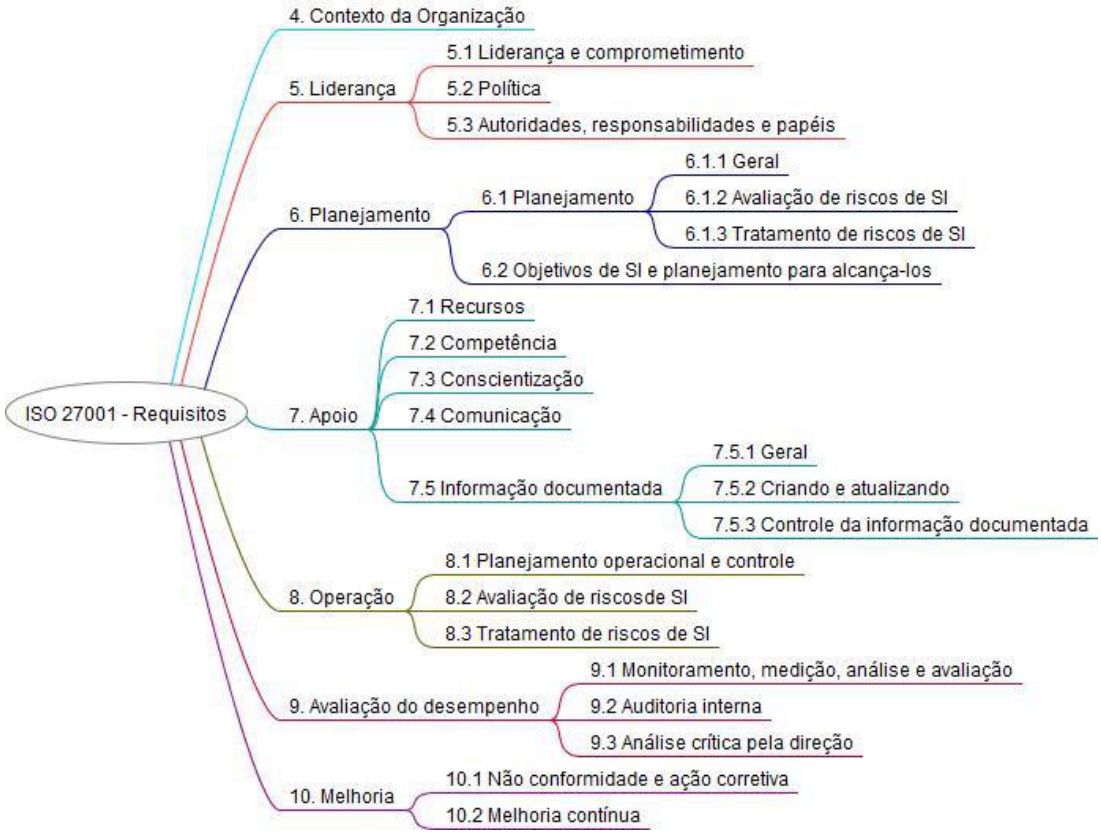
ISO/IEC 27001:2013 – SISTEMAS DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO VII



Melhoria

Não conformidade e ação corretiva — Quando uma não conformidade ocorre, a organização deve:

a) reagir à não conformidade, e conforme apropriado:

1) tomar ações para controlar e corrigi-la; e

2) tratar com as consequências;

Isso é uma das coisas que a organização deve fazer ao encontrar uma não conformidade. Além disso, ela deve:

b) avaliar a necessidade de ações para eliminar as causas de não conformidade, para evitar sua repetição ou ocorrência, por um dos seguintes meios:

1) analisando criticamente a não conformidade;

ANOTAÇÕES

2) determinando as causas da não conformidade; e

3) determinando se não conformidades similares existem, ou podem potencialmente ocorrer.

Ainda, a organização deve:

c) implementar quaisquer ações necessárias;

d) analisar criticamente a eficácia de quaisquer ações corretivas tomadas; e

e) realizar mudanças no sistema de gestão da segurança da informação, quando necessário.

Então, existem várias obrigações que a organização tem por obrigação realizar ao encontrar uma não conformidade.

Nesse sentido, essas ações corretivas devem ser apropriadas aos efeitos das não conformidades encontradas. A organização deve reter informação documentada como evidência da:

a) natureza das não conformidades e quaisquer ações subsequentes tomadas; e

b) resultados de qualquer ação corretiva.

Melhoria Contínua

No que diz respeito à melhoria contínua, a organização deve continuamente melhorar a pertinência, adequação e eficácia do sistema de gestão da segurança da informação.

Anexo A

A norma ISO/IEC 27001:2013 traz um anexo que faz referência aos objetivos de controle. Posto isso, os controles e objetivos de controles listados na Tabela A.1 são derivados diretamente e estão alinhados com aqueles listados na ABNT NBR ISO/IEC 27002:2013 – seções 5 a 18, e devem ser usados em alinhamento com o item 6.1.3

5m

DIRETO DO CONCURSO

1. (2018/IADES/SES-DF/ANALISTA DE SISTEMAS) De acordo com a ABNT NBR ISO/IEC 27001:2013, quando uma não conformidade ocorre, a organização deve reter informação documentada

a. como evidência dos resultados de qualquer ação corretiva.

b. dos resultados das avaliações de risco de segurança da informação.

ANOTAÇÕES

c. dos resultados do tratamento dos riscos de segurança da informação.
d. como evidência dos programas da auditoria e dos resultados desta.
e. como evidência dos resultados das análises críticas pela direção.

2. (2019/FCC/SANASA CAMPINAS/ANALISTA DE TECNOLOGIA DA INFORMAÇÃO/ SUPORTE DE INFRAESTRUTURA TI) A Norma ABNT NBR ISO/IEC 27001:2013 provê requisitos para orientar organizações que desejam implantar um sistema de gestão de segurança da informação, e

a. pode ser usada somente por partes internas da organização para avaliar sua capacidade em atender aos seus próprios requisitos de segurança da informação.
b. não inclui requisitos para avaliação e tratamento de riscos de segurança da informação, mas indica a norma que orienta sobre este assunto.
c. apresenta requisitos genéricos que podem ser aplicáveis a todas as organizações, independentemente do tipo, tamanho ou natureza.
d. possui diversos requisitos nas seções que tratam do contexto da organização (seção 4) e melhoria (seção 10) que podem ser ignorados mesmo por organizações que buscam conformidade com esta Norma.
e. possui anexo “Referência ao conjunto de potenciais riscos de segurança da informação” que estão necessariamente alinhados com a Norma ABNT NBR ISO/IEC 27002:2018.

COMENTÁRIO

10m

- a. Ela pode ser usada também pelas partes externas da organização.
- b. Ela inclui requisitos para a avaliação e tratamento de risco de segurança da informação.
- c. Os requisitos são genéricos e, com isso, podem ser utilizados por qualquer organização.
- d. Caso se busque conformidade coma norma, não se pode ignorar os requisitos que estão numa seção.

ANOTAÇÕES

GABARITO

1. a
2. c

Este material foi elaborado pela equipe pedagógica do Gran Cursos Online, de acordo com a aula preparada e ministrada pelo professor Jósis Alves.
A presente degravação tem como objetivo auxiliar no acompanhamento e na revisão do conteúdo ministrado na videoaula. Não recomendamos a substituição do estudo em vídeo pela leitura exclusiva deste material.

ANOTAÇÕES