

Disc.: **INTRODUÇÃO À SEGURANÇA DA INFORMAÇÃO**Acertos: **10,0** de 10,0

07/03/2023



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
- ☐ Indica uma simples observação a ser feita
- ☐ Não se aplica a esta norma
- ☒ Sim

Respondido em 07/03/2023 12:24:17

**Explicação:**

A resposta correta é: Sim.



Questão

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

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

- ☐ Fornece segurança a todas as partes interessadas
- ☒ Isola recursos com outros sistemas de gerenciamento
- ☐ Mecanismo para minimizar o fracasso do sistema
- ☐ Participação da gerência na Segurança da Informação
- ☐ Oportunidade de identificar e eliminar fraquezas

Respondido em 07/03/2023 12:24:47

Explicação:

A resposta correta é: Isola recursos com outros sistemas de gerenciamento.



3ª Questão

Acerto: 1,0 / 1,0

"Todo acesso a cada objeto deve ser verificado quanto à autoridade. Esse princípio, quando aplicado sistematicamente, é o principal fundamento do sistema de proteção". Selecione a opção que se refere a esse mecanismo de proteção:

- ☐ Compartilhamento mínimo.
- ☐ Privilégio mínimo.
- ☐ Padrões à prova de falhas.
- ☒ ✓ Mediação completa.
- ☐ Separação de privilégios.

Respondido em 07/03/2023 12:25:05

Explicação:

A resposta correta é: Mediação completa.



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 a cópia dos dados criados e modificados desde o último backup.
- ☐ É exatamente igual ao backup diferencial.
- ☐ Também é chamado de backup incremental cumulativo.

Respondido em 07/03/2023 12:25:47

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:

- ☐ Monitoramento e controle de riscos.
- ☒ ✓ Processo de avaliação de riscos.

- ☐ Aceitação do risco (residual).
- ☐ Terminação de riscos.
- ☐ Definição do contexto.

Respondido em 07/03/2023 12:31:24

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:

- ☒  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.
- ☐ Normalmente não podem ser controlados.
- ☐ Não pode ser analisado em termos probabilísticos, uma vez que sempre está presente.
- ☐ Evento súbito e imprevisto que provoca grandes perdas ou danos a uma organização.

Respondido em 07/03/2023 12:32:16

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

Na questão que avalia conhecimento de informática, a menos que seja explicitamente informado o contrário, considere que: todos os programas mencionados estejam em configuração-padrão, em português; o mouse esteja configurado para pessoas destros; expressões como clicar, clique simples e clique duplo refiram-se a cliques com o botão esquerdo do mouse; e teclar corresponda à operação de pressionar uma tecla e, rapidamente, liberá-la, acionando-a apenas uma vez. Considere também que não haja restrições de proteção, de funcionamento e de uso em relação aos programas, arquivos, diretórios, recursos e equipamentos mencionados.

Assinale a alternativa que apresenta procedimento de segurança da informação que pode ser adotado pelas organizações.

- ☐ direcionar os funcionários apenas para o exercício de suas funções diárias; pois treinamentos em segurança da informação ou outros eventos relacionados devem ser evitados
- ☒  realizar, periodicamente, análises de riscos, com o objetivo de contemplar as mudanças nos requisitos de segurança da informação
- ☐ conceder aos funcionários o acesso completo aos sistemas e à rede (intranet) da organização
- ☐ não envolver a direção com a segurança da informação, tendo em vista que ela já possui diversas outras atribuições
- ☐ descartar o inventário dos ativos, caso a organização possua

Respondido em 07/03/2023 12:33:26

Explicação:

A resposta correta é: realizar, periodicamente, análises de riscos, com o objetivo de contemplar as mudanças nos requisitos de segurança da informação.



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

Respondido em 07/03/2023 12:28:01

#### 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 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:

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

Respondido em 07/03/2023 12:26:57

#### Explicação:

A resposta correta é: Ransomware




### 10ª Questão

Acerto: 1,0 / 1,0

Considere que uma equipe esteja trabalhando num software web com severas restrições de segurança. Além dos desenvolvedores e analistas, essa equipe conta com profissionais

especialistas em segurança que têm, entre outras atribuições, a responsabilidade de realizar a revisão dos códigos a fim de evitar vulnerabilidades. Se durante a etapa de desenvolvimento um revisor da equipe de segurança detectar uma vulnerabilidade, é sua responsabilidade:

- ☐ Isolar o problema e solicitar que a equipe de desenvolvimento corrija a vulnerabilidade imediatamente.
- ☐ Corrigir o problema e relatar a vulnerabilidade à equipe de segurança.
- ☐ Separar a vulnerabilidade, tratando o código com erro como mais um problema que requer correção.
- ☐ Corrigir a vulnerabilidade, contatando os desenvolvedores que programaram o trecho de código vulnerável.
- ☒  Separar a vulnerabilidade e alertar a equipe de segurança para que o problema seja resolvido.

Respondido em 07/03/2023 12:36:02

**Explicação:**

A resposta correta é: Separar a vulnerabilidade e alertar a equipe de segurança para que o problema seja resolvido.