globalsuitesolutions.com

# ¿Qué es ISO 27000 - Seguridad de la Información? GlobalSuite Solutions

5-7 minutos

---

## ISO 27000 y el conjunto de estándares de Seguridad de la Información


Las normas que forman la serie ISO/IEC-27000 son un conjunto de estándares creados y gestionados por la ***Organización Internacional para la Estandarización*** (ISO) y ***la Comisión Electrónica Internacional*** (IEC). Ambas organizaciones internacionales están participadas por multitud de países, lo que garantiza su amplia difusión, implantación  y reconocimiento en todo el mundo.

Las series 27000 están orientadas al establecimiento de buenas prácticas en relación con la implantación, mantenimiento y gestión del ***Sistema de Gestión de Seguridad de la***

***Información*** (SGSI) o por su denominación en inglés ***Information Security Management System*** (ISMS). Estas guías tienen como objetivo establecer las mejores prácticas en relación con diferentes aspectos vinculados a la gestión de la seguridad de la información, con una fuerte orientación a la mejora continua y la mitigación de riesgos.

**ISO 27000:** facilita las bases y lenguaje común para el resto de las normas de la serie.

## ¿Que es la ISO 27001?

- **ISO 27001:** Especifica los requerimientos necesarios para implantar y gestionar un SGSI. Esta norma es certificable.
- **ISO 27002:** define un conjunto de buenas prácticas para la implantación del SGSI, a través de 114 controles, estructurados en 14 dominios y 35 objetivos de controles.
- **ISO 27003**: proporciona una guía para la implantación de forma correcta un SGSI, centrándose en los aspectos importantes para realizar con éxito dicho proceso.
- **ISO 27004:** proporciona pauta orientadas a la correcta definición y establecimiento de métricas que permitan evaluar de forma correcta el rendimiento del SGSI
- **ISO 27005:** define como 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 d  verificar

y certificar implementaciones de la ISO/IEC-27001

- **ISO 27008:** define como 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 27001 para incluir requisitos y nuevos controles añadidos que son de aplicación en sectores específicos, con el objetivos 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 27001 (SGSI) y  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, para que las organizaciones puedan evaluar, monitorizar y comunicar las actividades relacionadas con la seguridad de la información.
- **ISO 27015:** facilita los principios de implantación de un SGSI en empresas que prestan servicios financieros, tales como servicios bancarios o banca electrónica.
- **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 de 37 controles específicos para los servicios cloud, estos controles están basados en la norma 27002.
- **ISO 27018:** complementa a las normas 27001 y 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 27002 para aplicar a las industrias vinculadas al sector de la energía, de forma que puedan implantar un SGSI.

  Destacan del mencionado conjunto la 27001 donde se especifican los requerimientos necesarios para implantar, mantener y gestionar un SGSI, dentro del proceso de mejora continua conocido como Ciclo Deming o PDCA, acrónimo de Plan-Do-Check-Act, en relación con las fases de Planificar, Hacer, Verificar y Actuar. Por otra parte la 27002, es un conjunto de 114 controles, agrupados en 14 dominios, que tienen como objetivo facilitar buenas prácticas en relación con la gestión del SGSI

### ¿Cómo abordar ISO 27001 a través de un software?

Desde GlobalSuite Solutions disponemos de un software de sistema de seguridad. Una herramienta que permite la implantación, gestión y mantenimiento de Sistemas de Gestión de Seguridad de la Información basados en **la norma ISO 27001**. Una herramienta que ayuda a las empresas y equipos de trabajo en la gestión integral de la norma y cumple con el ciclo completo de la misma, desde el inicio y planificación del proyecto hasta el mantenimiento y su mejora continua.


Descubre las claves que abordan los CISOs en su día a día y cómo un software de gestión ayuda en estas tareas de seguridad de la información

**Más artículos**