ISO/IEC 27000-series

La serie de normas ISO/IEC 27000 son estándares de seguridad publicados por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (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. Introducción y base para el resto. Tercera versión: enero de 2014. Quinta versión: febrero 2018. ISO/IEC 27000:2018

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. Revisada en septiembre de 2013.

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. Fue publicada en julio de 2005 como ISO 17799:2005 y recibió su nombre oficial ISO/IEC 27002:2005 el 1 de julio de 2007. Última versión: 27002:2013, de setiembre de 2013.

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 de 2010. No es certificable.

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 de 2009, no se encuentra traducida al español actualmente.

ISO/IEC 27005 - trata la gestión de riesgos en seguridad de la información. Es la que proporciona recomendaciones y lineamientos de métodos y técnicas de evaluación de riesgos de Seguridad en la Información, en soporte del proceso de gestión de riesgos de la norma ISO/IEC 27001. Es la más relacionada a la actual British Standard BS 7799 parte 3. Publicada en junio de 2008. Revisada en junio de 2011.

ISO/IEC 27006 - Requisitos para la acreditación de las organizaciones que proporcionan la certificación de los sistemas de gestión de la seguridad de la información. Esta norma especifica requisitos específicos para la certificación de SGSI y es usada en conjunto con la norma 17021-1, la norma genérica de acreditación. Publicada en 2007 y revisada en diciembre de 2011 y septiembre de 2015.

ISO/IEC 27007 - es una guía para auditar al SGSI. Publicada en noviembre de 2011.

ISO/IEC 27008 - es una guía para auditar los controles seleccionados para implantar un SGSI. No es certificable. Publicada en octubre de 2011.

ISO/IEC 27009 - detalla los requisitos para usar la norma ISO/IEC 27001 en cualquier otro ámbito. No es certificable. Publicada en junio de 2016.

ISO/IEC 27010 - es una guía para gestionar la seguridad de la información cuando se comparte entre distintas organizaciones. Es aplicable a todas las formas de intercambio y difusión de información. Publicada en octubre de 2012 y revisada en noviembre de 2015.

ISO/IEC 27011 - es una guía de interpretación de la información y gestión de la seguridad de esta información en organizaciones del sector de telecomunicaciones. Publicada en diciembre de 2008 y fue revisada en diciembre de 2016.

ISO/IEC 27014 - es una guía de gobierno corporativo de la seguridad de la información. Publicada en abril de 2013.

ISO/IEC 27015 - es una guía de SGSI orientada a organizaciones del sector financiero y de seguros. Publicada en noviembre de 2012.

ISO/IEC 27016 - es una norma que se concentra en un análisis financiero y económico de equipos y procedimientos de la seguridad de la información. Publicada en febrero de 2014.

ISO/IEC 27017 - es una guía de seguridad para Cloud Computing. Publicada en diciembre de 2015.

ISO/IEC 27018 - es una guía para controlar la protección de datos para servicios de computación en cloud computing. Publicado en julio de 2014.

ISO/IEC 27031 - es una guía de apoyo para la adecuación de las tecnologías d ela información y comunicación. No es certificable. Publicada en marzo de 2011.

ISO/IEC 27035:2011 - Seguridad de la información – Técnicas de Seguridad – Gestión de Incidentes de Seguridad. Este standard hace foco en las actividades de: detección, reporte y evaluación de incidentes de seguridad y sus vulnerabilidades. Publicada en agosto de 2011.1

ISO/IEC 27038 - es una guía de especificación para seguridad en la redacción digital.

ISO/IEC 27039 - es una guía para la selección, despliegue y operación de sistemas de detección y prevención de intrusión.

ISO/IEC 27040 - es una guía para la seguridad en medios de almacenamiento.

ISO/IEC 27041 - es una guía para garantizar la idoneidad y adecuación de los métodos de investigación.

ISO/IEC 27042 - es una guía con directrices para el análisis e interpretación de las evidencias digitales.

ISO/IEC 27043 - desarrolla principios de investigación para la recopilación de evidencias digitales.

ISO/IEC 27050 - desarrolla en tres partes sobre la información almacenada en dispositivos electrónicos.

ISO/IEC 27103:2018 - es una norma desarrollada para proporcionar orientación sobre cómo aprovechar las normas existentes en un marco de ciberseguridad.

ISO/IEC 27799:2008 - es una guía para implementar ISO/IEC 27002 en la industria de la salud.