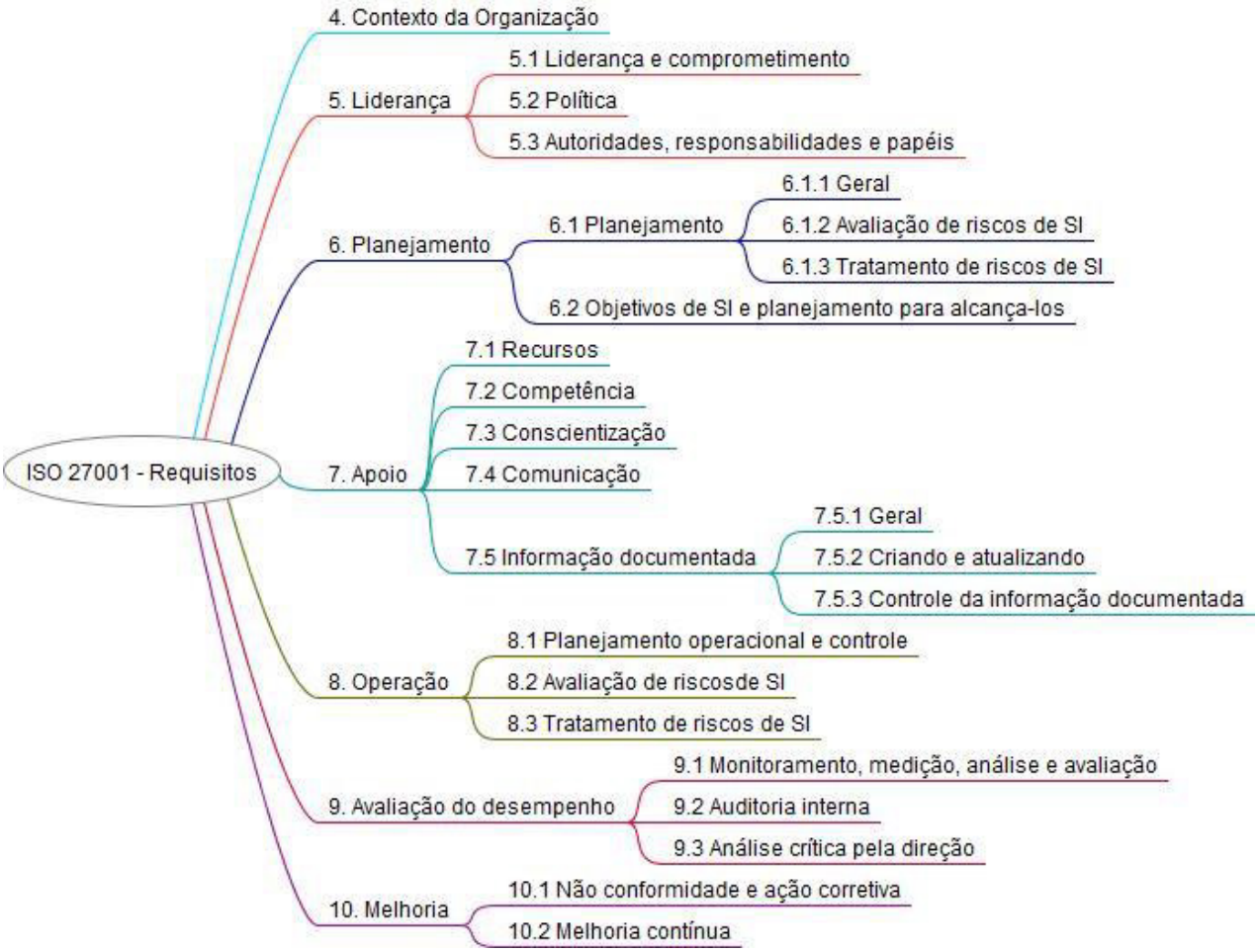
Viu algum erro neste material? Contate-nos em: degravacoes@grancursosonline.com.br

ISOIEC 270012013 – SISTEMAS DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO IV



Novamente, a imagem acima é do mapa mental que apresenta a divisão da Norma ISO 27001:2013. Nesta aula, tratar-se-á do item 7, relativo ao apoio.

Norma ISO 27001:2013

ANOTAÇÕES

7. APOIO

7.1 Recursos

A organização deve determinar e prover recursos para estabelecer, implementar, manutenir e melhorar continuamente o SGSI quanto à:

- Competência técnica do pessoal (treinamento funcionários);
- Conscientização (política de segurança da informação);
- Comunicação (internas e externas).

O quê, Quando, Quem fará, Quem será e O processo.

- Informação documentação.

Norma ISO 27001:2013

7. APOIO

7.2 Competência

A organização deve:

a) determinar a competência necessária das pessoas que realizam trabalho sob o seu controle e que afeta o desempenho da segurança da informação;

b) assegurar que essas pessoas são competentes com base na educação, treinamento ou experiência apropriados;

Norma ISO 27001:2013

7. APOIO

7.2 Competência

A organização deve:

c) onde aplicado, tomar ações para adquirir a competência necessária e avaliar a eficácia das ações tomadas; e

ANOTAÇÕES

d) reter informação documentada apropriada como evidência da competência.

Nota: Ações apropriadas podem incluir, por exemplo: fornecimento de treinamento para os facilitadores, os funcionários atuais, ou pessoas competentes, próprias ou contratadas.

Obs.: com isso, não se pode negar as ações tomadas pelos envolvidos para prover competências, por conta de toda a documentação referente a treinamentos, educação, orientação, workshops etc.

Norma ISO 27001:2013

7. APOIO

7.3 Conscientização

Pessoas que realizam trabalho sob o controle da organização devem estar cientes da:

a) política de segurança da informação;

b) suas contribuições para a eficácia do sistema de gestão da segurança da informação, incluindo os benefícios da melhoria do desempenho da segurança da informação; e

c) implicações da não conformidade com os requisitos do sistema de gestão da segurança da informação.

5m

Norma ISO 27001:2013

7. APOIO

7.4 Comunicação

A organização deve determinar as comunicações internas e externas relevantes para o sistema de gestão da segurança da informação, incluindo:

a) o que comunicar;

b) quando comunicar;

c) quem comunicar;

d) quem será comunicado; e

e) o processo pelo qual a comunicação será realizada.

Norma ISO 27001:2013

ANOTAÇÕES

7. APOIO

7.5 Informação documentada

7.5.1 Geral

O sistema de gestão da segurança da informação deve incluir:

a) informação documentada requerida por esta norma;

b) informação documentada determinada pela organização como sendo necessária para a eficácia do sistema de gestão da segurança da informação.

Norma ISO 27001:2013

7. APOIO

7.5 Informação documentada

7.5.1 Geral

Nota: a abrangência da informação documentada para o sistema de gestão da segurança da informação pode variar de uma organização para outra, devido a:

a) tamanho da organização e seu tipo de atividades, processos, produtos e serviços;

Obs.: em geral, organizações de grande porte possuem muito mais informações do que as empresas de médio e de pequeno porte.

b) a complexidade dos processos e suas interações;

c) a competência das pessoas.

Norma ISO 27001:2013

ANOTAÇÕES

7. APOIO

7.5 Informação documentada

7.5.2 Criando e atualizando

Quando da criação e atualização da informação documentada, a organização deve assegurar de forma apropriada:

a) identificação e descrição (por exemplo, título, data, autor ou um número de referência);

b) formato (por exemplo, linguagem, versão do software, gráficos) e o seu meio (por exemplo, papel, eletrônico); e

c) análise crítica e aprovação para pertinência e adequação.

Norma ISO 27001:2013

7. APOIO

7.5 Informação documentada

7.5.3 Controle da informação documentada

A informação documentada requerida pelo sistema de gestão da segurança da informação e por esta norma deve ser controlada para assegurar:

a) que está disponível e adequada para o uso, onde e quando é necessário;

b) que está adequadamente protegida (por exemplo, contra perda de confidencialidade, uso impróprio ou perda de integridade).

10m

Norma ISO 27001:2013

7. APOIO

7.5 Informação documentada

7.5.3 Controle da informação documentada

Para o controle da informação documentada, a organização deve considerar as seguintes atividades, conforme aplicada:

ANOTAÇÕES

a) distribuição, acesso, recuperação e uso;
b) armazenagem e preservação, incluindo a preservação da legibilidade;
c) controle de mudanças (por exemplo, controle de versão);
d) Retenção e disposição.
Norma ISO 27001:2013

7. APOIO

7.5 Informação documentada

7.5.3 Controle da informação documentada

A informação documentada de origem externa, determinada pela organização, como necessária para o planejamento e operação do sistema de gestão da segurança da informação, deve ser identificada como apropriada e controlada.

Nota: o acesso implica uma decisão quanto à permissão para apenas ler a informação documentada, ou a permissão e autoridade para ver e alterar a informação documentada.

DIRETO DO CONCURSO

1. (2021/CESPE/CEBRASPE/SEFAZ-AL/CESPE/CEBRASPE/2021/SEFAZ-AL/AUDITOR FISCAL DE FINANÇAS E CONTROLE DE ARRECADAÇÃO DA FAZENDA ESTADUAL) A NBR ISO/IEC 27001 prescreve que, por medida de segurança, as informações documentadas como evidências de monitoramento, de auditoria e de análises críticas da segurança da informação sejam descartadas imediatamente após serem apresentadas aos gestores principais da organização.

COMENTÁRIO

Não há prescrição na norma que indique o descarte de informações após apresentação para os gestores.

2. Não se faz necessário que todos que trabalham na organização tenham ciência da política de segurança da informação, já que se trata de documento voltado à área de tecnologia da informação.

ANOTAÇÕES

COMENTÁRIO

Obviamente que é extremamente necessário que todos que trabalham na organização tenham ciência da política de segurança, e a norma realiza tal prescrição.

GABARITO

1. E
2 E

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