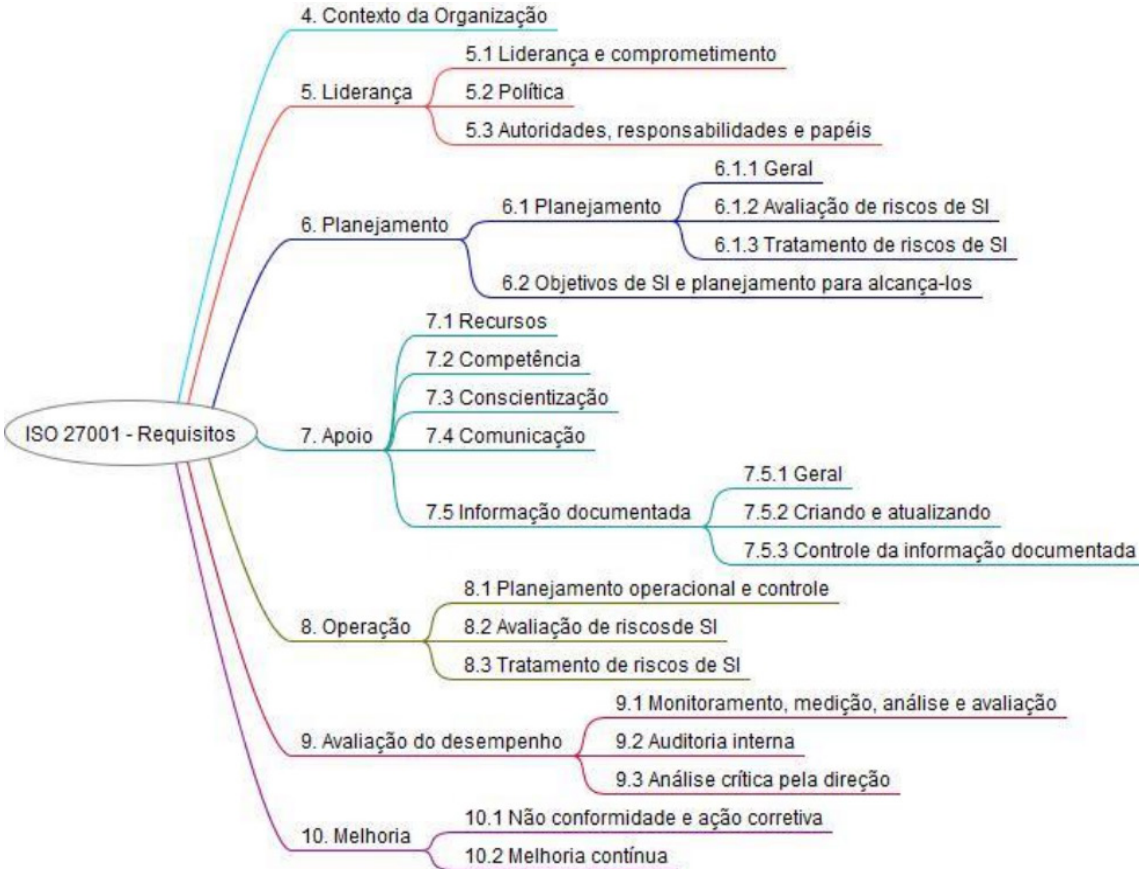
ISO/IEC 27001:2013 – SISTEMAS DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO V



Novamente, a imagem é do mapa mental que apresenta a divisão da Norma ISO 27001:2013. Nesta aula, tratar-se-á do item 8, relativo às operações.

8. Operação

8.1 Planejamento operacional e controle

A organização deve planejar, implementar e controlar os processos necessários para atender os requisitos de segurança da informação e para implementar as ações determinadas em 6.1 (Ações para contemplar riscos e oportunidades).

A organização deve também implementar planos para alcançar os objetivos de segurança da informação determinados em 6.2 (Objetivo de segurança da informação e planos para alcançá-los).

ANOTAÇÕES

Obs.: a manutenção da documentação não se trata de uma novidade propriamente. Os demais itens da Norma ISO também prezam por essa manutenção.

Norma ISO 27001:2013

8.1 Planejamento operacional e controle.

A organização deve manter a informação documentada na abrangência necessária para gerar confiança de que os processos estão sendo realizados conforme planejado.

Obs.: até mesmo a tentativa de prever certos problemas para planejar mudanças e respostas é bastante importante, mas a capacidade de análise crítica quanto à mudança não prevista também é essencial.

A organização deve controlar as mudanças planejadas e analisar criticamente as consequências de mudanças não previstas, tomando ações para mitigar quaisquer efeitos adversos, conforme necessário.

A organização deve assegurar que os processos terceirizados estão determinados e são controlados.

Obs.: frisa-se que a existência de processos terceirizados é bastante comum.

8. Operação

8.2 Avaliação de riscos de segurança da informação

A organização deve realizar avaliações de riscos de segurança da informação a intervalos planejados, quando mudanças significativas são propostas ou ocorrem, levando em conta os critérios estabelecidos em 6.1.2 a.

5m

A organização deve reter informação documentada dos resultados das avaliações de risco de segurança da informação.

8. Operação

8.2 Avaliação de riscos de segurança da informação

ANOTAÇÕES

6.2.1

a) A organização deve definir e aplicar um processo de avaliação de riscos de segurança da informação que:

a) estabeleça e mantenha critérios de riscos de segurança da informação que incluam:

1) os critérios de aceitação do risco; e

2) os critérios para o desempenho das avaliações dos riscos de segurança da informação;

Norma ISO 27001:2013

8. Operação

8.3 Tratamento de riscos de segurança da informação

A organização deve implementar o plano de tratamento de riscos de segurança da informação. A organização deve reter informação documentada dos resultados do tratamento dos riscos de segurança da informação.

EXERCÍCIOS DE FIXAÇÃO

1. É motivo para que organização mantenha informação documentada a geração de confiança de que os processos estão sendo realizados conforme planejado. (Autoral)

COMENTÁRIO

É essencial a manutenção da informação documentada como forma de garantir a geração de confiança na forma como se realizam os processos.

2. Uma vez realizado o tratamento de riscos, os resultados serão descartados. (Autoral)

COMENTÁRIO

Segundo a norma, o certo é que as informações devem ser sempre documentadas.

GABARITO

1. C
2. E