# ISO 27001:2013 - Certificado de Sistemas de gestión de seguridad de la información

## Introducción

Esta Norma Internacional ha sido preparada para proporcionar requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información. La adopción de un sistema de gestión de seguridad de la información es una decisión estratégica para una organización. El establecimiento e implementación del sistema de gestión de seguridad de la información de una organización está influenciado por las necesidades y objetivos de la organización, los requisitos de seguridad, los procesos organizacionales utilizados y el tamaño y estructura de la organización. Se espera que todos estos factores de influencia cambien con el tiempo.

El sistema de gestión de seguridad de la información preserva la confidencialidad, integridad y disponibilidad de la información mediante la aplicación de un proceso de gestión de riesgos y da confianza a las partes interesadas en que los riesgos se gestionan adecuadamente.

Es importante que el sistema de gestión de seguridad de la información forme parte de los procesos y la estructura de gestión general de la organización y que esté integrado con ellos, y que la seguridad de la información se considere en el diseño de procesos, sistemas de información y controles. Se espera que la implementación de un sistema de gestión de seguridad de la información se escale de acuerdo con las necesidades de la organización.

Esta Norma Internacional puede ser utilizada por partes internas y externas para evaluar la capacidad de la organización para cumplir con los propios requisitos de seguridad de la información de la organización.

El orden en el que se presentan los requisitos en esta Norma Internacional no refleja su importancia ni implica el orden en el que se implementarán. Los elementos de la lista se enumeran solo con fines de referencia.

ISO / IEC 27000 describe la descripción general y el vocabulario de los sistemas de gestión de seguridad de la información, haciendo referencia a la familia de normas del sistema de gestión de seguridad de la información (incluidas ISO / IEC 27003 [ 2 ] , ISO / IEC 27004 [ 3 ] e ISO / IEC 27005 [ 4 ] ), con términos y definiciones relacionados.

## Objeto y campo de aplicació

Esta Norma Internacional especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información dentro del contexto de la organización. Esta Norma Internacional también incluye requisitos para la evaluación y el tratamiento de los riesgos de seguridad de la información adaptados a las necesidades de la organización. Los requisitos establecidos en esta Norma Internacional son genéricos y están destinados a ser aplicables a todas las organizaciones, independientemente de su tipo, tamaño o naturaleza. No es aceptable excluir cualquiera de los requisitos especificados en las Cláusulas 4 a 10 cuando una organización declara conformidad con esta Norma Internacional.