

Meus Simulados

Teste seu conhecimento acumulado

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

Aluno(a): **KATIA REJANE RABELO SILVA**

202305362843

Acertos: **9,0** de 10,0

30/06/2023

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"?

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

Respondido em 30/06/2023 20:03:27

Explicação:


A resposta correta é: Sim.

2ª 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:

- ☐ Mecanismo para minimizar o fracasso do sistema
- ☐ Oportunidade de identificar e eliminar fraquezas

- ☐ Participação da gerência na Segurança da Informação
- ☐ Fornece segurança a todas as partes interessadas
- ☒  Isola recursos com outros sistemas de gerenciamento


Respondido em 30/06/2023 20:00:03

Explicação:

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

**3ª 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 baixar programas de fornecedores oficiais.
- ☐ Desabilitar o firewall do sistema operacional.
- ☐ Sempre abrir links ou fazer download de arquivos enviados por e-mails não confiáveis ou de remetentes desconhecidos.
- ☐ Sempre utilizar antivírus desatualizados.
- ☒  Nunca compartilhar senhas.


Respondido em 30/06/2023 19:58:49

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.

**4ª Questão**Acerto: **1,0 / 1,0**

Complete a frase corretamente: "as funções de hash, por exemplo, são adequadas para garantir a integridade dos dados, porque ..."

- ☐ Geralmente podem ser calculadas muito mais rápido que os valores de criptografia de chave pública.
- ☐ Fazem a troca de chaves na chave simétrica.
- ☒  Qualquer alteração feita no conteúdo de uma mensagem fará com que o receptor calcule um valor de hash diferente daquele colocado na transmissão pelo remetente.
- ☐ Usam chave única para criptografar e *descriptografar* a mensagem.
- ☐ Utilizam algoritmos de criptografia de chave pública.

Respondido em 30/06/2023 19:59:24

Explicação:

A resposta correta é: Qualquer alteração feita no conteúdo de uma mensagem fará com que o receptor calcule um valor de hash diferente daquele colocado na transmissão pelo remetente.



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:

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

Respondido em 30/06/2023 20:06:46

Explicação:

A resposta correta é: Evento



6ª Questão

Acerto: 1,0 / 1,0

O Gerenciamento da Continuidade dos Serviços de Tecnologia Informação (GCSTI) é um processo essencial para que o negócio possa voltar a operar com o suporte dos serviços de TI o mais rápido possível após a ocorrência de um cenário de desastre. Selecione a opção que apresenta um possível desafio de desenvolvimento de um GCSTI:

- ☐ Encontrar apoio profissional no mercado para dar suporte ao desenvolvimento da GCSTI.
- ☒ Criar um GCSTI quando não existirem planos de gerenciamento de continuidade de negócios.
- ☐ Obter exemplos no mercado de casos de sucesso do desenvolvimento, da implantação e da aplicação da GCSTI.
- ☐ Justificar a importância do desenvolvimento da GCSTI.
- ☐ Obter referências para adoção das melhores práticas apropriadas em TI.

Respondido em 30/06/2023 20:13:40

Explicação:

A resposta correta é: Criar um GCSTI quando não existirem planos de gerenciamento de continuidade de negócios.



7ª 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:

- ☒ autenticação.

- ☐ configuração.
- ☐ cadastro.
- ☐ confiabilidade.
- ☐ acessibilidade.

Respondido em 30/06/2023 20:01:40

Explicação:

A resposta correta é: Autenticação.

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

Respondido em 30/06/2023 20:02:01

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.

**9ª Questão**

Acerto: 0,0 / 1,0

(UFES/2014) O termo "Engenharia Social" é comumente utilizado para se referir a técnicas utilizadas por pessoas mal-intencionadas que abusam de relações sociais para conseguir informações sigilosas ou acesso a sistemas. Dos cenários abaixo, NÃO caracteriza um caso de Engenharia Social o que está descrito em

- ☒ Você recebe um e-mail alertando sobre um novo vírus muito perigoso e orientando-o a procurar por determinado arquivo em seu sistema e, caso ele exista, excluí-lo imediatamente e repassar a mensagem a todos os seus conhecidos.
- ☒ Após fornecer seu endereço de e-mail em um site para se cadastrar, você recebe uma mensagem de e-mail desse site pedindo que você clique em um link para confirmar o seu cadastro.
- ☐ Em um ambiente de trabalho, uma pessoa liga, identifica-se como administrador dos sistemas da empresa e solicita que você siga uma série de passos, incluindo acesso a sites na internet e instalação de softwares, para melhorar o desempenho da sua máquina.

- ☐ Você recebe um e-mail indicando que acaba de ser sorteado com um prêmio e instruindo-o a acessar um determinado site e preencher o cadastro para coletar o seu prêmio.
- ☐ Uma pessoa liga para você, identifica-se como sendo de uma empresa prestadora de serviços (ex.: de telefonia), explica que há um problema no seu cadastro e pede que você informe vários dados pessoais, como nome completo, endereço, etc.

Respondido em 30/06/2023 20:08:55

Explicação:

A Engenharia Social é um método de ataque que utiliza a persuasão para obter dados sigilosos do usuário, seja por meios eletrônicos ou não. Normalmente, o atacante se passa por alguém confiável, como uma instituição conhecida, como um banco ou empresa. A opção correta mencionada refere-se apenas a um procedimento de confirmação, comum quando você se cadastra em um site e recebe uma mensagem para confirmar a validade do seu endereço de e-mail.



10ª Questão

Acerto: 1,0 / 1,0

(FCC/2012 - Adaptada) Códigos maliciosos (malwares) são programas que objetivam executar ações danosas e atividades maliciosas em um computador. Neste contexto encontram-se bots e botnets, sobre os quais é correto afirmar:

- ☐ A comunicação entre o invasor e o computador infectado pelo bot pode ocorrer exclusivamente via redes do tipo P2P. Ao se comunicar, o invasor pode enviar instruções para que ações maliciosas sejam executadas, como desferir ataques, furtar dados do computador infectado e enviar spam.
- ☐ Um computador infectado por um bot costuma ser chamado de attack base, pois serve de base para o atacante estabelecer suas ações maliciosas. Também pode ser chamado de spam host, pois o bot instalado tem o objetivo de enviar infinitamente spams para a caixa de e-mail de quem é vítima do ataque.
- ☒ Algumas das ações maliciosas que costumam ser executadas por intermédio de botnets são: ataques de negação de serviço, propagação de códigos maliciosos, coleta de informações de um grande número de computadores, envio de spam e camuflagem da identidade do atacante.
- ☐ Botnet é um software malicioso de monitoramento de rede que tem a função de furtar dados que transitam pela rede e, normalmente, tornar a rede indisponível disparando uma grande carga de dados direcionados ao servidor da rede.
- ☐ Bot é um programa que dispõe de mecanismos de comunicação com o invasor e possui um processo de infecção e propagação igual ao do vírus, ou seja, não é capaz de se propagar automaticamente.

Respondido em 30/06/2023 20:16:51

Explicação:

Botnets, também conhecido como rede zumbi, é um conjunto de equipamentos que sofreu um ataque, resultando no controle do equipamento pelo hacker. Através de botnets é possível fazer ataques de negação de serviço, envios de e-mails em massa e vários outros.