

Disc.: **INTRODUÇÃO À SEGURANÇA DA INFORMAÇÃO**Acertos: **9,0 de 10,0****14/04/2023****1ª** QuestãoAcerto: **1,0 / 1,0**

Dentre as opções a seguir, qual Norma Técnica apresenta um código de prática para a gestão da segurança da informação?

- ☐ ABNT NBR ISO 9001:2008
- ☐ ABNT NBR ISO/IEC 27001:2013
- ☒  ABNT NBR ISO/IEC 27002:2013
- ☐ ABNT NBR ISO/IEC 20000-1:2011
- ☐ ABNT NBR ISO 14001:2004


Respondido em 14/04/2023 21:21:24

**Explicação:**

A resposta correta é: ABNT NBR ISO/IEC 27002:2013

**2ª** QuestãoAcerto: **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:

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

Respondido em 14/04/2023 21:16:50

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:

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

Respondido em 14/04/2023 21:20:18

Explicação:

A resposta correta é: Mediação completa.



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 ..."

- ☐ Utilizam algoritmos de criptografia de chave pública.
- ☐ Usam chave única para criptografar e *descriptografar* a mensagem.
- ☐ 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.

Respondido em 14/04/2023 21:29:46

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

Um ataque de negação de serviço tenta afetar a disponibilidade de um ativo, por exemplo, inundando um servidor de aplicação em rede com mais dados do que é capaz de processar por unidade de tempo.

Se existe uma ferramenta, dentro do domínio do servidor, que reage a um ataque de negação de serviço, ela é classificada como uma medida de controle:

- ☐ Detectora
- ☐ Recuperadora
- ☐ Limitadora
- ☐ Preventiva
- ☒ Reativa

Respondido em 14/04/2023 21:19:04

Explicação:

A resposta correta é: Reativa



6ª Questão

Acerto: 0,0 / 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:

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

Respondido em 14/04/2023 21:28:27

Explicação:

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



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 referam-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.

- ☐ conceder aos funcionários o acesso completo aos sistemas e à rede (intranet) da organização
- ☐ descartar o inventário dos ativos, caso a organização possua
- ☐ 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
- ☐ não envolver a direção com a segurança da informação, tendo em vista que ela já possui diversas outras atribuições

Respondido em 14/04/2023 21:25:25

#### 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

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:

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

Respondido em 14/04/2023 21:27:45

#### 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

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:

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

Respondido em 14/04/2023 21:26:09

Explicação:

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



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
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	Sem contrato de manutenção periódica	Defeito no firmware	Perda da confidencialidade nos acessos a internet

ATIVO	VULNERABILIDADE	INCIDENTE/AMEAÇA	IMPACTO
Firewall da rede	Falta de atualizações do IOS	Perda de desempenho	Não suporta atualizações de hardware

ATIVO	VULNERABILIDADE	INCIDENTE/AMEAÇA	IMPACTO
Servidor Web	Ataque Hacker DDoS	Falta de atualizações do sistema operacional	Indisponibilidade

ATIVO	VULNERABILIDADE	INCIDENTE/AMEAÇA	IMPACTO
Servidor Web	Servidor de aplicação acessível pela internet	Ataque Hacker DDoS	Integridade

Respondido em 14/04/2023 21:22:33

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