REGULACIÓN COLOMBIANA Y SISTEMAS DE GESTIÓN.

Latorre Sánchez, Rodrigo Hernán
rodlat16@gmail.com
Universidad Piloto de Colombia

Resumen— En la actualidad, los sistemas de gestión, sin importar su objetivo, ya sean de seguridad, de calidad, para la administración de proyectos, gestión de la continuidad del negocio, etc., están marcando la pauta para que las empresas, ya sean de ámbito privado o financiero, así como de su naturaleza ya sea financiera, salud de servicios, etc., cuenten con diferentes marcos de referencia y buenas prácticas para que lograr que sus procesos y activos de información se le apliquen las debidos controles y los objetivos establecidos por la organización, sean cumplidos de una manera ordenada. En este artículo se realiza una relación entre los sistemas de gestión COBIT, la ISO 27001 y dos circulares externas, la 052 de 2007 y la 014 de 2009, expedidas por la Superintendencia Financiera de Colombia, en las cuales se especifican los criterios obligatorios para las entidades financieras cuenten con un sistema de gestión de seguridad de la información basado en buenas prácticas y en el estándar internacional ISO 27001, y el sistema de control interno, alineado con los objetivos de control de COBIT.

Índice de términos— ISO 27001, COBIT, ISO 22301, continuidad del negocio, riesgos, seguridad de la información, gobierno de TI.

Abstract— At present, management systems, regardless of their objective, whether security, quality, for project management, business continuity management, etc., are setting the standard for companies, whether Private or financial, as well as their nature, whether financial, health services, etc., have different frames of reference and good practices to ensure that their processes and information assets are applied due controls and established objectives By the organization, be fulfilled in an orderly manner. In this article a relationship is made between the COBIT management systems, ISO 27001 and two external circulars, the 052 of 2007 and the 014 of 2009, issued by the Superintendence of Finance of Colombia, which specify the mandatory criteria for Financial institutions have an information security management system based on best practices and the international standard ISO 27001, and the internal control system, aligned with COBIT control objectives.

Keywords— ISO 27001, COBIT, ISO 22301, business continuity, risk, information security, TI government.

I. INTRODUCCIÓN

Actualmente, los activos de una organización (el hardware, el software, los procesos, las personas y principalmente la información) son focos de amenazas, representados en millones de pesos en pérdidas. Debido al progreso de la informática, de las redes de comunicación, las redes sociales, etc., en donde la información está de forma digital representada por bytes, forma muy diferente de la original, pero que por esta razón no dejan de tener el mismo valor que su representación real, y en muchos casos esta información tiene mucho más valor que los reales.

Por esto y otros motivos, la información se convierte en el activo de mayor valor en una organización, y surge la necesidad de protegerla contra toda amenaza posible. Es así, que la seguridad de la información es un asunto tan importante para todas las organizaciones, ya que afecta directamente el negocio de la misma o de cualquier individuo.

Por otra parte, asociados a todos los conceptos de riesgos, vulnerabilidades, impactos, activos tecnológicos, etc., la implementación de sistemas de gestión de seguridad de la información alineados a la norma ISO 27001, sistemas de gestión de TI como lo es COBIT y otros más, generan un valor agregado a aquellas organizaciones donde se encuentra implementado, ya que el tratamiento de la seguridad de los activos de la misma organización y de la información de los clientes a los cuales prestan sus servicios.

En Colombia existen entidades de control, que mediante sus circulares externas han hecho que diferentes organizaciones (financieras en su mayoría) adopten modelos de gestión de TI (COBIT), modelos para la gestión de seguridad de la información (ISO 27001) y realizan la gestión de sus proyectos a través de metodologías internacionales (PMI). Una de las entidades es la Superintendencia Financiera de Colombia. Esta

entidad a través de las diferentes circulares de obligatorio cumplimiento, se ha apoyado en los anteriores estándares – y otros más - para su desarrollo, con el objetivo de establecer los suficientes controles de seguridad de la información y control en los procesos, mejorando los niveles de seguridad para la información de los clientes, su principal activo de información.

En el presente artículo se presenta una relación de como mediante una circular, La Superintendencia Financiera de Colombia, expide la circular externa 014 de 2009 en la cual se exige a las entidades financieras vigiladas a implementar estos sistemas de gestión, cambiando la forma de operar que y gestionar que se tenía antes de su publicación.

II. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO 27001

La norma ISO 27001 [3] es una norma internacional expedida por la *Organización Internacional de Normalización* (ISO por sus iniciales en inglés) y describe los requisitos para la implementación y operación de un *Sistema de Gestión de Seguridad de la Información* (SGSI por sus iniciales).

La versión más reciente es la publicada en 2013. Proporciona una metodología para implementar la seguridad de la información en una organización. Su implementación se puede realizar en cualquier tipo de organización.

Teniendo en cuenta lo anterior, la norma ISO 27000 de 2014, define seguridad de la información como: "*Preservación de confidencialidad, integridad y disponibilidad de la información*" [1]. Visto de esta manera, el objetivo de la seguridad de la información es proteger los activos de la organización y se dividen en los siguientes:

1) La información.

2) La infraestructura tecnológica que la soporta (software, hardware, redes, entre otros).

3) Los procesos que la involucran.

4) Las personas que la utilizan.

Es importante, además, que todos los empleados de la organización tomen conciencia sobre el manejo de la información de forma segura, ya que sería una pérdida de recursos y tiempo tener el macro sistema de seguridad de la información si los empleados que lo soportan no hacen parte activa del mismo.

Dado la clasificación anterior, las organizaciones están expuestas a todas las amenazas del mercado. Dichas amenazas son entes externos, que buscan puntos débiles en el sistema de la organización y generar un incidente lo que se traduce en un impacto, que puede ser de orden económico, reputacional, de disponibilidad, etc. Es así como muchas organizaciones año a año, tienen por objetivo obtener la certificación de un sistema de gestión de seguridad de la información, lo que es sinónimo de la gestión de riesgos asociados y la implementación de medidas o controles que minimicen el impacto en los activos de información, reducción de los costos generados por incidentes y la satisfacción de clientes y asociados. Como se observa en la figura 1, año a año se ha incrementado en número de certificados expedidos (al año 2012) a organizaciones a nivel mundial.

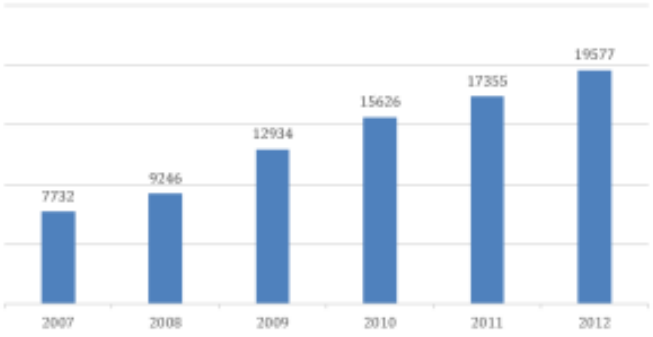

Fig. 1. Número de certificados expedidos a 2012 a nivel mundial [2].

Pero que a ciencia cierta, ¿qué es el SGSI? Es la sigla con la que comúnmente se denomina sistema de gestión de la seguridad de la información y su definición es: "*Un Sistema de Gestión de la Seguridad de la Información (SGSI) consiste en las políticas, procedimientos, directrices, Y los recursos y actividades asociados, gestionados colectivamente por una organización, en la búsqueda de la protección de sus activos de información*" [1]. Para entender mejor esta relación debemos iniciar por comprender que la información es toda aquella documentación (sin importar su forma física) que se encuentre en poder de la organización e independientemente de cómo se guarde y transmita, del origen o de la fecha de la creación.

Por esta razón, la seguridad de la información busca y está encaminado en el mantenimiento de la integridad, la confidencialidad y la disponibilidad de la información, así como de los sistemas implicados en su tratamiento dentro de la organización. Así que sobre estos tres términos se constituye la base sobre la cual se cimienta todo la construcción de la seguridad de la información:

A. Integridad: mantenimiento de la exactitud de los activos de la organización.

B. Confidencialidad: acceso a los activos de la organización únicamente por quienes estén autorizados.

C. Disponibilidad: los usuarios deben tener acceso a los activos de la organización a los cuales estén autorizados en el momento que lo requieran.

Mediante la implementación de un proceso metódico, sistemático, documentado y conocido por toda la organización se garantiza que la seguridad de la información es gestionada correctamente. Este proceso, es el que constituye un sistema de gestión de la seguridad de la información o SGSI y podría considerarse, por analogía con una norma tan conocida como la ISO 9001, como el sistema de calidad para la seguridad de la información.

El propósito de un sistema de gestión de la seguridad de la información en cualquier organización es, por tanto, garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

El proceso de implantación de un sistema de gestión de la seguridad de la información de acuerdo con la norma ISO 27001 debe seguir el modelo PDCA (plan-do-check-act, planear-hacer-verificar-actuar en español). Este modelo se muestra de forma gráfica en la figura 2.

Es importante destacar que uno de los componentes más importantes del SGSI, es la definición de una metodología que permita realizar la gestión del riesgo.

Esta actividad presente en la fase de planeación del sistema, debe permitir identificar, analizar, valorar y realizar el respectivo tratamiento de los riesgos evaluados. Dentro de las normas ISO, encontramos la norma ISO 31000 de 2009, la cual establece un marco para la gestión del riesgo, como se ve en la figura 3.

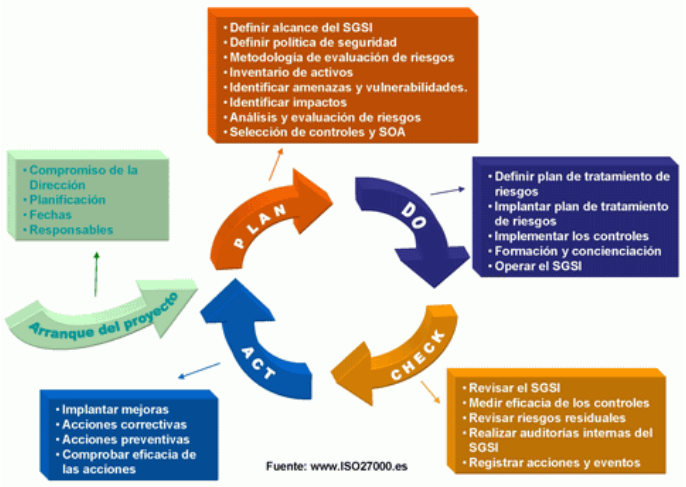

Fig. 2. Modelo PDCA para un Sistema de Seguridad de la Información basado en la norma ISO 27001 [2].

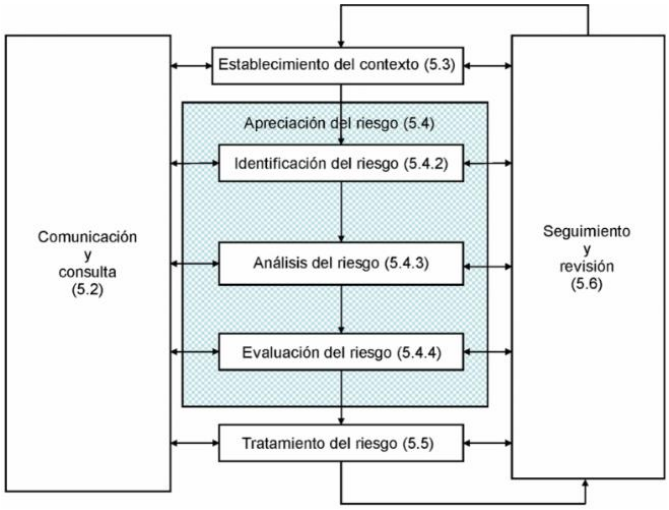

Fig. 3. Metodología para la gestión del riesgo ISO 31000:2011 [4].

III. OBJETIVOS DE CONTROL PARA LA INFORMACIÓN Y LA TECNOLOGÍA RELACIONADA

Como se ha dicho en el desarrollo del presente artículo, en la actualidad para la mayoría de las empresas, la información y la tecnología (hardware, software) que la soportan, son consideradas sus activos más importantes, aunque en la mayoría de ellas, no se les presta la adecuada atención.

La mayoría de empresas que tiene éxito son conscientes de los beneficios de las tecnologías de información y las utilizan para impulsar el valor entre sus clientes e interesados. Adicional, estas empresas implementan modelos de gestión del riesgo, incluyendo el riesgo de requerimientos regulatorios, así como la dependencia de los procesos de negocio en Tecnologías de Información.

Dado lo anterior, surge el término de Gobierno Corporativo, en la cual se relaciona las necesidades de una organización para asegurar el valor de los activos de tecnologías de información, la administración de los riesgos de tecnología, y los constantes requerimientos para el control de la información, como lo son las circulares obligatorias expedidas por las entidades de control (por ejemplo en Colombia la Superintendencia Financiera). Estos son elementos clave para el gobierno corporativo, y bajo la responsabilidad de directivos, se requiere estructuras y procesos a nivel organizacional que garanticen que las tecnologías de información sean sostenibles y se encuentren alineadas con los objetivos de la organización.

En Colombia, los entes de control regularmente expiden circulares con requisitos de obligatorio cumplimiento. De esta manera, y dependiendo del requisito exigido, las organizaciones deben integrar la calidad y la seguridad en su información, así como en todos sus activos. Y para lograr estos objetivos, las directivas deben optimizar el uso de los recursos disponibles de las tecnologías de información, incluyendo las aplicaciones, la información misma, la infraestructura (hardware e instalaciones) y las personas. Es así como para moderar estas responsabilidades, y para lograr el cumplimiento de sus objetivos, las directivas deben entender el nivel de su arquitectura empresarial y decidir qué tipo de gobierno y de control debe aplicar.

Para ayudar a la consecución de estas premisas, las organizaciones tienen a la mano a los *Objetivos de Control para la Información y la Tecnología Relacionada* (COBIT por sus iniciales en inglés), los cuales brindan buenas prácticas a través de un marco de trabajo de dominios y procesos, y presenta las actividades en una estructura manejable y lógica [5]. Estas prácticas están enfocadas fuertemente en el control y menos en la ejecución de las actividades y ayudarán a optimizar las inversiones habilitadas por TI, asegurarán la entrega del servicio y brindarán una medida contra la cual juzgar cuando las cosas no vayan bien [5].

Para que las tecnologías de información tengan éxito en satisfacer los requerimientos del negocio, la dirección debe implementar un sistema de control interno o un marco de trabajo. El marco de trabajo de control COBIT contribuye a estas necesidades de la siguiente manera:

A. Estableciendo un vínculo con los requerimientos del negocio.
B. Organizando las actividades de las tecnologías de información en un modelo de procesos generalmente aceptado.
C. Identificando los principales recursos de las tecnologías de información a ser utilizados.
D. Definiendo los objetivos de control gerenciales a ser considerados.

La orientación al negocio que enfoca COBIT consiste en alinear las metas de negocio con las metas de las tecnologías de información, brindando métricas y modelos de madurez para medir sus logros, e identificando las responsabilidades asociadas de los dueños de los procesos de negocio y de las tecnologías de información. La versión 5 de COBIT, se basa en cinco principios claves para el gobierno y la gestión de las TI empresariales como se ve la figura 4.

Mediante los 5 principios de COBIT, 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, la toma de decisiones y midiendo el rendimiento y el cumplimiento respecto a la dirección y metas acordadas [5].

Pero todo esto suena complicado para implantarlo en una organización. Así que nace la duda: ¿Vale la pena? Para responder a esta pregunta, se han realizado estudios los cuales reflejan la percepción del modelo COBIT en las organizaciones.

Según lo expone el señor Álvaro Iván Almanza Gómez en su ensayo “LA APLICACIÓN DE COBIT EN LAS ORGANIZACIONES ¿VALE LA PENA EL ESFUERZO?”, uno de esos estudios de ellos fue realizado por el grupo de servicios

financieros de ING en el año 2004 (IT Governance Institute, 2006) y concluye que las inversiones bien balanceadas entre las necesidades de producto y las tecnologías referentes de una organización representan un alto retorno de valor para las mismas comparadas con las inversiones hechas en otro tipo de bienes o servicios. A pesar de esto, en otro estudio hecho en el año 2005 por Son & Laurent se encontró que a pesar de que el 91% de los gerentes de las 335 compañías encuestadas reconocen que las tecnologías de información y comunicación son vitales para el éxito de sus organizaciones y han representado buenos dividendos, sólo la tercera parte se sienten tranquilos al hablar de cómo hacen el manejo y control de las mismas [8].

Fig. 4. Principios de COBIT 5 [5].

También expone que "Dependiendo de factores como el tipo de organización, su tamaño o la ubicación geográfica, se prioriza en mayor o menor forma, la consecución de estos objetivos. Es por esto que como siempre hemos visto, lo importante no es tomar todos los modelos al pie de la letra, sino que debemos desarrollar esa gran habilidad de aplicar lo más relevante de cada uno a nuestra situación específica, buscando alcanzar el éxito como un estado permanente y no como el resultado de una casualidad" [8].

Esto lleva a la siguiente conclusión: "La aplicación de este modelo no es sencilla. Aunque pueden parecer muchas razones para pensar más de dos veces el embarcarse en esta aventura, más en nuestro país donde la mayoría de organizaciones son de tipo pequeño y mediano y la inversión en este tipo de infraestructura no suele ser la prioridad, si los comparamos con las ventajas que nos ofrece la implementación del modelo, la decisión no debería ser tan difícil de tomar. Basta con que la alta gerencia se asesore adecuadamente y evalúe la disponibilidad que tendrá de tiempo y recursos para buscar este objetivo, teniendo siempre en cuenta que se debe tomar como que el hacerlo no va a ser un desgaste para la organización sino que, muy por el contrario, será una enorme ventaja competitiva con la cual logrará sacar distancias enormes frente a aquellas competidoras del mismo sector que no tengan esta decisión" [8].

Sin embargo en nuestro país, las entidades regulatorias, como lo es la Superintendencia Financiera de Colombia, en uso de sus facultades, ha desarrollado circulares que de una u otra manera ha llevado a que las entidades vigiladas implementen de manera obligatoria, ya que el modelo descrito en la circular 014 de 2009 para la implementación del Sistema de Control Interno está basado en el control de los procesos organizacionales de tecnologías de información descrito en COBIT. No obstante y aunque sea un trabajo arduo y extenso, la implementación de modelos como COBIT, aseguran que una organización, tenga definido sus procesos de tecnologías de información, y asociados a los procesos, se encuentren definidos los objetivos de cada proceso, se tengan claramente identificadas las entradas, las actividades a realizar y los productos de cada proceso, así como las métricas para la evaluación del desempeño de los controles que han sido implementados por proceso.

IV. CIRCULARES EXTERNAS SUPERINTENDENCIA FINANCIERA COLOMBIA [6][7]

La Superintendencia Financiera de Colombia es un organismo técnico adscrito al Ministerio de Hacienda y Crédito Público, con personería jurídica, autonomía administrativa y financiera y patrimonio propio. A través de ella, el presidente de la Republica, ejercerá la inspección, vigilancia y control sobre las personas que realicen actividades

financiera, bursátil, aseguradora y cualquier otra relacionada con el manejo, aprovechamiento o inversión de recursos captados del público.

Tiene por objetivo supervisar el sistema financiero colombiano con el fin de preservar su estabilidad, seguridad y confianza, así como, promover, organizar y desarrollar el mercado de valores colombiano y la protección de los inversionistas, ahorradores y asegurados. Los objetivos estratégicos de la superintendencia son los siguientes:

1) Fortalecer la gestión funcional de la SFC.

2) Desarrollar la supervisión basada en riesgos bajo la metodología MIS.

3) Fortalecer la supervisión consolidada.

4) Robustecer los requerimientos prudenciales para las entidades vigiladas.

5) Contribuir con mecanismos de inclusión y educación financiera.

6) Velar por la protección al Consumidor Financiero.

7) Apoyar el desarrollo del Mercado de Capitales.

8) Fortalecer la gestión administrativa, financiera y defensa judicial de la Entidad.

De esta manera, dado el objeto principal, y sus objetivos estratégicos, la Superintendencia Financiera de Colombia expide regularmente circulares para las entidades que vigila y controla. Estas circulares son carácter obligatorio y a continuación presentamos dos circulares que hacer relevancia a los sistemas de gestión que tratamos en el presente artículo:

A. Circular 052 de 2007.

Circular expedida por la Superintendencia, en donde se establecen los requerimientos mínimos de seguridad y calidad en el manejo de información a través de medios y canales de distribución de productos y servicios para clientes y usuarios. Considerado necesario instruir a las entidades sometidas a inspección y vigilancia sobre los requerimientos mínimos de seguridad y calidad que deben atender para el manejo de la información a través de los diferentes medios y canales utilizados para la distribución de los productos y servicios que ofrecen a sus clientes y usuarios [6].

B. Circular 014 de 2009.

Circular expedida por la Superintendencia, que en uso de sus facultades legales, en especial de la consagrada en el numeral 9° del artículo 11 del Decreto 4327 de 2005, dada la importancia que deben otorgar las entidades supervisadas al fortalecimiento de los sistemas de control interno y a la evaluación continua de su eficiencia, estima necesario que ellas estructuren, implementen y mantengan un Sistema de Control Interno (en adelante SCI) o lo adecuen, según el caso, a los lineamientos establecidos en la presente circular, de tal manera que dicho sistema contribuya al logro de sus objetivos y fortalezca la apropiada administración de los riesgos a los cuales se ven expuestas en el desarrollo de su actividad, realizándolas en condiciones de seguridad, transparencia y eficiencia [7].

Estas dos circulares en especial, que son de carácter obligatorio para las entidades vigiladas, están alineadas con los Objetivos de Control para la Información y la Tecnología relacionada - COBIT y los lineamientos para la implementación de un sistema de gestión de seguridad de la información basado en la norma ISO 27001, lo cual demuestra que los sistemas de gestión apoyan la normatividad de las organizaciones y más aún cuando los entes reguladores, expiden este tipo de regulaciones que son de carácter obligatorio.

V. REGULACIÓN COLOMBIANA Y SISTEMAS DE GESTIÓN

Mediante las circulares expedidas por la Superintendencia, las organizaciones financieras de Colombia se han visto en la obligación de implementar sistemas de gestión y controles asociados a los activos de información. Dichas circulares basan sus requisitos en estándares reconocidos internacionalmente. De esta manera el Sistema de Gestión de Seguridad de la Información basado en la norma internacional "*ISO 27001:2013 SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN"* se convierte en aliado de la circular 052 del 2007 (y sus diferentes actualizaciones) la cual imparte instrucciones relacionadas con los requerimientos mínimos de seguridad y calidad en el manejo de información a través de medios y canales de distribución de productos y servicios para clientes y usuarios [6] y los "*Objetivos de Control para la*

Información y la Tecnología relacionada (COBIT®)" se toma como base para el desarrollo de la circular externa 014 de 2009 [7], la cual Imparte instrucciones relativas a la revisión y adecuación del Sistema de Control Interno (SCI) de las entidades supervisadas.

Si revisan los puntos específicos descritos en los anexos de cada circular y se realiza un mapeo con los numerales de cada sistema de gestión (SGSI y COBIT) se obtiene lo siguiente:

A. CIRCULAR 052, numeral 3.1. Seguridad y Calidad.

En desarrollo de los criterios de seguridad y calidad, y considerando los canales de distribución utilizados, las entidades deberán cumplir, como mínimo, con los siguientes requerimientos: "Gestionar la seguridad de la información, para lo cual podrán tener como referencia los estándares ISO 17799 y 27001, o el último estándar disponible" [6].

Esto quiere decir que las organizaciones vigiladas por la Superintendencia, deben obligatoriamente realizar la implementación de un Sistema de Gestión de Seguridad de la Información, basado en la norma ISO 27001. Si bien se ve en el requerimiento, no hay ninguna exclusión de los requisitos del sistema ni de los controles descritos en el anexo A.

B. Circular 014, numeral 7.3. DEFINICIÓN Y OBJETIVO DEL SISTEMA DE CONTROL INTERNO [7].

"Se entiende por Sistema de Control Interno, al conjunto de políticas, principios, normas, procedimientos y mecanismos de verificación y evaluación establecidos por la junta directiva u órgano equivalente, la alta dirección y demás funcionarios de una organización para proporcionar un grado de seguridad razonable en cuanto a la consecución de los siguientes objetivos:

1) Mejorar la eficiencia y eficacia en las operaciones de las entidades supervisadas. Para el efecto, se entiende por eficacia la capacidad de alcanzar las metas y/o resultados propuestos; y por eficiencia la capacidad de producir el máximo de resultados con el mínimo de recursos, energía y tiempo.

2) Prevenir y mitigar la ocurrencia de fraudes, originados tanto al interior como al exterior de las organizaciones.

3) Realizar una gestión adecuada de los riesgos.

Aumentar la confiabilidad y oportunidad en la Información generada por la organización.

4) Dar un adecuado cumplimiento de la normatividad y regulaciones aplicables a la organización.

En la medida en que se logren los objetivos antes mencionados, el SCI brindará mayor seguridad a los diferentes grupos de interés que interactúan con la entidad" [7].

C. Circular 014, numeral 7.5. ELEMENTOS DEL SISTEMA DE CONTROL INTERNO [7].

Para el cumplimiento de los principios y objetivos indicados con anterioridad, las entidades supervisadas deberán consolidar una estructura de control interno que considere por lo menos los elementos que se señalan a continuación:

1) Numeral 7.5.1. Ambiente de Control.
2) Numeral 7.5.2. Gestión de Riesgos.
3) Numeral 7.5.3. Actividades de Control.
4) Numeral 7.5.4. Información y Comunicación.
5) Numeral 7.5.5. Monitoreo.
6) Numeral 7.5.6. Evaluaciones independientes.

Al realizar el desglose y mapeo con las actividades puntuales del requerimiento de la Circular con los 4 dominios de COBIT, como se observa a continuación:

TABLA I
MAPEO REQUISITOS CIRCULAR 014 – PROCESOS COBIT

Requisito circular 014	Proceso COBIT
Numeral 7.3	No aplica
Numeral 7.5.1	PO – Planear y Organizar
Numeral 7.5.2	PO – Planear y Organizar
Numeral 7.5.3	AI – Adquirir e Implementar
Numeral 7.5.4	DS – Entrega y Soporte
Numeral 7.5.5	ME – Monitorear y Evaluar
Numeral 7.5.6	ME – Monitorear y Evaluar

Tabla de relación requisitos Circular 014 para los numerales relacionados con tecnología con los 4 dominios de COBIT 4.1, Fuente: el autor.

Lo anterior demuestra que las organizaciones vigiladas por la Superintendencia, adicional al SGSI, deben implementar sus sistemas de control interno, bajo los lineamientos de las mejores prácticas de COBIT.

VI. CONCLUSIONES

En la actualidad, la información se convierte en el activo de mayor valor en una organización, y surge la necesidad de protegerla contra toda amenaza posible. Es así, que la seguridad de la información es un asunto tan importante para todas las organizaciones, ya que afecta directamente el negocio de la misma o de cualquier individuo.

Durante los años, la relación entre una organización y las tecnologías se ha vuelto muy estrecha. Gracias a entidades como ISACA, la BSI, ISO, etc., se han construido estándares que colaboran a las entidades en la implementación de sistemas de gestión que mejoran los procesos organizacionales, aumentando la eficiencia y eficacia de la información. Esto mejora la percepción de los clientes e interesados de las organizaciones.

Tener un modelo estándar como COBIT, para la definición de procesos de tecnologías de información dentro de una organización, permite identificar la caracterización completa de dichos procesos, identificando los objetivos, las entradas, los responsables, las actividades, las salidas, los controles y los mecanismos para la medición de los objetivos de cada proceso.

Al ser normas internacionales, las organizaciones que a la fecha han implementado el Sistema de Gestión de Seguridad de la Información – SGSI – y los Objetivos de Control para la Información y la Tecnología relacionada – COBIT, pueden lograr ser casos de éxito a nivel internacional, y modelos a seguir para las diferentes organizaciones de otros sectores, como lo son los de servicios, de salud, etc.

No obstante y aunque sea un trabajo arduo y extenso, la implementación de modelos como COBIT, aseguran que una organización, tenga definido sus procesos de tecnologías de información, y asociados a los procesos, se encuentren definidos los objetivos de cada proceso, se tengan claramente identificadas las entradas, las actividades a realizar y los productos de cada proceso, así como las métricas para la evaluación del desempeño de los controles que han sido implementados por proceso.

En países como Colombia, las entidades de control, han utilizado estándares internacionales, para soportar normas y regulaciones a aplicar dentro de las organizaciones vigiladas. La implementación de dichos estándares, y de las mejores prácticas, estandarizan los modelos empresariales, definiendo sus procesos de tecnologías de información y los métodos para medir dichos procesos.

Mediante esta implementación, las entidades de control buscan estandarizar la definición de procesos y de controles en las entidades vigiladas, mejorando el funcionamiento, los controles y la percepción de los clientes, lo que lleva a mejorar la confianza entre las partes.

REFERENCIAS

[1] INTERNATIONAL STANDARD. (2014, Enero). ISO/IEC 27000 Information technology — Security techniques — Information security management systems — Overview and vocabulary.

[2] Kosutic, Dejan. (2013). What is ISO 27001? [Online]. Disponible en: http://advisera.com/27001academy/es/que-es-iso-27001/ .

[3] ICONTEC. (2013, Diciembre). NORMA TÉCNICA COLOMBIANA NTC-ISO-IEC 27001.

[4] ICONTEC. (2011). NORMA TÉCNICA COLOMBIANA 31000:2011, Gestión del riesgo. Principios y directrices.

[5] ISACA. (2012). COBIT 5 AN ISACA FRAMEWORK. Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa.

[6] Superintendencia Financiera de Colombia. (2007, Octubre). Circular Externa 052 [Online]. Disponible en: https://www.superfinanciera.gov.co/descargas?com=institucional&name=pubFile13713&downloadname=ce052_07.rtf.

[7] Superintendencia Financiera de Colombia. (2009, Mayo). Circular Externa 014 [Online]. Disponible en: https://www.superfinanciera.gov.co/descargas?com=institucional&name=pubFile22255&downloadname=ce014_09.doc.

[8] Superintendencia Financiera de Colombia. (2016, Noviembre). Acerca de la SFC [Online]. Disponible en: https://www.superfinanciera.gov.co/jsp/loader.jsf?lServicio=Publicaciones&lTipo=publicaciones&lFuncion=loadContenidoPublicacion&id=60607

[9] Almanza Gómez, Álvaro Iván. (2012). "*La aplicación de COBIT en las organizaciones ¿vale la pena el*

esfuerzo?" [Online]. Disponible en: http://repository.unimilitar.edu.co/bitstream/10654/6537/2/AlmanzaGomezAlvaroIvan2012.pdf

Latorre Sánchez, Rodrigo Hernán.
Ingeniero de Sistemas de la Universidad Distrital Francisco José de Caldas, con especialización en Proyectos Informáticos, título propio de la Universidad Distrital Francisco José de Caldas. Auditor interno Sistema de gestión de Continuidad del Negocio ISO 22301:2012 expedido por la entidad SGS. Experiencia en seguridad de la información, gestión de riesgos, continuidad del negocio, gestión de proyectos, auditoria y desarrollo de software en lenguajes JAVA, .NET, y gestión de bases de datos.