



Meus Simulados

Teste seu conhecimento acumulado

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

Aluno(a):

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

17/09/2023



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

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
- ☐ Mecanismo para eliminar o sucesso do sistema
- ☐ Não participação da gerência na Segurança da Informação
- ☐ Fornece insegurança a todas as partes interessadas
- ☐ Isola recursos com outros sistemas de gerenciamento

Respondido em 17/09/2023 20:55:26

Explicação:

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



3ª Questão

Acerto: 1,0 / 1,0

(TRE-TO/2006 - Adaptada) Entre as medidas técnicas utilizadas no processo de proteção de dados, estão o uso de criptografia para garantir a confidencialidade das informações, o controle de acesso para limitar quem pode acessar os dados e em que condições, e a realização de backups regulares para garantir a disponibilidade dos dados em caso de falhas ou desastres. Nesse sentido, assinale a opção correta a respeito de criptografia.

- ☐ Um dos pontos fortes dos sistemas de criptografia simétrica é a facilidade da distribuição da chave aos seus usuários.
- ☐ Na criptografia assimétrica, são utilizadas duas chaves, uma pública e uma privada, sendo uma especificamente utilizada para cifrar e a outra, para decifrar.
- ☐ Na criptografia assimétrica, é utilizada uma única chave para cifração e decifração.

- ☒ A criptografia assimétrica provê sigilo, integridade, autenticidade e não-repúdio dos dados cifrados.
- ☐ A criptografia simétrica provê sigilo, integridade e autenticidade dos dados cifrados.

Respondido em 17/09/2023 20:52:08

Explicação:

A criptografia simétrica **não provê autenticidade**. A criptografia assimétrica utiliza **duas chaves, uma pública e uma privada**. Como a criptografia simétrica utiliza apenas uma chave para criptografar/descriptografar, a mensagem será comprometida caso o invasor consiga capturar tal chave. Para garantir a segurança de divulgação da chave secreta, utiliza-se a criptografia assimétrica em conjunto. Dessa forma, é notória a **dificuldade** de distribuição da chave simétrica.



4ª Questão

Acerto: 1,0 / 1,0

Segurança da informação é um conjunto de práticas e medidas destinadas a proteger a confidencialidade, integridade e disponibilidade de informações. Qual das opções abaixo é considerada uma boa prática de segurança?

- ☒ Nunca compartilhar senhas.
- ☐ Desabilitar o firewall do sistema operacional.
- ☐ Sempre utilizar antivírus desatualizados.
- ☐ Sempre abrir links ou fazer download de arquivos enviados por e-mails não confiáveis ou de remetentes desconhecidos.
- ☐ Nunca baixar programas de fornecedores oficiais.

Respondido em 17/09/2023 20:45:34

Explicação:

O compartilhamento de senhas é uma prática arriscada e pode comprometer a segurança da informação, já que uma vez que a senha é compartilhada, a pessoa que a recebe pode ter acesso a informações confidenciais. Portanto, manter senhas seguras e não compartilhá-las é uma boa prática para proteger a confidencialidade das informações.



5ª Questão

Acerto: 1,0 / 1,0

O sistema de monitoramento de *nobreak* detectou uma variação na tensão elétrica na entrada dos aparelhos, mas essa variação não foi o suficiente para causar danos aos equipamentos de computação a eles conectados.

Conforme os termos relacionados à segurança da informação, o que ocorreu pode ser classificado como:

- ☐ Dano
- ☐ Eletricidade
- ☐ Variação
- ☒ ✓ Evento
- ☐ Tensionamento

Respondido em 17/09/2023 20:42:06

Explicação:

A resposta correta é: Evento



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:

- ☐ 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.
- ☐ Não pode ser analisado em termos probabilísticos, uma vez que sempre está presente.
- ☐ Normalmente não podem ser controlados.
- ☒ ✓ Possível evento que pode causar perdas ou danos, ou dificultar o atingimento de objetivos.

Respondido em 17/09/2023 20:39:11

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



Suponha que uma entidade R (remetente) deseja enviar uma mensagem m para outra entidade D (destinatário) utilizando a internet. Para se comunicarem, R e D utilizam criptografia de chave pública. R^+ e R^- são as chaves pública e privada de R, respectivamente, e D^+ e D^- são as chaves pública e privada de D, respectivamente.

A partir dessa situação, avalie o que se afirma.

- I - Se R utilizar D^+ para criptografar m , então D poderá utilizar D^- para decriptar m .
- II - Se R utilizar R^+ para criptografar m , então D poderá utilizar D^- para decriptar m .
- III - Se R utilizar R^- para criptografar m , então D poderá utilizar R^+ para decriptar m .
- IV - Se R utilizar D^- para criptografar m , então D poderá utilizar R^+ para decriptar m .

Está correto apenas o que se afirma em:

- ☒ I e III.
- ☐ I e IV.
- ☐ III e IV.
- ☐ II e IV.
- ☐ II e III.

Respondido em 17/09/2023 20:36:32

Explicação:

A resposta correta é: I e III.



8ª Questão

Acerto: 1,0 / 1,0

O crescimento das redes abertas fez com que surgissem vários problemas de segurança, que vão desde o roubo de senhas e interrupção de serviços até problemas de personificação, em que uma pessoa faz-se passar por outra para obter acesso privilegiado. Com isso, surgiu a necessidade de verificação da identidade tanto dos usuários quanto dos sistemas e processos. Dentro desse contexto, esse ato de verificação é chamado:

- ☐ confiabilidade.
- ☐ acessibilidade.
- ☒ autenticação.
- ☐ configuração.
- ☐ cadastro.

Respondido em 17/09/2023 20:33:51

Explicação:

A resposta correta é: Autenticação.



9ª Questão

Acerto: 1,0 / 1,0

Ativos são recursos econômicos controlados por uma organização que possuem valor e podem gerar benefícios futuros. Eles são divididos em duas categorias principais: ativos tangíveis e ativos intangíveis. De maneira geral, qual exemplo pode ser considerado um ativo lógico tangível?

- ☐ Humanos.
- ☐ Imagem da organização.
- ☐ Marca.
- ☐ Colaboradores.
- ☒ Informação.

Respondido em 17/09/2023 20:31:08

Explicação:

Ativos tangíveis lógicos são aqueles que envolvem a informação e sua representação em algoritmos, por exemplo, uma fórmula química, os detalhes sobre a safra da laranja no mercado norte-americano, o algoritmo principal de busca do Google, os detalhes técnicos das baterias dos carros do Elon Musk.



10ª Questão

Acerto: 1,0 / 1,0

(FEPESE/2017) Identifique abaixo as afirmativas verdadeiras (V) e as falsas (F) sobre Negação de Serviço (DoS e DDoS):

- () Negação de serviço, ou DoS (Denial of Service) é uma técnica pela qual um atacante utiliza um computador para tirar de operação um serviço, um computador ou uma rede conectada à Internet.
- () Quando utilizada de forma coordenada e distribuída, ou seja, quando um conjunto de computadores é utilizado no ataque, recebe o nome de negação de serviço distribuído, ou DDoS (Distributed Denial of Service).
- () O principal objetivo dos ataques de Negação de Serviço (DoS e DDoS) é invadir e coletar informações do alvo.
- () Uma pessoa pode voluntariamente usar ferramentas e fazer com que seu computador seja utilizado em ataques. A grande maioria dos computadores, porém, participa dos ataques sem o conhecimento de seu dono, por estar infectado e fazendo parte de botnets.

Assinale a alternativa que indica a sequência correta, de cima para baixo.

- ☐ V F F F
- ☐ F F V F
- ☐ F V V F
- ☒ V V F V
- ☐ V F F V

Respondido em 17/09/2023 20:29:06

Explicação:

Podemos assumir que o principal objetivo dos ataques de Negação de Serviço (DoS e DDoS) é paralisar as operações do alvo.