Modelo para el gobierno de las TIC basado en las normas ISO

Carlos Manuel Fernández Sánchez
y Mario Piattini Velthuis *(Coords.)*

AENOR ediciones

Título: *Modelo para el gobierno de las TIC basado en las normas ISO*
Coordinadores de la obra: Carlos Manuel Fernández Sánchez y Mario Piattini Velthuis

ISBN: 978-84-8143-764-5
Impreso en España - Printed in Spain

Edita: AENOR
Maqueta y diseño de cubierta: AENOR

Nota: AENOR no se hace responsable de las opiniones expresadas por los autores en esta obra.

AENOR Asociación Española de Normalización y Certificación

Génova, 6. 28004 Madrid • Tel.: 902 102 201 • Fax: 913 103 695
comercial@aenor.es • www.aenor.es

Índice

Prólogo

Desde finales de los años 90, ante el emergente desarrollo de la normalización en el sector de las tecnologías de la información, AENOR comienza una nueva andadura y abre un amplio horizonte con la creación, dentro de la División de Desarrollo, del Área de Tecnologías de la Información y Comunicaciones (TIC), bajo el principio de I+D+i, poniendo especial énfasis en la innovación en el sector de las TIC y en la utilización de las normas ISO como referenciales internacionalmente reconocidos para la evaluación de la conformidad.

En el año 2004 y, siguiendo la línea de innovación continua en las TIC, pusimos en marcha el primer piloto de certificación de sistema de gestión de la seguridad de información con la norma española UNE 71502:2004 en una empresa del sector financiero, que culminó con su certificación en ese mismo año; sería la primera de las muchas que la seguirían.

Dos años más tarde, desde el área de TIC, Carlos Manuel Fernández Sánchez diseña y desarrolla un modelo de gobierno y gestión de las normas ISO, racionalizando y simplificando el entramado normativo y su aplicación. Desde su creación, en estos últimos seis años, se han llevado a cabo distintos pilotos de implantación y certificación en grandes corporaciones y pymes, tanto en España y Europa como en Latinoamérica, llegando a alcanzar casi un total de quinientas empresas y entidades certificadas en algún sistema del modelo, con el objetivo de alcanzar la calidad y seguridad de los servicios de tecnología de la información, y la madurez del ciclo de ingeniería del software.

Este modelo, diseñado y extendido desde AENOR, que tiene por objetivo la implantación en las empresas del ciclo de mejora continua o ciclo de Deming (PDCA), orientado a los objetivos de las distintas organizaciones, es el descrito en esta publicación que, además, recoge las experiencias de múltiples empresas que han alcanzado

su certificación por AENOR, porque es precisamente en base a ellas por lo que surge la creación del modelo.

Hasta aquí el resumen de la senda abierta hasta este momento, que sin duda ha de seguir siendo recorrida y ampliada en un futuro. Solo me queda expresar mi agradecimiento a las personas que han hecho posible, con su dedicación y empeño, esta realidad que he tenido el placer de supervisar: Carlos Manuel Fernández Sánchez y Boris Delgado Riss. Asimismo, mi gratitud al catedrático Mario Piattini Velthuis, por su inestimable asesoramiento y colaboración en esta publicación y, por supuesto, a todos los coautores de la misma, ya que son grandes profesionales del sector.

También quiero hacer mención a las que son el objeto de toda esta labor: las empresas y entidades que, con amplitud de miras y apostando por el futuro, han depositado la confianza de su auditoría y certificación en AENOR, haciendo realidad el éxito alcanzado por el modelo propuesto.

Es nuestro deseo que este libro resulte de gran ayuda para los directores generales, directores de TIC y profesionales del sector, en la búsqueda constante de la excelencia en el gobierno y gestión de las TIC.

José Luis Tejera Oliver
Director de la Dirección
de Desarrollo de AENOR

Introducción

Las tecnologías y los sistemas de información (TSI) se han convertido en el elemento más esencial para la supervivencia de las organizaciones, ya que de las TSI dependen el buen funcionamiento y la evolución de sus procesos de negocio, así como la información que necesitan para tomar todas sus decisiones operacionales, tácticas y estratégicas.

Por ello, cobran cada día más interés el **gobierno** y la **gestión** de las TSI, temas en los cuales el director de TI, conocido habitualmente como CIO por las siglas de su denominación en inglés (*Chief Information Officer*), es llamado a desempeñar un papel crucial. El director de TI deberá implementar un conjunto de buenas prácticas de gobierno y de gestión en las diferentes áreas relacionadas con la prestación de servicios, desarrollo de software, seguridad, gestión de activos, etc.

En los últimos años, y especialmente a partir de 2006, se han publicado varias normas internacionales relacionadas con el gobierno y la gestión de las TSI que pueden resultar de mucho interés para las organizaciones, ya que recogen estas buenas prácticas, validadas y consensuadas a nivel internacional por más de 155 países.

Con este libro pretendemos ayudar al director de TI en su labor de gobierno y gestión de las TSI, dando a conocer las normas y explicando cómo utilizarlas en la "realidad", con el fin de articular un sistema de gobierno y de gestión en el que encajen las diferentes buenas prácticas. En definitiva, esta publicación es el resultado de la aplicación real del modelo de AENOR de gobierno y gestión de las TSI con estándares ISO.

La obra consta de catorce capítulos, escritos por diferentes autores: el capítulo 1 es una introducción al gobierno y gestión de las TSI, y el capítulo 2 ofrece una panorámica de la normalización en esta área. Los capítulos del 3 al 12 están dedicados a presentar una norma o una serie de normas que abordan un área concreta del gobierno o de la gestión de las TSI, además de incluir (cuando ha sido posible) una experiencia

práctica sobre la aplicación de dicha norma. A modo de resumen, los coordinadores hemos incluido una "ficha" para cada capítulo, en la que sintetizamos el problema que intenta resolver la norma, cómo contribuye la misma al gobierno o a la gestión de las TSI, y cuáles son los principales factores críticos de éxito a tener en cuenta a la hora de aplicar las buenas prácticas que recoge dicha norma.

Por último, se incluyen dos capítulos que abordan sendos problemas de gran interés para las organizaciones: en el capítulo 13 se trata la integración de diferentes normas, mientras que el capítulo 14 está centrado en la certificación.

Debido a su alcance, la lectura de esta obra puede realizarse de maneras muy distintas dependiendo de la finalidad y conocimientos previos del lector. En cualquier caso, es recomendable empezar por los capítulos 1 y 2, luego abordar el capítulo concreto en el que se tenga mayor interés y, si se está persiguiendo una certificación, finalizar con la lectura del capítulo 14. La estructura del libro (los capítulos son independientes e incluyen su propia bibliografía) lo hace adecuado para consultar cualquier norma de manera independiente.

Agradecimientos

Querríamos expresar nuestro agradecimiento, en primer lugar, a los autores que colaboran en esta obra y que son sus verdaderos artífices: sus conocimientos y experiencia en el gobierno y la gestión de las TSI, así como en la aplicación (en muchos casos pionera a nivel internacional) de las diferentes normas, constituyen el verdadero valor de este libro.

A las empresas que han implantado y certificado estos estándares, y a los auditores de AENOR y de entidades colaboradoras, por su trabajo de campo y colaboración constante.

A D. José Luis Tejera, Director de Desarrollo Estratégico e impulsor del área de las TIC dentro de AENOR, bajo cuya dirección se ha diseñado y desarrollado el modelo de ISO en las TIC que se refleja en este libro, y por haber aceptado escribir el prólogo del mismo.

A la Dirección de Servicios de Información y al Departamento Editorial de AENOR por su ánimo y apoyo constantes, haciendo posible que esta publicación concluyera con éxito.

Carlos Manuel Fernández Sánchez
Mario G. Piattini Velthuis
(Coordinadores)

Normas

- ISO/IEC 38500:2008 *Corporate governance of information technology*.
- UNE-ISO/IEC 20000-1:2007 *Tecnología de la información. Gestión del servicio. Parte 1: Especificaciones* (ISO/IEC 20000-1:2005).
- UNE-ISO/IEC 20000-2:2007 *Tecnología de la información. Gestión del servicio. Parte 2: Código de buenas prácticas* (ISO/IEC 20000-2:2005).
- ISO/IEC 20000-2:2012 *Information technology – Service management – Part 2: Guidance on the application of service management systems*.
- UNE-ISO/IEC 20000-1:2011 *Tecnología de la información. Gestión del servicio. Parte 1: Requisitos del Sistema de Gestión del Servicio (SGS)*.
- UNE-ISO/IEC 27001:2007 *Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos* (ISO/IEC 27001:2005).
- UNE-ISO/IEC 27002:2009 *Tecnología de la Información. Técnicas de seguridad. Código de buenas prácticas para la gestión de la seguridad de la información.*
- ISO/IEC 15504-3:2004 *Information technology – Process assessment – Part 3: Guidance on performing an assessment*.
- ISO/IEC 15504-4:2004 *Information technology – Process assessment – Part 4: Guidance on use for process improvement and process capability determination.*
- ISO/IEC 15504-1:2004 *Information technology – Process assessment – Part 1: Concepts and vocabulary*.
- ISO/IEC TR 15504-7:2008 *Information technology – Process assessment – Part 7: Assessment of organizational maturity*.
- ISO/IEC TS 15504-10:2011 *Information technology – Process assessment – Part 10: Safety extension*.
- ISO/IEC TR 15504-6:2008 *Information technology – Process assessment – Part 6: An exemplar system life cycle process assessment model*.
- ISO/IEC 12207:2008 *Systems and software engineering – Software life cycle processes*.
- ISO/IEC TR 29110 *Software engineering – Lifecycle profiles for Very Small Entities (VSEs)*.
- UNE-ISO/IEC 19770-1:2008 *Tecnología de la Información. Gestión de activos de software (SAM). Parte 1: Procesos.*

- UNE 71599-1:2010 *Gestión de la continuidad del negocio. Parte 1: Código de práctica.*
- UNE 71599-2:2010 *Gestión de la continuidad del negocio. Parte 2: Especificaciones.*
- ISO/IEC 25000:2005 *Software Engineering – Software product Quality Requirements and Evaluation (SQuaRE) – Guide to SquaRE.*
- ISO/IEC/IEE 29119 *Software and systems engineering – Software testing.*

Problema a resolver

El gobierno y la gestión de un Centro de Proceso de Datos/Centro de Cómputo utilizando las mejores prácticas (estándares/normas ISO, consensuadas por más de 155 países) y aplicando tres factores imprescindibles, como son la eficiencia, la eficacia y la economía.

Contribución de la norma para la gestión de las TIC

El modelo de ISO en las TIC de AENOR contempla el gobierno y la gestión, incluyendo estándares para ambos conceptos. El modelo aquí presentado ha sido implementado inicialmente con pilotos por múltiples empresas en el mundo y certificado los sistemas por AENOR.

Factores críticos de éxito

- El modelo ISO en las TIC está orientado a los objetivos de negocio, ya sean nuevos proyectos o servicios.
- El modelo ISO en las TIC consta de dos elementos primordiales que suelen estar reflejados en dos estándares que componen un sistema de gestión: el ciclo PHVA-motor y el control interno de tecnologías de la información-conocimiento. El ciclo PHVA está orientado a la mejora continua.
- La simplicidad del ciclo PHVA orientado a los objetivos de negocio facilita la labor de gestión y gobierno en las TIC.
- El modelo ISO en las TIC no es una moda: es aplicar el control interno de tecnologías de la información (considerando los objetivos de negocio) a cualquier nueva tecnología, negocio o servicio de TIC.
- El modelo ISO en las TIC incorpora la calidad y la seguridad en los servicios y proyectos de TIC.
- El modelo ISO en las TIC contempla indicadores (objetivo de la métrica) y métricas orientadas al negocio en el mundo de las TIC.
- Cualquier proyecto de innovación se puede incorporar en el modelo ISO en las TIC.
- En definitiva, el objetivo del modelo ISO en las TIC consiste en que el plan de TIC cumpla con los objetivos definidos en el plan estratégico de la organización.

1 El gobierno y la gestión de las tecnologías y sistemas de la información

Carlos Manuel Fernández Sánchez
Mario Piattini Velthuis

1.1. Definición de gobierno de las tecnologías y sistemas de la información

El concepto de gobierno de las tecnologías y sistemas de la información (TSI), conocido normalmente por gobierno de las TI (tecnologías de la información) o también por gobernanza de las TI, no es actual, ya que se viene tratando más o menos implícitamente desde los años sesenta, si bien es verdad que con este nombre se empezó a utilizar a finales de los noventa (por ejemplo, Brown (1997) y Sambamurthy y Zmud (1999)).

Existen multitud de definiciones de gobierno de las TI; así, por ejemplo, el ITGI (IT Governance Institute)[1] destaca que el gobierno de las TI es "responsabilidad del comité de dirección y de los ejecutivos. Es una parte integral del gobierno de la organización y 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" (ITGI, 2003).

Weill (2004) define gobierno de las TI como "la especificación del marco sobre los derechos y responsabilidades de decisión para alentar el comportamiento deseable del uso de las TI". En este sentido cabe recordar que Allen (2005) define gobierno como "fijar expectativas claras para la conducta (comportamiento y acciones) de la entidad que está siendo gobernada, y dirigir, controlar e influenciar fuertemente dicha entidad para cumplir estas expectativas". Por ello, este autor afirma que el gobierno puede resumirse de manera sencilla en que "la organización está haciendo las cosas adecuadas y adecuadamente en el tiempo oportuno". Esto implica que los directivos toman las

[1] Fundado por la ISACA (Information Systems Audit and Control Association) en 1998.

decisiones adecuadas obteniendo los resultados adecuados, para lo cual es imprescindible que también las TI funcionen de manera adecuada. Todo ello teniendo en cuenta que cosas "adecuadas" y "adecuadamente" son conceptos relativos, que variarán de una organización a otra y que cambiarán en el tiempo, al cambiar los objetivos de la organización. En efecto, la implementación del gobierno de las TI no ocurre en el vacío, sino que viene determinada por diferentes circunstancias (Kordel, 2004) como:

- La ética y la cultura de la organización y el sector al que pertenece.
- Las leyes, regulaciones y guías de actuación, tanto internas como externas.
- La misión, visión y valores de la organización.
- Los modelos de la organización relativos a los roles y responsabilidades.
- Las políticas y las prácticas de gobierno de la organización y la industria.
- El plan de negocio y los propósitos estratégicos de la organización.

Otra definición sobre gobierno de las TI es la de Dahlberg y Kivijärvi (2006), quienes señalan que el gobierno de las TI debe ser integral e incluir tanto los procesos de gobierno como las perspectivas de estructura, integrando las estructuras y procesos de gobierno, el alineamiento de negocio, las operaciones de TI y la medición del desempeño y la entrega de valor.

Webb *et ál.* (2006) analizan otras doce definiciones existentes de gobierno, de las que destacan cinco elementos:

- Alineamiento estratégico.
- Entrega de valor de negocio a través de las TI.
- Gestión del desempeño.
- Gestión de riesgos.
- Control y responsabilidades.

A partir de estas definiciones, los autores proponen una definición "definitiva" para gobierno de las TI: "El gobierno de las TI es el alineamiento estratégico de las TI con la organización de forma tal que se consigue el máximo valor de negocio por medio del desarrollo y mantenimiento de un control y responsabilidades efectivas, gestión del desempeño y gestión de riesgos de las TI".

Más recientemente, la norma ISO/IEC 38500:2008 *Corporate governance of information technology* (ISO/IEC, 2008) define el gobierno de las TI como "el sistema por el que se dirige y controla la utilización actual y futura de la tecnología de la información".

Otra definición muy actual la podemos encontrar en el sitio web impulsado por el ITGI, conocido como *Taking Governance Forward*[2], en el que se define el gobierno de las TI como "una vista de gobierno que consta del gobierno de negocio de las TI (asegurar que las TI soportan y permiten llevar a cabo la estrategia empresarial) y una vista de gobierno funcional de las TI (asegurar que la función de TI en sí misma se ejecuta de manera eficiente y efectiva)".

1.2. Diferencia entre gobierno y gestión de las TSI

Hay que tener en cuenta que, mientras que la gestión de las TSI está más enfocada al suministro interno de TSI y tiene su orientación temporal en el presente, el gobierno de las TSI es más amplio ya que, además, pretende atender las demandas externas (de los clientes) y en un horizonte temporal futuro (Peterson, 2003). Así, la gestión se centraría en administrar e implementar las estrategias en el día a día, mientras que el gobierno se encargaría de fijar dichas estrategias junto con la política y la cultura de la organización.

Por otro lado, según Hamaker y Hutton (2004), mientras que el gobierno de la organización se refiere al marco de responsabilidad global que coordina todas las actividades de gestión respecto a todos los *stakeholders* (partes interesadas), el gobierno corporativo corresponde principalmente a la junta o consejo de gobierno, el equipo de gestión ejecutiva y los accionistas. El gobierno de las TI, por su parte, se centra en el uso de la tecnología para satisfacer los objetivos de la organización fijados por la dirección. Por ello, el gobierno corporativo incluye aspectos del gobierno de las TI, ya que, sin una gestión eficaz de las TI, los encargados de las responsabilidades corporativas no podrían desempeñarse de forma efectiva (Fink *et ál.*, 2006).

Desde hace algunos años, la palabra "gobierno" se ha generalizado y puesto de moda; así, se habla, entre otros, de: gobierno de proyectos software, gobierno de arquitectura software, gobierno de bases de datos, gobierno de SOA, gobierno de desarrollo de software, gobierno de la seguridad, etc. Ahora bien, aunque en todas estas áreas específicas se pueda considerar que hay aspectos de "gobierno", realmente el gobierno se centra en los seis principios, a saber: responsabilidad, estrategia, adquisición, rendimiento, conformidad y factor humano; y en las tres funciones de evaluar, dirigir y monitorizar (en las que se profundiza en el capítulo 3).

En definitiva, ante la aparición de nuevos negocios y nuevas herramientas para las empresas, el gobierno de las TI se encargará de alinear el plan de las TIC con el *business plan* o plan estratégico de la empresa; mientras que la factoría de las TIC será la encargada de gestionar las áreas específicas con los nuevos servicios u operaciones que se puedan ir incorporando (véase la figura 1.1).

[2] http://www.takinggovernanceforward.org/Pages/glossary.aspx#midpage

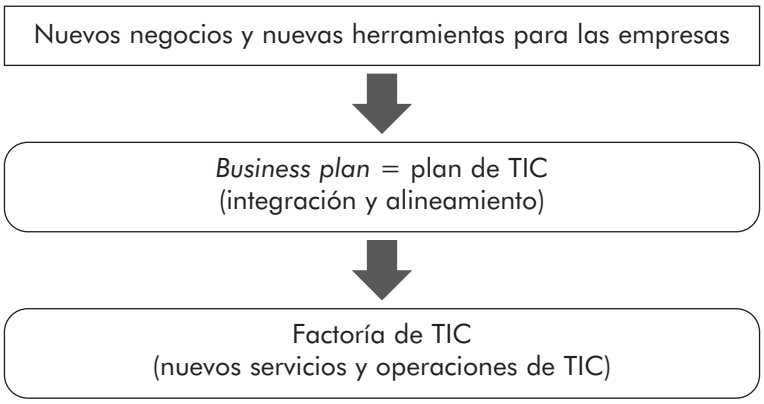


Figura 1.1. **Las TIC como apoyo a la gestión de las empresas**

1.3. Marcos para el gobierno y la gestión de las TSI

Existen multitud de marcos para el gobierno y gestión de las TSI, algunos de los cuales se describen en Hervada y Piattini (2007). Entre los más conocidos probablemente se encuentren COSO, COBIT, CMMi, UNE-ISO/IEC 27001:2007, ISO/IEC 15504:2004, ISO/IEC 15408:2009, ITIL, PMBOK, etc.

Algunos se centran en áreas muy concretas, como ISO/IEC 15408:2009 o PMBOK, mientras que otros son muy amplios, como es el caso de COBIT o COSO.

En el sitio anteriormente citado, *Taking Governance Forward*, se clasifican varios de estos marcos como se muestra en la figura 1.2.

1.4. Las normas y el gobierno y la gestión de las TSI

La propia evolución del sector de las TIC y su uso masivo por parte de las empresas y organizaciones ha provocado en los últimos años un reenfoque en el papel de las normas, pasando de la normalización de requisitos técnicos de productos electrónicos a una visión más global de sistemas de gestión, donde dichos aparatos y equipos no se entienden como elementos aislados, sino como parte de un conjunto donde interactúan entre sí y aportan valor añadido al sistema.

La inclusión en el sector de las TIC de criterios de gestión basados en la calidad, la seguridad y la protección ambiental también ha contribuido a este cambio de mentalidad.

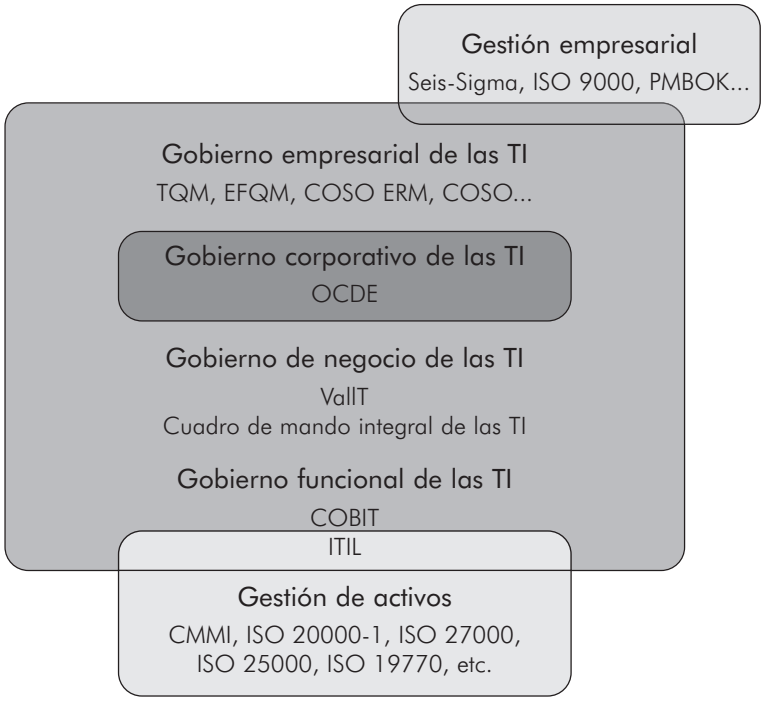


Figura 1.2. **Marcos para el gobierno y la gestión de las TSI (adaptado del sitio web *Taking Governance Forward*)**

Concretamente en España, las TIC vivieron un crecimiento inusitado durante la década de 1990 que las colocó en primera línea de la modernización del tejido empresarial y de la Administración Pública. Fruto de estas nuevas demandas, ya a principios de la primera década del siglo XXI, AENOR comenzó a estudiar la posibilidad de responder a ellas desde la certificación y, lo más importante, desde una nueva visión del papel que han de jugar las TIC en el conjunto de una organización.

Hasta ese momento, las empresas que querían aportar un valor añadido a su departamento de TIC recurrían a la certificación en sistemas de gestión de la calidad a través de las normas de la familia ISO 9001, excelentes en sus resultados pero un tanto generalistas para las incipientes necesidades del sector de las tecnologías de la información y la comunicación, que a todas luces comenzaba a demandar respuestas más centradas en su actividad. Como casi siempre ha ocurrido en la vida de las TIC, la velocidad a la que se producen las necesidades no es mayor que a la que aparecen las novedades que las cubren.

Tras un período de gestación de un par de años, AENOR presentó en 2006 su respuesta en el ámbito de la certificación para las TIC y su creciente protagonismo. Se

trataba de la hoja de ruta para el gobierno y la gestión de las TIC, un esquema de certificación que proponía nada menos que un cambio cultural en la que, por aquel entonces, era la visión de las TIC, su responsabilidad, espacio y competencias dentro de la organización.

La clave estaba en entender desde otra perspectiva la función del Centro de Proceso de Datos (CPD) de la organización. El CPD deja de ser un departamento que hace que todo funcione (redes, ordenadores, etc.) para convertirse en una pieza más del engranaje de la empresa enfocada a objetivos de negocio. Cambia la visibilidad del CPD, y la certificación que propone este nuevo modelo de AENOR hace que la gestión de las TIC se vincule directamente con la actividad de negocio. Se puede decir que, gracias a este modelo, el CPD y el resto de la organización comienzan a hablar el mismo lenguaje y a interconectar de manera más natural y eficiente. Las TIC y sus responsables se vuelcan en los objetivos empresariales como un área más de la organización, además de entender la calidad como un principio global en su actividad.

Gracias a este modelo de gobierno y gestión de AENOR para las TIC, los responsables de los CPD pueden entender los beneficios de la certificación, conocer cuál es la más adecuada para cada caso, ordenar sus prioridades, organizar su estructura y, quizás lo más importante, alinear sus objetivos y sus respuestas con los propios objetivos y necesidades del plan estratégico global de la organización.

Aun a riesgo de parecer contradictorio, el modelo de gobierno y gestión de las TIC que propuso AENOR hace ya seis años es una respuesta compleja a necesidades también complejas, pero desde la sencillez en su aprehensión. En la figura 1.3 se puede ver una versión ampliada del modelo propuesto por AENOR.

Básicamente, el modelo propone dos certificaciones para la parte de gobierno corporativo de las TIC y del sistema de gestión de continuidad del negocio (UNE 71599-2:2010 y ISO/IEC 38500:2008).

Para el área puramente de gestión, divide esta en dos campos: los sistemas de gestión de servicios de TI SGSTI (UNE-ISO/IEC 20000-1:2011) y los sistemas de gestión de la seguridad de la información SGSI (UNE-ISO/IEC 27001:2007).

Con la implantación del SGSTI (UNE-ISO/IEC 20000-1:2011) se alcanza la calidad en los servicios de las TIC considerando los objetivos del negocio. Con la implantación del SGSI (UNE-ISO/IEC 27001:2007) se logra gestionar los riesgos de los sistemas de información y, por tanto, la seguridad de los mismos.

Esto conlleva minimizar los posibles riesgos de las TIC y devolver calidad y confianza a los sistemas de información.

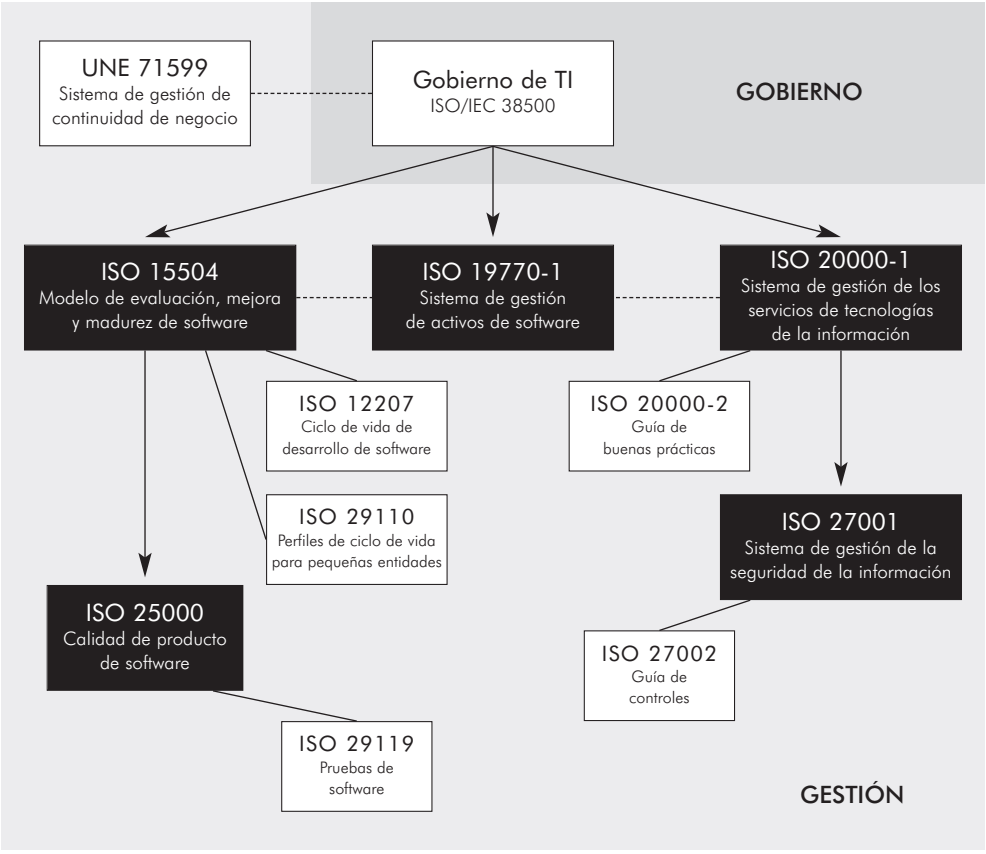


Figura 1.3. **Modelo ampliado de AENOR para las TIC**

El segundo campo del área de gestión es donde se agrupan las actividades de desarrollo de programas enfocado a la calidad del software (modelo de evaluación, mejora y madurez del software, SPICE ISO 15504:2004; ISO 12207:2008 *Systems and software engineering – Software life cycle processes* y UNE-ISO/IEC 19770-1:2008 *Tecnología de la Información. Gestión de activos de software (SAM). Parte 1: Procesos*). Este modelo puede ser complementado con un trabajo que se viene desarrollando hace algunos años sobre perfiles del ciclo de vida para pequeñas entidades (ISO/IEC 29110:2011) y con la familia de normas ISO/IEC 25000:2005 sobre calidad de producto software, y con la ISO/IEC 29119:2011 sobre pruebas de software.

Hay que tener en cuenta que las normas ISO/IEC, así como las normas nacionales, proporcionan a las empresas una serie de marcos de gestión para abordar la organización de las TI. Son marcos que gozan del reconocimiento internacional, basados en el esquema PHVA (Planificar-Hacer-Verificar-Actuar) y, por tanto, integrables con

otros modelos de gestión como el de la calidad (modelo 9000), o el medioambiental (modelo 14000).

Normalmente, la estructura compartida por los modelos de gestión consta de una norma general sobre terminología y vocabulario propios del modelo y otra que recoge una serie de recomendaciones o buenas prácticas de cara a la implantación de las especificaciones o requisitos propios del sistema de gestión, los cuales son recogidos en otra de las normas de la serie. Esta norma de requisitos es el referente de certificación de la serie, es decir, la norma respecto a la cual se puede obtener la conformidad, ya sea de manera interna o por parte de un tercero independiente.

Viene siendo habitual que las series se vayan enriqueciendo con normas que proporcionan directrices sobre cómo auditar el sistema de gestión o cómo seleccionar su alcance, y con otras normas dirigidas hacia la competencia de los organismos que auditan o certifican y que sirven de base al establecimiento de los esquemas de acreditación.

En algunos modelos se comienzan a desarrollar normas de carácter vertical, más específico, que recogen las recomendaciones y requisitos específicos para un sector determinado (por ejemplo, sanitario, telecomunicaciones, etc.), a partir de los criterios de la norma marco general.

Otras normas que complementan a las anteriores son:

- UNE-ISO/IEC 90003:2005 *Ingeniería del software. Guía de aplicación de la ISO 9001:2000 al software*, que ayuda a adaptar el sistema de gestión de la calidad de la empresa a las TI.
- La serie ISO/IEC 15408:2009 *Information technology – Security techniques – Evaluation criteria for IT security*, que establece criterios de evaluación para la seguridad de los sistemas informáticos.
- ISO/IEC TR 24766:2009 *Information technology – Systems and software engineering – Guide for requirements engineering tool capabilities*, que establece características específicas para herramientas de requisitos.
- ISO/IEC 24773:2008 *Software engineering – Certification of software engineering professionals – Comparison framework*, que establece las bases para la certificación del personal de TI.
- ISO 31000:2009 *Risk management – Principles and guidelines*, sobre modelos de gestión del riesgo.

1.5. Conclusiones

Los temas relativos al gobierno y a la gestión de las TSI son cada vez más importantes para las empresas, ya que el gasto e inversión en TSI no se controlan como se debiera, y en demasiadas ocasiones no se consigue un uso eficaz, eficiente y económico de las TIC. En los últimos años han surgido numerosos marcos y normas ISO para el gobierno y la gestión de las TSI, que consideramos como una valiosísima ayuda en la consecución de este objetivo, aun teniendo en cuenta que siempre deberemos evaluar los riesgos que suponen las TIC valorando su importancia respecto a los controles y costes que pueden conllevar.

Pensamos que, en un futuro cercano, todos los departamentos de informática deberán tener implantadas buenas prácticas que cubran las diferentes áreas de gobierno y gestión, para lo cual centrarán sus esfuerzos en definir, medir y analizar los procesos relacionados con las TSI y en su mejora continua.

Probablemente, como señalaba en 2008 David Flint, vicepresidente de Gartner-Research, los directores de informática (CIO) se convertirán en *Chief Process Officers* (CPO), alineados e integrados con los objetivos de sus empresas u organizaciones para lograr la excelencia en el servicio de las TIC, innovando y desarrollando nuevos productos. Y ello no es el fruto de una moda: es un síntoma de la madurez que está alcanzando el gobierno y la gestión de las TSI.

1.6. Bibliografía

Allen, J. *Governing for Enterprise Security*. Technical Note. CMU/SEI-2005-TN-023, Software Engineering Institute. 2005.

Brown, C. V. "Examining the emergence of hybrid IS governance solutions: Evidence from a single case site". *Information Systems Research*. Vol. 8(1), pp. 69-95. 1997.

Dahlberg, T. y Kivijärvi, H. *An Integrated Framework for IT Governance and the Development and Validation of an Assessment Instrument*. Proc. of the 39th Hawaii International Conference on System Sciences. IEEE Computer Society. 2006.

Fernández Sánchez, C. M. Documentación de la asignatura Control y auditoría de sistemas de información. Universidad Pontificia de Salamanca. Curso 2010-2011.

Fink, D.; Huegle, T. y Dortschy, M. *A Model of Information Security Governance for E-Business*. Idea Group Publishing. 2006.

Hamaker, S. y Hutton, A. "Principles of IT Governance". *Information Systems Control Journal*. Vol. 2. 2004.

Hervada, F. y Piattini, M. (eds.). *Gobierno de las tecnologías y los sistemas de información*. Ra-Ma. Madrid, 2007.

ISO/IEC 38500:2008 *Corporate governance of information technology*.

ITGI. *IT Governance Executive Summary*. IT Governance Institute. 2003.

Kordel, L. "IT Governance Hands-on: Using CobiT to Implement IT Governance". *Information Systems Control Journal*. Vol. 2. 2004.

Peterson, R. R. *Integration Strategies and Tactics for Information Technology Governance. Strategies for Information Technology Governance*. Idea Group Publishing. 2003.

Sambamurthy, V. y Zmud, W. "Arrangements for information technology governance: A theory of multiple contingencies". *MIS Quarterly*. Vol. 23(2), pp. 261-291. 1999.

Webb, P.; Pollard, C. y Ridley, G. *Attempting to Define IT Governance: Wisdom or Folly?* Proc. of the 39th Hawaii International Conference on System Sciences. IEEE Computer Society. 2006.

Weill, P. "Don't Just Lead, Govern: How Top-Performing Firms Govern IT". *MIS Quarterly Executive*. Vol. 3 (1), pp. 1-17. 2004.

Sobre los autores

Carlos Manuel Fernández Sánchez (Coordinador)

Ingeniero en Informática por la Universidad Politécnica de Madrid (UPM). MBA por CECO. Diplomado en Estudios avanzados en informática por la Universidad Pontificia de Salamanca en Madrid (UPSAM). Diplomado en ADE en CEPADE-UPM. CISA y CISM por ISACA. Tiene más de 35 años de experiencia en el sector de las TIC en España, Europa y América.

Desde 2004, Coordinador de TIC/Jefe de certificaciones TIC en AENOR (Desarrollo, investigación y certificación en el área de TI de la Dirección de Desarrollo estratégico).

Profesor asociado de la UPSAM y profesor del máster de auditoría de sistemas de información y seguridad en la UPM y en la Universidad de Alcalá de Henares.

Patrono de la Fundación I+D software libre.

Directivo del Colegio Profesional de Ingenieros en informática de Madrid.

Fundador de la Asociación de Auditores Informáticos de España – ASIA – Chapter ISACA Madrid.

Mario Piattini Velthuis (Coordinador)

Doctor y licenciado en Informática por la Universidad Politécnica de Madrid. Licenciado en Psicología por la UNED. Máster en auditoría informática (CENEI). Especialista en la aplicación de tecnologías de la información en la gestión empresarial (CEPADE-UPM). CISA, CISM, CRISC, y CGEIT por ISACA. Diplomado en Calidad por la AEC. CSQE por ASQ. Auditor 15504 por AENOR, y CMMI, ITIL y TMap Foundations.

Catedrático de Universidad de Lenguajes y sistemas informáticos en la Escuela Superior de Informática de la Universidad de Castilla-La Mancha (UCLM), donde dirige el grupo de investigación Alarcos, especializado en calidad de sistemas de información. También es Director del Centro Mixto de Investigación y Desarrollo de Software UCLM-Indra y Director del Instituto de Tecnologías y Sistemas de Información (ITSI) de la UCLM.

Manuel Ballester Fernández

Doctor e Ingeniero Industrial. CISA, CISM y CGEIT por ISACA. MBA. Tiene más de 35 años de experiencia en el sector de las TIC donde ha desempeñado diversos cargos directivos.

Ha sido Former Presidente del Capítulo de ISACA en Madrid y pertenece a varios comités de ISACA Internacional. Vicepresidente de la Academia Mexicana de Ciencia de Sistemas, miembro del JTC1/WG6 y coeditor de la Norma ISO/IEC 38500.

Actualmente es Socio-Director de la firma Auren, habiendo desarrollado su carrera profesional en implantaciones de sistemas de gobierno TI y de gestión en corporaciones multinacionales. Además, es catedrático en Inttelmex en México DF.

Julio Ballesteros García

Licenciado en Ciencias Políticas y de la Administración por la Universidad Complutense de Madrid. Certificado ITIL Expert e ITIL approved trainer por APMG. Tiene más de 10 años de experiencia en el sector de las TIC.

Actualmente es consultor senior y líder en la práctica de calidad y gestión de proyectos. Especialista en proyectos de organización, de diseño e implantación de modelos de gobierno y gestión de servicios de TI. Además, es auditor de sistemas de gestión de calidad, ambientales y de seguridad de la información. Miembro de itSMF España. Miembro del AEN/CTN 71/GT25 de AENOR *Gestión y buen gobierno de los servicios de Tecnologías de la Información*. Vocal del comité de calidad de servicios TIC de la AEC.

Antonio Carretero Peña

Doctor e Ingeniero Industrial de la especialidad química por la ETS de Ingenieros Industriales de la Universidad Politécnica de Madrid (UPM). Técnico superior de prevención de riesgos laborales por la CAM en seguridad industrial, higiene en el trabajo y ergonomía/psicosociología laboral.

Posee una amplia experiencia profesional en España y Latinoamérica como auditor de sistemas de gestión ambiental.

En la actualidad, trabaja en novedosas actividades ambientales, energéticas y preventivas desde AENOR como Subdirector de la Dirección de Desarrollo.

Boris Delgado Riss

Ingeniero en Informática por la Universidad Pontificia de Salamanca (UPSAM). Máster en Seguridad y auditoría informática por la Universidad Politécnica de Madrid (UPM). CISA, CISM por ISACA. Certificado en ITIL. Certificado en ISO/IEC 15504 por IntRSA. Tiene más de 10 años de experiencia como consultor y auditor en TIC en España y Latinoamérica.

Desde 2007 es auditor jefe de TIC en AENOR (Desarrollo, Investigación y Certificación en el área de TI de la Dirección de Desarrollo Estratégico). Profesor colaborador del Máster de Seguridad de sistemas de información (UPSAM) y Universidad de Alcalá de Henares (UAH).

Colegiado en el Colegio profesional de ingenieros en informática de Madrid.

Miembro asociado del Chapter Madrid – ISACA.

María Honorina Diez López

Ingeniero de Telecomunicación por la Universidad Politécnica de Madrid (UPM). Postgrado en Dirección integral de seguridad por la Universidad de Vic. Director de seguridad homologado por el Ministerio del Interior. CISA y CRISC por ISACA. MCSA. *Lead* auditor ISO 27001 y 20000-1. Auditor interno ISO 90001. Con más de 10 años de experiencia en TIC como consultor de seguridad y arquitecto de sistemas.

Actualmente, consultor independiente.

Carmen Fernández Prieto

Ingeniero Superior de Telecomunicación por la Universidad Politécnica de Madrid (UPM). CISA por ISACA. Con más de 30 años de experiencia en tecnologías de la información y las comunicaciones, ha desarrollado su carrera profesional en el ámbito de las tecnologías de la información como Directora de Procesos y calidad en Telefónica Soluciones y como Gerente de Planificación y calidad en Telefónica Investigación y Desarrollo.

Actualmente es Socio-Directora en FERCON 3 T.I. Además, es auditor jefe por AENOR en las normas ISO 27001 e ISO 20000-1.

Paloma García López

Ingeniero Industrial por la Universidad Politécnica de Madrid (UPM).

Desde 1999 desarrolla su actividad profesional en AENOR. Ha desempeñado durante 10 años el puesto de Jefe de Telecomunicaciones y Tecnologías de la Información en la Dirección de Normalización, coordinando la actividad de los comités nacionales de normalización de este ámbito y participando activamente en las iniciativas europeas e internacionales del sector, siendo la representante de AENOR en el Instituto Europeo de Normas de Telecomunicación (ETSI) y en el Comité internacional de tecnologías de la información (ISO/IEC JTC1).

Actualmente es la Responsable de desarrollo de nuevos negocios en la Dirección de Normalización.

Javier Garzas Parra

Doctor (Ph.D.) (*cum laude por unanimidad*) e Ingeniero superior en Informática (premio extraordinario). Cursó estudios postdoctorales y fue investigador invitado en la Universidad Carnegie Mellon (Pittsburgh, Pennsylvania, EEUU).

Actualmente trabaja en la empresa Kybele Consulting S.L. (*spin-off* del grupo de investigación de la Universidad Rey Juan Carlos) y es profesor titular en la Universidad Rey Juan Carlos. Auditor jefe por AENOR en SPICE-ISO 15504.

Ha trabajado para más de 40 empresas, en cuatro países, y dispone de más de 80 publicaciones en revistas y conferencias del sector.

Mantiene periódicamente el blog www.javiergarzas.com con noticias sobre el sector.

Emanuel Irrazabal

Doctor e Ingeniero superior en Informática y Máster oficial en Tecnologías de la información y sistemas informáticos (Escuela Superior de Ingeniería Informática – Universidad Rey Juan Carlos). Mención de Calidad MEC. Actualmente se encuentra terminando su tesis doctoral sobre la ingeniería del software basada en valor. Es auditor jefe por AENOR (ISO 15504), CISA (Certified Information Systems Auditor) por la ISACA, y acreditado como tecnólogo por el programa Torres Quevedo.

Desde 2009 es consultor senior en Kybele Consulting, trabajando en varios proyectos en administraciones y empresas tales como Sistemas Técnicos de Loterías (STL), AENOR, Siemens, Neoris, etc. Actualmente es también profesor asociado de la Universidad Rey Juan Carlos y miembro del SC7/GT24 de AENOR.

Pedro Pablo López Bernal

Técnico Informático. Máster Auditoría informática (CENEI). Máster Seguridad global.

CISA por ISACA. Tiene más de 30 años de experiencia en TIC.

Desde 1986 trabaja en Rural Servicios Informáticos. Actualmente es Gerente de seguridad, privacidad y continuidad global.

Forma parte del grupo de seguridad y comisión de seguridad, prevención y fraude del Centro Cooperación Interbancaria (CCI), en representación de la Unión Nacional de Cooperativas Crédito (UNACC), grupo de trabajo pionero en lucha contra el fraude *online* en España, así como del Consorcio Español Continuidad Negocio (CECON), en el que participan entidades financieras, bolsa, valores, seguros, Banco de España, entre, otros; y comités técnicos de normalización de AENOR.

Tesorero y miembro fundador del Nuevo Instituto de Continuidad de Negocio Español (CONTINUAM).

Enrique Martín Menéndez

Ingeniero en Informatica por la Universidad Pontificia de Salamanca en Madrid (UPSAM). Máster de Seguridad por la Universidad Oberta de Cataluña (UOC). CISA, CISM y CRISC por ISACA. Con más de 15 años de experiencia en el sector de las TIC.

Actualmente es Responsable de continuidad de negocio y seguridad IT del Grupo Sanitas.

Marlon Molina Rodríguez

Ingeniero en Informática. Máster en Gestión de la seguridad de la información (Universidad Pontificia de Salamanca en Madrid). MBA por la University of Phoenix. Posgrado en Information systems por la Alabama State University. Certificado como Instructor internacional de ITIL, instructor PRINCE2 y certificado en LeanIT y GreenIT. Tiene 10 años de experiencia como consultor de gestión de servicios de TI y más de 5 años como instructor de tecnologías y proyectos de TI.

Actualmente es Director general de TECNOFOR y Director de publicaciones de itSMF España. Conferenciante, escritor y columnista en diversos medios.

Luis Morán Abad

Ingeniero Industrial e Ingeniero Informático. Certificado ITILv2 Service Manager e ITILv3 Expert. Con más de 25 años de experiencia, ha desarrollado su carrera

profesional en el ámbito de las tecnologías de la información en los sectores de telecomunicaciones, financiero y energético.

Actualmente es Gerente de Gestión de la producción de Telefónica Global Technologies.

Desde 2010 es Vicepresidente de itSMF España.

Hanna Oktaba

Es profesora de la Universidad Nacional Autónoma de México en Ingeniería de software. Ha dirigido proyectos del modelo de procesos para las pequeñas organizaciones de software MoProSoft, modelo de evaluación EvalProSoft y pruebas controladas, apoyados por PROSOFT de la Secretaría de Economía, cuyo resultado fue la creación de la norma mexicana MNX-I-059-NYCE-2005. Es representante de México en el ISO JTC1/SC7 *Software and System Engeeniring*. Ha sido coeditora de las partes 4-1 y 5-1-2 de la Norma ISO/IEC 29110.

Orlando Pereda Soriano

Doctor y licenciado en Informática por la Universidad Politécnica de Madrid (UPM). Es miembro de ISACA y del Comité Técnico de Normalización CTN71/SC7/GT25. Con más de 25 años de experiencia en el sector de las TIC, ha desarrollado su carrera profesional como consultor estratégico en gestión y gobierno TI.

Actualmente dirige el programa de adecuación de los procesos TIC de informática del Corte Inglés, siendo el Coordinador de su sistema integrado de gestión, habiéndolo certificado acorde a las normas ISO/IEC 20000-1, ISO 9001 e ISO/IEC 27001.

Además es Director del Comité de estándares y modelos de referencia de itSMF España, y coordinador del grupo de trabajo de difusión ISO 20000.

Cristo Manuel Pérez Rosquete

Ingeniero superior en Informática y Máster en Seguridad informática por la Universidad Politécnica de Madrid (UPM). CISA, CISM y CRISC por ISACA. Tiene más de 15 años de experiencia en el sector de las TIC.

Ha desarrollado su carrera profesional en el área de la seguridad, desempeñando cargos de Gerente de Seguridad informática y Jefe de Control de fraude y riesgos.

Actualmente forma parte del área de seguridad informática de Sanitas Seguros, siendo el responsable de la plataforma de gestión de identidades y control de acceso y está a cargo del SGSI de la gestión y administración de la seguridad de los sistemas de información de Sanitas Seguros y del SGCN del Grupo Sanitas.

Alejandro Pérez Sánchez

Máster en Dirección informática. CISA por ISACA, certificado ISO/IEC 20000, ITIL Service Manager e ITIL Expert. Especialista TI con más 30 años de experiencia en el sector TIC.

Desde 2004 desempeña su actividad profesional en Telefónica Global Technology, donde ha estado involucrado en diferentes iniciativas corporativas del Grupo Telefónica, impulsando las mejores prácticas de gestión y buen gobierno de TI.

Coordinador del SC7/GT25 de AENOR *Gestión y buen gobierno de los servicios de TI*, que participa en la evolución de las normas internacionales ISO/IEC 20000 e ISO/IEC 38500.

Socio fundador de itSMF España y socio senior de ATI.

Francisco J. Pino Correa

Doctor Ingeniero en Informática por la Universidad de Castilla-La Mancha (España), Especialista en Redes y servicios telemáticos e Ingeniero en Electrónica y telecomunicaciones por la Universidad del Cauca (Colombia). Profesor titular adscrito a la Facultad de Ingeniería electrónica y telecomunicaciones de la Universidad del Cauca. Miembro del Grupo IDIS (Investigación y desarrollo en ingeniería del software) de la Universidad del Cauca y del Grupo ALARCOS de la Universidad Castilla-La Mancha. Auditor jefe por AENOR en SPICE-ISO 15504.

Socio fundador de la empresa Kybele Consulting Colombia, S.A.S. dedicada a la consultoría en calidad de software.

Moisés Rodríguez Monje

Ingeniero Superior en Informática por la Universidad de Castilla-La Mancha y CISA por ISACA. Auditor jefe por AENOR (ISO 15504), ScrumManager Certified y Foundation Certificate en TMAP Next.

Ha trabajado como consultor para numerosas empresas y administraciones, y actualmente es CTO de Alarcos Quality Center, *spin-off* de la UCLM orientada a prestar servicios para la mejora de la calidad del software. En el ámbito investigador, destacan varias publicaciones en libros, revistas y congresos, relacionadas con la seguridad y el aseguramiento de la calidad software. Ha dirigido varios proyectos de I+D y desde 2008 es miembro del SC7/GT26 de AENOR.

Francisco Ruiz González

Doctor Ingeniero en Informática y Licenciado en Ciencias Químicas. Catedrático en la Universidad de Castilla-La Mancha (UCLM). Ha sido Director de la Escuela Superior de Informática de Ciudad Real y de los Servicios informáticos de la UCLM. Ha trabajado de analista-programador y jefe de proyectos en varias compañías privadas. Actualmente trabaja en *software development business frameworks*, integrando: arquitectura de empresa (TOGAF, Zachman), orientación a servicios (SOaML), modelado del negocio (Archimate, BMM), mejora de procesos de negocio (BPM, BPMN), ingeniería de métodos (SPEM) y planificación de proyectos software. Es miembro de ACM, IEEE-CS, ATI, SISTEDES, AEC, EASST, AENUI y ACTA.

René Salinas

Ingeniero en Computación por la Universidad Nacional Autónoma de México (UNAM). Maestría de la Universidad Iberoamericana en Administración de servicios de TI. Certificación como Project Management Professional por PMI, certificado en Certified Business Continuity Professional.

Tiene más de 20 años de experiencia profesional en TIC, concretamente en seguridad de la información, sector financiero y consultoría de sistemas.

Actualmente es Director de Sistemas-CIO de Buró de Crédito.

Javier Tuya González

Ingeniero y Doctor por la Universidad de Oviedo. Certificado TMap Next Foundations. Actualmente ocupa el puesto de Catedrático de Universidad en el Departamento de Informática. Ha sido Responsable de los Servicios de informática de la universidad, y ha dirigido múltiples proyectos de investigación y transferencia tecnológica, así como publicado en diferentes conferencias y revistas internacionales. Actualmente es Director de la Cátedra Indra-Universidad de Oviedo y miembro del grupo de trabajo de ISO JTC1/SC7/WG26 *Software Testing* que trabaja en la elaboración de la nueva norma ISO/IEC 29119. Asimismo, es el coordinador actual del correspondiente grupo de trabajo AEN/CTN 71/SC7/GT26 de AENOR.

Javier Verdugo Lara

Ingeniero superior en Informática por la Universidad de Castilla-La Mancha. Consultor en materia de mejora de la calidad del software.

Comenzó su carrera profesional en el ámbito de la investigación dentro del grupo Alarcos, perteneciente a la Universidad de Castilla-La Mancha. Se especializó en temas

relacionados con la ingeniería del software, modelos de procesos software, modelos de mejora de procesos, pruebas del software y calidad del producto software.

Desde 2008 es consultor de Alarcos Quality Center, *spin-off* de la Universidad de Castilla-La Mancha orientada a prestar servicios de consultoría para la mejora de la calidad del software y del proceso de pruebas.

Manuel Viscasillas Ramírez

Máster Oficial (EEES) en Ciencia y Tecnología Informática por la Universidad Carlos III de Madrid. Postgrado en Informática por la Universidad de Zaragoza. CISA y CISM por ISACA. Titulado superior militar. Diplomado en Informática militar. Con más de 20 años de experiencia en el sector de las TIC.

Ha desarrollado su actividad en el área de las tecnologías de la información en el sector público, ejército de tierra, donde entre otros puestos fue profesor de Ingeniería del software y seguridad en la Escuela de Informática del ejército de tierra (actualmente en la reserva).

Actualmente es consultor, auditor y gerente del área de tecnologías de la información en la empresa Profolp Consultores S.L. Además, es auditor jefe por AENOR en las normas ISO 27001, ISO 20000-1 e ISO 15504.

Publicaciones

Gestión energética

Pack Eficiencia energética

+ **Libro** "Gestión de la eficiencia energética: cálculo del consumo, indicadores y mejora"
+ **Normas** UNE-EN ISO 50001 y UNE 216501
+ **Hojas de cálculo** de los ejemplos sectoriales
+ **Vídeo y reportaje** de los autores

2012 • Rústica + CD-ROM • 65 €

Gestión de la eficiencia energética: cálculo del consumo, indicadores y mejora

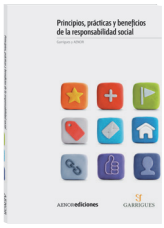
2012 • 216 págs. • 20,95 €
Ebook • 14,95 €

Responsabilidad social

Pack Responsabilidad social

+ **Libro** "Principios, prácticas y beneficios de la responsabilidad social"
+ **Norma** UNE-ISO 26000:2012 "Guía de responsabilidad social"
+ Otros **documentos** de interés sobre RS

2012 • Rústica + CD-ROM • 60 €



Principios, prácticas y beneficios de la responsabilidad social

2012 • 136 págs. • 20,80 €
Ebook • 9,95 €

TIC

Modelo para el gobierno de las TIC basado en las normas ISO

2012 • 434 págs. • 24,96 €
Ebook • 12 €

Gestión y calidad

Aspectos clave de la integración de sistemas de gestión

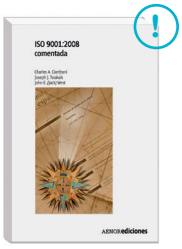
2012 • 214 págs. • 19,95 €
Ebook • 9,95 €

Factores que contribuyen al éxito de una auditoría integrada

2011 • 240 págs. • 34 €

Configuración y usos de un mapa de procesos

2012 • 156 págs. • 24 €
Ebook • 12 €



ISO 9001:2008 comentada

2009 • 292 págs. • 31,20 €

ISO 9000 Las preguntas del auditor

2.ª edición

2009 • 170 págs. • 26 €

Después de la certificación ISO 9001

2.ª edición

2010 • 122 págs. • 20,80 €

ISO 9001:2008 comentada + ISO 9000 Las preguntas del auditor + Después de la certificación ISO 9001 60 €

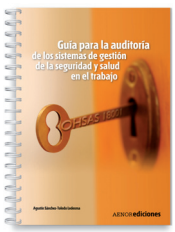
Seguridad y salud en el trabajo

Modelo de empresa saludable. Healthy workplace model

2012 • 84 págs. • 10,04 €
Ebook • 7,26 €

Cómo implantar con éxito OHSAS 18001

2008 • 344 págs. • 25 €



Guía para la auditoría de los sistemas de gestión de la seguridad y salud en el trabajo. OHSAS 18001

2008 • 128 págs. • 31,20 €

OHSAS 18001:2007 Sistemas de gestión de la seguridad y salud en el trabajo

2007 • 46 págs. • 23,50 €
PDF • 26,67 €

OHSAS 18002:2008 Sistemas de gestión de la seguridad y salud en el trabajo. Directrices para la implementación de OHSAS 18001:2007

2009 • 116 págs. • 31,20 €
PDF • 35,40 €

Gestión de la seguridad y salud en el trabajo según OHSAS 18001. Actitudes y percepciones de empresas certificadas

2010 • 160 págs. • 31,50 €

OHSAS 18001 + OHSAS 18002 en soporte impreso **46,49 €**

AENORmás
NORMAS AL DÍA

Una solución a medida para la gestión de sus **Normas UNE**

¿Qué es?

Una solución on-line que le permite disponer del texto completo de las normas UNE seleccionadas por usted, mantenerlas siempre actualizadas y consultarlas a cualquier hora del día, todos los días del año y con total seguridad.

¿Qué le ofrece?

1 Elegir las normas de su interés
Diseñe sus colecciones personalizadas eligiendo entre 25 000 normas o seleccione una de las ya diseñadas por nuestros expertos.

2 Estar informado puntualmente
Tendrá la seguridad de tener la última versión de las normas UNE incluidas en su colección. Un sistema de alertas le mantendrá siempre al día de las novedades.

3 Optimizar su tiempo
Nosotros le realizamos la búsqueda de cualquier cambio que se produzca en el estado de sus normas, hacemos el seguimiento por usted.

4 Garantizarle el cumplimiento de requisitos
Le ayudamos a cumplir los requisitos de sus productos y servicios tanto legales como los exigidos por los sistemas de gestión.

5 Ahorrarle costes
Con la tarifa plana obtendrá precios ventajosos frente a la compra unitaria.

6 Un equipo técnico a su servicio
Dispondrá de un equipo de asesores que le ayudarán a diseñar su colección personalizada de normas UNE.

7 Una herramienta en constante evolución
AENORMÁS es una solución dinámica que incorporará mejoras para adaptarse a sus necesidades y al entorno tecnológico.

AENORmás
NORMAS AL DÍA

www.aenor.es - info@aenor.es - 902 102 201

Realice la visita guiada en AENORMÁS y empiece a crear su colección de normas UNE

AENORmás
NORMAS AL DÍA

Una solución a medida para la gestión de sus Normas UNE

Colección de normas UNE "Modelo de gobierno TIC" Oferta especial

Norma	Título
UNE-EN ISO 9000:2005	Sistemas de gestión de la calidad. Fundamentos y vocabulario. *(ISO 9000:2005)*
UNE-EN ISO 9001:2008	Sistemas de gestión de la calidad. Requisitos. *(ISO 9001:2008)*
UNE-EN ISO 9001:2008/AC:2009	Sistemas de gestión de la calidad. Requisitos. *(ISO 9001:2008/Cor 1:2009)*
UNE 66177:2005	Sistemas de gestión. Guía para la integración de los sistemas de gestión
UNE-EN ISO 14001:2004	Sistemas de gestión ambiental. Requisitos con orientación para su uso. *(ISO 14001:2004)*
UNE-EN ISO 14001:2004/AC:2009	Sistemas de gestión ambiental. Requisitos con orientación para su uso. *(ISO 14001:2004/Cor 1:2009)*
UNE-EN ISO 19011:2012	Directrices para la auditoría de los sistemas de gestión. *(ISO 19011:2011)*
UNE 66172:2003 IN	Directrices para la justificación y desarrollo de normas de sistemas de gestión.
UNE-EN ISO/IEC 17021:2011	Evaluación de la conformidad. Requisitos para los organismos que realizan la auditoría y la certificación de sistemas de gestión. *(ISO/IEC 17021:2011)*
UNE-EN ISO/IEC 17000:2004	Evaluación de la conformidad. Vocabulario y principios generales *(ISO/IEC 17000:2004)*
UNE-EN ISO/IEC 17000:2004 ERRATUM:2005	Evaluación de la conformidad. Vocabulario y principios generales *(ISO/IEC 17000:2004)*
UNE-EN ISO/IEC 17025:2005	Evaluación de la conformidad. Requisitos generales para la competencia de los laboratorios de ensayo y de calibración.
UNE-EN ISO/IEC 17025:2005 ERRATUM:2006	Evaluación de la conformidad. Requisitos generales para la competencia de los laboratorios de ensayo y de calibración. *(ISO/IEC 17025:2005/Cor. 1:2006)*
UNE 71599-1:2010	Gestión de la continuidad del negocio. Parte 1: Código de práctica.
UNE 71599-2:2010	Gestión de la continuidad del negocio. Parte 2: Especificaciones.
UNE-ISO 31000:2010	Gestión del riesgo. Principios y directrices.
UNE-EN 31010:2011*(PAG.COLOR)*	Gestión del riesgo. Técnicas de apreciación del riesgo.
UNE-ISO GUIA 73:2010 IN	Gestión del riesgo. Vocabulario.
UNE-ISO 15489-1:2006	Información y documentación. Gestión de documentos. Parte 1: Generalidades.
UNE-ISO/TR 15489-2:2006	Información y documentación. Gestión de documentos. Parte 2: Directrices. *(ISO/TR 15489-2:2001)*
UNE-ISO 30300:2011 *(PÁG. COLOR)*	Información y documentación. Sistemas de gestión para los documentos. Fundamentos y vocabulario.
UNE-ISO 30301:2011 *(PÁG. COLOR)*	Información y documentación. Sistemas de gestión para los documentos. Requisitos.
UNE-EN ISO 27799:2010 *(PAG.COLOR)*	Informática sanitaria. Gestión de la seguridad de la información en sanidad utilizando la Norma ISO/IEC 27002 *(ISO 27799:2008)*
UNE-ISO/IEC 15939:2009	Ingeniería del software y sistemas. Procesos de medición *(ISO/IEC 15939: 2007)*
UNE-ISO/IEC 9126-1:2004	Ingeniería del software. Calidad del producto software. Parte 1: Modelo de calidad
UNE-ISO/IEC 90003:2005	Ingeniería del software. Guía de aplicación de la ISO 9001:2000 al software
UNE-ISO/IEC 14598-1:2004	Tecnología de la información. Evaluación del producto software. Parte 1: Visión general

Colección de normas UNE "Modelo de gobierno TIC"
Oferta especial

Norma	Título
UNE-ISO/IEC 14598-2:2004	Tecnología de la información. Evaluación del producto software. Parte 2: Planificación y gestión
UNE-ISO/IEC 14598-3:2005	Tecnología de la información. Evaluación del producto software. Parte 3: Procedimiento para desarrolladores.
UNE-ISO/IEC 14598-4:2006	Tecnología de la información. Evaluación del producto software. Parte 4: Procedimiento para compradores (ISO/IEC 14598-4:1999)
UNE-ISO/IEC 14598-5:2006	Tecnología de la Información. Evaluación del producto software. Parte 5: Procedimiento para evaluadores (ISO/IEC 14598-5:1998)
UNE-ISO/IEC 19770-1:2008	Tecnología de la Información. Gestión de activos de software (SAM). Parte 1: Procesos.
UNE-ISO/IEC 20000-1:2007/1M:2009	Tecnología de la información. Gestión del servicio. Parte 1: Especificaciones.
UNE-ISO/IEC 20000-1:2007	Tecnología de la información. Gestión del servicio. Parte 1: Especificaciones. (ISO/IEC 20000-1:2005)
UNE-ISO/IEC 20000-1:2011	Tecnología de la información. Gestión del Servicio. Parte 1: Requisitos del Sistema de Gestión del Servicio (SGS).
UNE-ISO/IEC 20000-2:2007	Tecnología de la información. Gestión del servicio. Parte 2: Código de buenas prácticas. (ISO/IEC 20000-2:2005)
UNE-ISO/IEC TR 20000-3:2011 IN	Tecnología de la información. Gestión del servicio. Parte 3: Directrices para la definición del alcance y aplicabilidad de la Norma ISO/IEC 20000-1:2005.
UNE-ISO/IEC 14598-6:2007	Tecnología de la información. Ingeniería del software. Evaluación del producto software. Parte 6: Documentación de los módulos de evaluación. (ISO/IEC 14598-6:2001)
UNE-ISO/IEC 27002:2009	Tecnología de la Información. Técnicas de seguridad. Código de buenas prácticas para la gestión de la seguridad de la información
UNE-ISO/IEC 27001:2007/1M:2009	Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos.
UNE-ISO/IEC 27001:2007	Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos. (ISO/IEC 27001:2005)

Modalidades de suscripción

- **Colección de normas UNE + Actualización automática del documento**
  El servicio AENORMÁS le permite disponer en un espacio único de las normas de la colección contratada y, además, se irán incorporando de forma automática los textos de las nuevas versiones de sus normas y sus modificaciones.