1

Marcar para revisão

O sistema de backup de missão crítica é também chamado de ambiente de:

A *Ransomware*.

B *Disaster Recovery.*

C *Daily Backup.*

D *Personal Unblocking Key.*

E *Personal Identification Number.*

2

Marcar para revisão

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?

A Nunca compartilhar senhas.

B Sempre utilizar antivírus desatualizados.

C Desabilitar o firewall do sistema operacional.

D Nunca baixar programas de fornecedores oficiais.

E Sempre abrir links ou fazer download de arquivos enviados por e-mails não confiáveis ou de remetentes desconhecidos.

3

Marcar para revisão

Quanto mais complexa for uma senha, mais difícil será para o invasor quebrá-la com o uso de programas, exclusivamente. Levando em consideração essa afirmação, selecione a opção que possui a senha com maior grau de dificuldade de ser descoberta por um invasor:

A aX1!@7s5

B 69910814sa

C SeNhA123

D X1234Y1

E MaRiA96

4

Marcar para revisão

Em relação ao backup incremental, selecione a opção **correta**:

A Faz cópias de todos os dados, inclusive dos logs de transações associados, para outro conjunto de mídia, que pode ser fita, disco, um DVD ou CD.

B É a cópia dos dados criados e modificados desde o último backup.

C É a cópia de todos os dados que foram modificados desde o último backup de qualquer tipo.

D É exatamente igual ao backup diferencial.

E Também é chamado de backup incremental cumulativo.

5

Marcar para revisão

(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.

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

B Na criptografia assimétrica, são utilizadas duas chaves, uma pública e uma privada, sendo uma especificamente utilizada para cifrar e a outra, para decifrar.

C A criptografia simétrica provê sigilo, integridade e autenticidade dos dados cifrados.

D Na criptografia assimétrica, é utilizada uma única chave para cifração e decifração.

E Um dos pontos fortes dos sistemas de criptografia simétrica é a facilidade da distribuição da chave aos seus usuários.

6

Marcar para revisão

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

A Geralmente podem ser calculadas muito mais rápido que os valores de criptografia de chave pública.

B Fazem a troca de chaves na chave simétrica.

C Usam chave única para criptografar e *descriptografar* a mensagem.

D 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.

E Utilizam algoritmos de criptografia de chave pública.

7

Marcar para revisão

O processo de proteção de dados é um conjunto de ações que têm como objetivo garantir a segurança e a privacidade das informações armazenadas por uma organização ou indivíduo. Esse processo envolve a implementação de medidas técnicas, organizacionais e legais que visam prevenir o acesso, o uso, a alteração, a destruição ou a divulgação não autorizada de dados sensíveis. Nesse sentido, qual das opções abaixo é uma razão válida para justificar a importância de se realizar backups regularmente como medida de segurança da informação?

A Os backups são úteis apenas para fins de auditoria e conformidade regulatória, e não têm relação direta com a segurança da informação.

B Os backups são importantes apenas para grandes empresas que precisam proteger grandes quantidades de dados confidenciais.

C Caso as informações sejam perdidas ou corrompidas devido a falhas de hardware, malware ou erros humanos, um backup recente pode ser restaurado, garantindo a continuidade das operações.

D Realizar backups permite que você se livre de dados antigos e desnecessários, liberando espaço de armazenamento valioso.

E Backup é um desperdício de tempo e recursos, uma vez que as informações raramente são perdidas ou corrompidas.

8

Marcar para revisão

(AMEOSC/2022 - Adaptada) Protege o computador contra outros programas potencialmente danosos. Ele detecta, impede e atua na remoção de programas maliciosos, como vírus e worms.
Marque a alternativa CORRETA que corresponde ao contexto acima.

A Proxy.

B Antivírus.

C Firewall.

D Painel de Controle.

E Roteador.

9

Marcar para revisão

(CESGRANRIO/2012) O uso de criptografia simétrica no compartilhamento de informações secretas requer o compartilhamento de chave simétrica. Uma forma segura para um emissor enviar uma chave simétrica por meios de comunicação inseguros para um receptor é criptografar essa chave com a chave:

A privada do emissor.

B privada do receptor.

C pública do emissor.

D pública do receptor.

E pública do emissor e a chave privada do receptor.

10

Marcar para revisão

"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:

A Mediação completa.

B Padrões à prova de falhas.

C Privilégio mínimo.

D Compartilhamento mínimo.

E Separação de privilégios.

Questão **1** de 10

1 2 3 4 5
6 7 8 9 10

○ Em branco **(10)**