

ISO 27001:2013 - Certificado de Sistemas de gestão de segurança da informação

Introdução

Esta Norma foi preparada para fornecer requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão de segurança da informação. A adoção de um sistema de gestão de segurança da informação é uma decisão estratégica para uma organização. O estabelecimento e implementação de um sistema de gerenciamento de segurança da informação de uma organização são influenciados pelas necessidades e objetivos da organização, requisitos de segurança, processos organizacionais usados e o tamanho e estrutura da organização. Espera-se que todos esses fatores de influência mudem com o tempo.

O sistema de gestão da segurança da informação preserva a confidencialidade, integridade e disponibilidade da informação aplicando um processo de gestão de risco e dá confiança às partes interessadas de que os riscos são geridos de forma adequada.

É importante que o sistema de gestão da segurança da informação faça parte e esteja integrado aos processos da organização e à estrutura geral de gestão e que a segurança da informação seja considerada no projeto de processos, sistemas de informação e controles. Espera-se que a implementação de um sistema de gestão de segurança da informação seja dimensionada de acordo com as necessidades da organização.

Esta Norma Internacional pode ser usada por partes internas e externas para avaliar a capacidade da organização de atender aos requisitos de segurança da informação da própria organização.

A ordem em que os requisitos são apresentados nesta Norma não reflete sua importância ou implica a ordem em que devem ser implementados. Os itens da lista são enumerados apenas para fins de referência.

ISO / IEC 27000 descreve a visão geral e o vocabulário dos sistemas de gerenciamento de segurança da informação, referenciando a família de padrões do sistema de gerenciamento de segurança da informação (incluindo ISO / IEC 27003 [2] , ISO / IEC 27004 [3] e ISO / IEC 27005 [4]), com termos e definições relacionados

Escopo

Esta Norma especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gerenciamento de segurança da informação no contexto da organização. Esta Norma também inclui requisitos para a avaliação e tratamento de riscos de segurança da informação adaptados às necessidades da organização. Os requisitos estabelecidos nesta Norma são genéricos e se destinam a ser aplicáveis a todas as organizações, independentemente do tipo, tamanho ou natureza. A exclusão de qualquer um dos requisitos especificados nas Cláusulas 4 a 10 não é aceitável quando uma organização reivindica conformidade com esta Norma.