ISO 27001 Internal Auditor/Lead Auditor (I27001IA/LA)

Perguntas de Apoio V092020

1. Qual das seguintes alternativas não é um controle do Anexo A?

a) Políticas de segurança da informação.
b) A proteção e a privacidade de dados.
c) Políticas de continuidade do serviço.
d) Procedimentos e controles para garantir o nível exigido de continuidade da segurança da informação.

2. Quais são os controles do anexo A, segundo a norma ISO 27001?

a) Direitos de Propriedade Intelectual (DPI).
b) Terceirização do desenvolvimento de software.
c) Acordos de confidencialidade ou não-revelação.
d) Apenas A e B.
e) Apenas B e C.
f) A, B e C estão corretas.

3. Qual é a definição de disponibilidade, segundo a família de normas ISO 27000?

a) Estar acessível e pronto para o uso ou demanda de uma entidade autorizada.
b) Recurso consistente em que uma empresa seja o que afirma ser.
c) Propriedade sobre a informação para que se mantenha inacessível.
d) Nenhuma das anteriores.

4. Qual das seguintes alternativas é um requisito obrigatório da norma ISO 27001?

a) A informação documentada inclui a informação documentada exigida pela norma internacional.
b) A organização deve estabelecer os objetivos de segurança da informação nas funções e níveis pertinentes.
c) Elaborar uma "Declaração de Aplicabilidade" excluindo os controles que não serão implementados.
d) A organização deve manter a informação documentada sobre o processo de tratamento de riscos de segurança da informação.

5. Com base na ISO 19011, as atividades de preparação da auditoria incluem?

a) Revisar a documentação.
b) Preparar o programa de auditoria.
c) Atribuir o trabalho à equipe auditora.
d) Preparar os documentos de trabalho.
e) Nenhuma das anteriores, estes tópicos são da etapa de condução da auditoria.
f) Todas as anteriores.

6. Qual das seguintes alternativas fazem parte do estabelecimento do programa de auditoria?

a) Definir a competência do gestor do programa de auditoria.
b) Estabelecer a duração do programa de auditoria.
c) Identificar e avaliar os riscos do programa de auditoria.
d) Apenas A e B.
e) Apenas A e C.
f) A, B e C estão corretas.

7. Todos os controles do anexo A devem ser implementados no sistema de gestão de segurança da informação?

a) Verdadeiro.
b) Falso.

8. Qual ou quais das alternativas são requisitos de documentação na norma ISO 27001 e/ou seu anexo?

a) Declaração de aplicabilidade.
b) Programa de tratamento de riscos.
c) Informativo de avaliação de riscos.
d) Apenas A e B.
e) Apenas A e C.
f) A, B e C estão corretas.

9. Qual auditor é responsável pela liderança da equipe de auditoria?

a) O co-auditor.
b) O representante da direção.
c) O auditor líder.
d) O auditor interno.

10. Qual das alternativas abaixo faz parte da equipe de auditoria, mas não audita?

a) Auditor Júnior.
b) Auditor Interno.
c) Observador.
d) Auditor Líder.

11. O que denomina-se conjunto de uma ou mais auditorias planejadas no período?

a) Plano de auditoria.
b) Programa de auditoria.
c) Lista de verificação geral.
d) Sistema de gestão.

12. O que é uma não-conformidade em uma auditoria?

a) O não cumprimento do programa planejado pela auditoria.
b) O não cumprimento de um requisito da norma.
c) Fazer uma lista de verificação e não usá-la durante a auditoria.
d) Um requisito que o auditor acredita não ser verdadeiro e por isso não o analisa.

13. Quais das alternativas formam os princípios do auditor?

a) Ter discrição como parte de seu comportamento ético.
b) Exatidão nos relatórios de auditoria.
c) Devido cuidado professional.
d) Todas as anteriores.

14. O que deve ser feito durante uma reunião de abertura de auditoria de terceira parte?

a) Não existe auditoria de terceira parte.
b) Revisar o escopo.
c) Determinar que o único ponto de contato com o acreditador seja auditor líder.
d) Não responder perguntas do processo até o início da auditoria.

15. Quais os métodos de auditoria que existem?

a) Auditoria remota.
b) Auditora no local.
c) Apenas A.
d) Apenas B.
e) A e B estão corretas.

16. Selecione a melhor resposta, para a realização de auditoria interna no interior de uma organização:

a) Determinar a conformidade do sistema de gestão as oportunidades de melhoria.
b) Determinar a possibilidade de certificar- se por um provedor de serviços.
c) Pesquisar violações sob o critério do auditor.
d) Cumprir a exigência da norma.

17. Para auditores lideres com mais de 3 anos exercidos como auditor, é possível que por sua experiência não se façam um programa de auditoria.

a) Verdadeiro.
b) Falso.

18. A lista de verificação pode ser definida através de:

a) Listagem exaustiva dos requisitos da norma.
b) Guia usada pelo auditor para avaliar alguns requisitos da norma.
c) Listagem das atividades a realizar durante a reunião de abertura.
d) Material exigido para o programa de auditoria.

19. Apenas se documentam as não-conformidades de um sistema de gestão se estas forem maiores que “dois”?

a) Verdadeiro, porquê duas não-conformidades determinam que o sistema está fora de controle.
b) Verdadeiro, porquê são exigidas duas não-conformidades para a não certificação um sistema.
c) Falso, todas as não conformidades devem ser documentadas.
d) Falso, apenas a partir de três não cumprimentos de um requisito se documenta uma não-conformidade.

20. Se define como "Situação que potencialmente pode afetar o sistema de gestão de qualidade":

a) Não-conformidade menor.
b) Descoberta.
c) Observação.
d) Registro de Melhoria.

21. Durante uma reunião de encerramento da auditoria externa NÂO se deve?

a) Fazer o resumo do processo.
b) Explicar sobre a visão do auditor líder porquê o requisito foi violado.
c) Estipular datas para o encerramento das ações corretivas.
d) Confirmar o escopo da auditoria.

22. Não são importantes na redação das não-conformidades:

a) As opiniões do auditor.
b) A evidência.
c) A referência aos requisitos da norma.
d) Escrever sobre um requisito por vez.

23. A norma ISO 27001, é a única forma que uma empresa pode avaliar a capacidade da organização para cumprir com suas próprias exigências de segurança.

a) Verdadeiro.
b) Falso.

24. De acordo com a norma ISO 27001, os requisitos das partes interessadas que são relevantes para a segurança da informação devem ser:

a) Requisitos internos.
b) Requisitos externos.
c) Requisitos contratuais.
d) Apenas A e C.
e) Apenas B e C.
f) A, B e C são corretas.

25. Fazem parte da implementação do programa de auditoria:

a) Definir os objetivos, abrangência e critérios para uma auditoria individual.
b) Selecionar os métodos de auditoria.
c) Selecionar os membros da equipe auditora.
d) Atribuir responsabilidades para a auditoria individual ao líder da equipe auditora.
e) Todas as anteriores.

26. São procedimentos documentados exigidos na norma ISO 27001 ou seu anexo dependendo da declaração de aplicabilidade:

a) Procedimentos de gestão de incidentes.
b) Procedimentos de continuidade do negócio.
c) Procedimentos operacionais para a gestão de TI.
d) Apenas A e B.
e) Apenas A e C.
f) Apenas B e C.
g) A, B e C estão corretos.

27. A norma ISO 27001 e/ou seu anexo, onde for aplicada exige como requisito?

a) Programa de tratamento de riscos internos.
b) Programa de tratamento de riscos.
c) Cronograma de tratamento de riscos.
d) Política específica de tratamento de riscos.

28. São registros exigidos pela norma ISO 27001 ou pela aplicação do controle do anexo:

a) Registros de treinamento, habilidades, experiência e qualificações.
b) Registros de incidentes de segurança.
c) Apenas A.
d) Apenas B.
e) A e B são registros exigidos.

29. São resultados exigidos pelos controles da norma que poderiam estar sujeitos à auditoria:

a) Resultados de monitoramento e medição.
b) Resultados de auditorias internas.
c) Resultados de revisão da gestão.
d) Resultados de ações corretivas.
e) Todas estão corretas exceto A.
f) Todas estão corretas exceto C.
g) A, B, C e D estão corretas.

30. É possível necessitar criar uma política de controle de acesso no momento de aplicar os controles da Norma.

a) Verdadeiro.
b) Falso.

31. A Declaração de aplicabilidade é MELHOR resumida como:

a) Um requisito da norma.
b) A forma de estabelecer que não será incluída no escopo.
c) O principal documento a ser avaliado na auditoria.
d) A justificativa da exclusão de qualquer um dos controles do anexo A.

32. A organização deve determinar a necessidade de comunicação interna e externa que inclua:

a) Quem faz a comunicação.
b) A quem se comunica.
c) O que se comunica.
d) Todas as anteriores.

33. O tamanho da organização e seu tipo de atividade, processos, produtos e serviços podem determinar o escopo da informação documentada na ISO 27001?

a) Verdadeiro.
b) Falso.

34. Os processos contratados externamente estão fora do escopo de controle e quando são documentados estão sempre dentro das exclusões do sistema de gestão.

a) Verdadeiro.
b) Falso.

35. Planejar, criar, implementar e manter um único programa de auditoria é um requisito da norma ISO 27001?

a) Verdadeiro.
b) Falso.

36. O requisito da norma onde se refere que à alta direção deve revisar o sistema de gestão da segurança da informação da organização, está estabelecido para que seja realizado:

a) Ao menos a cada seis meses.
b) Ao menos em cada auditoria interna.
c) A intervalos planejados definidos no sistema.
d) Não se faz revisão do sistema de segurança da informação.

37. De acordo com a ISO 27001, com base nas atuais tendências e mantendo sempre um enfoque proativo não se deve excluir o controle do trabalho "home office".

a) Verdadeiro.
b) Falso.

38. A seguinte definição se refere a qual conceito: "Incidente único ou série de incidentes da segurança da informação, inesperados ou não desejados".

a) Problema de segurança da informação.
b) Incidência de segurança da informação.
c) Alerta de segurança da informação.
d) Nenhuma das anteriores.

39. De acordo com a ISO 27000, a seguinte definição corresponde a: "Aplicações, serviços, ativos de tecnologia da informação e outros compostos para tratar a informação".

a) Sistema de segurança da informação.
b) Sistema de informação.
c) Sistema de gestão de segurança da informação.
d) Nenhuma das anteriores.

40. A definição "Magnitude de um risco ou combinação de riscos, expressados em termos da combinação das consequências e de sua probabilidade". Se refere a:

a) Declaração de aplicabilidade.
b) Análise de risos.
c) Nível de riscos.
d) Gestão de riscos.

Respostas

1.	C
2.	F
3.	A
4.	C
5.	F
6.	F
7.	B
8.	F
9.	C
10.	C
11.	B
12.	B
13.	D
14.	B
15.	E
16.	A
17.	B
18.	B
19.	C
20.	C
21.	B
22.	A
23.	B
24.	F
25.	E
26.	G
27.	B
28.	E
29.	G
30.	A
31.	A
32.	D
33.	A
34.	B
35.	B
36.	C
37.	B
38.	B
39.	B
40.	C