Conceitos-chave de Segurança de Informação

Total de pontos 300/550

Para cada questão que se segue, marque UMA E ÚNICA alternativa, a MAIS CORRECTA

Email *

belarminosimaojunior@gmail.com

90 de 170 pontos

✗ 1. Categoria de objectos, pessoas ou outras entidades que representam um perigo para um activo. 0/10

- (●) Agente de ameaça ✗
- ( ) Ameaça
- ( ) Risco
- ( ) Nenhuma

Resposta correta

- (●) Ameaça

Feedback

Resposta incorrecta :(

✓ 2. Está sempre presente e pode ser propositada ou involuntária. 10/10

- ○ Agente de ameaça
- ◉ Ameaça ✓
- ○ As opções acima estão correctas
- ○ Nenhuma

Feedback

Parabéns, a tua resposta está correcta!

✗ 3. Instância ou componente específico de uma ameaça. 0/10

- (●) Ataque ✗
- ( ) Agente de ameaça
- ( ) As opções acima estão correctas
- ( ) nenhuma

Resposta correta

- (●) Agente de ameaça

Feedback

Resposta incorrecta :(

✓ 4. Julian Assange, um trovão, uma tempestade de granizo, ou um tornado são: 10/10

- (●) Agentes de ameaças ✓
- ( ) Ameaças
- ( ) Riscos
- ( ) Nenhuma

Feedback

Parabéns, a tua resposta está correcta!

✓ 5. Probabilidade de que algo indesejável irá acontecer. 10/10

- ○ Ameaça
- ○ Dano
- ◉ Risco ✓
- ○ Nenhuma

Feedback

Parabéns, a tua resposta está correcta!

✗ 6. Computador ou dispositivo de rede utilizado por um hacker para realizar um ataque. 0/10

- ○ Activo
- ○ Sujeito
- ◉ Objecto ✗
- ○ Nenhuma

Resposta correta

- ◉ Sujeito

Feedback

Resposta incorrecta :(

✗ 7. Computador ou dispositivo de rede que é alvo de um ataque. 0/10

- (●) Activo ✗
- ( ) Sujeito
- ( ) Objecto
- ( ) Nenhuma

Resposta correta

- (●) Objecto

Feedback

Resposta incorrecta :(

✓ 8. Recurso organizacional que é protegido. 10/10

- (●) Activo ✓
- ( ) Sujeito
- ( ) Objecto
- ( ) Nenhuma

Feedback

Parabéns, a tua reposta está correcta!

✓ 9. Pode definido como: “Uma falha, brecha, descuido ou erro que pode ser explorado para violar a política de segurança do sistema”. 10/10

- ○ Ameaça
- ○ Ataque
- ○ Risco
- ◉ Nenhuma ✓

Feedback

Parabéns! Está é a definição de vulnerabilidade.

✗ 10. Em segurança de informação, considera-se que existe apenas quando uma vulnerabilidade é conhecida pelo atacante. 0/10

- ○ Ataque
- ◉ Ameaça ✗
- ○ Risco
- ○ Nenhuma

Resposta correta

- ◉ Nenhuma

Feedback

Resposta incorrecta :(

✓ 11. Qual dos seguintes termos pode ser definido como mecanismos de segurança, políticas ou procedimentos que podem combater ataques com sucesso, reduzir riscos, resolver vulnerabilidades e melhorar a segurança dentro de uma organização. 10/10

- (●) Controle, salvaguarda ou contramedida. ✓
- ( ) Postura de segurança ou perfil de protecção
- ( ) Programa de segurança
- ( ) Nenhuma

Feedback

Parabéns, a tua resposta está correcta!

✓ 12. Uma única instância de um ativo de informação que sofre danos ou destruição, modificação ou divulgação não intencional ou não autorizada ou negação de uso. 10/10

- ○ Agente de ameaça
- ○ Ameaça
- ○ Activo
- ◉ Nenhuma ✓

Feedback

Parabéns, a tua resposta está correcta!
Está é a definição de "Perda".

✗ 13. Compreende, maioritariamente, a aspectos gerenciais de segurança, incluindo planejamento, pessoal e programas subordinados. 0/10

- ○ Programa de segurança
- ◉ Postura de segurança ✗
- ○ Contramedidas de segurança
- ○ Nenhuma

Resposta correta

- ◉ Programa de segurança

Feedback

Resposta incorrecta :(

✗ 14. Técnica usada para comprometer um sistema. 0/10

- (●) Ataque ✗
- ( ) Ameaça
- ( ) Agente de ameaça
- ( ) Nenhuma

Resposta correta

- (●) Nenhuma

Feedback

Resposta incorrecta :(

✓ 15. Um computador B sofreu ataque de um outro computador A, e o atacante utiliza este (o computador B) para invadir outros computadores da organização. Desta forma o computador B é: 10/10

- ○ Objecto de ataque
- ○ Sujeito de ataque
- ◉ As alíneas acima estão todas correctas ✓
- ○ Nenhuma

Feedback

Parabéns, a tua resposta está correcta!

✓ 16. O(A) estudante de Criptografia e Segurança de Dados recebeu um email contendo informações bancárias de um(a) fulano(a) por engano e leu, todavia ele(a) deletou-o em seguida quando se apercebeu da falha. Neste caso, o(a) fulano(a): 10/10

- ○ sofreu um ataque activo.
- ◉ sofreu um ataque passivo. ✓
- ○ sofreu nenhum ataque, dado que o(a) estudante não usou a informação para acções maliciosas.
- ○ apenas as duas primeiras alíneas estão correctas

Feedback

Parabéns, a tua resposta está correcta.

✗ 17. Todo o conjunto de controles e salvaguardas, incluindo política, educação, treinamento e conscientização e tecnologia, que a organização implementa para proteger o ativo. 0/10

- (●) Programa de segurança. ✗
- ( ) Postura de segurança.
- ( ) contramedidas de segurança.
- ( ) Nenhuma.

Resposta correta

- (●) Postura de segurança.

Feedback

Resposta incorrecta :(

Introdução à Segurança de Informação 100 de 160 pontos

Para cada questão que se segue, marque UMA E ÚNICA alternativa, a MAIS CORRECTA

✗ 1. Os teóricos sobre a segurança de informação (INFOSEC) ensinam-nos que devemos ter: 0/10

- ○ (A) maior foco na probabilidade de o inimigo não atacar.
- ○ (B) menor foco na probabilidade de o inimigo não atacar.
- ○ (C) maior foco na nossa preparação para nos defender.
- ◉ (D) As alíneas A e C estão correctas. ✗
- ○ (E) As alíneas B e C estão correctas.
- ○ Outra: .....

Resposta correta

- ◉ (E) As alíneas B e C estão correctas.

Feedback

Resposta incorrecta :(

✗ 2. A INFOSEC divide-se em três áreas de actividade. Em termos de RH/IT, indique a mais dispendiosa: 0/10

- (●) Defesa contra catástrofes. ✗
- ( ) Defesa contra faltas ou falhas previsíveis.
- ( ) Defesa contra actividades não autorizadas.
- ( ) Nenhuma é mais dispendiosa que a outra.

Resposta correta

- (●) Defesa contra actividades não autorizadas.

Feedback

Resposta incorrecta :(

✗ 3. A estratégia de sobrevivência é utilizada para evitar: 0/10

- ○ Bloqueio de aplicações/SOs.
- ○ Falhas prolongadas de conectividade.
- ○ Vandalismo.
- ◉ Nenhuma alternativa está correcta. ✗

Resposta correta

- ◉ Falhas prolongadas de conectividade.

Feedback

Resposta incorrecta :(

✓ 4. A defesa de perímetro: 10/10

- ( ) (A) consiste num universo de recursos e pessoas sujeitos ao mesmo perímetro de segurança.
- ( ) (B) permite detectar problemas internos em domínios de segurança.
- (•) (C) permite evitar interacções indesejáveis entre dois lados de um perímetro. ✓
- ( ) As alíneas A e B estão correctas.

Feedback

Parabéns, a tua resposta está correcta!

✓ 5. Qual das seguintes atitudes realistas sobre a INFOSEC enquadra-se na frase: “A arte da guerra nos ensina a contar não só com a probabilidade do inimigo não chegar, mas com a nossa própria prontidão em recebê-lo e em tornar nossa posição inatacável - Sun Tzu” 10/10

- (●) Não existe segurança a cem por cento. ✓
- ( ) A segurança efectiva é cara e retorno do investimento é difícil de avaliar.
- ( ) A segurança contrasta com a disponibilidade.
- ( ) Nenhuma alternativa está correcta.

Feedback

Parabéns, a tua resposta está correcta!

✓ 6. Pertencem ao triângulo C.I.A as seguintes variavéis: 10/10

- [x] Confidencialidade ✓
- [x] Integridade ✓
- [ ] Autenticidade
- [x] Disponibilidade ✓

Feedback

Parabéns, a tua resposta está correcta!

✓ 7. Garantia de acesso, uso oportuno e confiável da informação. 10/10

- ○ Confidecialidade
- ○ Integridade
- ○ Autenticidade
- ◉ Disponiblidade ✓

Feedback

Parabéns, a tua resposta está correcta!

✓ 8. Verificar se os usuários são quem dizem ser e que cada entrada que chega ao sistema veio de uma fonte confiável. 10/10

- ○ Confidencialidade
- ○ Integridade
- ◉ Autenticidade ✓
- ○ Disponibidade

Feedback

Parabéns, a tua resposta está correcta!

9. Selecione a definição correspondente a cada característica crítica de informação.

	Confidencialidade	Integridade	Autenticidade	Disponibilidade	Utilidade
descreve como os dados estão livres de erros e têm o valor que o usuário espera.	○	○	○	○	○
descreve como os dados são genuínos ou originais em vez de reproduzidos ou fabricados.	○	◉	○	○	○
descreve como os dados são acessíveis e formatados corretamente para uso sem interferência ou obstrução.	○	○	○	◉	○

descreve como os dados são protegidos contra divulgação ou exposição a indivíduos ou sistemas não autorizados.	○	○	○	○	○
descreve como os dados são inteiros, completos e não corrompidos.	○	◉	○	○	○
descreve como a propriedade ou controle dos dados é legítimo ou autorizado.	○	○	○	○	○
descreve como os dados têm valor ou utilidade para um propósito final.	○	○	○	○	◉

propósito final.

Respostas corretas

	Confidencialidade	Integridade	Autenticidade	Disponibilidade	Utilidade	F
descreve como os dados são genuínos ou originais em vez de reproduzidos ou fabricados.	○	○	◉	○	○	
descreve como os dados são protegidos contra divulgação ou exposição a indivíduos ou sistemas não autorizados.	◉	○	○	○	○	

✗ 10. São componentes de sistema de informação EXCEPTO: 0/10

- [ ] Procedimentos
- [ ] Tecnologias
- [ ] Dados
- [x] Educação ✓

Resposta correta

- [x] Tecnologias
- [x] Educação

Feedback

Resposta incorrecta :(

CVDSS/SecSDLC 50 de 140 pontos

Leia atentamente as questões que se seguem e responda acertadamente.

✗ 1. A implementação de sistemas de segurança nas organizações não pode ser de dia para noite porque requer: 0/10

- [ ] coordenação.
- [ ] noção de custo-benefício.
- [ ] paciência.
- [x] tempo ✓

Resposta correta

- [x] coordenação.
- [x] paciência.
- [x] tempo

Feedback

Resposta incorrecta ou parcialmente correcta.

✗ 2. A implementação de sistemas de segurança pode ser executada sob duas abordagens: Top-down ou Bottom-up, sendo a primeira superior à segunda porque: 0/10

- [ ] Possui métodos para influenciar a cultura organizacional.
- [x] Possui um processo claro de planeamento e implementação. ✓
- [ ] Tem maior perícia técnica dos administradores individuais
- [ ] Tem um campeão e fundos dedicados

Resposta correta

- [x] Possui métodos para influenciar a cultura organizacional.
- [x] Possui um processo claro de planeamento e implementação.
- [x] Tem um campeão e fundos dedicados

Feedback

Resposta incorrecta ou parcialmente correcta.

✓ 3. A Empresa YYY, o(a) nomeou como CISO (Chief Information Security Officer), sendo que, suas actividades incluem: supervisionar o armazenamento e backup de dados, implementar os procedimentos e políticas específicos estabelecidos no EISP (Enterprise Information Security Policies) e fazer relatórios informativos dos dados. Em qual categoria de 'Responsabilidade sobre os dados' mais se enquadraria? 10/10

- (●) Guardões de dados. ✓
- ( ) Proprietários de dados.
- ( ) Utilizadores de dados
- ( ) Nenhuma

Feedback

Parabéns, a tua resposta está correcta!

✗ 4. A Empresa YYY, o(a) contratou para garantir que um determinado software siga princípios de desenvolvimento seguro, tendo em conta o que aprendeu no decorrer das apresentações em grupo diga, quais destes consideraria DISPENSÁVEIS? 0/10

- [ ] Aceitabilidade psicológica.
- [ ] Design Aberto
- [ ] Optimização do software
- [x] Padrão baseada em permissões ✗
- [x] Privilégio mínimo possível ✗
- [x] Separação de deveres ✓
- [x] Separação de Privilégios ✗

Resposta correta

- [x] Optimização do software
- [x] Separação de deveres

Feedback

Resposta incorrecta ou parciamente correcta.

5. Para cada actividade abaixo, indique a que fase do CVDSS pertence.

	Investigação	Análise	Desenho Lógico	Desenho Físico	Implementação	Manutençã
Estuda-se a viabilidade para determinar a prontidão da organização para o projecto proposto.	○	◉	○	○	○	○
Faz-se o exame e implementação de políticas-chave que influenciarão as decisões futuras	○	○	◉	○	○	○
Efectua-se a monitoria.	○	○	○	○	○	◉
São seleccionadas aplicações para prover serviços necessários	○	○	○	◉	○	○
Começa com elaboração de um plano	○	◉	○	○	○	○

chamado EISP

Respostas corretas

	Investigação	Análise	Desenho Lógico	Desenho Físico	Implementação	Manutenção
Estuda-se a viabilidade para determinar a prontidão da organização para o projecto proposto.	○	○	○	◉	○	○
São seleccionadas aplicações para prover serviços necessários	○	○	◉	○	○	○
Começa com elaboração de um plano chamado EISP	◉	○	○	○	○	○

5. Para cada actividade abaixo, indique a que fase do CVDSS pertence.

	Investigação	Análise	Desenho Lógico	Desenho Físico	Implementação	Manutenção
Faz-se a avaliação das competências técnicas	◉	○	○	○	○	○
Começa com a avaliação dos sistemas existentes e termina com a actualização da análise da viabilidade	○	◉	○	○	○	○
Decorre a análise da viabilidade organizacional para aferir se a organização pode ou não avançar à fase seguinte	○	◉	○	○	○	○
Avaliação de tecnologias de segurança de informação	○	○	◉	○	○	○
Faz-se a planificação	○	○	◉	○	○	○

de acções de resposta aos incidentes

Respostas corretas

	Investigação	Análise	Desenho Lógico	Desenho Físico	Implementação	Manutenção
Faz-se a avaliação das competências técnicas	○	○	○	○	◉	○
Decorre a análise da viabilidade organizacional para aferir se a organização pode ou não avançar à fase seguinte	◉	○	○	○	○	○
Avaliação de tecnologias de segurança de informação	○	○	○	◉	○	○

Necessidade de Segurança 60 de 80 pontos

Leia atentamente as questões que se seguem e responda acertadamente.

✗ 1. As Principais diferenças existentes entre ameaça e ataque, no contexto da disciplina, são: 0/10

- [ ] Ao contrário das ameaças, que estão sempre presentes, os ataques existem apenas quando um acto específico pode causar um prejuízo.
- [ ] Ao contrário dos ataques, que estão sempre presentes, as ameaças existem apenas quando um acto específico pode causar um prejuízo.
- [ ] Um ataque representa um risco potencial para um activo de informação, enquanto uma ameaça representa um acto contínuo contra o ativo que pode resultar em perda.
- [x] Uma ameaça representa um risco potencial para um activo de informação, enquanto um ataque representa um acto contínuo contra o ativo que pode resultar em perda. ✓

Resposta correta

- [x] Ao contrário das ameaças, que estão sempre presentes, os ataques existem apenas quando um acto específico pode causar um prejuízo.
- [x] Uma ameaça representa um risco potencial para um activo de informação, enquanto um ataque representa um acto contínuo contra o ativo que pode resultar em perda.

Feedback

Upsi :(

✓ 2. A razão primordial para uma organização se preocupar com segurança como actividade de suporte aos seus sistemas de informação é a existência de: 10/10

- ○ Vulnerabilidade
- ◉ Risco ✓
- ○ Ameaça
- ○ Agente de ameaça

Feedback

Parabéns, a tua resposta está correcta!

✗ 3. São funções de segurança de informação EXCEPTO. 0/10

- ○ Contratar um auditor para implementação de PCI DSS (Payment Card Industry Data Security Standard) numa organização financeira.
- ◉ Proteger a funcionalidade de uma organização. ✗
- ○ Garantir uma operação segura das aplicações.
- ○ Proteger os dados que a organização colecciona e usa.
- ○ Salvaguardar os activos tecnológicos organizacionais.
- ○ Nenhuma das alíneas anteriores está correcta.

Resposta correta

- ◉ Contratar um auditor para implementação de PCI DSS (Payment Card Industry Data Security Standard) numa organização financeira.

Feedback

Resposta incorrecta :(

✓ 4. Qual das 'actividades' de segurança de informação tem mais a ver com a frase: 'proteger os dados em transmissão, processamento e em repouso - é um aspecto crítico da segurança da informação.' 10/10

- ○ Contratar um auditor para implementação de PCI DSS numa organização financeira.
- ○ Proteger a funcionalidade de uma organização
- ○ Garantir uma operação segura das aplicações
- ◉ Proteger os dados que a organização colecciona e usa ✓
- ○ Salvaguardar os activos tecnológicos organizacionais
- ○ Nenhuma

Feedback

Parabéns, a tua resposta está correcta!

✓ 5. O(A) atacante utiliza recursos computacionais e de rede para experimentar todas as combinações de senhas possíveis no sistema da vítima. 10/10

- (●) Ataque de força bruta ✓
- ( ) Engenharia social
- ( ) Phishing
- ( ) Pharming
- ( ) Spoofing
- ( ) Sniffing

Feedback

Parabéns, a tua resposta está correcta!

✓ 6. Redirecionamento do tráfego da Web de usuários legítimos para sites ilegítimos com a intenção de coletar informações pessoais. 10/10

- ○ Ataque de força bruta
- ○ Engenharia social
- ○ Phishing
- ◉ Pharming ✓
- ○ Spoofing
- ○ Sniffing

Feedback

Parabéns, a tua resposta está correcta!

✓ 7. Uma técnica para obter acesso não autorizado a computadores usando um endereço IP de origem forjado ou modificado para dar a percepção de que as mensagens são provenientes de um host confiável. 10/10

- ○ Ataque de força bruta
- ○ Engenharia social
- ○ Phishing
- ○ Pharming
- ◉ Spoofing ✓
- ○ Sniffing

Feedback

Parabéns, a tua resposta está correcta!

✓ 8. A propriedade intelectual, como segredos comerciais, direitos autorais, marcas registradas ou patentes, são ativos intangíveis que podem ser atacados por meio de: 10/10

- ○ Pirataria de software.
- ○ Exploração de controles de proteção de ativos
- ◉ As alíneas acima estão todas correctas ✓
- ○ Nenhuma

Feedback

Parabéns, a tua resposta está correcta!