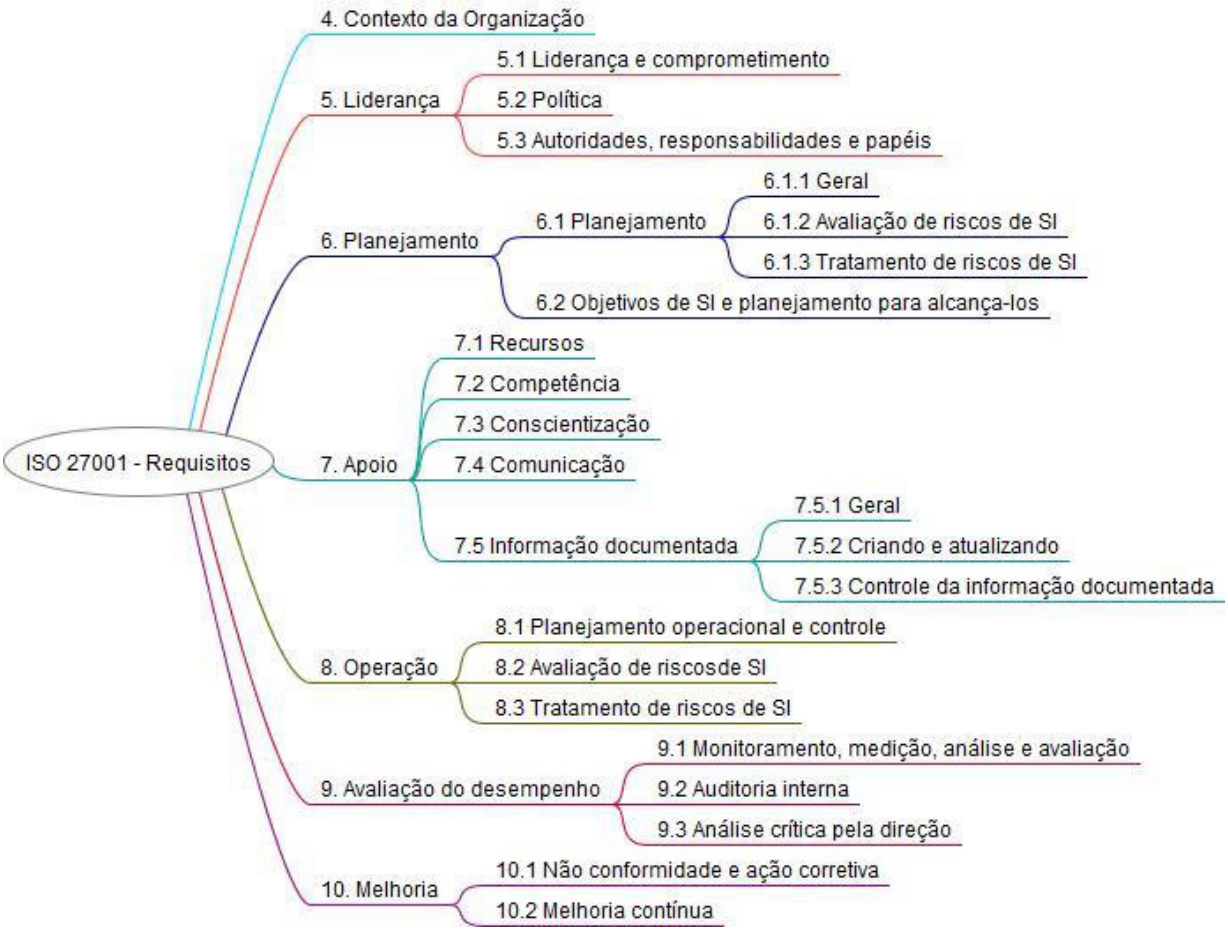
# ISO/IEC 27001:2013 – SISTEMAS DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO II

A ISO 27001 prevê vários requisitos em relação às seções:

- Seção 4: estabelece o contexto da organização.
- Seção 5: diz respeito à liderança e está subdividida em liderança e comprometimento; política; autoridades, responsabilidades e papéis.
- Seção 6: estabelece o planejamento e está subdividida em planejamento; objetivos de SI e planejamento para alcançá-los.
- Seção 7: diz respeito ao apoio e está subdividida em recursos; competência; conscientização; comunicação; informação documentada.
- Seção 8: fala sobre operação e está subdividida em planejamento operacional e controle; avaliação de riscos de SI; tratamento de riscos de SI.
- Seção 9: aborda sobre avaliação de desempenho e está subdividida em monitoramento, medição, análise e avaliação; auditoria interna; análise crítica pela direção.
- Seção 10: trata sobre melhoria e está subdividida em não conformidade e ação corretiva; melhoria contínua.



Para as organizações que buscam a conformidade com a norma, certificação ISO 27001 não é aceitável a exclusão de nenhum dos requisitos especificados por ela.

## 4. CONTEXTO DA ORGANIZAÇÃO

Formas de contexto da organização:

- Entendendo a organização e seu contexto determinando as questões internas e externas relevantes ao seu propósito, e que afetem os resultados pretendidos pelo SGSI. (ISO 31000). A ISSO 3100 é a que trata sobre gestão de riscos corporativos.
- Entendendo as necessidades e as expectativas das partes interessadas, devendo determinar as partes interessadas e os seus requisitos (legais, regulamentares e contratuais).
- Determinando o escopo do SGSI devendo a organização considerar as questões internas e externas e as necessidades das partes interessadas.

## 5. LIDERANÇA

### 5.1 Liderança e Comprometimento

5m

A liderança e o comprometimento devem ser demonstrados pela Alta Direção em relação ao SGSI.

A Alta Direção deve demonstrar sua liderança e comprometimento em relação ao sistema de gestão da segurança da informação pelos seguintes meios:

a. Assegurando que a política de segurança da informação (PSI) e os objetivos de segurança da informação estão estabelecidos e são compatíveis com a direção estratégica da organização.

b. Garantindo a integração dos requisitos do sistema de gestão da segurança da informação dentro dos processos da organização.

c. Assegurando que os recursos necessários para o sistema de gestão da segurança da informação estejam disponíveis.

d. Comunicando a importância de uma gestão eficaz da segurança da informação e da conformidade com os requisitos do sistema de gestão da segurança da informação.

ANOTAÇÕES

e. Assegurando que o sistema de gestão da segurança da informação alcança seus resultados pretendidos.

f. Orientando e apoiando pessoas que contribuam para a eficácia do sistema de gestão da segurança da informação.

g. Promovendo a melhoria contínua no SGSI.

h. Apoiando outros papéis relevantes da gestão para demostrar como sua liderança se aplica às áreas sob sua responsabilidade.

### 5.2 Política de SI

A política de SI é estabelecida pela Alta Direção:

- De acordo com o propósito da organização.
- Tenha os objetivos de SI ou que forneça a estrutura para tal.
- Tenha o comprometimento para a realização dos requisitos aplicáveis em SI.
- Tenha o comprometimento com a melhoria contínua.

A Política de SI deverá:

10m

- Estar disponível em documento (Formal). Um documento formal é aquele que é assinado pela Alta Direção.
- Ser comunicada na organização (Comunicação). A Segurança da Informação deve ser do conhecimento de todos, uma vez que ela vira um documento formal, deve ser comunicada.
- Disponível as partes interessadas (Informada). As partes interessadas são os sócios, parceiros comerciais, clientes da organização.

### 5.3 Autoridades, Responsabilidades e Papéis

Cabe a atribuição pela Alta Direção de responsáveis e autoridades para:

- Assegurar a conformidade do SGSI com a norma. A Alta Direção cabe a atribuição dos responsáveis e autoridades que vão fazer com que a conformidade do SGSI esteja assegurada de acordo com a norma.
- E também relatar o desempenho do SGSI.

ANOTAÇÕES

## EXERCÍCIOS DE FIXAÇÃO

1. De acordo com a Norma NBR ISO/IEC 27001 2013 a ação da Alta Direção de orientar e apoiar pessoas que contribuam para a eficácia do sistema de gestão da segurança faz parte do tópico: (Autoral)
   a. Política.
   b. Autoridade.
   c. Responsabilidade.
   d. Papéis organizacionais.
   e. Liderança e comprometimento.

## COMENTÁRIO

Os requisitos que dizem respeito ao comando da questão estão em liderança e comprometimento.

## DIRETO DO CONCURSO

2. (CESPE/TRT 7 ª REGIÃO (CE)/ ANALISTA JUDICIÁRIO TECNOLOGIA DA INFORMAÇÃO) De acordo com a ABNT NBR ISO/IEC 27001 a alta direção da organização tem papel fundamental no sistema de gestão de segurança da informação ( SGSI). Nesse contexto, ela deve estabelecer uma política de segurança da informação que:
   a. inclua o comprometimento com a melhoria contínua do SGSI.
   b. reduza efeitos indesejados.
   c. informe responsáveis por cada ativo de informação.
   d. crie mecanismos de avaliação de riscos compatíveis com o framework Cobit 5.

## COMENTÁRIO

A alta direção deve estabelecer um PSI que inclua o comprometimento com a melhoria contínua do SGSI.

15m

ANOTAÇÕES

3. (FCC/TRF 5 ª REGIÃO/ANALISTA JUDICIÁRIO–INFORMÁTICA INFRAESTRUTURA) Considere que PSI se refere à Política de Segurança da Informação e SGSI se refere ao Sistema de Gestão da Segurança da Informação. De acordo com a Norma ABNT NBR ISO/IEC 27001:2013 dentre as atribuições da Alta Direção inclui-se:
   a. estabelecer uma PSI que atenda aos propósitos da Norma antes dos propósitos da organização.
   b. definir os objetivos da segurança da informação para que a estrutura organizacional possa aplicá-los.
   c. estabelecer uma PSI que inclua o comprometimento em satisfazer os requisitos da segurança da informação com base nos habilitadores do COBIT 5 ª edição.
   d. atribuir responsabilidade e autoridade para assegurar que o SGSI está em conformidade com os requisitos da Norma e para relatar o desempenho do SGSI dentro da organização e para a própria Alta Direção.
   e. estabelecer uma PSI que inclua o comprometimento com a melhoria contínua do SGSI com base no estágio Melhoria Contínua da ITL v 3ª edição 2011.

## COMENTÁRIO

É dever da Alta Direção fazer a atribuição de responsabilidade e autoridade para assegurar que o SGSI está em conformidade com os requisitos da Norma e para relatar o desempenho do SGSI dentro da organização para a própria Alta Direção.

## GABARITO

1. e
2. a
3. d

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