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

Gestão da Segurança da Informação

Nesta aula, vamos apresentar a família de normas mais comumente cobradas da família 27000, normas que versam sobre segurança da informação.

Siglas

Siglas utilizadas em normativos e padrões:

ISO: é um padrão internacional de organização – International Organization for Standardization – que padroniza vários assuntos no que diz respeito, inclusive, a sistemas de gestão da segurança da informação.

IEC: é a comissão internacional eletrotécnica – International Electrotechnical Commission – que também tem como finalidade a padronização e criação de padrões técnicos para a área de equipamentos elétricos e eletrônicos.

ABNT: Associação Brasileira de Normas Técnicas.

NBR: Norma Brasileira.

Por vezes, uma norma ISO não está ainda no padrão brasileiro, ou seja, não se tornou uma norma brasileira, uma NBR, por isso, ela ainda não é uma norma vigente. Acontece, por exemplo, quando sai uma nova versão de alguma norma e, dentro do Brasil, não foi normatizada, reconhecida como uma norma brasileira.

SI: Segurança da Informação.

SGSI: Sistema de Gerenciamento de Segurança da Informação.

DIRETO DO CONCURSO

1. (2021/FGV/IMBEL/ANALISTA ESPECIALIZADO ANALISTA DE SISTEMAS REAPLICAÇÃO) A Associação Brasileira de Normas Técnicas, ABNT, é responsável pela elaboração das Normas Brasileiras como, por exemplo, a ABNT NBR ISO/IEC 27001 2013 sobre aspectos da Segurança da Informação

Dado que a sigla ISO deriva de International Organization for Standardization assinale a correta natureza das normas NBR ISO.

ANOTAÇÕES

a. São normas brasileiras que passam a ser adotadas pela ISO.
b. São normas definidas em conjunto com a ISO.
c. São traduções de normas da ISO que passam a ser adotadas pela ABNT.
d. São normas da ISO adaptadas pela ABNT às práticas brasileiras.
e. São normas brasileiras compiladas a partir da combinação de outras normas da ISO.

5m

COMENTÁRIO

NBR ISO são traduções da norma da ISO, que passam a ser adotadas pela ABNT.

Bibliografia – Família 27000

- ABNT NBR ISO/IEC 27000

Objetiva dar uma visão geral e o vocabulário, termos e conceitos relacionados ao Sistema e Gerenciamento da Segurança de Informação – SGSI – e, também, é uma referência às normas da família 27000. Os termos e conceitos são utilizados nas outras normas da família 27000.

- ABNT NBR ISO/IEC 27001

Norma que especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um SGSI.

Determina o que deve ser feito para se estabelecer um SGSI.

Caso a organização queira demonstrar que ela está em conformidade, em compliance, com a 27001, ela precisa utilizar todos os controles existentes, não podendo excluir nenhum. Dessa forma, estará em conformidade com a 27001, comprovando e conseguindo, assim, obter a certificação.

- ABNT NBR ISO/IEC 27002

Concede as práticas para a gestão de SI, ou seja, na 27002 estão as recomendações em relação às boas práticas, às diretrizes para o Sistema de Gestão de Segurança da Informação.

A diferença entre as duas é que a 27001 dá requisitos, aquilo que deve ser feito; a 27002 traz as boas práticas, as recomendações.

ANOTAÇÕES

- ABNT NBR ISO/IEC 27003

Atribui as diretrizes para a implantação de um SGSI.

A norma descreve o processo de especificação e projeto do SGSI e de design, desde a concepção até a elaboração dos planos de implantação.

Ela descreve o processo para obter a aprovação da direção da organização para implementar o SGSI.

- ABNT NBR ISO/IEC 27004

É a norma que orienta sobre monitoramento, medição, análise e avaliação.

- ABNT NBR ISO/IEC 27005

10m

É a norma que define as diretrizes sobre gestão de riscos de segurança da informação (Diretrizes). Não é uma norma de gestão de riscos corporativa.

- ABNT NBR ISO/IEC 27006

Norma que especifica os requisitos para as empresas de auditoria e de certificação de SGSI.

- ABNT NBR ISO/IEC 27007

Norma que fornece as diretrizes para auditoria de SGSI.

Norma ISO 27001:2013

O que é?

- É a norma que provê REQUISITOS para estabelecer, implementar, manter e melhorar continuamente um SGSI. Os requisitos devem ser cumpridos pela organização.
- A adoção de SGSI é uma decisão estratégica para a organização. Não é uma decisão tática gerencial nem operacional. Está no topo da pirâmide organizacional.

ANOTAÇÕES

- "O estabelecimento e a implementação do SGSI de uma organização são influenciados pelas suas necessidades e objetivos, requisitos de segurança, processos organizacionais usados, tamanho e estrutura da organização."

Para que serve?

- Um SGSI preserva as propriedades da segurança da informação: Confidencialidade, Integridade e Disponibilidade (CID) das informações.
- Isso é feito por meio da aplicação de um processo de gestão de riscos. Faz-se a gestão de riscos, para preservar os pilares importantes para a organização.
- Visa fornecer confiança aos *stakeholders,* as partes interessadas, pois os riscos estão sendo gerenciados adequadamente.

15m

Todos aqueles que tem influência em relação à organização – cliente, sócio, funcionários, parceiros – ao saberem que tem implementado um sistema de gestão de segurança da informação, vão entender que os riscos estão sendo gerenciados adequadamente.

Pilares da segurança da informação:

- Confidencialidade;
- Integridade;
- Disponibilidade.

DIRETO DO CONCURSO

2. (2021/SELECON/EMGEPRON/ANALISTA TÉCNICO – SEGURANÇA DA INFORMAÇÃO) Entre as Normas da ISO/IEC 27000, a ISO 27001 é uma norma relacionada ao Sistema de Gerenciamento da Segurança da Informação (ISMS) no que diz respeito ao seguinte aspecto:

a. guia para auditoria do ISMS;
b. processo de certificação e registro do ISMS;
c. especificação formal associada aos requisitos do ISMS;
d. diretriz de ISMS para empresas de telecomunicações.

ANOTAÇÕES

COMENTÁRIO

A ISO 27001 é a norma da família 2700 da ISO no que diz respeito à especificação formal associada aos requisitos do ISMS (SGSI).

- A norma pode ser usada por partes internas e externas, no que diz respeito ao atendimento dos requisitos de SI.
- A norma também contempla os requisitos para realizar a avaliação e o tratamento de riscos de segurança da informação.
- Apresenta requisitos genéricos. Não são requisitos específicos.
- São aplicáveis a TODAS as organizações, independentemente do tipo, tamanho ou natureza.

DIRETO DO CONCURSO

3. (IESES/MSGÁS/ANALISTA DE TECNOLOGIA DA INFORMAÇÃO) A norma que especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da organização é a:

a. ABNT NBR ISO/IEC 27004:2010.
b. ABNT NBR ISO/IEC 27001:2013.
c. ABNT NBR ISO/IEC 27003:2011.
d. ABNT NBR ISO/IEC 27002:2013.

COMENTÁRIO

20m

A norma que especifica tais requisitos é a ABNT NBR ISO/IEC 27001/2013.
Por vezes, as organizações se utilizam de normativos para se estabelecer e até implementar, mas não levam as boas práticas para manter o sistema que foi implementado de acordo com a realidade da organização. Manter é fazer com que aquilo que foi realizado esteja sempre de acordo com a realidade da organização. Manter e melhorar continuamente é responsabilidade da organização.

ANOTAÇÕES

4. (CESPE/TCU/AUDITOR FEDERAL DE CONTROLE EXTERNO – TECNOLOGIA DA INFORMAÇÃO) De acordo com a NBR ISO/IEC 27001:2013, a organização deve estabelecer, implementar, manter e continuamente melhorar um sistema de gestão da segurança da informação (SGSI). A esse respeito, julgue o item subsequente.

Na especificação e na implementação do SGSI, devem-se considerar as necessidades, os objetivos e os requisitos de segurança da organização, mas elas não devem ser influenciadas por seu tamanho nem por sua estrutura.

( ) Certo
( ) Errado

COMENTÁRIO

O estabelecimento e a implementação do SGSI de uma organização são influenciados pelas suas necessidades e objetivos, requisitos de segurança, processos organizacionais usados, tamanho e estrutura da organização.

- Anexo A – preconiza os controles e objetivos de controle, alinhados com a Norma ABNT NBR ISO/IEC 27002:2013, que deverão ser aplicados na organização.

GABARITO

1. c
2. c
3. b
4. E

25m

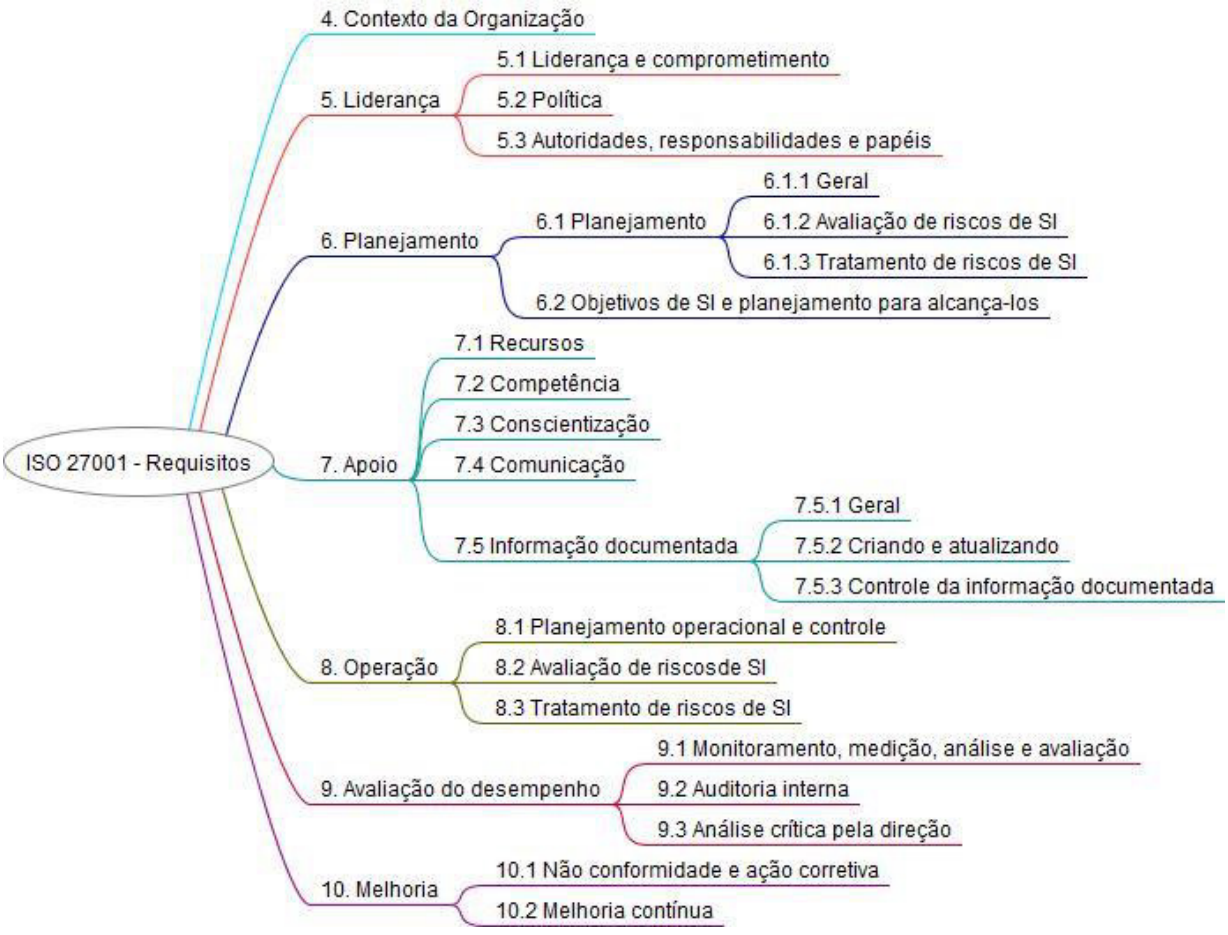
Este material foi elaborado pela equipe pedagógica do Gran Cursos Online, de acordo com a aula preparada e ministrada pelo professor Jósis Alves.
A presente degravação tem como objetivo auxiliar no acompanhamento e na revisão do conteúdo ministrado na videoaula. Não recomendamos a substituição do estudo em vídeo pela leitura exclusiva deste material.

ANOTAÇÕES

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.

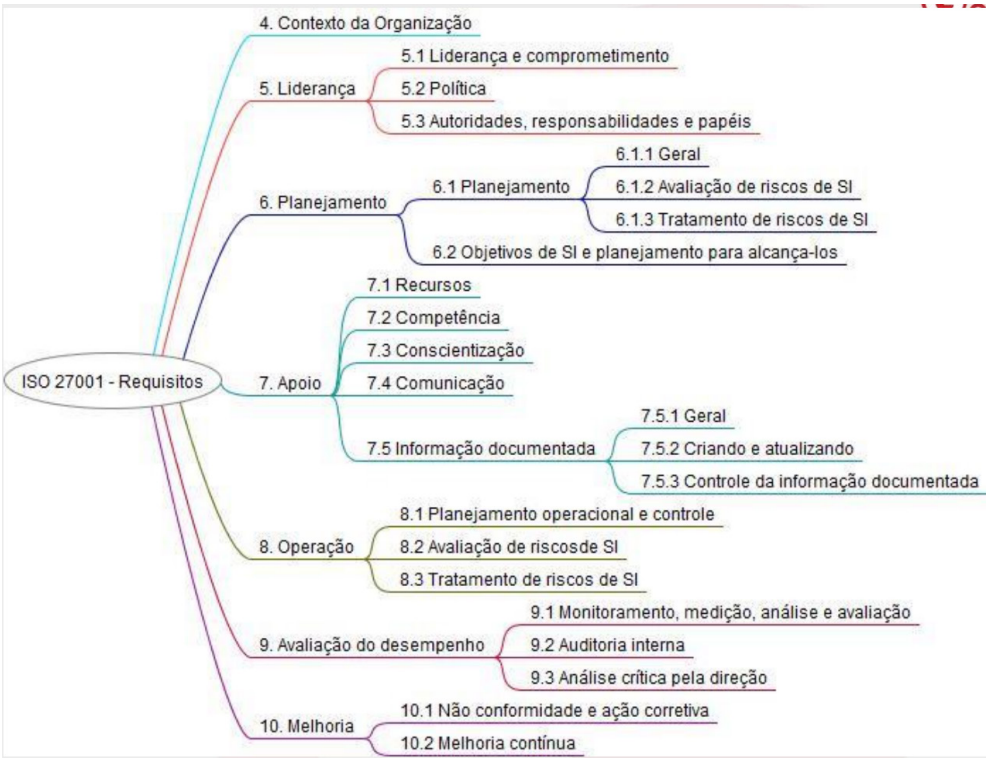
GABARITO

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

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

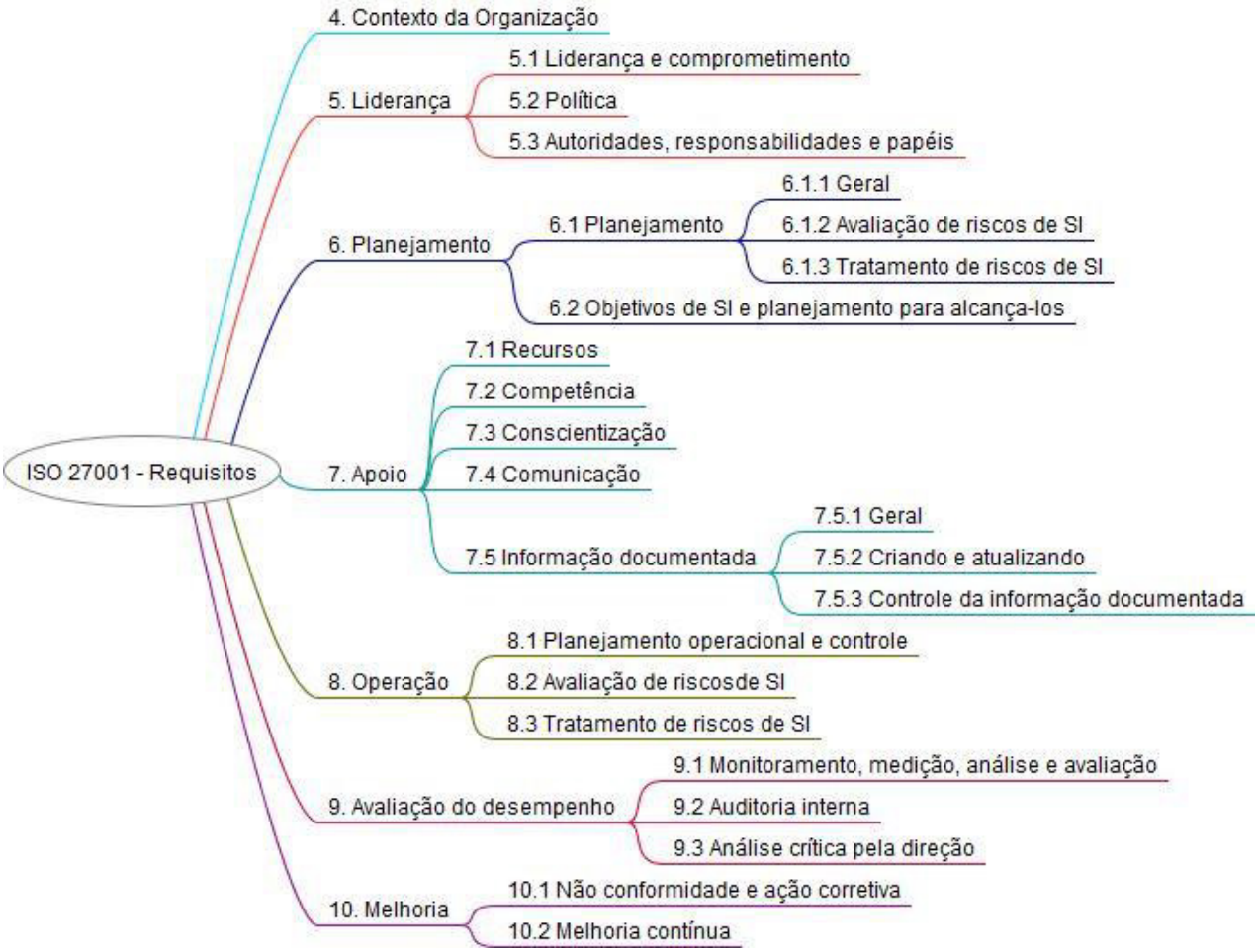
e) como os resultados serão avaliados.

GABARITO

1. C

ANOTAÇÕES

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

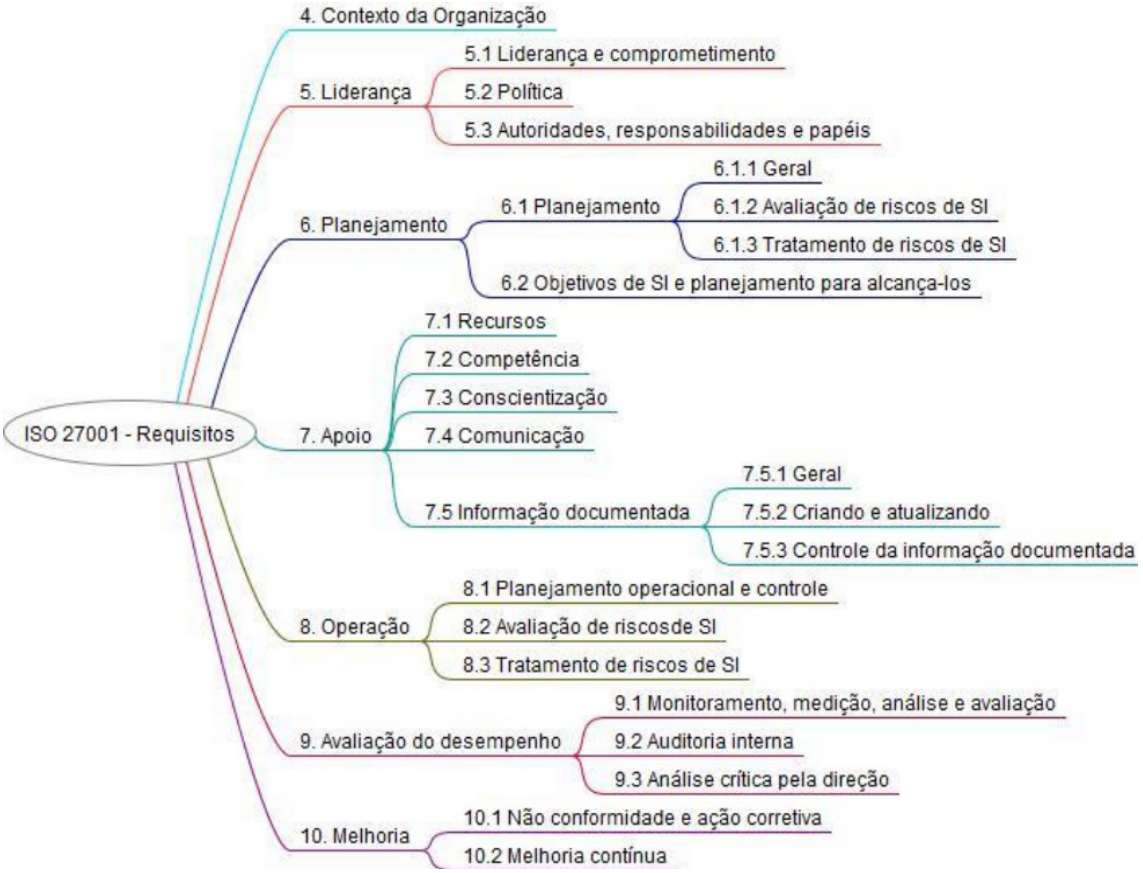
Obviamente que é extremamente necessário que todos que trabalham na organização tenham ciência da política de segurança, e a norma realiza tal prescrição.

GABARITO

1. E
2 E

ANOTAÇÕES

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)

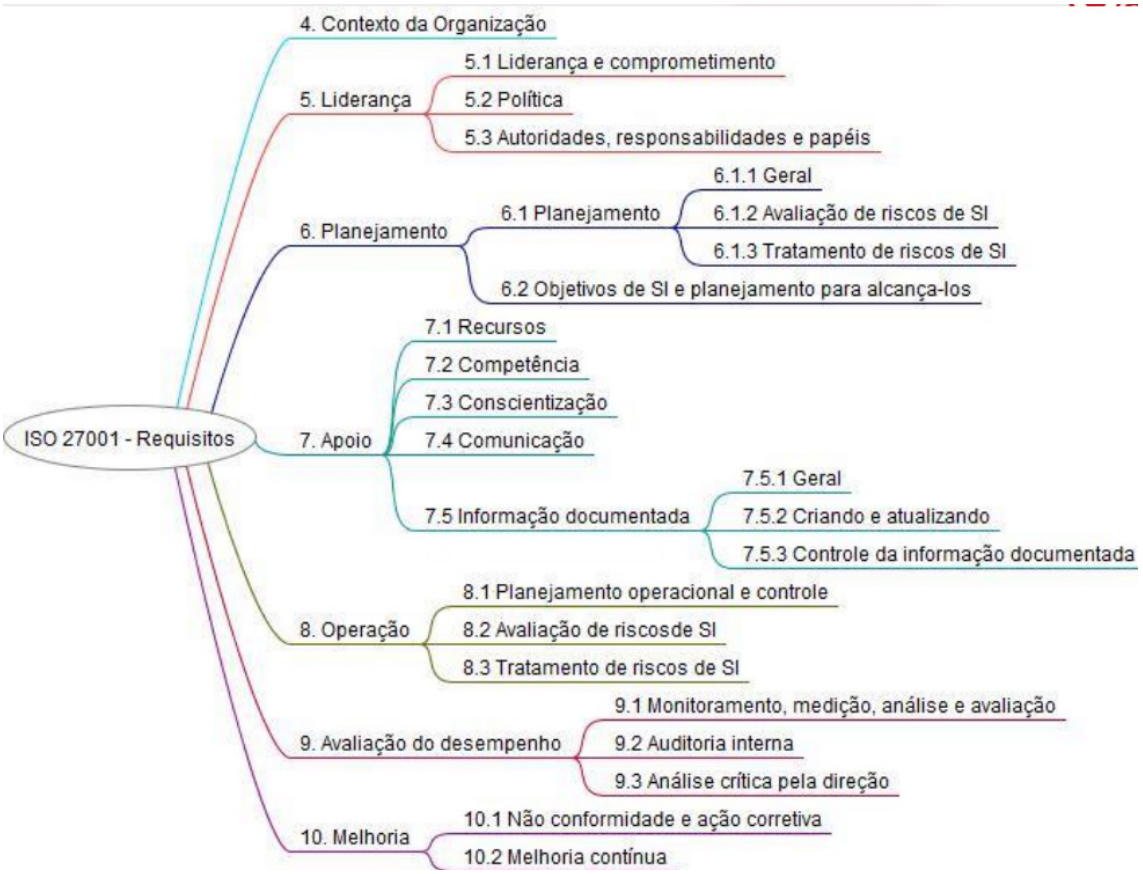
COMENTÁRIO

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

GABARITO

1. C
2. E

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.

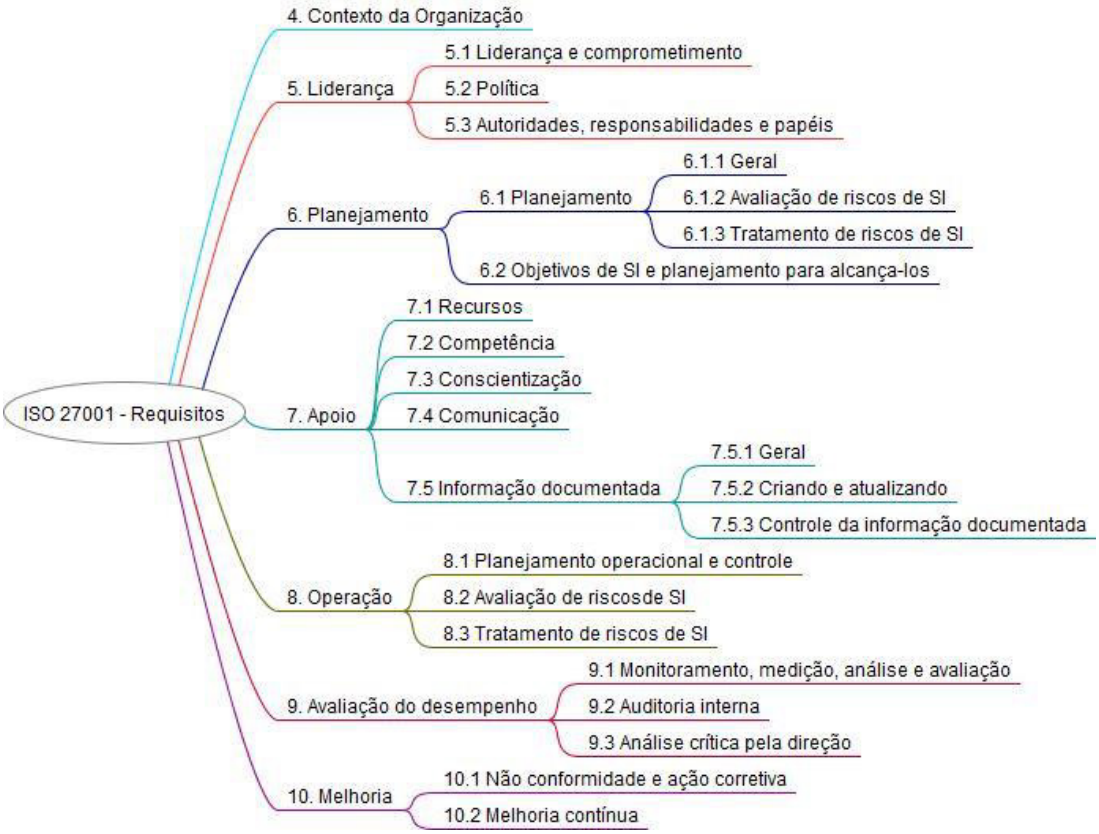
GABARITO

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

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



Melhoria

Não conformidade e ação corretiva — Quando uma não conformidade ocorre, a organização deve:

a) reagir à não conformidade, e conforme apropriado:

1) tomar ações para controlar e corrigi-la; e

2) tratar com as consequências;

Isso é uma das coisas que a organização deve fazer ao encontrar uma não conformidade. Além disso, ela deve:

b) avaliar a necessidade de ações para eliminar as causas de não conformidade, para evitar sua repetição ou ocorrência, por um dos seguintes meios:

1) analisando criticamente a não conformidade;

ANOTAÇÕES

2) determinando as causas da não conformidade; e

3) determinando se não conformidades similares existem, ou podem potencialmente ocorrer.

Ainda, a organização deve:

c) implementar quaisquer ações necessárias;

d) analisar criticamente a eficácia de quaisquer ações corretivas tomadas; e

e) realizar mudanças no sistema de gestão da segurança da informação, quando necessário.

Então, existem várias obrigações que a organização tem por obrigação realizar ao encontrar uma não conformidade.

Nesse sentido, essas ações corretivas devem ser apropriadas aos efeitos das não conformidades encontradas. A organização deve reter informação documentada como evidência da:

a) natureza das não conformidades e quaisquer ações subsequentes tomadas; e

b) resultados de qualquer ação corretiva.

Melhoria Contínua

No que diz respeito à melhoria contínua, a organização deve continuamente melhorar a pertinência, adequação e eficácia do sistema de gestão da segurança da informação.

Anexo A

A norma ISO/IEC 27001:2013 traz um anexo que faz referência aos objetivos de controle. Posto isso, os controles e objetivos de controles listados na Tabela A.1 são derivados diretamente e estão alinhados com aqueles listados na ABNT NBR ISO/IEC 27002:2013 – seções 5 a 18, e devem ser usados em alinhamento com o item 6.1.3

5m

DIRETO DO CONCURSO

1. (2018/IADES/SES-DF/ANALISTA DE SISTEMAS) De acordo com a ABNT NBR ISO/IEC 27001:2013, quando uma não conformidade ocorre, a organização deve reter informação documentada

a. como evidência dos resultados de qualquer ação corretiva.

b. dos resultados das avaliações de risco de segurança da informação.

ANOTAÇÕES

c. dos resultados do tratamento dos riscos de segurança da informação.
d. como evidência dos programas da auditoria e dos resultados desta.
e. como evidência dos resultados das análises críticas pela direção.

2. (2019/FCC/SANASA CAMPINAS/ANALISTA DE TECNOLOGIA DA INFORMAÇÃO/ SUPORTE DE INFRAESTRUTURA TI) A Norma ABNT NBR ISO/IEC 27001:2013 provê requisitos para orientar organizações que desejam implantar um sistema de gestão de segurança da informação, e

a. pode ser usada somente por partes internas da organização para avaliar sua capacidade em atender aos seus próprios requisitos de segurança da informação.
b. não inclui requisitos para avaliação e tratamento de riscos de segurança da informação, mas indica a norma que orienta sobre este assunto.
c. apresenta requisitos genéricos que podem ser aplicáveis a todas as organizações, independentemente do tipo, tamanho ou natureza.
d. possui diversos requisitos nas seções que tratam do contexto da organização (seção 4) e melhoria (seção 10) que podem ser ignorados mesmo por organizações que buscam conformidade com esta Norma.
e. possui anexo “Referência ao conjunto de potenciais riscos de segurança da informação” que estão necessariamente alinhados com a Norma ABNT NBR ISO/IEC 27002:2018.

COMENTÁRIO

10m

- a. Ela pode ser usada também pelas partes externas da organização.
- b. Ela inclui requisitos para a avaliação e tratamento de risco de segurança da informação.
- c. Os requisitos são genéricos e, com isso, podem ser utilizados por qualquer organização.
- d. Caso se busque conformidade coma norma, não se pode ignorar os requisitos que estão numa seção.

ANOTAÇÕES

GABARITO

1. a
2. 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