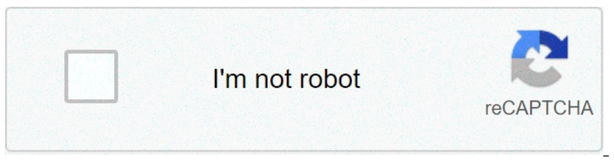

Continue

Iso 27001 versión 2013 pdf download español

You're Reading a Free Preview Pages 7 to 9 are not shown in this preview. You're Reading a Free Preview Pages 16 to 33 are not shown in this preview. Este artículo o sección necesita referencias que aparezcan en una publicación acreditada.Este aviso fue puesto el 14 de septiembre de 2011. ISO/IEC 27001 es un estándar para la seguridad de la información (Information technology - Security techniques - Information security management systems - Requirements) aprobado y publicado como estándar internacional en octubre de 2005 por International Organization for Standardization y por la comisión International Electrotechnical Commission.[1] Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI) según el conocido como "Ciclo de Deming": PDCA - acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar). Es consistente con las mejores prácticas descritas en ISO/IEC 27002, anteriormente conocida como ISO/IEC 17799, con orígenes en la norma BS 7799-2:2002, desarrollada por la entidad de normalización británica, la British Standards Institution (BSI). Estructura España La versión actual de la norma (NTC-ISO-IEC 27001:2013) se encuentra normalizada por el Instituto Madrileño de Normas y Técnicas y Certificación IMONTEC.[2] Dicha norma es una adopción idéntica (IDT) por traducción de la norma ISO/IEC 27001:2013.[2] La norma se encuentra dividida en dos partes; la primera se compone de 10 puntos entre los cuales se encuentran: Objeto y campo de aplicación: Especifica la finalidad de la norma, su uso dentro de una organización y el modo de aplicación del estándar. Referencias normativas: recomendación de la consulta a documentos necesarios para la aplicación del estándar. Término y definiciones: Los términos y definiciones usados se basan en la norma ISO/IEC 27000. Contexto de la organización: Se busca determinar las necesidades y expectativas dentro y fuera de la organización que afecten directa o indirectamente al sistema de gestión de la seguridad de la información (SGSI). Adicional a esto, se debe determinar el alcance. Entendiendo la organización y su contexto Entendiendo las necesidades y expectativas de los implicados Determinando el campo de aplicación del SGSI Sistema de gestión de la seguridad de la información Liderazgo: Habla sobre la importancia de la alta dirección y su compromiso con el sistema de gestión, estableciendo políticas y asignando a los empleados de la organización roles, responsabilidades y autoridades, asegurando así la integración de los requisitos del sistema de seguridad en los procesos de la organización, así como los recursos necesarios para su implementación y operatividad. Liderazgo y compromiso Políticas Roles organizativos, responsabilidad y autoridades Planificación: Se deben valorar, analizar y evaluar los riesgos de seguridad de acuerdo a los criterios de aceptación de riesgos, adicionalmente se debe dar un tratamiento a los riesgos de la seguridad de la información. Los objetivos y los planes para lograr dichos objetivos también se deben definir en este punto. Acciones para abordar riesgos y oportunidades Objetivos de la seguridad de la información y cómo conseguirlos Soporte: Se trata sobre los recursos destinados por la organización, la competencia de personal, la toma de conciencia por parte de las partes interesadas, la importancia sobre la comunicación en la organización. La importancia de la información documentada, también se trata en este punto. Recursos Competencias Concienciación Comunicación Información documentación Operación: El cómo se debe planificar, implementar y controlar los procesos de la operación, así como la valoración de los riesgos y su tratamiento. Planificación operacional Evaluación de riesgos Tratamiento de los riesgos Evaluación de desempeño: Debido a la importancia del ciclo PHVA (Planificar, Hacer, Verificar, Actuar), se debe realizar un seguimiento, una medición, un análisis, una evaluación, una auditoría interna y una revisión por la dirección del SGSI del sistema de gestión de la información, para asegurar su correcto funcionamiento. Supervisión, medida, análisis y evaluación Auditorías internas Revisiones de la gestión Mejora: Habla sobre el tratamiento de las no conformidades, las acciones correctivas y a mejora continua. Disconformidades y acciones correctivas Mejora continuada La segunda parte, esta conformada por el anexo A, el cual establece los objetivos de control y los controles de referencia.[2] Evolución España En el año 2004 se publicó la UNE 71502 titulada Especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI) y que fue elaborada por el comité técnico AEN/CTN 71. Es una adaptación nacional de la norma británica British Standard BS 7799-2:2002. Con la publicación de UNE-ISO/IEC 27001 (traducción al español del original inglés) dejó de estar vigente la UNE 71502 y las empresas nacionales certificadas en esta última están pasando progresivamente sus certificaciones a UNE-ISO/IEC 27001. ISO 27001:2013 Existen varios cambios con respecto a la versión 2005 en esta versión 2013. Entre ellos destacan:[3] Desaparece la sección "enfoque a procesos" dando mayor flexibilidad para la elección de metodologías de trabajo para el análisis de riesgos y mejoras. Cambia su estructura conforme al anexo SL común al resto de estándares de la ISO. Pasa de 102 requisitos a 130. Considerables cambios en los controles establecidos en el Anexo A, incrementando el número de dominios a 14 y disminuyendo el número de controles a 114. Inclusión de un nuevo dominio sobre "Relaciones con el Proveedor" por las crecientes relaciones entre empresa y proveedor en la nube. Se parte del análisis de riesgos para determinar los controles necesarios y compararlos con el Anexo A, en lugar de identificar primero los activos, las amenazas y sus vulnerabilidades. Beneficios que aporta este a los objetivos de la organización Demuestra la garantía independiente de los controles internos y cumple los requisitos de gestión corporativa y de continuidad de la actividad comercial. Demuestra independientemente que se respetan las leyes y normativas que sean de aplicación. Proporciona una ventaja competitiva al cumplir los requisitos contractuales y demostrar a los clientes que la seguridad de su información es primordial. Verifica independientemente que los riesgos de la organización estén correctamente identificados, evaluados y gestionados al tiempo que formaliza unos procesos, procedimientos y documentación de protección de la información. Demuestra el compromiso de la cúpula directiva de su organización con la seguridad de la información. El proceso de evaluaciones periódicas ayuda a supervisar continuamente el rendimiento y la mejora. Nota: las organizaciones que simplemente cumplen la norma ISO/IEC 27001 o las recomendaciones de la norma del código profesional, ISO/IEC 27002 no logran estas ventajas. Implantación La implantación de ISO/IEC 27001 en una organización es un proyecto que suele tener una duración entre 6 y 12 meses, dependiendo del grado de madurez en seguridad de la información y el alcance, entendiendo por alcance el ámbito de la organización que va a estar sometido al Sistema de Gestión de la Seguridad de la Información elegido. En general, es recomendable la ayuda de consultores externos. Artículo principal: Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales Aquellas organizaciones que hayan adecuado previamente de forma rigurosa sus sistemas de información y sus procesos de trabajo a las exigencias de las normativas legales de protección de datos (p.ej., en España la conocida LOPD y sus normas de desarrollo, siendo el más importante el Real Decreto 1720/2007, de 21 de diciembre de desarrollo de la Ley Orgánica de Protección de Datos) o que hayan realizado un acercamiento progresivo a la seguridad de la información mediante la aplicación de las buenas prácticas de ISO/IEC 27002, partirán de una posición más ventajosa a la hora de implantar ISO/IEC 27001. El equipo de proyecto de implantación debe estar formado por representantes de todas las áreas de la organización que se vean afectadas por el SGSI, liderado por la dirección y asesorado por consultores externos especializados en seguridad informática generalmente Ingenieros o Ingenieros Técnicos en Informática, derecho de las nuevas tecnologías, protección de datos y sistemas de gestión de seguridad de la información (que hayan realizado un curso de implantador de SGSI). Certificación La certificación de un SGSI es un proceso mediante el cual una entidad de certificación externa, independiente y acreditada audita el sistema, determinando su conformidad con ISO/IEC 27001, su grado de implantación real y su eficacia y, en caso positivo, emite el correspondiente certificado. Antes de la publicación del estándar ISO 27001, las organizaciones interesadas eran certificadas según el estándar británico BS 7799-2. Desde finales de 2005, las organizaciones ya pueden obtener la certificación ISO/IEC 27001 en su primera certificación con éxito o mediante su recertificación trienal, puesto que la certificación BS 7799-2 ha quedado reemplazada. El Anexo C de la norma muestra las correspondencias del Sistema de Gestión de la Seguridad de la Información (SGSI) con el Sistema de Gestión de la Calidad según ISO 9001:2000 y con el Sistema de Gestión Medio Ambiental según ISO 14001:2004 (ver ISO 14000), hasta el punto de poder llegar a certificar una organización en varias normas y con base en un sistema de gestión común. Serie 27000 Artículo principal: ISO/IEC 27000-series La seguridad de la información tiene asignada la serie 27000 dentro de los estándares ISO/IEC: ISO 27000: Publicada en mayo de 2009. Contiene la descripción general y vocabulario a ser empleado en toda la serie 27000. Se puede utilizar para tener un entendimiento más claro de la serie y la relación entre los diferentes documentos que la conforman. UNE-ISO/IEC 27001:2007 "Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos". Fecha de la de la versión española 29 de noviembre de 2007. Es la norma principal de requisitos de un Sistema de Gestión de Seguridad de la Información. Los SGSIs deberán ser certificados por auditores externos a las organizaciones. En su Anexo A, contempla una lista con los objetivos de control y controles que desarrolla la ISO 27002 (anteriormente denominada ISO 17799). ISO/IEC 27002: (anteriormente denominada ISO 17799). Guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información con 11 dominios, 39 objetivos de control y 133 controles. ISO/IEC 27003: En fase de desarrollo; probable publicación en 2009. Contendrá una guía de implementación de SGSI e información acerca del uso del modelo PDCA y de los requisitos de sus diferentes fases. Tiene su origen en el anexo B de la norma BS 7799-2 y en la serie de documentos publicados por BSI a lo largo de los años con recomendaciones y guías de implantación. ISO 27004: Publicada en diciembre de 2009. Especifica las métricas y las técnicas de medida aplicables para determinar la eficiencia y eficacia de la implantación de un SGSI y de los controles relacionados. ISO 27005: Publicada en junio de 2008. Consiste en una guía para la gestión del riesgo de la seguridad de la información y sirve, por tanto, de apoyo a la ISO 27001 y a la implantación de un SGSI. Incluye partes de la ISO 13335. ISO 27006: Publicada en febrero de 2007. Especifica los requisitos para acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información. Otros SGSI SOGP Otro SGSI que compite en el mercado es el llamado "Information Security Forum's Standard of Good Practice" (SOGP). Este SGSI es más una "best practice" (buenas prácticas), basado en las experiencias del ISF. ISM3 Information Security Management Maturity Model ("ISM3") (conocida como ISM-cubed o ISM3) está construido en estándares como ITIL, ISO 20000, ISO 9001, CMM, ISO/IEC 27001,[4] e información general de conceptos de seguridad de los gobiernos. ISM3 puede ser usado como plantilla para un ISO 9001 compliant. Mientras que la ISO/IEC 27001 está basada en controles. ISM3 está basada en proceso e incluye métricas de proceso. COBIT En el caso de COBIT, los controles son aún más amplios que en la ISO-IEC 27001. La versión más actual es la COBIT 2019. Herramientas PILAR: Herramienta que permite realizar el análisis de riesgos. SECITOR: Herramienta de Análisis y Gestión de Riesgos de alto nivel que permite la gestión integral de la Seguridad de la Información siendo un sistema multimarco (ISO 27001, Protección de datos, ISO 19001, ENS, etc), además de una monitorización en tiempo real de la seguridad de la organización, siendo integrable con Nagios, OCS inventory, Splunk, SIEM, directorio activo, pilar, etc. Véase también Ley Orgánica de Protección de Datos de Carácter Personal de España Privacidad SGSI Seguridad de la información Seguridad informática Referencias ↑ «¿Conoces la nueva norma para la gestión de la privacidad?» (html). Instituto Nacional de Ciberseguridad. 10 de octubre de 2019. Archivado desde el original el 11 de octubre de 2019. Consultado el 11 de octubre de 2019. «Así, en 2005, la norma ISO 27001 se convirtió en una norma internacional de referencia para gestionar y garantizar la seguridad de la información en empresas y organizaciones. Esta norma se ha tomado como punto de partida para el desarrollo de normas que verifiquen el cumplimiento del RGPD, ya que ampara los datos de clientes o proveedores ya se encuentren en activos digitales o impresos de cualquier organización.» ↑ a b c IMONTEC (2015). IMONTEC, ed. Compendio seguridad de la información (Segunda edición edición). España: IMONTEC Internacional. ISBN 978-958-8585-53-6. ↑ Estaban, Luis (27 de septiembre de 2013). «Nueva versión ISO/IEC 27001:2013» (html). Instituto Nacional de Ciberseguridad. Archivado desde el original el 10 de marzo de 2020. Consultado el 9 de marzo de 2020. ↑ «ISO/IEC 27701:2019» (html). Organización Internacional de Normalización (en inglés). agosto de 2019. Archivado desde el original el 6 de agosto de 2019. Consultado el 11 de octubre de 2019. «Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines». ISO/IEC 27001:2005 Information technology — Security techniques — Information security management systems - Requirements ISO/IEC 27005:2008 Information technology — Security techniques — Information security risk management ISO/IEC 27006:2007 Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems ISO/IEC 27002:2005 Information technology — Security techniques — Code of practice for information security management (anterior ISO/IEC 17799:2005) ISO 9001:2000, Quality management systems — Requirements ISO/IEC 13335-1:2004, Information technology — Security techniques — Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security management ISO/IEC TR 13335-3:1998, Information technology — Guidelines for the management of IT Security — Part 3: Techniques for the management of IT security ISO/IEC TR 13335-4:2000, Information technology — Guidelines for the management of IT Security — Part 4: Selection of safeguards ISO 14001:2004, Environmental management systems — Requirements with guidance for use ISO/IEC TR 18044:2004, Information technology — Security techniques — Information security incident management ISO 19011:2002, Guidelines for quality and/or environmental management systems auditing ISO 90011:2003, GUILLEN AUIDIT ENVIROMENTAL Enlaces externos Norma ISO 27001: importancia para la seguridad de la información, Telefónica. British Standards Institution, BSI www.pmg-ssi.com Blog dedicado en exclusiva a la norma ISO 27001 y el Programa de Mejoramiento de la Gestión ISO JTC 1/SC 27: Página del subcomité ISO/IEC a cargo de normas de seguridad informática ISO 27001.es: Portal en español con información sobre la serie ISO 27000. [1]: Vídeo 5 aspectos importantes sobre la implantación ISO 27001. Blog que muestra noticias e información tecnológica Datos: Q852641 Obtenido de « iso 27001 versión 2013 pdf download español