ISO 20000 E ISO 27001: TAN DISTINTAS Y TAN IGUALES

Recibido: 03/07/07
Aceptado: 23/07/07

ISO 20000 AND ISO 27001: SO DIFFERENT AND SO EQUAL

Joseba Enjuto Gozalo
Ingeniero Superior de Telecomunicaciones
Consultor Senior
Nextel, S.A.

INTRODUCCIÓN

En los últimos tiempos, las normas ISO han irrumpido con fuerza en los entornos relacionados con los sistemas de información. Por un lado, la ISO 20000 y su desarrollo a nivel táctico, la famosa *ITIL*[1], con el objetivo de regular la prestación de servicios IT. Por otro, la ISO 27001 y su hermana local, la UNE 71502, tratando de optimizar la gestión de la seguridad de la información. Y, en medio, muchas empresas que ven en ambas normas un salvavidas al que aferrarse y, al mismo tiempo, un lastre capaz de hundirlas.

En principio, ambas normas son capaces de ayudar a cualquier organización a gestionar mejor sus infraestructuras. La norma ISO 20000 define la estructura de un sistema de gestión de los servicios IT (ITSMS, *Information Technologies Service Management System*), regulando tanto la prestación de los servicios como su gestión. Esta norma facilita la definición adecuada del catálogo de servicios y permite desarrollar de forma efectiva los SLAs[2] que los regulen.

Por su parte, la ISO 27001 define la estructura de un sistema de gestión de la seguridad de la información (ISMS, *Information Security Management System*) que desarrolla los controles organizativos y técnicos necesarios para garantizar el mantenimiento de una seguridad adecuada en la organización. La norma también define los requisitos mínimos para establecer la gestión óptima de los incidentes de seguridad, y cubre desde las debilidades en materia de seguridad hasta el desarrollo del Plan de Continuidad de negocio de la organización.

Por lo tanto, es evidente que la adopción de ambas normas supone unos beneficios claros para cualquier organización. Sin embargo, las empresas ven con cierto recelo la adopción e implantación de estos estándares por diversos motivos.

Por un lado, las empresas desconfían de forma sistemática de las distintas normas y estándares de gestión que van apareciendo. Lamentablemente, son muy habituales las experiencias negativas a raíz de una incorrecta implantación de estándares como la ISO 9001, donde una interpretación literal de la norma y una pésima personalización suele provocar la adopción de una burocracia rígida y poco útil que sólo ocasiona enfados y pérdida de eficacia.

Por otro, la adopción de este tipo de metodologías suele suponer una inversión inicial importante debido a la necesidad de contratar los servicios de unos consultores que aseguren, en la medida de lo posible, el éxito de una implantación cuyos resultados reales no están, *a priori*, nada claros. Y ése es precisamente el más importante de los factores que provoca las dudas de las empresas. Los beneficios prácticos parecen dudosos, se desconoce cómo va a afectar la implantación en el día a día de las personas y hay personas que tienen la sospecha de que estos sistemas de gestión supondrán más carga de trabajo para todos los implicados.

Estas dudas, que ya son un duro escollo a superar ante la implantación de cualquiera de las dos normas, se multiplican en caso de que una organización se plantee la adopción de ambas. Dos sistemas de gestión, dificultades al cuadrado. Por ello, el primer paso es analizar los beneficios de esa doble implantación. Y no hay mejor forma que estudiar sus coincidencias para ver que, en realidad, una implantación conjunta de ambos estándares supone un importante ahorro de esfuerzos y dinero, y la garantía de un sistema de gestión integrado que incremente los beneficios que cada una de ellas ofrece a la compañía.

Cuestión de alcances

Antes de profundizar en los paralelismos y coincidencias de ambos estándares, tenemos que acotar un poco más nuestro campo de actuación. La ISO 27001 plantea el desarrollo de un SGSI[3] general cuyo alcance puede in-

1 Information Technology Infrastructure Library
2 Service Level Agreement
3 Sistema de Gestión de la Seguridad de la Información

cluir cualquier tipo de proceso de la organización. Sin embargo, y debido a las implicaciones que tiene esta norma ante los sistemas de información, suele ser una decisión común en muchas organizaciones el comenzar su implantación en un alcance que se reduce a los procesos desarrollados por el área de sistemas. Y es precisamente bajo este alcance donde podemos encontrar estas coincidencias de forma más evidente, en un entorno en el que la ISO 20000 regule la prestación de servicios IT tanto a nivel interno como a clientes, si es el caso, y la ISO 27001 garantice la gestión segura de los mismos.

Por otro lado, si nos ponemos a analizar la ISO 20000, vemos que uno de los procesos que exige implantar es el correspondiente a la gestión de la seguridad de la información.

Es decir, que la propia ISO 20000 exige implementar un pequeño SGSI dentro del ámbito de los Sistemas de Información. Y no sólo eso, sino que la propia norma nos remite a la ISO 17799 (código de buenas prácticas para la ISO 27001) como referencia para la implantación de dicho proceso. Por lo tanto, parece evidente que, si nos centramos en el alcance correspondiente al área de sistemas de información, probablemente encontremos muchos elementos en común.

Dirección Gestión Comercial Producción Infraestructuras

Sistemas de Información ISO 27001

ISO 20000 Alcance seleccionado

Semejanzas y diferencias

En primer lugar, tanto la ISO 27001 como la ISO 20000 definen un sistema de gestión completo. Como tal, ambas siguen un modelo PDCA[4] y, por tanto, van a requerir el desarrollo de un ciclo de revisión y mejora continua en el que existan recursos dedicados a la gestión, monitorización, seguimiento, revisión, auditoría y optimización de ambos sistemas. Sin embargo, nada impide que estos recursos sean los mismos y que, en ambos caso, el ciclo de revisión y mejora continua se desarrolle bajo las mismas estructuras organizativas. Además, ambas normas exigen que el ciclo de revisión sea liderado desde la alta dirección, en función de unas responsabilidades coincidentes que pasan por la definición de políticas y objetivos, la provisión de los recursos necesarios, la difusión del sistema de gestión y la garantía de cumplimiento de lo establecido.

En segundo lugar, ambas normas centran parte de sus objetivos en el desarrollo de una documentación completa que regule y formalice las actividades desarrolladas bajo ambos sistemas de gestión. Y, en esa línea, ambas exigen el desarrollo de una gestión documental completa que cubra todo lo relativo a la gestión de cambios y versiones y estandarice el proceso de revisión y validación formal de la misma, garantizando su viabilidad y operatividad. En este caso, no sólo ambas normas coinciden de manera exacta en este requisito, sino que otros sistemas de gestión más extendidos como los que definen la norma ISO 9001 o la 14001 también lo incluyen, y en caso de que alguna de ellas esté ya implantada

(lo que cada día es más habitual) será una tarea que nos podremos ahorrar.

Otro de los principales elementos que encontramos común a ambas normas es el relativo a la gestión de terceras partes. Ambas exigen una adecuada gestión de los servicios proporcionados por los distintos proveedores, así como su correcta evaluación y selección. La ISO 20000 se centra más en la óptima integración de las terceras partes en la cadena de prestación del servicio, mientras que la ISO 27001 profundiza más en los riesgos asociados al intercambio de información que se lleva a cabo con ellos. Sin embargo, ambas normas acaban exigiendo el desarrollo, de forma más o menos exhaustiva, de acuerdos de nivel de servicio que regulen las relaciones que se mantienen con estas terceras partes y el modo en el que se gestionan los cambios a este respecto.

A partir de este punto, podemos descubrir una gran cantidad de coincidencias entre controles de ISO 27001 y procesos de ISO 20000. De hecho, algunos de los controles más importantes a la hora de implementar un SGSI están desarrollados en forma de procesos dentro de ISO 20000. Por tanto, podríamos considerar que la ISO 20000 amplía la definición de dichos controles, planteando no sólo los requisitos que se deben cumplir sino la forma en la que se deben llevar a cabo.

Uno de estos controles es el relativo a la gestión de cambios. Gestión de cambios no sólo a nivel documental, como ya se ha indicado anteriormente, sino a nivel global.

Ambas normas exigen una correcta gestión de cambios en las características de los servicios prestados, en las infraestructuras de soporte, en los procedimientos, en

4 Plan Do Check Act

los sistemas de información o en el propio sistema de gestión. Como ya se ha señalado, la ISO 20000 es más exhaustiva a la hora de definir los requisitos en este ámbito, definiendo un proceso específico para ello, pero ambas normas exigen el desarrollo de un ciclo completo de autorización, análisis, evaluación, pruebas, validación, verificación y aceptación para cualquier cambio significativo que se lleve a cabo dentro de cualquiera de los elementos contemplados en el alcance.

A la hora de garantizar la continuidad de los servicios, ambas normas se integran y complementan a la perfección. Por un lado, la ISO 20000 se centra en la disponibilidad de los servicios, exigiendo el desarrollo de planes de contingencia y recuperación que garanticen su continuidad a corto plazo. Por otro, la ISO 27001 amplía estas consideraciones y extiende el concepto de disponibilidad hasta los planes de continuidad de negocio, exigiendo su existencia como garantía de la continuidad de los servicios a largo plazo. De este modo, la ISO 20000 permite una aproximación más concreta a los planes de contingencia mientras que la ISO 27001 define el marco de gestión de la continuidad en el que se deben incluir todos los planes desarrollados.

Uno de los apartados en los que la ISO 27001 es más exhaustiva y exigente que la ISO 20000 es el relativo al análisis de riesgos. La segunda únicamente señala que se analicen los riesgos asociados a la prestación de servicios IT de forma genérica, mientras que la ISO 27001 define con mayor profundidad los requisitos y condiciones que debe cumplir dicho análisis. Además, la ISO 27001 es más extensa a la hora de definir el modo en el que debe desarrollarse la gestión de los riesgos, llegando a proponer una serie de controles (el conocido Anexo A) que deben implementarse para garantizar un nivel de seguridad adecuado dentro del alcance en el que nos encontramos, los sistemas de información.

Uno de los aspectos en los que ISO 27001 e ISO 20000 son bastante similares es en lo relativo a la gestión

de incidentes. Ambas normas llevan a cabo un importante esfuerzo a la hora de definir una metodología de gestión de incidentes, que contemple no sólo las propias incidencias sino también los problemas. En ambos casos se contemplan los incidentes dentro del sistema de gestión, y se especifican en mayor o menor medida tanto las estructuras organizativas que deben garantizar esta gestión como los pasos que se deben seguir para llevar a cabo esta gestión de forma correcta y los resultados mínimos que deben obtenerse.

Por último, otro de los elementos más destacables respecto a las coincidencias entre ambas normas es el relativo a la planificación de la capacidad. En este caso, la ISO 20000 vuelve a ser más exhaustiva a la hora de definir requisitos, ya que define un proceso completo cuyo objetivo principal es garantizar la suficiente capacidad de los sistemas para prestar los servicios, pero la ISO 27001 también hace referencia a este hecho al definir un control específico a tal efecto, que exige que se garantice el rendimiento futuro de los sistemas a través de monitorizaciones y proyecciones que permitan predecir dichas necesidades. Por tanto, una gestión adecuada de la capacidad de los sistemas va a permitir el cumplimiento simultáneo de ambas normas en lo que a este respecto se refiere.

CONCLUSIONES

Podríamos seguir enumerando, a más bajo nivel, otra serie de aspectos en los que la implementación de ambos sistemas de gestión presenta coincidencias, pero es más apropiado quedarse en este punto y recalcar el mensaje contenido en este artículo.

Tanto la ISO 20000 como la ISO 27001 proponen sistemas de gestión que, aunque con objetivos distintos, exigen la implementación de medidas coincidentes en muchos casos. La implementación integrada de ambas normas en un entorno como el de los sistemas de información nos va a permitir el desarrollo de un sistema de gestión único que cumpla simultáneamente con los requisitos de ambos estándares.

Este hecho, además de aportar todas las ventajas que supone la adopción de un sistema único de gestión doblemente certificable, nos va a permitir desarrollar una infraestructura de gestión técnica que garantice de forma global, tanto a nivel de prestación de servicios como de seguridad de todos sus elementos, la necesaria calidad de las actividades desarrolladas en este entorno. Por lo tanto, podemos afirmar que estamos ante una inmejorable oportunidad de desarrollar, gracias al cumplimiento de estándares internacionalmente reconocidos, una infraestructura de gestión que permita garantizar la adecuación óptima del núcleo tecnológico de nuestras organizaciones a las exigencias, tanto propias como de nuestros clientes, de unos servicios seguros y de calidad óptima.

BIBLIOGRAFÍA

- ISO / IEC 17799:2005. Information technology – Security techniques - Code of practice for information security management.

- ISO / IEC 27001:2005.Information technology -Security techniques - Information Security Management Systems – Requirements.

- UNE-ISO / IEC 20000-1:2006. Tecnologías de la Información- Gestión del servicio- Parte1: Especificación. –

- UNE-ISO / IEC 20000-2:2006 Tecnologías de la Información- Gestión del servicio- Parte 2: Código de prácticas. ■