Normas para la seguridad de la información: una visión general

André Saeckel

Experto en normas DQS para la seguridad de la información

nov. 12 , 2022

Normas de seguridad de la información

Seguridad de la información frente a seguridad informática

En una época en la que los datos y la información se comercializan como si fueran mercancías, es esencial protegerlos. Una forma de hacerlo es aplicar una gestión de la seguridad de la información basada en la serie de normas de seguridad de la información ISO/IEC 2700x. Se trata de una familia internacional de normas para la seguridad informática y de la información en organizaciones privadas, públicas o sin ánimo de lucro. Sobre la base de la norma ISO 27001, se puede implementar un sistema de gestión de la seguridad de la información (SGSI) que las organizaciones y las autoridades públicas pueden establecer, aplicar y certificar para su propia protección.

CONTENIDO

Normas para la seguridad de la información: La familia de normas ISO 2700X

Las normas individuales para la seguridad de la información de la serie ISO 2700x tratan diversos temas en el ámbito de la seguridad de la información. Por ejemplo, la norma internacional especifica **ISO 27001** Un sistema de gestión de la seguridad de la información (SGSI), **ISO 27701** un sistema de gestión de la protección de datos, la norma ISO 27017 ofrece orientación sobre las medidas de seguridad de la información para la computación en la nube, y la norma ISO 27005 proporciona directrices para la gestión de los riesgos de seguridad de la información.

Las empresas de todos los sectores pueden beneficiarse del enfoque sistemáticamente estructurado de estas normas para la seguridad de la información. Permite proteger los datos confidenciales contra la pérdida y el uso indebido, y ayuda a identificar y reducir de forma fiable las amenazas (potenciales). El enfoque ayuda a garantizar la disponibilidad de los sistemas informáticos de la empresa, contribuyendo así a la optimización de los procesos empresariales, los costes de las TI y los procesos, y la minimización de los riesgos empresariales y de responsabilidad.

La certificación es una ventaja competitiva

La certificación según **la norma ISO 27001**, por ejemplo, por parte de **DQS**, requiere una cierta cantidad de preparación y esfuerzo. Sin embargo, la empresa proporciona una prueba documentada de que cumple los requisitos de seguridad de la información y aplica medidas para proteger los datos sensibles de la empresa. Esto supone una clara ventaja competitiva.

Diez normas ISO sobre seguridad de la información que debería conocer

La siguiente lista ofrece una visión general informativa del estado actual de la serie de normas ISO 2700x en materia de seguridad de la información. Todas las normas pueden adquirirse en el sitio web de la ISO.

ISO 27001 - Requisitos para los sistemas de gestión de la seguridad de la información

En una época en la que los datos y la información se negocian como si fueran mercancías raras, su protección es esencial. Una base óptima para la aplicación eficaz de una estrategia de seguridad holística la proporciona un sistema de gestión de la seguridad de la información (SGSI) bien estructurado de acuerdo con la norma **ISO 27001**. Se trata de una norma reconocida internacionalmente para la seguridad de la información en organizaciones privadas, públicas o sin ánimo de lucro, que no sólo cubre los aspectos de la seguridad informática.

ISO 27001 en la práctica

La guía de auditoría de DQS

La guía de auditoría de DQS (basada en ISO 27001:2013)

Benefíciese de buenas **preguntas de auditoría** y posible **evidencia** sobre controles seleccionados del Anexo A.

De expertos en la materia.

¡Es más que una simple lista de control! ¡Descargar ahora!

Un SGSI ISO 27001 define los requisitos, reglas y métodos para garantizar la seguridad de la información que requiere protección en las organizaciones. La norma ISO proporciona un modelo para establecer, implementar, supervisar y mejorar el nivel de protección. El objetivo es identificar los riesgos potenciales para la empresa, analizarlos y hacerlos controlables mediante las medidas adecuadas. La norma ISO 27001 formula los requisitos de dicho **sistema de gestión**, que se auditan en el marco de un **proceso de certificación** externa **.**

Con la norma se puede conseguir

- Hacer de la seguridad de la información sensible una parte integral de los procesos corporativos.
- Salvaguardar de forma preventiva los objetivos de protección de la confidencialidad, disponibilidad e integridad de la información
- Mantenimiento de la continuidad del negocio mediante la mejora continua del nivel de seguridad
- Sensibilización de los empleados y aumento significativo de la conciencia de seguridad en todos los niveles de la empresa
- Creación de confianza con las partes interesadas
- Establecimiento de un proceso eficaz de gestión de riesgos

ISO/IEC 27001:2013 Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información - Requisitos

La versión revisada se publicó el 25 de octubre de 2022. La versión actual ISO/IEC 27001:2013 expirará en octubre de 2025.

ISO 27019 - Medidas de seguridad de la información para el suministro de energía.

La norma ISO 27019 sobre seguridad de la información formula medidas complementarias para el sector de la industria energética.

ISO/IEC 27019:2017 Tecnología de la información - Técnicas de seguridad - Controles de seguridad de la información para la industria de suministro de energía

Qué puede hacer con la norma:

- Garantizar sistemáticamente los objetivos de protección de la confidencialidad, la disponibilidad y la integridad de la información.
- Mejorar continuamente el nivel de seguridad y la resistencia al acceso no autorizado
- Lograr una mayor seguridad de actuación y seguridad jurídica, mejorar la adhesión a los requisitos de cumplimiento pertinentes
- Aumentar la conciencia de seguridad entre los empleados y los directivos
- Lograr un alto nivel de confianza y lealtad entre todas las partes interesadas
- Demostrar una prueba reconocida de la eficacia de sus medidas de seguridad a las autoridades, como la Agencia Federal de Redes alemana (BNetzA)

ISO 27006 - Requisitos para los organismos de certificación

La norma ISO 27006 está dirigida a organismos como DQS que realizan certificaciones de sistemas de gestión de la seguridad de la información. La norma de acreditación ISO 27006 describe los requisitos que deben seguir los organismos de certificación al evaluar los sistemas de gestión de sus clientes según la norma ISO 27001 para su certificación.

ISO/IEC 27006:2021 Tecnología de la información - Técnicas de seguridad - Requisitos para los organismos que proporcionan la auditoría y certificación de los sistemas de gestión de la seguridad de la información

Esto incluye, por ejemplo, la prueba de los esfuerzos de auditoría especificados o las especificaciones sobre las calificaciones de los **auditores**. Los procesos de acreditación descritos en la norma garantizan que los certificados ISO 27001 emitidos por organismos de certificación acreditados tengan validez internacional.

Lo que se puede conseguir con esta norma

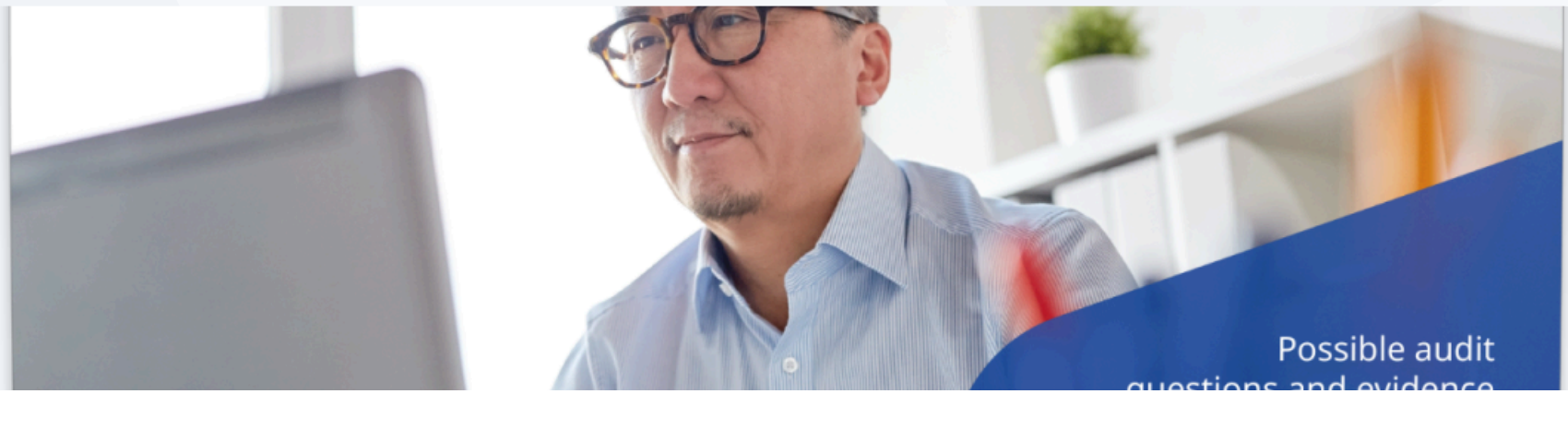
- Criterios uniformes para los procedimientos de auditoría de certificación, mantenimiento y recertificación
- Garantizar la validez de los certificados ISO 27001
- Garantizar los requisitos mínimos para el esfuerzo de auditoría y la calificación del personal que calcula y realiza los procedimientos de certificación

ISO 27002 - Orientación sobre los controles de seguridad de la información

El Sistema de Gestión de Seguridad de la Información (SGSI) según ISO 27001 contiene un Anexo A normativo: Controles y objetivos de control de referencia. Este Anexo contiene medidas específicas a ser implementadas como parte del sistema de gestión, según sea relevante para la organización. ISO 27002es una guía con recomendaciones para la implementación de medidas de ISO 27001.

La directriz se revisó y actualizó exhaustivamente a principios de 2022. La nueva edición brinda a los gerentes de seguridad de la información una guía de implementación precisa para garantizar que no se pase por alto ninguna medida importante para abordar el riesgo de seguridad de la información.

ISO/IEC 27002:2022 Seguridad de la información, ciberseguridad y protección de la privacidad - Controles de seguridad de la información



Guía de auditoría de ISO 27001

Anexo A

De nuestros expertos en la materia.

La directriz se basa en ISO/IEC 27001:2013.

Benefíciese de buenas preguntas de auditoría y posible evidencia sobre controles seleccionados en el Anexo A.

Más que una lista de verificación. ¡Descarga la Guía de Auditoría!

Puede hacerlo con la norma:

- Apoyo a la implementación de la norma ISO 27001
- Implementación de las recomendaciones para las medidas del Anexo A de la ISO 27001

ISO 27000 - Visión general y vocabulario de los sistemas de gestión de la seguridad de la información

La norma ISO 27000 contiene términos y definiciones que se utilizan en la serie de normas ISO 2700X. La norma ISO 27000 proporciona una visión general de los sistemas de gestión de la seguridad de la información y de la serie de normas ISO 2700x con sus normas de seguridad de la información.

ISO/IEC 27000:2018 Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información - Visión general y vocabulario

En un glosario, los términos (técnicos) se definen de manera explícita y formal.

Lo que puede hacer con esta norma:

- Glosario: cobertura de la mayoría de los términos técnicos utilizados en la serie de normas ISO2700x en el ámbito de la seguridad de la información.
- Claridad sobre la terminología
- Clara comprensión del vocabulario entre asesores y evaluadores ("un lenguaje común")
- Visión general de los sistemas de gestión de la seguridad de la información: introducción a la seguridad de la información, a la gestión de riesgos y de la seguridad y a los sistemas de gestión

ISO 27701 - Orientación sobre la gestión de la protección de datos

La norma para la seguridad de la información relacionada específicamente con la privacidad de los datos **ISO 27701** especifica un **sistema de gestión de la protección de datos** basado en las normas ISO 27001, ISO 27002 (controles de seguridad de la información) e ISO 29100 (marco de privacidad de los datos) para tratar adecuadamente tanto el tratamiento de los datos personales como la seguridad de la información. Esto se aplica tanto a los controladores como a los procesadores de datos personales.

y directrices

Cómo puede tener éxito con esta norma:

- Mejor gestión de los datos personales y de la seguridad de la información
- Aplicación más sencilla de los principios comunes de gestión de riesgos de la información a los datos personales
- Alinear y ampliar los controles dentro de la norma ISO 27001, así como la ISO 27002 relacionada

ISO 27017 - Guía de medidas de seguridad de la información en los servicios en la nube

La norma ISO 27017 proporciona orientación sobre las medidas de seguridad de la información en la computación en nube dentro de las normas de seguridad de la información.

ISO/IEC 27017:2015 Tecnología de la información - Técnicas de seguridad - Código de prácticas para los controles de seguridad de la información basados en la norma ISO/IEC 27002 para los servicios en la nube

Recomienda, apoya y proporciona medidas adicionales para implementar controles de seguridad de la información específicos para la nube.

Lo que puede lograr con esta norma:

- Comprender los aspectos de seguridad de la información de la computación en nube.
- Diseñar e implementar controles de seguridad de la información específicos para la nube
- Controlar las opciones de selección, implementación y gestión de la seguridad de la información para la computación en nube

ISO 27018 - Orientación sobre la protección de datos en los servicios en la nube.

La norma ISO 27018 proporciona orientación para garantizar que los proveedores de servicios en la nube ofrezcan controles de seguridad de la información adecuados para proteger la privacidad de los clientes de sus clientes, asegurando los datos personales que se les confían.

ISO/IEC 27018:2019 Tecnología de la información - técnicas - Código de prácticas para la protección de la información personal identificable (PII) en las nubes públicas que actúan como procesadores de PII

A esta norma le sigue la ISO 27017 (Medidas de seguridad de la información en los servicios en la nube), que cubre otros aspectos de la seguridad de la información en la computación en la nube además de la protección de datos.

Esto es lo que puedes hacer con la norma:

- Seleccionar los controles de protección de la IPI como parte de la implementación de un sistema de gestión de la seguridad de la información en la computación en nube basado en la norma ISO 27001.
- Implementar los controles de protección PII comúnmente aceptados.
- Profundizar en los conocimientos, ya que la norma se basa en la ISO 27002 y amplía sus consejos generales en algunas áreas
- Vincular los principios de privacidad de la OCDE plasmados en varias leyes y reglamentos de protección de datos

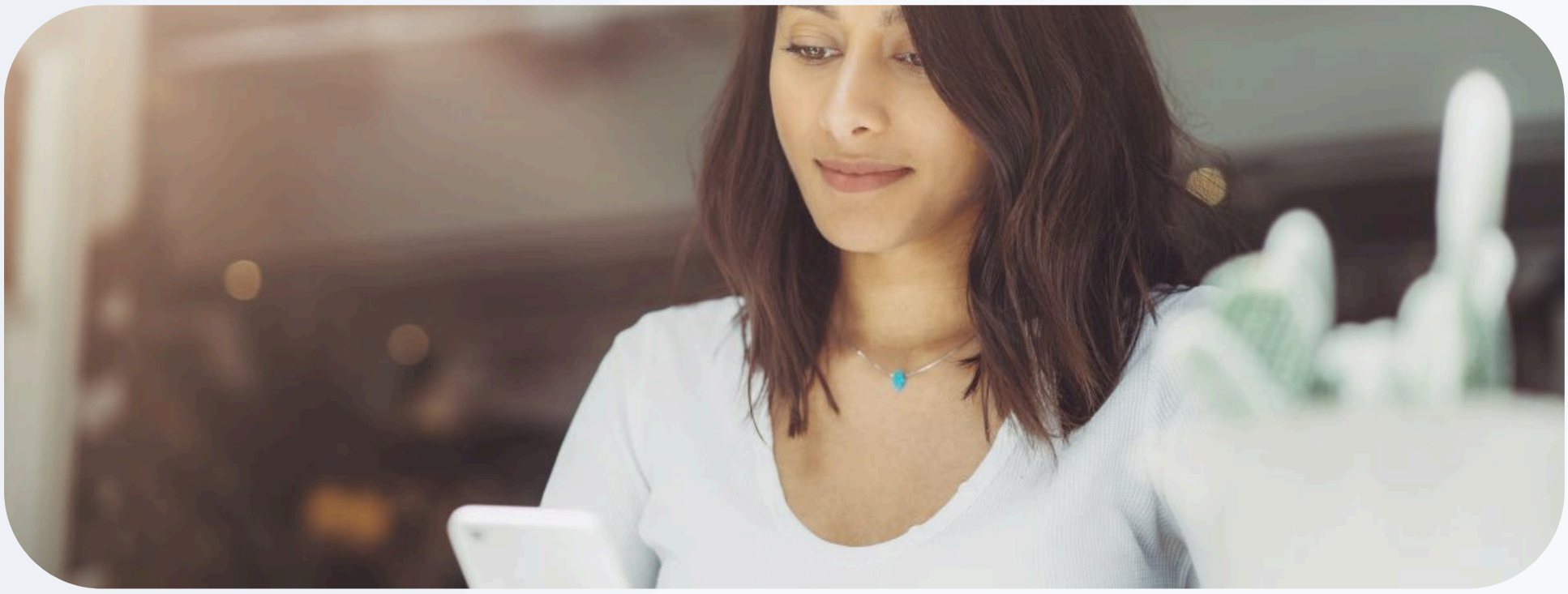
La norma ISO 27005 ofrece orientación sobre la gestión de riesgos de la seguridad de la información y apoya los conceptos generales al respecto establecidos en la norma ISO 27001.

ISO/IEC 27005:2018-07 Tecnología de la información - Técnicas de seguridad informática - Gestión de riesgos de seguridad de la información.

La norma ISO 27005 también pretende apoyar la implementación de la seguridad de la información basada en un concepto de gestión de riesgos.

Puede hacerlo con la norma:

- Implementar la seguridad de la información basada en un enfoque de gestión de riesgos.
- Definición del contexto de gestión de riesgos
- Evaluación cuantitativa o cualitativa (es decir, identificación, análisis y evaluación) de los riesgos de la información pertinentes
- Seguimiento y revisión continuos de los riesgos, tratamientos de riesgos, requisitos y criterios
- Tratamiento adecuado de los riesgos
- Comunicación continua de todas las partes interesadas



Never miss a thing...

Nuestro **boletín gratuito** le mantiene al día sobre auditorías, sistemas de gestión y certificaciones. Lea nuestros ejemplos de mejores prácticas y obtenga consejos para su agenda.

¡Quiero suscribirme!

ISO 27007 - Guía para auditar el SGSI

La norma ISO 27007 es una guía para la realización de auditorías y está dirigida a los auditores internos y externos que evalúan un SGSI según la norma ISO/IEC 27001.

ISO/IEC 27007:2020 Seguridad de la información, ciberseguridad y protección de la privacidad - Directrices para la auditoría de los sistemas de gestión de la

La guía se basa en gran medida en la Guía para la auditoría de sistemas de gestión (ISO 19011) y proporciona orientación adicional para un sistema de gestión de la seguridad de la información (SGSI).

A continuación se explica cómo puede tener éxito con la norma:

- Orientación específica para las auditorías del SGSI de la norma ISO 27001
- Orientación sobre la planificación y realización de auditorías integradas de la norma ISO 19011
- Información importante sobre las competencias de los auditores del SGSI
- Comprensión y realización de auditorías del SGSI

DQS - lo que podemos hacer por usted

DQS es un especialista líder en la certificación de sistemas y procesos de gestión desde 1985. Desde entonces, la historia de DQS ha estado estrechamente vinculada a la historia de la norma ISO 9001. Aportamos nuestro conocimiento mundial y nuestra amplia comprensión de las normas a nuestros clientes en unos 30.000 días de auditoría al año. Así podrá ver cuáles son sus opciones.

Confianza y experiencia

Nuestros textos y libros blancos están escritos exclusivamente por nuestros expertos en normas o auditores de larga trayectoria. Lo mismo ocurre con el resumen de las normas de seguridad de la información. Si tiene alguna pregunta sobre el contenido de los textos o sobre nuestros servicios a nuestro autor, no dude en ponerse en contacto con nosotros.

Normas de seguridad de la información: Otros temas de la familia de normas ISO 2700X

ISO 27003 - Guía para el desarrollo e implementación de un SGSI

ISO/IEC 27003:2017

Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información - Guía.

ISO 27004 - Guía para los métodos de medición de la gestión de la seguridad de la información

ISO/IEC 27004:2016

Tecnología de la información - Técnicas de seguridad - Gestión de la seguridad de la información - Seguimiento, medición, análisis y evaluación.

ISO 27008 - Guía para la evaluación de las medidas de seguridad de la información.

ISO/IEC TS 27008:2019

Tecnología de la información - Técnicas de seguridad - Directrices para la evaluación de los controles de seguridad de la información

ISO 27009 - Guía para la aplicación sectorial de un sistema de gestión de la información

ISO/IEC 27009:2020

Seguridad de la información, ciberseguridad y protección de la privacidad - Aplicación sectorial de la norma ISO/IEC 27001 - Requisitos

ISO 27010 - Guía sobre la gestión de la seguridad de la información para las comunicaciones intersectoriales e interorganizacionales

ISO/IEC 27010:2015

Tecnología de la información - Técnicas de seguridad - Gestión de la seguridad de la información para las comunicaciones intersectoriales e interorganizacionales

telecomunicaciones

ISO/IEC 27011:2016

Tecnología de la información - Técnicas de seguridad - Código de prácticas para los controles de seguridad de la información basados en la norma ISO/IEC 27002 para las organizaciones de telecomunicaciones

ISO 27013 - Guía para la implementación integrada de un SGSI y la gestión de servicios de TI

ISO/IEC 27013:2021

Seguridad de la información, ciberseguridad y protección de la privacidad - Guía para la implementación integrada de ISO/IEC 27001 e ISO/IEC 20000-1

ISO 27014 - "Gobierno" de la seguridad de la información

ISO/IEC DIS 27014:2020

Seguridad de la información, ciberseguridad y protección de la privacidad - Gobierno de la seguridad de la información

ISO 27016 - Economía de la gestión de la seguridad de la información

ISO/IEC TR 27016:2014

Tecnología de la información - Técnicas de seguridad - Gestión de la seguridad de la información - Economía de la organización

ISO 27021 - Requisitos para la competencia de los profesionales del SGSI

ISO/IEC 27021:2017/AMD 1:2021

Técnicas - Requisitos de competencia para los profesionales de los sistemas de gestión de la seguridad de la información - Enmienda 1: Adición de cláusulas o subcláusulas ISO/IEC 27001:2013 a los requisitos de competencia

ISO 27031 - Orientación sobre la continuidad del negocio

ISO/IEC 27031:2011

Tecnología de la información - Técnicas de seguridad - Directrices para la preparación de la tecnología de la información y la comunicación para la continuidad del negocio

CONSEJO: Lea nuestra entrada del blog sobre la gestión de la continuidad del negocio para saber qué recomienda la norma ISO 22301 para garantizar la continuidad de la empresa en situaciones excepcionales.

ISO 27032 - Guía de ciberseguridad

ISO/IEC 27032:2012

Tecnología de la información - Técnicas de seguridad - Guía de ciberseguridad

ISO 27033 - Guía sobre la seguridad de las redes

ISO/IEC 27033

Tecnología de la información - Técnicas de seguridad - Seguridad de la red
Parte 1: Visión general y conceptos, Parte 2: Directrices para el diseño y la implementación de la seguridad de la red, Parte 3: Escenarios de red de referencia -Amenazas, técnicas de diseño y cuestiones de control, Parte 4: Aseguramiento de las comunicaciones entre redes mediante pasarelas de seguridad, Parte 5: Aseguramiento de las comunicaciones entre redes mediante redes privadas virtuales (VPN), Parte 6: Aseguramiento del acceso a redes IP inalámbricas

ISO 27034 - Orientación sobre la seguridad de las aplicaciones

ISO/IEC 27034

seguridad

ISO 27035 - Guía para la gestión de incidentes de seguridad de la información

ISO/IEC 27035

Tecnología de la información - Prácticas de seguridad informática - Gestión de incidentes de seguridad de la información
Parte 1: Fundamentos de la gestión de incidentes, Parte 2: Directrices para la planificación y preparación de la respuesta a incidentes, Parte 3: Directrices para la respuesta a incidentes de tecnologías de la información y las comunicaciones (borrador)

ISO 27036 - Orientación sobre las relaciones con los proveedores

ISO/IEC 27036

Tecnología de la información - Técnicas de seguridad - Seguridad de la información para las relaciones con los proveedores
Parte 1: Visión general y conceptos, Parte 2: Requisitos, Parte 3: Directrices para la seguridad de la cadena de suministro de las tecnologías de la información y las comunicaciones, Parte 4: Directrices para la seguridad de los servicios en la nube

ISO 27037 - Directrices para el manejo de la evidencia digital.

ISO/IEC 27037:2012

Tecnología de la información - Técnicas de seguridad - Directrices para la identificación, recogida, adquisición y preservación de las pruebas digitales

ISO 27038 - Especificación para la redacción digital

ISO/IEC 27038:2014

Tecnología de la información - Técnicas de seguridad - Especificación para la redacción digital

ISO 27039 - Guidance on intrusion detection systems (IDPS)

ISO/IEC 27039:2015

Tecnología de la información - Técnicas de seguridad - Selección, despliegue y operaciones de los sistemas de detección y prevención de intrusiones (IDPS)

ISO 27040 - Orientación sobre la seguridad del almacenamiento

ISO/IEC 27040:2015

Tecnología de la información - Técnicas de seguridad - Seguridad del almacenamiento

ISO 27041 - Guidance on incident investigation methods (Guía sobre métodos de investigación de incidentes)

ISO/IEC 27041:2015

Tecnología de la información - Técnicas de seguridad - Guía para asegurar la idoneidad y adecuación del método de investigación de incidentes

ISO 27042 - Orientación sobre el análisis y la interpretación de las pruebas digitales.

ISO/IEC 27042:2015

Tecnología de la información - Técnicas de seguridad - Directrices para el análisis y la interpretación de las pruebas digitales

ISO 27043 - Guía sobre los procesos de investigación de incidentes.

ISO/IEC 27043:2015

Tecnología de la información - Técnicas de seguridad - Principios y procesos de investigación de incidentes.

ISO/IEC 27050

Tecnología de la información - Detección electrónica
Parte 1: Visión general y conceptos, Parte 2: Guía para el gobierno y la gestión de la detección electrónica, Parte 3: Código de prácticas para la detección electrónica

ISO 27102 - Orientación sobre el ciberseguro

ISO/IEC 27102:2019

Gestión de la seguridad de la información - Directrices para el ciberseguro

ISO 27103 - Guía sobre ciberseguridad y normas ISO/IEC

ISO/IEC TR 27103:2018

Tecnología de la información - Técnicas de seguridad - Ciberseguridad y normas ISO e IEC

ISO 27550 - Ingeniería de la privacidad para los procesos del ciclo de vida del sistema

ISO/IEC TR 27550:2019-09

Tecnología de la información - Técnicas de seguridad - Ingeniería de la privacidad para los procesos del ciclo de vida del sistema

ISO 27799 - Gestión de la seguridad de la información en el sector sanitario

ISO 27799:2016

Informática de la salud - Gestión de la seguridad de la información en la salud utilizando la norma ISO/IEC 27002

Autor

André Saeckel

Director de producto en DQS para la gestión de la seguridad de la información. Como experto en normas para el área de la seguridad de la información y el catálogo de seguridad informática (infraestructuras críticas), André Säckel es responsable, entre otras, de las siguientes normas y estándares específicos del sector ISO 27001, ISIS12, ISO 20000-1, KRITIS y TISAX (seguridad de la información en la industria automotriz). También es miembro del grupo de trabajo ISO/IEC JTC 1/SC 27/WG 1 como delegado nacional del Instituto Alemán de Normalización DIN.