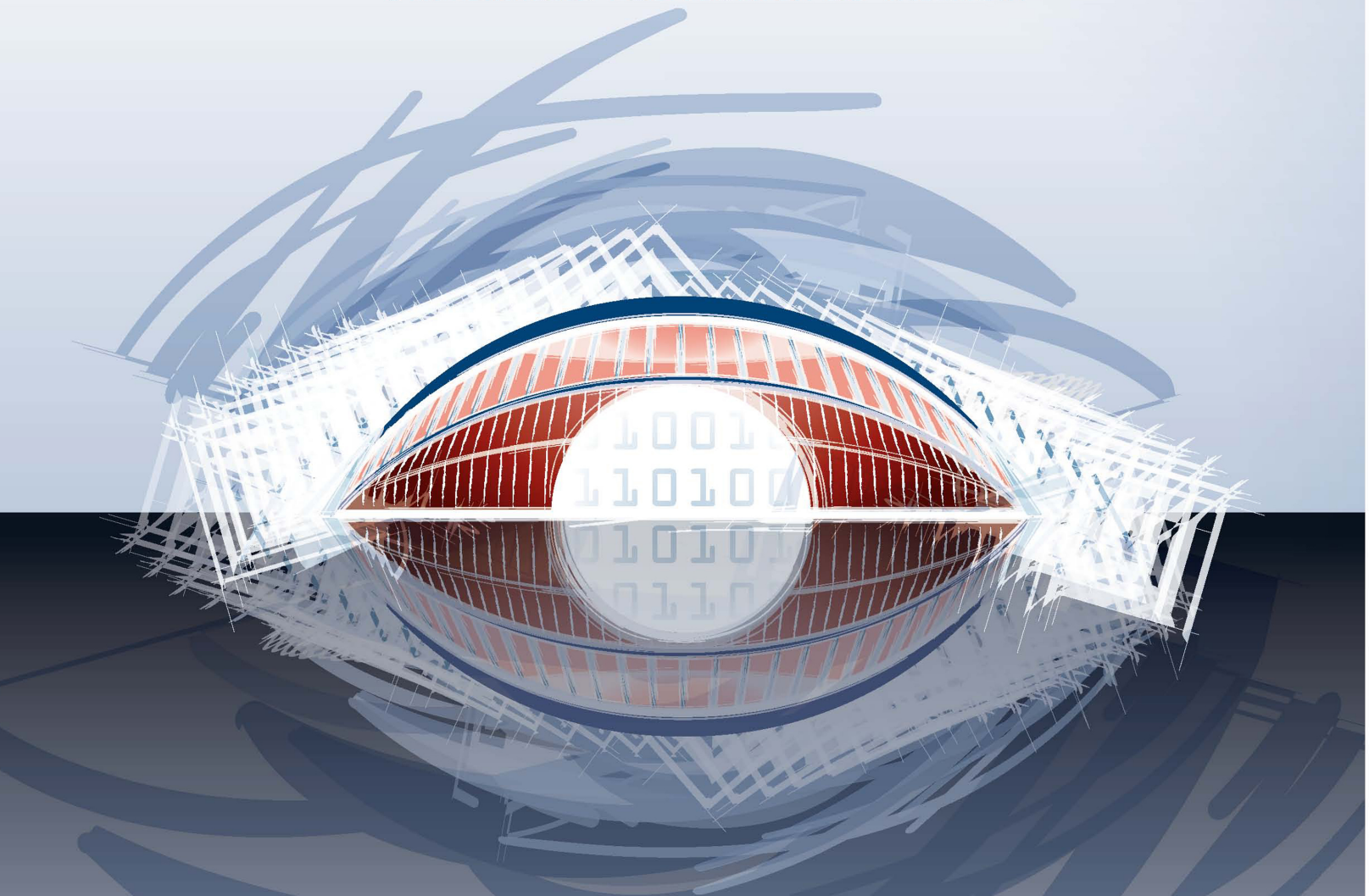
Garceta
grupo editorial

CEDI 2010 VALENCIA

7 A 10 DE SEPTIEMBRE DE 2010

III CONGRESO ESPAÑOL DE INFORMÁTICA

UNIVERSIDAD POLITÉCNICA DE VALENCIA



Actas de las XV Jornadas de Ingeniería del Software y Bases de Datos

| JISBD2010 | (SISTEDES)

EDITORES
Ernest Teniente, Silvia Abrahão

Nuevos retos científicos y tecnológicos en Ingeniería Informática

ACTAS DE LAS XV JORNADAS DE INGENIERÍA DEL SOFTWARE Y BASES DE DATOS

EDITORES
Ernest Teniente
Silvia Abrahão

PATROCINAN

ACTAS DE LAS XV JORNADAS DE INGENIERÍA DEL SOFTWARE Y BASES DE DATOS (JISBD 2010)

Editores: Ernest Teniente y Silvia Abrahão

ISBN: 978-84-92812-51-6
IBERGARCETA PUBLICACIONES, S.L., Madrid, 2010

Edición: 1ª
Impresión: 1ª
Nº de páginas: 374
Formato: 17 x 24
Materia CDU: 004 Ciencia y tecnología de los ordenadores. Informática

1ª Edición, 1ª Impresión

ISBN: 978-84-92812-51-6

Depósito legal: M-

Maquetación: Los Editores

Coordinación del proyecto: @LIBROTEX

Portada: Estudio Dixi

Impresión y encuadernación:

OI: 14/2010

PRINT HOUSE, S.A.

IMPRESO EN ESPAÑA -PRINTED IN SPAIN

Comité Ejecutivo

Presidente del Comité de Programa:
Ernest Teniente (Univ. Politècnica de Catalunya)

Presidenta del Comité Organizador y relaciones con CEDI 2010:
Silvia Abrahão (Univ. Politécnica de Valencia)

Coordinador de Talleres:
Juan Trujillo (Univ. de Alicante)

Coordinador de Demostraciones:
Alfredo Goñi (Univ. del País Vasco)

Coordinador de Tutoriales:
Vicente Pelechano (Univ. Politécnica de Valencia)

Coordinadora de Divulgación de Trabajos Relevantes ya Publicados:
Ana M. Moreno (Univ. Politécnica de Madrid)

Coordinador de Publicidad:
David Benavides (Univ. de Sevilla)

Coordinador de Actas:
Emilio Insfrán (Univ. Politécnica de Valencia)

Coordinador de la Web:
José Ángel Carsí (Univ. Politécnica de Valencia)

Comité Organizador (Univ. Politécnica de Valencia)

Abrahao, Silvia
Blanes, David
Canós, José Hilario
Carsí, José Ángel
Costa, Cristóbal
Fernández, Adrián
Gómez, Abel
González, Javier
Insfran, Emilio
Letelier, Patricio
Llavador, Manuel
Marante, María Isabel
Montagud, Sonia
Montero, Emanuel
Penadés, Ma. Carmen
Rodriguez, Lorena

Actas de las JISBD 2010, pp. III-V, ISBN: 978-84-92812-51-6

Comité de Programa

Aldana, José (Univ. de Málaga)
Álvarez, Bárbara (Univ. Polit. Cartagena)
Aramburu, María José (Univ. Jaume I)
Araujo, Joao (Univ. Nova Lisboa)
Barrena, Manuel (Univ. de Extremadura)
Berlanga, Rafael (Univ. Jaume I)
Boronat, Artur (Univ. de Leicester)
Botella, Pere (Univ. Polit. Catalunya)
Brisaboa, Nieves (Univ. A. Coruña)
Cabot, Jordi (Univ. Oberta Catalunya)
Cachero, Cristina (Univ. Alicante)
Calero, Coral (Univ. Castilla-La Mancha)
Canós, Hilario (Univ. Polit. Valencia)
Cavero, José (Univ. Rey Juan Carlos)
Corchuelo, Rafael (Univ. Sevilla)
Costal, Dolors (Univ. Polit. Catalunya)
Crespo, Yania (Univ. Valladolid)
De la Fuente, Pablo (Univ. Valladolid)
Dieste, Oscar (Univ. Polit. Madrid)
Falcão e Cunha, João (Univ. Porto)
Farré, Carles (Univ. Polit. Catalunya)
Fdez-Bertoa, Manuel (Univ. Málaga)
Fdez-Medina, Eduardo (Univ. Castilla-La Mancha)
Fons, Joan (Univ. Polit. de Valencia)
Franch, Xavier (Univ. Polit. Catalunya)
Garbajosa, Juan (Univ. Polit. Madrid)
García Molina, Jesús (Univ. Murcia)
Garrigós, Irene (Univ. de Alicante)
Genero, Marcela (Univ. Castilla-La Mancha)
Génova, Gonzalo (Univ. Carlos III)
Gómez, Jaime (Univ. Alicante)
Guerra, Esther (Univ. Carlos III)
Hernández, Juan (Univ. Extremadura)
Illarramendi, Arantza (Univ. País Vasco)
Irastorza, Arantza (Univ. País Vasco)
Iribarne, Luis (Univ. Almeria)
Iturrioz, Jon (Univ. País Vasco)
Juristo, Natalia (Univ. Polit. Madrid)
Laguna, Miguel A. (Univ. Valladolid)
Lara, Juan de (Univ. Aut. Madrid)
Lopes, Antonia (Univ. Lisboa)
Luque, Vicente (Univ. Carlos III)
Marcos, Esperanza (Univ. Rey Juan Carlos)
Mazón, José Norberto (Univ. Alicante)
Mena, Eduardo (Univ. Zaragoza)
Moreira, Ana (Univ. Nova Lisboa)
Moreno, Juan José (Univ. Polit. Madrid)
Murillo, Juan (Univ. Extremadura)
Paramá, José Ramón (Univ. Coruña)
Pastor, Oscar (Univ. Polit. Valencia)
Piattini, Mario (Univ. Castilla-La Mancha)
Pimentel, Ernesto (Univ. Málaga)
Polo, Antonio (Univ. Extremadura)
Quer, Carme (Univ. Polit. Catalunya)
Ramos, Isidro (Univ. Polit. Valencia)
Riquelme, José (Univ. Sevilla)
Rito, Antonio (Univ. Tec. Lisboa)
Roda, José Luis (Univ. La Laguna)
Romero, José Raúl (Univ. Córdoba)
Ruíz, Francisco (Univ. Castilla-La Mancha)
Ruíz-Cortés, Antonio (Univ. Sevilla)
Sagardui, Goiuria (Univ. Mondragón)
Samos, José (Univ. Granada)
Sánchez, Juan (Univ. Polit. Valencia)
Sánchez, Víctor (Open Canarias)
Toro, Miguel (Univ. de Sevilla)
Toval, Ambrosio (Univ. Murcia)
Trujillo, Salvador (IKERLAN)
Tuya, Javier (Univ. Oviedo)
Urpí, Toni (Univ. Polit. Catalunya)
Vallecillo, Antonio (Univ. Málaga)
Vela, Belén (Univ. Rey Juan Carlos)
Vicente, Cristina (Univ. Polit. Cartagena)

Revisores Adicionales

David Ameller
Maider Azanza
Beatriz Bernárdez
Mª José Casany
Pedro J. Clemente
Jordi Conesa
Antonio Fariña
Jorge García
Abel Gómez
Manuel Llavador
Esperanza Manso
Jorge Martínez Gil
Ana Moreno
Susana Muñoz Hernández
Marc Oriol
Oscar Pedreira
Beatriz Pontes
Manuel Resinas
Esteban Robles Luna
Sergio Segura
Juan Manuel Vara
Sira Vegas

Conferencia Auspiciada por

Prólogo

Las XV Jornadas de Ingeniería del Software y Bases de Datos (JISBD) se celebraron en Valencia del 7 al 10 de Septiembre de 2010, en el marco del III Congreso Español de Informática (CEDI 2010). El objetivo principal de estas Jornadas fue el de debatir e intercambiar ideas, compartir experiencias y divulgar resultados, estableciendo, además, un marco propicio de colaboración entre los distintos sectores y grupos de trabajo de las áreas de ingeniería del software y de las bases de datos en la península ibérica. Las JISBD están organizadas bajo los auspicios de SISTEDES, la Sociedad de Ingeniería del Software y Tecnologías de Desarrollo de Software.

Las JISBD 2010 incluyeron tres tipos distintos de contribuciones: artículos de investigación originales, artículos ya publicados y demostraciones de herramientas. Los primeros describían resultados de investigación o experiencias industriales relativas a los campos de la ingeniería del software y de las bases de datos. En total se recibieron 37 artículos. Todos ellos fueron revisados por cuatro miembros del Comité de Programa siguiendo un sistema de revisión por pares. Finalmente, 21 de estos artículos fueron aceptados para su presentación en las Jornadas. Además, 2 artículos fueron seleccionados para participar en la conferencia como artículos cortos. Nos gustaría expresar desde aquí nuestro agradecimiento a todos los miembros del Comité de Programa por dedicar parte de su precioso tiempo revisando los artículos y proporcionando valiosos comentarios y valoraciones que han sido muy útiles durante el proceso de selección. Por supuesto, también queremos agradecer a todos los autores que enviaron artículos a las Jornadas por el esfuerzo realizado y por su interés en el evento. También merece la pena mencionar a EasyChair, el sistema de revisión de artículos que hemos utilizado, y que tan buenos resultados nos ha proporcionado.

Además de los artículos originales, las JISBD 2010 incluyeron 18 artículos ya publicados y 7 demostraciones de herramientas. El objetivo de la divulgación de trabajos ya publicados en fuentes de prestigio es, por una parte, dar a conocer dichas investigaciones en nuestro propio entorno, y por otra, contribuir a estimular a nuestros investigadores emergentes hacia este tipo de publicaciones. El número de artículos seleccionados supone un récord en las cuatro ediciones de las JISBD en las que se ha solicitado este tipo de contribución y es una demostración palpable de la madurez y del reconocimiento de la comunidad JISBD a nivel internacional. Las demostraciones de herramientas son el camino elegido por las JISBD para demostrar la viabilidad práctica de las propuestas teóricas y metodológicas formuladas por los equipos de investigación. Es de vital importancia insistir en la relevancia y utilidad de este objetivo en aras de conseguir un número más elevado de contribuciones de este tipo en próximas ediciones de las jornadas.

Como en ediciones anteriores, y contando asimismo con una importante participación e interés, se desarrollaron los Talleres asociados durante el primer día de las jornadas. En esta edición se realizaron un total de 6 talleres que han representado un importante centro de interés para los investigadores que trabajan en algunos temas determinados y que aprovecharon la ocasión para profundizar en estos temas e intentar realizar investigaciones en común con investigadores de otros grupos. Dos de estos talleres (ISELEAR e ADIS) celebraron ya su décima edición lo que supone una muestra de la madurez que han adquirido al largo de los años, DSDM su séptima, PRIS la quinta y los dos más noveles (PNIS y WASELF) realizaban ya su tercera edición. Un agradecimiento muy sincero también para todos los organizadores de los Talleres por la importante tarea que realizaron para asegurar el éxito de los mismos.

En referencia al programa, mencionar también la participación de Gustavo Alonso, investigador español trabajando en el ETH de Zurich (Suiza), conferenciante invitado de reconocido prestigio internacional, que nos ofreció la conferencia “Cloud computing y su impacto en la informática”. Nuestro agradecimiento a Gustavo por su interés y disponibilidad a participar en esta edición de las Jornadas.

El programa de las JISBD 2010 también incluyó dos tutoriales de candente actualidad sobre una aplicación práctica de una arquitectura dirigida por modelos y sobre la incorporación de requisitos de accesibilidad Web en el proceso de desarrollo de software. Es importante destacar que este año se

Actas de las JISBD 2010, pp. IX-X, ISBN: 978-84-92812-51-6 © 2010 Los Autores

recibieron cuatro propuestas muy interesantes de tutoriales aunque dos de ellas tuvieron que quedar fuera por motivos de capacidad organizativa. Muchas gracias a todos los ponentes por sus propuestas y desde aquí animamos a los que no lo pudieron conseguir esta vez a que lo intenten en futuras ocasiones.

Finalmente, y aunque parezca una obviedad, destacar que la organización de un evento de la magnitud de las Jornadas no hubiera sido posible sin la colaboración de un grupo de personas excepcional y que asumieron su responsabilidad con la exigencia que un reto de estas características requería. Nos estamos refiriendo a los otros miembros del Comité Ejecutivo, que como tales se han encargado de impulsar y de coordinar los distintos aspectos que engloban la realización de las Jornadas: Talleres (Juan Carlos Trujillo), Demostraciones (Alfredo Goñi), Tutoriales (Vicente Pelechano), Divulgación de Trabajos Relevantes ya Publicados (Ana M. Moreno), Publicidad (David Benavides), Actas (Emilio Insfrán) y Web (José A. Carsí). Nuestro agradecimiento más sincero a todos ellos por su trabajo. También nuestro agradecimiento especial a todos los miembros del comité de organización local de JISBD por su dedicación y apoyo constante. Su inestimable esfuerzo, muchas veces poco visible, ha facilitado en gran medida la organización de estas Jornadas. Por último, queremos dar las gracias al Comité Permanente de las JISBD por confiar en nosotros para organizar esta quinceava edición de las Jornadas y por el apoyo continuo que nos ha proporcionado. Muchas gracias también a todos los patrocinadores de esta edición: Universidad Politécnica de Valencia (UPV), Departamento de Sistemas Informáticos y Computación de la UPV, la empresa InterSystems, la revista Novática y el Ministerio de Ciencia e Innovación, por su respaldo material en estos tiempos tan difíciles.

Valencia, Septiembre de 2010

Ernest Teniente y Silvia Abrahão (editores)

Tabla de Contenidos

I Conferencia Invitada

II Sesión 1. Desarrollo de Software Dirigido por Modelos

III Sesión 2. Ingeniería de Requisitos

Actas de las JISBD 2010, pp. XI-XVI, ISBN: 978-84-92812-51-6

IV Sesión 3. Cambio y Evolución del Software

V Sesión 4. Ingeniería Web

VI Sesión 5. Recuperación de la Información

VII Sesión 6. Integración de Aplicaciones / Ontologías

VIII Sesión 7. Calidad y Aplicaciones de la Ingeniería del Software

IX Sesión 8. Servicios

X Sesión 9. Validación y Verificación

XI Sesión 10. Miscelánea

XII Tutoriales

XIII Talleres

Armonizando ISO/IEC 20000 e ISO/IEC 27001 para integrar la gestión de servicios y la seguridad de la información

César Pardo,
Francisco J. Pino
Grupo IDIS. Departamento de Ingeniería de Sistemas
Univ. del Cauca, Calle 5 No. 4-70.
Kybele Consulting Colombia
Popayán, Colombia.
cpardo@unicauca.edu.co
fjpino@unicauca.edu.co

Félix García, Mario Piattini
Departamento de Tecnologías y Sistemas de Información
Esc. Superior de Informática
Univ. de Castilla-La Mancha.
13005 Ciudad Real, España.
Felix.Garcia@uclm.es
Mario.Piattini@uclm.es

Javier Rosado
Audisec, Seguridad de la Información S.L, Polígono Industrial Avanzado
Avda. de la ciencia 1
13005 Ciudad Real, España.
jrosado@audisec.es

Resumen

Actualmente con el fin de mantener una política integrada, eficiente y homogénea, los Sistemas de Gestión Integrado (SGI) surgen como una oportunidad para mejorar los procesos relacionados con Tecnologías de la Información (TI) de forma modular, consistente y ordenada en las organizaciones. Las normas ISO 27001 e ISO 20000 proveen buenas prácticas para crear y/o reforzar infraestructuras de gestión orientadas a la seguridad de la información y servicios de las TI. Con el objetivo de ofrecer información de cómo estas normas se encuentran relacionadas y de facilitar su integración bajo un mismo SGI, este artículo presenta la estrategia y resultados de la armonización de las normas ISO 27001 e ISO 20000 en una organización. Asimismo, se realiza un análisis detallado de las semejanzas y diferencias encontradas y se muestran los beneficios alcanzados por la organización.

1. Introducción

En la actualidad existe un amplio abanico de modelos y estándares que pueden ser utilizados por las organizaciones de software para llevar a cabo la mejora y certificación de sus procesos. Por ejemplo CMMI, ISO 9001, ISO 12207, ISO 90003, ITIL, COBIT, entre otros.

Actualmente, se ha incrementado el interés de las organizaciones por obtener la certificación en los estándares definidos por la Organización Internacional para la Estandarización (ISO) relacionados con los entornos de información como medio para mejorar sus distintos departamentos a través de un mismo SGI, ver [1]. Dos de esos entornos son los abordados por los estándares ISO 27001e ISO 20000. Por un lado, el estándar ISO 27001 define una amplia descripción y controles en materia de Seguridad de la Información, y el estándar ISO 20000 define las prácticas y procesos para la gestión de servicios y gestión de TI mediante el uso de un servicio de asistencia basado en ITIL.

Aunque en principio los estándares ISO 27001 e ISO 20000 son distintos y proveen soporte a infraestructuras diferentes de gestión en una organización, creemos que la adopción integrada puede suponer grandes beneficios, entre ellos: mejora de la competitividad, desarrollo de la organización, seguridad, gestión de riesgos, mejora de la gestión a nivel corporativo y garantía para las partes interesadas y mejora continua. Asimismo, incidiría positivamente en la fidelización y captación de nuevos clientes gracias a la garantía que se ofrece en la prestación de servicios que satisfacen sus necesidades y expectativas. Es posible que la integración apropiada de ISO 27001 e ISO 20000 permita generar una sólida y poderosa combinación para la gestión de TI de una organización. Asimismo, fomentar la reutilización de los esfuerzos, tiempo, dinero y talento humano involucrado en proyectos de mejora realizados anteriormente. En la medida que sea posible dicha “reutilización”, las organizaciones, en especial las pequeñas y medianas empresas (PyMEs), se verían seriamente beneficiadas, pues el esfuerzo y los costos asociados para la implementación de un nuevo

Actas de las JISBD 2010, pp. 225-235, ISBN: 978-84-92812-51-6

modelo con respecto a uno ya institucionalizado podrían verse reducidos. El modelo previamente implementado en la organización puede satisfacer parte de los requisitos del nuevo modelo a establecer, un ejemplo de esto son los resultados obtenidos en este trabajo o la comparación y armonización de otros modelos como por ejemplo los "mappings" o mapeos aplicados a ISO 9001:2000 y CMMI [2] y la armonización de ISO 15504 y CMMI [3].

En este sentido, y con el objetivo de intentar guiar a las organizaciones a través de la armonización de las normas ISO 27001 e ISO 20000, en este artículo se presenta una estrategia de armonización utilizada para homogeneizar, comparar y alinear los procesos de la ISO 27001 con los procesos de la ISO 20000. Una estrategia de armonización permite llevar a cabo la armonización de múltiples modelos mediante un conjunto de métodos y técnicas configurados sistemáticamente [4]. Con este trabajo se intenta proporcionar una guía para que las organizaciones relacionadas con los entornos de sistemas de información, gestionen, homogenicen, comparen e integren en un mismo sistema de gestión las normas armonizadas.

Este artículo está estructurado de la siguiente manera: en la sección 2 se presenta un resumen de los trabajos relacionados. La sección 3 presenta en detalle la armonización de los estándares ISO 27001 e ISO 20000 y la estrategia de armonización utilizada. La sección 4 presenta un análisis detallado de las relaciones identificadas entre ISO 27001 e ISO 20000-2. La sección 5 presenta los beneficios alcanzados por la organización. Por último, en la sección 6 se presentan las conclusiones y trabajos futuros.

2. Trabajos relacionados

Con base en los resultados de una revisión sistemática realizada en [5], la cual involucra el análisis de las propuestas para la armonización de múltiples modelos, es posible observar algunos trabajos que muestran un interés en integrar múltiples modelos, en los cuales incluyen algunas normas ISO. Un ejemplo es el proyecto PrIME financiado por el Software Engineering Institute (SEI), el cual estudia el valor de la armonización de múltiples tecnologías, entre ellas: CMMI, Six-Sigma, ITIL, ISO 27001, entre otros [6-8]. Asimismo, se han llevado a cabo estudios que se enfocan hacia el análisis e integración de las normas ISO con otros modelos, algunos de ellos son: análisis e integración de ITIL e ISO 20000 [9], y la definición de Sistemas de Gestión Integrados (SGIs) a partir de: ISO 9001 e ISO 27001 [10], ISO 9001, ISO 20000 e ISO 27001 [11], ISO 9001, ISO 14001 y OHSAS 18000 [12], entre otros.

Otros estudios llevan a cabo la comparación y mapeo entre marcos específicos (entre la misma familia o no más de dos marcos diferentes), por lo general la familia ISO 9001 vs. CMMI [13], CMMI e ISO/IEC TR 15504-2:1998 [14, 15].

Aunque es posible notar un amplio uso de las normas ISO y SEI en los trabajos relacionados, los modelos más usados son los modelos ISO 9001, ISO 15504 y CMMI.

Con relación a la bibliografía existente, y teniendo en cuenta que no se han encontrado estudios donde se analizacen las relaciones y diferencias de las normas ISO 27001 e ISO 20000, en este artículo se presenta la armonización de estas dos normas. Asimismo, este trabajo propone una solución a la necesidad manifestada por Audisec, organización consultora en las normas ISO 27001 e ISO 20000, la cual está interesada en llevar a cabo la implementación de estas dos enfoques bajo un mismo SGI.

3. Armonizando los estándares ISO 27001 e ISO 20000

Esta sección describe la armonización de las normas ISO 27001 e ISO 20000 en términos de las necesidades de armonización identificadas en una organización y la estrategia de armonización seguida. Asimismo, la estrategia de armonización también ha sido posible aplicarla a otros modelos, por ejemplo, ver la homogeneización de ISO 9001:2000 [16] y la armonización de CMMI-DEV e ISO/IEC 15504 [3].

3.1. Necesidades de armonización identificadas

La integración de las normas ISO 27001 e ISO 20000 se llevó a cabo teniendo en cuenta las necesidades establecidas por Audisec, organización que brinda servicios de consultoría y soporte en la certificación de los estándares ISO 20000 e ISO 27001. Las necesidades planteadas

por Audisec para llevar a cabo la armonización de ISO 27001 e ISO 20000 fueron:

- Facilitar la certificación en la norma ISO 20000 a las organizaciones certificadas previamente bajo la norma ISO 27001.
- Reducir costos, tiempo y recursos asociados con la reutilización de esfuerzos empleados previamente en la certificación de ISO 27001.
- Minimizar la complejidad de la aplicación de múltiples estándares sin una debida armonización e integración.

Con base en las anteriores necesidades, el objetivo de armonización de las dos normas estuvo enfocada en definir una estrategia de armonización conformada a partir de un conjunto de técnicas que permitiera llevar a cabo la (i) la solución de las diferencias con relación a sus estructuras, (ii) analizar el nivel de detalle y profundidad de las normas, (iii) comparar e identificar las diferencias y similitudes e (iv) identificar el nivel de cobertura de los procesos de la ISO 27001 sobre los procesos definidos en la ISO 20000. El grado de cobertura se puede definir como la medida que indica cómo una entidad de proceso de un modelo soporta, aborda o tiene relación con la entidad de proceso de otro modelo con el que se compara [3].

3.2. Estrategia de armonización

La gestión del proyecto de armonización de ISO 27001 e ISO 20000 se llevó a cabo con la implementación del proceso para la armonización de múltiples modelos descrito en [17]. El propósito de este proceso es proporcionar una línea guía que facilite la gestión de las tareas relacionadas a la definición y configuración de una estrategia de armonización para llevar a cabo la armonización de múltiples modelos.

Con base en las necesidades de armonización identificadas y la ejecución del proceso de armonización, se definió y configuró una estrategia de armonización teniendo en cuenta dos técnicas para tal fin, las técnicas fueron: una técnica de homogeneización y una técnica de comparación, ver [16] y [3] respectivamente. La Figura 1 muestra un resumen de los procesos aplicados en la armonización de ISO 27001 e ISO 20000-2. El primer proceso es el *proceso de armonización*, en [4] es posible observar un ejemplo de su aplicación con mayor detalle. Con la aplicación del proceso de armonización, el producto de trabajo resultante fue la estrategia para llevar a cabo la armonización de los modelos, la cual es descrita en profundidad en este artículo. Dentro de la estrategia de armonización, el propósito del conjunto de técnicas utilizadas fue el de proveer una guía detallada del "qué hacer" y "cómo" llevar a cabo la armonización de los modelos a través del objetivo de armonización definido. Tanto el proceso como las técnicas de armonización utilizadas hacen parte del Framework para la armonización e integración de múltiples modelos que actualmente estamos desarrollando, el proceso es posible verlo en [17].

La definición y configuración de la estrategia de armonización tuvo en cuenta el análisis y comprensión de las actividades, tareas y roles propuestos por cada técnica. Con base en el análisis realizado, se seleccionaron las entidades de proceso que se consideraron necesarios. La Tabla 1 muestra la estrategia de armonización conformada a partir de la selección de las actividades y tareas definidas por cada técnica. Con el fin de establecer una secuencia de ejecución en las actividades y tareas a desarrollar, se asignó un orden a cada tarea. La Figura 2 muestra la configuración del proceso, roles y actividades de la estrategia de armonización definida. El proceso usa la notación de SPEM 2.0.

3.2.1. Análisis de los modelos

De acuerdo a [18], el propósito de ISO 27001 es ayudar a las organizaciones a establecer, implementar, operar, monitorear, revisar, mantener y mejorar sus Sistemas de Gestión de Seguridad de la Información (SGSI). La implementación de esta norma trae consigo grandes beneficios, entre ellos y más importante es el focalizado en la reducción del riesgo de pérdida de información, robo o corrupción de información.

Por otra parte, de acuerdo a la parte 1 de la norma ISO 20000:20005 [19], el propósito de la serie de familias ISO 20000 es ayudar a las organizaciones a mejorar la eficacia en la prestación de los servicios tecnológicos a través de las directrices para una gestión de servicios de TI de calidad. Así mismo, esta norma tiene en cuenta aspectos con relación a la capacidad del sistema, niveles de gestión cuando el sistema

cambia, asignación de presupuestos financieros y control y distribución del software.

Antes de llevar a cabo la comparación de las dos normas y como se establece en el proceso de la estrategia de armonización (ver Figura 2), fue necesario homogeneizar los modelos a través de la técnica y estructura de entidades de proceso común descritas en [16]. Para llevar a cabo la homogeneización se tuvo en cuenta (i) la información descrita en la parte 1 de ISO 27000 o ISO 27001 y (ii) la parte 2 de ISO 20000 o ISO 20000-2. La parte 2 de ISO 20000 se tuvo en cuenta debido a que en esta sección se describen las buenas prácticas o requisitos en términos de procesos que se deben llevar a cabo para cumplir con la norma.

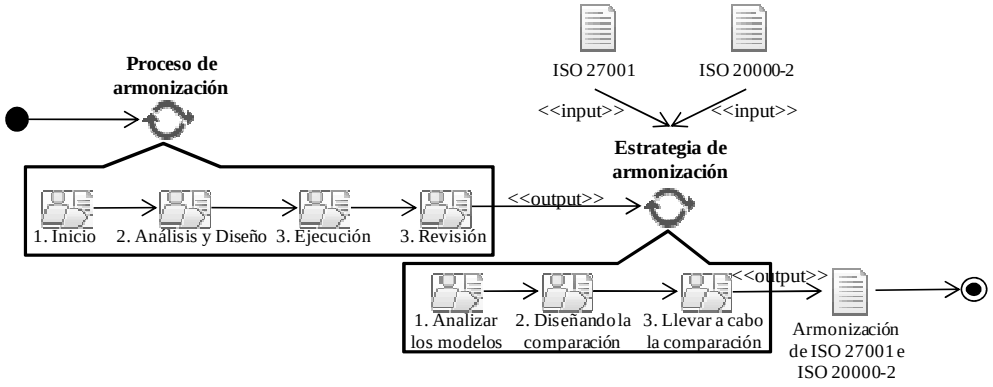


Figura 1. Procesos aplicados en la armonización de ISO 27001 e ISO 20000-2.

Técnicas	Actividades	Tareas	Secuencia
1. Técnica de Homogeneización	*1.1. Análisis de la estructura y terminología*	Adquisición de conocimientos acerca de los modelos a homogeneizar	1.1.1
		Análisis de la estructura de cada modelo	1.1.2
		Análisis de la terminología	1.1.3
	1.2. Identificación de los requisitos de homogeneización	Identificar las entidades de proceso de los modelos que serán homogeneizados	1.2.1
		Establecer un orden que permita priorizar la homogeneización de las entidades de proceso en cada modelo	1.2.2
	1.3. Llevar a cabo la homogeneización (Correspondencia)	*Pre-correspondencia:* establecer la relación entre las entidades de proceso de los modelos y las definidas en la estructura común de homogeneización definida por el proceso	1.3.1
		Correspondencia: llevar a cabo la correspondencia de las entidades de proceso de los modelos en las entidades de proceso de la estructura común.	1.3.2
2. Técnica de Comparación	*2.1. Análisis de los modelos*	Adquisición de conocimientos acerca de los modelos a comparar	(Realizadas en mayor detalle en la homogeneización)
		Analizar la estructura de estos modelos	
	2.2. Diseño de la comparación	Proceso de fijación de las entidades que deben compararse	2.2.1
		Definición de la escala de comparación	2.2.2
		Fijación de la direccionalidad de la comparación	2.2.3
		Definición de una plantilla de comparación	2.2.4
	2.3. Llevar a cabo la comparación	Llevar a cabo un análisis comparativo	2.3.1
		Resolver discrepancias generadas durante la comparación	2.3.2
		Verificar y validar resultados	2.3.3
	2.4. Presentación de los resultados		Homogeneización Comparación
	2.5. Analizar los resultados de la comparación		

Tabla 1. Configuración de la estrategia de armonización

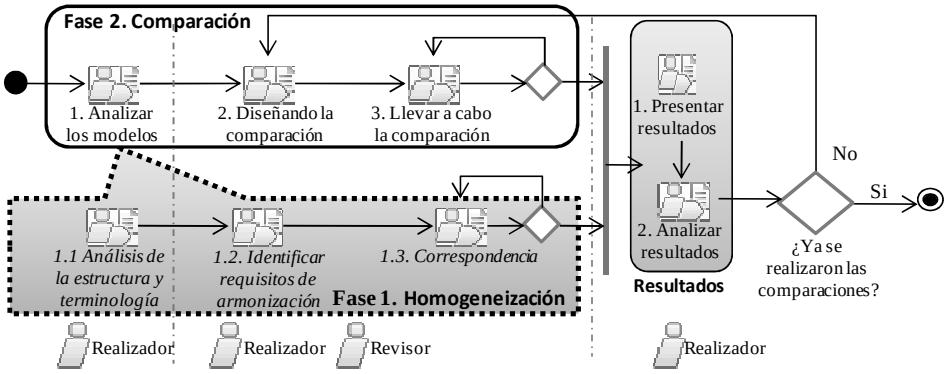


Figura 2. Proceso de la estrategia de armonización

Cláusula 8. Mejora del SGSI				
SD1.1 Grupo de Procesos		5. Mejora del SGSI.		
SD1.2 Procesos	***ID***	Cláusula 8	***Nombre***	Mejora del SGSI.
SD1.3 Actividades		***SD1.4 Tareas***		***S2C.1 Artefactos***
1. La cláusula 8.1 hace referencia a la Mejora continua.		1. La organización debe mejorar de manera continua la eficacia del SGSI, mediante el uso de la política y de los objetivos de seguridad de la información, de los resultados de las auditorías, del análisis de la monitorización de eventos, de las acciones correctivas y preventivas y de las revisiones de la Dirección.		1. En la cláusula 8.2 se indica el procedimiento documentado para las acciones correctivas. Este debe definir los requisitos para: a. Identificar las no conformidades; b. Determinar las causas de las no conformidades; c. Evaluar la necesidad de adoptar acciones para asegurarse de que las no conformidades no vuelvan a producirse; d. Determinar e implantar las acciones correctivas necesarias; e. Registrar los resultados de las acciones realizadas; f. Revisar las acciones correctivas realizadas. 2. En la cláusula 8.3 se indica el procedimiento documentado para las acciones preventivas. Este debe definir los requisitos para: a. Identificar las posibles no conformidades y sus causas; b. Evaluar la necesidad de adoptar acciones para prevenir la ocurrencia de no conformidades; c. Determinar e implementar las acciones preventivas necesarias; d. Registrar los resultados de las acciones adoptadas; y, e. Revisar las acciones preventivas adoptadas.
2. La cláusula 8.2 hace referencia a la Acción correctiva.		1. La organización debe realizar acciones para eliminar la causa de las no conformidades con los requisitos del SGSI, a fin de evitar que vuelvan a producirse.		
3. La cláusula 8.3 hace referencia a la Acción preventiva.		1. La organización debe determinar las acciones necesarias para eliminar la causa de las posibles no conformidades con los requisitos del SGSI, para evitar que éstas vuelvan a producirse. Las acciones preventivas adoptadas deben ser apropiadas en relación a los efectos de los problemas. 2. La organización debe identificar los cambios en los riesgos, así como los requisitos de las acciones preventivas, centrando la atención en los riesgos que hayan sufrido cambios significativos. 3. La prioridad de las acciones preventivas debe determinarse basándose en los resultados de la evaluación de riesgos.		
S3IA.1 Procesos Relacionados		El Sistema de Gestión de la Seguridad de la Información de ISO 27001 puede relacionar cláusulas de sí misma o de otras. Las relaciones existentes son las siguientes: La cláusula 8.1 se relaciona con la cláusula 7 y la cláusula 8.2 y 8.3 se relacionan con la cláusula 4.3.3.		

Tabla 2. Homogeneización de la cláusula 8 de la Norma ISO 27001

La organización de las descripciones de cada una de las normas en la estructura común, permitió comparar las normas a un alto nivel de abstracción con relación a las entidades de proceso definidos en la estructura de homogeneización. Las entidades de proceso identificadas fueron las mismas para las dos normas. Si bien, la estructura común originalmente propone cuatro secciones de entidades de proceso (ver [16]), ésta fue adaptada excluyendo la sección de roles y recursos por no aparecer en las dos normas, identificándose así las siguientes entidades de proceso: grupo de procesos, procesos, actividades, tareas, artefactos y procesos relacionados.

La tabla 2 muestra un ejemplo de la correspondencia final de la descripción de la cláusula 8 de la norma ISO 27001 correspondiente a la mejora del Sistema de Gestión de la Seguridad de la Información. La homogeneización de las cláusulas en cada norma se realizó de forma

iterativa incremental, (ver proceso de la estrategia de armonización en la Figura 2).

3.2.2. Diseño de la comparación

La comparación se enfocó en la realización de un análisis comparativo desde el punto de vista de las relaciones y diferencias de las entidades de proceso de más bajo nivel (actividades y tareas). Con base en la técnica de comparación descrita en [3], la comparación de las normas se llevó a cabo siguiendo un enfoque iterativo e incremental para facilitar (i) la gestión de la complejidad que entraña una comparación en la que se trata con entidades de bajo nivel de abstracción y (ii) aprovechar la experiencia ganada en iteraciones anteriores cuando se pasa a realizar una nueva.

Para registrar y levantar la información de la comparación, se diseñó una plantilla de documento, la cual permitió registrar los resultados de los procesos, actividades y tareas comparadas. La tabla 3 muestra la plantilla utilizada en la comparación de las tareas de la cláusula 8 de la Norma ISO 27001 y las tareas de la cláusula 9.2.2 de la Norma. ISO 20000-2.

Con el fin de expresar el grado de relación entre ISO 27001 e ISO 20000-2, se utilizó la escala de relación presentada en [3]. La escala está conformada por los siguientes elementos: No relacionados (N) (0%), Débilmente relacionados (D) (1% a 15%), Parcialmente relacionados (P) (16% a 50%), Ampliamente relacionados (A) (51% a 85%) y Fuertemente relacionados (F) (86% a 100%). El porcentaje de relación puede ser hallado dividiendo el número de actividades donde se ha encontrado alguna relación entre ISO 27001 e ISO 20000-2, sobre el total de número de actividades de la ISO 27001.

Como la comparación involucraría entidades a un bajo nivel de abstracción, fue necesario definir la direccionalidad de la comparación, la cual se definió a partir de un conjunto de criterios obtenidos a través de las necesidades manifestadas por la organización, estos fueron: (i) expandir el mercado para las organizaciones certificadas en ISO 20000, (ii) certificar en ISO 20000 a las organizaciones certificadas en ISO 27001 y (iii) tomar ventaja del esfuerzo realizado previamente en las certificaciones ISO 27001. En ese sentido, la direccionalidad definida fue comparar la ISO 27001 con respecto a la ISO 20000-2.

3.2.3. Ejecución de la comparación

La comparación se llevó a cabo según el diseño de comparación definido. En ese sentido, el análisis se enfocó en estudiar cómo las tareas de la ISO 27001 abordan de alguna manera (o no), algunos aspectos de las tareas identificadas en la ISO 20000. Al finalizar cada iteración de comparación, los resultados obtenidos fueron analizados por dos pares revisores (ver Figura 2). La revisión permitió verificar la fiabilidad de los resultados y el proceso de comparación. La tabla 3 muestra un ejemplo detallado de la relación identificada entre las tareas de la cláusula 8 referente al *SGSI* de la Norma ISO/IEC 27001 y la cláusula 9.2.2 referente al *Cierre y revisión de una solicitud de cambio* de la Norma ISO/IEC 20000-2

ISO/IEC 20000-2 / GP7: 9. Procesos de control / P2: Proceso 9.2 Gestión del cambio / A2: 2. La cláusula 9.2.2 hace referencia al Cierre y revisión de una solicitud de cambio.

Dirección del Mapeo
Desde la norma ISO 27001 a la norma ISO 20000-2
Entidades de proceso comparadas
Para ISO 27001 e ISO 20000-2: Tareas.
Pregunta de comparación
- ¿Qué tareas de ISO 27001 pueden ofrecer soporte al cumplimiento de las tareas de ISO 20000-2?
Objetivo de la comparación
Determinar el grado de relación entre las tareas de ISO 27001 y las tareas de ISO 20000-2.
Nomenclaturas Utilizadas
T: Tareas, A: Actividades, GP: Grupo de Procesos, P: Procesos.

Tareas	T1: Todos los cambios se deberían revisar en relación a su éxito o fallo después de la implementación y cualquier mejora debería ser registrada.	T2: Toda no conformidad se debería registrar y tomarse las acciones pertinentes.	T3: Cualquier debilidad o deficiencia identificada en la revisión del proceso de gestión del cambio, debería alimentar los planes de mejora del servicio.
Grado de Relación	P (1 de 3)		

ISO 27001 / GP5: 8. Mejora del SGSI. / P1: Cláusula 8. Mejora del SGSI / A2: 2. La cláusula 8.2 hace referencia a la Acción correctiva.

Tareas	T1: La organización debe realizar acciones para eliminar la causa de las no conformidades con los requisitos del SGSI, a fin de evitar que vuelvan a producirse.			

Tabla 3.Mapeo detallado entre la cláusula 8 referente al SGSI de la Norma ISO/IEC 27001 y cláusula 9.2.2 referente al Cierre y revisión de una solicitud de cambio de la Norma ISO/IEC 20000-2

4. Relaciones entre los procesos de la ISO 27001 e ISO 20000-2

Con base en las actividades realizadas en la estrategia de armonización descrita en las secciones anteriores, a continuación se lleva cabo un análisis detallado del grado de las relaciones encontrado entre los procesos de la ISO 27001 sobre los procesos de la ISO 20000-2. Este análisis involucra una identificación de la correspondencia, soporte y cobertura de los procesos comparados. La Tabla 4 muestra la comparación con relación a los procesos comparados de las dos normas.

4.1. Análisis de los resultados

El total de posibles relaciones que se identificaron entre los procesos de la ISO 27001 e ISO 20000-2 es de 133, en 48 de ellas se identificó algún tipo de relación de acuerdo a la escala de comparación. En ese sentido, el grado de relación general es del 36% (48 de 133 ó 48:133). Del 36% donde se encontró algún tipo de relación el 5% (7:133) corresponde a relaciones fuertes, el 5% (6:133) a relaciones ampliamente relacionadas, 24% (32:133) a relaciones parciales y 2% (3:133) a relacione débiles. El resto de posibles relaciones, corresponde al 64% (85:133) donde no se encontró ninguna relación. Las relaciones identificadas de acuerdo a la escala de comparación establecida, es una manera de conocer que las tareas comparadas de ISO 270001 con respecto a la ISO 20000-2 están relacionadas de alguna manera, por ejemplo, las (7) relaciones *F* entre los procesos comparados se aproximan o están al 100% de relación. Esto no significa que los procesos sean idénticos, sino que todas las tareas analizadas de ISO 27001 han encontrado algún tipo de relación con alguna tarea de ISO 20000-2.

Dirección del Mapeo
Desde la norma ISO 27001 a la norma ISO 20000-2
Entidades de proceso comparadas
Para ISO 27001 e ISO 20000-2: Procesos.
Pregunta de comparación
- ¿Qué actividades y tareas de ISO 27001 pueden ofrecer soporte al cumplimiento de las actividades y tareas de ISO 20000-2?
- ¿Qué actividades y tareas de ISO 27001 pueden están fuertemente relacionadas para soportar el cumplimiento de las actividades y tareas de ISO 20000-2?
Objetivo de la comparación
Determinar el grado de relación entre las tareas y actividades identificadas en ISO 27001 y las tareas y actividades de ISO 20000-2.
Escala de comparación
Fuertemente relacionado 86%-100%,
Ampliamente relacionado 51%-85%,
Parcialmente relacionado 16%-50% y
Débilmente relacionado 1%-15%
No relacionado 0%.
Nomenclaturas Utilizadas
GP: Grupo de Procesos
P: Procesos

			ISO/IEC 20000-2																				
			GP1 3. El Sistema de Gestión	**GP2 4. Planificación e Implementación de la Gestión del Servicio**				**GP3 5. Planificación e Implementación de nuevos servicios o servicios modificados.**	**GP4 6. Procesos de la provisión del servicio**						**GP5 7. Procesos de las relaciones**		**GP6 8. Procesos de resolución**		**GP7 9. Procesos de control**		**GP8 10. Procesos de entrega**
			P1: 3 El Sistema de Gestión	P1: 4.1 Planificación de la Gestión del Servicio (Planificar)	P2: 4.2 Implementación de la Gestión del Servicio y la Provisión del Servicio (Hacer).	P3: 4.3 Monitorización, medición y revisión (Verificar)	P4: 4.4 Mejora continua (Actuar)	P1: 5 Planificación e Implementación de nuevos servicios, o de servicios modificados	P1: 6.1 Gestión de Nivel de Servicio	P2: 6.2 Generación de informes del servicio	P3: 6.3 Gestión de la continuidad y disponibilidad del servicio	P4: 6.4 Elaboración del presupuesto y contabilidad de los servicios de TI.	P5: 6.5 Gestión de la capacidad	P6: 6.6 Gestión de la Seguridad de la Información	P1: 7.2 Gestión de las relaciones con el negocio	P2: 7.3 Gestión de suministradores	P2: 8.2 Gestión del incidente	P3: 8.3 Gestión del problema	P1: 9.1 Gestión de la Configuración	P2: 9.2 Gestión del cambio	P1: 10.1 Proceso de gestión de la entrega
ISO /IEC 27001	**GP1 4. Sistema de Gestión de la Seguridad de la Información**	P1 4.2 Creación y Gestión del SGSI	**A**	**P**	**P**	**A**	**P**	**N**	**D**	**N**	**P**	**P**	**N**	**F**	**P**	**N**	**D**	**A**	**A**	**P**	**F**
		P2 4.3 Requisitos de la documentación	**P**	**N**	**N**	**N**	**N**	**N**	**N**	**P**	**N**	**N**	**N**	**F**	**P**	**N**	**N**	**P**	**A**	**P**	**P**
	GP2 5. Responsabilidad de la Dirección	P1 5.1 Compromiso de la Dirección	**N**	**N**	**N**	**P**	**N**	**F**	**N**	**N**	**N**	**N**	**N**	**F**	**N**	**N**	**N**	**N**	**N**	**N**	**N**
		P2 5.2 Gestión de los recursos	**P**	**N**	**N**	**P**	**N**	**P**	**N**	**N**	**N**	**N**	**N**	**P**	**F**	**P**	**P**	**F**	**N**	**A**	**P**
	GP3 6. Auditorías internas del SGSI	P1 6. Auditorías internas del SGSI	**P**	**N**	**N**	**N**	**N**	**N**	**N**	**N**	**N**	**N**	**N**	**P**	**N**	**N**	**N**	**N**	**P**	**N**	**N**
	GP4 7. Revisión del SGSI por la Dirección	P1 7. Revisión del SGSI por la Dirección	**N**	**N**	**N**	**P**	**N**	**N**	**N**	**N**	**N**	**N**	**N**	**N**	**P**	**N**	**N**	**N**	**N**	**P**	**N**
	GP5 8. Mejora del SGSI	P1 8. Mejora del SGSI	**P**	**N**	**N**	**P**	**P**	**N**	**N**	**N**	**D**	**N**	**N**	**N**	**N**	**N**	**N**	**N**	**P**	**P**	**N**

Tabla 4. Resumen de la comparación entre los procesos de ISO 27001 e ISO 20000-2

El proceso de ISO 20000-2 donde no se identificó ninguna relación con los procesos de ISO 27001 fue el relacionado con la cláusula *6.5 Capacidad de Gestión*, proceso encargado de asegurar que la organización tiene todo el tiempo suficiente capacidad para cumplir con el grado mínimo de demanda de los negocios. Por ser un proceso de soporte fundamental a las actividades orientadas a los servicios, es lógico que no se encuentren relaciones con la norma ISO 27001. En resumen, la mayor cantidad de relaciones encontradas corresponden a relaciones parciales, seguido por relaciones fuertes y amplias en la misma cantidad, y débiles en menor cantidad. La Tabla 5 muestra la correspondencia de los procesos comparados.

4.2. Cobertura de la ISO 27001 sobre los procesos de la ISO 20000-2

Con el objetivo de entender cómo los procesos de la ISO 27001 soportan o abordan los procesos de la ISO 20000-2, se identificó el nivel de cobertura de las normas comparadas con relación a las tareas identificadas. El grado de cobertura en este trabajo estuvo enfocado a identificar cómo los procesos de la ISO 27001; soportan, abordan o tienen relación con los procesos definidos en la ISO 20000-2. Con base al objetivo de armonización definido y direccionalidad de la comparación, la comparación resultante fue una relación de uno a muchos. La Tabla 6 muestra el grado de cobertura de los procesos de ISO 200002 con relación a los procesos de la ISO 27001.

Procesos ISO/IEC 20000-2	**Procesos ISO/IEC 27001**
P1: 3 El Sistema de Gestión	P1 4.2 Creación y Gestión del SGSI P2 4.3 Requisitos de la documentación P2 5.2 Gestión de los recursos P1 6. Auditorías internas del SGSI P1 8. Mejora del SGSI
P1: 4.1 Planificación de la Gestión del Servicio (Planificar)	P1 4.2 Creación y Gestión del SGSI
P2: 4.2 Implementación de la Gestión del Servicio y la Provisión del Servicio (Hacer).	P1 4.2 Creación y Gestión del SGSI
P3: 4.3 Monitorización, medición y revisión (Verificar)	P1 4.2 Creación y Gestión del SGSI P1 5.1 Compromiso de la Dirección P2 5.2 Gestión de los recursos P1 7. Revisión del SGSI por la Dirección P1 8. Mejora del SGSI
P4: 4.4 Mejora continua (Actuar)	P1 4.2 Creación y Gestión del SGSI P1 8. Mejora del SGSI
P1: 5 Planificación e Implementación de nuevos servicios, o de servicios modificados	P2 5.2 Gestión de los recursos P1 5.1 Compromiso de la Dirección
P1: 6.1 Gestión de Nivel de Servicio	P1 4.2 Creación y Gestión del SGSI
P2: 6.2 Generación de informes del servicio	P2 4.3 Requisitos de la documentación
P3: 6.3 Gestión de la continuidad y disponibilidad del servicio.	P1 4.2 Creación y Gestión del SGSI
P4: 6.4 Elaboración del presupuesto y contabilidad de los servicios de TI.	P1 4.2 Creación y Gestión del SGSI
P5: 6.5 Gestión de la capacidad	No se encontró relación.
P6: 6.6 Gestión de la Seguridad de la Información	P1 4.2 Creación y Gestión del SGSI P2 4.3 Requisitos de la documentación P1 6. Auditorías internas del SGSI P2 5.2 Gestión de los recursos P1 5.1 Compromiso de la Dirección
P1: 7.2 Gestión de las relaciones con el negocio	P1 4.2 Creación y Gestión del SGSI P2 4.3 Requisitos de la documentación P2 5.2 Gestión de los recursos
P2: 7.3 Gestión de suministradores	P2 5.2 Gestión de los recursos
P2: 8.2 Gestión del incidente	P1 4.2 Creación y Gestión del SGSI P2 5.2 Gestión de los recursos
P3: 8.3 Gestión del problema	P1 4.2 Creación y Gestión del SGSI P2 4.3 Requisitos de la documentación P2 5.2 Gestión de los recursos
P1: 9.1 Gestión de la Configuración	P1 4.2 Creación y Gestión del SGSI P2 4.3 Requisitos de la documentación P1 6. Auditorías internas del SGSI P1 8. Mejora del SGSI
P2: 9.2 Gestión del cambio	P1 4.2 Creación y Gestión del SGSI P2 4.3 Requisitos de la documentación P2 5.2 Gestión de los recursos P1 7. Revisión del SGSI por la Dirección P1 8. Mejora del SGSI
P1: 10.1 Proceso de gestión de la entrega	P1 4.2 Creación y Gestión del SGSI P2 4.3 Requisitos de la documentación P2 5.2 Gestión de los recursos

Tabla 5. Correspondencia entre los procesos de la ISO 27001 e ISO 20000-2

Nomenclaturas Utilizadas
GP: Grupo de Procesos
#relaciones encontradas (:) #relaciones totales por GP. Lectura: por ejemplo (5 relaciones encontradas "de" 7 posibles relaciones)

			Grupos de Procesos de ISO/IEC 20000-2							
			GP1: 3 El Sistema de Gestión	**GP2: 4. Planificación e Implementación de la Gestión del Servicio**	**GP3: 5. Planificación e Implementación de nuevos servicios o servicios modificados.**	**GP4: 6. Procesos de la provisión del servicio**	**GP5: 7. Procesos de las relaciones**	**GP6: 8. Procesos de resolución**	**GP7: 9. Procesos de control**	**GP8: 10. Procesos de entrega**
GPs ISO/IEC 27001	**GP1 4. Sistema de Gestión de la Seguridad de la Información.**	P1 4.2 Creación y Gestión del SGSI	1:1	4:4	0:1	4:6	1:2	2:2	2:2	1:1
		P2 4.3 Requisitos de la documentación	1:1	0:4	0:1	2:6	1:2	1:2	2:2	1:1
	GP2 5. Responsabilidad de la Dirección.	P1 5.1 Compromiso de la Dirección	0:1	1:4	1:1	1:6	0:2	0:2	0:2	0:0
		P2 5.2 Gestión de los recursos	1:1	1:4	1:1	1:6	2:2	2:2	1:2	2:2
	GP3 6. Auditorías internas del SGSI	P1 6. Auditorías internas del SGSI	1:1	0:4	0:1	1:6	0:2	0:2	1:2	0:1
	GP4 7. Revisión del SGSI por la Dirección.	P1 7. Revisión del SGSI por la Dirección	0:1	1:4	0:1	0:6	1:2	0:2	1:2	0:1
	GP5 8. Mejora del SGSI.	P1 8. Mejora del SGSI	1:1	2:4	0:1	1:6	0:2	0:2	2:2	0:1
		Total	5:7	9:28	2:7	10:42	5:14	5:14	9:14	3:7
		Porcentaje de cobertura	A (71%)	P (32%)	P (29%)	P (24%)	P (36%)	P (36%)	A (64%)	P (43%)

Tabla 6. Cobertura de la ISO 27001 sobre los GPs de la ISO 20000-2

En la Tabla 6 es posible observar que al menos un grupo de procesos de la ISO 27001 soporta un GP de la ISO 20000-2. El grupo de procesos al cual ISO 27001 ofrece mayor cobertura es el GP1: 3 Sistema de Gestión (71%), seguido se encuentra el GP7: 9 Procesos de control (64%), GP8: 10 Procesos de entrega (43%), GP5: 7 Procesos de las relaciones y GP6: 8 Procesos de control (36%), GP2: 4 Planificación e Implementación de la gestión del servicio (32%), GP3: 5 Planificación e Implementación de nuevos servicios o servicios modificados (29%) y GP4: 6 Procesos de la provisión del servicio (24%). El porcentaje de cobertura puede ser hallado dividiendo el número de actividades donde se ha encontrado alguna relación entre la ISO 27001 e ISO 20000-2, sobre el total de posibles relaciones con respecto al grupo de procesos de la ISO 20000-2.

Con base en los resultados obtenidos, es posible identificar algunas coincidencias y diferencias entre la ISO 27001 y la ISO 20000-2, por ejemplo, a nivel de la *Gestión de la Seguridad de la Información* es posible observar que la ISO 27001 presenta una serie de *objetivos de control y controles* necesarios para garantizar la seguridad de la información. Por su parte, la ISO 20000-2 profundiza en los riegos asociados, operación y mantenimiento de los controles propuestos en la ISO 27001. En ese sentido, la ISO 20000 amplía la descripción de dichos controles describiendo en mayor detalle la forma en la que se deben llevar a cabo. Esta característica es posible observarla en varios de los procesos comparados, sin embargo, estas relaciones no se identificaron debido a que esta primera comparación de las normas se realizó sólo a nivel de las descripciones de sus cláusulas y no involucró los *objetivos de control y controles* definidos en el anexo A de la norma ISO 27001. En ese sentido, es posible que puedan establecerse más relaciones. Como trabajo futuro, se abordará la comparación de los modelos teniendo en cuenta los objetivos de control y controles definidos en la norma ISO 27001.

5. Beneficios alcanzados

Con la armonización de las normas ISO 27001 e ISO 20000-2, Audisec ha reportado varios beneficios, algunos de ellos y más significativos son:

- Al armonizar ISO 27001 e ISO 20000-2, es posible pensar que al ser normas estructuralmente compatibles, no es necesario llevar a cabo la homogeneización de sus entidades de proceso utilizando una estructura de elementos de proceso común. Sin embargo, el análisis semántico realizado para organizar las descripciones de las cláusulas en la estructura común mejoró el entendimiento de las normas, ya que facilitó la identificación, interpretación, interiorización y clasificación de las descripciones en entidades de proceso

más detalladas y bajo una estructura orientada hacia los procesos. Un ejemplo es presentado en la Tabla 2.

- La estrategia de armonización utilizada ha permitido definir una guía de armonización sistemática, la cual ha facilitado el análisis, la identificación de las relaciones, diferencias y apalancamiento entre ISO 27001 e ISO 20000-2. Según Audisec, "la estrategia de armonización fue una guía práctica y poderosa para llevar a cabo la armonización de ISO 27001 e ISO 20000-2".
- Con los resultados obtenidos, la organización ha desarrollado una herramienta software para soportar la consultoría en ISO 20000. Esta herramienta ha sido desarrollada teniendo en cuenta las relaciones encontradas entre las tareas, actividades y procesos de ISO 27001 e ISO 20000-2. Con base en los resultados obtenidos, la herramienta ha permitido reducir el esfuerzo involucrado en la institucionalización de la norma ISO 20000 en organizaciones que han implantado ISO 27001 previamente, esto debido a que identifica las relaciones entre los procesos de las dos normas.

6. Conclusiones y trabajo futuro

En este trabajo se ha presentado la armonización de las normas ISO 27001 e ISO 20000-2. Para llevar a cabo la armonización de estas normas, se definió y configuró una estrategia de armonización conformada por una técnica de homogeneización y una técnica de comparación. La estrategia de armonización obtenida es el resultado de la implementación de un proceso de armonización, el cual soporta la definición y configuración de estrategias para la armonización de múltiples modelos.

Tanto la ISO 27001 como la ISO 20000 describen enfoques, buenas prácticas y objetivos distintos para mejorar los sistemas de gestión de las organizaciones. Sin embargo, es posible hallar coincidencias en sus descripciones y a diferente nivel de detalle. Esta característica permite suponer que las semejanzas identificadas pueden ser armonizadas e integradas bajo un mismo sistema de gestión, impactando de manera positiva en los costos, tiempo y recursos asociados que si se implementaran por separado. En ese sentido, la comparación de la norma ISO 20000-2 con relación a la norma ISO 27001 realizado en este trabajo, puede suponer un beneficio práctico y específico para aquellas organizaciones certificadas en ISO 27001 que desean institucionalizar los procesos de la ISO 20000-2.

Teniendo en cuenta las actividades, tareas y procesos identificados en las normas ISO 27001 e ISO 20000-2, hemos podido observar que existe una relación parcial del 36%. Esto quiere decir que se han podido identificar 48 relaciones donde ISO 27001 ofrece algún tipo de relación sobre los procesos de la ISO 20000-2. Aunque el número de relaciones fuertes y amplias encontradas es apenas del 10%, es importante destacar que aunque la norma ISO 27001 e ISO 20000-2 definen buenas prácticas para distintos enfoques de aplicación, los modelos no son del todo diferentes, y es posible encontrar estrechas relaciones, por ejemplo los GPs a los que ISO 27001 ofrece mayor cobertura son los que describen prácticas para soportar los procesos del sistema de gestión y control de procesos, ellos son: el GP1: 3 El sistema de Gestión (71%) y GP9: 7 Procesos de Control respectivamente (64%).

Las relaciones conceptuales establecidas entre las normas, han sido identificadas bajo el criterio y experiencia del realizador encargado del análisis y comparación de los modelos. Como trabajo futuro, se llevará a cabo un estudio empírico que permita mapear las subcaracterísticas de calidad desde la opinión de varios expertos y/o personas involucradas en el uso de las normas ISO 27001 e ISO 20000 en algunas organizaciones. Esta validación permitiría comprobar su correspondencia desde un punto de vista no solo teórico, sino también empírico-práctico.

Debido a que la comparación de las dos normas se realizó sólo a nivel de las descripciones de las cláusulas sin tener en cuenta los *objetivos de control y controles* definidos en el anexo A de la norma ISO 27001, es posible que se hayan omitido posibles coincidencias y relaciones entre las normas. En ese sentido, como trabajo futuro se llevará a cabo la comparación de los *objetivos de control y controles* definidos en la norma ISO 27001 con los procesos, actividades y tareas de la norma ISO 20000-2.

Agradecimientos

Este trabajo ha sido financiado por los proyectos: ARMONÍAS (JCCM, PII2I09-0223-7948), PEGASO/MAGO (MICINN y FEDER, TIN2009-13718-C02-01), ARCA (CEC – JCCM y FEDER, HITO-2009-06) y (ECA-SPI, 3531-403-20708, Colciencias de Colombia).

Referencias

[1] ISO: itSMF and ISO/IEC 20000. (2010). Available on http://www.isoiec20000certification.com

[2] Paulk, M.C., How ISO 9001 compares with the CMM, *IEEE Software* **12**(1) (1995) 74–83.

[3] Pino, F., Balssarre, M.T., Piattini, M., Visaggio, G., Harmonizing maturity levels from CMMI-DEV and ISO/IEC 15504, *Journal of Software Maintenance and Evolution: Research and Practice* **22**(4) (2010) 279-296.

[4] Pardo, C., Pino, F., García, F., Piattini, M., Apoyando la armonización de diferentes marcos de referencia de procesos, in *Proc. XIII Ibero-American Conference on Software Engineering (CIbSE'2010)*, Ecuador, Cuenca, 2010, pp. 299-304.

[5] Pardo, C., Pino, F.J., García, F., Piattini, M., Baldassarre, M.T., A systematic review on the harmonization of reference models, in *Proc. 5th International Conference on Evaluation of Novel Approaches to Software Engineering*, Athens, Greece, 2010, pp. In press.

[6] Siviy, J., Kirwan, P., Marino, L., Morley, J., The Value of Harmonization Multiple Improvement Technologies: A Process Improvement Professional's View, Technical report, (Ed.: Software Engineering Institute, Carnegie Mellon, 2008),

[7] Siviy, J., Kirwan, P., Morley, J., Marino, L., Maximizing your Process Improvement ROI through Harmonization, Technical report, (Ed.: Software Engineering Institute (SEI). Carnegie Mellon University, 2008),

[8] Siviy, J., Kirwan, P., Renato, V., Peter, K., Gerhard, G., SEPG Europe 2008, in *Proc. Multimodel Improvement in Practice*, 2008, pp. 23.

[9] Brenner, M., Schaaf, T., Scherer, A., Towards an information model for ITIL and ISO/IEC 20000 processes, in *Proc.* New York, NY, 2009, pp. 113-116.

[10] Wang, C.H., Tsai, D.R., Integrated installing ISO 9000 and ISO 27000 management systems on an organization, in *Proc.* Zurich, 2009, pp. 265-267.

[11] LRQA, Case study: Datafort is the first russian company to have successfully Implemented an integrated management system (IMS), Technical report, (Ed.: Lloyd's Register Quality Assurance Ltd, 2007),

[12] Arifin, K., Aiyub, K., Awang, A., Jahi, J.M., Iteng, R., Implementation of Integrated Management System in Malaysia: The Level of Organization's Understanding and Awareness, *European Journal of Scientific Research* **31**(2) (2009) 188-195.

[13] Yoo, C., Yoon, J., Lee, B., Lee, C., Lee, J., Hyun, S., Wu, C., A unified model for the implementation of both ISO 9001:2000 and CMMI by ISO-certified organizations, *Journal of Systems and Software* **79**(7) (2006) 954-961.

[14] Rout, T.P., Tuffley, A., Harmonizing ISO-IEC 15504 and CMMI, ed. Chichester, UK, 2007, pp. 361-371.

[15] Wangenheim, C.G.v., Thiry, M., Analyzing the Integration of ISO/IEC 15504 and CMMI-SE/SW, Technical report, (Ed.: LQPS - Laboratorio de Qualidade e Productividade de Software. Universidad do Vale do Itajaí - UNIVALI, 2005),

[16] Pardo, C., Pino, F., García, F., Piattini, M., Homogenization of Models to Support multi-model processes in Improvement Environments, in *Proc. 4th ICSOFT´09*, Sofía, Bulgaria, 2009, pp. 151–156.

[17] ARMONÍAS: A Process for Driving Multi-models Harmonization, ARMONÍAS Project. (2009). Available on http://alarcos.esi.uclm.es/armonias/

[18] ISO, ISO/IEC 27001: Information Security Management System (ISMS) requirements, 2005, Technical report, (Ed.: 2005),

[19] ISO, International Organization for Standardization: Information technology – Service management – Part 1: Specification, ISO/IEC 20000-1:2005-12, Technical report, (Ed.: 2005),