

ISO 20000

Sistemas de Gestión de Tecnología de la Información (TI)

De manera paulatina, y a nivel internacional, vemos que se empiezan a realizar normas específicas por sectores.

La ISO 9001:2000 (Certificación de Sistemas de Calidad) se va desmembrando en diversas normativas de Calidad sectoriales, ya sea TS 16949 (Sistemas de Calidad en el Sector de la Automoción), ISO 27001 (Sistemas de Seguridad de la Información), Q- ITCE (Sistemas de Calidad en el sector turístico)...

Dentro de esta especialización aparece una nueva normativa denominada ISO 20000 (Sistemas de Gestión de Tecnología de la Información). Esta norma se centra en cubrir esas actividades relacionadas con los servicios TI que la norma ISO 9001/2000 no podía cubrir con el celo necesario.

La normativa ISO 20000 se centra en los Sistemas de Gestión de Servicios de Tecnología de la Información (TI), que dan apoyo a una o más áreas de nuestros negocios. Podríamos definir la norma ISO 20000 como la primera normativa a nivel mundial enfocada específicamente a la gestión del servicio TI.

Dicha norma se compone, a su vez, de la siguiente normativa:

- ISO/IEC 20000-1:2005: Gestión de la Tecnología de la Información. Parte 1. Especificación. Esta parte 1 es certificable, es decir, podría ser el equivalente a la ISO 9001/2000.

- ISO/IEC 20000-2:2005: Gestión de la Tecnología de la Información. Parte 2. Código de buenas prácticas. Es una guía para implantar la parte 1. Una empresa se podrá certificar contra ISO/IEC 20000-1:2005, pero nunca contra ISO/IEC 20000-2:2005, ya que se utiliza la parte 2 para realizar la correcta implantación de la parte 1. Es decir, es el equivalente en Calidad a la ISO 9004; uno utiliza la ISO 9004 para realizar una correcta implantación de la norma ISO 9001/2000, y la certificación se realiza contra ISO 9001/2000.

A su vez, nos podemos ayudar de más documentos con el fin que la implantación de nuestro Sistema TI sea perfecta. Estos documentos son los BIP's. Nos gustaría destacar como útiles algunos de ellos:

- BIP 0005: Una guía para la correcta gestión del servicio TI.

- BIP 0015: Libro de trabajo y lista de chequeo para la realización de auditorías internas.
- Los BIP que van del 0030 al 0039, que se podrían considerar de "bastante aprovechables".

Pero ¿cuál es la historia de dicha normativa? ¿Cómo apareció?

Nos tenemos que trasladar al año 1989, cuando el Gobierno británico editó una guía en la que se definían los procesos y buenas prácticas dentro de los Sistemas TI. Estas guías fueron conocidas mundialmente como ITIL.

Ante la importancia que empezó a adquirir esta guía, se decide crear un Comité que la gestione, por lo que, en 1991 se crea el ITSMF (Information Technology Management Forum), con el fin de controlar y mejorar esta guía y las buenas prácticas.

La demanda de este sector aumentaba, por lo que el ITSMF se aproxima a BSI (British Standards Institution) y le

“La normativa ISO 20000 se centra en los Sistemas de Gestión de Servicios de Tecnología de la Información (TI), que dan apoyo a una o más áreas de nuestros negocios”

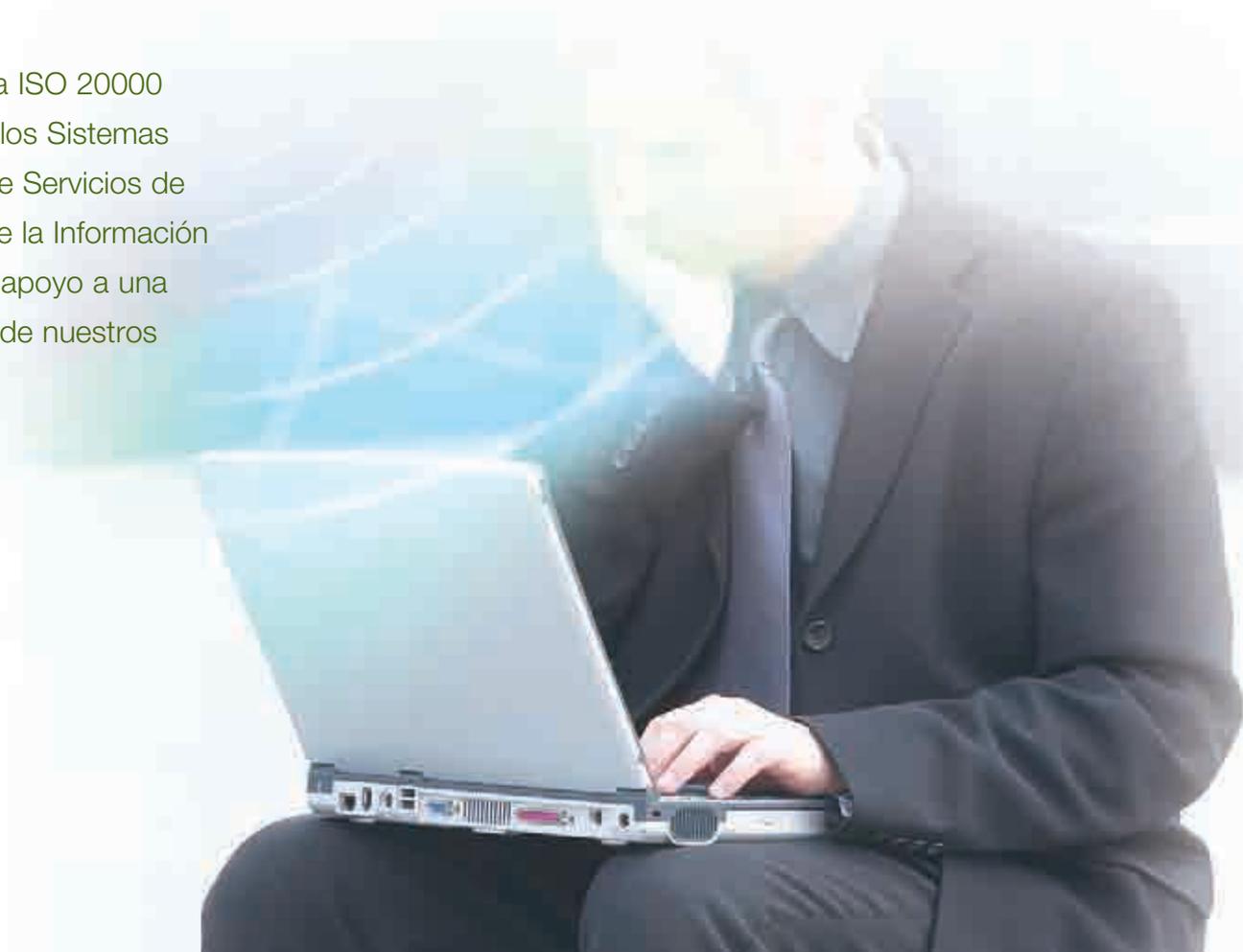
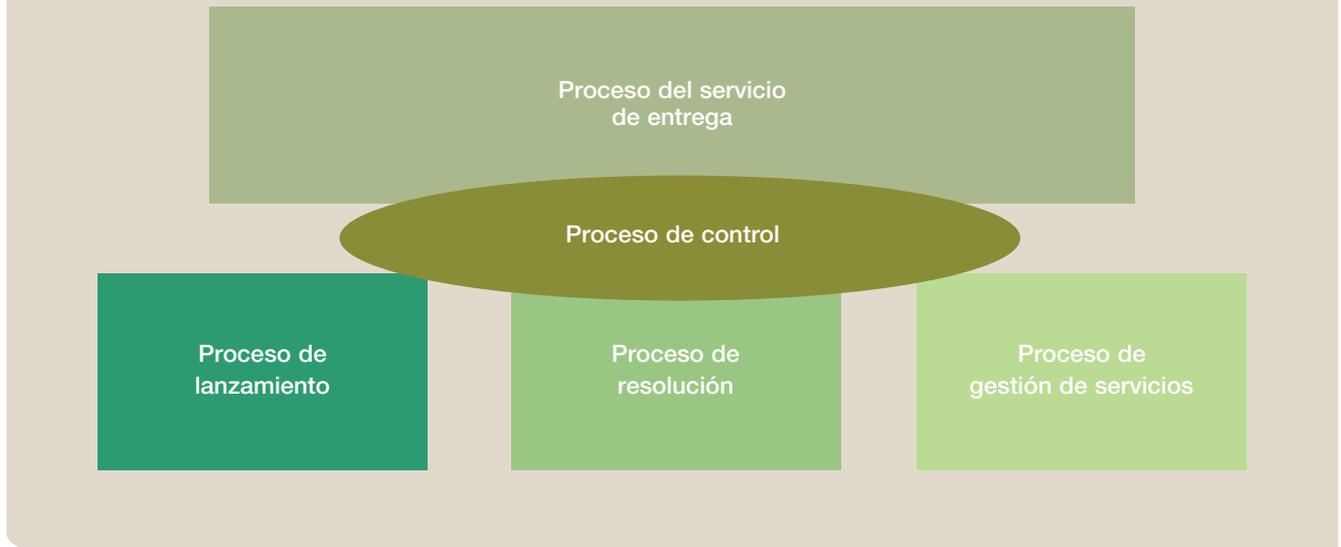


FIGURA 1



encarga la confección de una norma específica de este sector.

En el año 2000, BSI (como Entidad de Normalización) publica la BS 15000, normativa británica enfocada al sector. En el año 2002 se realiza una revisión a dicha norma con el fin de adaptarla a las exigencias del mercado.

Así, en marzo de 2006, y ante el éxito de la norma BS 15000 a nivel mundial, se presenta dicha norma al Comité ISO y se aprueba, pasando la norma BS 15000 a denominarse ISO 20000, es decir, pasa a considerarse una normativa mundialmente aceptada. De este modo, la ISO 20000 (antigua BS 15000) se centra de manera enfática en dar un apoyo y contribuir a una mejora a la calidad de los servicios TI.

Los objetivos de la ISO 20000 se podrían definir como:

- Promover la adopción de procesos integrados con el fin de suministrar la gestión de los servicios para obtener los requisitos tanto de nuestros clientes como del mercado en sí.
- Medir la comprensión de nuestras “buenas prácticas”, objetivos, beneficios

y posibles problemas dentro de nuestro sistema de gestión.

- Ayudar a las organizaciones a generar facturación, o bien, generar costes efectivos o beneficios dentro de la vía profesional del servicio TI que se suministra a los clientes.

¿Por qué la ISO 20000 será una norma exitosa en los próximos años?

Por las siguientes razones:

- Las empresas dependen más de sus Sistemas TI y necesitan una correcta gestión y mantenimiento de éstos.
- Los fallos e incidencias son cada vez más visibles, por lo que necesitamos un sistema que nos permita subsanarlos.
- Aumenta exponencialmente el número de demandantes de servicios TI a nivel mundial.
- Las infraestructuras son cada vez más complejas y el mercado necesita especialistas en el sector.
- Continuo cambio de los Sistemas TI (continuo avance de la tecnología).
- Poseer la ISO 20000 será una ventaja competitiva dentro del sector y una

referencia positiva muy valorada por los clientes.

De igual modo, es interesante destacar la relación que existe entre ITIL e ISO 20000:

- ISO 20000 es certificable; ITIL no, son sólo unas “buenas prácticas”.
- Para certificar ISO 20000 no es necesario implantar ITIL, pero su utilización puede hacer al Sistema más robusto, además de simplificar la obtención y el cumplimiento de la normativa.
- La estructuración de la organización no es un requisito de ISO 20000 mientras que PDCA (Plan, Do, Check, Act) es fundamental.
- ISO 20000 incluye relaciones y control de proveedores y subcontratistas.
- Dentro del ISO 20000, el servicio de confección de informes e información al Comité se considera un proceso independiente.
- El Plan de Continuidad de Negocio no es obligatorio en ITIL.
- ITIL cubre la gestión financiera, mientras que ISO 20000 cubre presupuestos y contabilidad.

- ISO 20000 incluye requisitos de Seguridad de la Información (ISO 27001).
- ITIL incluye requisitos de software, mientras que ISO 20000 cubre la configuración del Sistema.

En ISO 20000, el servicio se divide en cinco subprocesos (*figura 1*):

a) *Proceso del servicio de entrega*. Este proceso se centra en:

- Gestión del nivel de servicio.
- Información del servicio suministrado.
- Continuidad del negocio y gestión de la disponibilidad.
- Financiación y contabilidad para servicios TI.
- Gestión de capacidad.
- Gestión de seguridad de la información.

b) *Proceso de gestión de servicios*. Básicamente sería una homologación de los proveedores críticos del proceso suministrado.

c) *Procesos de control*. Basado en gestión del cambio y gestión de la configuración. Concretamente en el

concepto de gestión del cambio habría que definir:

- Integración de Sistemas utilizados a nivel TI. Definición de "interfaces".
- Identificación, control y seguimiento de los procesos TI.
- Proporcionar la información necesaria para poder cambiar el proceso de gestión
- Gestionar el impacto en las configuraciones del servicio y de la infraestructura.
- Aseguramiento de la integridad de los sistemas a través de los procedimientos.
- Definición de la Baseline de la CI (configuración del ítem) antes del lanzamiento al entorno.
- El alcance ha de estar claramente definido y documentado.
- De igual modo habría que definir la configuración de la base de datos.
- No hay que olvidar la gestión del cambio, basada en el aseguramiento de que los cambios estén:

- Auditados.
- Aprobados.

- Implementados.
- Revisados.

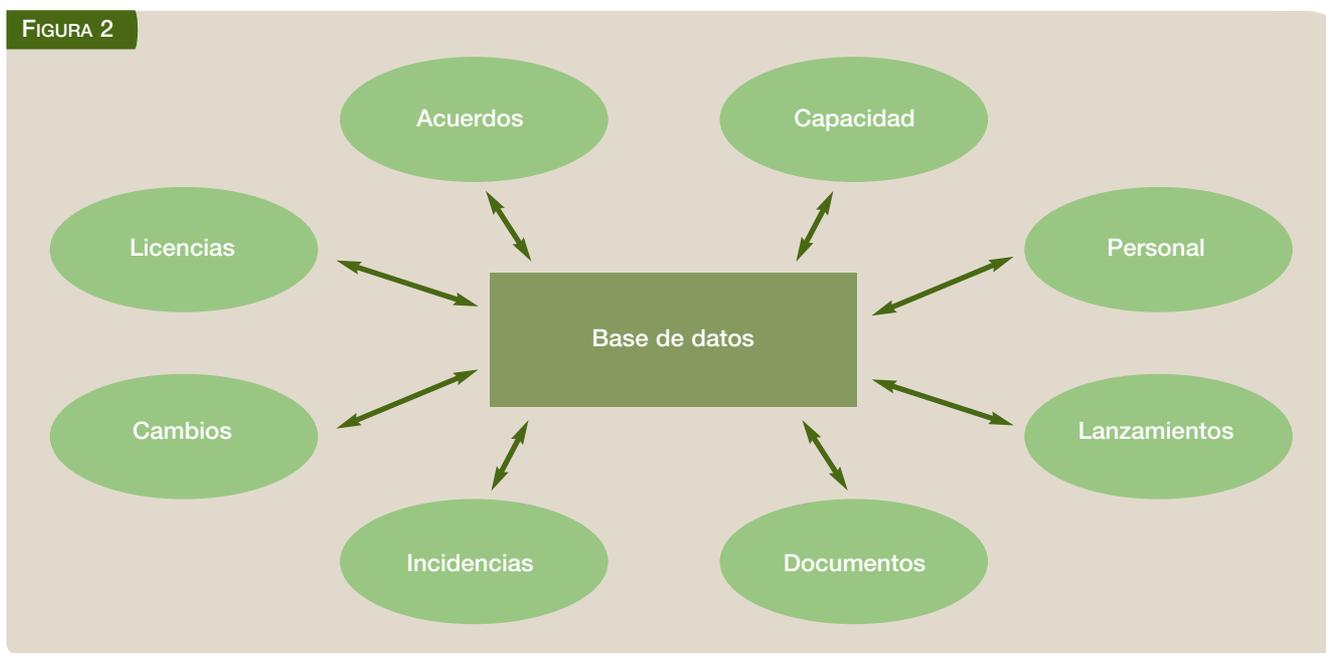
En materia de configuración habría que definir la configuración de la base de datos y la gestión del ítem (*figura 2*).

d) *Proceso de lanzamiento*. Identificando actividades de control y *reporting*. Nos deberíamos hacer las siguientes preguntas cuando nos encontramos en esta etapa.

- ¿Existe algún mecanismo de gestión y de control del lanzamiento de una *baseline*?
- ¿Existe algún proceso de *back-out*?
- ¿Se registran los proyectos con todo detalle?
- ¿Se prueban todos los lanzamientos?
- ¿Se informa sobre los incidentes producidos?
- ¿Son analizados los lanzamientos fallidos o exitosos?

e) *Proceso de resolución*. La gestión de incidencias y de problemas son

FIGURA 2



procesos separados, aunque estén estrechamente unidos.

La gestión de incidencias tiene que informar sobre la resolución del servicio solicitado lo antes posible.

Respecto a la gestión de problemas, se ha de:

- Responder al servicio requerido.
- Grabar todos los problemas identificados.
- Documentar procedimientos de resolución de problemas.
- Generar acciones preventivas.

- Tener un proceso definido de gestión de cambios con la finalidad de tener un histórico del problema.
- Revisar la efectividad en la resolución de un problema.
- Registrar las acciones de mejora.

Básicamente, éstos serían los requisitos a considerar. Con ello queda clara la complejidad de este tipo de sistemas.

En materia de auditoría de certificación, por el momento, la entidades de acreditación (ENAC, UKAS, RVA...) no

poseen esquema de acreditación, por lo que los certificados de ISO 20000 han de llevar el registro del ITSMP, lo cual garantizará la fiabilidad del proceso de auditoría.

El interés y la demanda de la normativa ISO 20000 crece de manera exponencial, por lo que nos encontramos, sin duda, ante una norma que dará mucho que hablar en el futuro. ■

Alejandro García
Vocal del Comité de Entidades de Certificación de la AEC

“El interés y la demanda de la normativa ISO 20000 crece de manera exponencial, por lo que nos encontramos, sin duda, ante una norma que dará mucho que hablar en el futuro”

