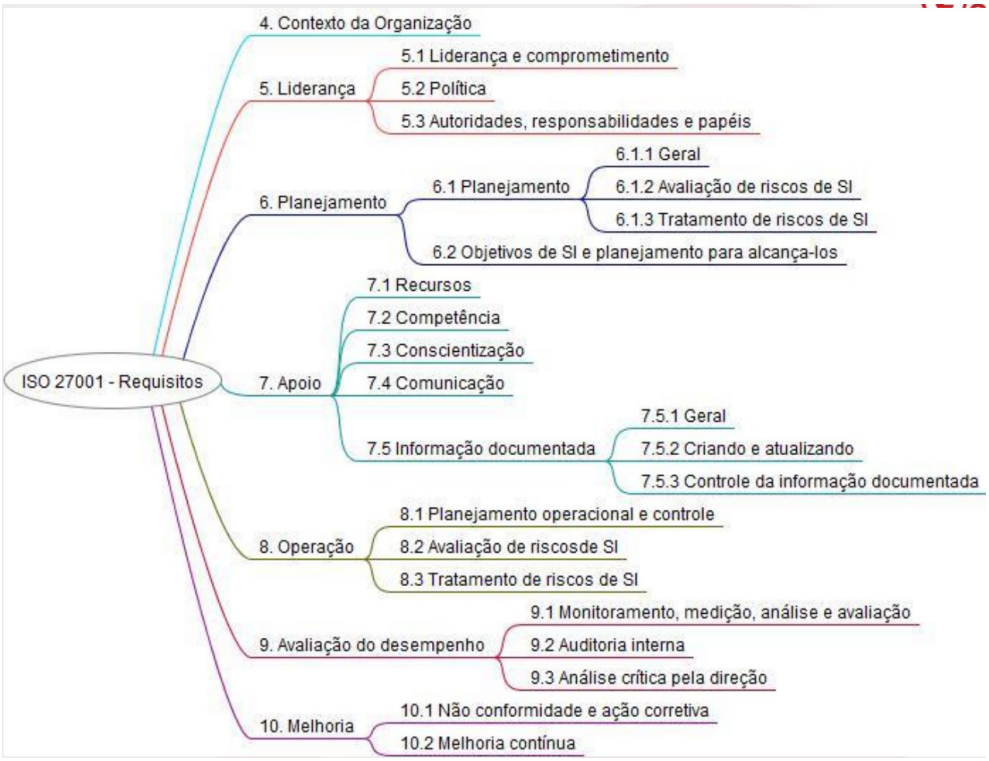
ISO/IEC 27001:2013 – SISTEMAS DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO III



Norma ISO 27001:2013

6. Planejamento

Ações para contemplar riscos e oportunidades, quando do planejamento, a organização deverá, além de considerar (o contexto organizacional, necessidades e expectativas das partes interessadas), os riscos e oportunidades para:

- Assegurar que o SGSI poderá alcançar seus resultados;
- Prevenir ou reduzir os efeitos indesejados; e
- Alcançar a melhoria contínua.

Obs.: São diversos os pontos a serem observados pela organização, considerando-se todos os clientes, acionistas, parceiros etc.

ANOTAÇÕES

Norma ISO 27001:2013
Para isso, a organização deverá:

- Planejar as ações (considerando os riscos e oportunidades);
- Integrar e implementar essas ações dentro dos processos do SGSI.
- Avaliar a eficácia dessas ações.

Norma ISO 27001:2013

6. Planejamento
Avaliação de riscos de segurança da informação – deverá:

- Estabelecer e manter critérios de riscos de SI;
- Aceitação de risco;
- Desempenho das avaliações dos riscos;
- Assegurar avaliações que produzam resultados (comparáveis, válidos e consistentes);

5m

Obs.: inclusive, esse ponto já foi objeto dos certames.

- Identificação dos riscos;
- Riscos associados à perda da CID;
- Responsáveis dos riscos.
- Analisar os riscos identificados, avaliando consequências potenciais, se materializados.
- Analisar os riscos identificados, avaliando a probabilidade de ocorrência.
- Determinar os níveis de risco.

Avaliar os riscos:

- Comparando os resultados da análise em relação aos critérios que foram estabelecidos (aceitação e desempenho de avaliação);
- Priorizando-os para tratamento.

Obs.: Percebe-se que a análise de risco busca a otimização do tempo e a priorização do que realmente pode afetar a companhia.

ANOTAÇÕES

- A organização deve ter o processo de Avaliação de Riscos documentado.

DIRETO DO CONCURSO

1. (2022/CESPE/CEBRASPE/PGE-RJ/ANALISTA DE SISTEMAS E MÉTODOS) Com base nas normas relacionadas à gestão de segurança, julgue o item a seguir. Segundo a ABNT NBR ISO/IEC 27001:2013, a organização deve definir um processo de avaliação de riscos de segurança da informação que mantenha critérios desses riscos; essas avaliações devem ser realizadas em intervalos planejados.

COMENTÁRIO

Sabe-se que há uma obrigação de definir o processo de avaliação de riscos, devendo-se realizar as avaliações em horários planejados.

10m

Tratamento de riscos de segurança da informação, deverá definir e aplicar um processo de tratamento de riscos para:

- Selecionar, de forma apropriada, as opções de tratamento dos riscos de SI, levando em consideração os resultados da avaliação do risco;
- Determinar todos os controles que são necessários* à implementação das opções escolhidas;
- Comparar os controles determinados* com os do anexo A, verificando a omissão de algum controle necessário.

Norma ISO 27001:2013

Anexo A:

- Lista detalhada dos Controles e Objetivos de Controle.
- Derivados diretamente e alinhados com a ISO 27002:2013.
- Não são exaustivos (poderão existir outros além desses).

A.5 Políticas de segurança da informação

ANOTAÇÕES

A.5.1 Orientação da Direção e apoio para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes.

Objetivo: Prover orientação da Direção e apoio para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações.

A.5.1.1 Políticas para segurança da informação

Controle: Um conjunto de políticas de segurança da informação deve ser definido, aprovado pela Direção, publicado e comunicado para os funcionários e partes externas relevantes.

Norma ISO 27001:2013

6. Planejamento

Tratamento de riscos de segurança da informação, deverá:

- Elaborar uma Declaração de Aplicabilidade que contenha:
  - Os controles necessários.
  - Justificativa para inclusões.
  - Justificativa para exclusões dos controles Anexo A.

- Preparar um plano para tratamento.
- Obter aprovação dos responsáveis pelos riscos, bem como a aceitação dos riscos residuais.
- A organização deve ter o processo de Tratamento de Riscos documentado.

15m

Norma ISO 27001:2013

Objetivo de segurança da informação e planejamento para alcançá-los, estabelecendo objetivos de SI, sendo:

- Consistentes com a Política de Segurança da Informação
- Mensuráveis (se aplicável)
- Levados em conta os requisitos de SI aplicáveis e os resultados da avaliação e tratamento dos riscos
- Comunicados
- Atualizados
- A organização deve ter os Objetivos de SI documentados.

Norma ISO 27001:2013

ANOTAÇÕES

Quando do planejamento para alcançar os seus objetivos de segurança da informação, a organização deve determinar:

a) o que será feito;

b) quais recursos serão necessários;

c) quem será responsável;

d) quando estará concluído; e

e) como os resultados serão avaliados.

GABARITO

1. C

ANOTAÇÕES