.

¿Cómo integra COBIT 4.1 el estándar ISO 27001 para obtener un gobierno de seguridad de la información?

Estrada Rodríguez, Leidy Johanna, Páez Arévalo, Yenny Patricia.
Johanna.estrada@hotmail.com, ypatyko_86@hotmail.com
Universidad Piloto de Colombia

Abstract—In this paper we present the integration and connection of COBIT framework and the ISO 27001 standard, who base their structure on the Deming cycle; model used to establish, implement, monitor and improve the ISMS within organizations. Deming cycle aka PDCA phase starts in "plan", resumes the execution of activities or "do" and subsequently "check" results and implement corrective actions within the phase "act". Also shows how the COBIT framework integrates the security controls of information, established in ISO 27001, helping to strengthen and properly guide the implementation of the SGSI for the benefit of information security in organizations.

Resumen—En este artículo se presenta la integración y relación del marco de referencia COBIT y la norma ISO 27001, que basan su estructura en el ciclo Deming; modelo utilizado para establecer, implementar, monitorear y mejorar el SGSI en las organizaciones. El ciclo Deming también conocido como PDCA, inicia en la fase de "planear", continúa con la ejecución de actividades o "hacer" y posteriormente "verificar" los resultados e implementar medidas correctivas dentro de la fase "actuar". Adicionalmente muestra como el marco de referencia COBIT integra los controles de seguridad de la información, establecidos en la norma ISO 27001, ayudando a fortalecer y guiar de manera apropiada la implementación del SGSI en beneficio de la seguridad de la información en las organizaciones.

Índice de Términos— *Ciclo Deming CID, COBIT, Gobierno de T.I., ISACA, Standard, SGSI.*

I. INTRODUCCIÓN

Hoy en día es necesario que las organizaciones certifiquen sus procesos para ser competitivas, reconocidas y confiables. La normalización y reorganización de los procesos ha generado en las empresas el reto de conocer, integrar e implementar múltiples estándares que permitan cumplir los requerimientos que cada una de estas certificaciones requiere.

En algunas ocasiones se implementan variedad de estándares de una forma independiente a los demás procesos que no contribuyen con los objetivos estratégicos y generan desorganización, mal uso de los recursos, sobrecostos e incumplimientos.

Es importante que las empresas definan e implementen un marco de gobierno de T.I., para la organización de los procesos alineado a los objetivos estratégicos.

Si bien, la implementación de estándares depende de la aplicabilidad y requerimientos normativos de cada organización, el marco de gobierno de T.I, debe contribuir como columna vertebral desde la perspectiva tecnológica en su implementación.

En este documento plantearemos la integración entre COBIT 4.1 como el marco de gobierno de T.I. y el estándar ISO 27001, que entre sí contemplan controles de seguridad de la información.

"De acuerdo con ISO/IEC 27014 Information Security Governance, el gobierno corporativo es la forma como se toman decisiones corporativas, para definir la dirección y para ejecutar las decisiones tomadas."
Para gobernar las actividades corporativas de forma efectiva:

- Un marco de gestión de riesgo debe ser establecido

- Debe soportarse en un sistema de control interno
- La dirección debe responder por sus acciones" [1].

COBIT 4.1 (Objetivos de Control para la Información y Tecnología relacionada) es un marco de gobierno y gestión de T.I., creado y actualizado por ISACA (Information System Control Standard).

"COBIT brinda un lenguaje común a los ejecutivos de negocios para comunicar las metas, objetivos y resultados a los profesionales de auditoría, informática y otras disciplinas."[2]. Está conformado por 4 dominios, 34 procesos de T.I, 28 objetivos de T.I y 17 objetivos de negocio e interrelaciona sus componentes como se observa en la "fig1".

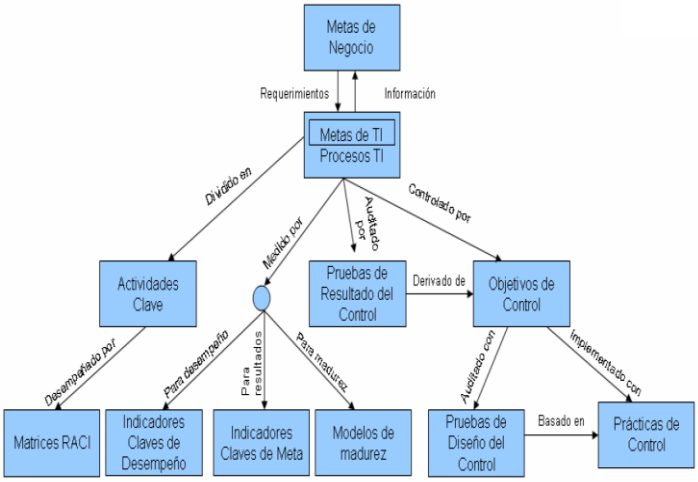

Fig1. Interrelación de los componentes de COBIT. Tomado de COBIT 4.1. IT Governance Institute

ISO 27001 es un estándar que consta de 10 dominios en los que detalla controles de seguridad de la información con un nivel mayor que COBIT, pero que al integrarse con este marco de gobierno de T.I., se considera como una guía apropiada de implementación de los SGSI.[1]

La combinación de COBIT 4.1 y la ISO 27001 nos contextualiza en un gobierno de seguridad de la información (ISG) que de acuerdo con ISACA, "consiste en el liderazgo, estructura organizacional y proceso para proteger la información. Es un subconjunto del gobierno corporativo de la organización que provee dirección estratégica, garantiza los objetivos establecidos, gestiona los riesgos de forma apropiada, usa los recursos organizacionales responsablemente y monitorea el éxito o falla del programa de seguridad de la organización." [3].

II. Retos de las organizaciones en S.I.

El Global State of Information Security Survey en el año 2010, realizó un estudio en el que se encontró que el 77% de las empresas se encuentran implementando estándares de seguridad para asumir y cumplir los requerimientos normativos y legales.

Continúa la ocurrencia de incidentes de seguridad, de los cuales el 39% desconoce su origen y no se le ha prestado el respectivo tratamiento.

Las nuevas tecnologías incrementan la necesidad de reducir costos en hardware, software y servicios pero aumentan las vulnerabilidades de seguridad. Es necesario contar con mecanismos que mitiguen estos riesgos y que a su vez contribuyan con la visión del negocio.

Reducir, mitigar y transferir los riesgos mayores es para el 81% de las organizaciones unos de los mayores retos en Seguridad de la Información.[2]

III. Ciclo Deming (PHVA)

Este ciclo también conocido como PDCA, permite la mejora continua durante la implementación de estándares y procesos. Inicia en la fase de "planear", continua con la ejecución de actividades o "hacer" para posteriormente "verificar" los resultados e implementar medidas correctivas dentro de la fase "actuar". Es un ciclo iterativo que permite obtener lecciones aprendidas de cada una de las fases y obtener la madurez de los procesos.
COBIT 4.1 y la norma ISO 27001 basan su estructura en el ciclo Deming, como observamos en la "fig. 2".

[1] SGSI. Sistema de Gestión de Seguridad de la Información.

[2] Tomado de Technology Risk Services - PricewaterhouseCoopers

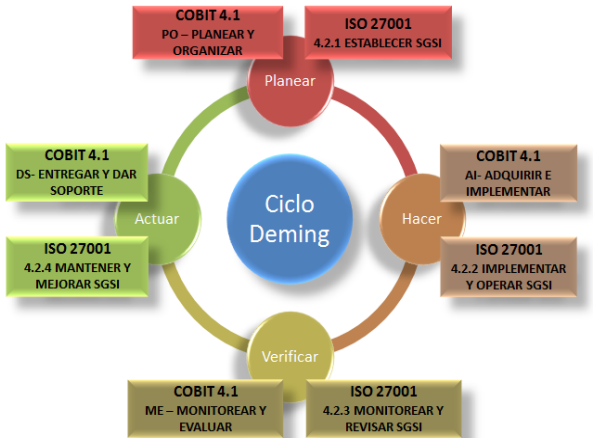

Fig.2. Ciclo PHVA en COBIT 4.1 y la ISO 27001

A. Planear

Es la primera fase del ciclo Deming. El dominio PO- Planear y Organizar de COBIT 4.1 establece diez (10) procesos que "identifican la manera en que TI puede contribuir de la mejor manera al logro de los objetivos del negocio. Además, la realización de la visión estratégica requiere ser planeada, comunicada y administrada desde diferentes perspectivas. Finalmente, se debe implementar una estructura y tecnológica apropiada." [2].

Observamos en la Tabla I, la relación que existe entre los procesos del dominio PO definidos por COBIT 4.1 y la ISO 27001. Tanto el marco de gobierno de T.I., como el estándar de seguridad de la información centran la etapa de planeación en la definición estratégica apoyada por las directrices del SGSI.

Establecer una metodología de gestión de riesgos desde la identificación de los activos de información hasta la aplicabilidad de controles que minimicen el riesgo inherente, son sus ejes comunes.

TABLA I
FASE DE PLANEACIÓN – COBIT 4.1 VS. ISO 27001

ETAPA PHVA	COBIT 4.1	ISO 27001
PLANEAR	PO1 – Definir un plan estratégico de T.I.	• Definir el alcance y los límites del SGSI en términos de las características del negocio. • Definir Política del SGSI.
	PO2 – Definir la Arquitectura de la Información	• Inventario de activos y propietarios de los mismos.
	PO3 – Determinar la Organización de T.I.	
	PO4 - Definir los Procesos, Organización y Relaciones de TI	• Definir el alcance y los límites del SGSI en términos de las características del negocio. • Definir roles y responsabilidades con el SGSI.
	PO5 - Administrar la Inversión en TI	
	PO6 - Comunicar las Aspiraciones y la Dirección de la Gerencia	• Declaración de Aplicabilidad
	PO7 - Administrar Recursos Humanos de TI	• Aplicar controles de roles y responsabilidades • Aplicar controles en la capacitación y entrenamiento del SGSI
	PO8 - Administrar la Calidad	• Aplicabilidad de controles para terceros
	PO9 - Evaluar y Administrar los Riesgos de TI	• Identificación de amenazas, vulnerabilidades, riesgos, impacto • Definir metodología de evaluación de Riesgos • Análisis y evaluación de riesgos • Evaluar alternativas para el Plan de tratamiento de riesgos • Aceptación de riesgos
	PO10 - Administrar Proyectos	

B. Hacer

Corresponde a las actividades de ejecución producto de la etapa de planeación.

La adquisición, mantenimiento, implementación y continuidad de las operaciones e infraestructura tecnológica (hardware, software, comunicaciones), son el objetivo de esta fase.

ISO 27001 define controles para alcanzar el cumplimiento de sus objetivos. La interacción de estos controles con los procesos de COBIT 4.1 y las métricas del marco de gobierno ayudan en la implementación del SGSI y minimizan las brechas de seguridad que pueden presentarse si se adoptan de forma independiente.

En la tabla II presentamos la relación analizada entre los procesos AI (Adquirir e Implementar) de COBIT 4.1 y los objetivos de control detallados en la ISO27001.

.

TABLA II
FASE DE EJECUCIÓN (HACER) – COBIT 4.1 VS. ISO 27001

ETAPA PHVA	COBIT 4.1	ISO 27001
HACER	AI1-Identificar soluciones automatizadas	Respaldo (Back-up) Protección contra software malicioso y código móvil Control de acceso Seguridad en los archivos del sistema
	AI2- Adquirir y mantener software aplicativo	Respaldo (Back-up) Protección contra software malicioso y código móvil Control de acceso Seguridad en los archivos del sistema
	AI3- Adquirir y mantener infraestructura tecnológica	Adquisición, desarrollo y mantenimiento de los Sistemas de Información Implementar programas de formación y sensibilización
	AI4- Facilitar la operación y el uso	Implementar procedimientos y controles para la gestión de incidentes de Seguridad. Gestionar la operación del SGSI. Continuidad del negocio
	AI5- Adquirir recursos de TI	Gestionar recursos.
	AI6- Administrar cambios	Gestión de las Comunicaciones y Operaciones
	AI7- Instalar y acreditar soluciones y cambios	Planeación y aceptación del sistema

C. Verificar

Corresponde al dominio ME- Monitorear y Evaluar dentro del marco de referencia de COBIT 4.1, que se encarga de evaluar, verificar la calidad y suficiencia de los requerimientos de control, integridad y confidencialidad, como se describe textualmente en su marco de referencia.

"Todos los procesos de TI deben evaluarse de forma regular en el tiempo en cuanto a su calidad y cumplimiento de los requerimientos de control. Este dominio abarca la administración del desempeño, el monitoreo del control interno, el cumplimiento regulatorio y la aplicación del gobierno."[2].

Esta fase nos muestra la importancia que existe en cualquier organización de supervisar, evaluar controles internos, desempeño y cumplimiento regulatorio de TI, por esta razón COBIT integra los controles de la norma ISO 27001 que se encuentran en el dominio Monitorear y Revisar del SGSI, dentro de los que se encuentran:

- Ejecutar procedimientos de monitoreo, revisión de controles y efectividad.
- Ejecutar procedimientos de monitoreo y revisión de controles que ayuden a detectar los eventos de seguridad mediante el uso de indicadores.
- Realizar revisiones regulares de la efectividad del SGSI y revisar los controles de seguridad.

COBIT integra estos controles y los utiliza como estrategia para evaluar las necesidades de las organizaciones y verificar si realmente los sistemas todavía encuentran los objetivos para los cuales fueron diseñados y cumple con las exigencias de TI.

En el siguiente cuadro comparativo se encuentra la fase de verificación del ciclo PHVA, donde se integra COBIT 4.1 y la norma ISO 27001.

TABLA III
FASE DE VERIFICACIÓN (VERIFICAR) – COBIT 4.1 VS. ISO 27001

ETAPA PHVA	COBIT 4.1	ISO 27001
VERIFICAR	ME1 Monitorear y Evaluar el Desempeño de TI	Ejecución de procedimientos de monitoreo, revisión de controles y efectividad.
	ME2 Monitorear y Evaluar el Control Interno	Ejecución de procedimientos de monitoreo y revisión de controles que ayudan a detectar los eventos de seguridad mediante el uso de indicadores.
	ME3 Garantizar el Cumplimiento Regulatorio	Realizar revisiones regulares de la efectividad del SGSI y revisar los controles de seguridad.
	ME4 Proporcionar Gobierno de TI	

Ambos enfoques coinciden en la necesidad de implementar controles que permitan a las organizaciones evaluar, verificar y garantizar que los procesos críticos del negocio estén alineados con la estrategia, objetivos y planes del negocio.

D. Actuar

La última fase que presenta el ciclo Deming se denomina Actuar y se define en el marco de referencia de COBIT 4.1 como DS- Entregar y Dar Soporte.

"Este dominio cubre la entrega en sí de los servicios requeridos, lo que incluye la prestación del servicio, la administración de la seguridad y de la continuidad, el soporte del servicio a los usuarios, la administración de los datos y de las instalaciones operativas."[2].

Mantener y mejorar el SGSI es definido en la norma ISO 27001 como la fase de Actuar, en esta se enfocan aspectos de la tecnología de información que cubre áreas como administración de configuraciones, problemas, ejecución de acciones correctivas y preventivas, protección de software, educación etc., que son ejecutados dentro del sistema de TI y el resultado de estos controles, apoyan procesos que permiten la ejecución eficaz y eficiente de estos sistemas.
Estos procesos de apoyo y control incluyen seguridad y educación.

"La norma ISO 27001 adopta acciones correctivas y preventivas basadas en auditorías y revisiones internas ó en otra información relevante a fin de alcanzar la mejora continua del SGSI."[5].

De esta forma COBIT integra los controles presentados en la norma ISO 27001 como la administración de problemas, documentación de procedimientos, e integración del servicio de Mesa de servicio e implementación de mejoras sobre el SGSI que aseguran y ayudan a lograr los objetivos señalados.

En el siguiente cuadro comparativo se encuentra la fase Actuar del ciclo PHVA, donde se integra COBIT 4.1 y la norma ISO 27001.

TABLA IV
FASE DE EJECUCIÓN (ACTUAR) – COBIT 4.1 VS. ISO 27001

ETAPA PHVA	COBIT 4.1	ISO 27001
ACTUAR	DS13 Administrar las operaciones	Documentar y mantener los procedimientos de operación. Implementar planes para mantener o restaurar la operación. Implementar las mejoras identificadas en el SGSI y asegurar que logren sus objetivos señalados.

ETAPA PHVA	COBIT 4.1	ISO 27001
ACTUAR	DS1 Definir y administrar los niveles de servicio	Definiciones de servicios y niveles de entrega incluidos en los contratos establecidos
	DS2 Administrar los servicios de terceros	Asegurar que los terceros implementen, operen y mantengan los controles de seguridad. Definiciones de servicio y niveles de entrega incluidos en el contrato establecidos.
	DS3 Administrar el desempeño y la capacidad	Implementación de las mejoras identificadas en el SGSI y asegurar que logren sus objetivos señalados. Monitoreo y realización de proyecciones del uso de los recursos para asegurar el desempeño del sistema requerido.
	DS4 Garantizar la continuidad del servicio	Desarrollo y mantenimiento de un proceso gerencial para la continuidad del negocio, para tratar requerimientos de seguridad de la información.
	DS6 Identificar y asignar costos	
	DS7 Educar y entrenar a los usuarios.	Asegurar que todos los empleados, contratistas reciban y tengan una apropiada capacitación.

ETAPA PHVA	COBIT 4.1	ISO 27001
ACTUAR	DS8 Administrar la mesa de servicio y los incidentes	Ejecución de acciones correctivas y preventivas en la solución de incidentes. Reportar y escalar fallas presentadas en los servicios de TI. Cuantificar y monitorear los tipos, volúmenes y costos de los incidentes en la seguridad de la información.
	DS9 Administrar la configuración	Proteger la integridad del software y la información, para asegurar los procesos de configuración. Implementar las mejoras identificadas en el SGSI y asegurar que logren sus objetivos señalados.
	DS10 Administrar los problemas	Tomar las acciones correctivas y preventivas de manera apropiada para el impacto de los problema.
	DS11 Administrar los datos	Identificar los riesgos que se puede presentar sobre la información de la organización, utilizando controles de acceso apropiados. Implementar las mejoras identificadas en el SGSI y asegurar que logren sus objetivos señalados.
	DS12 Administrar el ambiente físico	Utilización de perímetros de seguridad y puertas de ingreso para proteger las áreas que contienen información . Proteger áreas comunes. Diseñar y aplicar seguridad física, control de acceso.

Integrando COBIT 4.1 con el Standard ISO 27001, se obtiene un gobierno de Seguridad de la Información, que permite implementar buenas

prácticas para la gestión de riesgos de seguridad de la información.

Este marco alinea los objetivos de seguridad informática con los objetivos del negocio, optimizando recursos y mejorando los procesos.

Contribuye en la madurez de los procesos de seguridad de la información durante su planeación, ejecución, monitoreo y mejora a través de controles medibles sobre el SGSI.

Como valor agregado, certifica ante los terceros que los proceso son confiables, controlados y con un enfoque de gestión de riesgos de SI.

Contribuye a las organizaciones en la reducción de costos por operación y garantiza la continuidad de los procesos críticos.

Son un excelente complemento para garantizar el CID[3] de la información.

IV. CONCLUSIONES

La integración del marco de referencia COBIT y la norma ISO27001 establecen mecanismos y controles que ayudan a mitigar riesgos y contribuyen con la visión del negocio y el liderazgo de estructuras organizacionales que establecen procesos para proteger la información y lograr una dirección estratégica.

COBIT como valor agregado, certifica ante los terceros que los proceso son confiables, controlados y con un enfoque de gestión de riesgos de SI.

Contribuye a las organizaciones en la reducción de costos por operación y garantiza la continuidad de los procesos críticos.

Son un excelente complemento para garantizar el CID[4] de la información.

[3] CID – Confiabilidad, Integridad, Disponibilidad

Al utilizar COBIT como estándar de gobernabilidad se incluyen los objetivos de control presentes en los dominios dentro de los niveles del marco conceptual propuesto.

REFERENCIAS

[1] Díaz, Evans Javier, "Modelo de Seguridad de la Información – Gobierno de Seguridad," in ACIS XI Jornada de Seguridad Informática, Junio 2011.

[2] IT Governance Institute, "Alineando Cobit 4.1 Itil V3 e ISO/IEC 27002 en beneficio del negocio," pp. 11–30.

[3] ISACA, "Guidance for Boards of Directors and Executive Management", www.isaca.org/Pages/default.aspx.

[4] ISO, "Estándar Internacional ISO/IEC 27001," ed. Primer, pp. 23-37.

[5] Turnbull, Shann, "Corporate Governance: Theories, Challenges and Paradigms", 2nd ed. vol. 1, 2000, pp. 11–43.

[6] Pallas, Gustavo, "Metodología de Implantación de un SGSI en un grupo empresarial jerárquico," Montevideo, diciembre 2009.

[7] Acevedo, Hector, "Integrando Cobit, ITIL e ISO 27000 - SCITUM".

[8] Varun, Arora, "Comparing different information security standards: COBIT v s. ISO 2700", http://ieeexplore.ieee.org.

Autores

YENNY PATRICIA PAEZ AREVALO, Ingeniera de Sistemas e Informática de la Universidad Libre de Colombia, especialización en Seguridad Informática (en proceso), certificada en ITIL Foundation Server, dos años de experiencia en Auditoria Informática y cuatro años de experiencia en acciones de gobernabilidad de T.I., conocimiento en normatividad vigente para entidades vigiladas por la Superintendencia Financiera de Colombia, gestión de procesos de tecnología basadas en

estándares y mejores prácticas como COBIT, ITIL, COSO e ISO 27001.

LEIDY JOHANNA ESTRADA RODRIGUEZ,
Ingeniera de Telecomunicaciones de la Universidad Piloto de Colombia, Especialización en Seguridad Informática (en proceso), experiencia como Líder de proyectos de tecnología informática y comunicaciones TIC y sólidos conocimientos en administración e implementación de soluciones de backup, recuperación de información, Storage y redes de almacenamiento (SAN), diseño, implementación y administración de plataformas de backup de diferentes fabricantes EMC Networker, Dataprotector, Tivoli TSM. Certificación ITIL V3.