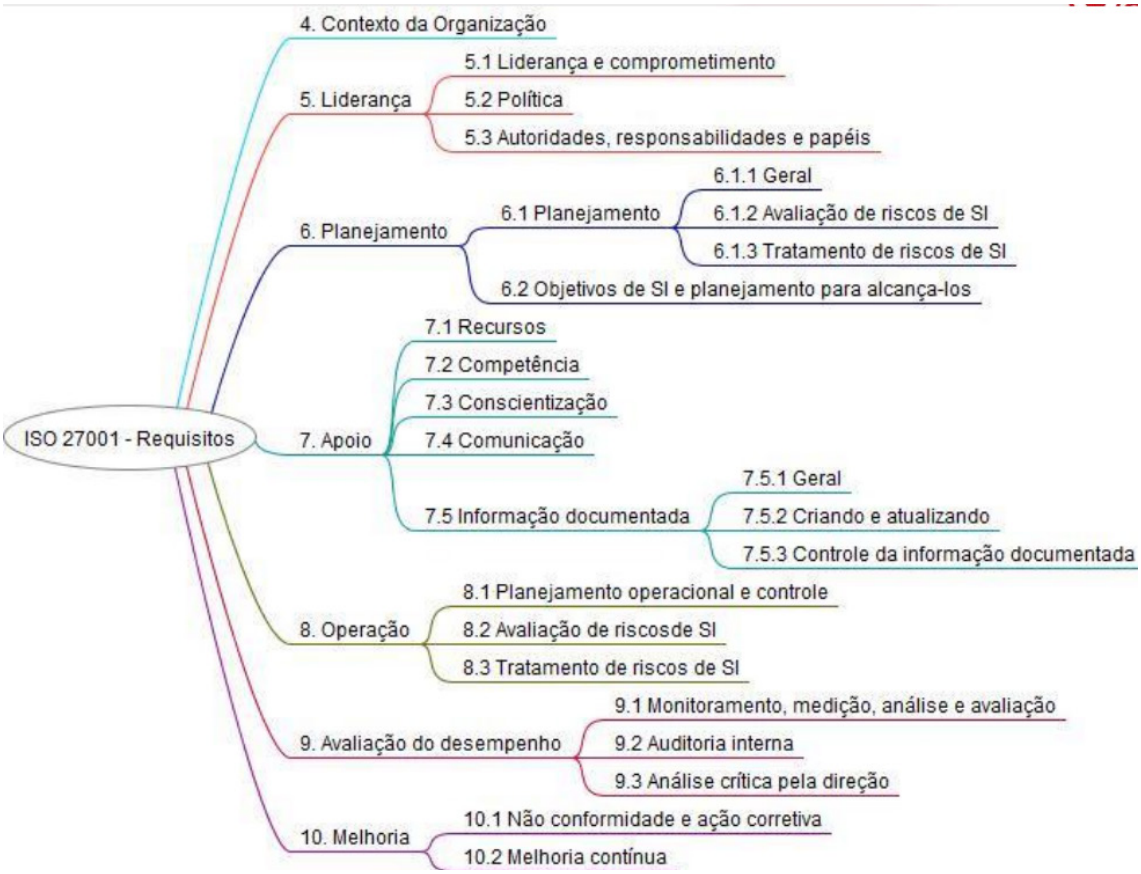
ISOIEC 270012013 – SISTEMAS DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO VI



Novamente, a imagem acima é do mapa mental que apresenta a divisão da Norma ISO 27001:2013. Nesta aula, tratar-se-á do item 9, relativo às avaliações de desempenho.

Norma ISO 27001:2013

9 Avaliação do desempenho

9.1 Monitoramento, medição, análise e avaliação

A organização deve avaliar o desempenho da segurança da informação e a eficácia do sistema de gestão da segurança da informação.

A organização deve determinar:

a. o que precisa ser monitorado e medido, incluindo controles e processos de segurança da informação;

ANOTAÇÕES

b. os métodos para monitoramento, medição, análise e avaliação, conforme aplicável, para assegurar resultados válidos;

Nota: Os métodos selecionados devem produzir resultados comparáveis e reproduzíveis para serem válidos.

c. Quando o monitoramento e a medição devem ser realizados;
d. o que deve ser monitorado e medido;
e. quando os resultados do monitoramento e da medição devem ser analisados e avaliados;
f. quem deve analisar e avaliar estes resultados.

A organização deve reter informação documentada apropriada como evidência do monitoramento e dos resultados da medição.

5m

Obs.: se a organização for questionada, a documentação retida poderá comprovar a idoneidade de suas ações.

Norma ISO 27001:2013
9 Avaliação do desempenho
9.2 Auditoria interna
A organização deve conduzir auditorias internas a intervalos planejados para prover informações sobre o quanto o sistema de gestão da segurança da informação:
a. está em conformidade com:

1. os próprios requisitos da organização para o seu sistema de gestão da segurança da informação;

2. os requisitos desta Norma;
b. está efetivamente implementado e mantido.
Norma ISO 27001:2013
9 Avaliação do desempenho
9.2 Auditoria interna
Organização deve:

ANOTAÇÕES

a. planejar, estabelecer, implementar e manter um programa de auditoria, incluindo a frequência, métodos, responsabilidades, requisitos de planejamento e relatórios.

Os programas de auditoria devem levar em conta a importância dos processos pertinentes e os resultados de auditorias anteriores;

Obs.: as observações de não conformidade declaradas em auditorias anteriores vão atestar se as ações para corrigir não conformidades foram de fato implementadas.

10m

b. definir os critérios e o escopo da auditoria, para cada auditoria;
c. selecionar auditores e conduzir auditorias que assegurem objetividade e imparcialidade do processo de auditoria;
d. assegurar que os resultados das auditorias são relatados para a direção pertinente;
e. reter a informação documentada como evidência dos programas da auditoria e dos resultados da auditoria.

DIRETO DO CONCURSO

1. (2021/CESPE/CEBRASPE/ANALISTA JURÍDICO/ANALISTA DE SISTEMA/SUPORTE E INFRAESTRUTURA) Com base na norma ISO/IEC 27001, julgue o item seguinte. Uma organização deve prever auditorias internas sobre o seu sistema de gestão de segurança da informação, em intervalos planejados, para verificar a conformidade com os requisitos da norma.

COMENTÁRIO

A norma prevê como obrigação da organização a previsão de um programa de auditorias internas em intervalos planejados para verificar conformidade com os requisitos da organização e da norma.

2. (2021/CESPE/CEBRASPE/SERPRO/ANALISTA/ESPECIALIZAÇÃO: DESENVOLVIMENTO DE SISTEMAS) Com relação à gerência de riscos, às disposições das NBR ISO/IEC 27001 e NBR ISO/IEC 27002 e às políticas de senhas, julgue o item a seguir. Segundo a NBR ISO/IEC 27001, as informações documentadas como evidências dos programas de auditoria interna devem ser destruídas após a finalização dos programas,

ANOTAÇÕES

desde que os resultados tenham sido aceitos pelas partes de interesse e homologados pelo conselho gestor da organização.

COMENTÁRIO

Os documentos devem ser preservados e mantidos, não sendo destruídos sob hipótese alguma.
É de suma importância que esses relatórios de auditorias anteriores sejam mantidos para verificar se as devidas providências foram tomadas para sanar os problemas encontrados.

Norma ISO 27001:2013
9 Avaliação do desempenho
9.3 Análise crítica pela direção
A Alta Direção deve analisar criticamente o sistema de gestão da segurança da informação da organização a intervalos planejados para assegurar a sua contínua adequação, pertinência e eficácia.

15m

A análise crítica pela Direção deve incluir considerações com relação a:
a. situação das ações de análises críticas anteriores, realizadas pela direção;
b. mudanças nas questões internas e externas, que sejam relevantes para o sistema de gestão da segurança da informação;
Norma ISO 27001:2013
A análise crítica pela Direção deve incluir considerações com relação a:
c. realimentação sobre o desempenho da segurança da informação, incluindo tendências nas:

1. não conformidades e ações corretivas;
2. monitoramento e resultados da medição;
3. resultados de auditorias; e
4. cumprimento dos objetivos de segurança da informação.

9 Avaliação do desempenho

ANOTAÇÕES

9.3 Análise crítica pela direção

A análise crítica pela Direção deve incluir considerações com relação a:

d. realimentação das partes interessadas;

e. resultados da avaliação dos riscos e situação do plano de tratamento dos riscos; e

f. oportunidades para melhoria contínua.

Os resultados da análise crítica pela Direção devem incluir decisões relativas a oportunidades para melhoria contínua e quaisquer necessidades para mudanças do sistema de gestão da segurança da informação.

A organização deve reter informação documentada como evidência dos resultados das análises críticas pela direção.

3. (2021/CESPE/CEBRASPE/PG-DF/ANALISTA JURÍDICO/ANALISTA DE SISTEMA/SUPORTE E INFRAESTRUTURA) Com base na norma ISO/IEC 27001, julgue o item seguinte. Ao analisar criticamente o sistema de gestão de segurança da informação (SGSI) da organização, a alta direção deve incluir oportunidades de melhoria nesse sistema.

COMENTÁRIO

Conforme observado, a análise crítica realizada pela direção tem como objetivo incluir oportunidades de melhoria no sistema.

GABARITO

1. C
2. E
3. 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