REVISTA COLOMBIANA DE COMPUTACIÓN
Volumen 18, número 1
Págs. 70 - 81

Normas ISO y marcos de referencia para gobernanza de las TIC. Revisión general

ISO standards and reference framework for ICT governance. General revision

Hugo Vecino P.
Universidad Nacional de Educación a Distancia-UNED
E-mail: : hvecino2@alumno.uned.es

Fecha de recibido: 23/02/2017 y Fecha de aprobación: 05/04/2017

Resumen

Actualmente existen diferentes normas, modelos y marcos de referencia en el tema de la gobernanza de las TIC, de manera general puede decirse que estos pretenden mostrar un camino a las empresas para que puedan alinear la misión corporativa con el uso adecuado, eficiente y eficaz de la tecnología, claramente en busca de conceptos como calidad, seguridad, disminución del riesgo, continuidad del servicio entre otros. En este artículo se hace una revisión de las principales normas internacionalmente reconocidas y asociadas al tema de la gobernanza de las TIC, con la intención de aproximar al lector interesado en este tópico, especialmente directores de TI o *Chief information officer* (CIO). También está dirigido a investigadores en el área, para que tengan una visión general de la normatividad vigente ya que estas buenas prácticas han sido validadas en su mayoría por más de 150 países.

Palabras Clave:

Gobernanza de las TIC
Normas ISO
ITIL
COBIT
CMMI

Abstract

Currently there are different norms, models and frames of reference in the topic of ICT Governance, in general, it can be said that these are intended to show a way for companies to align corporate mission with appropriate, efficient and effective use Of technology, clearly looking for concepts such as quality, safety, risk reduction, service continuity among others; This article reviews the main internationally recognized norms associated with the topic of ICT Governance, with the intention of bringing the reader interested in this topic, especially IT directors or CIO, To be directed to researchers in the area, so that they have an overview of the current regulations since these good practices have been validated in most of them by more than 150 countries.

Keywords:
ICT Governance
Standars ISO
ITIL
COBIT
CMMI

1. Introducción

El gobierno de las TIC o estrictamente gobernanza de las TIC, no debe confundirse con el concepto de eGovernment, que ha sido una iniciativa de los mandatorios locales y regionales para prestar los servicios de carácter gubernamental o asociados al gobierno (Ej, Alcaldías, Gobernaciones o Presidencia) y su idea ha sido la de integrar las TIC para transformar la prestación de servicios de carácter gubernamental [1], y aunque no son conceptos excluyentes sí son diferentes. El lector debe entender que existen varias definiciones de gobernanza de las TIC, por ejemplo, mientras que en el mundo de los negocios se ha centrado en la gestión del rendimiento y la creación de valor, en el mundo académico se ha centrado en especificar los derechos de decisión y un marco de responsabilidad para fomentar el comportamiento deseable en el uso de las TIC [2]. Sin embargo, y esto es importante, la eficacia del gobierno de TI de una empresa o unidad de negocio puede ser evaluada mediante la evaluación de lo bien que le permite a la TI cumplir con cuatro objetivos: la rentabilidad, la utilización de activos, el crecimiento del negocio y la flexibilidad empresarial [3]. Actualmente también existen diferentes marcos de referencia que pueden ser guías útiles para la implementación de la gobernanza de la información y la tecnología (TI) y que se describen a continuación. En este punto es importante hacer la diferencia entre gobierno y gestión. El gobierno se refiere efectivamente a la capacidad de una organización para alinear el uso de las TIC con su estrategia; mas formalmente se puede decir que “consiste en el liderazgo de las estructuras y procesos organizativos que aseguran que las TI de la organización sostienen y extienden la estrategia y los objetivos de la organización”[4], por otro lado la gestión se refiere a la gerencia o administración de todos los sistemas informáticos, incluidos hardware y software y las buenas prácticas que hay asociadas a estas, formalmente se puede decir que “Gestionar las Tecnologías de la Información (TI) consiste en tomar decisiones operativas dentro del gobierno de las TI. La gestión de la TI se refiere a los aspectos operativos para el suministro de productos y servicios de TI en la forma más eficaz” [5].

En la primera parte del artículo se muestran las normas y estándares asociados a la gobernanza de las TIC, en donde se hace una descripción en profundidad de las normas ISO/IEC. En la segunda parte se hace referencia a los “*frames*” o marcos de referencia más conocidos en el ámbito empresarial asociados al mismo tema, por último se hace un análisis de la situación actual y finalmente se presentan las conclusiones.

Para este artículo la metodología de recuperación de la información ha sido exploratoria, es decir que la búsqueda de los documentos consultados ha obedecido en primera instancia a la experiencia del autor y en segunda instancia a la consulta de textos especializados como artículos indexados en bases de datos especializadas como IEEEXplore, Science Direct, entre otros, también libros y portales de internet especializados en el tema.

2. Normas ISO/IEC

En este apartado se resumirán las principales normas y estándares internacionales asociados a la gobernanza de las TIC, validadas por la *International Standar Organization-ISO* y la *International Electrotechnical Commission (IEC);* la idea es mostrar al lector interesado una visión general de las herramientas desarrolladas para este fin.

2.1 ISO 38500

La norma ISO/IEC 38500:2008 se publicó en junio de 2008 con base en la norma australiana AS8015:2005. Es la primera de una serie de normas sobre gobierno de TIC. Su objetivo es proporcionar un marco de principios para que la dirección de las organizaciones lo utilice al evaluar, dirigir y monitorizar el uso de las tecnologías de la información y comunicaciones (TIC) [6]. Dentro de los beneficios de un buen gobierno de TIC estaría la conformidad de la organización con: Los estándares de seguridad, legislación de privacidad, legislación sobre el *Spam*, legislación sobre prácticas comerciales, derechos de propiedad intelectual incluyendo acuerdos de licencia de software, regulación medioambiental, normativa de seguridad y salud laboral, legislación sobre accesibilidad y estándares de responsabilidad social. También busca un buen rendimiento de las TIC mediante una apropiada implementación y operación de los activos de TIC, clarificación de las responsabilidades y rendición de cuentas en lograr los objetivos de la organización, continuidad y sostenibilidad del negocio, alineamiento de las TIC con las necesidades del negocio, asignación eficiente de los recursos, innovación en servicios, mercados y negocios, buenas prácticas en las relaciones con los interesados (*stakeholders*), reducción de costos y materialización efectiva de los beneficios esperados de cada inversión en TIC [6].

La norma incluye 19 definiciones de términos, seis principios del buen gobierno corporativo y tres tareas principales, para cada uno de los principios y proporciona una breve guía u orientación sobre cómo evaluar, dirigir y monitorizar la función de TIC.

2.2 ISO/IEC 27000

ISO/IEC 27000 es un conjunto de estándares desarrollados -o en fase de desarrollo- por ISO *(International Organization for Standardization)* e IEC *(International Electrotechnical Commission),* que proporciona un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización pública o privada, grande o pequeña. El estándar ISO 27001:2013 es una norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan; para los Sistemas Gestión de la Seguridad de la Información (SGSI) permite a las organizaciones la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos.

La aplicación de ISO-27001 significa una diferenciación respecto al resto, que mejora la competitividad y la imagen de una organización. La gestión de la seguridad de la información se complementa con las buenas prácticas o controles establecidos en la norma ISO 27002 [7]. ISO/IEC 27.002, publicada desde el 1° de Julio de 2007, es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios [8]. ISO/IEC 27.003 Describe el proceso de implementación del sistema, prestando soporte en los siguientes puntos: aprobación de dirección y autorización para la realización del proyecto, definición del alcance, límites y fronteras, la evaluación de los riesgos y el plan del tratamiento de los mismos, el diseño del SGSI y la planificación del proyecto de implementación [9]. ISO/IEC 27.004 da ejemplos documentados en sus anexos de cómo crear métricas para controles y cómo medir resultados para controles específicos de ISO 27001: 2005. Es una guía para el desarrollo y utilización de métricas y técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles o grupos de controles implementados según ISO/IEC 27001 [10]. ISO/IEC 27005. No

certificable. Proporciona directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001:2005 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos [11]. ISO/IEC 27006 En esta norma se hacen explícitos los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información, ayuda a interpretar los criterios de acreditación de ISO/IEC 17021 cuando se aplican a entidades de certificación de ISO 27001, pero no es una norma de acreditación por sí misma [12]. ISO/IEC TR 27008 Publicada el 15 de Octubre de 2011. No certificable. Es una guía de auditoría de los controles seleccionados en el marco de implantación de un SGSI.

2.3 ISO/IEC 20000

La Norma ISO/IEC 20000-1:2011 promueve la adopción de un enfoque de procesos integrados para una provisión eficaz de servicios gestionados de TI, que satisfaga los requisitos del negocio y de los clientes a través de la mejora continua mediante el modelo PDCA *(Plan Do Check Act).* Con la implantación de la Norma UNE-ISO/IEC 20000-1 se logra que los servicios TI estén orientados al negocio, es decir, el objetivo básico y fundamental del área de explotación/ producción es dar un servicio con la máxima calidad, bien a la propia organización o bien a sus clientes externos. El Código de Buenas Prácticas es la segunda parte de la Norma ISO/IEC 20000-2:2007 y representa el conjunto de mejores prácticas adoptadas y aceptadas por la industria en esta materia. Beneficios para su empresa: alinear los servicios de TI a las necesidades de negocio, proporcionar una adecuada gestión de la calidad del servicio de TI ofrecido, maximizar la calidad y eficiencia del servicio de TI, reducir los riesgos asociados a los servicios de TI, reducir costes y generar negocio, aumentar la satisfacción del cliente, tener una visión clara de la capacidad de los departamentos de TI, minimizar el tiempo del ciclo de incidentes y cambios y mejorar resultados con base en métricas, toma de decisiones con base en indicadores de negocio y TI, aportar un valor añadido de confianza mejorando su imagen de cara a otras empresas, convirtiéndose en un factor de distinción frente a la competencia [13]. Esta norma se centra en la integración y aplicación de los procesos coordinados de gestión de servicios. Su objetivo es proporcionar un control continuo, una mayor eficiencia y oportunidades para seguir mejorando. Eso significa trabajar dentro de la organización para alinear el personal y los procedimientos del servicio al cliente, servicios de apoyo, prestación de servicios y equipo de operaciones. Esta norma, está destinada a lograr la garantía de calidad en el servicio de TI y se compone de dos partes principales como se mencionó anteriormente [14].

2.4 ISO 19770

El estándar ISO / IEC 19770 es una familia de normas internacionales para gestión de activos de software (SAM) - *(Software Asset Management)* y aborda tanto los procesos relacionados para la gestión de activos de software como de activos de TI. Debido a que las TIC son facilitadoras esenciales para casi todas las actividades en el mundo de hoy, estos estándares deben integrarse firmemente con todos los componentes de TI. Por ejemplo, desde una perspectiva de proceso, los estándares SAM deben poder utilizarse con todos los estándares del sistema de gestión, porque la gestión de software y el software como tal son componentes esenciales de cualquier sistema de gestión actualmente. Desde una perspectiva tecnológica, los estándares SAM para las estructuras de información proporcionan no sólo la interoperabilidad de datos de gestión de software, sino que también proporcionan la base para muchos beneficios relacionados, como una seguridad más efectiva en el uso de software. Los estándares SAM para estructuras de información también facilitan la automatización significativa de la funcionalidad de TI, como la autenticación mejorada de software y la vinculación a bases de datos de tipo nacional para identificar posibles exposiciones a vulnerabilidades y así identificar y mitigar de forma más automatizada la posible exposición [15].

2.5 ISO / IEC 12207: 2008

Establece un marco común para los procesos del ciclo de vida del software, con una terminología bien definida que puede ser referenciada por la industria del software. Contiene procesos, actividades y tareas que se van a aplicar durante la adquisición de un producto o servicio de software y durante el suministro, desarrollo, operación, mantenimiento y eliminación de productos de software. El software incluye la porción de software del firmware. Se aplica a la adquisición de sistemas y productos y servicios de software, al suministro, desarrollo, operación, mantenimiento y eliminación de productos de software y la porción de software de un sistema, ya sea interna o externamente a una organización. Se incluyen aquellos aspectos de la definición del sistema necesarios para proporcionar el contexto de los productos y servicios de software. También proporciona un proceso que se puede emplear para definir, controlar y mejorar los procesos del ciclo de vida del software [16].

2.6 ISO/IEC 15504

Es un modelo para la mejora y evaluación de los procesos de desarrollo y mantenimiento de sistemas de información y productos de software. ISO/IEC 15504, también conocido como *Software Process Improvement Capability Determination* (SPICE) significa Determinación de la Capacidad de Mejora del Proceso de Software es un emergente estándar internacional de evaluación y determinación de la capacidad y mejora continua de procesos de ingeniería del software, con la filosofía de desarrollar un conjunto de medidas de capacidad estructuradas para todos los procesos del ciclo de vida y para todos los participantes. Es el resultado de un esfuerzo internacional de trabajo y colaboración y tiene la innovación, en comparación con otros modelos, del proceso paralelo de evaluación empírica del resultado. Norma que trata los procesos de ingeniería, gestión, relación cliente-proveedor, de la organización y del soporte. Se creó por la alta competencia del mercado de desarrollo de software, a la difícil tarea de identificar los riesgos, cumplir con el calendario, controlar los costos y mejorar la eficiencia y calidad. Este engloba un modelo de referencia para los procesos y sus potencialidades sobre la base de la experiencia de compañías grandes, medianas y pequeñas [17].

2.7 ISO/IEC 29110

La ISO/IEC 29110 fue desarrollada por el Grupo de Trabajo 24 (WG24) del sub comité 7 (SC7) del Comité Técnico Conjunto 1 (JCT1) de la Organización Internacional de Normalización (ISO) y la Comisión Electrónica Internacional (IEC). La ISO/IEC 29110 ha sido desarrollada para mejorar la calidad del producto y/o servicio de software, y para mejorar el desempeño de la organización, sin pretender excluir el uso de diferentes metodologías de Ciclo de Vida tales como: Cascada, Iterativo, Incremental, Evolutivo o Ágil [18]. Los procesos de ciclo de vida definidos en ISO / IEC 29110 pueden ser utilizados por VSEs *(Very Small Entities)* al adquirir y usar, así como al crear y suministrar un software y sistemas. Una VSE es una empresa, organización, departamento o proyecto que cuenta con al menos 25 personas. Pueden aplicarse a cualquier nivel en una estructura de software y sistemas y en cualquier etapa del ciclo de vida. Los procesos descritos en ISO / IEC 29110 no pretenden impedir o desalentar el uso de procesos adicionales que los VSEs consideren útiles [19].

2.8 ISO/IEC/IEEE 29119

Es el nuevo estándar internacional para pruebas de software. Este estándar comenzó su andadura en 2007, año en el que ISO aprobó la constitución del grupo de trabajo 26 (WG26) dentro del subcomité ISO/IEC JTC1/SC7 *"Software and Systems Enginering".* La estructura de ISO/IEC 29119 consta de cuatro partes: 1. Conceptos y vocabulario; 2. Proceso de pruebas; 3. Documentación de pruebas; 4. Técnicas de prueba [20].

2.9 ISO 25000

ISO / IEC 25000: 2014 proporciona orientación para el uso de la nueva serie de Normas Internacionales denominada Sistemas y Requisitos de Calidad de Software y Evaluación (SQuaRE)-*Systems and software Quality Requirements and Evaluation.* El propósito de ISO / IEC 25000: 2014 es proporcionar una visión general de los contenidos de SQuaRE, modelos de referencia y definiciones comunes, así como la relación entre los documentos, permitiendo a los usuarios de la guía un buen entendimiento de dichas series de estándares, de acuerdo a su propósito de uso. También contiene una explicación del proceso de transición entre la antigua ISO / IEC 9126 y la serie ISO / IEC 14598 y SQuaRE [21].

2.10 UNE-ISO 22301:2015

Protección y seguridad de los ciudadanos. Sistema de Gestión de la Continuidad del Negocio. Esta norma Anula a: UNE 71599-2:2010 y Anula a: UNE-ISO 22301:2013. Esta norma internacional sobre la gestión de la continuidad del negocio, especifica los requisitos para la planificación, el establecimiento, la implantación, la operación, la supervisión, la revisión, el mantenimiento y la mejora continua de un sistema de gestión documentado, a fin de que el negocio esté protegido contra incidentes disruptivos, así como reducir la probabilidad de ocurrencia de estos, estar preparado contra, responder a, y recuperarse de ellos cuando se presentan. Los requisitos especificados en esta norma internacional son genéricos y están previstos para ser de aplicación a todas las organizaciones, o partes de ellas, con independencia del tipo, tamaño y naturaleza de la organización. La amplitud de la aplicación de estos requisitos depende del entorno de operación de la organización y de la complejidad de esta. Esta norma internacional no pretende establecer una estructura uniforme para un sistema de gestión de la continuidad del negocio (SGCN), sino que una organización diseñe un SGCN que sea apropiado a sus necesidades y que cumpla los requisitos de sus partes interesadas. Estas necesidades se modelan según requisitos legales, reguladores, organizacionales e industriales, los productos y servicios, los procesos utilizados, el tamaño y estructura de la organización y los requisitos de las partes interesadas [22].

3. Marcos de Referencia

Se conocen como *Marcos Best Practice,* debido a que en general refieren buenas prácticas a ser desarrolladas. Estas en su mayoría han sido probadas en corporaciones de diferentes países; igualmente es importante resaltar el hecho de que gozan de reconocimiento y aceptación internacional. No son normas internacionales, pero en algunos casos pueden estar alineadas con normas, institutos de certificación de procesos de mucho prestigio, algunas de ellas se han integrado con normas ISO y en algunos casos sirven para allanar el camino a la certificación de una norma, a la vez que estos marcos también son certificables en algunos casos. A continuación, se mencionan los más conocidos internacionalmente y que están alineados con el concepto de gobernanza de las TIC.

3.1 ITIL- Information Technology Infrastructure Library

Aboga por que los servicios de TI estén alineados con las necesidades del negocio y apoyen sus procesos centrales. Proporciona orientación a organizaciones e individuos sobre cómo utilizar la TI como una herramienta para facilitar el cambio, la transformación y el crecimiento del negocio. Las mejores prácticas de ITIL se detallan actualmente en cinco publicaciones principales: Estrategia de Servicio de ITIL, Diseño de servicio de ITIL, Transición de servicios de ITIL, Operación de servicio de ITIL, Mejora continua del servicio de ITIL. Estos cinco volúmenes mapean todo el Ciclo de

Vida de Servicio de ITIL, comenzando con la identificación de las necesidades de los clientes y los conductores de los requerimientos de TI, hasta el diseño e implementación del servicio y finalmente, la fase de monitoreo y mejora del servicio [23].

3.2 COBIT 5 - Control Objectives for Information and Related Technologies

Para poder hablar de COBIT es necesario primero hablar de ISACA® (isaca.org), que ayuda a los profesionales globales a liderar, adaptar y asegurar la confianza en un mundo digital en evolución ofreciendo conocimiento, estándares, relaciones, acreditación y desarrollo de carrera innovadores y de primera clase. Establecida en 1969, ISACA es una asociación global sin ánimo de lucro de 140.000 profesionales en 180 países. COBIT 5 proporciona un marco integral que ayuda a las Organizaciones a lograr sus metas y entregar valor mediante un gobierno y una administración efectivos de la TI de la Organización. Los cinco Principios de COBIT 5: Satisfacer las necesidades de las partes interesadas, cubrir la compañía de forma integral, aplicar un solo marco Integrado, habilitar un enfoque holístico y separar el gobierno de la administración. ISACA ha desarrollado el marco de COBIT 5 para ayudar a las compañías a implementar unos habilitadores de gobierno sanos. De hecho, la implementación de un buen GEIT - (Gobierno Corporativo de la Tecnología de la Información) es casi imposible sin la activación de un marco efectivo de gobierno. El Modelo de Referencia de Procesos de COBIT 5 subdivide las actividades y prácticas de la Organización relacionadas con la TI en dos áreas principales – Gobierno y Administración – con la Administración a su vez dividida en dominios de procesos: El Dominio de Gobierno contiene cinco procesos de gobierno; dentro de cada proceso se definen las prácticas para Evaluar, Dirigir y Monitorear (EDM). Los cuatro dominios de la Administración están alineados con las áreas de responsabilidad de Planificar, Construir, Operar y Monitorear (PBRM por su sigla en inglés) [24].

3.3 CMMI - Capability Maturity Model Integration

El modelo CMMI vio la luz en 1987 como *Capability Maturity Model* (CMM), un proyecto del *Software Engineering Institute,* que es un centro de investigación de la Universidad Carnegie-Mellon. Este centro lo fundó y lo financia el Departamento de Defensa de los Estados Unidos. En 1991, se publicó por primera vez el modelo *CMM for Software*, que está basado en una lista de comprobación de los principales factores de éxito de los proyectos de desarrollo de software realizados a finales de los años setenta y principios de los años ochenta. El modelo también se fundamenta en las investigaciones realizadas por *International Business Machines* (IBM) Corporation y por Philip Crosby y W. Edwards Deming, destacados representantes del ámbito de control de calidad del siglo XX. Tanto el nombre, *Capability Maturity Model,* como los cinco niveles de la representación por etapas están inspirados en el modelo de madurez *Manufacturing Maturity Model de Crosby.* Aplicado principalmente a programas de defensa, el modelo CMM ha logrado una aceptación considerable y se ha sometido a varias revisiones e iteraciones. Su éxito condujo al desarrollo de modelos CMM para diversos ámbitos más allá del ámbito de software. La proliferación de nuevos modelos dio lugar a confusión, por lo que el gobierno financió un proyecto de dos años en el que participaban más de 200 expertos del mundo industrial y académico a fin de crear un solo marco extensible para la ingeniería de sistemas, la ingeniería de software y el desarrollo de productos. El resultado fue CMMI [25]. En general CMMI es un modelo de mejora del rendimiento de clase mundial para organizaciones competitivas que desean lograr operaciones de alto rendimiento. Probado en organizaciones y gobiernos a nivel mundial en los últimos 25 años, CMMI consiste en recolectar las mejores prácticas diseñadas para promover los comportamientos que conducen a un mejor desempeño en cualquier organización [26].

4. Análisis

En este punto es posible que el lector se pregunte sobre la relación que existe entre las normas y los "*frames*" o marcos de referencia y cuales son las ventajas y desventajas de unos y otros. Lo cierto es que ambos, es decir las normas ISO en general los "*frames*" están orientadas a los objetivos del negocio, en general lo que buscan es poner puntos de control en la empresa, desde la perspectiva de la gestión y el gobierno corporativo. Para explicar una posible relación se puede referenciar la Figura 1. Que muestra las posibles intersecciones entre las normas y los marcos de referencia.

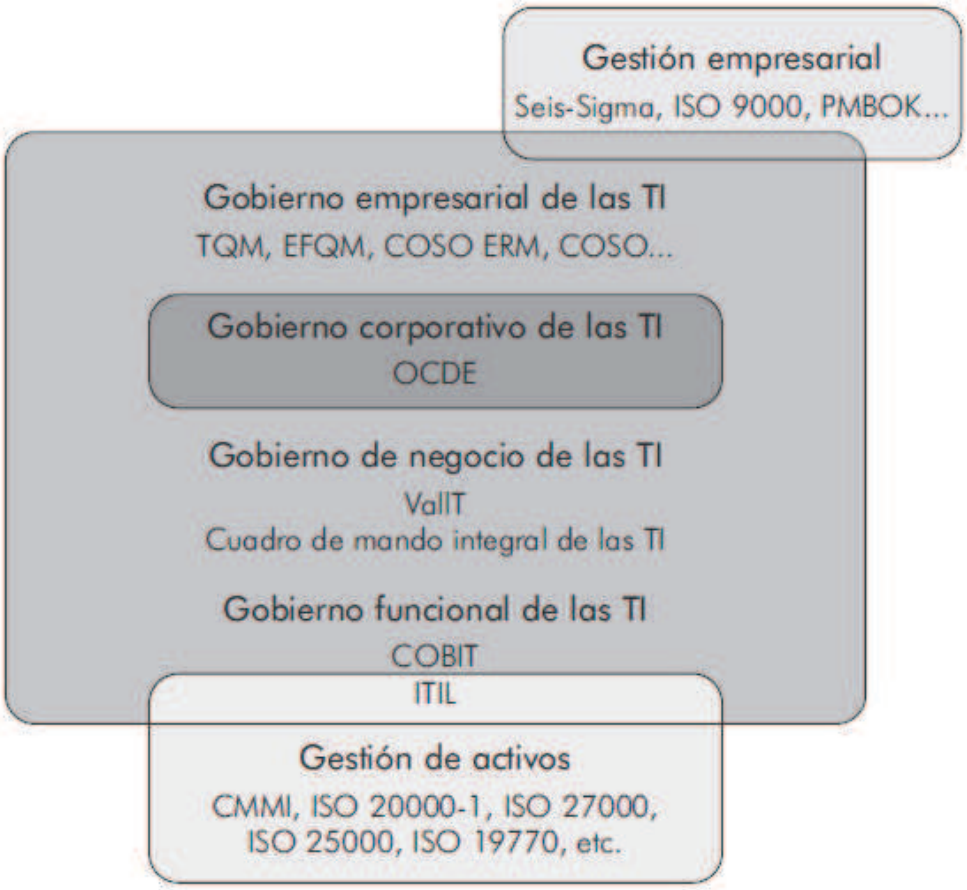

Figura 1. Marcos para el gobierno y la gestión de las tecnologías y sistemas de información [13].

Para continuar, se hace importante mencionar a Aenor[1], quienes proponen que la gestión de las TIC se vincule directamente con la actividad del negocio, la idea es que las TIC y los responsables empresariales puedan entender el concepto de calidad como una parte fundamental de la gestión corporativa y así se puedan alienar y ordenar prioridades, pues normalmente en las organizaciones siempre se pregunta por cuál es la certificación que se debe implementar primero, o cuál es el marco de referencia que se debe certificar primero; básicamente el modelo de Aenor en su propuesta plantea dos certificaciones para la parte de gobierno UNE[2] 7599 e ISO/IEC 38.500; luego la parte de gestión que se desprende del gobierno, subdividirla en tres ramas, la primera evalúa madurez del software ISO 15504, la segunda el sistema de gestión de activos ISO 19770-1, y la tercera el sistema de gestión de servicios ISO 20000-1, como se observa en la Figura 2.

1 Asociación Española de Normalización y Certificación, creada en 1986. AENOR desarrolla también una potente actividad editorial, diseña software para la gestión de sistemas, imparte formación especializada y ofrece distintos servicios de información. Más información en http://www.aenor.es

2 UNE. La Asociación Española de Normalización, UNE, es el organismo legalmente responsable del desarrollo y difusión de las normas técnicas en España. Las normas indican cómo debe ser un producto o cómo debe funcionar un servicio para que sea seguro y responda a lo que el consumidor espera de él

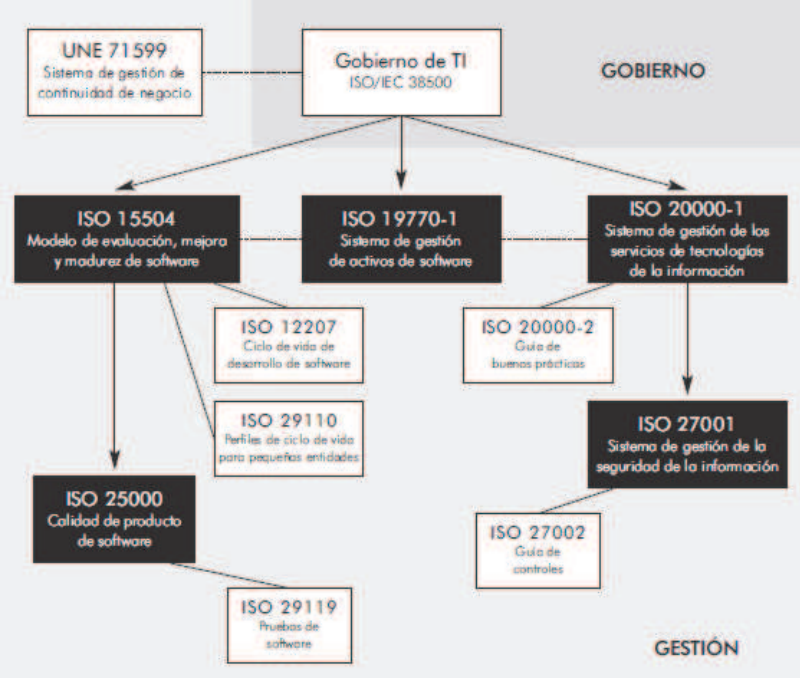

Figura 2. Modelo ampliado de AENOR para las TIC [13]

Es importante entender que los marcos y normas pueden coexistir y en general puede decirse que buscan el mismo objetivo: cuál es el apoyo para la continuidad del negocio, la Figura 3 muestra la norma ISO 38.500 funcionando en un marco teórico unificado y sincronizado, usando marcos y normas en diferentes partes del modelo. En general este tipo de arquitecturas buscan la creación de una cultura de la gestión responsable, garantizando de manera sostenible y a largo plazo el gobierno corporativo, como se observa en la Figura 3, se plantea un modelo de 5 capas, unificando los diferentes sistemas.

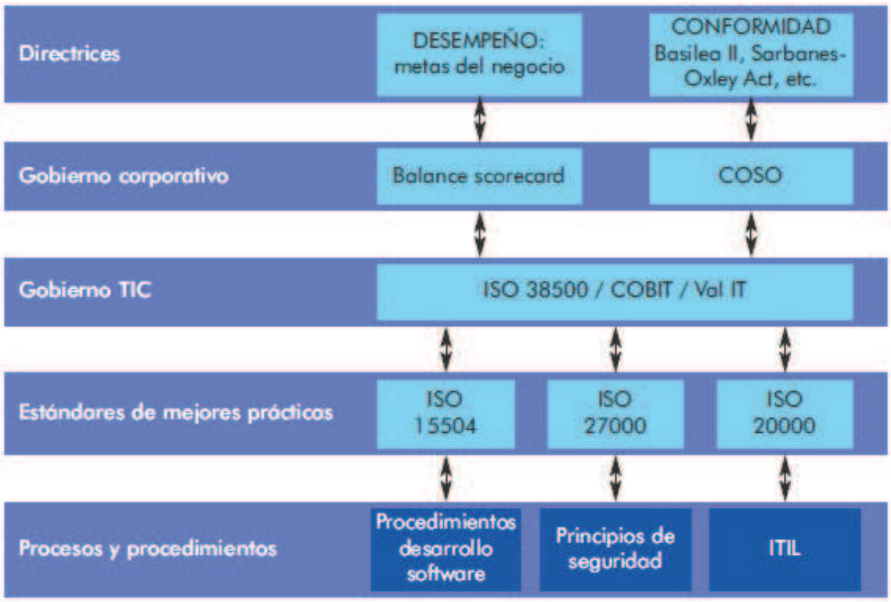

Figura 3. La norma ISO38.500 como marco de operación [13]

5. Conclusiones y trabajo futuro

En esta sección del artículo se presenta esta revisión general da cuenta que, actualmente existe un material documental extenso asociado al tema de la Gobernanza de las TIC, que servirá en cualquier proceso de investigación para abordar este problema, pues este articulo permite hacer comparaciones y ofrece posibilidades para comprender el problema mismo de la gobernanza de las TIC en las organizaciones.

Las normas y marcos de referencia esbozados en este artículo, ofrecen métodos y técnicas precisas para las buenas prácticas asociadas al concepto de gobernanza y gestión de las TIC en las diferentes áreas que normalmente existen en una empresa y que hoy en día deben ser de interés para la alta gerencia, especialmente directores de tecnología que quieran dar un paso adelante en la posibilidad de alinear la tecnología con los intereses misionales en cualquier organización.

Tal como se muestra en este artículo, las normas ISO son una familia compuesta de métodos y procedimientos que permiten de manera independiente a los fabricantes de tecnología, abordar los conceptos de calidad, gestión continuidad, seguridad, evaluación del riesgo, entre otras, y que además desde el ámbito regulatorio, son un camino a seguir justamente para asegurar y disponer de procedimientos documentados, para que cualquier organización logre sus objetivos misionales, cumpliendo la ley y al mismo tiempo mejorando su prestigio y posición en el mercado.

En cuanto a los marcos de referencia internacionales, justifican su estudio, implantación o certificación, debido a que están alineados con las normas internacionales y los beneficios que éstas traen consigo, también desde una arista corporativa, muestran el nivel de compromiso que puede existir en un momento dado en una empresa para que todas las personas involucradas en procesos de gestión o certificación de calidad demuestren que poseen competencias y habilidades para llevar a cabo sus tareas en tiempos oportunos, permitiendo en el mejor de los casos ejecutar la estrategia empresarial evaluando dirigiendo y monitoreando procesos.

Agradecimientos

El autor expresa su agradecimiento al profesor José Antonio Cerrada Somolinos, Director de Departamento de Ingeniería de Software y Sistemas Informáticos, E.T. Superior de Ingeniería Informática de la UNED, por su guía y orientación.

Referencias

[1] B. Gupta, S. Dasgupta, and A. Gupta, “Adoption of ICT in a government organization in a developing country: An empirical study,” *J. Strateg. Inf. Syst.*, vol. 17, no. 2, pp. 140–154, 2008.

[2] P. Weill and J. W. Ross, “How Top Performers Manage IT Decisions Rights for Superior Results,” *IT Gov.*, no. Harvard Business School Press Boston, Massachusetts, pp. 1–10, 2004.

[3] P. Weill and J. Ross, “A Matrixed Approach to Designing IT Governance,” *MIT Sloan Manag. Rev.*, vol. 46, no. 2, pp. 26–34, 2005.

[4] C. M. F. Sánchez and M. P. Velthius, *Modelo para el gobierno de las TIC basado en las normas ISO*. AENOR Ediciones, 2012.

[5] Asociación Española para la Calidad, “Gestión TIC,” 2017. [Online]. Available: https://www.aec.es/web/guest/centro- conocimiento/gestion-tic. [Accessed: 21-Nov-2017].

[6] M. Ballester, "JOnline: Gobierno de las TIC ISO/IEC 38500," 2010. [Online]. Available: https://www.isaca.org/Journal/archives/2010/Volume-1/Pages/Gobierno-de-las-TIC-ISO-IEC-385001.aspx?utm_referrer=. [Accessed: 21-Nov-2017].

[7] ISOTools, "¿Qué es la ISO 27001?," 2017. [Online]. Available: https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001. [Accessed: 21-Nov-2017].

[8] ISO27000.es, "ISO27000.es - El portal de ISO 27001 en español. Gestión de Seguridad de la Información.," 2017. [Online]. Available: http://www.iso27000.es/iso27000.html. [Accessed: 21-Nov-2017].

[9] M. C. P. Alonso, "Seguridad de la información en el Uruguay: políticas de Estado en la administración pública," *Rev. la Asoc. Escribanos del Uruguay*, vol. 97, pp. 137–156, 2011.

[10] K. Hajdarevic and C. Pattinson, "Information security measurement infrastructure for KPI visualization," *Int. Conv. Inf. Commun. Technol. Electron. Microelectron. MIPRO*, pp. 1543–1548, 2012.

[11] A. Leitner and I. Schaumuller-Bichl, "ARiMA - A New Approach to Implement ISO/IEC 27005," in *2009 2nd International Symposium on Logistics and Industrial Informatics*, 2009, pp. 1–6.

[12] M. M. Cabero, "Certificación de calidad en los archivos. Análisis y prospectiva," *Rev. Española Doc. Científica*, vol. 34, no. 3, pp. 447–460, 2011.

[13] AENOR, "Certificación ISO 20000 del Sistema de Gestión de Servicios de Tecnologías de la Información," 2016. [Online]. Available: https://www.aenor.es/aenor/certificacion/calidad/calidad_serviciosti_20000.asp#.WhWHs1WnFph. [Accessed: 21-Nov-2017].

[14] SGS, "ISO 20000 - CERTIFICACIÓN DE TI," 2017. [Online]. Available: http://www.sgs.co/es-es/health-safety/quality-health-safety-and-environment/risk-assessment-and-management/security-management/iso-20000-it-certification. [Accessed: 21-Nov-2017].

[15] ISO, "ISO/IEC 19770-5:2015(en) Information technology — IT asset management — Overview and vocabulary — Part 5," 2015. [Online]. Available: https://www.iso.org/obp/ui#iso:std:iso-iec:19770:-5:ed-2:v1:en. [Accessed: 21-Nov-2017].

[16] ISO, "ISO/IEC 12207:2008 Systems and software engineering -- Software life cycle processes," 2008. [Online]. Available: https://www.iso.org/standard/43447.html. [Accessed: 21-Nov-2017].

[17] EcuRED, "ISO 15504," 2017. [Online]. Available: https://www.ecured.cu/ISO_15504. [Accessed: 21-Nov-2017].

[18] NYCE Colombia, "ISO/IEC 29110," 2016. [Online]. Available: http://nycecolombia.co/isoiec-29110. [Accessed: 21-Nov-2017].

[19] ISO, "ISO/IEC TR 29110-5-1-2:2011 Software engineering -- Lifecycle profiles for Very Small Entities (VSEs) -- Part 5-1-2: Management and engineering guide: Generic profile group: Basic profile," 2011. [Online]. Available: https://www.iso.org/standard/51153.html. [Accessed: 21-Nov-2017].

[20] GT26, "Grupo de Trabajo AEN/CTN71/SC7/GT26 Pruebas de Software. ISO/IEC/IEEE 29119 Software Testing Standard," 2017. [Online]. Available: http://in2test.lsi.uniovi.es/gt26/. [Accessed: 21-Nov-2017].

[21] ISO, "ISO/IEC 25000:2014 Systems and software engineering -- Systems and software Quality Requirements and Evaluation (SQuaRE) -- Guide to SQuaRE," 2014. [Online]. Available: https://www.iso.org/standard/64764.html. [Accessed: 21-Nov-2017].

[22] AENOR, “UNE-EN ISO 22301:2015,” 2015. [Online]. Available: http://www.aenor.es/aenor/normas/normas/fichanorma.asp?tipo=N&codigo=N0054336#.WhWMxlWnFpg. [Accessed: 21-Nov-2017].

[23] AXELOS, “What is ITIL® Best Practice?,” 2017. [Online]. Available: https://www.axelos.com/best-practice-solutions/itil/what-is-itil. [Accessed: 21-Nov-2017].

[24] ISACA, “Acerca de ISACA,” 2017. [Online]. Available: http://www.isaca.org/spanish/Pages/default.aspx. [Accessed: 21-Nov-2017].

[25] Microsoft, “Información general de CMMI,” 2017. [Online]. Available: https://msdn.microsoft.com/es-es/esco/library/ee461556.aspx. [Accessed: 21-Nov-2017].

[26] CMMI Institute, “What Is Capability Maturity Model Integration (CMMI)®?,” 2017. [Online]. Available: http://cmmiinstitute.com/capability-maturity-model-integration. [Accessed: 21-Nov-2017].

Sobre los Autores

Hugo Vecino P. Universidad Nacional de Educación a Distancia-UNED, Escuela Internacional de Doctorado, Doctorado en Ingeniería de Sistemas y Control.

Este artículo se cita:

IEEE

H. Vecino P., “Normas ISO y marcos de referencia para gobernanza de las TIC. Revision general,” Rev. Colomb. Comput., vol. 18, no. 1, pp. 70–81, 2017.

APA

Vecino P., H. (2017). Normas ISO y marcos de referencia para gobernanza de las TIC. Revision general. Revista Colombiana de Computación, 18(1), 70–81.