Gobierno de Seguridad de la Información, un enfoque hacia el cumplimiento regulatorio

Paúl Adrián Ochoa Arévalo

Facultad de Administración de Empresas, Universidad del Azuay, Av. 24 de Mayo 7-77 y Hernán Malo, Cuenca, Ecuador
pochoaa@uazuay.edu.ec

Resumen. La Seguridad de la Información es un asunto corporativo y es la forma como la deben percibir las Instituciones Financieras de manera que pueda encarar un entorno altamente competitivo y regulado; es por esta razón que la perspectiva correcta para llegar a un cumplimiento regulatorio satisfactorio, es tratar a esta actividad desde un enfoque de Gobierno, el cual es transversal en toda la organización no solamente un enfoque hacia los Sistemas de Información; bajo este contexto la aplicación de mejores prácticas tales como Cobit 5 e ISO 27000 nos dan los lineamientos claros para establecer el alcance de la implementación, objetivos de mejora, planificar soluciones y proyectos, definir las mediciones y una operación sostenible de los catalizadores que permitan un Gobierno y Gestión Empresarial de Seguridad de la Información.

Abstract. The information security is a corporate issue and this is how Financial Institutions must face it in order to deal with a highly and competitive environment that is regulated.
For this reason, the correct perspective to satisfactorily compliance regulations is accepting Information Security from a Government perspective, which is transversal in the whole institution and not only focused in the Information Systems.
Under this context, applying better tools like Cobit 5 and ISO 27000 give us a clear way to established: the implementation achievement, objectives improvement, project and solutions planning, mesuring tools, and sustainable operations of the enablers that allow a business Government and Business Management for Information Security.

Palabras Clave: Gobierno de Seguridad de la Información, Seguridad de la Información, Cobit 5, ISO 27000, cumplimiento regulatorio

1. Introducción

Sin lugar a dudas los sistemas de información forman parte integral de las prácticas negocio, los cuales entregan beneficios tales como: eficiencia en operaciones, mejora en la toma de decisiones, mejora en la atención de clientes, etc. Sin embargo, los mismos se enfrentan a riesgos propios del ambiente en los cuales se desarrollan. Además el incremento de regulaciones y leyes exigen mayor cumplimiento, lo que plantea la necesidad de establecer un marco para el Gobierno de la Seguridad de la Información, la cual puede ser aplicada a cualquier tipo de empresa ya sea pública o

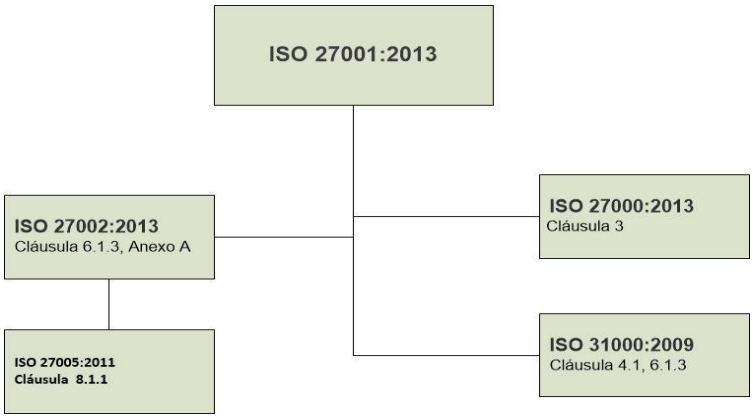
privada. A menudo este campo, se percibe con un enfoque limitado que únicamente abarca los Sistemas de Información y Tecnología relacionada; sin embargo, la Seguridad de la Información tiene un enfoque más amplio, por lo cual es necesario aplicar prácticas de Gobierno y Gestión de Seguridad de la Información. Desde esta perspectiva toma relevancia el marco Cobit para la Seguridad de la Información publicado por ISACA (Asociación de Auditoría y Control de Sistemas de Información) en 2012; el cual proporciona una visión transversal de la Seguridad de la Información en las organizaciones e incluye un conjunto de catalizadores los cuales son factores que influyen en el funcionamiento del Gobierno y Gestión de la empresa TI, dentro de los cuales tenemos:

- Políticas, procedimientos y prácticas
- Procesos
- Estructuras organizativas
- Cultura, ética y comportamiento
- Información
- Servicios, aplicaciones e infraestructura
- Personas, habilidades y competencias

Ante esta realidad, la Superintendencia de Bancos y Seguros, mediante resolución JB-2014-3066 emitida el 2 de septiembre del 2014, realiza una reforma a la norma de Gestión de Riesgo Operativo JB-2005-834, la cual indica entre sus principales cambios que las instituciones controladas deben tomar como referencia la ISO/IEC 27000 o la que lo sustituya.

ISO/IEC 27000, 27001, 27002 y 27005 son un conjunto de estándares desarrollados por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la Seguridad de la Información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña. [1]

Figura 1: ISO 27001:2013 y su relación con otras ISO [2]



En este contexto, resulta imperativo el establecimiento de un marco que permita Gobernar la Seguridad de la Información, el cual considere aspectos como:

- Seguridad de la Información como apoyo a la estrategia de negocio.
- Desempeño de la Seguridad de la Información por medio de la aplicación mejores prácticas como ISO 27002.
- Cumplimiento regulatorio.
- Recomendaciones efectuadas por organismos de control, así como recomendaciones efectuadas por auditores internos y externos.

2. Métodos y aplicación

La investigación de casos es particularmente útil dentro del área de Tecnología de la Información, debido a que nos permite el estudio de un fenómeno en su estado natural. Un estudio de un único caso es apropiado cuando este representa un caso de prueba para una teoría bien definida. [3]. De esta manera un caso de estudio es usado para el estudio del Gobierno de Seguridad de la Información, su desarrollo e implementación en una institución financiera.

Uno de los aspectos medulares dentro de la implementación de Gobierno de la Seguridad de la Información, radica en el establecimiento del alcance, el cual consideró: alineamiento estratégico, desempeño de Seguridad de la Información, cumplimiento normativo y la identificación de riesgos como insumo principal para la priorización de los esfuerzos de implementación.

Para el establecimiento del alcance basado en los catalizadores propuestos por Cobit se consideró:

a. **Traducir los requerimientos normativos en prácticas generalmente aceptadas.**

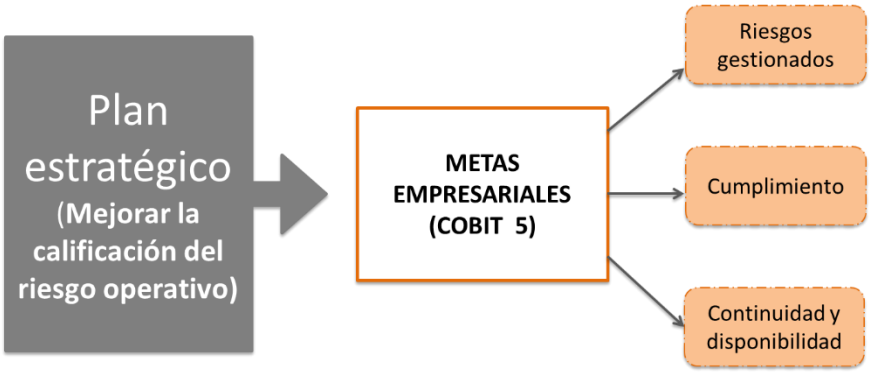
Cuadro 1: Mapeo Resol. JB 2005-834 actualizada con JB-2014-3066 y Cobit 5 (extracto)

No.	Requerimiento normativo	Procesos / práctica	Descripción práctica	Proceso	Descripción proceso
21.1	Determinar funciones y responsables de la implementación y administración de un sistema de gestión de seguridad de la información que cumpla con los criterios de confidencialidad, integridad y disponibilidad, acorde al tamaño y complejidad de los procesos administrados por el negocio; para lo cual las instituciones del sistema financiero podrán conformar un comité de seguridad de la información que se encargue de planificar, coordinar y supervisar el sistema de gestión de seguridad de la información…..	APO13.01	Establecer y mantener un SGSI.	APO13	Gestionar la seguridad
		APO01.01	Definir la estructura organizativa	APO01	Gestionar el Marco de Gestión de TI

b. **Enlace entre objetivos de negocio y objetivos de TI**

En función de las estrategias establecidas por la organización, se procedió a seleccionar el objetivo que guarda relación con Seguridad de la Información; y de esta manera haciendo uso de la cascada de metas propuesta en Cobit 5, se efectúo el mapeo con metas genéricas de negocio, metas de TI y procesos de TI; obteniendo de esta manera los procesos de TI que se requieren para soportar la estrategia de negocio.

Figura 2: mapeo plan estratégico – metas empresariales genéricas [4]



Nota: Calificación de riesgo operativo = opinión sobre la solvencia de corto plazo y la sostenibilidad institucional a largo plazo por medio de una evaluación completa de los riesgos, el desempeño y el posicionamiento en el mercado. [5]

Figura 3: mapeo plan estratégico de TI (PETI) – metas de TI genéricas [4]

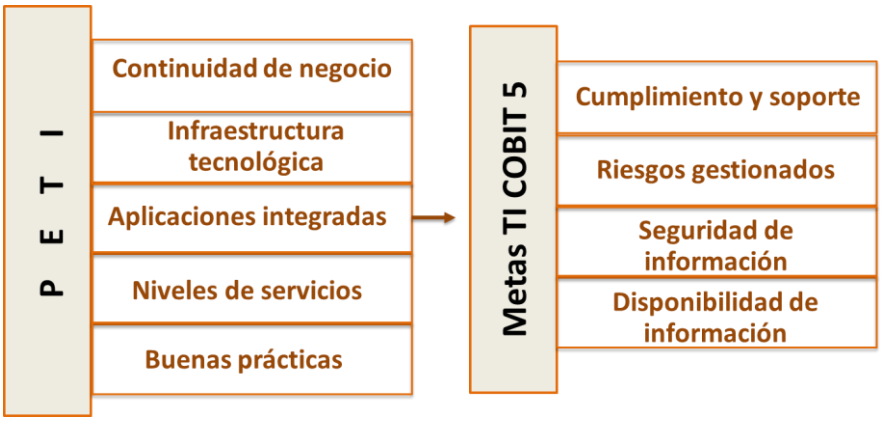
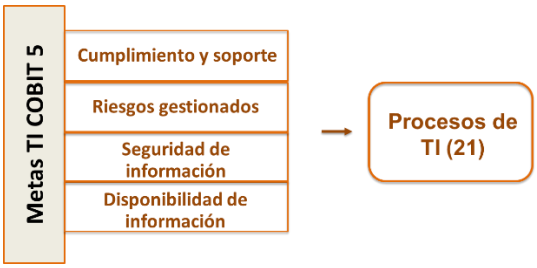


Figura 4: metas de TI genéricas VS procesos de TI a considerar dentro del alcance con enfoque en Seguridad de la Información [4]



c. **Enlace entre procesos de TI (Cobit 5) y norma ISO 27001/27002**

Cobit 5 integra las mejores prácticas dentro de las cuales está ISO 27001 y 27002 respectivamente, de esta manera se identificaron los procesos enfocados de manera principal con dichas normas, lo que nos permitió identificar los procesos Cobit que permiten aplicar una mejor práctica, de manera que se mejore el desempeño de la Seguridad de la Información.

Cuadro 2: mapeo procesos de TI (Cobit 5) y norma ISO 27001/27002 (Extracto)
[4]

Procesos de TI		ISO 27001:2013	ISO 27002:2013
APO10	Gestionar los proveedores	A.15 Relación con proveedores	13.2.4 Acuerdos de confidencialidad o de no divulgación
			15.1.1 Política de seguridad de la información para proveedores
			15.1.2 Abordar la seguridad dentro de acuerdos con proveedores
			7.1.1 Selección
			7.1.2 Términos y condiciones de empleo
			15.2.2 Gestión de cambios en los servicios de proveedores
			13.2.2 Acuerdos sobre la transferencia de información
			14.2.7 Outsourcing de desarrollo
			18.1.4 Privacidad y protección de datos personales
			13.1.2 Seguridad de los servicios de red
			14.2.6 Entorno de desarrollo seguro
			15.1.1 Política de seguridad de la información para proveedores
			15.1.3 Cadena de suministro para información y tecnología de las comunicaciones

d. **Establecimiento de los procesos de TI a implementar**

En base a los procesos de Gobierno y Gestión de TI los cuales fueron mapeados con: estrategia corporativa, ISO 27001/27002 y normativa vigente; se procedió a efectuar un mapeo que considere los tres elementos citados, de manera que se constituya el insumo inicial en el proceso de definición del alcance.

Cuadro 3: ejemplo de mapeo de alcance de procesos [4]

Proceso	Descripción	Plan estratégico	ISO 27002	Normativa	% de Contribución
EDM01	Asegurar el establecimiento y mantenimiento del marco de gobierno	NO	NO	SI	33%
EDM04	Asegurar la optimización de los recursos	SI	NO	SI	67%
EDM05	Asegurar la transparencia hacia las partes interesadas	NO	SI	SI	67%
APO01	Gestionar el marco de gestión de TI	SI	SI	SI	100 %
APO02	Gestionar la estrategia	NO	NO	SI	33%
APO05	Gestionar el portafolio	NO	NO	SI	33%

El porcentaje de contribución, nutre al factor de importancia denominado "Importancia para la compañía" de manera que:

Importancia para la compañía	Porcentaje de contribución
0	0%
1	33%
2	67%
3	100%

e. **Evaluación de los factores de importancia de los procesos**

A continuación se presenta los factores de importancia con sus respectivos criterios de evaluación:

Cuadro 4: Factores de importancia para los procesos de TI [4]

Importancia para la compañía	Capacidad del proceso basado en ISO/IEC 15504	Resultado de auditorías previas

0 = proceso no aplicable o proceso con importancia baja (no necesario para el cumplimiento con alguno de los criterios)	0 = no existe brecha en el nivel de capacidad	0 = No aplicable o conclusión de auditoría buena
1 = proceso necesario para cubrir 1/3 criterios: alineamiento estratégico, ISO 27002, normativa	1 = brecha en el nivel de capacidad **leve**	1 = Auditoría con conclusión que requiere mejoras menores
2 = proceso necesario para cubrir 2/3 criterios: alineamiento estratégico, ISO 27002, normativa	2 = brecha en el nivel de capacidad **significativa**	2 = Auditoría con conclusión que requiere mejoras importantes
3 = proceso necesario para cubrir 3/3 criterios: alineamiento estratégico, ISO 27002, normativa	3 = brecha en el nivel de capacidad **sustancial**	3 =Auditoría con conclusión deficiente o proceso nunca auditado

A partir de estos factores se procedió a evaluar cada uno de los procesos de Gobierno y Gestión de TI, de manera que pudimos calcular su respectivo factor de importancia con la siguiente fórmula:

Factor = importancia para la compañía + capacidad del proceso + resultado de auditorías previas

Cuadro 5: ejemplo evaluación de procesos [4]

Proceso	**Descripción**	**Importancia para la compañía**	**Capacidad del proceso**	**Resultado de auditorías previas**	
		Nivel	**Nivel**	**Nivel**	**Factor**
EDM01	Asegurar el establecimiento y mantenimiento del marco de gobierno	1	3	3	**7.00**
EDM04	Asegurar la optimización de los recursos	2	3	3	**8.00**
EDM05	Asegurar la transparencia hacia las partes interesadas	2	3	3	**8.00**
APO01	Gestionar el marco de gestión de TI	3	1	2	**6.00**
APO02	Gestionar la estrategia	1	1	2	**4.00**
APO05	Gestionar el portafolio	1	2	3	**6.00**

f. **Evaluación de riesgos procesos de TI**

Para cada proceso de Gestión y Gobierno de TI se identificó el riesgo inherente, su tipo y escenarios de riesgos. Posteriormente se asignó su respectivo impacto y prioridad a cada riesgo identificado.

Figura 5: evaluación de riesgos procesos de TI [4]

		TIPO DE RIESGO						
Proceso	Descripción	Habilitación de Beneficio Valor	Entrega del Programa / Proyecto	Entrega del servicio / para las operaciones TI	Riesgo	Impacto	Probabilidad	Nivel de Riesgo
EDM01	Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno	x			Proyectos que no se terminan de manera oportuna y fracasan por costes, retrasos, alcances mal definidos o cambios en las prioridades del negocio	4	3	12
		x			Sobrecoste aislado del presupuesto en los proyectos de TI	2	2	4
		x			Sobrecostes consistentes e importantes en los presupuestos de los proyectos de TI	4	2	8
		x			Ausencia de visión sobre el portafolio y la economía del proyecto	3	3	9
			x		Amplia dependencia y uso de soluciones informáticas para usuario final y ad hoc para necesidades informáticas importantes	4	3	12
			x		Soluciones de TI separadas y no integradas para soportar procesos de negocio	4	4	16
		x			El negocio no asume responsabilidad sobre aquellas áreas de las TI en las que debería, tales como requerimientos funcionales, desarrollo de prioridades y valoración de oportunidades a través de nuevas tecnologías	3	2	6
			x		Retraso ocasional en la entrega de proyectos de TI por parte del departamento de desarrollo interno	2	2	4
			x		Retraso rutinario importante en la entrega de proyectos de TI	4	2	8
			x		Retraso excesivo en el desarrollo de proyectos de TI externalizados	4	3	12
				x	Falta de cumplimiento con las regulaciones contables y de producción	4	3	12

El nivel de riesgo se calculó en función de la siguiente fórmula:

Nivel de riesgo = impacto x probabilidad

g. Evaluación de riesgos activos de TI

Se establecieron los procesos de negocio críticos en función de la metodología BIA(Análisis del Impacto al Negocio), lo que permitió obtener los activos de TI que soportan cada uno de los procesos, para los cuales se identificaron y evaluaron los riesgos de manera que se establecieron acciones para minimizar los riesgos identificados.

Figura 6: evaluación de riesgos activos de TI (Extracto) [4]

No:	Descripción del Bien	Valor		Razón (CID)		Responsable	Amenaza	Tipo	Fuente	Control	Vulnerabilidad	Consecuencias	Impacto	Probabilidad	Nivel de Riesgo	Promedio	Prioridad
		MA, A, M, B	Confidencialidad	Integridad	Disponibilidad												
Bases de Datos																	
2	Base de Datos de Tarjetas de Débito (Autorizador)	MA	MA	MA	MA	DBA	Falsificación de derechos	Compromiso de la información	Pirata informático, intruso ilegal	Política de control de accesos	Gestión deficiente de contraseñas	Tiempo de investigación y reparación	4	2	8	10	1

3. Resultado

Se priorizo los procesos en función del cálculo de factor de importancia y nivel de riesgo

Cálculo

Resultado = promedio (nivel de riesgo) * factor

Prioridad

- Se consideran los procesos con alta prioridad (Color rojo) de implementación a los que el resultado sea > 54, en base a la siguiente tabla:

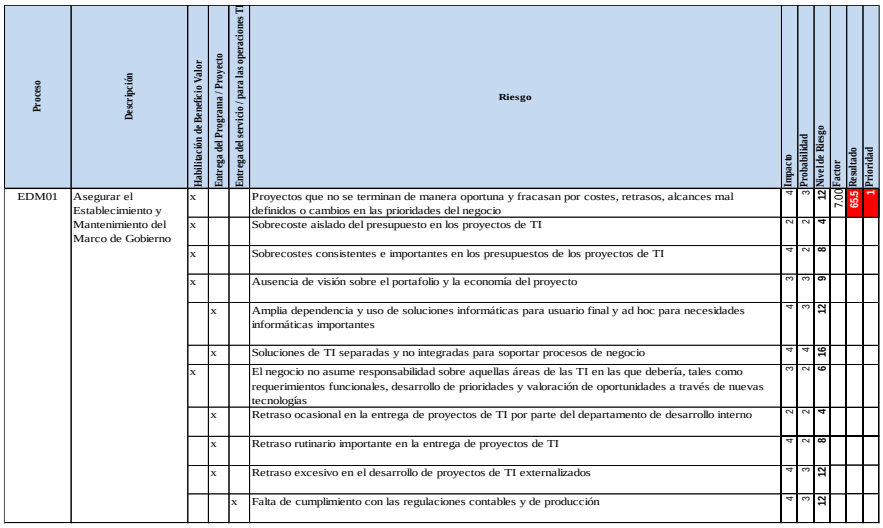
Cuadro 6: tabla para priorización de procesos

	Impacto	Probabilidad	Nivel de riesgo	Factor	Resultado
Referencia	3	3	**9**	6.00	**54.0**
	3	3	**9**		
	3	3	**9**		
	3	3	**9**		

Fuente: [6]

- Se consideran los procesos con prioridad media (Color amarillo) de implementación a los que el resultado sea > 36
- Se consideran los procesos con baja prioridad (Color verde) de implementación a los que el resultado sea > 0

Figura 7: cálculo prioridad [4]



Proceso	Descripción	Habilitación de Beneficio Valor	Entrega del Programa / Proyecto	Entrega del servicio / para las operaciones TI	Riesgo	Impacto	Probabilidad	Nivel de Riesgo	Factor	Resultado	Prioridad
EDM01	Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno	x			Proyectos que no se terminan de manera oportuna y fracasan por costes, retrasos, alcances mal definidos o cambios en las prioridades del negocio	4	3	12	7,00	65,5	1
		x			Sobrecoste aislado del presupuesto en los proyectos de TI	2	2	4			
		x			Sobrecostes consistentes e importantes en los presupuestos de los proyectos de TI	4	2	8			
		x			Ausencia de visión sobre el portafolio y la economía del proyecto	3	3	9			
			x		Amplia dependencia y uso de soluciones informáticas para usuario final y ad hoc para necesidades informáticas importantes	4	3	12			
			x		Soluciones de TI separadas y no integradas para soportar procesos de negocio	4	4	16			
		x			El negocio no asume responsabilidad sobre aquellas áreas de las TI en las que debería, tales como requerimientos funcionales, desarrollo de prioridades y valoración de oportunidades a través de nuevas tecnologías	3	2	6			
			x		Retraso ocasional en la entrega de proyectos de TI por parte del departamento de desarrollo interno	2	2	4			
			x		Retraso rutinario importante en la entrega de proyectos de TI	4	2	8			
			x		Retraso excesivo en el desarrollo de proyectos de TI externalizados	4	3	12			
				x	Falta de cumplimiento con las regulaciones contables y de producción	4	3	12			

Una vez se establecieron los procesos prioritarios se obtuvieron los demás catalizadores a implementar como:

Información: para cada proceso se identificó la información que los procesos deben generar o usar para su procesamiento:

Cuadro 7: relación procesos – información (extracto) [4]

Proceso	Descripción	Información
APO13	Gestionar la seguridad	Política de SGSI
		Declaración de alcance del SGSI
		Plan de tratamiento de riesgos de Seguridad de la Información
		Informes de auditoría de SGSI
		Casos de negocio para Seguridad de la Información
APO10	Gestionar los proveedores	Catálogo de proveedores
		Matriz de riesgos de proveedores
		Informes del resultado al monitoreo de cumplimiento de los proveedores
DSS02	Gestionar las peticiones y los Incidentes del Servicio	Esquema de clasificación de incidentes de Seguridad de la Información
		Procedimientos de recolección de evidencia
		Plan de respuesta a incidentes

		Documento de lecciones aprendidas

Políticas: se identificaron las políticas por medio de los procesos identificados con prioritarios

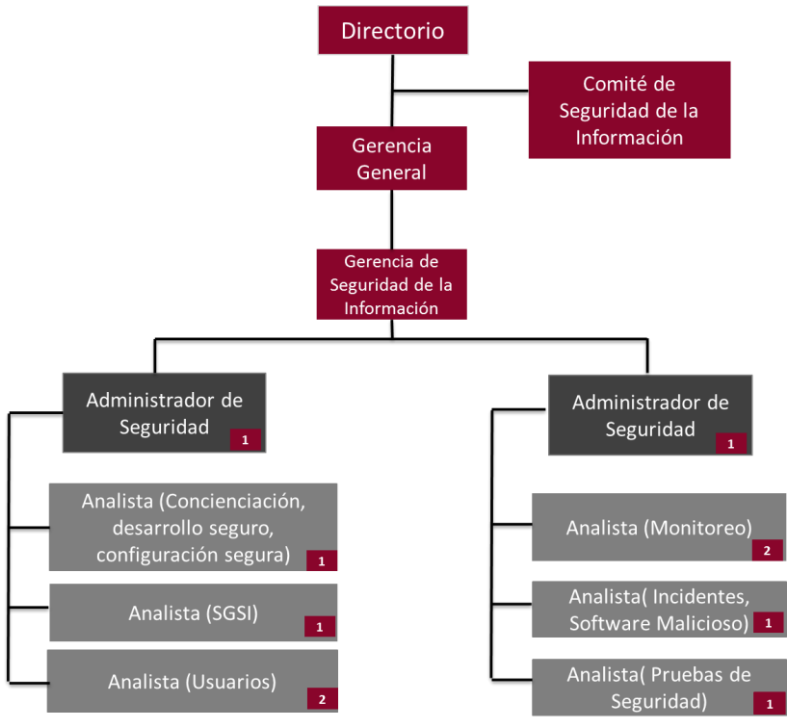
Cuadro 8: relación procesos – políticas seguridad de la información [4]

Proceso	Descripción	Políticas
APO13	Gestionar la seguridad	Política de SGSI
		Política de cumplimiento
		Política de gestión de activos
APO10	Gestionar los proveedores	Política de gestión de proveedores
DSS02	Gestionar las peticiones y los incidentes del servicio	Política de respuesta a incidentes
APO12	Gestionar el riesgo	Política de gestión de riesgos
DSS03	Gestionar los problemas	Políticas para tratar las causas raíz
DSS04	Gestionar la continuidad	Política de continuidad de negocio
DSS01	Gestionar las operaciones	Política de gestión de operaciones y comunicaciones
		Política de Seguridad física y ambiental
APO07	Gestionar los recursos humanos	Política de seguridad de información personal
		Política de reglas de comportamiento
		Políticas de confidencialidad debidamente firmadas

DSS05	Gestionar los servicios de seguridad	Política de prevención de software malicioso
		Política de conectividad
		Política de control de acceso
		Política de seguridad para dispositivos de usuario final

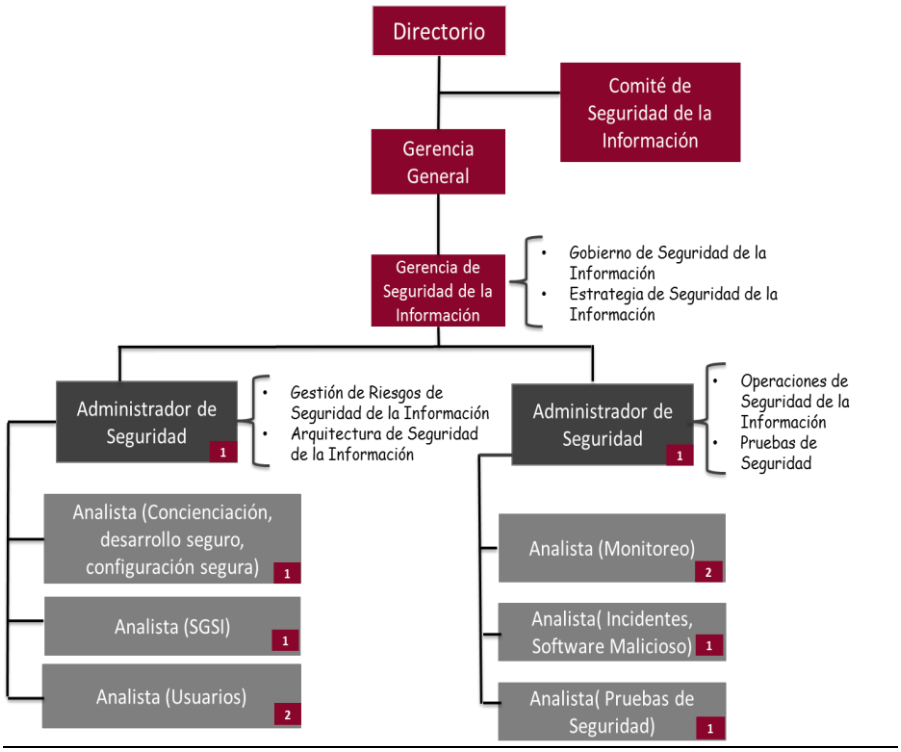
Estructuras organizacionales: por medio de las matrices RACI de los procesos priorizados, se identificaron las siguientes estructuras necesarias.

Figura 8: estructuras organizacionales [4]



Personas, habilidades y competencias: Tomando en consideración los procesos y roles claves, se consideraron las siguientes habilidades.

Figura 9: personas, habilidades y competencias en función procesos y roles claves. [4]



Cultura, ética y comportamiento: de manera que se influencie el comportamiento deseado en los aspectos de seguridad de la información se consideró la concienciación de Seguridad de la Información

Servicios, aplicaciones e infraestructura: se definieron los servicios de seguridad de la información tomando en consideración los roles y responsabilidades existente en la estructura organizacional, así como los procesos priorizados, objetivos de seguridad de la información y las necesidades de cumplimiento normativo:

- Concienciación sobre seguridad.
- Desarrollo seguro.
- Evaluaciones de seguridad.
- Sistemas adecuadamente asegurados y configurados.
- Accesos a los usuarios y derechos de acceso.
- Protección frente a software malicioso, ataques externos e intentos de intrusión.
- Respuesta a incidentes.
- Pruebas de seguridad.
- Proporcionar servicios de monitorización y alerta par a eventos relacionados con la seguridad.

Para las aplicaciones e infraestructura el alcance está en función de ISO 27005 la cual estableció la pauta en base a los procesos críticos de Negocio, para la obtención de los activos de TI que los soportan y necesitan protección.

Cuadro 9: aplicaciones

Aplicaciones	Localización / IP
Aplicación 1	192.x.x.17
Aplicación 2	192.x.x.57

Cuadro 10: sistemas operativos

Sistemas Operativos de Aplicaciones	Localización / IP
AIX	192.x.x.17
Windows 2008 Server SE SP 2	192.x.x.57

Cuadro 11: bases de datos

Bases de Datos	Localización / IP
Base de Datos Oracle	192.x.x.17
SQL Server	192.x.x.57

4. Discusión

La Superintendencia de Bancos y Seguros emitió la resolución JB-2005-834 en el año 2005 y dio un plazo de cumplimiento inicial a Octubre 2008; sin embargo, la misma resolución ha venido siendo actualizada y los plazos han sido modificados. Actualmente los mismo oscilan entre Diciembre 2014 y Diciembre 2015. Es por esta razón que el planteamiento de la investigación se enfoca en hacer un lado los criterios subjetivos de las Instituciones Financieras para el cumplimiento con cada punto normativo y establecer guías claras; apoyadas por mejores prácticas para que las instituciones vinculen sus estrategias y cumplimiento regulatorio, tales como Cobit 5 e ISO 27000; logrando de esta manera mejorar los niveles de cumplimiento y un Gobierno y Gestión de Seguridad de la Información, acorde a las necesidades de la Banca actual, tomando en cuenta un principio fundamental que la Seguridad de la Información es un asunto corporativo.

5. Conclusiones

A la Seguridad de la Información se la debe percibir desde un enfoque de Gobierno de Seguridad de la Información y la cual es responsabilidad de la Junta Directiva y Gerencia Ejecutiva.

El manejo conjunto de Cobit 5 para la Seguridad de la Información y la familia ISO 27000 permite establecer un Gobierno efectivo de Seguridad de la Información, debido a que Cobit provee una visión empresarial de seguridad de la información basada en catalizadores e ISO proporciona un mejor desempeño de Seguridad de la Información.

6. Referencias

[1] «iso27000.es,» 09 06 2013. [En línea]. Available: http://www.iso27000.es/iso27000.html.

[2] ISO, ISO/IEC 27001, ISO/IEC, 2013.

[3] D. K. G. a. M. M. Izak Benbasat, «The case research strategy in studies of information systems,» vol. 11, nº 3, 1987.

[4] P. Ochoa, *Elaboración de la Planeación de Auditoria de Seguridad de la Información Basada en Riesgos,aplicadas a una Institución del Sector Financiero*, Guayaquil, 2013.

[5] MicroFinanzaRating, «MicroFinanzaRating,» [En línea]. Available: http://www.microfinanzarating.com/index.php?option=com_content&view=article&id=145&Itemid=176&lang=es. [Último acceso: 10 10 2014].

[6] M. A. Diaz, «Evolución de Metodologías de Evaluación de Riesgos de Auditoría - Ejemplo de Aplicación,» Santiago, 2011.

[7] ISACA, Cobit 5 for Information Security, ISACA, 2012.

[8] Instituto Ecuatoriano de Nomalizacion, Gestion del Riesgo en la Seguridad de la Informacion, 2011.

[9] ISO, ISO/IEC 27002, ISO/IEC, 2013.

[10] ISACA, Cobit 5 Un Marco de Negocio para el Gobierno y la Gestión de la Empresa, ISACA, 2012.