¿ISO 20000 o ISO 27000?

EL ANÁLISIS DE RIESGO ES TRATADO CON MAYOR DETALLE EN ISO-27001 QUE EN ISO-20000, SI BIEN ESTA ACTIVIDAD ES IMPRESCINDIBLE EN AMBOS PARA OBTENER EFICIENTES RESULTADOS

Alejandro Corletti
DIRECTOR DIVISIÓN SEGURIDAD INFORMÁTICA
NCS

Carmen de Alba Muñoz
RESPONSABLE ISO-27000
NCS

Introducción

Muchos de vosotros os preguntaréis qué tiene que ver este interrogante. A decir verdad la respuesta es casi filosófica, pues "Todo depende del ángulo en que se mire"... Por nuestra parte desde NCS ya nos han hecho esta pregunta varios clientes, y "Cuando el río suena, agua lleva", así que nos hemos decidido a escribir estas breves líneas pues, evidentemente aún no se tiene un panorama claro sobre:

¿Qué es esto de la gestión y de la calidad, que se está normalizando en todos los ámbitos?

Para ser sinceros, es muy justo que el panorama no esté claro, pues esta gente de ISO, parece que se propuso hacernos comprar todos los estándares para que nuestras empresas tengan "Calidad" y podamos demostrar que las "Gestionamos" como corresponde. Empezaron con la familia 9000, luego la 14000, la 27000, y se ve que el salto del 14 al 27 les pareció muy grande, entonces tuvieron que crear la 20 (para que se quede en el medio), y no se puede estar al tanto de cada uno de sus puntos con el detalle necesario, pues encima hay que releerlas varias veces para llegar a su fondo.

> ISO/IEC 20000 está formada por dos partes bajo el mismo título "Tecnología de la Información -Gestión del Servicio"

En este artículo, nos centraremos en las dos que más conocemos (pues son nicho de negocio en **NCS**) y queremos sencillamente, presentar con mucha síntesis la ISO 20000, para poder luego hacer las comparaciones necesarias con ISO 27000 (de la que no hablaremos, pues de ella hemos escrito en este revista desde que nació), y por último presentar nuestra visión sobre ambas a ver si es válido o no, el plantearse ¿ISO 20000 o ISO 27000?

Breve Presentación de ISO 20000

ISO/IEC 20000 está formada por dos partes bajo el mismo título **"Tecnología de la Información - Gestión del Servicio":**

- **Parte 1:** Especificaciones.
- **Parte 2:** Código de buenas prácticas.

Esta división, en realidad responde a un mismo desarrollo del temario, en el cual la parte uno, se centra más en los aspectos de forma o definiciones (es la que se certifica), y la parte dos, amplía el desarrollo de cada uno de los puntos de este índice.

La versión en inglés se publicó a finales de 2005, y recientemente (en Junio de 2007), AENOR dio a conocer su versión española bajo el nombre: **UNE–ISO/IEC 2000–1** y **UNE–ISO/IEC 2000–2.**

En la introducción hay una frase que llama la atención: *"Los **servicios y la gestión** de estos servicios son esenciales para ayudar a las organizaciones a **generar ingresos y ser rentables**"*. Es decir, a esta altura del siglo ninguna organización puede dudar más, que todo proceso o

aplicación informática, es una de las principales fuentes de dinero para la empresa.

Se trata de una **norma eminentemente basada en procesos**, y a lo largo de su desarrollo, especifica trece de ellos, agrupados en seis grupos que se corresponden a los puntos 5 al 10 del estándar.

El **punto 1**, que habla del objetivo y alcance de esta norma. Establece que la misma puede ser aplicada en empresas que solicitan ofertas o desean un enfoque consistente con sus proveedores de servicio, por los mismos proveedores para medir su eficiencia o demostrarla, como base para una evaluación independiente, o por cualquier organización que desee mejorar sus propios servicios. De todo esto, es muy importante recalcar que el ámbito más genérico estará siempre bajo el enfoque de "Servicios".

El **punto 2** aborda las definiciones, y los **puntos 3 y 4** se refieren al Sistema de Gestión. Cubren desde el compromiso de la Dirección, hasta los documentos, procesos y la formación. Luego pasa con buen nivel de detalle al ciclo PDCA (Plan–Do–Check–Act), perfectamente conocido por todos nosotros a través de las publicaciones anteriores.

El **punto 5** (muy breve por cierto), trata la planificación e implementación de nuevos servicios o servicios modificados, sin entrar en mucho detalle.

A partir del punto 6 y hasta el 10 es donde describe la implementación de estos seis grupos de procesos, cuyo temario referimos a continuación.

Punto 6. Procesos para la provisión del servicio. Incluye: Gestión del nivel del servicio, Generación de informes de servicio, Gestión de la continuidad y disponibilidad del servicio, Elaboración de presupuesto y contabilidad de los servicios de TI, Gestión de la capacidad y Gestión de la seguridad de la información.

Muchos de los procesos que propone ISO 20000, forman parte de un "mensaje subliminal" u oculto hacia la seguridad

Objetivos del punto 6: Planificar, diseñar, dimensionar, generar, valorar económicamente y asegurar la provisión de un servicio.

Punto 7. Procesos de relaciones. Comprende: Gestión de las relaciones con el negocio y Gestión de suministradores.

Objetivos del punto 7: Establecer un marco de buena colaboración entre el cliente y el proveedor, garantizando las mejores condiciones.

Punto 8. Procesos de resolución. Este punto trata dos aspectos: Gestión del incidente y Gestión del problema, los cuales a pesar de estar íntimamente relacionados son procesos separados.

Objetivos del punto 8: Minimizar problemas y en caso de producirse, restaurarlos lo antes posible.

Punto 9. Procesos de control. Comprende dos procesos: Gestión de configuración y Gestión del cambio.

Objetivos del punto 9: Detallar al máximo todos los procesos implementados, mantenerlos actualizados con información precisa y planificar cambios para asegurar su estabilidad.

Punto 10. Proceso de entrega. Se refiere exclusivamente a la Gestión de la entrega.

Objetivos del punto 10: Su finalidad es la de regular toda la actividad de entrega para los entornos en producción, el seguimiento, los plazos, posibilidades de marcha atrás, entornos de prueba, y las mediciones de éxito y fallo de las mismas.

Si nos propusiéramos graficar esta norma, podríamos representarla de la siguiente forma:

La Figura 1 nos muestra qué es lo que administra y regula la ISO 20000 Parte 1: un **Sistema de Gestión de Servicios de TI.** En esta administración se debe encontrar un equilibrio entre la calidad de los servicios prestados y los recursos (gente, tecnología y procesos) que dan soporte a esos servicios. Para alcanzar este objetivo, es necesario establecer un sistema de gestión adecuado que permita disminuir los plazos de entrega y soporte, mejorando los niveles de servicio con costes más bajos.

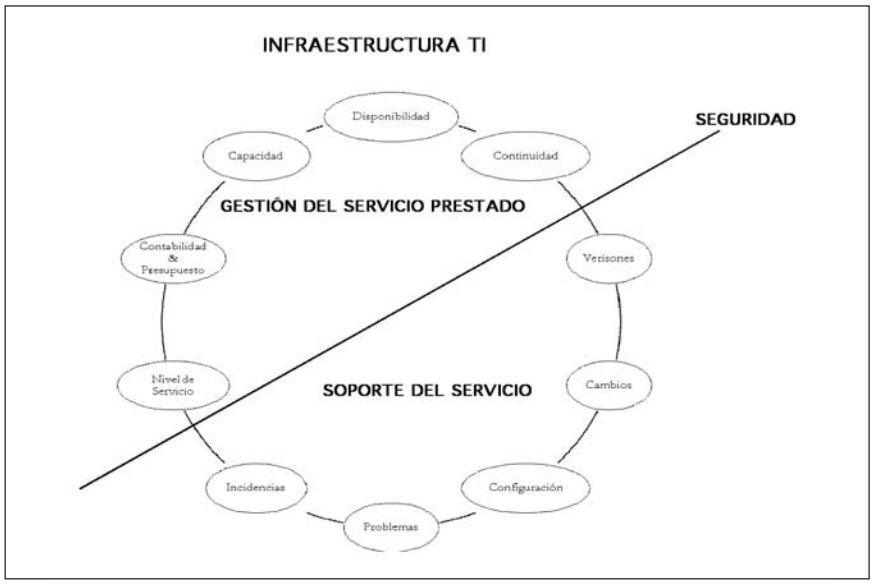

Figura 1

Qué Encontramos en Común

- Sobre todo, y lo más importante es la fuerte orientación que hacen hacia la gestión a través del compromiso de la Dirección, para seguir avanzando en el ciclo PDCA. Debemos recordar que las dos grandes diferencias entre ISO 17799 e ISO 27001, fueron la inclusión del Análisis de Riesgo y el ciclo PDCA (presentado bajo la forma de SGSI).
- No se puede dejar pasar por alto, que existe una diferencia importante en la visión del análisis de riesgo, pues para ISO-27001, esta tares es uno de los pilares fundamentales. En cambio ISO-20000, lo menciona, sin hacer tanto hincapié.
- La eminente orientación a procesos, también es un denominador común, pues en la ISO–27001, cada uno de los controles que propone, hace mención a que debe ser "auditable", para permitir con ello verificar su evolución, lo cual no es nada menos que un proceso continuo.
- Muchos de los procesos que propone ISO 20000, forman parte de un "mensaje subliminal" u oculto hacia seguridad, pues la disponibilidad, las incidencias, la recuperación, los contratos, las pruebas de maqueta, la continuidad, los registros, etc., son temas que incluye también ISO 27000. No es de extrañar pues la Disponibilidad de un servicio, es una de las palabras mágicas de la terminología de seguridad. Si se presta atención a la sección definiciones y términos de ISO 20000–1, pareciera una norma de "Seguridad" y no de "Gestión de Servicio"... hummm. ¿No estamos hablando de algo muy parecido?
- Las referencias a **"disponibilidad"** aparecen 32 veces en ambas partes de ISO 20000, mientras que "Integridad" aparece 4 veces, y "Confidencialidad" no aparece ninguna. Estas cuentas, aunque parezcan triviales, no lo son, pues nos están dejando la evidente intención que tiene la norma, es decir la **"DISPONIBILIDAD" de los servicios.**
- Nos atreveríamos casi a asegurar, que la "Seguridad", luego de la Gestión (y en ese orden) es el pilar más robusto de la "Gestión de Servicio".
- Todo lo referido a "Seguridad" en ISO-20000, quedaría cubierto (y más aún) si ya se posee una certificación en ISO-27001. Afirmamos que más aún, pues si se aborda una certificación en ISO-27001, esto implica un enorme "Know How" y un cúmulo de documentación, plantillas, procesos, análisis, planificación, concienciación, metodologías, etc., que serán "reutilizadas" si se aborda luego una certificación ISO-20000.

Si aún no se han iniciado metodologías de gestión y calidad, lo importante es plantearse PDCA

Conclusiones

■ ISO 20000 está orientada exclusivamente a Gestionar Servicios. Por lo tanto hay que evaluar qué porcentaje de los procesos de negocio de la empresa están muy relacionados con servicios, si esta tasa es baja, no es una buena decisión ponerse a trabajar con ISO 20000.

Hay Servicios, y servicios... Si los mismos tienen una importante relación con la seguridad, datos íntimos, financieros, policiales, I+D, estratégicos, etc. (Ejemplo: Aseguradoras, banca, industria farmacológica o petrolera, Justicia, policial, etc.), la mejor opción sería comenzar pensando en **ISO 27001**. Si los Servicios no procesan información tan clasificada, dependen de un alto volumen de transacciones,

Si la empresa es prestadora de servicios, ISO 20000 es importante como señal de seriedad y esfuerzo

la **"confidencialidad e Integridad"** no son los parámetros cruciales, etc. (Ejemplo: centros de venta, control de stock, almacenaje, fabricación en serie, etc.) un buen camino es **ISO 20000**. En definitiva, se trata de ser capaz de alinear los **procesos de negocio** (desde el punto de vista de servicios), con los objetivos empresariales.

■ Si la empresa es prestadora de servicios, ISO 20000 es importante como señal de seriedad y esfuerzo, si esos servicios están orientadas a empresas cuyos procesos guardan relación con "Confidencialidad e Integridad", entonces cuidado con ISO 27001.

■ Si la magnitud de la empresa es pequeña (PyMEs), ISO 20000 no es tan sencillo y por el contrario, si lo es ISO 27001 (tal cual venimos reiterando en nuestras publicaciones "ISO 27001 y las PyMEs").

■ Si aún no se han iniciado metodologías de gestión y calidad, antes de plantearse cuál de los dos, lo importante es plantearse PDCA, bajo cualquier familia.

■ Si bien, el análisis de riesgo, es tratado con mayor detalle en ISO-27001, que en ISO-20000, esta actividad es imprescindible en ambos para obtener eficientes resultados.