



# Meus Simulados

Teste seu conhecimento acumulado

Disc.: **INTRODUÇÃO À SEGURANÇA DA INFORMAÇÃO**

Aluno(a): **DAVID PERES**

**202302645471**

Acertos: **10,0** de 10,0

**17/03/2023**

## 1ª Questão

Acerto: **1,0 / 1,0**

Observe o que diz o item 6.1.3 da norma técnica ABNT NBR ISO/IEC 27001:2013:

### 6.1.3 Tratamento de riscos de segurança da informação

A organização deve definir e aplicar um processo de tratamento de riscos de segurança da informação para:


(...)

b) determinar todos os controles que são necessários para implementar as opções escolhidas do tratamento do risco da segurança da informação.

d) elaborar uma declaração de aplicabilidade, que contenha os controles necessários (ver 6.1.3 b) e c)), e a justificativa para inclusões, sejam eles implementados ou não, bem como a justificativa para a exclusão dos controles do Anexo A.

Uma empresa que está se preparando para sofrer uma auditoria checkou que não constam na Declaração de Aplicabilidade, a exclusão e nem a justificativa de exclusão dos objetivos de controle e controles constantes na norma.

De acordo com o item 6.1.3 da norma, isso é passível de ser classificado como "Não-conformidade"?

- ☐ Indica uma simples observação a ser feita
- ☐ Falta informação nessa checagem para classificar
- ☐ Não se aplica a esta norma
- ☒  Sim
- ☐ Não

Respondido em 17/03/2023 19:18:39


### Explicação:

A resposta correta é: Sim.

## 2ª Questão

Acerto: **1,0 / 1,0**

Assinale a assertiva que representa um dos benefícios para a adoção da norma ABNT NBR ISO/IEC 27001:2013 por uma organização:

- ☒  Oportunidade de identificar e eliminar fraquezas
- ☐ Não participação da gerência na Segurança da Informação

- ☐ Mecanismo para eliminar o sucesso do sistema
- ☐ Fornece insegurança a todas as partes interessadas
- ☐ Isola recursos com outros sistemas de gerenciamento

Respondido em 17/03/2023 19:18:57

**Explicação:**

A resposta correta é: Oportunidade de identificar e eliminar fraquezas.

**3ª Questão**

Acerto: 1,0 / 1,0

Quanto mais complexa for uma senha, mais difícil será para o invasor quebrá-la com o uso de programas, exclusivamente. Levando em consideração essa afirmação, selecione a opção que possui a senha com maior grau de dificuldade de ser descoberta por um invasor:

- ☐ MaRiA96
- ☐ X1234Y1
- ☒ aX1!@7s5
- ☐ SeNhA123
- ☐ 69910814sa

Respondido em 17/03/2023 19:19:14

**Explicação:**

A resposta correta é: aX1!@7s5

**4ª Questão**

Acerto: 1,0 / 1,0

O sistema de backup de missão crítica é também chamado de ambiente de:

- ☐ Ransomware.
- ☐ Personal Identification Number.
- ☐ Daily Backup.
- ☒ Disaster Recovery.
- ☐ Personal Unblocking Key.

Respondido em 17/03/2023 19:19:34

**Explicação:**

A resposta correta é: Disaster Recovery.

**5ª Questão**

Acerto: 1,0 / 1,0

Um membro da comissão de segurança precisa saber informações sobre cada um dos processos da GR. Ele consultará uma dentre as normas da família ISO/IEC 27000, que definem uma série de normas relacionadas à segurança da informação. Ele precisa obter a norma:

- ☐ ISO/IEC 27002
- ☐ ISO/IEC 27000
- ☐ ISO/IEC 27001
- ☒ ISO/IEC 27005
- ☐ ISO/IEC 31000

Respondido em 17/03/2023 19:20:58

**Explicação:**

A resposta correta é: ISO/IEC 27005

**6ª Questão**

Acerto: 1,0 / 1,0

Um Plano de Recuperação de Desastres (PRD) é o documento que define os recursos, ações, tarefas e dados requeridos para administrar \_\_\_\_\_ e \_\_\_\_\_ que suportam os Processos de Negócio. Selecione a opção que preenche corretamente as lacunas:

- ☐ o plano de operação; avaliar os pontos de controle.
- ☐ o plano de continuidade; tratamento dos eventos previsíveis.
- ☒ o processo de recuperação; restauração dos componentes.
- ☐ as consequências dos desastres previsíveis; na criação de planos de ação.
- ☐ o plano de continuidade; tratamento dos eventos imprevisíveis.

Respondido em 17/03/2023 19:22:07

**Explicação:**

A resposta correta é: o processo de recuperação; restauração dos componentes.

**7ª Questão**

Acerto: 1,0 / 1,0

Redes de computadores conectadas à internet são alvos de invasões por parte de hackers. A ferramenta para permitir o acesso à rede apenas por endereços autorizados é:

- ☐ Antivírus.
- ☐ Criptografia.
- ☐ Modem.
- ☒ Firewall.
- ☐ Certificado digital.

Respondido em 17/03/2023 19:23:09

**Explicação:**

A resposta correta: Firewall.

**8ª Questão**

Acerto: 1,0 / 1,0

A informação é estruturação e organização dos dados. Assim, os dados constituem a matéria prima da informação. Dentro dos aspectos da segurança da informação que exigem atenção são: confidencialidade, integridade e disponibilidade. A respeito da:

I - Na confidencialidade, as informações serão acessadas por quem tiver a devida autorização.

II - Na integridade, a informação que chega ao receptor pode não ser a que foi enviada pelo emissor

III - Disponibilidade, as informações podem ser acessadas por sistemas autorizados para tal fim.

Podemos considerar como corretas:

- ☐ I, II, III.
- ☐ II e III.
- ☐ III apenas.
- ☐ I apenas.
- ☒ I e III.

Respondido em 17/03/2023 19:24:32

#### Explicação:

A resposta correta é: I e III.

Na integridade, a informação que chega ao receptor é a que foi enviada pelo emissor. Ou seja, não houve modificação no envio da informação.



Questão

Acerto: 1,0 / 1,0

Indique a alternativa que pode conter um relacionamento mais apropriado entre os conceitos de AMEAÇA, IMPACTO, INCIDENTE e VULNERABILIDADE tratados pela Gestão de Riscos na Tecnologia da Informação.

- ☐
- | ATIVO            | VULNERABILIDADE                      | INCIDENTE/AMEAÇA           | IMPACTO   |
|------------------|--------------------------------------|----------------------------|---|
| Firewall da rede | Sem contrato de manutenção periódica | Defeito no <i>firmware</i> | Perda da confidencialidade nos acessos a internet |
- ☐
- | ATIVO        | VULNERABILIDADE                               | INCIDENTE/AMEAÇA   | IMPACTO     |
|--------------|---|--------------------|-------------|
| Servidor Web | Servidor de aplicação acessível pela internet | Ataque Hacker DDoS | Integridade |
- ☐
- | ATIVO        | VULNERABILIDADE    | INCIDENTE/AMEAÇA                             | IMPACTO           |
|--------------|--------------------|--|-------------------|
| Servidor Web | Ataque Hacker DDoS | Falta de atualizações do sistema operacional | Indisponibilidade |
- ☒
- | ATIVO                 | VULNERABILIDADE                              | INCIDENTE/AMEAÇA                          | IMPACTO   |
|-----------------------|--|---|---|
| Servidor de aplicação | Falta de atualizações do sistema operacional | Exploração de vulnerabilidades conhecidas | Perda de Confidencialidade, Integridade e Disponibilidade |
- ☐
- | ATIVO            | VULNERABILIDADE              | INCIDENTE/AMEAÇA    | IMPACTO                              |
|------------------|------------------------------|---------------------|--------------------------------------|
| Firewall da rede | Falta de atualizações do IOS | Perda de desempenho | Não suporta atualizações de hardware |

Respondido em 17/03/2023 19:26:22

#### Explicação:

A resposta correta é:

ATIVO	VULNERABILIDADE	INCIDENTE/AMEAÇA	IMPACTO
Servidor de aplicação	Falta de atualizações do sistema operacional	Exploração de vulnerabilidades conhecidas	Perda de Confidencialidade, Integridade e Disponibilidade



Questão

Acerto: 1,0 / 1,0

É um tipo de malware feito para extorquir dinheiro de sua vítima. Esse tipo de ciberataque irá criptografar os arquivos do usuário e exigir um pagamento para que seja enviada a solução de descryptografia dos dados da vítima. O scareware é seu tipo mais comum e usa táticas ameaçadoras ou intimidadoras para induzir as vítimas a pagar.

O texto se refere ao:

- ☒ Ransomware
- ☐ Spyware
- ☐ DDoS
- ☐ Botnet
- ☐ Spam

Respondido em 17/03/2023 19:29:31

**Explicação:**

A resposta correta é: Ransomware