ISSN: 1692-7257 - Volumen 2 – Número 32 - 2018

Revista Colombiana de Tecnologías de Avanzada

Recibido: 30 de abril de 2018
Aceptado:1 julio e 2018

INTEGRACIÓN DE SEGURIDAD Y GESTIÓN DE SERVICIOS EN EL GOBIERNO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

INTEGRATION OF SECURITY AND MANAGEMENT OF SERVICES IN THE GOVERNMENT OF INFORMATION TECHNOLOGIES

***Msc (c), Esp. Deisy Esthér Castro Márquez, *PhD. Torcoroma Velásquez Pérez, **Phd. Hugo F. Castro Silva**

[*] **Universidad Francisco de Paula Santander Ocaña,** Facultad de Ingeniería, Programa de Maestría en Gobierno de Tecnología de Información, Grupo de Investigación GITYD. Vía Acolsure Sede el Algodonal, Ocaña, Norte de Santander, Colombia.
Teléfono, (57) (7)5690088
E-mail: {dcastrom,tvelasquezp}@ufpso.edu.co.
****Univesidad Pedagógica y Tecnológica de Colombia**, Calle 4 A Sur No. 15-134, Sogamoso, Boyacá, Colombia.
E-mail: {hugofernado.castro}@uptc.edu.co

Resumen: Este artículo presenta la integración de diversas disciplinas en la aplicación de las tecnologías de la información a nivel organizacional a partir de la adopción de buenas prácticas, estándares, marcos de referencias y normativas de seguridad de la información, gestión de servicios y gobierno de TI.

Palabras clave: Gobierno de TI, estándares, marco de referencia, seguridad de la información, gestión de servicios de TI.

Abstract: This article presents the integration of various disciplines in the application of information technologies at the organizational level from the adoption of good practices, standards, reference frameworks and regulations on information security, management of services and IT governance.

Keywords: IT governance, standards, reference framework, information security, IT service management.

1. INTRODUCCIÓN

Actualmente las empresas tienen la necesidad de aplicar estándares o buenas prácticas como herramientas para dirigir, controlar y supervisar las actividades relacionadas con la seguridad, gestión y gobierno de TI, estableciendo maneras de integrarlas con el fin de optimizar recursos o cumplir requerimientos normativos. Para este artículo se ha querido recopilar material relevante de las mejores prácticas para el Gobierno de TI utilizando marcos de referencia como COBIT, ITIL, ISO 38500 y ISO 27001. Y a partir de lo anterior, a través de un enfoque heurístico descubrir estudios realizados y el estado actual de la integración de estas buenas prácticas como fundamento al desarrollo y optimización de los procesos de la organización desde un enfoque

estratégico en la implementación de las tecnologías, gestión y seguridad de la información. De acuerdo a lo anterior, a continuación, se muestra el estado del arte que, en este contexto de integralidad de buenas prácticas de seguridad, gestión de servicios en el gobierno de las tecnologías en las organizaciones.

2. ESTADO DEL ARTE

2.1 Estándares, Marcos de Referencia y Normatividad

2.1.1 Evolución de Estándares, Marcos de Referencia y Normatividad

En el contexto fijado en este estudio sobre la seguridad, gestión de servicios y gobierno de TI, se identificó que existe una gran variedad de Estándares, Marcos de Referencias y Normatividad, que a lo largo de su existencia han venido evolucionando y mejorando al nivel de las tecnologías que en su momento han estado vigentes en el mercado, y han servido como guía o base para el desarrollo de las organizaciones.

Organizaciones como ISACA y la Organización de Estándares Internacionales (ISO) han trabajado en desarrollo de estándares y buenas prácticas que conlleven a la organización a un enfoque de gobierno de TI. ISACA ha desarrollado desde 1996 la primera edición de COBIT referente a buenas prácticas de auditoría de TI, en 1998 en su segunda edición se refiere a auditoría y control, la tercera edición en el año 2000 referente a la administración de TI, la cuarta edición en el 2005 referente a gobierno de TI y la quinta edición en el 2012 es reconocida a nivel de gobierno corporativo de TI. Así, inicialmente nació como un marco de referencia a partir de lineamientos para la auditoría, controles, administración, gobierno de TI y que a través de su evolución ha llegado a posicionarse a nivel corporativo en términos de una buena práctica para establecer un concepto de gobierno de corporativo de TI para la organización. Así mismo, la Organización de Estándares Internacionales (ISO), en este mismo contexto ha definido el estándar ISO:38500 de 2008 relacionada con el Gobierno de TI para las organizaciones.

En términos de seguridad de la información la Organización de Estándares Internacionales (ISO), como la entidad más reconocida a nivel mundial en el manejo de buenas prácticas internacionales sobre esta temática, ha trabajado en este campo desde décadas atrás. A partir de 1995 el estándar BS 7799-1, el cual habla de administración de la seguridad de la información. Así mismo, en 1998 nace la BS 7799-2 referente a requisitos para implementar un sistema de gestión de seguridad de la información. Dichas normas evolucionan a partir del año 2005, en el cual la BS 7799-2 pasa a ser norma certificable siendo reemplazada por la ISO 27001:2005. De igual manera, ocurrió con la BS 7799-2 el cual es reemplazada por la ISO 27002:2007 haciendo referencia como una guía de buenas prácticas de seguridad de la información.

La gestión de servicios de TI, ha sido reconocida especialmente, por los trabajos realizados a partir de buenas prácticas como ITIL desarrollada por la Central Computing and Telecommunications Agency (CCTA). A finales de los años 80 desarrollan la primera edición de ITILv1 en 1988 como una buena práctica, evolucionando hasta la tercera edición ITILv3 conforme a las tecnologías del momento. Así mismo, la Organización de Estándares Internacionales (ISO), ha desarrollado la norma ISO 20000 a partir del año 2011, como un estándar certificable en la gestión de servicios de TI para las organizaciones.

2.1.2 Marco Teórico de Estándares, Marcos de Referencia y Normatividad

COBIT es un marco de referencia globalmente aceptado para el gobierno de TI basado en estándares de la industria y las mejores prácticas. Una vez implementado, los ejecutivos pueden asegurarse que se ajusta de manera eficaz con los objetivos del negocio y dirigir mejor el uso de TI para obtener ventajas comerciales.

ITIL es un marco de trabajo de las mejores prácticas destinadas a facilitar la entrega de servicios de tecnologías de la información (TI). ITIL resume un extenso conjunto de procedimientos de gestión ideados para ayudar a las organizaciones a lograr calidad y eficiencia en las operaciones de TI.

ISO/IEC 27001 (2005) define la seguridad de la información como la preservación de la confidencialidad, integridad y disponibilidad de la Información. ISO/IEC 38500 (2008) hace referencia al gobierno corporativo de tecnologías de la información. ISO/IEC 20000 (2011) define un estándar para la gestión de servicios de TI.

2.2 Integración de Estándares

Se han encontrado a nivel mundial países o empresas donde se ha trabajado en la alineación de estándares relacionados con Cobit, Itil e ISO 27000. El Governance Institute (2008) propone una alineación de estándares de COBIT 4.1, ITIL V3 e ISO/IEC 27002 en beneficio del negocio como un marco de referencia para apoyar a la empresa. En Malasia, en Centro de Ingeniería de Software Avanzado (CASE), de la Universidad Tecnológica de Malasia (2008) realiza una Combinación de ITIL, COBIT e ISO / IEC 27002 con el fin de diseñar un Marco Integral de TI en Organizaciones. Igualmente, Mesquida et al (2014) hace referencia a la Integración de Estándares de Gestión de TI mediante MIN-ITs (Marco Integrado de Estándares de Gestión de TI), el cual facilita la implantación integrada de diferentes estándares ISO de gestión de TI (ISO/IEC 15504, ISO 9001, ISO/IEC 20000, ISO/IEC 27000 e Itil), para las empresas de desarrollo. De igual manera, en la Tesis Doctoral de Antoni Lluís Mesquida Calafat (2012), se habla de Un Modelo para Facilitar la Integración de Estándares de Gestión de TI en Entornos Maduros. A nivel nacional, la Universidad ICESI de Cali, en proyecto de grado de Maestría, Herrera César Alonso y Jaramillo Edward (2012), desarrollan un modelo de integración de algunos marcos de referencia para el gobierno de TI, en el cual incluyen buenas prácticas de COBIT y la norma internacional ISO 38500.

En estudio desarrollado a nivel regional (Rojas & Sánchez, 2012) diseñaron una base de conocimiento para el servicio de soporte de servicios de tecnologías de información y la arquitectura de software de apoyo a los servicios de soporte. El trabajo (Bonfante & Castillo, 2014) presenta la justificación de la integración de tres (3) tecnologías: Sistema Multi-Agente, Ontologías, y Procesos de Negocios para el soporte de la Estrategia "Gobierno en Línea" de Colombia.

Dentro del proyecto MuNet de la OEA con el apoyo de los gobiernos de Colombia, Panamá y Uruguay. (Cardona et al, 2014) desarrollaron un patrón de uso de las TIC por parte de los líderes municipales presentando un marco teórico de los conceptos sociedad del conocimiento, Gobierno corporativo, TIC, modelos de aceptación tecnológica y la norma ISO/IEC 38500. En otro trabajo (Tangarife et al, 2014) con la gestión de interventoría para el seguimiento a los contratos de software en el marco de las buenas prácticas de la guía PMBOK®, norma ISO 21500® y el gobierno IT COBIT®, tomando como referencia la Gestión del Alcance, y validando con un estudio comparativo de los proyectos de software de la organización.
La normalización o estandarización de los procesos y del trabajo conllevan a la especialización y al logro de los objetivos trazados en la empresa, considerando a Mintzberg (1988) en su libro estructuración de las organizaciones.

El mercado mundial hoy en día demanda una estandarización en los procesos de las organizaciones en beneficio de ser más competitivos y sostenibles en el campo empresarial, especialmente, en el uso de las tecnologías que se han convertido en apoyo fundamental para la optimización de los mismos, y como efecto de la globalización que se está presentando. Así, lo establecen estudios realizados por Yáñez & Yáñez, 2012 sobre Auditorías, Mejora Continua y Normas ISO: factores clave para la evolución de las organizaciones, el cual manifiestan las exigencias de calidad de los productos y servicios en el mercado local y global.

En Colombia con base a lo manifestado, el gobierno ha visto la necesidad de adaptar las empresas a las nuevas perspectivas empresariales con el fin de prevalecer en la globalización que hoy en día se vive con el uso adecuado de las tecnologías, manteniéndolas seguras y utilizándolas en un contexto organizativo que conlleve la utilización de las mismas en razón de prestar servicios que satisfagan a sus clientes en el mercado nacional e internacional. Estudios realizados como el "marco de referencia para auditorías integrales de sistemas en las mipymes colombianas" de Roberto Díaz Alonso (2012), indican la importancia que tiene la auditoría en la evaluación de normas y estándares que se aplican en Colombia. Así mismo, se viene adoptando buenas prácticas asociadas a la implementación de estándares mínimos de gestión y seguridad tecnológica y de la información. Sin embargo, empresas colombianas sometidas a la regulación tienden a implementar tecnologías y buenas prácticas relacionadas con el control de las mismas, sin tener la conciencia en ocasiones que deben estar sujetas a un entorno estratégico en la organización que vaya relacionado al cumplimiento de sus metas establecidas, razón por la cual, muchas veces dicha aplicación representa a la organización grandes inversiones económicas, tiempo y demás recursos que solo terminan en una inversión deficiente conllevando a la organización a una aplicación "Divergente" o "Independiente"

de estándares por el afán de cumplir solo requisitos legales.

3. PROBLEMÁTICA

La integración de estándares y marcos de referencias de seguridad, calidad y Gestión de Servicios y Gobierno de TI son conceptos que se han venido tratando en el sector empresarial como alternativas para el mejoramiento de sus procesos. Sin embargo, se ha hace necesario normalizar su significado en razón de mantener una aplicación homogénea a nivel conceptual que permita a la organización un entendimiento común en el mercado. Existen diversas definiciones sobre los términos mencionados, la Norma ICONTEC ISO/IEC 27001 (2005) define la Seguridad de la Información como la preservación de la confidencialidad, integridad y disponibilidad de la Información. Así mismo, la Guía Práctica ISO 20000 (2005) define gestión de servicios como el conjunto de capacidades y procesos para dirigir y controlar las actividades del proveedor de servicios, y los recursos para el diseño, transición, provisión y mejora de los servicios para cumplir con los requisitos de los contratos. Igualmente, COBIT 5 (2013) define el gobierno de TI como un enfoque de gobierno que garantiza que las tecnologías de información y las relacionadas soportan y habilitan la estrategia de la empresa y la consecución de las metas corporativas. También incluye el gobierno funcional de TI, por ejemplo, garantizando que las capacidades de TI son provistas de forma eficiente y efectiva.

Considerando este estudio del estado del arte, es beneficioso para la empresa colombiana la implementación de buenas prácticas de seguridad de la información, gestión de servicios y gobierno de TI de manera "Divergente" o "Independiente" en el cual se enfocan primordialmente al cumplimiento de la normatividad interna o externa del país sin darle la relevancia necesaria a nivel de gobierno corporativo de las mismas como parte de ser organizaciones sostenibles, competitivas y adaptable a las necesidades de la globalización?

En Colombia la empresa tiende a aplicar en sus operaciones el uso de las tecnologías como parte de la optimización en el desarrollo del manejo de la información en sus procesos y de la competitividad que necesitan tener frente al mercado empresarial. En razón de la problemática que actualmente enfrenta la empresa colombiana frente a la aplicación "Divergente" o "Independiente" de buenas prácticas sobre el manejo de la seguridad y gestión de servicios de las tecnologías, enraizadas al afán del cumplimiento de normativas internas y externas a nivel del mercado, se propone el diseño de un MODELO INTEGRAL DE SEGURIDAD Y GESTIÓN DE SERVICIOS EN EL GOBIERNO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN que apoye no solo a la organización al cumplimiento de sus requisitos legales, sino a optimizar la efectividad en la aplicación de estándares vigentes, optimizando recursos y manteniendo una integralidad en su operación, como parte fundamental al logro de su misión y visión empresarial, haciéndola sólida y sostenible en su actuar.

En Colombia se han realizado estudios a través de auditorías a diferentes sectores empresariales como el financiero, aseguradores, crediticios, educativos, entre otras, que adaptan estándares o buenas prácticas de gestión de servicios, seguridad y gestión de tecnologías de la información, en razón de cumplir un requisito legal. De igual manera, lo manifiestan estudios realizados a través de "auditorias integrales de sistemas en las mipymes colombianas". (Díaz, 2012)

Respecto a Modelos de Integración de Seguridad y Gestión de Servicios en el Gobierno de Tecnologías de la Información, no se evidenció en Colombia modelos referentes que cumplan con la normatividad actual vigente. A nivel internacional, se han identificado algunos esquemas como la "Alineación de Cobit 4.1, Itil V3 e ISO 27002 del año 2005. (Governance Institute, 2008)

Considerando la problemática actual de la empresa Colombiana en la aplicación de estándares y buenas prácticas de TI con el fin de establecer una convergencia entre las mismas, se propone el diseño del Modelo Integral de Seguridad y Gestión de Servicios en el Gobierno de las Tecnologías de la Información, que contribuya a nivel tecnológico al desarrollo organizacional al ser un esquema que aportará a la empresa la aplicación integrada de buenas prácticas soportadas en las normas ISO 27001 (2013), ISO38500 (2015) y COBIT 5 (2013), como alternativa de mejora y parte fundamental para cumplir sus metas y objetivos que le permitan ser sostenible y competitiva en el ambiente empresarial.

4. CONCLUSIONES

El estado actual frente a lo realizado hasta el momento sobre la integración de estándares de seguridad, gestión de servicios y gobierno de TI, se enfoca en una alineación de controles o lineamientos en común de los mismos, para cumplir comúnmente un requerimiento normativo, muchas veces independiente o divergente de las necesidades propias de la compañía en términos de su misión y visión empresarial.

Las organizaciones necesitan un modelo integral que permita adoptar a nivel estratégico y corporativo todo estándar o buena práctica adaptable a su negocio, el cual contribuya al cumplimiento de sus metas y objetivos empresariales.

La integración de estándares y buenas prácticas de seguridad, gestión de servicios y gobierno de TI contribuyen al mejoramiento continuo de las organizaciones en un contexto propiamente corporativo.

REFERENCIAS

Bofante, M.,Castillo A., (2014) " Integración de sistema multi-agente, ontologías y procesos de negocios como marco tecnológico de la estrategia gobierno en línea". Revista Colombiana de Tecnología de Avanzada ISSN 1692-7257 Volumen 1 Nro 23

Cardona, D., Rivera, M., López, L.,(2014)" Marco teórico para identificar el patrón de uso de las tic por parte de líderes municipales". Revista Colombiana de Tecnología de Avanzada ISSN 1692-7257 Volumen 2 Nr 24.

Díaz, A., Roberto. Marco de referencia para auditorías integrales de sistemas en las mipymes colombianas. Colombia, 2012.

Herrera, César y Jaramillo Edward. (2012). Modelo de integración de algunos marcos de referencia para el gobierno de TI y los procesos de gestión de la empresa del Marco eTOM (Mapa de Operaciones Telecom mejorado). Cali.

Instituto Colombiano de Normas Técnicas y Certificación, 2005. Tecnología de la Información. Sistema de Gestión de Seguridad de la Información (SGSI). Bogotá D.C., ICONTEC, NTC ISO/IEC 27001.

Instituto Colombiano de Normas Técnicas y Certificación. 2008. ISO/IEC 38500. Bogotá D.C

Instituto Colombiano de Normas Técnicas y Certificación. 2011. ISO/IEC 20000. Bogotá D.C

Álvaréz, Ana. (2016). Guía Práctica de ISO/IEC 20000-1. AENOR. España.

ISACA. (2013). COBIT 5 Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa. Estados Unidos.

GOVERNANCE INSTITUTE. (2008). Alineando Cobit 4.1, Itil V3 e ISO 27002 en Beneficio del Negocio. Estados Unidos.

Shamsul Sahibudin, Mohammad Sharifi and Masarat Ayat. (2008). Combining ITIL, COBIT and ISO/IEC 27002 in Order to Design a Comprehensive IT Framework in Organizations. University Teknologi Malaysia.

Zhitao Huang, Pavol Zavarsky, Ron Ruhl. (2014). An Efficient Framework for IT Controls of Bill 198 (Canada Sarbanes-Oxley) Compliance by Aligning COBIT 4.1, ITIL v3 and ISO/IEC 27002. Concordia University College of Alberta.

Mesquida, A., Mas, A., San Felui, T., & Arcilla, M. (2014). Integración de Estándares de Gestión de TI mediante MIN-ITs . Revista Iberica de Sistemas y Tegnologías de la Información , 31-45.

Mesquida, Antoni. (2012). Un Modelo para Facilitar la Integración de Estándares de Gestión de TI en Entornos Maduros. Tésis Doctoral.

Mintzberg, H. (1988). La estructuración de las organizaciones. Grupo Planeta (GBS).

SUPERINTENDENCIA FINANCIERA DE COLOMBIA. Circular 042 de 2012 y Circular 029 de 2014. Disponible en: https://www.superfinanciera.gov.co

Antoni Lluís Mesquida Calafat. Tesis Doctoral Un Modelo para Facilitar la Integración de Estándares de Gestión de TI en Entornos Maduros. Palma, 2012.

ISMS. Registro de Empresas Certificadas ISO 27001. Disponible en: https://www.ismsforum.es/iso27001.

DÍAZ ROBERTO. Marco de referencia para auditorías integrales de sistemas en las mipymes colombianas. Colombia, 2012.

HERRERA CÉSAR Y JARAMILLO EDWARD. Proyecto de Grado Modelo de integración de algunos marcos de referencia para el gobierno de TI y los procesos de gestión de la empresa del Marco eTOM (Mapa de Operaciones Telecom mejorado). Santiago de Cali, 2012.

ITIL Foundation. ITIL V4. Disponible en: https://www.itil.org.uk/

Rojas, M., Sánchez, M. (2012) "Arquitectura de software para el servicio de soporte de tecnología de información basada en servicios web". Revista Colombiana de Tecnología de Avanzada ISSN 1692-7257 Volumen 2 Nro 20.

Tangarife, L., Sánchez, M., Rojas, M. (2014) "Modelo de interventoría de tecnologías de información en el área de conocimiento de la gestión del alcance de pmbok® y alineado con iso 21500 y cobit®". Revista Colombiana de Tecnología de Avanzada ISSN 1692-7257 Volumen 1 Nr 23.

Yánez, J., & Yánez, R. (2012). Auditorías, Mejora Continua y Normas ISO: factores clave para la evolución de las organizaciones. Actualidad y Nuevas Tendencias, 83-92.