ISO 27001 FOUNDATION (I27001F)

CertiProf®
Professional Knowledge
ISO 27001 FOUNDATION
I27001F

CertiProf®
Professional Knowledge

(I27001F) VERSÃO 092020

www.certiprof.com

ISO 27001 Foundation (I27001F)

Perguntas de Apoio V092020

1. A aprovação do plano de tratamento de riscos e a aceitação do risco residual é responsabilidade: (Selecione a melhor resposta).

a) Alta direção.
b) Proprietário do risco.
c) Diretor de Informação.
d) Diretor de Segurança.

2. Qual dos seguintes não é um requerimento da ISO/IEC 27001? (Selecione a melhor resposta).

a) Ter um papel dedicado como Gerente de Segurança da Informação.
b) Que a alta direção promova a melhoria contínua.
c) Que sejam comunicados os objetivos de segurança da informação.
d) Documentar o plano de tratamento de risco.

3. Os objetivos de segurança da informação devem ser consistentes com: (Selecione a melhor resposta).

a) O plano de tratamento de risco.
b) A política de segurança da informação.
c) A declaração de aplicabilidade.
d) A metodologia de avaliação de risco.

4. A organização possui vários locais que executam backups de informações e determina que eles precisam documentar seu processo para manter a consistência e garantir a eficácia. Este documento deve ser: (Selecione a melhor resposta).

a) Aprovado pelo comitê de direção de segurança da informação.
b) Disponível e apropriado para uso, quando e onde seja necessário.
c) Listado na matriz mestra de documentos.
d) Disponível no formato eletrônico e impresso.

5. O fornecedor de seguros de saúde mantém bases de dados de informação confidencial de clientes. A consequência potencial de divulgar informação privada de qualquer cliente deve ser mencionada: (Selecione a melhor resposta).

a) Na declaração de missão da organização.
b) No plano de tratamento de risco.
c) No plano de conformidade.
d) Na avaliação de risco.

6. O escopo do SGSI de uma organização gira em torno da prestação de serviços financeiros. Na política de segurança da informação, a alta administração declara sua intenção de operar dentro dos requisitos estaduais e federais. O restante da política de segurança da informação se concentra em como a TI fornecerá serviços financeiros. Esta política: (Selecione a melhor resposta).

a) Não está de acordo com a ISO/IEC 27001.
b) Está de acordo com a ISO/IEC 27001.
c) Está de acordo com ISO/IEC 27001, mas poderia ser melhorada.
d) Não se aplica à linhas específicas de negócios.

7. Uma organização de desenvolvimento de software decidiu terceirizar seu help desk, que também lida com chamadas de incidentes de segurança. A organização recebe um relatório do help desk, subcontratado mensalmente, que contém métricas de desempenho de chamadas que consistem em tempo médio de espera, tempo ocioso do agente e número médio de chamadas na fila. A organização usa o relatório como um meio de demonstrar controle sobre o suporte técnico do ponto de vista dos requisitos de segurança da informação. Isto está de acordo coma ISO/IEC 27001?

a) Verdadeiro.
b) Falso.

8. As atividades coordenadas para dirigir e controlar uma organização com relação ao risco são conhecidas como: (Selecione a melhor resposta).

a) Avaliação do risco.
b) Tratamento do risco.
c) Gestão do risco.
d) Estimação do risco.

9. A propriedade de proteger a exatidão e integridade da propriedade é: (Selecione a melhor resposta).

a) Integridade.
b) Correção.
c) Interoperatividade.
d) Não rejeição.

10. Uma medida que está modificando o risco pode ser referida como: (Selecione a melhor resposta).

a) Remediação do risco.
b) Sistema de Gestão de Segurança da Informação (SGSI).
c) Controle.
d) Análise de impacto do negócio.

11. Pode-se dizer que o SGSI da organização é efetivo se: (Selecione a melhor resposta).

a) O help desk minimizou sua equipe e ainda atinge seus objetivos.
b) Tem sido demonstrado que todas as áreas do processo têm planos e estabeleceram objetivos, tomaram ações para melhorar.
c) As equipes de auditoria interna e compliance foram identificadas numerosas.
d) A administração deu ao gerente de TI autoridade absoluta sobre segurança e concedeu ao departamento de TI um orçamento limitado.

12. Um controle físico foi implementado no SGSI de um hospital. Eles determinaram que seu controle particular deve ser medido e garantem que ele seja medido. Como que as cargas de trabalho e os cronogramas mudam constantemente, eles não determinaram uma única pessoa para fazer a medição. Isto está de acordo com a ISO/IEC 27001:

a) Verdadeiro.
b) Falso.

13. O SGSI de um hospital está sujeito a requerimentos legais. Do ponto de vista de um sistema de gestão, a avaliação da conformidade legal consistirá em: (Selecione a melhor resposta).

a) Confirmar que existe um processo dentro do hospital para manter o cumprimento dos requerimentos legais e regulatórios.
b) Nenhuma ação adicional visto que os padrões ISO lidam somente com a conformidade.
c) Entrar em contato com o departamento jurídico para confirmar que não há situações legais pendentes.
d) Analisar a declaração do Conselho de Diretores do hospital onde eles estipulam que manterão as exigências legais.

14. A conformidade é vista como satisfazer os requisitos do ponto de vista de um sistema de gestão, enquanto que o cumprimento é visto como atender aos requisitos de uma perspectiva legal; isto é:

a) Verdadeiro.
b) Falso.

15. Uma operação financeira selecionou suas operações de troca de valores mobiliários, pois o escopo de seu SGSI, revisando sua política de segurança de informações, não pode ver onde a organização se compromete a cumprir as regulamentações de segurança do governo. Isto cumpre as exigências da ISO/IEC 27001?

a) Verdadeiro.
b) Falso.

16. Uma organização fez das operações de seu processamento de reclamações o escopo de seu SGSI. Os controles que selecionou foram determinados em qual processo? (Selecione a melhor resposta).

a) Política de segurança.
b) Revisão da administração.
c) Avaliação de risco.
d) Tratamento do risco.

17. Numa organização formada por dez laboratórios médicos, onde os pacientes passam por testes e estão sob a direção de um escritório central. A alta gerência determinou que o escopo de seu SGSI será a proteção de todas as informações pessoais dos pacientes e cobrirá a sede central. Isto cumpre as exigências da ISO/IEC 27001?

a) Verdadeiro.
b) Falso.

18. Segundo a ISO/IEC 27001, uma avaliação de risco incluirá: (Selecione a melhor resposta).

a) Possibilidade de ocorrência de um risco.
b) Partes interessadas do SGSI.
c) Opções para tratamento de risco de segurança.
d) Resultados de medidas de controle.

19. Uma organização definiu um processo de avaliação de risco. Este é anualmente realizado em suas instalações locais e em todos os seus locais no exterior. Isso produz consistência e resultados comparáveis?

a) Verdadeiro.
b) Falso.

20. Uma organização que identificou exigências regulamentares como um fator externo e mantém a conformidade regulatória como um objetivo de segurança da informação exigirá o que, em sua avaliação de risco: (Selecione a melhor resposta).

a) O risco associado com o cumprimento de obrigações contratuais.
b) A possibilidade de ser descoberto operando fora das exigências regulatórias.
c) As potenciais consequências associadas ao não cumprimento das exigências regulatórias.
d) Um processo documentado para manter a conformidade com os requisitos legais e regulamentares.

21. Uma organização fez das operações de vendas o escopo de seu SGSI. Uma avaliação de risco para as informações de vendas de uma organização deve incluir: (selecione a melhor resposta).

a) O valor financeiro associado a perda de confidencialidade na informação de vendas.
b) O risco associado a vendedores que transportam a informação de vendas em seus Laptops.
c) Uma política de uso aceitável de ativos da empresa.
d) Criptografia de nomes e endereços de clientes.

22. Uma grande cadeia de distribuição nacional tem o objetivo de garantir que os clientes possam inserir a informação de sua conta ao menos 98 % das vezes. A avaliação de risco deverá: (Selecione a melhor resposta).

a) Incluir o risco associado a disponibilização da informação.
b) Garantir que a permissão de acesso aos clientes satisfaça as exigências regulatórias.
c) Incluir o risco associado ao desenvolvimento do software do cliente por uma empresa de desenvolvimento subcontratada.
d) Ser completado pelo departamento de TI, visto que é o responsável pelos arquivos de contas dos clientes.

23. A Declaração de Aplicabilidade deve conter os controles necessários para implementar a opção de tratamento de risco escolhida, sejam implementados ou não, e ... (Selecione a melhor resposta).

a) A lista de todos os ativos aos quais se aplicam os controles e riscos associados.
b) A justificativa para a seleção de controles e a exclusão de qualquer controle.
c) Uma lista de todas as políticas e procedimentos associados e os controles com os quais se relacionam.
d) Os valores totais de risco calculado, ordenado do maio para o menor.

24. Se um dos objetivos de segurança da informação de uma organização é impedir a divulgação não autorizada de informações confidenciais no caso de um dispositivo portátil ser roubado, os controles selecionados para tratar do risco e na Declaração de Aplicabilidade devem incluir: (Selecione a melhor resposta).

a) Responsabilidades do usuário.
b) Criptografia.
c) Proteção contra Malware.
d) Segurança do RH – Prévia a contratação.

25. A avaliação de risco de segurança da informação deve ser realizada: (Selecione a melhor resposta).

a) Anualmente.
b) Semestralmente.
c) Em intervalos planejados.
d) Apenas quando for especificado pelo auditor.

26. Se uma organização que planeja fazer uma mudança em um processo dentro do escopo do seu SGSI, deve: (Selecione a melhor resposta).

a) Calcular os custos da mudança.
b) Atualizar a política do SGSI.
c) Controlar a mudança.
d) Atualizar os objetivos do SGSI.

27. Se mudanças significativas ocorrem ou são propostas, a organização deve: (Selecione a melhor resposta).

a) Implementar controles para mitigar o novo risco.
b) Ter na administração um conselho de revisão.
c) Revisar e atualizar seus objetivos de segurança da informação.
d) Realizar uma avaliação de risco de segurança da informação.

28. Para cumprir as exigências de licenciamento de software, a organização usará qual controle? (Selecione a melhor resposta).

a) A.5.1.1- Políticas para a segurança da informação.
b) A.18.1.2 – Revisão independente da segurança da informação.
c) A.9.2.3 - Gestão de privilégios de acesso.
d) A.12.1.4 - Separação dos recursos de desenvolvimento, prova e operação.

29. Qual controle do anexo A seria selecionado para mitigar o risco dos funcionários usarem equipamentos de treinamento de propriedade da organização, para uso pessoal? (Selecione a melhor resposta).

a) A.8.1.3 – Gerenciamento de suporte removível.
b) A.7.1.2 – Termos e condições de uso.
c) A.7.2.3 – Processo disciplinar.
d) A.18.2.2 – Cumprimento das políticas e normas de segurança.

30. Qual controle poderia ser selecionado para mitigar o risco associado com a atualização de software nos servidores empresariais? (Selecione a melhor resposta).

a) A.14.2.2 – Procedimento de controle de mudanças no sistema.
b) A.12.7.1 – Controles de auditoria de sistemas de informação.
c) A.12.1.2 – Gestão de Mudanças.
d) A.9.4.5 – Controle de acesso ao código fonte dos programas.

31. O termo "Achados de auditoria" automaticamente significa Não Conformidade.

a) Verdadeiro
b) Falso

32. Uma pessoa ou organização que solicita uma auditoria é referida como: (Selecione a melhor resposta).

a) Auditor.
b) Auditado.
c) Cliente de Auditoria.
d) Equipe de Auditoria.

33. Quando se estabelece um programa de auditoria para um sistema de gerenciamento, a organização deverá dar prioridade aos recursos de auditoria para tratar: (Selecione a melhor resposta).

a) Necessidades do Negócio.
b) Riscos.
c) Oportunidades de mercado.
d) Integração aos planos de continuidade do negócio.

34. Os objetivos da auditoria podem incluir:

a) Avaliação da efetividade do sistema de gerenciamento.
b) Manutenção dos registros de auditoria.
c) Seleção de um líder de equipe.
d) Oferecimento de certificação para uma norma.

35. O escopo de uma auditoria sempre é o mesmo que o escopo do sistema de gerenciamento.

a) Verdadeiro.
b) Falso.

36. Qual dos seguintes fatores seriam levados em consideração para determinar a viabilidade de uma auditoria? (Selecione a melhor resposta).

a) Temas relacionados com o relatório da auditoria.
b) Disponibilidade de informação suficiente para planejar a auditoria.
c) Cooperação adequada da equipe de auditoria.
d) Diretrizes do gerente de admissão.

37. Os documentos de trabalho do auditor podem incluir: (Selecione a melhor resposta).

a) O código de conduta do auditor.
b) Identificação, incluindo fotografia.
c) Listas de verificação, planos e formatos de levantamento de evidência.
d) Instruções para a instalação que será auditada.

38. A informação aceita como evidência de auditoria deverá ser: (Selecione a melhor resposta).

a) Verificável.
b) Documentada.
c) Identificada pelo menos duas vezes.
d) Confirmada por guia.

39. Um relatório de auditoria deverá incluir, ou se referir a:

a) Uma lista completa de todos os funcionários da organização auditada.
b) Uma lista completa de todos os documentos utilizados durante a auditoria.
c) Uma descrição completa e detalhada do processo de auditoria.
d) Um resumo dos achados da auditoria.

40. O relatório da auditoria deverá ser distribuído para:

a) Os destinatários definidos no procedimento ou plano de auditoria.
b) Os destinatários definidos pelo líder da equipe de auditoria.
c) Os destinatários definidos pela direção da organização auditada.
d) Os destinatários definidos pelo representante da gerência da organização auditada.

Respostas

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