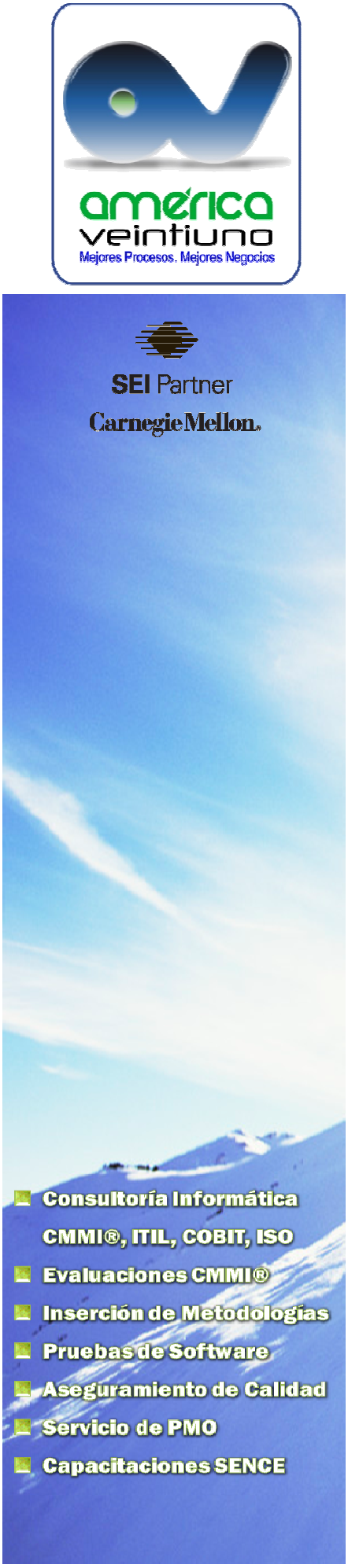


Normas ISO

INTRODUCCIÓN

La **Organización Internacional para la Normalización** o **ISO** (del griego, ἴσος (*isos*), 'igual', y cuyo nombre en inglés es *International Organization for Standardization*), nacida tras la Segunda Guerra Mundial (23 de febrero de 1947), es el organismo encargado de promover el desarrollo de normas internacionales de fabricación, comercio y comunicación para todas las ramas industriales a excepción de la eléctrica y la electrónica. Su función principal es la de buscar la estandarización de normas de productos y seguridad para las empresas u organizaciones a nivel internacional.

La ISO es una red de los institutos de normas nacionales de 160 países, sobre la base de un miembro por país, con una Secretaría Central en Ginebra (Suiza) que coordina el sistema.

Las normas desarrolladas por ISO son voluntarias, comprendiendo que ISO es un organismo no gubernamental y no depende de ningún otro organismo internacional, por lo tanto, no tiene autoridad para imponer sus normas a ningún país.

Los Estándares mas conocidos ámbito informático y tenemos capacidad de implementar son: ISO 9000 - 20000 - 27000 - 29119 - 12207 - 9126

NORMAS ISO DISPONIBLES

ISO 9000

La norma ISO 9000 es un estándar para sistemas de administración de la calidad. La norma es publicada y mantenida por la ISO (Organización Internacional para la estandarización, aunque ISO no es un acrónimo y solo sugiere igualdad), mientras que es administrada por entidades externas de acreditación y certificación. Lo que certifica la norma es el ajuste a las especificaciones del producto o servicio, y no el concepto popular de calidad como algo objetivamente bueno.

La ISO como organización no otorga directamente la certificación, sino que lo hacen organismos de acreditación certificados. El proceso de certificación se lleva a cabo mediante un proceso auditorias, llevadas a cabo por auditores externos a la compañía en cuestión; los procesos de auditorias están normados asimismo por la ISO 19011. La empresa se debe preparar para su certificación, asegurando de que todos sus procesos se ajusten a los requerimientos de la norma. Una vez obtenida la certificación, esta debe ser renovada a intervalos regulares, lo que es determinado por el organismo certificador.

En estricto rigor, la certificación que se obtiene es la de ISO 9001:2000, ya que la norma consta de una serie de documentos, entre los cuales este es el específico sobre los requerimientos de un sistema de aseguramiento de la calidad. La sección ISO 9000:2000 del documento, consta de los fundamentos de la norma y del vocabulario, y la sección 9004, contiene guías para el mejoramiento en es desempeño de un sistema.

Actualmente existe:

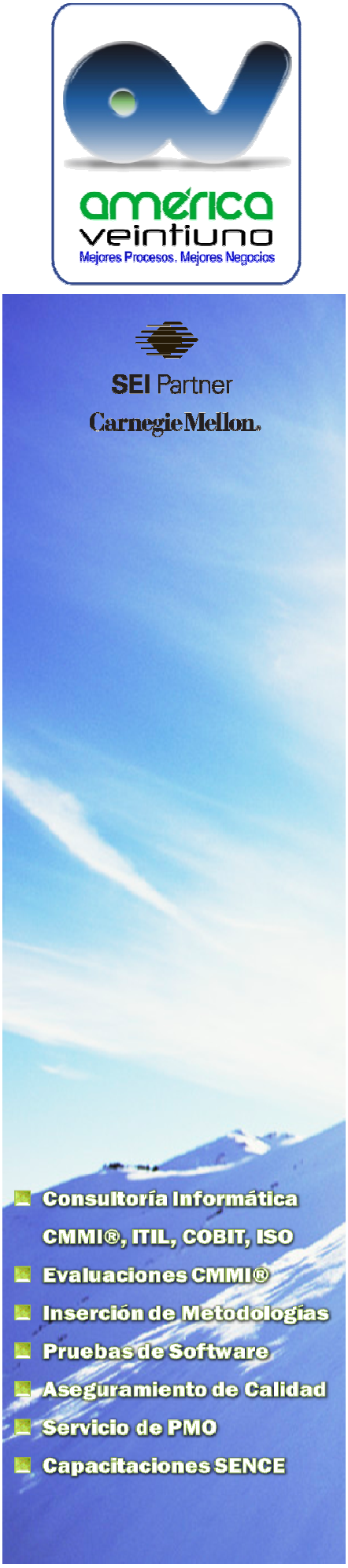
ISO 9001:2008: requisitos para certificarse

ISO 9000:2008: Fundamentos y Glosario

ISO 9004:2008: Guía para la Mejora

ISO 20000

La serie **ISO/IEC 20000 - Service Management** normalizada y publicada por las organizaciones ISO e IEC el 14 de



Normas ISO

diciembre de 2005, es el estándar reconocido internacionalmente en gestión de servicios de TI (Tecnologías de la Información).

La ISO/IEC 20000 es totalmente compatible con la ITIL (IT Infrastructure Library), o guía de mejores prácticas para el proceso de GSTI. La diferencia es que el ITIL no es medible y puede ser implantado de muchas maneras, mientras que en la ISO/IEC 20000, las organizaciones deben ser auditadas y medidas frente a un conjunto establecido de requisitos.

La ISO/IEC 20000 es aplicable a cualquier organización, pequeña o grande, en cualquier sector o parte del mundo donde confían en los servicios de TI. La norma es particularmente aplicable para proveedores de servicios internos de TI, tales como departamentos de Información Tecnológica, proveedores externos de TI o incluso organizaciones subcontratadas. La norma está impactando positivamente en algunos de los sectores que necesitan TI tales como subcontratación de negocios, Telecomunicaciones, Finanzas y el Sector Público.

ISO 27000

La serie de normas ISO/IEC 27000 son estándares de seguridad publicados por la ISO y la IEC.

La serie contiene las mejores prácticas recomendadas en Seguridad de la información para desarrollar, implementar y mantener Especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI). la mayoría de estas normas se encuentran en preparación e incluyen:

ISO/IEC 27000 - es un vocabulario estándar para el SGSI. Se encuentra en desarrollo actualmente.

ISO/IEC 27001 - es la certificación que deben obtener las organizaciones. Norma que especifica los requisitos para la implantación del SGSI. Es la norma más importante de la familia. Adopta un enfoque de gestión de riesgos y promueve la mejora continua de los procesos. Fue publicada como estándar internacional en octubre de 2005.

ISO/IEC 27002 - Information technology - Security techniques - Code of practice for information security management. Previamente BS 7799 Parte 1 y la norma ISO/IEC 17799. Es código de buenas prácticas para la gestión de seguridad de la información.

ISO/IEC 27003 - son directrices para la implementación de un SGSI. Es el soporte de la norma ISO/IEC 27001. Publicada el 1 de febrero del 2010, No esta certificada actualmente.

ISO/IEC 27004 - son métricas para la gestión de seguridad de la información. Es la que proporciona recomendaciones de quién, cuándo y cómo realizar mediciones de seguridad de la información. Publicada el 7 de diciembre del 2009, no se encuentra traducida al español actualmente.