos que constan en su modelo de referencia de procesos, éstas pueden ser adaptadas por las organizaciones según puedan ser implementadas, ya que COBIT 5 no es prescriptivo[46] sino que constituye un marco de referencia de buenas prácticas.

Con el fin de establecer un conjunto de métricas más fácilmente adaptables al modelo de negocio de las instituciones financieras, se han revisado y afinado las métricas propuestas por COBIT 5 para cada uno de los procesos seleccionados, con lo cual en la siguiente tabla se propone 1 métrica para cada meta, y para cada catalizador evaluado:

Tabla 26: Métricas sugeridas para medir el Gobierno de TI

	Gobierno		
	Evaluar, Dirigir y Monitorear	**Métrica / Fórmula de cálculo**	**Tipo**
EDM01	**Asegurar el establecimiento y mantenimiento de un marco de trabajo de Gobierno**		
1	Modelo estratégico de toma de decisiones para que las TI sean efectivas y estén alineadas con el entorno externo e interno de la empresa y los requerimientos de las partes interesadas.	Nivel de satisfacción de los interesados con el alcance del portfolio de programas y servicios planificado	Positivo
		# de interesados satisfechos con el alcance del portfolio de programas y servicios planificado / Total de interesados	
2	Garantizar que el sistema de gobierno para TI está incorporado al gobierno corporativo.	Porcentaje de procesos y prácticas aplicados a TI con clara trazabilidad a los principios organizacionales	Positivo
		# de procesos y prácticas de TI con trazabilidad a los principios organizacionales / Total de procesos y prácticas de TI	
3	Obtener garantías de que el sistema de gobierno para TI está operando de manera efectiva.	Frecuencia del reporte del gobierno de TI al Comité Ejecutivo y a la dirección	Positivo
		# de reportes del gobierno de TI al Comité Ejecutivo y a la dirección en un período / # de días del período	
EDM02	**Asegurar la entrega de beneficios**		
1	La empresa está asegurando un valor óptimo de su portafolio de iniciativas TI, servicios y activos aprobados.	Nivel de satisfacción de la gestión ejecutiva con la entrega de valor y los costos de TI	Positivo
		# de ejecutivos satisfechos con la entrega de valor y los costos de TI / Total de ejecutivos	
2	Se deriva un valor óptimo de la inversión TI mediante prácticas de gestión del valor en la empresa.	Porcentaje de incidentes mensuales que ocurren debido a la actual o tentativa evasión de los principios y prácticas establecidos para gestionar el valor	Negativo
		# de incidentes ocurridos en un período / # de días del período	
3	Las inversiones individuales en TI contribuyen a un valor óptimo.	Porcentaje del valor esperado realizado	Positivo
		Valor realizado / Valor esperado	

[46] ISACA, *COBIT 5 Procesos Catalizadores*, USA, ISACA, 2012. Págs. 11, 16.

EDM03	**Asegurar la optimización de riesgos**		
1	Los umbrales de riesgo son definidos y comunicados y los riesgos clave relacionados con la TI son conocidos	Porcentaje de potenciales riesgos TI identificados y gestionados # riesgos TI identificados y gestionados / Total riesgos TI	Positivo
2	La empresa gestiona el riesgo crítico empresarial relacionado con las TI eficaz y eficientemente	Porcentaje de riesgos altos y críticos que han sido mitigados por debajo del umbral de riesgo # de riesgos altos y críticos mitigados / Total de riesgos altos y críticos	Positivo
3	Los riesgos empresariales relacionados con las TI no exceden el apetito de riesgo y el impacto del riesgo TI en el valor de la empresa es identificado y gestionado	Porcentaje de riesgos TI que exceden el riesgo empresarial tolerado # riesgos TI que exceden el umbral / Total riesgos TI	Negativo
EDM04	**Asegurar la optimización de recursos**		
1	Las necesidades de recursos de la empresa son cubiertos con capacidades óptimas	Porcentaje de recursos que son utilizados del 50% al 80% de su capacidad # de recursos del 50% al 80% de su capacidad / Total de recursos	Positivo
2	Los recursos se asignan para satisfacer mejor las prioridades de la empresa dentro del presupuesto y restricciones	Porcentaje de proyectos prioritarios con asignación de recursos adecuados # de proyectos prioritarios con asignación de recursos adecuados / Total de proyectos prioritarios	Positivo
3	El uso óptimo de los recursos se logra a lo largo de su completo ciclo de vida económico	Porcentaje de proyectos y programas con un estado de riesgo medio o alto debido a problemas en la gestión de recursos # de proyectos y programas con riesgo medio o alto por problemas en la gestión de recursos / Total proyectos y programas	Negativo
EDM05	**Asegurar la transparencia de los interesados**		
1	Los informes para las partes interesadas se ajustan a sus requisitos	Nivel de satisfacción de los interesados con el contenido de los informes # de interesados satisfechos con el contenido de los informes / Total de interesados	Positivo
2	La elaboración de informes es completa, oportuna y precisa	Porcentaje de informes no presentados a tiempo, o con imprecisiones # de informes mensuales no presentados a tiempo o con imprecisiones / Total de informes del mes	Negativo
3	La comunicación es eficaz y las partes interesadas están satisfechas	Porcentaje de interesados satisfechos con la oportunidad y profundidad de los informes # de interesados satisfechos con la oportunidad y profundidad de los informes / Total de interesados	Positivo
	Administración		
	Alinear, Planear y Organizar	**Métrica / Fórmula de cálculo**	**Tipo**
APO01	**Administrar el marco de trabajo de Administración de TI**		
1	Se ha definido y se mantiene un conjunto eficaz de políticas	Porcentaje de políticas, estándares y otros elementos catalizadores activos, documentados, actualizados y publicados # de políticas, estándares y otros elementos catalizadores activos, documentados, actualizados y publicados / Total documentos	Positivo
2	Todos tienen conocimiento de las políticas y de cómo deberían implementarse	Porcentaje de asistencia a sesiones de formación o de sensibilización # de empleados que asistieron a sesiones de formación o de sensibilización / Total de empleados	Positivo
APO02	**Administrar la Estrategia**		

1	Todos los aspectos de la estrategia de TI están alineados con la estrategia del negocio	Porcentaje de objetivos en la estrategia de TI que dan soporte a la estrategia de negocio	Positivo
		# de objetivos en la estrategia de TI alineados al negocio / Total de objetivos de TI	
2	La estrategia de TI es coste-efectiva, apropiada, realista, factible, enfocada al negocio y equilibrada	Porcentaje de iniciativas en la estrategia de TI autofinanciadas (los beneficios superan los costos)	Positivo
		# de iniciativas de TI autofinanciadas / Total de iniciativas de TI	
3	Se pueden derivar objetivos a corto plazo claros, concretos, y trazables de iniciativas a largo plazo específicas, y se pueden traducir en planes operativos	Porcentaje de proyectos de TI que pueden ser directamente trazables con la estrategia de TI	Positivo
		# de proyectos de TI trazables con la estrategia de TI / Total de proyectos de TI	
4	TI es un generador de valor para el negocio	Porcentaje de objetivos estratégicos empresariales obtenidos como resultado de iniciativas de TI	Positivo
		# de objetivos estratégicos empresariales soportados por iniciativas de TI / Total de objetivos estratégicos empresariales	
5	Existe conciencia de la estrategia de TI y una clara asignación de responsabilidades para su entrega	Porcentaje de logro de resultados estratégicos de TI obtenido en la medición de desempeño del personal	Positivo
		Resultados estratégicos de TI logrados por el personal / Resultados estratégicos de TI esperados	
APO03	**Administrar la Arquitectura Empresarial**		
1	La arquitectura y los estándares son eficaces apoyando a la empresa	Frecuencia de cambios solicitados y concedidos en los estándares de la arquitectura básica	Negativo
		# de cambios solicitados y concedidos en un período / # de días del período	
2	La cartera de servicios de la arquitectura de empresa soporta el cambio empresarial ágil	Porcentaje de proyectos que usan los servicios de la arquitectura de empresa	Positivo
		# de proyectos que usan los servicios de la arquitectura de empresa / Total de proyectos	
3	Existen dominios apropiados y actualizados y/o arquitecturas federadas que proveen información fiable de la arquitectura	Porcentaje de deficiencias detectadas en los modelos de los dominios de empresa, información, datos, aplicaciones y arquitectura de tecnología	Negativo
		# de deficiencias detectadas en los modelos de arquitectura en un período / # de días del período	
4	Se utiliza un marco de arquitectura de empresa y una metodología común, así como un repositorio de arquitectura integrado, con el fin de permitir la reutilización de eficiencias dentro de la empresa	Porcentaje de proyectos que utilizan el marco de trabajo y la metodología para reutilizar componentes ya definidos	Positivo
		# de proyectos que utilizan el marco de trabajo y la metodología para reutilizar componentes / Total de proyectos	
APO04	**Administrar la Innovación**		
1	El valor de empresa es creado mediante la cualificación y puesta en escena de los avances e innovaciones tecnológicas más apropiadas, los métodos y las soluciones TI utilizadas	Penetración en el mercado o mejora en la competitividad de la empresa debido a la innovación	Positivo
		# de clientes de la empresa con productos innovadores / Total de clientes potenciales del mercado objetivo	
2	Los objetivos de la empresa se cumplen por la mejora de los beneficios de la calidad y/o la reducción de costes como resultado de la identificación e implementación de soluciones innovadoras	Porcentaje de objetivos estratégicos empresariales obtenidos como resultado de iniciativas innovadoras de TI	Positivo
		# de objetivos estratégicos empresariales logrados debido a iniciativas innovadoras de TI / Total de objetivos estratégicos	
3	La innovación se permite y se promueve y forma parte de la cultura de la empresa	Porcentaje de objetivos de innovación o relacionados con tecnologías emergentes en las metas de rendimiento para personal relevante	Positivo

		# de objetivos de innovación en las metas de rendimiento de personal relevante / Total de objetivos de personal relevante	
APO05	**Administrar el Portafolio**		
1	Se ha definido una mezcla apropiada de inversión alineada con la estrategia corporativa	Porcentaje de inversiones TI que tienen trazabilidad con la estrategia, riesgos y costos de la compañía	Positivo
		# de inversiones TI trazables a la estrategia, riesgos y costos de la compañía / Total de inversiones TI	
2	Fuentes de fondos de inversión identificados y están disponibles	Porcentaje de fondos usados, de entre los asignados	Positivo
		Fondos de inversión usados / Fondos asignados	
3	Casos de negocio de programa evaluados y priorizados antes de que se asignen los fondos	Porcentaje de unidades de negocio involucradas en la elaboración de casos de negocio y priorización de programas	Positivo
		# de unidades de negocio involucradas en la elaboración de casos de negocio y priorización de programas / Total de unidades de negocio	
4	Existe una vista precisa y comprensiva del rendimiento de las inversiones del portafolio	Frecuencia de medición del rendimiento de las inversiones del portafolio	Positivo
		# de mediciones del rendimiento de las inversiones del portafolio en un período / # de días del período	
5	Los cambios en el programa de inversiones se reflejan en los portafolios relevantes de servicios, activos y recursos de TI	Porcentaje de cambios del programa de inversiones reflejados en los portafolios relevantes de TI	Positivo
		# de cambios del programa de inversiones reflejados en los portafolios relevantes de TI / Total de cambios del programa de inversiones	
6	Los beneficios han sido generados debido a los beneficios de la monitorización	Porcentaje de inversiones en los que los beneficios producidos han sido medidos y comparados con el caso de negocio, y gestionados para su logro	Positivo
		# de inversiones con beneficios medidos y gestionados / Total de inversiones	
APO07	**Administrar los Recursos Humanos**		
1	La estructura organizacional y las relaciones de TI son flexibles y dan respuesta ágil	Porcentaje de tiempo que transcurre en la gerencia para la aprobación de decisiones estratégicas	Negativo
		# de días transcurridos / # de días esperados	
2	Los recursos humanos son gestionados eficaz y eficientemente	Porcentaje de rotación del personal	Negativo
		((# de entradas + # de salidas en el período) / 2) / ((# de empleados al inicio + # de empleados al final del período) / 2)	
APO08	**Administrar las Relaciones**		
1	Las estrategias, planes y requisitos de negocio están bien entendidos, documentados y aprobados	Porcentaje de servicios TI definidos en términos de los requisitos del negocio	Positivo
		# de servicios TI definidos en términos de negocio / # de servicios TI	
2	Existencia de buenas relaciones entre la empresa y las TI	Porcentaje de usuarios y de personal de TI satisfechos con su relación	Positivo
		# de usuarios y de personal de TI satisfechos con su relación / Total de usuarios y personal de TI	
3	Las partes interesadas del negocio son conscientes de las oportunidades posibilitadas por la TI	Porcentaje de usuarios que conocen los servicios disponibles, beneficios y limitaciones de la TI	Positivo
		# de usuarios que conocen los servicios disponibles, beneficios y limitaciones de la TI / Total de usuarios	
APO10	**Administrar los Proveedores**		
1	Los proveedores rinden según lo acordado	Frecuencia de infracciones de servicio causadas por los proveedores	Negativo
		# de infracciones de servicio causadas por los proveedores en un período / # de días del período	

2	El riesgo de los proveedores se evalúa y trata adecuadamente	Frecuencia de incidentes ocurridos relacionados con el riesgo de proveedores	Negativo
		# de incidentes ocurridos por riesgos de proveedores / Total de incidentes	
3	Las relaciones con los proveedores son eficaces	Porcentaje de disputas con proveedores resueltas adecuadamente y en un tiempo razonable	Positivo
		# de disputas con proveedores resueltas oportunamente / Total de disputas presentadas con proveedores	
APO11	**Administrar la Calidad**		
1	Las partes interesadas están satisfechas con la calidad de los servicios y las soluciones	Promedio de satisfacción de las partes interesadas con las soluciones y servicios	Positivo
		# de interesados satisfechos con las soluciones y servicios / Total de interesados	
2	Los resultados de los proyectos y de los servicios entregados son predecibles	Frecuencia de defectos sin descubrir antes de la puesta en producción	Negativo
		# de defectos presentados en producción en un período / # de días del período	
3	Los requisitos de calidad están implementados en todos los procesos	Porcentaje de procesos con un informe de evaluación formal de la calidad	Positivo
		# de procesos con un informe de evaluación de su calidad / Total de procesos	
APO12	**Administrar los Riesgos**		
1	El riesgo relacionado con TI está identificado, analizado, gestionado y reportado	Porcentaje de eventos de pérdida ocurridos, no capturados en repositorios	Negativo
		# de eventos de pérdida ocurridos, no capturados en repositorios / # de eventos de riesgo registrados en el repositorio	
2	Existe un perfil de riesgo actual y completo	Porcentaje de procesos de negocio claves incluidos en el perfil de riesgo	Positivo
		# de procesos de negocio claves con perfil de riesgo / Total de procesos	
3	Todas las acciones de gestión para los riesgos significativos están gestionadas y bajo control	Grado de avance en la gestión de los riesgos significativos, respecto de su planificación	Positivo
		Promedio de avance en la gestión de los riesgos significativos	
4	Las acciones de gestión de riesgos están efectivamente implementadas	Brecha entre el riesgo residual actual frente al nivel de riesgo esperado luego de la implementación de las acciones de gestión de riesgos	Positivo
		% de riesgo esperado por cada acción de gestión - % de riesgo residual actual	
	Construir, Adquirir y Operar	**Métrica / Fórmula de cálculo**	**Tipo**
BAI01	**Administrar Programas y Proyectos**		
1	Las partes interesadas relevantes están comprometidas con los programas y los proyectos	Porcentaje de partes interesadas que están participando en el proyecto	Positivo
		# de interesados participando en el proyecto / Total de interesados	
2	El alcance y los resultados de los programas y proyectos son viables y están alineados con los objetivos	Porcentaje de proyectos emprendidos sin casos de negocio aprobados	Negativo
		# de proyectos emprendidos sin casos de negocio aprobados / Total de proyectos emprendidos	
3	Los planes de programas y proyectos tienen probabilidades de lograr los resultados esperados	Porcentaje de programas y proyectos con riesgos identificados y su plan de mitigación	Positivo
		# de programas y proyectos con riesgos identificados y plan de mitigación / Total de programas y proyectos	
4	Las actividades de los programas y proyectos se ejecutan de acuerdo a los planes	Porcentaje de proyectos con desviaciones del plan de referencia	Negativo
		# de proyectos con desviaciones del plan de referencia / Total de proyectos	

5	Existen suficientes recursos de los programas y proyectos para realizar las actividades de acuerdo a los planes	Frecuencia de desviaciones e incidentes ocurridos por los recursos (por ejemplo, habilidades, capacidad)	Negativo
		# de desviaciones e incidentes ocurridos por los recursos en un período / # de días del período	
6	Los beneficios esperados de los programas y proyectos son obtenidos y aceptados	Porcentaje de beneficios esperados que se han alcanzado	Positivo
		# de beneficios alcanzados / Total de beneficios esperados	
BAI02	**Administrar la Definición de Requerimientos**		
1	Los requerimientos funcionales y técnicos del negocio reflejan las necesidades y expectativas de la organización	Frecuencia de requerimientos repetidos debido a la no alineación entre las necesidades y expectativas de la organización	Negativo
		# de requerimientos repetidos debido a la no alineación con las necesidades de la organización en un período / # de días del período	
2	La solución propuesta satisface los requerimientos funcionales, técnicos y de cumplimiento del negocio	Porcentaje de requerimientos satisfechos por la solución propuesta	Positivo
		# de requerimientos satisfechos por la solución propuesta / Total de requerimientos efectuados	
3	El riesgo asociado con los requerimientos ha sido tomado en cuenta en la solución propuesta	Porcentaje de incidentes no identificados como riesgo o con un riesgo superior al esperado	Negativo
		# de incidentes no identificados como riesgo o con un riesgo superior al esperado / Total de incidentes	
4	Los requerimientos y soluciones propuestas cumplen con los objetivos del caso de negocio (valor esperado y costos probables)	Porcentaje de los objetivos y beneficios del caso de negocio alcanzados por la solución propuesta	Positivo
		# de objetivos y beneficios del caso de negocio alcanzados por la solución propuesta / Total de objetivos y beneficios esperados	
BAI05	**Administrar la Habilitación del Cambio Organizacional**		
1	El deseo de cambio de las partes interesadas ha sido entendido	Promedio del nivel de entendimiento del cambio requerido en las partes interesadas	Positivo
		Promedio del % de entendimiento del cambio requerido en las partes interesadas	
2	El equipo de implementación es competente y está habilitado para conducir el cambio	Promedio de calificación de competencias y habilidades de los miembros del equipo de implementación	Positivo
		Promedio del % de desarrollo de competencias y habilidades de los miembros del equipo de implementación	
3	El cambio deseado es comprendido y aceptado por las partes interesadas	Porcentaje de partes interesadas que están participando en el proyecto	Positivo
		# de interesados participando en el proyecto / Total de interesados	
4	Los que juegan algún papel están facultados para entregar el cambio	Porcentaje de los que juegan algún papel con una autoridad asignada adecuada	Positivo
		# de los que juegan algún papel con una autoridad asignada adecuada / Total de los que juegan algún papel	
5	Todos los que juegan algún papel están habilitados para operar, utilizar y mantener el cambio	Promedio de autoevaluación de capacidades relevantes por parte de los involucrados en operar, utilizar o mantener el cambio	Positivo
		Promedio de autoevaluación del % de desarrollo de capacidades por parte de los involucrados en operar, utilizar o mantener el cambio	
6	El cambio está integrado y sostenido	Nivel de satisfacción de los usuarios con la adopción del cambio	Positivo
		# de usuarios satisfechos con la adopción del cambio / Total de usuarios	
BAI08	**Administrar el Conocimiento**		

1	Las fuentes de información son identificadas y clasificadas	Porcentaje de procesos de negocio cuyas fuentes de información han sido identificadas y clasificadas	Positivo
		# de procesos de negocio con fuentes de información identificadas y clasificadas / Total de procesos	
2	El conocimiento es utilizado y compartido	Frecuencia de reportes e informes del sistema gerencial no utilizados al menos trimestralmente	Negativo
		# de reportes e informes del sistema gerencial no utilizados en un período / # de días del período	
3	La compartición de conocimiento está integrada en la cultura de la empresa	Porcentaje de usuarios formados en el uso y compartición de conocimiento	Positivo
		# de usuarios formados en el uso y compartición de conocimiento / Total de usuarios	
4	El conocimiento es actualizado y mejorado para dar soporte a los requisitos	Porcentaje de actualización del conocimiento disponible	Positivo
		# de fuentes de información actualizadas en un período / Total de fuentes de información	
	Monitorear, Evaluar y Valorar	**Métrica / Fórmula de cálculo**	**Tipo**
MEA01	**Monitorear, Evaluar y Valorar el Desempeño y Conformidad**		
1	Objetivos y métricas aprobadas por las partes interesadas	Porcentaje de servicios que cuentan con objetivos y métricas de desempeño aprobadas por las partes interesadas	Positivo
		# de servicios que cuentan con objetivos y métricas de desempeño aprobados / Total de servicios	
2	Procesos medidos acorde a las métricas y objetivos acordados	Porcentaje de procesos que cumplen con los objetivos y métricas de desempeño y conformidad definidas	Positivo
		# de procesos que cumplen con los objetivos y métricas de desempeño y conformidad / Total de procesos	
3	La monitorización, evaluación y generación de información es efectiva y operativa	Porcentaje de procesos cuyas desviaciones en la evaluación han sido gestionadas	Positivo
		# de procesos con desviaciones gestionadas / Total de procesos con desviaciones	
4	Objetivos y métricas integradas dentro de los sistemas de supervisión de la empresa	Porcentaje de objetivos y métricas cuyo cumplimiento se informa periódicamente	Positivo
		# de objetivos y métricas cuyo cumplimiento se informa periódicamente / Total de objetivos y métricas	
5	Los informes acerca del rendimiento y conformidad de los procesos es útil y a tiempo	Porcentaje de informes de rendimiento entregados dentro del plazo previsto	Positivo
		# de informes de rendimiento entregados dentro del plazo previsto / Total de informes entregados	
MEA02	**Monitorear, Evaluar y Valorar el Sistema de Control Interno**		
1	Los procesos, recursos e información cumplen con los requisitos del sistema de control interno de la empresa	Porcentaje de procesos y salidas que están conformes con las metas de control interno	Positivo
		# de procesos y salidas que están conformes con las metas de control interno / Total de procesos y salidas	
2	Todas las iniciativas de aseguramiento se planean y ejecutan de forma efectiva	Porcentaje de iniciativas de aseguramiento ejecutadas frente a las aprobadas en la planificación	Positivo
		# de iniciativas de aseguramiento ejecutadas / # de iniciativas de aseguramiento planificadas y aprobadas	
3	Se proporciona aseguramiento independiente de que el sistema de control interno es operativo y efectivo	Porcentaje de procesos bajo revisión independiente	Positivo
		# de procesos bajo revisión independiente / Total de procesos	
4	El control interno está establecido y las deficiencias son	Porcentaje de debilidades identificadas en los informes externos de certificación y cualificación	Negativo

	identificadas y comunicadas	# de debilidades identificadas en los informes externos de certificación y cualificación en un período / # de días del período	
MEA03	**Monitorear, Evaluar y Valorar el Cumplimiento con Requerimientos Externos**		
1	La totalidad de los requisitos externos de cumplimiento se han identificado	Frecuencia de revisiones de cumplimiento # de revisiones de cumplimiento en un período / # de días del período	Positivo
2	Tratar adecuadamente los requisitos externos de cumplimiento	Tiempo medio transcurrido entre el plazo de los requisitos de cumplimiento y su implementación # de días del plazo de cumplimiento - # de días transcurridos para su implementación	Positivo
Catalizadores		**Métrica / Fórmula de cálculo**	**Tipo**
CAT1	Principios, políticas y marcos de referencia	Porcentaje de aplicación de los principios, políticas y marcos de referencia # de principios, políticas y marcos de referencia aplicados / Total de principios, políticas y marcos de referencia	Positivo
CAT2	Procesos	Porcentaje de procesos cuyo diseño recoge las necesidades de provisión de información, ejecución, control y rendición de cuentas de las partes interesadas # de procesos cuyo diseño recoge las necesidades de las partes interesadas / Total de procesos	Positivo
CAT3	Estructuras organizativas	Nivel de satisfacción de los interesados con los niveles de autoridad, apoyo y asesoría existentes # de interesados satisfechos con los niveles de autoridad, apoyo y asesoría existentes / Total interesados	Positivo
CAT4	Cultura, ética y comportamiento	Porcentaje de principios y valores corporativos recogidos en el código de ética y la política de toma de riesgos # de principios y valores corporativos recogidos en el código de ética y la política de toma de riesgos / Total de principios y valores corporativos	Positivo
CAT5	Información	Porcentaje de fuentes de información cuyos propietarios no han sido formalmente definidos # de fuentes de información sin propietarios definidos / Total de fuentes de información	Negativo
CAT6	Servicios, infraestructuras y aplicaciones	Promedio del porcentaje de procesos de negocio que cuentan con los servicios, infraestructura, tecnología y aplicaciones requeridos # de procesos de negocio que cuentan con los servicios, infraestructura, tecnología y aplicaciones requeridos / Total de procesos de negocio	Positivo
CAT7	Personas, habilidades y competencias	Porcentaje de personal cuyos conocimientos, habilidades y competencias han sido evaluados antes de ser seleccionados y reclutados # de empleados con conocimientos, habilidades y competencias evaluados previo a su selección / Total de empleados	Positivo

Fuente: ISACA **Elaborado por**: Katalina Coronel Hoyos

En la tabla anterior se ha definido además la fórmula de cálculo para obtener la métrica a utilizar en la mejora del sistema de Gobierno de TI, para aquellos elementos que hayan sido seleccionados. Dependiendo de las prioridades y recursos de la organización, debe establecerse la meta esperada para cada métrica, tomando en

consideración su tipo, es decir, si el valor es mejor al tener un incremento o decremento de las variables involucradas, así como los valores mínimo, aceptable y máximo que se espera en cada métrica.

Adicionalmente, se debe definir la periodicidad con que serán calculadas las métricas, el área o persona responsable de realizar la medición, y a quién deben ser presentados sus resultados. Para ello, se puede elaborar una matriz similar a la que se muestra en el siguiente ejemplo:

Tabla 27: Formato para documentar la matriz de métricas

			Meta					
Métrica	**Tipo**	**Fórmula de cálculo**	**Mín.**	**Aceptable**	**Máx.**	**Frecuencia de cálculo**	**Responsable de medición**	**Informar a**
Nivel de satisfacción de los interesados con los niveles de autoridad, apoyo y asesoría existentes	Positivo	# interesados satisfechos con los niveles de autoridad, apoyo y asesoría existentes / Total interesados	75%	80%	95%	Anual	Desarrollo Organizacional	Comité Estratégico

Fuente: Tesis – Tabla 26 **Elaborado por**: Katalina Coronel Hoyos

Es importante también contar con una línea base de medición para conocer la situación actual de la que se parte hacia la iniciativa de mejora, lo cual permitirá determinar el grado de avance que se tenga en cada medición.

Con estos indicadores y los resultados presentados en este capítulo, se espera contribuir con una guía metodológica concreta que permita mejorar el Gobierno, Riesgos y Cumplimiento de TI en las instituciones financieras ecuatorianas, lo cual optimizará la creación del valor empresarial que satisfaga las expectativas de todas sus partes interesantes, dentro de un contexto amplio de Gobierno Corporativo.

CAPÍTULO 5 - CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

Para el desarrollo de la presente metodología de evaluación del Gobierno, Riesgos y Cumplimiento de TI, se utilizó como base conceptual el marco de trabajo de COBIT 5, el mismo que provee de elementos, herramientas y lineamientos de mejores prácticas para que las empresas alcancen sus metas para el gobierno y la gestión de la tecnología de información corporativa.

En el marco de trabajo de COBIT 5 se establece una clara distinción entre gobierno y gestión, ya que engloban diferentes tipos de actividades, requieren diferentes estructuras organizacionales y se enfocan en diferentes propósitos. Ello implica que no todos los elementos y herramientas que provee COBIT 5 apoyan de la misma manera al Gobierno corporativo de la organización, por lo que en esta metodología fue necesario seleccionar aquellos procesos y catalizadores que contribuyen de manera más directa a proveer de información y dar soporte al cuerpo de gobierno de la institución evaluada.

Los elementos seleccionados, las actividades realizadas y los mecanismos diseñados para evaluar el Gobierno, Riesgos y Cumplimiento de TI, permitieron cumplir con los objetivos planteados para el desarrollo de esta metodología, que fueron:

a. Investigar y documentar los conceptos teóricos que permitan identificar los elementos de COBIT 5 y el estándar ISO/IEC 27005, así como los requerimientos normativos de tecnología de información que deben cumplir las instituciones del sistema financiero ecuatoriano.
b. Identificar los elementos de COBIT 5 relacionados con el Gobierno de TI, a ser evaluados.
c. Homologar los requerimientos normativos de tecnología de información de la Superintendencia de Bancos y Seguros para las instituciones financieras, con los requerimientos del estándar ISO/IEC 27005, y los objetivos de control de COBIT 5 que los satisfacen.
d. Generar una matriz de riesgos calórica en la que se refleje el nivel de riesgo de cada elemento evaluado, según su importancia en la institución financiera

Para la aplicación de esta metodología, es necesario contar con un conocimiento básico de COBIT 5 con el fin de evaluar adecuadamente el logro de las metas y la ejecución de las actividades clave de los procesos seleccionados.

Durante la aplicación de esta metodología, se podrían observar subvaloraciones o sobrevaloraciones de los logros alcanzados por los elementos evaluados en la institución financiera, ya que las respuestas pueden estar influenciadas por el tipo y nivel de involucramiento que tenga la persona evaluadora con respecto al negocio, por lo que es importante dotarle de independencia y objetividad a la evaluación.

Esta metodología puede ser aplicada no solo a las instituciones financieras ecuatorianas controladas por la Superintendencia de Bancos y Seguros, sino a cualquier tipo y tamaño de empresa, pública o privada, de bienes o servicios, ya que entre sus variables para la evaluación del Gobierno, Riesgos y Cumplimiento de TI considera el tamaño en activos de la organización examinada, lo cual permite regular el nivel de exigencia en la aplicación de las buenas prácticas que sugiere COBIT 5, de acuerdo con su capacidad y recursos.

Las buenas prácticas internacionales sobre Gobierno, Riesgos y Cumplimiento de TI generan ventajas competitivas a las organizaciones que las aplican, por lo cual esta temática debería ser parte de la formación académica de estudiantes y maestrantes de las carreras de la PUCE, de modo que se promueva la autorregulación o cumplimiento proactivo de prácticas y procedimientos que otorgan valor a las empresas.

5.2. Recomendaciones

Debido a que esta metodología facilita la identificación de debilidades y áreas de posible mejora que permitan contar con un sólido sistema de Gobierno Corporativo basado en buenas prácticas internacionales, se recomienda difundirla, especialmente entre las instituciones financieras medianas y pequeñas, para que con su aplicación puedan incrementar la posibilidad de éxito en el logro de sus objetivos estratégicos corporativos, así como fortalecer su ambiente de control interno, mientras se optimizan los riesgos y se realiza un uso de los recursos de forma más eficiente.

Previo a aplicar esta metodología en una institución financiera, se recomienda dictar un taller de COBIT 5 de al menos 8 horas al personal que participará en la evaluación, con el fin de garantizar la comprensión del alcance de la misma, y que los resultados arrojados proporcionen un diagnóstico ajustado a la realidad de la organización. Esto facilitará además la identificación de las iniciativas que se requiere implementar para mejorar el sistema de Gobierno corporativo de TI en la institución.

Para evitar una subvaluación o sobrevaluación del logro alcanzado por los procesos y catalizadores de la institución evaluada con esta metodología, se recomienda que en su aplicación intervenga un equipo multidisciplinario, integrada por al menos 2 personas de diferentes áreas de la organización, y de preferencia pertenecientes al área de Auditoría Interna, lo que generará mayor independencia y objetividad a la evaluación.

Con el propósito de perfeccionar esta metodología con insumos tomados de las actividades empresariales cotidianas, se recomienda aplicar la misma en al menos una institución financiera de cada tipo y rango de activos, lo cual permitirá conocer las diversas o comunes dificultades y limitaciones que presenten dichos tipos de instituciones en la implementación de un adecuado sistema de Gobierno, Riesgos y Cumplimiento de TI.

Por último, y dada su relevancia e incidencia en el logro de los objetivos empresariales, es recomendable que los temas relativos a Gobierno Corporativo, Gestión de Riesgos y Cumplimiento de TI, sean incorporados al pensum académico de la carrera de Ingeniería en Sistemas, así como en los programas de maestría de la PUCE relacionados con la tecnología, de modo que se tenga una visión amplia y práctica de lo que las organizaciones deben gestionar para garantizar su sostenibilidad en el tiempo, y generar el valor que esperan todas sus partes interesadas, con un nivel óptimo de sus riesgos y de uso de sus recursos.

BIBLIOGRAFÍA

- Beltrán, Marta. *Matriz de riesgos*. Internet. http://redindustria.blogspot.com/2010/05/matriz-de-riesgos.html. Acceso: 1-abr-2013.
- ISACA. *COBIT 5 Un Marco de Negocio para el Gobierno y la Gestión de la empresa*, USA, ISACA, 2012.
- ISACA. *COBIT 5 Procesos Catalizadores*, USA, ISACA, 2012.
- ISACA. *Process Assessment Model (PAM): Using COBIT 5*, USA, ISACA, 2013.
- ISO/IEC 2008, *INTERNATIONAL STANDARD ISO/IEC 27005,* Suiza, 2008.
- Marks, Larry. "Governance Implementation – COBIT 5 and ISO", *Journal*, Volumen 1, 2013, ISACA, USA.
- De Haes, Steven; Haest, Rogier; Van Grembergen, Wim. "IT Governance and Business-IT Alignment in SMEs", *Journal*, Volumen 6, 2010, ISACA, USA.
- Superintendencia de Bancos y Seguros. *Estadísticas – Boletines mensuales*. Internet. www.sbs.gob.ec. Acceso: 15-junio-2013.
- Superintendencia de Bancos y Seguros. *Codificación de Resoluciones de la Superintendencia de Bancos y Seguros y de la Junta Bancaria*, Quito - Ecuador, SBS, 2011. Título II, Capítulo I, Sección VIII.
- Superintendencia de Bancos y Seguros. *Codificación de Resoluciones de la Superintendencia de Bancos y Seguros y de la Junta Bancaria*, Quito - Ecuador, SBS, 2005. Título X, Capítulo V.

ANEXOS

ANEXO A: Mapeo entre las metas corporativas de COBIT 5 y las metas de TI[47]:

Figura 22—Mapeo entre las Metas Corporativas de COBIT 5 y las Metas Relacionadas con las TI

		Meta corporativa																
		Valor para las partes interesadas de las Inversiones de Negocio	Cartera de productos y servicios competitivos	Riesgos de negocio gestionados (salvaguarda de activos)	Cumplimiento de leyes y regulaciones externas	Transparencia financiera	Cultura de servicio orientada al cliente	Continuidad y disponibilidad del servicio de negocio	Respuestas ágiles a un entorno de negocio cambiante	Toma estratégica de Decisiones basadas en información	Optimización de costes de entrega del servicio	Optimización de la funcionalidad de los procesos de negocio	Optimización de los costes de los procesos de negocio	Programas gestionados de cambio en el negocio	Productividad operacional y de los empleados	Cumplimiento con las políticas internas	Personas preparadas y motivadas	Cultura de innovación del producto y del negocio
		1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.	16.	17.
	Meta relacionada con las TI	**Financiera**					**Cliente**					**Interna**					**Aprendizaje y Crecimiento**	
Financiera	01 Alineamiento de TI y la estrategia de negocio	P	P	S			P	S	P	P	S	P	S	P			S	S
	02 Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas			S	P											P		
	03 Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	P	S	S					S	S		S		P			S	S
	04 Riesgos de negocio relacionados con las TI gestionados			P	S			P	S		P			S		S	S	
	05 Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI	P	P				S		S		S	S	P		S			S
	06 Transparencia de los costes, beneficios y riesgos de las TI	S		S		P				S	P		P					
Cliente	07 Entrega de servicios de TI de acuerdo a los requisitos del negocio	P	P	S	S		P	S	P	S		P	S	S			S	S
	08 Uso adecuado de aplicaciones, información y soluciones tecnológicas	S	S	S			S	S		S	S	P	S		P		S	S
Interna	09 Agilidad de las TI	S	P	S			S		P			P		S	S		S	P
	10 Seguridad de la información, infraestructuras de procesamiento y aplicaciones			P	P			P								P		
	11 Optimización de activos, recursos y capacidades de las TI	P	S						S		P	S	P	S	S			S
	12 Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio	S	P	S			S		S		S	P	S	S	S			S
	13 Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad	P	S	S			S				S		S	P				
	14 Disponibilidad de información útil y relevante para la toma de decisiones	S	S	S	S			P		P		S						
	15 Cumplimiento de TI con las políticas internas			S	S											P		
Aprendizaje y Crecimiento	16 Personal del negocio y de las TI competente y motivado	S	S	P			S		S						P		P	S
	17 Conocimiento, experiencia e iniciativas para la innovación de negocio	S	P				S		P	S		S		S			S	P

[47] ISACA, *COBIT 5 Un Marco de Negocio para el Gobierno y la Gestión de la empresa*, USA, ISACA, 2012. Pág. 50.

ANEXO B: Mapeo entre metas de TI y procesos de COBIT 5[48]:

Figura 23—Mapeo entre las Metas Relacionadas con las TI de COBIT 5 y los Procesos

			Meta relacionada con las TI																
			Alineamiento de TI y la estrategia de negocio	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	Riesgos de negocio relacionados con las TI gestionados	Realización de beneficios del portafolio de inversiones y Servicios relacionados con las TI	Transparencia de los costes, beneficios y riesgos de las TI	Entrega de servicios de TI de acuerdo a los requisitos del negocio	Uso adecuado de aplicaciones, información y soluciones tecnológicas	Agilidad de las TI	Seguridad de la información, infraestructura de procesamiento y aplicaciones	Optimización de activos, recursos y capacidades de las TI	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio	Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad	Disponibilidad de información útil y relevante para la toma de decisiones	Cumplimiento de las políticas internas por parte de las TI	Personal del negocio y de las TI competente y motivado	Conocimiento, experiencia e iniciativas para la innovación de negocio
			01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17
	Procesos de COBIT 5		Financiera						Cliente		Interna							Aprendizaje y Crecimiento	
Evaluar, Orientar y Supervisar	EDM01	Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno	P	S	P	S	S	S	P		S	S	S	S	S	S	S	S	S
	EDM02	Asegurar la Entrega de Beneficios	P		S		P	P	P	S			S	S	S	S		S	P
	EDM03	Asegurar la Optimización del Riesgo	S	S	S	P		P	S	S		P			S	S	P	S	S
	EDM04	Asegurar la Optimización de los Recursos	S		S	S	S	S	S	S	P		P		S			P	S
	EDM05	Asegurar la Transparencia hacia las partes interesadas	S	S	P			P	P						S	S	S		S
Alinear, Planificar y Organizar	APO01	Gestionar el Marco de Gestión de TI	P	P	S	S			S		P	S	P	S	S	S	P	P	P
	APO02	Gestionar la Estrategia	P		S	S	S		P	S	S		S	S	S	S	S	S	P
	APO03	Gestionar la Arquitectura Empresarial	P		S	S	S	S	S	S	P	S	P	S		S			S
	APO04	Gestionar la Innovación	S			S	P			P	P		P	S		S			P
	APO05	Gestionar el portafolio	P		S	S	P	S	S	S	S		S		P				S
	APO06	Gestionar el Presupuesto y los Costes	S		S	S	P	P	S	S			S		S				
	APO07	Gestionar los Recursos Humanos	P	S	S	S			S		S	S	P		P		S	P	P
	APO08	Gestionar las Relaciones	P		S	S	S	S	P	S			S	P	S		S	S	P
	APO09	Gestionar los Acuerdos de Servicio	S			S	S	S	P	S	S	S	S		S	P	S		
	APO10	Gestionar los Proveedores		S		P	S	S	P	S	P	S	S		S	S	S		S
	APO11	Gestionar la Calidad	S	S		S	P		P	S	S		S		P	S	S	S	S
	APO12	Gestionar el Riesgo		P		P		P	S	S	S	P			P	S	S	S	S
	APO13	Gestionar la Seguridad		P		P		P	S	S		P				P			

[48] ISACA, *COBIT 5 Un Marco de Negocio para el Gobierno y la Gestión de la empresa*, USA, ISACA, 2012. Pág. 52, 53.

Figura 23—Mapeo entre las Metas Relacionadas con las TI de COBIT 5 y los Procesos *(cont.)*

			Meta relacionada con las TI																
			Alineamiento de TI y la estrategia de negocio	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	Riesgos de negocio relacionados con las TI gestionados	Realización de beneficios del portafolio de inversiones y Servicios relacionados con las TI	Transparencia de los costes, beneficios y riesgos de las TI	Entrega de servicios de TI de acuerdo a los requisitos del negocio	Uso adecuado de aplicaciones, información y soluciones tecnológicas	Agilidad de las TI	Seguridad de la información, infraestructura de procesamiento y aplicaciones	Optimización de activos, recursos y capacidades de las TI	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio	Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad;	Disponibilidad de información útil y relevante para la toma de decisiones	Cumplimiento de las políticas internas por parte de las TI	Personal del negocio y de las TI competente y motivado	Conocimiento, experiencia e iniciativas para la innovación de negocio
			01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17
Procesos de COBIT 5			Financiera						Cliente		Interna							Aprendizaje y Crecimiento	
Construcción, Adquisición e Implementación	BAI01	Gestionar los Programas y Proyectos	P		S	P	P	S	S	S			S		P			S	S
	BAI02	Gestionar la Definición de Requisitos	P	S	S	S	S		P	S	S	S	S	P	S	S			S
	BAI03	Gestionar la Identificación y la Construcción de Soluciones	S			S	S		P	S			S	S	S	S			S
	BAI04	Gestionar la Disponibilidad y la Capacidad				S	S		P	S	S		P		S	P			S
	BAI05	Gestionar la introducción de Cambios Organizativos	S		S		S		S	P	S		S	S	P				P
	BAI06	Gestionar los Cambios			S	P	S		P	S	S	P	S	S	S	S	S		S
	BAI07	Gestionar la Aceptación del Cambio y de la Transición				S	S		S	P	S			P	S	S	S		S
	BAI08	Gestionar el Conocimiento	S				S		S	S	P	S	S			S		S	P
	BAI09	Gestionar los Activos		S		S		P	S		S	S	P			S	S		
	BAI10	Gestionar la Configuración		P		S		S		S	S	S	P			P	S		
Entregar, dar Servicio y Soporte	DSS01	Gestionar las Operaciones		S		P	S		P	S	S	S	P			S	S	S	S
	DSS02	Gestionar las Peticiones y los Incidentes del Servicio				P			P	S		S				S	S		S
	DSS03	Gestionar los Problemas		S		P	S		P	S	S		P	S		P	S		S
	DSS04	Gestionar la Continuidad	S	S		P	S		P	S	S	S	S	S		P	S	S	S
	DSS05	Gestionar los Servicios de Seguridad	S	P		P			S	S		P	S	S		S	S		
	DSS06	Gestionar los Controles de los Procesos del Negocio		S		P			P	S		S	S	S		S	S	S	S
Supervisión, Evaluación y Verificación	MEA01	Supervisar, Evaluar y Valorar Rendimiento y Conformidad	S	S	S	P	S	S	P	S	S	S	P		S	S	P	S	S
	MEA02	Supervisar, Evaluar y Valorar el Sistema de Control Interno		P		P		S	S	S		S				S	P		S
	MEA03	Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos		P		P	S		S			S					S		S

ANEXO C: Cuestionarios de evaluación de los Catalizadores de COBIT 5[49]

1. Principios, políticas y marcos de referencia

Dimensión	Aspectos a evaluar	Puntuación
Grupos de interés	La organización ha establecido principios y políticas de comportamiento para su personal	85
	La organización ha adoptado marcos de referencia para la gestión de su negocio	85
	Los principios, políticas y marcos de referencia recogen las necesidades de las partes interesadas internas y externas	50
	Están identificados formalmente los responsables de su definición y mantenimiento	85
	Están identificados formalmente los responsables del monitoreo de su cumplimiento	25
	Están identificados formalmente los responsables de su supervisión	25
25%	**PROMEDIO:**	**59.17**
Metas	Los principios son limitados en número	85
	Los principios expresan los valores fundamentales y éticos de la empresa y están redactados en lenguaje sencillo	100
	Las políticas son efectivas, eficientes y no intrusivas	50
	Las políticas están disponibles y ampliamente difundidas	25
	Se han definido objetivos y métricas para evaluar el rendimiento de los principios, políticas y marcos de trabajo	25
	Se mide periódicamente el cumplimiento de los objetivos y métricas establecidos y se toman acciones correctivas	10
15%	**PROMEDIO:**	**49.17**
Ciclo de vida	Las políticas y marcos de trabajo se actualizan periódicamente o siempre que existen nuevos requerimientos normativos	25
	Existen mecanismos sólidos que garantizan que las personas están al corriente de las novedades	25
	Existen procedimientos adecuados para difundir oportunamente las políticas y marcos de trabajo al personal y medir su cumplimiento	15
20%	**PROMEDIO:**	**21.67**
Buenas prácticas	Las políticas se ciñen a los principios y valores institucionales	50
	Para todas las políticas, está establecido su alcance y validez	25
	Las consecuencias por el no cumplimiento de las políticas están definidas formalmente	50
	En los casos necesarios, se han establecido las excepciones que se pueden considerar en el cumplimiento de las políticas	25
	Las políticas están alineadas con el umbral de riesgo de la organización	25
40%	**PROMEDIO:**	**35.00**
	PUNTAJE TOTAL:	**40.50**

[49] Los valores colocados en la columna "Puntuación" son solo ejemplos de evaluación de cada aspecto de las dimensiones, cuya participación en el cálculo del Puntaje Total fue explicado detalladamente en la sección 2.2 del capítulo 2.

2. Procesos

Dimensión	Aspectos a evaluar	Puntuación
Grupos de interés	El diseño del proceso recoge las necesidades de provisión de información, ejecución, control y rendición de cuentas de las partes interesadas internas	100
	El diseño del proceso recoge las necesidades de provisión de información, ejecución, control y rendición de cuentas de las partes interesadas externas	85
	Están identificados formalmente los responsables de su diseño y actualización	50
	Están identificados formalmente los responsables de su ejecución, provisión de información y rendición de cuentas (matriz RACI)	50
20%	**PROMEDIO:**	**71.25**
Metas	Están definidas formalmente metas a ser cumplidas por el proceso	25
	La ejecución del proceso agrega valor al negocio (es relevante)	25
	El proceso es comprensible y fácil de aplicar	25
	El proceso se particulariza y se adapta a la situación específica de la empresa	25
	El proceso se mantiene confidencial y, cuando se requiere, está a disposición de quien tiene la necesidad	25
	Están definidas formalmente métricas de cumplimiento de las metas, válidas para gestionar la calidad del proceso	25
20%	**PROMEDIO:**	**25.00**
Ciclo de vida	El proceso se actualiza para adaptarse a cambios que se producen en el negocio	25
	En su definición y ejecución, se ha considerado la alineación a los objetivos empresariales	10
	Existen mecanismos sólidos que garantizan que los cambios se difunden y las personas están al corriente de los mismos	25
	Existen mecanismos de supervisión y optimización del proceso	25
25%	**PROMEDIO:**	**21.25**
Buenas prácticas	El ciclo de vida del proceso se basa en estándares o buenas prácticas	50
	Las prácticas y procedimientos se definen para proporcionar beneficios, así como para optimizar riesgos y el uso de recursos	15
	Están definidas y documentadas las entradas que requiere el proceso para su ejecución	25
	Están definidas y documentadas las salidas que produce el proceso, así como sus destinatarios autorizados	75
	Se aplican buenas prácticas para evaluar periódicamente la capacidad del proceso	25
35%	**PROMEDIO:**	**38.00**
	PUNTAJE TOTAL:	**37.86**

3. Estructuras organizacionales

Dimensión	Aspectos a evaluar	Puntuación
Grupos de interés	La estructura organizacional se encuentra formalmente documentada, aprobada y actualizada	100
	La estructura organizacional refleja los niveles de autoridad y responsabilidad para la toma de decisiones, apoyo y asesoría que requiere la organización para el logro de sus objetivos	25
	El diseño de la estructura organizacional recoge las necesidades de las partes interesadas internas y externas, incluyendo entidades organizativas, clientes, proveedores y reguladores	25
	Están identificados formalmente los responsables de su definición y mantenimiento	25
15%	**PROMEDIO:**	**43.75**
Metas	La estructura organizacional refleja las necesidades operacionales de los procesos y objetivos organizacionales	25
	La estructura organizacional permite la segregación de funciones y facilita un adecuado sistema de control interno	25
	La estructura organizacional y su documentación están actualizadas y disponibles para todos los interesados	50
	La interacción entre unidades organizacionales está claramente identificada y documentada a través de los procesos	25
25%	**PROMEDIO:**	**31.25**
Ciclo de vida	Se documenta y se aprueba una razón y un propósito para la creación o ajuste de una estructura organizacional	25
	Periódicamente, o ante requerimientos normativos, se efectúan revisiones y actualizaciones de la estructura organizacional	75
	Las creaciones, ajustes y eliminaciones organizacionales son aprobados y difundidos oportunamente a los interesados	25
30%	**PROMEDIO:**	**41.67**
Buenas prácticas	Se aplican principios operativos y de funcionamiento de la estructura, como frecuencia de reuniones, documentación y reglas de mantenimiento	50
	Las estructuras tienen miembros, los cuales son partes interesadas internas o externas reconocidas	25
	Los límites de los derechos de decisión de la estructura organizativa están claramente identificados.	25
	Están definidos, actualizados y se aplican niveles de autorización y/o derechos de decisión	10
	La estructura puede delegar (un subconjunto de) sus derechos de decisión a otras estructuras dependientes que le reportan.	50
	La ruta de escalamiento para una estructura organizacional describe las acciones requeridas en caso de problemas en la toma de decisiones.	5
30%	**PROMEDIO:**	**27.50**
	PUNTAJE TOTAL:	**35.13**

4. Cultura, ética y comportamiento

Dimensión	Aspectos a evaluar	Puntuación
Grupos de interés	Existen responsables de definir, implementar y reforzar comportamientos deseados en el personal	100
	El personal conoce oportunamente el alcance y la vigencia de los comportamientos esperados	25
	Existen responsables de supervisar el alineamiento del personal con las reglas y normas definidas	25
15%	**PROMEDIO:**	**50.00**
Metas	Está formalmente aprobado y difundido a todo el personal un código de ética organizacional, o un documento equivalente, que se alinea con los principios y valores por los cuales la empresa quiere subsistir	25
	Dentro del proceso de selección del personal se analizan factores externos tales como religión, origen étnico, antecedentes socioeconómicos, demográficos, y experiencias personales, para garantizar que el personal se enmarca dentro de la ética y cultura organizacional	25
	Existe una cultura de riesgos en la que se ha definido y aprobado un nivel de tolerancia y un umbral para todos los tipos de riesgo, que rigen la toma de riesgos	25
	Existe una cultura organizacional sólida frente a la aceptación y cumplimiento de políticas y normas internas y externas	25
	Para la organización, los resultados negativos son oportunidades de aprendizaje, corrección y mejoramiento	25
25%	**PROMEDIO:**	**25.00**
Ciclo de vida	El comportamiento ético, organizacional e individual están identificados y aceptados por todos los interesados	100
	Existen procedimientos oportunos y efectivos de comunicación y concientización de la cultura organizacional	25
	Se analizan, actualizan y difunden periódicamente los lineamientos que rigen el comportamiento, la ética y la cultura organizacional	25
20%	**PROMEDIO:**	**50.00**
Buenas prácticas	Existe una efectiva comunicación a lo largo de toda la empresa de los comportamientos deseados y los valores corporativos	100
	Se promueve la concienciación de los comportamientos deseados, fortalecidos por la conducta ejemplar de los gerentes de mayor cargo y otros líderes	100
	Existen incentivos para fomentar y elementos disuasivos para hacer cumplir los comportamientos deseados	100
	Existe consistencia entre el comportamiento individual y el esquema de recompensas de recursos humanos que la empresa ha implementado	25
	Están documentadas y actualizadas las reglas y normas que guían el comportamiento organizativo deseado, y se vinculan en forma muy clara con los principios y políticas de la empresa	25
40%	**PROMEDIO:**	**70.00**
	PUNTAJE TOTAL:	**51.75**

5. Información

Dimensión	Aspectos a evaluar	Puntuación
Grupos de interés	Están identificados y documentados los productores de datos o información, internos y externos	100
	Están identificados y documentados los custodios de datos o información, internos y externos	25
	Están identificados y documentados los consumidores de datos o información, internos y externos, y los niveles de acceso que deben tener.	25
15%	**PROMEDIO:**	**50.00**
Metas	Dentro de la calidad intrínseca de la información, se considera el grado en que los valores de los datos están en conformidad con los valores reales o verdaderos, en cuanto a: precisión, objetividad, credibilidad y reputación	25
	Dentro de la calidad contextual de la información, se considera el grado en que la información es aplicable a la tarea del usuario y es presentada en una manera clara e inteligible, incluyendo: relevancia, completitud, vigencia, cantidad, representación concisa, representación consistente, interpretabilidad, comprensibilidad y facilidad de manipulación.	25
	Se mide el grado en que la información está disponible cuando se requiera, o que es rápida y fácilmente recuperable	25
	Se mide el grado en que el acceso a la información se restringe adecuadamente a las partes autorizadas	25
25%	**PROMEDIO:**	**25.00**
Ciclo de vida	Se planifica la creación y uso del recurso información, incluyendo la identificación de objetivos, la planificación de la arquitectura de la información y el desarrollo de estándares y definiciones, p. ej., procedimientos de recolección de datos	100
	Existe un procedimiento participativo para el diseño de la información, tomando en cuenta las necesidades de las partes interesadas, así como los criterios de calidad intrínseca, calidad contextual, accesibilidad y disponibilidad	50
	Existe una fase de construcción o adquisición de información, que incluye la creación de registros de datos, la compra de datos y la carga de archivos externos, sobre la cual se aplican controles de validación de ingreso o carga de datos	25
	Se han implementado adecuados controles para las actividades en que se almacena, comparte y usa la información, para garantizar las metas de la información y el cumplimiento interno y externo	25
	Continuamente se realizan procedimientos de supervisión para comprobar que la información está actualizada, así como para la mejora, limpieza, fusión, y eliminación de datos duplicados de la información, en los casos que aplique	50
	Se detecta cuando la información ya no es útil, y se aplican procedimientos seguros para su eliminación o desecho	50
40%	**PROMEDIO:**	**50.00**
Buenas prácticas	Las inversiones en información y tecnologías relacionadas se basan en casos de negocio, que incluyen análisis costo-beneficio y factores tangibles e intangibles	100
	Cuando se requiere valorar la información, se lo hace a través de la identificación de su uso	100
	Para el diseño de aplicativos o sistemas, se analizan los atributos de la información, tales como: • Capa física—¿Dónde se almacenará la información? • Capa empírica—¿Cómo se puede acceder a la información? • Capa sintáctica—¿Cómo se estructurará y codificará la información? • Capa semántica—¿Qué tipo de información es? ¿Cuál es el nivel de información? • Capa pragmática—¿Cuáles son los requisitos de retención? ¿Qué otra información es necesaria para que esta información sea útil y utilizable?	50
20%	**PROMEDIO:**	**83.33**
	PUNTAJE TOTAL:	**50.42**

6. Servicios, Infraestructura y Aplicaciones

Dimensión	Aspectos a evaluar	Puntuación
Grupos de interés	Están identificadas y documentadas las partes interesadas internas que proveen servicios, infraestructura y aplicaciones	100
	Están identificadas y documentadas las partes interesadas externas que proveen servicios, infraestructura y aplicaciones	25
	Están identificadas y documentadas las partes interesadas internas que requieren servicios, infraestructura y aplicaciones	15
	Están identificadas y documentadas las partes interesadas externas que requieren servicios, infraestructura y aplicaciones	25
15%	**PROMEDIO:**	**41.25**
Metas	Están identificados todos los servicios, infraestructura, tecnología y aplicaciones que requieren los procesos de negocio	25
	Están definidos y acordados los niveles de servicio requeridos por los procesos de negocio	25
	Existen métricas que permiten medir el nivel de servicio prestado efectivamente a los procesos de negocio, por cada uno de los servicios	25
	Periódicamente se mide el nivel de contribución de los servicios, infraestructura, tecnología y aplicaciones a los procesos de negocio	25
25%	**PROMEDIO:**	**25.00**
Ciclo de vida	Cuando se planifica la capacidad de un nuevo servicio, se lo hace en función de las partes interesadas identificadas	25
	Para cada nuevo servicio, se diseña una arquitectura objetivo que cubre los bloques constituyentes, tales como futuras aplicaciones y el modelo de infraestructura objetivo y también describe los vínculos y las relaciones entre estos bloques de construcción	
	Las capacidades de servicio actuales están documentados en una arquitectura de base	25
	Cuando se construye/adquiere e implementa un nuevo servicio, se considera la documentación de una arquitectura de transición, que muestre la empresa en estados incrementales entre el objetivo y la arquitectura de referencia	25
	Existen responsables formalmente designados para la supervisión y aplicación de medidas correctivas ante desviaciones de los niveles de servicio acordados	25
	Se identifica oportunamente cuando un servicio ya no es requerido o requiere ajustes, y se lo elimina y/o actualiza su documentación	25
35%	**PROMEDIO:**	**25.00**
Buenas prácticas	Existen principios de arquitectura que rigen la implementación y utilización de los recursos relacionados con las TI dentro de la empresa, tales como reutilización, comprar frente a construir, simplicidad, agilidad, apertura	50
	Como definición empresarial, se utilizan las herramientas, modelos o diagramas más adecuados para mostrar las soluciones que satisfacen las necesidades de los diferentes interesados	25
	Se dispone de un repositorio de arquitectura, que se utiliza para almacenar diferentes tipos de productos arquitectónicos, incluyendo los principios de la arquitectura y estándares, modelos de arquitectura de referencia, etc., y que define los bloques que componen los servicios tales como: • Las aplicaciones que proporcionan la funcionalidad empresarial • La infraestructura tecnológica, incluyendo el hardware, el software del sistema y la infraestructura de redes • La infraestructura física	25
	Se definen y monitorean los niveles de servicio que deben ser definidos y alcanzados por los proveedores de servicio	25
	Se aplican otras buenas prácticas, tales como las sugeridas por TOGAF e ITIL para la prestación de servicios de TI	25
25%	**PROMEDIO:**	**30.00**
	PUNTAJE TOTAL:	**28.69**

7. Personas, Habilidades y Competencias

Dimensión	Aspectos a evaluar	Puntuación
Grupos de interés	Se toman en cuenta las capacidades y competencias de todas las partes interesadas internas: directivos, gerentes de proyectos, socios, reclutadores, desarrolladores, técnicos de TI, etc., para que sean asignados y asuman los diferentes roles	100
	Se toman en cuenta las capacidades y competencias de todas las partes interesadas externas: competidores, proveedores, reguladores, auditores externos, financistas, etc., para la ejecución de los procesos y proyectos de la organización	25
15%	**PROMEDIO:**	**62.5**
Metas	Los cargos del personal se diseñan en función de las necesidades de conocimientos, experiencia y comportamiento que requiere la organización	85
	Existen requisitos objetivos de formación para cada papel desempeñado por las distintas partes interesadas	100
	Se realizan mediciones del volumen de negocios frente a la capacidad actual de cada proceso para la asignación del número adecuado de personal	50
	Existen mecanismos de administración del personal que permiten garantizar su disponibilidad	25
25%	**PROMEDIO:**	**65.00**
Ciclo de vida	La empresa determina cuál es su base de conocimientos actual y planifica lo que tiene que ser, según influyan la estrategia y metas organizacionales, competitividad, mercado, etc., y establece la brecha existente	85
	Se desarrollan o adquieren las habilidades y competencias necesarias para cerrar la brecha encontrada en el personal	85
	Se eliminan las habilidades y competencias que ya no sean necesarias en la organización	25
	Al menos anualmente, se evalúan las competencias básicas para entender la evolución que se ha producido, y que se utilizará en el proceso de planificación del próximo período	25
	La evaluación periódica de competencias se utiliza como un insumo para la compensación y reconocimiento al personal	50
35%	**PROMEDIO:**	**54.00**
Buenas prácticas	Para cada cargo, están definidas las metas de habilidades y competencias, tales como niveles de educación y capacitación, habilidades técnicas, niveles de experiencia, conocimientos y habilidades de comportamiento necesarios para llevar a cabo con éxito las actividades del cargo	50
	La organización utiliza diversos niveles de habilidad para las diferentes categorías profesionales	25
	Está definido el nivel de habilidad apropiado en cada categoría profesional, y una definición de las cualificaciones	25
25%	**PROMEDIO:**	**33.33**
	PUNTAJE TOTAL:	**52.86**

ANEXO D: Mapeo de los requerimientos de la norma de Gestión del Riesgo Operativo de la SBS y las prácticas clave de COBIT 5

		Proceso de COBIT		Práctica clave
No.	Personas			
1	Personas.- Las instituciones controladas deben administrar el capital humano de forma adecuada, e identificar apropiadamente las fallas o insuficiencias asociadas al factor “personas”, tales como: falta de personal adecuado, negligencia, error humano, nepotismo de conformidad con las disposiciones legales vigentes, inapropiadas relaciones interpersonales y ambiente laboral desfavorable, falta de especificaciones claras en los términos de contratación del personal, entre otros.	**APO07**	Administrar los Recursos Humanos Catalizador Personas, habilidades y competencias	APO07.01
2	Dichos procesos corresponden a: 4.2.1 Los procesos de incorporación.- Que comprenden la planificación de necesidades, el reclutamiento, la selección, la contratación e inducción de nuevo personal;	**APO07**	Administrar los Recursos Humanos	APO07.01, APO07.05 Planificar y realizar un seguimiento del uso de recursos humanos de TI y del negocio.
3	4.2.2 Los procesos de permanencia.- Que cubren la creación de condiciones laborales idóneas; la promoción de actividades de capacitación y formación que permitan al personal aumentar y perfeccionar sus conocimientos, competencias y destrezas; la existencia de un sistema de evaluación del desempeño; desarrollo de carrera; rendición de cuentas; e incentivos que motiven la adhesión a los valores y controles institucionales; y,	**APO07**	Administrar los Recursos Humanos	APO07.03, APO07.04, APO07.06
4	4.2.3 Los procesos de desvinculación.- Que comprenden la planificación de la salida del personal por causas regulares, preparación de aspectos jurídicos para llegar al finiquito y la finalización de la relación laboral.	**APO07**	Administrar los Recursos Humanos	APO07.02 Identificar personal clave de TI.
5	Los procesos de incorporación, permanencia y desvinculación antes indicados deberán ser soportados técnicamente, ajustados a las disposiciones legales y transparentes para garantizar condiciones laborales idóneas.	**APO07**	Administrar los Recursos Humanos	APO07.01 Mantener la dotación de personal suficiente y adecuada.
6	Las instituciones controladas deberán analizar su organización con el objeto de evaluar si han definido el personal necesario y las competencias idóneas para el desempeño de cada puesto, considerando no sólo experiencia profesional, formación académica, sino también los valores, actitudes y habilidades personales que puedan servir como criterio para garantizar la excelencia institucional.	**APO07**	Administrar los Recursos Humanos Catalizador Personas, habilidades y competencias Catalizador Cultura, ética y comportamiento	APO07.03, APO07.04, APO07.06
7	Las instituciones controladas mantendrán información actualizada del capital humano, que permita una adecuada toma de decisiones por parte de los niveles directivos y la realización de análisis cualitativos y cuantitativos de acuerdo con sus necesidades.	**APO07**	Administrar los Recursos Humanos	APO07.05 Planificar y realizar un seguimiento del uso de recursos humanos de TI y del negocio.

8	Dicha información deberá referirse al personal existente en la institución; a la formación académica y experiencia; a la forma y fechas de selección, reclutamiento y contratación; información histórica sobre los eventos de capacitación en los que han participado; cargos que han desempeñado en la institución; resultados de evaluaciones realizadas; fechas y causas de separación del personal que se ha desvinculado de la institución; y, otra información que la institución controlada considere pertinente.	**APO07**	Administrar los Recursos Humanos	APO07.05 Planificar y realizar un seguimiento del uso de recursos humanos de TI y del negocio.
	Requerimientos de operación			
9	1.1 El apoyo y compromiso formal del directorio u organismo que haga sus veces y la alta gerencia;	**EDM01**	EDM01 Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno	EDM01.01 Evaluar el sistema de gobierno.
10	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;	**APO02**	Administrar la Estrategia	APO02.05 Definir el plan estratégico y la hoja de ruta
11	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;	**APO02**	Administrar la Estrategia	APO02.03 Definir el objetivo de las capacidades de TI, APO02.04 Realizar un análisis de diferencias.
12	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;	**DSS06**	Administrar los Controles de Procesos del Negocio	DSS06.02 Controlar el procesamiento de la información. DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.
13	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;	**APO01**	Administrar el marco de trabajo de Administración de TI Catalizador Principios, Políticas y Marcos de trabajo	APO01.03 Mantener los elementos catalizadores del sistema de gestión.
14	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,	**APO01**	Administrar el marco de trabajo de Gestión de TI Catalizador Principios, Políticas y Marcos de trabajo	APO01.03 Mantener los elementos catalizadores del sistema de gestión.
15	1.7 Capacitación y entrenamiento técnico al personal del área de tecnología de información y de los usuarios de la misma.	**APO07**	Administrar los Recursos Humanos	APO07.03 Mantener las habilidades y competencias del personal.
	Operaciones de tecnología			

16	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;	**DSS01**	Administrar las Operaciones	DSS01.01 Ejecutar procedimientos operativos
17	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;	**APO01**	Administrar el marco de trabajo de Gestión de TI	APO01.06 Definir la propiedad de la información (datos) y del sistema.
	Recursos y servicios provistos por terceros			
18	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,	**APO10**	Administrar los proveedores	APO10.02 Seleccionar proveedores.
19	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.	**APO10**	Administrar los proveedores	APO10.02 Seleccionar proveedores.
	Sistema de administración de seguridad			
20	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;	**APO13**	Administrar la Seguridad	APO13.01 Establecer y mantener un SGSI.
21	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;	**APO13**	Administrar la Seguridad	APO13.02 Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información.
22	4.3 Los controles necesarios para asegurar la integridad, disponibilidad y confidencialidad de la información administrada;	**APO13**	Administrar la Seguridad	APO13.02 Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información.
23	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;	**DSS05**	Administrar los Servicios de Seguridad	DSS05.04 Gestionar la identidad del usuario y el acceso lógico.
24	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;	**DSS05**	Administrar los Servicios de Seguridad	DSS05.04 Gestionar la identidad del usuario y el acceso lógico.

25	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;	**DSS05**	Administrar los Servicios de Seguridad	DSS05.02 Gestionar la seguridad de la red y las conexiones. DSS05.05 Gestionar el acceso físico a los activos de TI.
26	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;	**DSS05**	Administrar los Servicios de Seguridad	DSS05.01 Proteger contra software malicioso (malware).
		BAI09	Administrar los Activos	BAI09.05 Administrar licencias.
27	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;	**DSS05**	Administrar los Servicios de Seguridad	DSS05.03 Gestionar la seguridad de los puestos de usuario final. DSS05.02 Gestionar la seguridad de la red y las conexiones. DSS05.05 Gestionar el acceso físico a los activos de TI.
28	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;	**DSS05**	Administrar los Servicios de Seguridad	DSS05.05 Gestionar el acceso físico a los activos de TI.
29	4.10 Las condiciones físicas y ambientales necesarias para garantizar el correcto funcionamiento del entorno de la infraestructura de tecnología de información;	**DSS01**	Administrar las Operaciones	DSS01.04 Gestionar el entorno. DSS01.05 Gestionar las instalaciones
30	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,	**APO13**	Administrar la Seguridad	APO13.03 Supervisar y revisar el SGSI.
31	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.	**DSS05**	Administrar los Servicios de Seguridad	DSS05.04 Gestionar la identidad del usuario y el acceso lógico. DSS05.02 Gestionar la seguridad de la red y las conexiones.
		DSS04	Administrar la Continuidad	DSS04.02 Mantener una estrategia de continuidad. DSS04.03 Desarrollar e implementar una respuesta a la continuidad del negocio.
	Continuidad de las operaciones			
32	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;	**DSS01**	Administrar las Operaciones	DSS01.04 Gestionar el entorno. DSS01.05 Gestionar las instalaciones
33	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;	**DSS04**	Administrar la Continuidad	DSS04.07 Gestionar acuerdos de respaldo.
34	5.3 Mantener los sistemas de comunicación y redundancia de los mismos que permitan garantizar la continuidad de sus servicios; y,	**DSS01**	Administrar las Operaciones	DSS01.05 Gestionar las instalaciones
35	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.	**DSS04**	Administrar la Continuidad	DSS04.02 Mantener una estrategia de continuidad. DSS04.03 Desarrollar e implementar una respuesta a la

				continuidad del negocio.
	Adquisición y mantenimiento de aplicaciones			
36	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;	**BAI02**	Administrar la Definición de Requerimientos	BAI02.02 Realizar un estudio de viabilidad y proponer soluciones alternativas.
37	6.2 Documentación técnica y de usuario permanentemente actualizada de las aplicaciones de la institución;	**BAI05**	Administrar la Habilitación del Cambio Organizacional	BAI05.05 Facilitar la operación y el uso.
38	6.3 Controles que permitan asegurar la adecuada administración de versiones de las aplicaciones puestas en producción; y,	**BAI07**	Administrar la Aceptación y Transición del Cambio	BAI07.06 Pasar a producción y gestionar los lanzamientos.
39	6.4 Controles que permitan asegurar que la calidad de la información sometida a migración, cumple con las características de integridad, disponibilidad y confidencialidad.	**BAI07**	Administrar la Aceptación y Transición del Cambio	BAI07.02 Planificar la conversión de procesos de negocio, sistemas y datos.
	Infraestructura tecnológica			
40	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.	**BAI09**	Administrar los Activos	BAI09.02 Gestionar activos críticos
		DSS01	Administrar las Operaciones	DSS01.03 Supervisar la infraestructura de TI
		BAI10	Administrar la Configuración	BAI10.02 Establecer y mantener un repositorio de configuración y una base de referencia.
	Seguridad en canales electrónicos			
41	**4.3.8.1.** Las instituciones del sistema financiero deberán adoptar e implementar los estándares y buenas prácticas internacionales de seguridad vigentes a nivel mundial para el uso y manejo de canales electrónicos y consumos con tarjetas, los cuales deben ser permanentemente monitoreados para asegurar su cumplimiento;	**APO13**	Administrar la Seguridad	APO13.01 Establecer y mantener un SGSI.
42	**4.3.8.2.** Establecer procedimientos y mecanismos para monitorear de manera periódica la efectividad de los niveles de seguridad implementados en hardware, software, redes y comunicaciones, así como en cualquier otro elemento electrónico o tecnológico utilizado en los canales electrónicos, de tal manera que se garantice permanentemente la seguridad y calidad de la información;	**DSS05**	Administrar los Servicios de Seguridad	DSS05.01 Proteger contra software malicioso (malware). DSS05.02 Gestionar la seguridad de la red y las conexiones. DSS05.07 Supervisar la infraestructura para detectar eventos relacionados con la seguridad.
43	**4.3.8.3.** El envío de información confidencial de sus clientes y la relacionada con tarjetas, debe ser realizado bajo condiciones de seguridad de la información, considerando que cuando dicha información se envíe mediante correo electrónico o utilizando algún otro medio vía Internet, ésta deberá estar sometida a técnicas de encriptación acordes con los estándares internacionales vigentes;	**APO01**	Administrar el marco de trabajo de Gestión de TI	APO01.06 Definir la propiedad de la información (datos) y del sistema.
		DSS05	Administrar los Servicios de Seguridad	DSS05.02 Gestionar la seguridad de la red y las conexiones.
44	**4.3.8.4.** La información que se transmita entre el canal electrónico y el sitio principal de procesamiento de la entidad, deberá estar en todo momento protegida mediante el uso de técnicas de encriptación y deberá evaluarse con regularidad la efectividad y vigencia del mecanismo de encriptación utilizado;	**DSS05**	Administrar los Servicios de Seguridad	DSS05.02 Gestionar la seguridad de la red y las conexiones.

45	**4.3.8.5.** Las instituciones del sistema financiero deberán contar en todos sus canales electrónicos con software antimalware que esté permanentemente actualizado, el cual permita proteger el software instalado, detectar oportunamente cualquier intento o alteración en su código, configuración y/o funcionalidad, y emitir las alarmas correspondientes para el bloqueo del canal electrónico, su inactivación y revisión oportuna por parte de personal técnico autorizado de la institución;	**DSS05**	Administrar los Servicios de Seguridad	DSS05.01 Proteger contra software malicioso (malware).
46	**4.3.8.6.** Las instituciones del sistema financiero deberán utilizar hardware de propósito específico para la generación y validación de claves para ejecutar transacciones en los diferentes canales electrónicos y dicha información no deberá ser almacenada en ningún momento;	**DSS05**	Administrar los Servicios de Seguridad	DSS05.04 Gestionar la identidad del usuario y el acceso lógico. DSS05.06 Gestionar documentos sensibles y dispositivos de salida.
47	**4.3.8.7.** Establecer procedimientos para monitorear, controlar y emitir alarmas en línea que informen oportunamente sobre el estado de los canales electrónicos, con el fin de identificar eventos inusuales, fraudulentos o corregir las fallas;	**DSS01**	Administrar las Operaciones	DSS01.03 Supervisar la infraestructura de TI
		DSS05	Administrar los Servicios de Seguridad	DSS05.07 Supervisar la infraestructura para detectar eventos relacionados con la seguridad.
48	**4.3.8.8**. Ofrecer a los clientes los mecanismos necesarios para que personalicen las condiciones bajo las cuales desean realizar sus transacciones a través de los diferentes canales electrónicos y tarjetas, dentro de las condiciones o límites máximos que deberá establecer cada entidad. Entre las principales condiciones de personalización por cada tipo de canal electrónico, deberán estar: registro de las cuentas a las cuales desea realizar transferencias, registro de direcciones IP de computadores autorizados, el ó los números de telefonía móvil autorizados, montos máximos por transacción diaria, semanal y mensual, entre otros. Para el caso de consumos con tarjetas, se deberán personalizar los cupos máximos, principalmente para los siguientes servicios: consumos nacionales, consumos en el exterior, compras por internet, entre otros;	**BAI02**	Administrar la Definición de Requerimientos	BAI02.01 Definir y mantener los requerimientos técnicos y funcionales de negocio. BAI02.02 Realizar un estudio de viabilidad y proponer soluciones alternativas.
49	**4.3.8.9.** Incorporar en los procedimientos de administración de seguridad de la información la renovación de por lo menos una vez (1) al año de las claves de acceso a cajeros automáticos; dicha clave deberá ser diferente de aquella por la cual se accede a otros canales electrónicos;	**APO13**	Administrar la Seguridad	APO13.02 Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información.
50	**4.3.8.10.** Las instituciones deberán establecer procedimientos de control y mecanismos que permitan registrar el perfil de cada cliente sobre sus costumbres transaccionales en el uso de canales electrónicos y tarjetas y definir procedimientos para monitorear en línea y permitir o rechazar de manera oportuna la ejecución de transacciones que no correspondan a sus hábitos, lo cual deberá ser inmediatamente notificado al cliente mediante mensajería móvil, correo electrónico, u otro mecanismo;	**APO13**	Administrar la Seguridad	APO13.02 Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información.

51	**4.3.8.11.** Incorporar en los procedimientos de administración de la seguridad de la información, el bloqueo de los canales electrónicos o de las tarjetas cuando se presenten eventos inusuales que adviertan situaciones fraudulentas o después de un número máximo de tres (3) intentos de acceso fallido. Además, se deberán establecer procedimientos que permitan la notificación en línea al cliente a través de mensajería móvil, correo electrónico u otro mecanismo, así como su reactivación de manera segura;	**APO13**	Administrar la Seguridad	APO13.02 Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información.
52	**4.3.8.12.** Asegurar que exista una adecuada segregación de funciones entre el personal que administra, opera, mantiene y en general accede a los dispositivos y sistemas usados en los diferentes canales electrónicos y tarjetas;	**DSS06**	Administrar los Controles de Procesos del Negocio	DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.
53	**4.3.8.13.** Las entidades deberán establecer procedimientos y controles para la administración, transporte, instalación y mantenimiento de los elementos y dispositivos que permiten el uso de los canales electrónicos y de tarjetas;	**DSS05**	Administrar los Servicios de Seguridad	DSS05.05 Gestionar el acceso físico a los activos de TI.
		BAI10	Administrar la Configuración	BAI10.03 Mantener y controlar los elementos de configuración. BAI10.04 Generar informes de estado y configuración. BAI10.05 Verificar y revisar la integridad del repositorio de configuración.
54	**4.3.8.14.** Las instituciones del sistema financiero deben mantener sincronizados todos los relojes de sus sistemas de información que estén involucrados con el uso de canales electrónicos;	**BAI10**	Administrar la Configuración	BAI10.02 Establecer y mantener un repositorio de configuración y una base de referencia.
55	**4.3.8.15.** Mantener como mínimo durante doce (12) meses el registro histórico de todas las operaciones que se realicen a través de los canales electrónicos, el cual deberá contener como mínimo: fecha, hora, monto, números de cuenta (origen y destino en caso de aplicarse), código de la institución del sistema financiero de origen y de destino, número de transacción, código del dispositivo: para operaciones por cajero automático: código del ATM, para transacciones por internet: la dirección IP, para transacciones a través de sistemas de audio respuesta - IVR y para operaciones de banca electrónica mediante dispositivos móviles: el número de teléfono con el que se hizo la conexión. En caso de presentarse reclamos, la información deberá conservarse hasta que se agoten las instancias legales. Si dicha información constituye respaldo contable se aplicará lo previsto en el tercer inciso del artículo 80 de la Ley General de Instituciones del Sistema Financiero;	**DSS04**	Administrar la Continuidad	DSS04.07 Gestionar acuerdos de respaldo.
		BAI02	Administrar la Definición de Requerimientos	BAI02.01 Definir y mantener los requerimientos técnicos y funcionales de negocio.
56	**4.3.8.16.** Incorporar en los procedimientos de administración de la seguridad de la información, controles para impedir que funcionarios de la entidad que no estén debidamente autorizados tengan acceso a consultar información confidencial de los clientes en ambiente de producción. En el caso de información contenida en ambientes de desarrollo y pruebas, ésta deberá ser enmascarada o codificada. Todos estos procedimientos deberán estar debidamente documentados en los manuales respectivos.	**DSS06**	Administrar los Controles de Procesos del Negocio	DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.

57	Además, la entidad deberá mantener y monitorear un log de auditoría sobre las consultas realizadas por los funcionarios a la información confidencial de los clientes, la cual debe contener como mínimo: identificación del funcionario, sistema utilizado, identificación del equipo (IP), fecha, hora, e información consultada. Esta información deberá conservarse por lo menos por doce (12) meses;	**DSS05**	Administrar los Servicios de Seguridad	DSS05.04 Gestionar la identidad del usuario y el acceso lógico.
		DSS06	Administrar los Controles de Procesos del Negocio	DSS06.05 Asegurar la trazabilidad de los eventos y responsabilidades de información.
58	**4.3.8.17.** Las instituciones del sistema financiero deberán poner a disposición de sus clientes un acceso directo como parte de su centro de atención telefónica (call center) para el reporte de emergencias bancarias, el cual deberá funcionar las veinticuatro (24) horas al día, los siete (7) días de la semana;	**DSS02**	Administrar las Solicitudes de Servicio e Incidentes	DSS02.01 Definir esquemas de clasificación de incidentes y peticiones de servicio.
59	**4.3.8.18.** Mantener por lo menos durante seis (6) meses la grabación de las llamadas telefónicas realizadas por los clientes a los centros de atención telefónica (call center), específicamente cuando se consulten saldos, consumos o cupos disponibles; se realicen reclamos; se reporten emergencias bancarias; o, cuando se actualice su información. De presentarse reclamos, esa información deberá conservarse hasta que se agoten las instancias legales;	**DSS05**	Administrar los Servicios de Seguridad	DSS05.04 Gestionar la identidad del usuario y el acceso lógico.
		DSS06	Administrar los Controles de Procesos del Negocio	DSS06.05 Asegurar la trazabilidad de los eventos y responsabilidades de información.
60	**4.3.8.19.** Las entidades deberán implementar los controles necesarios para que la información de claves ingresadas por los clientes mediante los centros de atención telefónica (call center), estén sometidas a técnicas de encriptación acordes con los estándares internacionales vigentes;	**DSS05**	Administrar los Servicios de Seguridad	DSS05.03 Gestionar la seguridad de los puestos de usuario final.
61	**4.3.8.20.** Las instituciones del sistema financiero deberán ofrecer a los clientes el envío en línea a través de mensajería móvil, correo electrónico u otro mecanismo, la confirmación del acceso a la banca electrónica, así como de las transacciones realizadas mediante cualquiera de los canales electrónicos disponibles, o por medio de tarjetas;	**DSS05**	Administrar los Servicios de Seguridad	DSS05.05 Gestionar el acceso físico a los activos de TI.
62	**4.3.8.21.** Las tarjetas emitidas por las instituciones del sistema financiero que las ofrezcan deben ser tarjetas inteligentes, es decir, deben contar con microprocesador o chip; y, las entidades controladas deberán adoptar los estándares internacionales de seguridad y las mejores prácticas vigentes sobre su uso y manejo;	**DSS05**	Administrar los Servicios de Seguridad	DSS05.06 Gestionar documentos sensibles y dispositivos de salida.
63	**4.3.8.22.** Mantener permanentemente informados y capacitar a los clientes sobre los riesgos derivados del uso de canales electrónicos y de tarjetas; y, sobre las medidas de seguridad que se deben tener en cuenta al momento de efectuar transacciones a través de éstos;	**APO12**	Administrar los Riesgos	APO12.04 Expresar el riesgo.
64	**4.3.8.23.** Informar y capacitar permanentemente a los clientes sobre los procedimientos para el bloqueo, inactivación, reactivación y cancelación de los productos y servicios ofrecidos por la entidad;	**BAI05**	Administrar la Habilitación del Cambio Organizacional	BAI05.05 Facilitar la operación y el uso.
65	**4.3.8.24.** Es función de auditoría interna verificar oportunamente la efectividad de las medidas de seguridad que las instituciones del sistema financiero deben implementar en sus canales electrónicos; así también deberán informar sobre las medidas correctivas establecidas en los casos de reclamos de los usuarios financieros que involucren debilidades o violación de los niveles de seguridad;	**MEA03**	Monitorear, Evaluar y Valorar el Cumplimiento con Requerimientos Externos	MEA03.03 Confirmar el cumplimiento de requisitos externos.

66	**4.3.8.25.** Implementar técnicas de seguridad de la información en los procesos de desarrollo de las aplicaciones que soportan los canales electrónicos, con base en directrices de codificación segura a fin de que en estos procesos se contemple la prevención de vulnerabilidades;	**BAI03**	Administrar la Identificación y Construcción de Soluciones	BAI03.02 Diseñar los componentes detallados de la solución. BAI03.03 Desarrollar los componentes de la solución
	Cajeros automáticos			
67	**Cajeros automáticos.-** Con el objeto de garantizar la seguridad en las transacciones realizadas a través de los cajeros automáticos, las instituciones del sistema financiero deberán cumplir como mínimo con lo siguiente: **4.3.9.1.** Los dispositivos utilizados en los cajeros automáticos para la autenticación del cliente o usuario, deben encriptar la información ingresada a través de ellos; y, la información de las claves no debe ser almacenada en ningún momento;	**DSS05**	Administrar los Servicios de Seguridad	DSS05.03 Gestionar la seguridad de los puestos de usuario final. DSS05.06 Gestionar documentos sensibles y dispositivos de salida.
68	**4.3.9.2.** La institución controlada debe implementar mecanismos internos de autenticación del cajero automático que permitan asegurar que es un dispositivo autorizado por la institución del sistema financiero a la que pertenece;	**DSS05**	Administrar los Servicios de Seguridad	DSS05.03 Gestionar la seguridad de los puestos de usuario final.
69	**4.3.9.3.** Los cajeros automáticos deben ser capaces de procesar la información de tarjetas inteligentes o con chip;	**BAI04**	Administrar la Disponibilidad y Capacidad	BAI04.03 Planificar requisitos de servicio nuevos o modificados.
70	**4.3.9.4.** Los cajeros automáticos deben estar instalados de acuerdo con las especificaciones del fabricante, así como con los estándares de seguridad definidos en las políticas de la institución del sistema financiero, incluyendo el cambio de las contraseñas de sistemas y otros parámetros de seguridad provistos por los proveedores;	**BAI09**	Administrar los Activos	BAI09.02 Gestionar activos críticos
		DSS05	Administrar los Servicios de Seguridad	DSS05.03 Gestionar la seguridad de los puestos de usuario final.
71	**4.3.9.5.** Disponer de un programa o sistema de protección contra intrusos (Anti-malware) que permita proteger el software instalado en el cajero automático y que detecte oportunamente cualquier alteración en su código, configuración y/o funcionalidad. Así mismo, se deberán instalar mecanismos que sean capaces de identificar conexiones no autorizadas a través de los puertos USB, comunicaciones remotas, cambio de los discos duros y otros componentes que guarden o procesen información. En una situación de riesgo deben emitir alarmas a un centro de monitoreo o dejar inactivo al cajero automático hasta que se realice la inspección por parte del personal especializado de la institución;	**DSS05**	Administrar los Servicios de Seguridad	DSS05.01 Proteger contra software malicioso (malware).
		BAI10	Administrar la Configuración	BAI10.04 Generar informes de estado y configuración. BAI10.05 Verificar y revisar la integridad del repositorio de configuración.
72	**4.3.9.6.** Establecer y ejecutar procedimientos de auditoría de seguridad en sus cajeros automáticos por lo menos una vez al año, con el fin de identificar vulnerabilidades y mitigar los riesgos que podrían afectar a la seguridad de los servicios que se brindan a través de estos. Los procedimientos de auditoría deberán ser ejecutados por personal capacitado y con experiencia; y,	**DSS05**	Administrar los Servicios de Seguridad	DSS05.02 Gestionar la seguridad de la red y las conexiones.
73	**4.3.9.7.** Para la ejecución de transacciones de clientes, se deberán implementar mecanismos de autenticación que contemplen por lo menos dos de tres factores: “algo que se sabe, algo que se tiene, o algo que se es”;	**DSS05**	Administrar los Servicios de Seguridad	DSS05.04 Gestionar la identidad del usuario y el acceso lógico.
	Puntos de venta			

74	**Puntos de venta (POS y PIN Pad).-** Con el objeto de garantizar la seguridad en las transacciones realizadas a través de los dispositivos de puntos de venta, las instituciones del sistema financiero deberán cumplir como mínimo con lo siguiente: **4.3.10.1.** Establecer procedimientos que exijan que los técnicos que efectúan la instalación, mantenimiento o desinstalación de los puntos de venta (POS y PIN Pad) en los establecimientos comerciales confirmen su identidad a fin de asegurar que este personal cuenta con la debida autorización;	**BAI09**	Administrar los Activos	BAI09.02 Gestionar activos críticos
75	**4.3.10.2.** A fin de permitir que los establecimientos comerciales procesen en presencia del cliente o usuario las transacciones efectuadas a través de los dispositivos de puntos de venta (POS o PIN Pad), éstos deben permitir establecer sus comunicaciones de forma inalámbrica segura; y,	**DSS05**	Administrar los Servicios de Seguridad	DSS05.02 Gestionar la seguridad de la red y las conexiones.
76	**4.3.10.3.** Los dispositivos de puntos de venta (POS o PIN Pad) deben ser capaces de procesar la información de tarjetas inteligentes o con chip;	**BAI04**	Administrar la Disponibilidad y Capacidad	BAI04.03 Planificar requisitos de servicio nuevos o modificados.
	Banca electrónica			
77	**4.3.11. Banca electrónica.-** Con el objeto de garantizar la seguridad en las transacciones realizadas mediante la banca electrónica, las instituciones del sistema financiero que ofrezcan servicios por medio de este canal electrónico deberán cumplir como mínimo con lo siguiente: **4.3.11.1.** Implementar los algoritmos y protocolos seguros, así como certificados digitales, que ofrezcan las máximas seguridades en vigor dentro de las páginas web de las entidades controladas, a fin de garantizar una comunicación segura, la cual debe incluir el uso de técnicas de encriptación de los datos transmitidos acordes con los estándares internacionales vigentes	**DSS05**	Administrar los Servicios de Seguridad	DSS05.02 Gestionar la seguridad de la red y las conexiones.
78	**4.3.11.2.** Realizar como mínimo una vez (1) al año una prueba de vulnerabilidad y penetración a los equipos, dispositivos y medios de comunicación utilizados en la ejecución de transacciones por banca electrónica; y, en caso de que se realicen cambios en la plataforma que podrían afectar a la seguridad de este canal, se deberá efectuar una prueba adicional. Las pruebas de vulnerabilidad y penetración deberán ser efectuadas por personal independiente a la entidad, de comprobada competencia y aplicando estándares vigentes y reconocidos a nivel internacional. Las instituciones deberán definir y ejecutar planes de acción sobre las vulnerabilidades detectadas;	**DSS05**	Administrar los Servicios de Seguridad	DSS05.02 Gestionar la seguridad de la red y las conexiones.
79	**4.3.11.3.** Los informes de las pruebas de vulnerabilidad deberán estar a disposición de la Superintendencia de Bancos y Seguros, incluyendo un análisis comparativo del informe actual respecto del inmediatamente anterior;	**MEA01**	Monitorear, Evaluar y Valorar el Desempeño y Conformidad	MEA01.04 Analizar e informar sobre el rendimiento. MEA01.05 Asegurar la implantación de medidas correctivas.
80	**4.3.11.4.** Implementar mecanismos de control, autenticación mutua y monitoreo, que reduzcan la posibilidad de que los clientes accedan a páginas web falsas similares a las propias de las instituciones del sistema financiero;	**DSS05**	Administrar los Servicios de Seguridad	DSS05.02 Gestionar la seguridad de la red y las conexiones.
81	**4.3.11.5.** Implementar mecanismos de seguridad incluyendo dispositivos tales como IDS, IPS, firewalls, entre otros, que reduzcan la posibilidad	**DSS05**	Administrar los Servicios de Seguridad	DSS05.02 Gestionar la seguridad de la red y las conexiones.

	de que la información de las transacciones de los clientes sea capturada por terceros no autorizados durante la sesión;			
82	**4.3.11.6.** Establecer un tiempo máximo de inactividad, después del cual deberá ser cancelada la sesión y exigir un nuevo proceso de autenticación al cliente para realizar otras transacciones;	**DSS05**	Administrar los Servicios de Seguridad	DSS05.02 Gestionar la seguridad de la red y las conexiones.
83	**4.3.11.7.** Se deberá informar al cliente al inicio de cada sesión, la fecha y hora del último ingreso al canal de banca electrónica;	**DSS05**	Administrar los Servicios de Seguridad	DSS05.02 Gestionar la seguridad de la red y las conexiones.
84	**4.3.11.8.** La institución del sistema financiero deberá implementar mecanismos para impedir la copia de los diferentes componentes de su sitio web, verificar constantemente que no sean modificados sus enlaces (links), suplantados sus certificados digitales, ni modificada indebidamente la resolución de su sistema de nombres de dominio (DNS);	**DSS05**	Administrar los Servicios de Seguridad	DSS05.02 Gestionar la seguridad de la red y las conexiones.
85	**4.3.11.9.** La institución del sistema financiero debe implementar mecanismos de autenticación al inicio de sesión de los clientes, en donde el nombre de usuario debe ser distinto al número de cédula de identidad y éste así como su clave de acceso deben combinar caracteres numéricos y alfanuméricos con una longitud mínima de seis (6) caracteres;	**DSS05**	Administrar los Servicios de Seguridad	DSS05.04 Gestionar la identidad del usuario y el acceso lógico.
86	**4.3.11.10.** Para la ejecución de transacciones de clientes, se deberán implementar mecanismos de autenticación que contemplen por lo menos dos de tres factores: “algo que se sabe, algo que se tiene, o algo que se es”, considerando que uno de ellos debe: ser dinámico por cada vez que se efectúa una operación, ser una clave de una sola vez OTP (one time password), tener controles biométricos, entre otros;	**DSS05**	Administrar los Servicios de Seguridad	DSS05.04 Gestionar la identidad del usuario y el acceso lógico.
87	**4.3.11.11.** En todo momento en donde se solicite el ingreso de una clave numérica, los sitios web de las entidades deben exigir el ingreso de éstas a través de teclados virtuales, las mismas que deberán estar enmascaradas;	**DSS05**	Administrar los Servicios de Seguridad	DSS05.04 Gestionar la identidad del usuario y el acceso lógico.
	Planes de contingencia y continuidad			
88	**16.1** Las personas responsables de ejecutar cada actividad y la información (direcciones, teléfonos, correos electrónicos, entre otros) necesaria para contactarlos oportunamente;	**DSS04**	Administrar la Continuidad	DSS04.03 Desarrollar e implementar una respuesta a la continuidad del negocio.
89	**16.2** Acciones a ejecutar antes, durante y una vez ocurrido el incidente que ponga en peligro la operatividad de la institución;	**DSS04**	Administrar la Continuidad	DSS04.03 Desarrollar e implementar una respuesta a la continuidad del negocio.
90	**16.3** Acciones a realizar para trasladar las actividades de la institución a ubicaciones transitorias alternativas y para el restablecimiento de los negocios de manera urgente;	**DSS04**	Administrar la Continuidad	DSS04.03 Desarrollar e implementar una respuesta a la continuidad del negocio.
91	**16.4** Cronograma y procedimientos de prueba y mantenimiento del plan; y,	**DSS04**	Administrar la Continuidad	DSS04.04 Ejercitar, probar y revisar el plan de continuidad.
92	**16.5** Procedimientos de difusión, comunicación y concienciación del plan y su cumplimiento.	**DSS04**	Administrar la Continuidad	DSS04.06 Proporcionar formación en el plan de continuidad.
	Responsabilidades Unidad de Riesgos			
93	**19.1** Diseñar las políticas y el proceso de administración del riesgo operativo;	**APO01**	Administrar el marco de trabajo de	APO01.03 Mantener los elementos catalizadores del sistema de gestión.

			Administración de TI	
94	**19.2** Monitorear y evaluar los cambios significativos y la exposición a riesgos provenientes de los procesos, las personas, la tecnología de información y los eventos externos;	**EDM03**	Asegurar la optimización de riesgos	EDM03.03 Supervisar la gestión de riesgos.
95	**19.3** Analizar las políticas y procedimientos propuestos por el área respectiva, para los procesos, personas, eventos externos y tecnología de información, especialmente aquellas relacionadas con la seguridad de la información;	**EDM03**	Asegurar la optimización de riesgos	EDM03.01 Evaluar la gestión de riesgos.
96	**19.4** Liderar el desarrollo, la aplicabilidad y cumplimiento de los planes de contingencia y de continuidad del negocio, al que se refiere la sección IV de este capítulo; así como proponer los líderes de las áreas que deban cubrir el plan de contingencias y de continuidad del negocio; y,	**DSS04**	Administrar la Continuidad	Todo DSS04
97	**19.5** Analizar, monitorear y evaluar los procedimientos de orden legal de la institución; y, en coordinación con las áreas legales, emitir informes que determinen su real exposición al riesgo legal, los cuales deben ser puestos en conocimiento del comité de administración integral de riesgos.	**MEA03**	Monitorear, Evaluar y Valorar el Cumplimiento con Requerimientos Externos	MEA03.01 Identificar requisitos externos de cumplimiento.
	Servicios provistos por terceros			
98	**20.1** Contar con políticas, procesos y procedimientos efectivos que aseguren una adecuada selección y calificación de los proveedores, tales como: **20.1.1** Evaluación de la experiencia pertinente;	**APO10**	Administrar los Proveedores	APO10.02 Seleccionar proveedores.
99	**20.1.2** Desempeño de los proveedores en relación con los competidores;	**APO10**	Administrar los Proveedores	APO10.02 Seleccionar proveedores.
100	**20.1.3** Evaluación financiera para asegurar la viabilidad del proveedor durante todo el período de suministro y cooperación previsto;	**APO10**	Administrar los Proveedores	APO10.02 Seleccionar proveedores.
101	**20.1.4** Respuesta del proveedor a consultas, solicitudes de presupuesto y de ofertas;	**APO10**	Administrar los Proveedores	APO10.02 Seleccionar proveedores.
102	**20.1.5** Capacidad del servicio, instalación y apoyo e historial del desempeño en base a los requisitos;	**APO10**	Administrar los Proveedores	APO10.02 Seleccionar proveedores.
103	**20.1.6** Capacidad logística del proveedor incluyendo las instalaciones y recursos; y,	**APO10**	Administrar los Proveedores	APO10.02 Seleccionar proveedores. APO10.04 Gestionar el riesgo en el suministro.
104	**20.1.7** La reputación comercial del proveedor en la sociedad.	**APO10**	Administrar los Proveedores	APO10.02 Seleccionar proveedores.
105	**20.2** Contratos debidamente suscritos y legalizados que contengan cláusulas que detallen, entre otros, los niveles mínimos de servicio acordado; las penalizaciones por incumplimiento; y, que prevean facilidades para la revisión y seguimiento del servicio prestado, ya sea, por la unidad de auditoría interna u otra área que la entidad designe, así como, por parte de los auditores externos o de la Superintendencia de Bancos y Seguros; y,	**APO10**	Administrar los Proveedores	APO10.03 Gestionar contratos y relaciones con proveedores.
106	**20.3** Contar con proveedores alternos que tengan la capacidad de prestar el servicio.	**APO10**	Administrar los Proveedores	APO10.04 Gestionar el riesgo en el suministro.

ANEXO E: Mapeo de los requerimientos de la norma de Medidas de Seguridad de la SBS frente a las prácticas clave de COBIT 5

		Proceso de COBIT		Práctica clave
No.	**Medidas mínimas de seguridad**			
1	**32.1.1.** Incluyan la instalación y funcionamiento de dispositivos, mecanismos y equipos, con el objeto de contar con la protección requerida en los establecimientos, para clientes, empleados, público y patrimonio, estableciendo parámetros de acuerdo a la ubicación del establecimiento;	**DSS05**	Administrar los Servicios de Seguridad	DSS05.03 Gestionar la seguridad de los puestos de usuario final. DSS05.05 Gestionar el acceso físico a los activos de TI.
		BAI09	Administrar los Activos	BAI09.02 Gestionar activos críticos
2	**32.1.2.** En todo tiempo cuenten con sistemas de seguridad acordes con las disponibilidades técnicas del momento;	**APO13**	Administrar la Seguridad	APO13.01 Establecer y mantener un SGSI.
3	**32.1.3.** Cuenten con áreas seguras de iluminación adecuada y suficiente. En los lugares en donde se maneje efectivo, como bóvedas, cajas, cajeros automáticos, autobancos y consignatarios nocturnos, deberá reforzarse la iluminación y seguridad, debiendo asegurar la iluminación permanente de estos puntos ante un eventual corte de suministro eléctrico;	**DSS05**	Administrar los Servicios de Seguridad	DSS05.03 Gestionar la seguridad de los puestos de usuario final.
4	**32.1.4.** Mantengan controles de acceso al establecimiento, en caso de que presten servicio al público;	**DSS06**	Administrar los Controles de Procesos del Negocio	DSS06.06 Asegurar los activos de información.
5	**32.1.5.** Las puertas de entrada a la entidad financiera deben estar equipadas con dos cerraduras con llaves codificadas o de seguridad, a fin de requerir la presencia de dos personas al momento de la apertura y cierre de sus operaciones;	**DSS06**	Administrar los Controles de Procesos del Negocio	DSS06.06 Asegurar los activos de información.
6	**32.1.6.** Establezcan efectivos sistemas de seguridad y vigilancia en el interior de sus instalaciones, con guardias de empresas de seguridad privada, efectivos de la Policía Nacional o personal de seguridad de la propia entidad;	**APO13**	Administrar la Seguridad	APO13.02 Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información.
7	**32.1.7.** El área de cajas deberá ser de acceso restringido al público, al personal no autorizado de la entidad y estar ubicada de tal forma que se minimicen los riesgos de que terceras personas realicen sustracciones de dinero u otras actividades ilícitas; y,	**DSS06**	Administrar los Controles de Procesos del Negocio	DSS06.06 Asegurar los activos de información.
8	**32.1.8.** Garanticen el cumplimiento de la prohibición de que los funcionarios del área de cajeros porten teléfonos celulares, localizadores o beepers de uso personal. Se permite el uso de medios de comunicación bajo el control y supervisión de la entidad.	**DSS06**	Administrar los Controles de Procesos del Negocio	DSS06.06 Asegurar los activos de información.
	Manuales y políticas de seguridad y protección			
9	**33.1** Las políticas, normas, principios y procesos básicos conforme a los cuales las entidades bancarias deben formular sus medidas de seguridad y protección;	**APO13**	Administrar la Seguridad	APO13.01 Establecer y mantener un SGSI.
10	**33.2** Las medidas mínimas de seguridad contenidas en el presente capítulo, precisando sus características, y en su caso, dimensiones y calidad	**APO13**	Administrar la Seguridad	APO13.01 Establecer y mantener un SGSI.

	de los materiales;	**DSS01**	Administrar las Operaciones	DSS01.05 Gestionar las instalaciones
11	**33.3** Las demás medidas de seguridad que las entidades deseen adoptar como adicionales a las contenidas en el presente capítulo;	**APO13**	Administrar la Seguridad	APO13.01 Establecer y mantener un SGSI.
12	**33.4** Los criterios para el diseño y construcción de sus establecimientos, incluyendo la instalación, funcionamiento y control de dispositivos, mecanismos, centros de procesos de datos y de comunicación y equipo técnico de protección para la prestación de los servicios que le corresponda;	**DSS01**	Administrar las Operaciones	DSS01.05 Gestionar las instalaciones
13	**33.5** Los procesos, sistemas y controles operativos para la prevención y detección de irregularidades en la realización de sus operaciones y en el manejo de los recursos, efectivo y valores que tengan bajo su responsabilidad;	**DSS06**	Administrar los Controles de Procesos del Negocio	DSS06.06 Asegurar los activos de información.
14	**33.6** Las características que deberán reunir los sistemas de monitoreo y alarma, incluyendo los índices de calidad y disponibilidad, así como las demás características técnicas o tecnológicas necesarias para la efectiva emisión y transmisión de las señales e imágenes;	**DSS01**	Administrar las Operaciones	DSS01.05 Gestionar las instalaciones
15	**33.7** Los aspectos relativos a la seguridad de la información, tales como la seguridad física, lógica de redes y comunicación, entre otros;	**APO13**	Administrar la Seguridad	APO13.01 Establecer y mantener un SGSI.
16	**33.8** Los criterios para la selección, reclutamiento y capacitación del recurso humano, así como para la contratación de servicios profesionales para brindar seguridad y protección a los establecimientos;	**DSS06**	Administrar los Controles de Procesos del Negocio	DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.
17	**33.9** Los lineamientos y planes de capacitación e información al personal que labora en sus entidades, específicamente respecto del entrenamiento en caso de siniestros o durante la comisión de un delito, estos deberán actualizarse por lo menos una (1) vez al año;	**DSS04**	Administrar la Continuidad	DSS04.06 Proporcionar formación en el plan de continuidad.
18	**33.10** Los dispositivos, sistemas y procedimientos para controlar la entrada y salida de los empleados de la entidad;	**DSS05**	Administrar los Servicios de Seguridad	DSS05.05 Gestionar el acceso físico a los activos de TI.
19	**33.11** Los sistemas y procedimientos para controlar la entrada y salida de clientes, proveedores y otros a las instituciones financieras;	**DSS05**	Administrar los Servicios de Seguridad	DSS05.05 Gestionar el acceso físico a los activos de TI.
20	**33.12** Procedimientos relacionados con el manejo, custodia y resguardo de información relativa a los clientes de las entidades financieras; y,	**DSS06**	Administrar los Controles de Procesos del Negocio	DSS06.06 Asegurar los activos de información.
21	**33.13** Los planes de seguridad, emergencia, contingencia y continuidad de negocios de la entidad financiera en caso de siniestros o actos delictivos, cuya efectividad deberá revisarse y probarse mediante simulacros por lo menos una (1) vez al año dejando la constancia escrita de su ejecución y evaluación.	**DSS04**	Administrar la Continuidad	DSS04.03 Desarrollar e implementar una respuesta a la continuidad del negocio. DSS04.04 Ejercitar, probar y revisar el plan de continuidad.
	Personal de seguridad			
22	**34.1** Contar con empleados debidamente formados y capacitados que tengan la responsabilidad de las labores propias de un supervisor de seguridad bancaria, quien tendrá como tarea la dirección, gestión o coordinación de los planes y medidas de seguridad;	**DSS06**	Administrar los Controles de Procesos del Negocio	DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.

23	**34.2** Contar con personal o agentes de seguridad que custodiarán las instalaciones de la entidad en su interior o exterior al momento de apertura del establecimiento, durante el horario normal y diferido de atención al público y hasta tanto se encuentren empleados laborando. Además tendrán la responsabilidad de la revisión a los clientes, proveedores y otras personas que ingresen al establecimiento; que podrán ser personas contratadas directa o indirectamente por la entidad financiera para ejecutar esta función o personal de una empresa de seguridad privada;	**DSS06**	Administrar los Controles de Procesos del Negocio	DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.
24	**34.3** En aquellos casos donde las entidades financieras contraten empresas de seguridad privada, verificar que las mismas cumplan con los requisitos establecidos por la ley que regula la materia y el Ministerio del Interior; y,	**APO10**	Administrar los Proveedores	APO10.01 Identificar y evaluar las relaciones y contratos con proveedores.
25	**34.4** Verificar que al personal o agente de seguridad le sean asignadas funciones específicas de seguridad y por ninguna razón se les asignen otras funciones.	**DSS06**	Administrar los Controles de Procesos del Negocio	DSS06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.
	Bóvedas y cajas fuertes			
26	**35.1** Las bóvedas, cajas fuertes y sus áreas conexas en que se deposite efectivo y valores son de acceso restringido, por lo que deben contar con elementos y sistemas que proporcionen una adecuada seguridad y protección, tanto a su contenido como durante los procedimientos de depósito o retiro de efectivo y/o valores objeto de transportación y resguardo;	**DSS06**	Administrar los Controles de Procesos del Negocio	DSS06.06 Asegurar los activos de información.
27	**35.2** Deben cumplir con estándares internacionales para la construcción de bóvedas, cajas fuertes y puertas de bóveda; y, cumplir con las características de alta seguridad según los lineamientos y estándares internacionales. Además deberán mantener pólizas de seguro adecuadas;	**MEA03**	Monitorear, Evaluar y Valorar el Cumplimiento con Requerimientos Externos	MEA03.03 Confirmar el cumplimiento de requisitos externos.
		DSS06	Administrar los Controles de Procesos del Negocio	DSS06.06 Asegurar los activos de información.
28	**35.3** Las puertas de las bóvedas cuenten con relojes de tiempo y sistemas de ventilación; con sensores de humo, de movimiento, de vibración; y, adicionalmente, con botones de pánico y sistemas de comunicación ubicados estratégicamente;	**DSS01**	Administrar las Operaciones	DSS01.04 Gestionar el entorno
		DSS06	Administrar los Controles de Procesos del Negocio	DSS06.06 Asegurar los activos de información.
29	**35.4** Las bóvedas tengan cámaras en la parte interior de la misma;	**DSS06**	Administrar los Controles de Procesos del Negocio	DSS06.06 Asegurar los activos de información.
30	**35.5** Las entidades financieras deben establecer procedimientos para el cierre y la apertura de las bóvedas y para situaciones de emergencia, tales como en el caso de asalto, siniestro o si una persona permanece en su interior luego de su cierre; y,	**BAI05**	Administrar la Habilitación del Cambio Organizacional	BAI05.05 Facilitar la operación y el uso.
31	**35.6** Las cajas fuertes y los compartimentos que mantienen el efectivo de la reserva deben contar con relojes de tiempo.	**BAI10**	Administrar la Configuración	BAI10.02 Establecer y mantener un repositorio de configuración y una base de referencia.
	Sistemas de alarmas de robo e incendio			

32	**36.1** Todas las instalaciones de las entidades financieras, deben contar con sistemas de alarma contra robo e incendio, enlazados por frecuencia de radio o cable con centrales de monitoreo y respuesta; además, éstas deben estar comunicadas con la Policía Nacional, Cuerpo de Bomberos y empresas de seguridad privada, si es el caso;	**DSS06**	Administrar los Controles de Procesos del Negocio	DSS06.06 Asegurar los activos de información.
33	**36.2** Los sistemas de alarma para los riesgos de robo deben cumplir con estándares internacionales;	**MEA03**	Monitorear, Evaluar y Valorar el Cumplimiento con Requerimientos Externos	MEA03.03 Confirmar el cumplimiento de requisitos externos.
34	**36.3** Los sistemas de alarma deben verificarse permanentemente, con la finalidad de garantizar el funcionamiento correcto de los equipos y la prestancia del personal encargado. Así mismo, deben confirmarse los sistemas de comunicación con la Policía y las empresas de seguridad privada; y, especialmente, con el personal de seguridad encargado de la protección y los funcionarios y directivos de la institución financieras;	**DSS01**	Administrar las Operaciones	DSS01.05 Gestionar las instalaciones
35	**36.4** Cuando lo requiera la Superintendencia de Bancos y Seguros y en las oficinas que determine, se deberá realizar un ejercicio de simulacro para probar el sistema de seguridad y los planes para las diferentes emergencias y contingencias: caso de asalto, robo, incendio (previa coordinación con la Policía Nacional, Cuerpo de Bomberos y Protección Civil), amenaza de bombas, u otra eventualidad. De estos ejercicios y demás evaluaciones se debe mantener registros, incluyendo los informes de eficiencia del sistema; y,	**DSS04**	Administrar la Continuidad	DSS04.04 Ejercitar, probar y revisar el plan de continuidad.
36	**36.5** Todos los sistemas electrónicos, alarmas y demás elementos de seguridad de la institución financiera deben estar operativos en todo momento, captar y grabar, tanto las señales de alarma como las escenas de hechos delictivos o siniestros. Estas grabaciones serán proporcionadas sin costo a las autoridades competentes que las requieran.	**DSS01**	Administrar las Operaciones	DSS01.03 Supervisar la infraestructura de TI
	Sistemas de video vigilancia			
37	**37.1** Las instituciones financieras deben contar con un número adecuado de cámaras fijas y movibles de circuito cerrado de televisión con imágenes de alta resolución, equipadas con videograbadoras, disco duro o su equivalente en cámaras fotográficas para la toma de fotos instantáneas durante 24 horas. El sistema de video vigilancia debe ser evaluado permanentemente y mantener un registro actualizado de sus niveles de operación, a fin de garantizar su correcto funcionamiento, la nitidez y fidelidad de las imágenes;	**DSS06**	Administrar los Controles de Procesos del Negocio	DSS06.06 Asegurar los activos de información.
38	**37.2** Las cámaras de ubicación fija, como mínimo deben cubrir adecuadamente los lugares de acceso al público y personal de la institución financiera y las cajas de atención al público; y,	**DSS06**	Administrar los Controles de Procesos del Negocio	DSS06.06 Asegurar los activos de información.
39	**37.3** Los sistemas de grabación y almacenamiento de imágenes deben garantizar el archivo de por lo menos tres (3) meses de grabación, a través de cintas, de discos de video digital (DVD) o cualquier otro sistema.	**DSS01**	Administrar las Operaciones	DSS01.05 Gestionar las instalaciones
40	**ARTICULO 38.-** Las instituciones financieras establecerán estrictos procedimientos y normas que regulen o prohíban, según sea el caso, el uso de telefonía celular y cualquier otro mecanismo de	**DSS06**	Administrar los Controles de Procesos del Negocio	DSS06.06 Asegurar los activos de información.

	comunicación desde el interior de sus instalaciones.			
41	Complementariamente se instalará mecanismos tecnológicos inhibidores de comunicación en el área designada para cajas y hall de cajas, que permitan bloquear la comunicación a través de celulares, excluyendo la zona donde se encuentran instalados los cajeros automáticos, cuando éstos se encuentren fuera de las áreas de atención al público.	**DSS06**	Administrar los Controles de Procesos del Negocio	DSS06.06 Asegurar los activos de información.
	Cajeros automáticos			
42	**39.1 Protección al teclado**.- Contar en todo momento con los dispositivos conocidos como "protectores de teclado", que de una manera efectiva impidan la visibilidad al momento que el usuario digita su clave personal;	**DSS06**	Administrar los Controles de Procesos del Negocio	DSS06.06 Asegurar los activos de información.
43	**39.2 Protección contra clonación de tarjetas**.- Contar con dispositivos electrónicos y/o elementos físicos que impidan y detecten de manera efectiva la colocación de falsas lectoras de tarjetas, con el fin de evitar la clonación de tarjetas de débito o de crédito, además de los correspondientes mecanismos de monitoreo en línea de las alarmas que generen los dispositivos electrónicos en caso de suscitarse eventos inusuales;	**DSS06**	Administrar los Controles de Procesos del Negocio	DSS06.06 Asegurar los activos de información.
44	**39.3 Iluminación**.- Los cajeros automáticos instalados en áreas externas a las oficinas de las instituciones financieras, deberán estar ubicados en zonas suficientemente iluminadas que permitan la visualización de toda actividad a su alrededor;	**DSS06**	Administrar los Controles de Procesos del Negocio	DSS06.06 Asegurar los activos de información.
45	**39.4 Programas de vigilancia en sitio**.- Contar con un programa regular de visitas al sitio donde se encuentra instalado el cajero automático, con la finalidad de garantizar que no existan objetos extraños, dispositivos u otros mecanismos sospechosos instalados en el cajero automático;	**DSS01**	Administrar las Operaciones	DSS01.03 Supervisar la infraestructura de TI
46	**39.5 Mecanismo de anclaje**.- Los cajeros automáticos deben asegurarse adecuadamente al piso u otro soporte a fin de que dificulte su remoción, salvo el caso de aquellos que estén empotrados a la pared;	**DSS06**	Administrar los Controles de Procesos del Negocio	DSS06.06 Asegurar los activos de información.
47	**39.6 Protección al software e información del cajero automático.-** Disponer de un programa o sistema de protección contra intrusos (Anti-malware) que permita proteger el software instalado en el cajero automático y que detecte oportunamente cualquier alteración en su código, configuración y/o funcionalidad. Así mismo, se deberá instalar mecanismos que sean capaces de identificar conexiones no autorizadas a través de los puertos USB, comunicaciones remotas, cambio de los discos duros y otros componentes que guarden o procesen información. En una situación de riesgo deben emitir alarmas a un centro de monitoreo o dejar inactivo al cajero automático hasta que se realice la inspección por parte del personal especializado de la institución;	**DSS05**	Administrar los Servicios de Seguridad	DSS05.01 Proteger contra software malicioso (malware). DSS05.02 Gestionar la seguridad de la red y las conexiones.
		DSS06	Administrar los Controles de Procesos del Negocio	DSS06.06 Asegurar los activos de información.
48	**39.7 Procedimientos para el mantenimiento preventivo y correctivo en los cajeros automáticos.-** Disponer de procedimientos auditables debidamente acordados y coordinados entre la institución y los proveedores internos o externos para la ejecución de las tareas de mantenimiento preventivo y correctivo del hardware y software, provisión de suministros y recarga de dinero en las gavetas. Las claves de acceso tipo “administrador” del	**BAI09**	Administrar los Activos	BAI09.02 Gestionar activos críticos

	sistema del cajero automático deben ser únicas y reemplazadas periódicamente;			
49	**39.8 Accesos físicos al interior de los cajeros automáticos.-** Disponer de cerraduras de alta tecnología y seguridades que garanticen el acceso controlado al interior del cajero automático por parte del personal técnico o de mantenimiento que disponga de las respectivas llaves. Estas cerraduras deben operar con llaves únicas y no genéricas o maestras;	**DSS05**	Administrar los Servicios de Seguridad	DSS05.05 Gestionar el acceso físico a los activos de TI.
50	**39.9 Reportes de nivel de seguridad de los cajeros-** Comunicar oportunamente la información sobre los estándares de seguridad implementados en los cajeros automáticos, incidentes de seguridad (vandalismo y/o fraudes) identificados en sus cajeros automáticos y/o ambientes de software o hardware relacionados;	**DSS05**	Administrar los Servicios de Seguridad	DSS05.07 Supervisar la infraestructura para detectar eventos relacionados con la seguridad.
51	**39.10** Establecer los mecanismos y procedimientos adecuados para: **39.10.1.** Revisar periódicamente los anclajes, iluminación y entorno del cajero automático;	**DSS01**	Administrar las Operaciones	DSS01.05 Gestionar las instalaciones
52	**39.10.2.** Abastecer de dinero permanentemente a los cajeros automáticos;	**BAI09**	Administrar los Activos	BAI09.02 Gestionar activos críticos
53	**39.10.3.** Atender las alarmas generadas por los dispositivos electrónicos de control instalados en los cajeros automáticos; y,	**DSS01**	Administrar las Operaciones	DSS01.05 Gestionar las instalaciones
54	**39.10.4.** Contar con personal capacitado para la operación y mantenimiento diario del cajero.	**APO07**	Administrar los Recursos Humanos	APO07.03 Mantener las habilidades y competencias del personal.
55	**39.11 Campañas de capacitación a usuarios sobre medidas preventivas y buen uso del sistema**.- Llevar a cabo campañas educativas para los usuarios acerca del uso, ubicación y medidas de seguridad pertinentes durante el uso del cajero, incluyendo la colocación de letreros alusivos a éstas en los recintos de los cajeros; y,	**BAI08**	Administrar el Conocimiento	BAI08.04 Utilizar y compartir el conocimiento.
56	**39.12 Sistema de grabación o archivo de imágenes**.- Las instituciones financieras deberán mantener un archivo de cintas, de discos de video digital (DVD) o cualquier otro sistema de grabación o su equivalentes en cámaras fotográficas que cubra por lo menos noventa (90) días de archivo de imágenes.	**DSS01**	Administrar las Operaciones	DSS01.05 Gestionar las instalaciones
	Transporte de fondos y valores			
57	**40.1** Brindar apoyo a los clientes que solicitaren el servicio de seguridad para el retiro o depósito de dinero en efectivo, cuando se trate de altas sumas, esta actividad la realizarán en coordinación con la Policía Nacional;	**DSS06**	Administrar los Controles de Procesos del Negocio	DSS06.06 Asegurar los activos de información.
58	**40.2** En lo relacionado a la recepción y envío de efectivo y valores, efectuar en áreas de acceso restringido al público y por personal autorizado por la institución, que eviten su exposición a riesgos, debiendo incluirse estos procedimientos en los "Manuales de seguridad y protección";	**DSS06**	Administrar los Controles de Procesos del Negocio	DSS06.06 Asegurar los activos de información.
59	**40.3** En el traslado de fondos y valores, ser realizado por empresas debidamente autorizadas, utilizando vehículos blindados que cuenten con ventilación adecuada, sistemas de comunicación y personal de seguridad debidamente capacitado y entrenado. Las instituciones deberán mantener actualizadas las fichas con los nombres, firmas y fotografías del personal de la empresa transportadora de fondos y valores;	**DSS06**	Administrar los Controles de Procesos del Negocio	DSS06.06 Asegurar los activos de información.

60	**40.4** Sin perjuicio de lo dispuesto en el numeral 40.5, los vehículos blindados utilizados para tales transportaciones deberán cumplir con las normas técnicas determinadas en el artículo 9 del "Instructivo para el control, funcionamiento, supervisión del servicio de seguridad móvil en la transportación de valores y las normas de blindaje internacionales que deben cumplir los vehículos blindados que prestan este servicio", contenido en el Acuerdo Ministerial No. 1580 de 8 de julio del 2010; y,	**MEA03**	Monitorear, Evaluar y Valorar el Cumplimiento con Requerimientos Externos	MEA03.03 Confirmar el cumplimiento de requisitos externos.
61	**40.5** Aquellos bancos o instituciones financieras que requieran transportar por sus propios medios, fondos y valores, deberán hacerlo en los vehículos blindados mencionados en el numeral 40.3; o, en su defecto en compartimentos de seguridad, cuya combinación solo conozca el personal de la entidad encargado de recibir dichos fondos y valores, en compañía de un guardia de seguridad o personal de policía y dos (2) funcionarios de la entidad. En este último caso, los fondos y valores deben ser entregados en forma directa a las bóvedas y cajas fuertes.	**DSS06**	Administrar los Controles de Procesos del Negocio	DSS06.06 Asegurar los activos de información.
	Contrato de pólizas de seguro			
62	**ARTÍCULO 41.-** Las instituciones financieras contratarán anualmente con las compañías de seguro privado, coberturas que aseguren a la entidad contra fraudes generados a través de su tecnología de la información, sistemas telemáticos, electrónicos o similares, como mínimo ante los siguientes riesgos: 41.1 Alteraciones de bases de datos; 41.2 Accesos a los sistemas informáticos y de información de forma ilícita; 41.3 Falsedad informática; 41.4 Estafa informática; 41.5 Daño informático; y, 41.6 Destrucción a la infraestructura a las instalaciones físicas necesarias para la transmisión, recepción o procesamiento de información.	**DSS06**	Administrar los Controles de Procesos del Negocio	DSS06.06 Asegurar los activos de información.

ANEXO F: Mapeo de la norma de medidas de seguridad de la SBS con la norma ISO/IEC 27005

		Actividad		Acción
No.	**Medidas mínimas de seguridad**			
1	**32.1.1.** Incluyan la instalación y funcionamiento de dispositivos, mecanismos y equipos, con el objeto de contar con la protección requerida en los establecimientos, para clientes, empleados, público y patrimonio, estableciendo parámetros de acuerdo a la ubicación del establecimiento;	**9.1**	Descripción general del tratamiento de riesgos	Seleccionar los controles para reducir, retener, evitar o transferir los riesgos, y definir un plan de tratamiento de riesgos
2	**32.1.2.** En todo tiempo cuenten con sistemas de seguridad acordes con las disponibilidades técnicas del momento;	**9.1**	Descripción general del tratamiento de riesgos	Seleccionar los controles para reducir, retener, evitar o transferir los riesgos, y definir un plan de tratamiento de riesgos
3	**32.1.3.** Cuenten con áreas seguras de iluminación adecuada y suficiente. En los lugares en donde se maneje efectivo, como bóvedas, cajas, cajeros automáticos, autobancos y consignatarios nocturnos, deberá reforzarse la iluminación y seguridad, debiendo asegurar la iluminación permanente de estos puntos ante un eventual corte de suministro eléctrico;	**9.1**	Descripción general del tratamiento de riesgos	Seleccionar los controles para reducir, retener, evitar o transferir los riesgos, y definir un plan de tratamiento de riesgos
4	**32.1.4.** Mantengan controles de acceso al establecimiento, en caso de que presten servicio al público;	**9.1**	Descripción general del tratamiento de riesgos	Seleccionar los controles para reducir, retener, evitar o transferir los riesgos, y definir un plan de tratamiento de riesgos
5	**32.1.5.** Las puertas de entrada a la entidad financiera deben estar equipadas con dos cerraduras con llaves codificadas o de seguridad, a fin de requerir la presencia de dos personas al momento de la apertura y cierre de sus operaciones;	**9.1**	Descripción general del tratamiento de riesgos	Seleccionar los controles para reducir, retener, evitar o transferir los riesgos, y definir un plan de tratamiento de riesgos
6	**32.1.6.** Establezcan efectivos sistemas de seguridad y vigilancia en el interior de sus instalaciones, con guardias de empresas de seguridad privada, efectivos de la Policía Nacional o personal de seguridad de la propia entidad;	**9.1**	Descripción general del tratamiento de riesgos	Seleccionar los controles para reducir, retener, evitar o transferir los riesgos, y definir un plan de tratamiento de riesgos
7	**32.1.7.** El área de cajas deberá ser de acceso restringido al público, al personal no autorizado de la entidad y estar ubicada de tal forma que se minimicen los riesgos de que terceras personas realicen sustracciones de dinero u otras actividades ilícitas; y,	**9.1**	Descripción general del tratamiento de riesgos	Seleccionar los controles para reducir, retener, evitar o transferir los riesgos, y definir un plan de tratamiento de riesgos
8	**32.1.8.** Garanticen el cumplimiento de la prohibición de que los funcionarios del área de cajeros porten teléfonos celulares, localizadores o beepers de uso personal. Se permite el uso de medios de comunicación bajo el control y supervisión de la entidad.	**9.1**	Descripción general del tratamiento de riesgos	Seleccionar los controles para reducir, retener, evitar o transferir los riesgos, y definir un plan de tratamiento de riesgos
	Manuales y políticas de seguridad y protección			
9	**33.1** Las políticas, normas, principios y procesos básicos conforme a los cuales las entidades bancarias deben formular sus medidas de seguridad y protección;	**9.1**	Descripción general del tratamiento de riesgos	Seleccionar los controles para reducir, retener, evitar o transferir los riesgos, y definir un plan de tratamiento de riesgos
10	**33.2** Las medidas mínimas de seguridad contenidas en el presente capítulo, precisando sus características, y en su caso, dimensiones y	**9.1**	Descripción general del tratamiento de	Seleccionar los controles para reducir, retener, evitar o transferir los riesgos, y definir

	calidad de los materiales;		riesgos	un plan de tratamiento de riesgos
11	**33.3** Las demás medidas de seguridad que las entidades deseen adoptar como adicionales a las contenidas en el presente capítulo;	**9.1**	Descripción general del tratamiento de riesgos	Seleccionar los controles para reducir, retener, evitar o transferir los riesgos, y definir un plan de tratamiento de riesgos
12	**33.4** Los criterios para el diseño y construcción de sus establecimientos, incluyendo la instalación, funcionamiento y control de dispositivos, mecanismos, centros de procesos de datos y de comunicación y equipo técnico de protección para la prestación de los servicios que le corresponda;	**9.1**	Descripción general del tratamiento de riesgos	Seleccionar los controles para reducir, retener, evitar o transferir los riesgos, y definir un plan de tratamiento de riesgos
13	**33.5** Los procesos, sistemas y controles operativos para la prevención y detección de irregularidades en la realización de sus operaciones y en el manejo de los recursos, efectivo y valores que tengan bajo su responsabilidad;	**9.1**	Descripción general del tratamiento de riesgos	Seleccionar los controles para reducir, retener, evitar o transferir los riesgos, y definir un plan de tratamiento de riesgos
14	**33.6** Las características que deberán reunir los sistemas de monitoreo y alarma, incluyendo los índices de calidad y disponibilidad, así como las demás características técnicas o tecnológicas necesarias para la efectiva emisión y transmisión de las señales e imágenes;	**9.1**	Descripción general del tratamiento de riesgos	Seleccionar los controles para reducir, retener, evitar o transferir los riesgos, y definir un plan de tratamiento de riesgos
15	**33.7** Los aspectos relativos a la seguridad de la información, tales como la seguridad física, lógica de redes y comunicación, entre otros;	**9.1**	Descripción general del tratamiento de riesgos	Seleccionar los controles para reducir, retener, evitar o transferir los riesgos, y definir un plan de tratamiento de riesgos
16	**33.8** Los criterios para la selección, reclutamiento y capacitación del recurso humano, así como para la contratación de servicios profesionales para brindar seguridad y protección a los establecimientos;	**9.1**	Descripción general del tratamiento de riesgos	Seleccionar los controles para reducir, retener, evitar o transferir los riesgos, y definir un plan de tratamiento de riesgos
17	**33.9** Los lineamientos y planes de capacitación e información al personal que labora en sus entidades, específicamente respecto del entrenamiento en caso de siniestros o durante la comisión de un delito, estos deberán actualizarse por lo menos una (1) vez al año;	**9.1**	Descripción general del tratamiento de riesgos	Seleccionar los controles para reducir, retener, evitar o transferir los riesgos, y definir un plan de tratamiento de riesgos
18	**33.10** Los dispositivos, sistemas y procedimientos para controlar la entrada y salida de los empleados de la entidad;	**9.1**	Descripción general del tratamiento de riesgos	Seleccionar los controles para reducir, retener, evitar o transferir los riesgos, y definir un plan de tratamiento de riesgos
19	**33.11** Los sistemas y procedimientos para controlar la entrada y salida de clientes, proveedores y otros a las instituciones financieras;	**9.1**	Descripción general del tratamiento de riesgos	Seleccionar los controles para reducir, retener, evitar o transferir los riesgos, y definir un plan de tratamiento de riesgos
20	**33.12** Procedimientos relacionados con el manejo, custodia y resguardo de información relativa a los clientes de las entidades financieras; y,	**9.1**	Descripción general del tratamiento de riesgos	Seleccionar los controles para reducir, retener, evitar o transferir los riesgos, y definir un plan de tratamiento de riesgos
21	**33.13** Los planes de seguridad, emergencia, contingencia y continuidad de negocios de la entidad financiera en caso de siniestros o actos delictivos, cuya efectividad deberá revisarse y probarse mediante simulacros por lo menos una (1) vez al año dejando la constancia escrita de su ejecución y evaluación.	**9.1**	Descripción general del tratamiento de riesgos	Seleccionar los controles para reducir, retener, evitar o transferir los riesgos, y definir un plan de tratamiento de riesgos
	Personal de seguridad			

22	**34.1** Contar con empleados debidamente formados y capacitados que tengan la responsabilidad de las labores propias de un supervisor de seguridad bancaria, quien tendrá como tarea la dirección, gestión o coordinación de los planes y medidas de seguridad;	**8.2. 1.4**	Identificación de controles existentes	Los controles existentes y planeados deben ser identificados
23	**34.2** Contar con personal o agentes de seguridad que custodiarán las instalaciones de la entidad en su interior o exterior al momento de apertura del establecimiento, durante el horario normal y diferido de atención al público y hasta tanto se encuentren empleados laborando. Además tendrán la responsabilidad de la revisión a los clientes, proveedores y otras personas que ingresen al establecimiento; que podrán ser personas contratadas directa o indirectamente por la entidad financiera para ejecutar esta función o personal de una empresa de seguridad privada;	**8.2. 1.4**	Identificación de controles existentes	Los controles existentes y planeados deben ser identificados
24	**34.3** En aquellos casos donde las entidades financieras contraten empresas de seguridad privada, verificar que las mismas cumplan con los requisitos establecidos por la ley que regula la materia y el Ministerio del Interior; y,	**7.23**	Criterios básicos - Criterios de aceptación del riesgo	Establecer el criterio de aceptación del riesgo considerando: el criterio de negocio, aspectos legales y regulatorios, operaciones, tecnología, finanzas, factores sociales y humanitarios
25	**34.4** Verificar que al personal o agente de seguridad le sean asignadas funciones específicas de seguridad y por ninguna razón se les asignen otras funciones.	**7.22**	Criterios básicos - Criterios de evaluación del riesgo	Desarrollar el criterio de evaluación del riesgo de la organización, considerando requerimientos legales y regulatorios, y obligaciones contractuales
	Bóvedas y cajas fuertes			
26	**35.1** Las bóvedas, cajas fuertes y sus áreas conexas en que se deposite efectivo y valores son de acceso restringido, por lo que deben contar con elementos y sistemas que proporcionen una adecuada seguridad y protección, tanto a su contenido como durante los procedimientos de depósito o retiro de efectivo y/o valores objeto de transportación y resguardo;	**9.2**	Reducción del riesgo	El nivel de riesgo debe reducirse a través de la selección de controles de modo que el riesgo residual sea aceptable
27	**35.2** Deben cumplir con estándares internacionales para la construcción de bóvedas, cajas fuertes y puertas de bóveda; y, cumplir con las características de alta seguridad según los lineamientos y estándares internacionales. Además deberán mantener pólizas de seguro adecuadas;	**7.22**	Criterios básicos - Criterios de evaluación del riesgo	Desarrollar el criterio de evaluación del riesgo de la organización, considerando requerimientos legales y regulatorios, y obligaciones contractuales
28	**35.3** Las puertas de las bóvedas cuenten con relojes de tiempo y sistemas de ventilación; con sensores de humo, de movimiento, de vibración; y, adicionalmente, con botones de pánico y sistemas de comunicación ubicados estratégicamente;	**8.2. 1.4**	Identificación de controles existentes	Los controles existentes y planeados deben ser identificados
29	**35.4** Las bóvedas tengan cámaras en la parte interior de la misma;	**8.2. 1.4**	Identificación de controles existentes	Los controles existentes y planeados deben ser identificados
30	**35.5** Las entidades financieras deben establecer procedimientos para el cierre y la apertura de las bóvedas y para situaciones de emergencia, tales como en el caso de asalto, siniestro o si una persona permanece en su interior luego de su cierre; y,	**9.1**	Descripción general del tratamiento de riesgos	Seleccionar los controles para reducir, retener, evitar o transferir los riesgos, y definir un plan de tratamiento de riesgos
31	**35.6** Las cajas fuertes y los compartimentos que mantienen el efectivo de la reserva deben contar con relojes de tiempo.	**8.2. 1.4**	Identificación de controles existentes	Los controles existentes y planeados deben ser identificados
	Sistemas de alarmas de robo e incendio			

32	**36.1** Todas las instalaciones de las entidades financieras, deben contar con sistemas de alarma contra robo e incendio, enlazados por frecuencia de radio o cable con centrales de monitoreo y respuesta; además, éstas deben estar comunicadas con la Policía Nacional, Cuerpo de Bomberos y empresas de seguridad privada, si es el caso;	**8.2. 1.3**	Identificación de amenazas	Las amenazas y su origen deben ser identificados
33	**36.2** Los sistemas de alarma para los riesgos de robo deben cumplir con estándares internacionales;	**7.22**	Criterios básicos - Criterios de evaluación del riesgo	Desarrollar el criterio de evaluación del riesgo de la organización, considerando requerimientos legales y regulatorios, y obligaciones contractuales
34	**36.3** Los sistemas de alarma deben verificarse permanentemente, con la finalidad de garantizar el funcionamiento correcto de los equipos y la prestancia del personal encargado. Así mismo, deben confirmarse los sistemas de comunicación con la Policía y las empresas de seguridad privada; y, especialmente, con el personal de seguridad encargado de la protección y los funcionarios y directivos de la institución financieras;	**8.2. 1.5**	Identificación de vulnerabilidades	Las vulnerabilidades que pueden ser explotadas por amenazas para dañar los activos o la organización, deben ser identificados
35	**36.4** Cuando lo requiera la Superintendencia de Bancos y Seguros y en las oficinas que determine, se deberá realizar un ejercicio de simulacro para probar el sistema de seguridad y los planes para las diferentes emergencias y contingencias: caso de asalto, robo, incendio (previa coordinación con la Policía Nacional, Cuerpo de Bomberos y Protección Civil), amenaza de bombas, u otra eventualidad. De estos ejercicios y demás evaluaciones se debe mantener registros, incluyendo informes de eficiencia del sistema; y,	**8.2. 1.4**	Identificación de controles existentes	Los controles existentes y planeados deben ser identificados
36	**36.5** Todos los sistemas electrónicos, alarmas y demás elementos de seguridad de la institución financiera deben estar operativos en todo momento, captar y grabar, tanto las señales de alarma como las escenas de hechos delictivos o siniestros. Estas grabaciones serán proporcionadas sin costo a las autoridades competentes que las requieran.	**8.2. 1.5**	Identificación de vulnerabilidades	Las vulnerabilidades que pueden ser explotadas por amenazas para dañar los activos o la organización, deben ser identificados
	Sistemas de video vigilancia			
37	**37.1** Las instituciones financieras deben contar con un número adecuado de cámaras fijas y movibles de circuito cerrado de televisión con imágenes de alta resolución, equipadas con videograbadoras, disco duro o su equivalente en cámaras fotográficas para la toma de fotos instantáneas durante 24 horas. El sistema de video vigilancia debe ser evaluado permanentemente y mantener un registro actualizado de sus niveles de operación, a fin de garantizar su correcto funcionamiento, la nitidez y fidelidad de las imágenes;	**8.2. 1.4**	Identificación de controles existentes	Los controles existentes y planeados deben ser identificados
38	**37.2** Las cámaras de ubicación fija, como mínimo deben cubrir adecuadamente los lugares de acceso al público y personal de la institución financiera y las cajas de atención al público; y,	**8.2. 1.5**	Identificación de vulnerabilidades	Las vulnerabilidades que pueden ser explotadas por amenazas para dañar los activos o la organización, deben ser identificados
39	**37.3** Los sistemas de grabación y almacenamiento de imágenes deben garantizar el archivo de por lo menos tres (3) meses de grabación, a través de cintas, de discos de video digital (DVD) o cualquier otro sistema.	**8.2. 1.4**	Identificación de controles existentes	Los controles existentes y planeados deben ser identificados

40	**ARTICULO 38.-** Las instituciones financieras establecerán estrictos procedimientos y normas que regulen o prohíban, según sea el caso, el uso de telefonía celular y cualquier otro mecanismo de comunicación desde el interior de sus instalaciones.	**8.2. 1.4**	Identificación de controles existentes	Los controles existentes y planeados deben ser identificados
41	Complementariamente se instalará mecanismos tecnológicos inhibidores de comunicación en el área designada para cajas y hall de cajas, que permitan bloquear la comunicación a través de celulares, excluyendo la zona donde se encuentran instalados los cajeros automáticos, cuando éstos se encuentren fuera de las áreas de atención al público.	**8.2. 1.4**	Identificación de controles existentes	Los controles existentes y planeados deben ser identificados
	Cajeros automáticos			
42	**39.1 Protección al teclado**.- Contar en todo momento con los dispositivos conocidos como "protectores de teclado", que de una manera efectiva impidan la visibilidad al momento que el usuario digita su clave personal;	**9.2**	Reducción del riesgo	El nivel de riesgo debe reducirse a través de la selección de controles de modo que el riesgo residual sea aceptable
43	**39.2 Protección contra clonación de tarjetas**.- Contar con dispositivos electrónicos y/o elementos físicos que impidan y detecten de manera efectiva la colocación de falsas lectoras de tarjetas, con el fin de evitar la clonación de tarjetas de débito o de crédito, además de los correspondientes mecanismos de monitoreo en línea de las alarmas que generen los dispositivos electrónicos en caso de suscitarse eventos inusuales;	**9.2**	Reducción del riesgo	El nivel de riesgo debe reducirse a través de la selección de controles de modo que el riesgo residual sea aceptable
44	**39.3 Iluminación**.- Los cajeros automáticos instalados en áreas externas a las oficinas de las instituciones financieras, deberán estar ubicados en zonas suficientemente iluminadas que permitan la visualización de toda actividad a su alrededor;	**8.2. 1.4**	Identificación de controles existentes	Los controles existentes y planeados deben ser identificados
45	**39.4 Programas de vigilancia en sitio**.- Contar con un programa regular de visitas al sitio donde se encuentra instalado el cajero automático, con la finalidad de garantizar que no existan objetos extraños, dispositivos u otros mecanismos sospechosos instalados en el cajero automático;	**8.2. 1.4**	Identificación de controles existentes	Los controles existentes y planeados deben ser identificados
46	**39.5 Mecanismo de anclaje**.- Los cajeros automáticos deben asegurarse adecuadamente al piso u otro soporte a fin de que dificulte su remoción, salvo el caso de aquellos que estén empotrados a la pared;	**9.2**	Reducción del riesgo	El nivel de riesgo debe reducirse a través de la selección de controles de modo que el riesgo residual sea aceptable
47	**39.6 Protección al software e información del cajero automático.-** Disponer de un programa o sistema de protección contra intrusos (Anti-malware) que permita proteger el software instalado en el cajero automático y que detecte oportunamente cualquier alteración en su código, configuración y/o funcionalidad. Así mismo, se deberá instalar mecanismos que sean capaces de identificar conexiones no autorizadas a través de los puertos USB, comunicaciones remotas, cambio de los discos duros y otros componentes que guarden o procesen información. En una situación de riesgo deben emitir alarmas a un centro de monitoreo o dejar inactivo al cajero automático hasta que se realice la inspección por parte del personal especializado de la institución;	**9.2**	Reducción del riesgo	El nivel de riesgo debe reducirse a través de la selección de controles de modo que el riesgo residual sea aceptable

48	**39.7 Procedimientos para el mantenimiento preventivo y correctivo en los cajeros automáticos.-** Disponer de procedimientos auditables debidamente acordados y coordinados entre la institución y los proveedores internos o externos para la ejecución de las tareas de mantenimiento preventivo y correctivo del hardware y software, provisión de suministros y recarga de dinero en las gavetas. Las claves de acceso tipo "administrador" del sistema del cajero automático deben ser únicas y reemplazadas periódicamente;	**8.2. 1.4**	Identificación de controles existentes	Los controles existentes y planeados deben ser identificados
49	**39.8 Accesos físicos al interior de los cajeros automáticos.-** Disponer de cerraduras de alta tecnología y seguridades que garanticen el acceso controlado al interior del cajero automático por parte del personal técnico o de mantenimiento que disponga de las respectivas llaves. Estas cerraduras deben operar con llaves únicas y no genéricas o maestras;	**9.2**	Reducción del riesgo	El nivel de riesgo debe reducirse a través de la selección de controles de modo que el riesgo residual sea aceptable
50	**39.9 Reportes de nivel de seguridad de los cajeros-** Comunicar oportunamente la información sobre los estándares de seguridad implementados en los cajeros automáticos, incidentes de seguridad (vandalismo y/o fraudes) identificados en sus cajeros automáticos y/o ambientes de software o hardware relacionados;	**8.2. 1.4**	Identificación de controles existentes	Los controles existentes y planeados deben ser identificados
51	**39.10** Establecer los mecanismos y procedimientos adecuados para: **39.10.1.** Revisar periódicamente los anclajes, iluminación y entorno del cajero automático;	**8.2. 1.4**	Identificación de controles existentes	Los controles existentes y planeados deben ser identificados
52	**39.10.2.** Abastecer de dinero permanentemente a los cajeros automáticos;	**NA**		
53	**39.10.3.** Atender las alarmas generadas por los dispositivos electrónicos de control instalados en los cajeros automáticos; y,	**9.1**	Descripción general del tratamiento de riesgos	Seleccionar los controles para reducir, retener, evitar o transferir los riesgos, y definir un plan de tratamiento de riesgos
54	**39.10.4.** Contar con personal capacitado para la operación y mantenimiento diario del cajero.	**7.22**	Criterios básicos - Criterios de evaluación del riesgo	Desarrollar el criterio de evaluación del riesgo de la organización, considerando requerimientos legales y regulatorios, y obligaciones contractuales
55	**39.11 Campañas de capacitación a usuarios sobre medidas preventivas y buen uso del sistema**.- Llevar a cabo campañas educativas para los usuarios acerca del uso, ubicación y medidas de seguridad pertinentes durante el uso del cajero, incluyendo la colocación de letreros alusivos a éstas en los recintos de los cajeros; y,	**9.2**	Reducción del riesgo	El nivel de riesgo debe reducirse a través de la selección de controles de modo que el riesgo residual sea aceptable
56	**39.12 Sistema de grabación o archivo de imágenes**.- Las instituciones financieras deberán mantener un archivo de cintas, de discos de video digital (DVD) o cualquier otro sistema de grabación o su equivalentes en cámaras fotográficas que cubra por lo menos noventa (90) días de archivo de imágenes.	**8.2. 1.4**	Identificación de controles existentes	Los controles existentes y planeados deben ser identificados
	Transporte de fondos y valores			
57	**40.1** Brindar apoyo a los clientes que solicitaren el servicio de seguridad para el retiro o depósito de dinero en efectivo, cuando se trate de altas sumas, esta actividad la realizarán en coordinación con la Policía Nacional;	**9.2**	Reducción del riesgo	El nivel de riesgo debe reducirse a través de la selección de controles de modo que el riesgo residual sea aceptable

58	**40.2** En lo relacionado a la recepción y envío de efectivo y valores, efectuar en áreas de acceso restringido al público y por personal autorizado por la institución, que eviten su exposición a riesgos, debiendo incluirse estos procedimientos en los "Manuales de seguridad y protección";	**9.2**	Reducción del riesgo	El nivel de riesgo debe reducirse a través de la selección de controles de modo que el riesgo residual sea aceptable
59	**40.3** En el traslado de fondos y valores, ser realizado por empresas debidamente autorizadas, utilizando vehículos blindados que cuenten con ventilación adecuada, sistemas de comunicación y personal de seguridad debidamente capacitado y entrenado. Las instituciones deberán mantener actualizadas las fichas con los nombres, firmas y fotografías del personal de la empresa transportadora de fondos y valores;	**8.2. 1.4**	Identificación de controles existentes	Los controles existentes y planeados deben ser identificados
60	**40.4** Sin perjuicio de lo dispuesto en el numeral 40.5, los vehículos blindados utilizados para tales transportaciones deberán cumplir con las normas técnicas determinadas en el artículo 9 del "Instructivo para el control, funcionamiento, supervisión del servicio de seguridad móvil en la transportación de valores y las normas de blindaje internacionales que deben cumplir los vehículos blindados que prestan este servicio", contenido en el Acuerdo Ministerial No. 1580 de 8 de julio del 2010; y,	**7.22**	Criterios básicos - Criterios de evaluación del riesgo	Desarrollar el criterio de evaluación del riesgo de la organización, considerando requerimientos legales y regulatorios, y obligaciones contractuales
61	**40.5** Aquellos bancos o instituciones financieras que requieran transportar por sus propios medios, fondos y valores, deberán hacerlo en los vehículos blindados mencionados en el numeral 40.3; o, en su defecto en compartimentos de seguridad, cuya combinación solo conozca el personal de la entidad encargado de recibir dichos fondos y valores, en compañía de un guardia de seguridad o personal de policía y dos (2) funcionarios de la entidad. En este último caso, los fondos y valores deben ser entregados en forma directa a las bóvedas y cajas fuertes.	**9.2**	Reducción del riesgo	El nivel de riesgo debe reducirse a través de la selección de controles de modo que el riesgo residual sea aceptable
	Contrato de pólizas de seguro			
62	**ARTÍCULO 41.-** Las instituciones financieras contratarán anualmente con las compañías de seguro privado, coberturas que aseguren a la entidad contra fraudes generados a través de su tecnología de la información, sistemas telemáticos, electrónicos o similares, como mínimo ante los siguientes riesgos: 41.1 Alteraciones de bases de datos; 41.2 Accesos a los sistemas informáticos y de información de forma ilícita; 41.3 Falsedad informática; 41.4 Estafa informática; 41.5 Daño informático; y, 41.6 Destrucción a la infraestructura a las instalaciones físicas necesarias para la transmisión, recepción o procesamiento de información.	**9.5**	Transferencia del riesgo	El riesgo debe ser transferido a un tercero que pueda gestionar más efectivamente un riesgo particular, dependiendo de la evaluación del riesgo

ANEXO G: Cuestionario de aplicación de buenas prácticas de Gobierno de TI

CUESTIONARIO SOBRE BUENAS PRÁCTICAS DE GOBIERNO DE TI[50]

OBJETIVO: Identificar el nivel de aplicación de buenas prácticas sobre Gobierno Corporativo de la tecnología de la información, de acuerdo al tipo y tamaño de institución.
Tiempo estimado: 6 a 10 minutos
El cuestionario es anónimo y confidencial, pero si gusta conocer los resultados consolidados de este cuestionario puede solicitarlos a kcoronel2009@gmail.com

Con una "X", señale el país en que se encuentra su organización:

X	Ecuador
	Perú, Colombia, Uruguay, Paraguay, Panamá, Costa Rica
	Argentina, Chile, Brasil, EEUU, México, Canadá
	Guatemala, Belice, Honduras, Nicaragua, El Salvador
	Venezuela, Bolivia, Guayanas, Cuba, Rep. Dominicana, Haití
	Europa, Asia
	Otro

Actividad económica principal a la que se dedica su organización:

	Industria
	Comercio
X	Servicios financieros, contables, auditoría y supervisión
	Seguros y reaseguros privados y seguridad social
	Logística corporativa
	Tecnología y comunicaciones
	Marketing, comunicación social, recursos humanos
	Salud, medicina y bienestar personal
	Otros servicios profesionales

Por favor indique el tamaño de su organización en Activos de sus estados financieros:

(en dólares)

	De $400 a $1,100,000
	De $1,100,001 a $9,600,000
	De $9,600,001 a $500,000,000
	De $500,000,001 a $2,000,000,000
X	Más de $2,000,000,000 (dos mil millones)

Para las siguientes afirmaciones, por favor marque con una "X" el nivel de aplicación en su organización:

[50] Los valores registrados en este cuestionario fueron colocados como ejemplos de cómo debe ser llenado el formulario, por una institución financiera ecuatoriana grande; sin embargo, el mismo podría ser llenado por cualquier tipo de institución de cualquier nacionalidad.

0 **La administración no está consciente de esta buena práctica**
1 **La administración está consciente pero no tiene voluntad para implementarla**
2 **La voluntad para implementar la buena práctica existe, pero no se ha planificado**
3 **Se ha planificado e iniciado la implementación**
4 **La implementación está avanzando conforme se planificó**
5 **La buena práctica está implementada y se reciben los beneficios esperados**
6 **Se miden los resultados para conocer desviaciones y se las gestiona**
7 **Su ejecución está optimizada, de forma sistematizada**

En la columna "Impacto", indique si una falla en la práctica sugerida tendría consecuencias de impacto alto, medio o bajo en el negocio

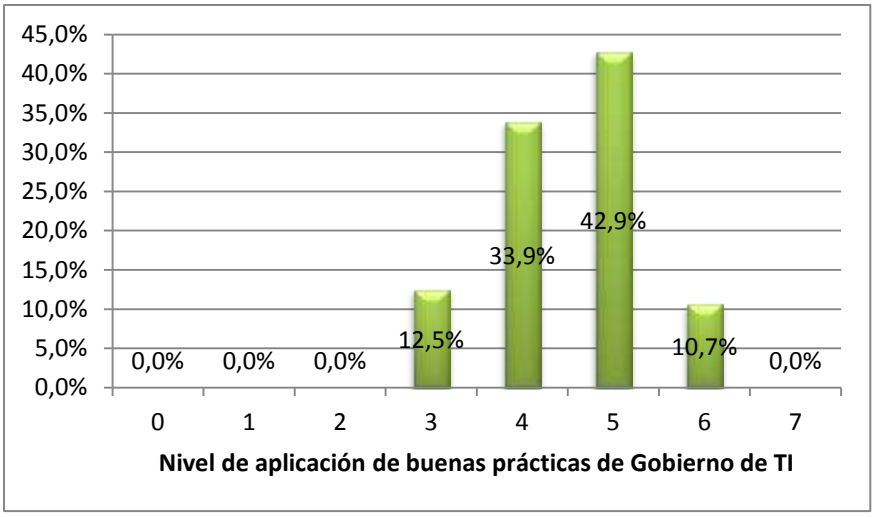
		Nivel de aplicación								
Buenas prácticas de Gobierno de TI		**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**Impacto**
1	Se toman en cuenta las capacidades y competencias de todas las partes interesadas internas: directivos, gerentes de proyectos, socios, reclutadores, desarrolladores, técnicos de TI, etc., para que sean asignados y asuman los diferentes roles en la organización						x			Alto
2	Se toman en cuenta las capacidades y competencias de todas las partes interesadas externas: competidores, proveedores, reguladores, auditores externos, financistas, etc., para la ejecución de los procesos y proyectos de la organización						x			Alto
3	La organización ha establecido principios y políticas de comportamiento para su personal, cuyo cumplimiento es evaluado periódicamente							x		Alto
4	El diseño de los procesos de la organización recoge las necesidades de provisión de información, ejecución, control y rendición de cuentas de las partes interesadas internas y externas					x				Medio
5	La estructura organizacional está formalmente documentada, y refleja los niveles de autoridad y responsabilidad para la toma de decisiones, apoyo y asesoría que requiere la organización para el logro de sus objetivos						x			Alto
6	Está formalmente aprobado y difundido a todo el personal un código de ética organizacional, o un documento equivalente, que se alinea con los principios y valores por los cuales la empresa subsiste							x		Alto
7	Están identificados y documentados los productores, custodios y consumidores de datos o información, internos y externos, y los niveles de acceso que deben tener.					x				Alto
8	Están identificados todos los servicios, infraestructura, tecnología y aplicaciones que requieren los procesos de negocio, así como sus niveles de servicio esperados					x				Alto
9	Existe un modelo estratégico de toma de decisiones para que las TI sean efectivas y estén alineadas con el entorno externo e interno de la organización					x				Alto
10	Existe un número suficiente de roles, responsabilidades y autoridades que participan en un Comité Institucional para gestionar el negocio y las tecnologías de forma adecuada						x			Alto
11	Periódicamente se generan reportes del Gobierno de TI a un Comité institucional y/o al Directorio o Consejo de Administración					x				Alto
12	Previo a realizar una inversión en TI, se analiza el valor que dicha inversión otorgará al negocio						x			Alto

13	Periódicamente, se evalúa el porcentaje del valor esperado que se ha obtenido de las inversiones en TI						x			Alto
14	El umbral de riesgo del negocio está identificado y comunicado						x			Medio
15	Se conoce el porcentaje de riesgos de TI que exceden el umbral de riesgos definido y se los gestiona oportunamente						x			Alto
16	Previo a la asignación de recursos a proyectos y procesos, se identifican los ahorros y beneficios que se lograrán a través de la utilización óptima de los recursos						x			Alto
17	Están establecidos principios de gestión de recursos; se identifica periódicamente el número de desviaciones y excepciones y se los gestiona oportunamente					x				Alto
18	Periódicamente se generan reportes informativos para las partes interesadas, según se analizan sus necesidades (transparencia)					x				Alto
19	La elaboración de informes para las partes interesadas es completa, oportuna y precisa					x				Alto
20	Se ha definido y se mantiene actualizado un conjunto eficaz de políticas, estándares y otros elementos catalizadores de la TI				x					Alto
21	Todas las partes interesadas tienen conocimiento de las políticas de TI y de cómo deberían implementarse				x					Medio
22	La estrategia de TI está alineada con la estrategia del negocio							x		Alto
23	Existe conciencia de la estrategia de TI y una clara asignación de responsabilidades para su entrega							x		Alto
24	Del plan estratégico de TI se pueden derivar objetivos a corto plazo claros, concretos, y trazables, que se pueden traducir en planes operativos						x			Alto
25	La arquitectura de la organización está definida mediante una descripción de alto nivel de las arquitecturas actual y objetivo, cubriendo los dominios de negocio, información, datos, aplicaciones y tecnología				x					Alto
26	Se utiliza el marco de arquitectura de empresa y una metodología común, así como un repositorio de arquitectura integrado, con el fin de permitir la reutilización de eficiencias dentro de la empresa				x					Alto
27	La innovación se permite y se promueve, y forma parte de la cultura de la empresa.						x			Alto
28	Los objetivos de la empresa se cumplen por la mejora de los beneficios de la calidad y/o la reducción de costos, como resultado de la identificación e implementación de soluciones innovadoras						x			Alto
29	Se ha definido una mezcla apropiada de inversión alineada con la estrategia corporativa, considerando al menos: costos, retorno de la inversión, beneficios, y riesgos.						x			Alto
30	Se evalúan y priorizan los casos de negocio de programas y proyectos antes de que se asignen los fondos						x			Alto
31	La estructura organizacional y las relaciones de TI son flexibles y dan respuesta ágil					x				Alto
32	Se mantienen y desarrollan las competencias y habilidades del personal					x				Alto
33	Los recursos humanos son gestionados eficaz y eficientemente, en cuanto a su suficiencia, adecuación y evaluación						x			Alto
34	Las estrategias, planes y requisitos de negocio están documentados y aprobados, y bien entendidos por el personal de TI					x				Alto
35	Existen buenas relaciones entre la empresa y las TI						x			Alto

36	Periódicamente, se evalúa el rendimiento de los proveedores según los requisitos acordados						x			Alto
37	El riesgo de los proveedores se evalúa y trata adecuadamente					x				Alto
38	Se definen requisitos de calidad para procesos y proyectos					x				Medio
39	Las partes interesadas están satisfechas con la calidad de los servicios y las soluciones de TI					x				Alto
40	Los riesgos tecnológicos están identificados de manera objetiva, y son analizados, gestionados y reportados a las partes interesadas							x		Alto
41	Las acciones de gestión de riesgos están efectivamente implementadas							x		Alto
42	Las partes interesadas relevantes están comprometidas con los programas y los proyectos						x			Medio
43	Se planifica la viabilidad, el alcance y los resultados de los programas y proyectos de TI, y están alineados con los objetivos corporativos						x			Alto
44	Se realizan revisiones frecuentes que garantizan que las actividades de los programas y proyectos se ejecutan de acuerdo a los planes, y se gestionan oportunamente las desviaciones						x			Alto
45	Los requerimientos funcionales y técnicos del negocio reflejan las necesidades y expectativas de la organización						x			Alto
46	Las soluciones propuestas por TI satisfacen los requerimientos funcionales, técnicos y de cumplimiento del negocio, así como sus objetivos de rentabilidad y de riesgos						x			Alto
47	Ante un nuevo cambio organizacional, se conforma un equipo de implementación competente y habilitado para conducir el cambio					x				Alto
48	El cambio deseado es comprendido y aceptado por las partes interesadas, y se lo integra a los procesos de la organización, de modo que sea sostenible en el tiempo					x				Alto
49	Se ha establecido el tipo de conocimiento que debe ser difundido entre las partes interesadas, y se han identificado y clasificado sus fuentes de información					x				Alto
50	El conocimiento es actualizado, utilizado y compartido, como parte de la cultura de la organización					x				Alto
51	Los procesos de la organización cuentan con objetivos y métricas aprobadas por las partes interesadas, cuyo cumplimiento es monitoreado periódicamente de forma efectiva				x					Alto
52	Los informes acerca del rendimiento y conformidad de los procesos son útiles y se entregan a tiempo a las instancias de revisión internas				x					Alto
53	Se proporciona aseguramiento independiente, interno o externo, de que el sistema de control interno es operativo y efectivo						x			Alto
54	Los procesos, recursos e información cumplen con los requisitos del sistema de control interno de la empresa, y las deficiencias son identificadas y comunicadas						x			Alto
55	La totalidad de los requisitos externos de cumplimiento se identifican oportunamente				x					Medio
56	Los requisitos externos de cumplimiento son tratados adecuadamente y dentro de los plazos exigidos					x				Medio
		0	0	0	7	19	24	6	0	
		0	1	2	3	4	5	6	7	

0.0 %	0.0 %	0.0 %	12.5%	33.9%	42.9%	10.7%	0.0 %	4.52 Promedio

Gracias por su colaboración!



Fuente: ISACA **Elaborado por**: Katalina Coronel Hoyos

Como se puede observar, el promedio ponderado del nivel de aplicación de estas buenas prácticas para este ejemplo es de 4.52, lo cual debe ser interpretado de acuerdo con la escala con la que el mismo fue obtenido, es decir:

0 La administración no está consciente de esta buena práctica
1 La administración está consciente pero no tiene voluntad para implementarla
2 La voluntad para implementar la buena práctica existe, pero no se ha planificado
3 Se ha planificado e iniciado la implementación
4 La implementación está avanzando conforme se planificó
5 La buena práctica está implementada y se reciben los beneficios esperados
6 Se miden los resultados para conocer desviaciones y se las gestiona
7 Su ejecución está optimizada, de forma sistematizada

En este caso, un promedio de 4.52 refleja un alto nivel de implementación de buenas prácticas, influido por un buen número de ellas que se encuentran implementadas y generando beneficios, y una pequeña porción que son medidas periódicamente.

ANEXO H: Activos de instituciones financieras por rangos

El objetivo de la segmentación de los activos de las instituciones financieras es determinar los rangos en los que se puede clasificar a las entidades de acuerdo con su tamaño, ya que ello implicaría la existencia de semejanzas en sus características de capacidad, tales como número de clientes, cobertura geográfica, número de productos, y especialmente su infraestructura operativa y tecnológica. Se incluye bancos privados, cooperativas, mutualistas, sociedades financieras, financieras públicas y tarjetas de crédito.

ACTIVOS POR TIPO DE INSTITUCIÓN AL 31-DIC-2012 (en miles de dólares)			
TIPO	**ENTIDAD**	**ACTIVOS**	**DIFERENCIAS**
SOCF	FIRESA	2,403.99	
COOP	SANTA ANA	8,357.87	5,953.88
COOP	9 DE OCTUBRE	9,061.14	703.27
COOP	LA DOLOROSA	10,430.27	1,369.12
COOP	COOPAD	10,474.67	44.41
BPRI	BP SUDAMERICANO	10,915.03	440.36
MUT	AMBATO	12,213.28	1,298.25
COOP	CALCETA	12,846.01	632.73
COOP	SAN PEDRO DE TABOADA	13,017.30	171.29
SOCF	INTERAMERICANA	13,048.70	31.40
COOP	COTOCOLLAO	19,028.47	5,979.77
SOCF	GLOBAL	19,643.79	615.32
COOP	SAN FRANCISCO DE ASIS	19,862.20	218.41
BPRI	BP DELBANK	20,199.11	336.91
SOCF	PROINCO	21,151.27	952.16
SOCF	FIDASA	24,253.60	3,102.33
COOP	GUARANDA	24,516.95	263.35
SOCF	LEASINGCORP	25,206.23	689.27
SOCF	CONSULCREDITO	26,302.16	1,095.94
BPRI	BP LITORAL	26,696.86	394.70
BPRI	BP COFIEC	27,590.16	893.30
COOP	11 DE JUNIO	27,642.66	52.50
MUT	IMBABURA	29,956.34	2,313.68
COOP	PADRE JULIAN LORENTE	30,752.10	795.76
COOP	COMERCIO	32,200.61	1,448.51
COOP	CHONE LTDA	33,229.35	1,028.74
COOP	CACPE LOJA	38,543.33	5,313.99
BPRI	BP COMERCIAL DE MANABI	43,263.14	4,719.81
COOP	CONSTRUCCION COMERCIO Y PRODUCCION LTDA	49,614.98	6,351.85
BPRI	BP FINCA	51,792.39	2,177.41
BPRI	BP D-MIRO S.A.	55,298.55	3,506.16
COOP	CACPE PASTAZA	56,519.78	1,221.23
SOCF	VAZCORP	62,282.67	5,762.89
COOP	SAN JOSE	62,649.44	366.76
COOP	TULCAN	69,115.02	6,465.59

COOP	PABLO MUÑOZ VEGA	69,552.15	437.13
COOP	CACPE BIBLIAN	71,748.71	2,196.56
COOP	SANTA ROSA	72,527.99	779.28
TCRE	INTERDIN	81,188.32	8,660.33
COOP	CODESARROLLO	82,324.88	1,136.56
COOP	CAMARA DE COMERCIO DE AMBATO	85,831.28	3,506.40
COOP	23 DE JULIO	86,334.82	503.54
COOP	ALIANZA DEL VALLE	97,676.50	11,341.68
COOP	ATUNTAQUI	97,762.60	86.10
COOP	15 DE ABRIL	97,793.53	30.93
COOP	EL SAGRARIO	103,835.70	6,042.16
MUT	AZUAY	103,898.54	62.84
COOP	ANDALUCIA	112,157.92	8,259.39
COOP	MUSHUC RUNA	127,091.29	14,933.37
SOCF	UNIFINSA	129,482.09	2,390.80
COOP	CACPECO	130,563.70	1,081.60
BPRI	BP CAPITAL	147,183.65	16,619.96
BPRI	BP TERRITORIAL	150,268.38	3,084.73
BPRI	BP COOPNACIONAL	156,561.30	6,292.92
BPRI	BP AMAZONAS	158,604.56	2,043.27
COOP	SAN FRANCISCO	166,815.58	8,211.02
COOP	RIOBAMBA	179,466.57	12,650.99
COOP	MEGO	191,672.47	12,205.90
COOP	OSCUS	193,760.32	2,087.84
COOP	COOPROGRESO	231,838.05	38,077.73
TCRE	PACIFICARD	245,164.25	13,326.19
COOP	29 DE OCTUBRE	266,189.26	21,025.01
FPUB	BANCO ECUATORIANO DE LA VIVIENDA	267,692.46	1,503.20
COOP	JARDIN AZUAYO	299,366.17	31,673.71
BPRI	BP SOLIDARIO	394,757.51	95,391.34
BPRI	BP LOJA	409,232.77	14,475.26
MUT	PICHINCHA	411,961.83	2,729.06
BPRI	BP UNIBANCO	415,244.60	3,282.77
BPRI	BP PROCREDIT	447,474.57	32,229.97
BPRI	BP CITIBANK	523,795.32	76,320.76
COOP	JUVENTUD ECUATORIANA PROGRESISTA	539,691.04	15,895.71
BPRI	BP GENERAL RUMIÑAHUI	572,069.02	32,377.98
BPRI	BP MACHALA	610,181.33	38,112.31
BPRI	BP PROMERICA	742,233.50	132,052.18
BPRI	BP AUSTRO	1,213,263.81	471,030.31
SOCF	DINERS CLUB	1,299,082.53	85,818.72
FPUB	BANCO DEL ESTADO	1,701,673.95	402,591.42
FPUB	BANCO NACIONAL DE FOMENTO	1,775,615.88	73,941.93
BPRI	BP INTERNACIONAL	2,118,817.28	343,201.40
BPRI	BP BOLIVARIANO	2,224,024.45	105,207.17
FPUB	CORPORACION FINANCIERA NACIONAL	2,599,120.89	375,096.43
BPRI	BP PACIFICO	2,601,146.12	2,025.24
BPRI	BP PRODUBANCO	2,601,146.12	0.00
BPRI	BP GUAYAQUIL	3,342,112.56	740,966.44
BPRI	BP PICHINCHA	8,092,708.41	4,750,595.85

Fuente: SBS, Boletines mensuales
Elaborado por: Katalina Coronel Hoyos