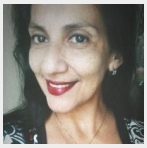
Fanny Vanessa Verano Hidalgo
Ingeniería Industrial



ISO 27000 y los Sistemas de Información

Ingeniería, 11/07/2021

Los sistemas de gestión sectoriales son herramientas que han sido especialmente adaptadas a la actividad principal de cada empresa, lo que a su vez brinda la posibilidad de añadir una certificación específica a la genérica, que encontramos dentro de los diferentes sistemas de gestión.

Por ejemplo ISO 22000 de Sistemas de Gestión de la Inocuidad de los Alimentos, o la ISO 14000 de Sistemas de Gestión Ambiental, ISO 9001 Sistemas de Gestión de Calidad, ISO 30001 Sistemas de Gestión de Riesgos, ISO 45000 Sistemas de Gestión de Seguridad y Salud Laboral, pero en lo que se refiere a la seguridad de la información, las empresas tienen a su disposición los Sistemas de Gestión de la Seguridad de la Información, que se implantan bajo los requisitos de la norma ISO 27000.

La ISO 27000 es una norma que define de qué manera se debe implantar un Sistema de Gestión de la Seguridad de la Información en una empresa u organización. Su implantación ofrece a la organización o empresa la ventaja de proteger su información de la forma más fiable posible, persiguiéndose para ello un total de tres objetivos principales:

Preservar la confidencialidad de sus datos.Conservar la integridad de sus datos.Disponibilidad de la información protegida.
Preservar la confidencialidad de sus datos.Conservar la integridad de sus datos.Disponibilidad de la información protegida.
Por lo tanto, todos los procesos de la información son controlados por la organización eficientemente, tanto de forma interna como al resto de las empresas.

Es interesante tener en cuenta que los sistemas de gestión implantados balo los requisitos de la norma ISO 27000 son totalmente compatibles con otros sistemas de gestión como son los sistemas de gestión de la calidad, de seguridad y salud laboral, de mantenimiento, entre otros.

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.

Destacan de un conjunto de 19 normas dentro de la familia 27000, 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