



Meus Simulados

Teste seu conhecimento acumulado

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

Aluno(a): XXXXXXXXXX

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

29/04/2023



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"?

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

Respondido em 29/04/2023 20:48:52

Explicação:

A resposta correta é: Sim.



2ª

Questão

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

O item 12.2.1 da norma ABNT NBR ISO/IEC 27002:2013 diz respeito aos controles contra *malware*, cujas diretrizes para implementação recomendam a proteção contra códigos maliciosos baseada em softwares de detecção de *malware* e reparo, na conscientização da informação, no controle de acesso adequado e nos planos de continuidade de negócio.

Com base no acima exposto, e no seu conhecimento de segurança da informação e sistemas de computação, marque a alternativa que possui uma das diretrizes recomendadas:

- ☐ Instalar e atualizar regularmente *softwares* de detecção e remoção de *malware*, independentemente da fabricante, procedência e confiabilidade, para o exame de computadores e mídias magnéticas.
- ☐ Estabelecer uma política informal proibindo o uso de *softwares* autorizados.
- ☒ Estabelecer uma política formal para proteção contra os riscos associados com a importação de arquivos e *softwares*, seja de redes externas, ou por qualquer outro meio, indicando quais medidas preventivas devem ser adotadas.
- ☐ Conduzir análises informais, esporádicas e descompromissadas dos *softwares* e dados dos sistemas que suportam processos críticos de negócio.
- ☐ Ignorar informalmente a presença de quaisquer arquivos não aprovados ou atualização não autorizada.

Respondido em 29/04/2023 20:50:00

Explicação:

A resposta correta é: Estabelecer uma política formal para proteção contra os riscos associados com a importação de arquivos e *softwares*, seja de redes externas, ou por qualquer outro meio, indicando quais medidas preventivas devem ser adotadas.



3ª 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.*
- ☐ *Personal Unblocking Key.*
- ☒ *Disaster Recovery.*

Respondido em 29/04/2023 20:50:05

Explicação:

A resposta correta é: *Disaster Recovery.*



4ª Questão

Acerto: 1,0 / 1,0

Em relação ao backup incremental, selecione a opção **correta**:

- ☒ É a cópia de todos os dados que foram modificados desde o último backup de qualquer tipo.
- ☐ Faz cópias de todos dados, inclusive dos logs de transações associados, para outro conjunto de mídia, que pode ser fita, disco, um DVD ou CD.
- ☐ É exatamente igual ao backup diferencial.
- ☐ Também é chamado de backup incremental cumulativo.
- ☐ É a cópia dos dados criados e modificados desde o último backup.

Respondido em 29/04/2023 20:50:34

Explicação:

A resposta correta é: É a cópia de todos os dados que foram modificados desde o último backup de qualquer tipo.



5ª Questão

Acerto: 1,0 / 1,0

Um funcionário de uma empresa concluiu que existe uma probabilidade de 67% de sobrecarga e problemas no serviço de distribuição de conteúdo de vídeo em um eventual aumento na demanda do servidor. Dentro da GR, essa conclusão pode ser obtida na etapa de:

- ☒ Processo de avaliação de riscos.
- ☐ Definição do contexto.
- ☐ Terminação de riscos.
- ☐ Monitoramento e controle de riscos.
- ☐ Aceitação do risco (residual).

Respondido em 29/04/2023 20:50:51

Explicação:

A resposta correta é: Processo de avaliação de riscos.



6ª Questão

Acerto: 1,0 / 1,0

O Risco é um conceito importante quando se trata do Plano de Continuidade de Negócios (PCN). A respeito do Risco, selecione a opção correta:

- ☐ Normalmente não podem ser controlados.
- ☐ Não pode ser analisado em termos probabilísticos, uma vez que sempre está presente.
- ☒ Possível evento que pode causar perdas ou danos, ou dificultar o atingimento de objetivos.
- ☐ É um conceito abstrato e com baixa chance de se transformar em um desastre.
- ☐ Evento súbito e imprevisto que provoca grandes perdas ou danos a uma organização.

Respondido em 29/04/2023 20:51:19

Explicação:

A resposta correta é: Possível evento que pode causar perdas ou danos, ou dificultar o atingimento de objetivos.



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:

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

Respondido em 29/04/2023 20:51:37

Explicação:

A resposta correta: Firewall.



8ª Questão

Acerto: 1,0 / 1,0

Em relação à segurança da informação e aos controles de acesso físico e lógico, considere:

I. Se um usuário não mais faz parte a lista de um grupo de acesso aos recursos de processamento da informação, é certo que o grupo seja extinto com a criação de um novo, contendo os usuários remanescentes.

II. Direitos de acesso (físicos e lógicos) que não foram aprovados para um novo trabalho devem ser retirados ou adaptados, incluindo chaves e qualquer tipo de identificação que associe a pessoa ao novo projeto.

III. O acesso às áreas em que são processadas ou armazenadas informações sensíveis deve ser controlado e restrito às pessoas autorizadas, preferencialmente por controles de autenticação, por exemplo, cartão de controle de acesso mais PIN (personal identification number).

Está correto o que se afirma em

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


Explicação:

Do ponto de vista de gerenciamento, não faz sentido excluir todos os usuários (o grupo) apenas para revogar o acesso de um único usuário que não tenha mais permissão.

**9ª** QuestãoAcerto: **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 descriptografia 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:

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

Respondido em 29/04/2023 20:52:27

Explicação:

A resposta correta é: Ransomware

**10ª** QuestãoAcerto: **1,0 / 1,0**

Sobre os conceitos de segurança da informação, analise as afirmativas a seguir:

I. Uma ameaça tem o poder de comprometer ativos vulneráveis.

II. Risco é a combinação das consequências de um incidente de segurança com a sua probabilidade de ocorrência.

III. Vulnerabilidades técnicas são mais críticas do que vulnerabilidades criadas por comportamento humano.

Está correto somente o que se afirma em:

- ☐ III
- ☐ II
- ☐ I e III



I



I e II

Respondido em 29/04/2023 20:52:56

Explicação:

A resposta correta é: I e II