1

Marcar para revisão

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

A *Personal Identification Number.*

B *Personal Unblocking Key.*

C *Ransomware.*

D *Disaster Recovery.*

E *Daily Backup.*

Resposta correta

Parabéns, você selecionou a alternativa correta. Confira o gabarito comentado!

Gabarito Comentado

O termo "Disaster Recovery" é o correto. Ele se refere a um conjunto de políticas e procedimentos que permitem a recuperação ou continuação de sistemas de tecnologia e infraestrutura vitais após um desastre natural ou humano. No contexto da pergunta, um sistema de backup de missão crítica é um exemplo de um ambiente de "Disaster Recovery", pois é projetado para garantir a continuidade dos negócios e minimizar o tempo de inatividade em caso de falhas graves ou desastres.

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

D Nunca baixar programas de fornecedores oficiais.

E Desabilitar o firewall do sistema operacional.

Resposta correta

Parabéns, você selecionou a alternativa correta. Confira o gabarito comentado!

Gabarito Comentado

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.

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 X1234Y1

B MaRiA96

C aX1!@7s5

D 69910814sa

E SeNhA123

Resposta correta

Parabéns, você selecionou a alternativa correta. Confira o gabarito comentado!

Gabarito Comentado

A senha "aX1!@7s5" é a mais complexa entre as opções apresentadas. Ela combina letras maiúsculas e minúsculas, números e caracteres especiais, tornando-a mais difícil de ser quebrada por programas de invasão. A complexidade de uma senha é determinada pela variedade de caracteres utilizados e pelo seu comprimento.

4

Marcar para revisão

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

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

B 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.

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

D Também é chamado de backup incremental cumulativo.

E É exatamente igual ao backup diferencial.

Resposta incorreta
Opa! A alternativa correta é a letra A. Confira o gabarito comentado!

Gabarito Comentado
O backup incremental é um tipo de backup que copia todos os dados que foram modificados desde o último backup de qualquer tipo. Isso significa que ele não copia todos os dados, mas apenas aqueles que foram alterados. Portanto, a alternativa A está correta, pois afirma que o backup incremental é a cópia de todos os dados que foram modificados desde o último backup de qualquer tipo.

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

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

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

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

Resposta correta
Parabéns, você selecionou a alternativa correta. Confira o gabarito comentado!

Gabarito Comentado
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.

6

Marcar para revisão

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

A 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.

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

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

D Fazem a troca de chaves na chave simétrica.

E Utilizam algoritmos de criptografia de chave pública.

Resposta correta
Parabéns, você selecionou a alternativa correta. Confira o gabarito comentado!

Gabarito Comentado
A alternativa correta é a letra A. As funções de hash são utilizadas para garantir a integridade dos dados. Isso ocorre porque qualquer alteração feita no conteúdo de uma mensagem resultará em um valor de hash diferente. Portanto, se o receptor calcular um valor de hash diferente daquele que foi colocado na transmissão pelo remetente, isso indica que a mensagem foi alterada de alguma forma, comprometendo a sua integridade.

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

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

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

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

Resposta correta
Parabéns, você selecionou a alternativa correta. Confira o gabarito comentado!

Gabarito Comentado
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. Realizar backups regularmente é uma medida fundamental de segurança da informação, pois permite que, em caso de perda, corrupção ou inacessibilidade de dados, uma cópia recente e íntegra possa ser restaurada, minimizando os prejuízos para a organização. Falhas de hardware, ataques de malware e erros humanos são comuns e podem resultar na perda de dados importantes. Portanto, é crucial que backups sejam realizados regularmente e que sejam armazenados em locais seguros e protegidos contra ameaças físicas e lógicas. Além disso,

backups também podem ser úteis em situações de desastres naturais, como incêndios, inundações e terremotos, que podem destruir completamente os dados armazenados em um único local.

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.

Resposta correta
Parabéns, você selecionou a alternativa correta. Confira o gabarito comentado!

Gabarito Comentado
O antivírus é um programa de segurança projetado para detectar, impedir e remover softwares maliciosos, como vírus e worms, que podem prejudicar o computador e seus arquivos. Ele trabalha constantemente em segundo plano para monitorar atividades suspeitas e alertar o usuário sobre possíveis ameaças. Por isso, o antivírus é uma medida importante de proteção contra ameaças virtuais e deve ser mantido sempre atualizado.

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.

Resposta correta
Parabéns, você selecionou a alternativa correta. Confira o gabarito comentado!

Gabarito Comentado
Para enviar uma chave simétrica por meios de comunicação inseguros, é necessário criptografá-la. Nesse caso, a criptografia deve ser realizada utilizando a chave pública 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 Separação de privilégios.

B Mediação completa.

C Compartilhamento mínimo.

D Privilégio mínimo.

E Padrões à prova de falhas.

Resposta correta
Parabéns, você selecionou a alternativa correta. Confira o gabarito comentado!

Gabarito Comentado
O princípio descrito no enunciado refere-se à "Mediação completa". Este princípio de segurança da informação estabelece que todo acesso a cada objeto deve ser verificado quanto à autoridade, ou seja, deve haver uma verificação completa de permissões antes de conceder acesso a qualquer recurso ou informação. Isso garante que apenas usuários autorizados possam acessar e manipular os dados, contribuindo para a proteção e integridade das informações.

Questão **1** de 10

1 2 3 4 5
6 7 8 9 10

Corretas **(9)**
Incorretas **(1)**
Em branco **(0)**