**Conjunto de estándares de la familia ISO 27000**

* **ISO 27001:** Especifica los requerimientos necesarios para implantar y gestionar un SGSI. Es la norma más importante de la familia y es certificable.
* **ISO 27002:** en soporte del proceso de gestión de riesgos de la norma ISO/IEC-27001, define un conjunto de buenas prácticas para la implantación del SGSI, a través de 93 controles, estructurados en 4 grandes dominios.
* **ISO 27003**: proporciona una guía para la implantación de forma correcta de un SGSI, centrándose en los aspectos importantes para realizar con éxito dicho proceso.
* **ISO 27004:**proporciona pautas orientadas a la correcta definición y establecimiento de métricas que permitan evaluar de forma correcta el rendimiento del SGSI.
* **ISO 27005:**define cómo se debe realizar la gestión de riesgos vinculados a los sistemas de gestión de la información, orientado en cómo establecer la metodología a emplear.
* **ISO 27006:**establece los requisitos que deben cumplir aquellas organizaciones que quieran ser acreditadas para certificar a otras en el cumplimiento de la ISO/IEC-27001.
* **ISO 27007:**es una guía que establece los procedimientos para realizar auditorías internas o externas con el objetivo de verificar y certificar implementaciones de la ISO/IEC-27001**.**
* **ISO 27008:**define cómo se deben evaluar los controles del SGSI con el fin de revisar la adecuación técnica de los mismos, de forma que sean eficaces para la mitigación de riesgos.
* **ISO 27009:**complementa la norma ISO/IEC-27001 para incluir requisitos y nuevos controles añadidos que son de aplicación en sectores específicos, con el objetivo de hacer más eficaz su implantación.
* **ISO 27010:**indica cómo debe ser tratada la información cuando es compartida entre varias organizaciones, qué riesgos pueden aparecer y los controles que se deben emplear para mitigarlos, especialmente cuando están relacionados con la gestión de la seguridad en infraestructuras críticas.
* **ISO 27011:**establece los principios para implantar, mantener y gestionar un SGSI en organizaciones de telecomunicaciones, indicando como implantar los controles de manera eficiente.
* **ISO 27013:**establece una guía para la integración de las normas ISO/IEC-27001 (SGSI) y ISO/IEC-20000 Sistema de Gestión de Servicios (SGS) en aquellas organizaciones que implementan ambas.
* **ISO 27014:**establece principios para el gobierno de la seguridad de la información.
* **ISO 27015:**facilita los principios de implantación de un SGSI en empresas que prestan servicios financieros y de seguros.
* **ISO 27016:**proporciona una guía para la toma de decisiones económicas vinculadas a la gestión de la seguridad de la información, como apoyo a la dirección de las organizaciones.
* **ISO 27017:**proporciona una guía para los servicios Cloud, con controles basados en la norma ISO/IEC-27002.
* **ISO 27018:**complementa a las normas ISO/IEC-27001 y ISO/IEC-27002 en la implantación de procedimientos y controles para proteger datos personales en aquellas organizaciones que proporcionan servicios en Cloud para terceros.
* **ISO 27019:**facilita una guía basada en la norma ISO/IEC-27002 para aplicar a las industrias vinculadas al sector de la energía, de forma que puedan implantar un SGSI.
* **ISO 27021:**establece los requisitos de competencia para los profesionales del SGSI que lideran o participan en el establecimiento, implementación, mantenimiento y mejora continua de uno o más procesos del SGSI.
* **ISO 27022:**proporciona un modelo de referencia de procesos para el SGSI.
* **ISO 27023:**facilita una guía de correspondencias entre las normas ISO/IEC-27001 y ISO/IEC-27002.
* **ISO 27031:**proporciona apoyo para la adecuación de las tecnologías de la información y comunicación.
* **ISO 27032:**facilita la identificación de las líneas generales para fortalecer el estado de la ciberseguridad en una compañía.
* **ISO 27033:**establece las pautas de seguridad de la administración, operación y uso de las redes.
* **ISO 27034:**proporciona orientación en el área de tecnología de la información, técnicas de seguridad y seguridad de la aplicación.
* **ISO 27035:**define un conjunto de mejores prácticas relacionadas con la gestión de incidentes de seguridad haciendo hincapié en la detección, reporte y evaluación de incidentes de seguridad.
* **ISO 27036:**referida a la Seguridad de la información para las relaciones con proveedores, ofrece orientación sobre la evaluación y el tratamiento de los riesgos de información involucrados en la adquisición de bienes y servicios de proveedores.
* **ISO 27037:**ofrece directrices para la identificación, recolección, adquisición y preservación de evidencias digitales.
* **ISO 27038:**especifica las características de las técnicas para la redacción digital.
* **ISO 27039:**proporciona una guía para ayudar a las compañías con la selección, despliegue y operación de sistemas de detección y prevención de intrusión.
* **ISO 27040:**facilita unas pautas para proteger la seguridad de los sistemas de almacenamiento, así como para la protección de los datos contenidos en los mismos.
* **ISO 27041:**ofrece una guía y directrices para garantizar la idoneidad y adecuación de los métodos de investigación de incidentes.
* **ISO 27042:**define las directrices para un correcto análisis e interpretación de evidencias digitales.
* **ISO 27043:**proporciona una guía de principios y procesos para la recopilación de evidencias digitales e investigación de incidentes.
* **ISO 27050:**se trata de una norma desarrollada en cuatro partes que trata sobre la información almacenada en dispositivos electrónicos.
* **ISO 27070:**define requisitos de seguridad que tienen como objetivo establecer raíces de confianza para la provisión de entornos informáticos confiables.
* **ISO 27099:**ofrece requisitos para gestionar la seguridad de la información para los proveedores de servicios de confianza de infraestructura de clave pública (PKI).
* **ISO 27100:**facilita una visión general de la ciberseguridad y define conceptos relevantes que estén relacionados.
* **ISO 27102:**describe pautas de gestión para cuando se considere la adquisición de seguros cibernéticos como una opción de tratamiento de riesgos.
* **ISO 27103:**ofrece una guía sobre el aprovechamiento de los estándares y normas existentes en un marco de ciberseguridad.
* **ISO 27110:**basada en los principios de flexibilidad, compatibilidad e interoperabilidad, esta norma proporciona directrices para estandarizar medidas de seguridad.
* **ISO 27400:**proporciona una guía basada en directrices sobre riesgos, principios y controles para la seguridad y privacidad de las soluciones de Internet de las cosas (IoT).
* **ISO 27550:**ofrece pautas de ingeniería de privacidad orientadas a ayudar a las organizaciones a integrar en sus procesos del sistema los avances en la ingeniería de privacidad.
* **ISO 27555:**facilita directrices para el desarrollo e implantación de políticas y procedimientos para la eliminación de la información de identificación personal (PII) en las organizaciones.
* **ISO 27570:**proporciona orientación sobre la protección de la privacidad en el desarrollo de los ecosistemas de las ciudades inteligentes.
* **ISO 27701:**desarrollada como una guía de extensión a los requerimientos y controles del la ISO 27001, aporta a las organizaciones los requisitos para administrar, gestionar los datos y proteger la privacidad de la información de identificación personal (PII).
* **ISO 27799:**define directrices para la implementación de la ISO/IEC-27002 en la industria de la salud