

A+



Alterar modo de visualização

Peso da Avaliação 1,50

Prova 47045235

Qtd. de Questões 10

Acertos/Erros 5/3

Canceladas 2

Nota 7,00

1 A intensificação do uso da computação e das redes de computadores trouxeram para as organizações a capacidade de produzir e consultar informações com uma velocidade e alcance nunca antes imaginados. Ao mesmo tempo, essas tecnologias apresentam vulnerabilidades e fragilidades que exigem medidas de prevenção, objetivando evitar o acesso não autorizado a estas informações. Assinale a alternativa CORRETA que denomina o objetivo de segurança referente a garantir que a informação seja acessada somente por usuários autorizados:

- A Legalidade.
- B Integridade.
- C Disponibilidade.
- D** Confidencialidade.

2 Segurança da informação é a proteção de um conjunto de dados, no sentido de preservar o valor que possuem para um indivíduo ou organização. O conceito de Segurança da Informática ou Segurança de Computadores está intimamente relacionado ao de Segurança da Informação, incluindo não apenas a segurança dos dados/informação, mas também a dos sistemas em si. Quais são os principais atributos que orientam a análise, o planejamento e a implementação da segurança para um grupo de informações que se deseja proteger?

- A Consistência, integridade e disponibilidade.
- B** Confidencialidade, integridade e disponibilidade.
- C Confidencialidade, integridade e durabilidade.
- D Confidencialidade, persistência e disponibilidade.

3 A quantidade de informação que uma empresa gerencia e utiliza atualmente é enorme e vem aumentando constantemente. Logo, faz-se necessário que a segurança dessas informações seja realizada desde o momento de sua coleta até o seu descarte, já que os riscos estão presentes em todo o seu ciclo de vida. Acerca das etapas do ciclo de vida da informação, assinale a alternativa CORRETA que apresenta a etapa em que a informação passa por um conjunto de processos, a fim de torná-la mais exequível aos usuários:

- A** Identificação das necessidades e requisitos.

- B Uso.
- C Obtenção.
- D Tratamento.**

4 A informação utilizada pela organização é um bem valioso e necessita ser protegido e gerenciado. Isso é feito para garantir a disponibilidade, a integridade, a confidencialidade, a legalidade e a auditabilidade da informação, independentemente do meio de armazenamento, de processamento ou de transmissão utilizado. Toda informação também deve ser protegida para que não seja alterada, acessada e destruída indevidamente. Com relação aos possíveis ataques à segurança, analise as afirmativas a seguir:

- I- O roubo de dados armazenados em arquivos magnéticos é um problema para a segurança lógica.
- II- A sabotagem de equipamentos e de arquivos de dados é uma forma de ataque físico.
- III- A limitação de acessos aos arquivos, através da disponibilidade limitada de acesso, é uma forma de segurança lógica.
- IV- A estrutura de controle da segurança da informação pode ser centralizada ou descentralizada.

Assinale a alternativa CORRETA

FONTE: FONTES, Eduardo. Segurança da informação: o usuário faz a diferença. São Paulo: Saraiva, 2006.

- A** As afirmativas II, III e IV estão corretas.
- B Somente a afirmativas IV está correta.
- C As afirmativas I, II e IV estão corretas.
- D** As afirmativas I, II e III estão corretas.

5 A gestão do risco representa uma das etapas mais importantes no estabelecimento de uma política de segurança de tecnologia da informação, possibilitando o estabelecimento de prioridades de segurança com base em fatores como probabilidade de ocorrência e impacto na organização. Com relação à gestão de riscos, classifique V para as sentenças verdadeiras e F para as falsas:

- () Medidas preventivas são controles que reduzem a probabilidade de uma ameaça se concretizar ou minimizam o grau de vulnerabilidade de determinado ativo.
- () Uma vez estabelecida uma política de gestão de riscos, esta somente será revista em caso de mudança de algum recurso computacional de hardware ou software.
- () A aplicação ou não de uma medida para diminuir a probabilidade de ocorrência de um evento ou para tratá-lo após sua ocorrência deve considerar como um dos principais critérios a relação custo/benefício. Por via de regra, não se gasta um valor superior ao do ativo com medidas de segurança para o mesmo.
- () A elaboração de uma matriz de riscos, considerando duas dimensões distintas: gravidade do impacto e probabilidade de ocorrência do incidente, representa um método qualitativo de avaliação de riscos.

Assinale a alternativa que apresenta a sequência CORRETA:

- A V - F - V - F.
- B F - V - F - V.**
- C V - F - V - V.
- D V - F - F - V.

6 A segurança da informação está relacionada com a proteção de um conjunto de informações, no sentido de preservar o valor que possuem para um indivíduo ou uma organização. Para alcançar esse objetivo, alguns princípios da segurança da informação devem ser seguidos, como confidencialidade, integridade, disponibilidade e não repúdio. Com base nesses princípios, analise as sentenças a seguir:

I- Na aplicação do princípio da confidencialidade, pode-se usar a criptografia.

II- Na aplicação do princípio da integridade, pode-se usar dispositivos biométricos.

III- Na aplicação do princípio da disponibilidade, pode-se usar sistemas de detecção de intrusão (IDS).

IV- Na aplicação do princípio do não repúdio, pode-se usar cópias de segurança.

Assinale a alternativa CORRETA:

- A As sentenças I e II estão corretas.
- B Somente a sentença I está correta.**
- C As sentenças I e III estão corretas.
- D As sentenças III e IV estão corretas.

7 Os sistemas de informação computadorizados e o acesso às dependências onde eles se encontram são em muitos casos negligenciados. Muito se ouve falar de criptografia, bloqueio, restrição de acesso e tantas outras técnicas criadas para dificultar o acesso de pessoas não autorizadas a dados sigilosos, no entanto, pouco sobre técnicas de segurança para proteger o hardware sobre o qual esses sistemas estão funcionando. Quando o assunto é colocado em pauta, as informações não são divulgadas como deveriam. Os profissionais usuários com pouco conhecimento de segurança em informática acabam por desacreditar da possibilidade de ocorrência de graves prejuízos para a empresa. Com relação ao acesso ao físico, classifique V para as sentenças verdadeiras e F para as falsas:

() Um firewall pode ser configurado para bloquear todo e qualquer tráfego no computador ou na rede.

() Como exemplo de uma barreira física, podemos citar uma simples parede ou até mesmo uma cerca elétrica, já na estrutura lógica, um logon em uma rede.

() Um exemplo de barreira física que limita o acesso seria uma sala-cofre ou roletas de controle de acesso físico.

() Quando a empresa define um acesso físico restrito, a segurança lógica acaba sendo desnecessária.

Assinale a alternativa que apresenta a sequência CORRETA:

FONTE: SILVA, Gilson Ferreira; SCHIMIGUEL, Juliano. Segurança em ambiente de TI: Segurança física da informação em pequenas empresas e estudo de caso em Jundiaí/SP. Revista Observatorio de la Economía Latinoamericana, Brasil, mar. 2017.

- ☒ A V - V - V - F.
- ☐ B V - V - F - V.
- ☐ C F - V - F - V.
- ☐ D V - F - V - F.

Atenção: Esta questão foi cancelada, porém a pontuação foi considerada.

8 Muitas organizações, mesmo tendo conhecimento de vários escândalos de espionagem ocorridos na internet, ainda não compreenderam a eminente necessidade da segurança da informação. Os riscos de acessos indevidos são uma ameaça constante e com um potencial enorme de causar danos irreparáveis e de grande prejuízo às organizações. Desta forma, faz-se necessário a análise e a adoção de medidas que visem a minimizar os riscos da segurança da informação. No que tange ao tratamento do risco, analise as sentenças a seguir:

- I- O tratamento de risco pode ser implementado através de medidas preventivas, como a instituição de uma política de segurança, a definição de controles de acesso físicos e lógicos, entre outros.
- II- A fase do tratamento de risco busca eliminar, reduzir, reter ou transferir os riscos identificados nas fases anteriores.
- III- Para um tratamento de risco adequado, devem-se utilizar todos os controles e práticas de segurança da informação disponíveis.
- IV- A ISO 17799 dispõe sobre os controles e práticas de segurança da informação, estabelecendo uma diretriz e os princípios gerais para gestão da segurança da informação em uma organização a partir dos riscos identificados.
- V- As medidas reativas são ações tomadas sempre após o incidente, a fim de minimizar as consequências dos danos gerados.

Assinale a alternativa CORRETA:

- ☐ A As sentenças I, II e V estão corretas.
- ☐ B As sentenças I, III e IV estão corretas.
- ☐ C As sentenças I, II e IV estão corretas.
- ☐ D As sentenças II, IV e V estão corretas.

9 A política de segurança da informação de uma organização deve considerar a informação um recurso de alto valor e, como tal, protegê-la de ameaças externas e internas. Neste sentido, é essencial considerar os aspectos referentes à segurança nos contextos lógico, físico e ambiental. Referente aos contextos de segurança da informação e suas particularidades, classifique V para as sentenças verdadeiras e F para as falsas:

() A segurança lógica compreende os aspectos relacionados à integridade, à confidencialidade e à disponibilidade das informações armazenadas em dispositivos computacionais e nas redes que os

interligam.

() A segurança física diz respeito às áreas e aos ambientes físicos da organização que não devem ser acessados por pessoas que não têm autorização. Por exemplo: a sala de servidores deve estar sempre trancada e a chave desta sala somente acessível por usuários que estejam autorizados a trabalhar nos servidores.

() Roubo de recursos computacionais (fitas, disquetes, discos rígidos etc.), acesso de pessoas não autorizadas em ambientes protegidos (sala de impressão, sala de servidores etc.) e sabotagem de equipamentos ou arquivos de dados são aspectos relacionados à segurança ambiental.

() A segurança ambiental refere-se à colocação dos recursos computacionais em local adequado, ao controle da temperatura e umidade no ambiente onde estes recursos serão instalados e ainda com cuidados quanto à rede elétrica (correto aterramento, utilização de para-raios, iluminação de emergência) que alimentará os equipamentos.

() A preocupação com a proteção da informação restringe-se a informações armazenadas em mídias digitais.

Agora, assinale a alternativa que apresenta a sequência CORRETA:

A V - V - F - V - F.

B V - F - V - V - V.

C F - V - V - F - F.

D F - V - F - V - F.

Atenção: Esta questão foi cancelada, porém a pontuação foi considerada.

10 Segurança da informação significa proteger seus dados e sistemas de informação de acessos e uso não autorizados, divulgação, modificação, leitura, gravação, inspeção e destruição. O conceito de segurança da informação está ligado à confidencialidade, à integridade e à disponibilidade da informação. O conceito de segurança de processamento está ligado à disponibilidade e à operação da infraestrutura computacional. Esses conceitos são complementares e asseguram a proteção e a disponibilidade das informações das organizações. O impacto da perda e/ou violação de informações para empresa é enorme e pode, em alguns casos, levá-la à falência. Com relação aos itens que devem ser observados na segurança ambiental das informações, classifique V para as opções verdadeiras e F para as falsas:

() Definição de perímetros lógicos.

() Energia alternativa.

() Política de mesa limpa e tela limpa.

Assinale a alternativa que apresenta a sequência CORRETA:

A F - V - V.

B V - V - V.

C F - V - F.

D F - F - V.

Imprimir