



Meus Simulados

Teste seu conhecimento acumulado

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

Aluno(a): **PAULO RICARDO TORRES MARQUES MARTINS MOURA E SILVA**

202303714629

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

16/05/2023

1ª Questão

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

Respondido em 16/05/2023 19:10:00

Explicação:


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

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.
- ☐ Ignorar informalmente a presença de quaisquer arquivos não aprovados ou atualização não autorizada.
- ☒  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.
- ☐ Estabelecer uma política informal proibindo o uso de *softwares* autorizados.

Respondido em 16/05/2023 19:13:46

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**

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 16/05/2023 19:10:56

Explicação:

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

**4ª 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:

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

Respondido em 16/05/2023 19:14:07

Explicação:

A resposta correta é: Mediação completa.

**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
- ☐ Dano
- ☒ Evento
- ☐ Eletricidade
- ☐ Tensionamento

Respondido em 16/05/2023 19:14:25

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:

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

Respondido em 16/05/2023 19:16:30

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

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

Respondido em 16/05/2023 19:12:26

Explicação:

A resposta correta: Firewall.



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:

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

Respondido em 16/05/2023 19:12:47

Explicação:

A resposta correta é: Autenticação.



9ª 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.
- ☐ Isolar o problema e solicitar que a equipe de desenvolvimento corrija a vulnerabilidade imediatamente.
- ☐ Corrigir a vulnerabilidade, contatando os desenvolvedores que programaram o trecho de código vulnerável.
- ☐ 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.

Respondido em 16/05/2023 19:18:55

Explicação:

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




10ª 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

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:

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

Respondido em 16/05/2023 19:11:27

Explicação:

A resposta correta é: Ransomware