Questão 1

A engenharia social é uma técnica de ataque utilizada para explorar a natureza Humana.
MITNICK, Kevin D.; SIMON, William M. A arte de enganar. São Paulo: Makron Books, 2003.
Aplicada em: 2017 **Banca:** IESES **Órgão:** IGP-SC **Prova:** Perito Criminal em Informática(adaptada)
Considerando as práticas do que se denomina 'Engenharia Social' no contexto da Segurança da Informação, é correto:

A. Algoritmos de 'força bruta' são um instrumento comumente utilizados para descoberta de informações.

B. **Um 'ataque' de engenharia social pode utilizar estratégias de relacionamento pessoal para obtenção de informações sigilosas.**

C. A instalação de softwares detectores de 'phishing' é uma estratégia para evitar ataques de um engenheiro social.

D. Usa firewall.

E. A utilização de certificados digitais A3 é mais adequada que certificados A1.

Questão 2

Os testes de penetração ou pentests, são também conhecidos como testes de intrusão e ethical hacking, e são realizados a partir do ambiente externo.
O teste de _____é também conhecido como teste com conhecimento total, e é conduzido com todo o conhecimento sobre o ambiente, que engloba o código-fonte, documentações e diagramas.

A. **Gray-Box.**

B. White-Box.

C. Red-Box.

D. Black-Box.

E. Yellow-Box.

< ANTERIOR PRÓXIMA >

Questão 3

Segurança da informação só é possível se todos da organização seguirem os mesmos princípios e realizarem suas tarefas do dia a dia com base em preocupações comuns de manutenção das propriedades da segurança da informação.
Complete a lacuna e assinale a alternativa correta.
Antes,a_____ tinha como objetivo a comunicação secreta, e atualmente foram acrescentados objetivos de autenticação de mensagens, assinatura digital, protocolos para troca de chaves secretas, protocolos de autenticação, leilões e eleições eletrônicas, dinheiro digital.

A. Disponibilidade
B. **Criptografia**
C. Política da Segurança
D. Segurança da Informação
E. Integridade

Questão 4

Há diversas alternativas e elas refletem diretamente em como a segurança e privacidade deve ser tratada por sua empresa, principalmente quanto às responsabilidades.
_____que realiza os testes de segurança de uma forma interativada um teste de segurança conhecido como, combinando os testes estáticos e dinâmicos.
O que preenche corretamente a coluna é:

A. LAST ou Lógica estática
B. SAST ou Análise estática
C. DAST ou Análise dinâmica
D. LDST ou Lógica dinâmica
E. **IAST ou Forma interativa**

< ANTERIOR PRÓXIMA >

Questão 5

Com o crescimento da internet e o uso de dispositivos móveis nas empresas é inevitável a ocorrência de problemas de segurança, é preciso muito planejamento e muito trabalho da equipe de TI para ligar com tudo isso. É importante criar normas rígidas e principalmente treinar toda a equipe interna e externa.
A NBR ISO/IEC 27005 define risco como a combinação das consequências advindas da ocorrência de um determinado evento indesejado com a probabilidade de ocorrência desse mesmo evento. A análise e a avaliação de riscos capacitam os gestores a priorizar os riscos. De acordo com essa norma, a atividade de análise de riscos inclui:

A. o tratamento e a aceitação de riscos.

B. a comunicação e a avaliação de riscos.

C. **a identificação e a estimativa de riscos.**

D. a estimativa e o tratamento de riscos.

E. a avaliação e o tratamento de riscos.

Questão 6

O avanço dos ataques cibernéticos, que vitimam indivíduos, empresas e países, é motivado por uma série de fatores que tornam ainda mais desafiador o trabalho do profissional de segurança da informação.
Banca: FCC, 2017, **Órgão:** TRF - 5ª REGIÃO **Prova:** Analista Judiciário - Informática Infraestrutura
O mecanismo de ação do *Distributed Denial of Service* - DDoS faz uso da escravização de vários computadores para esgotar os recursos de servidores da internet, impedindo-os de executar suas tarefas. Nesse contexto, para escravizar os computadores o atacante utiliza o código malicioso:

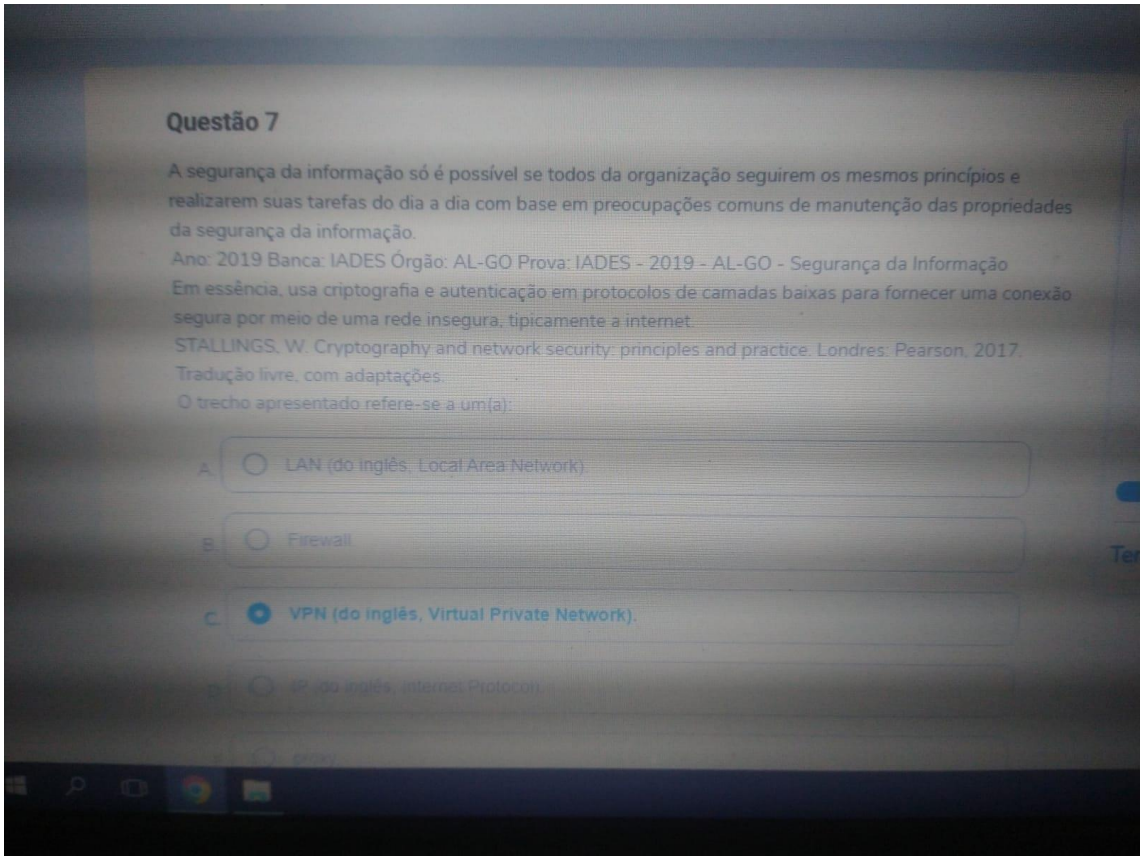
A. ***botnet.***

B. keylogger.

C. spyware.

D. backdoor.

E. adware.



Questão 7

A segurança da informação só é possível se todos da organização seguirem os mesmos princípios e realizarem suas tarefas do dia a dia com base em preocupações comuns de manutenção das propriedades da segurança da informação.

Ano: 2019 Banca: IADES Órgão: AL-GO Prova: IADES - 2019 - AL-GO - Segurança da Informação

Em essência, usa criptografia e autenticação em protocolos de camadas baixas para fornecer uma conexão segura por meio de uma rede insegura, tipicamente a internet.

STALLINGS, W. Cryptography and network security: principles and practice. Londres: Pearson, 2017. Tradução livre, com adaptações.

O trecho apresentado refere-se a um(a):

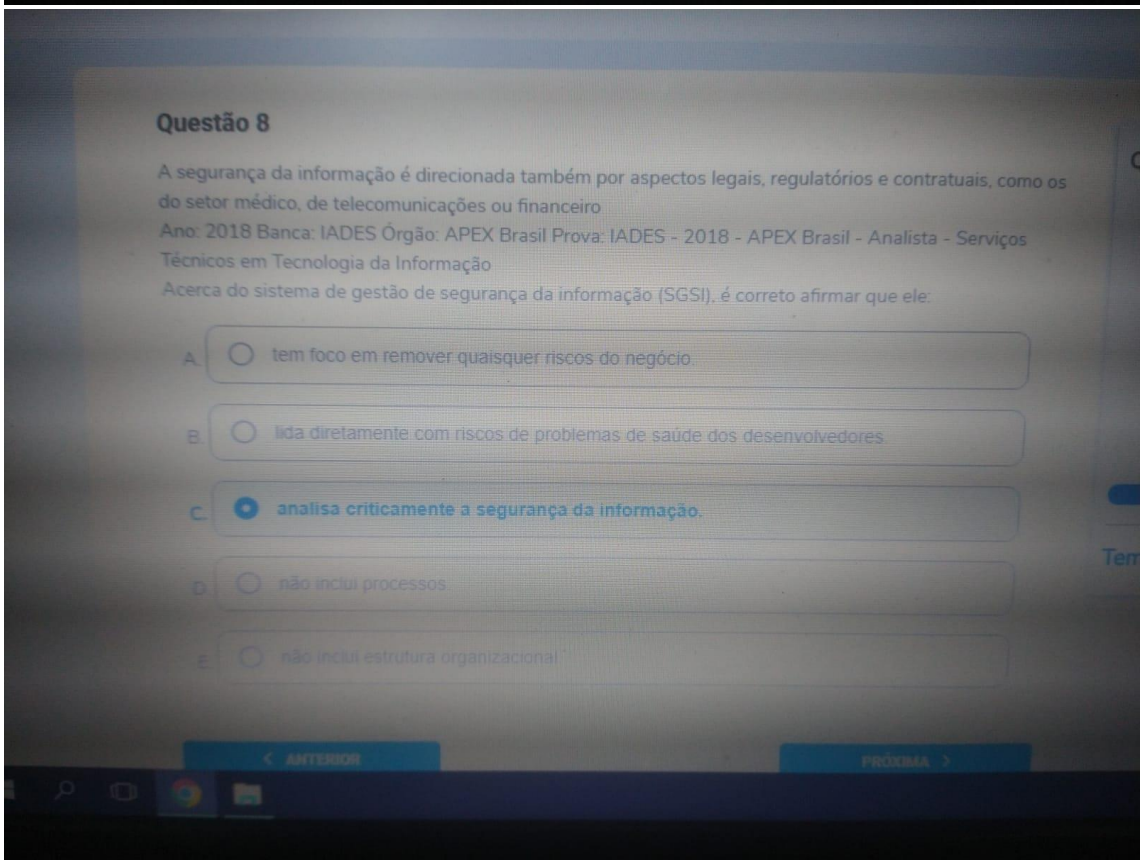
A. LAN (do inglês, Local Area Network).

B. Firewall.

C. **VPN (do inglês, Virtual Private Network).**

D. IP (do inglês, Internet Protocol).

E. PGP.



Questão 8

A segurança da informação é direcionada também por aspectos legais, regulatórios e contratuais, como os do setor médico, de telecomunicações ou financeiro.

Ano: 2018 Banca: IADES Órgão: APEX Brasil Prova: IADES - 2018 - APEX Brasil - Analista - Serviços Técnicos em Tecnologia da Informação

Acerca do sistema de gestão de segurança da informação (SGSI), é correto afirmar que ele:

A. tem foco em remover quaisquer riscos do negócio.

B. lida diretamente com riscos de problemas de saúde dos desenvolvedores.

C. **analisa criticamente a segurança da informação.**

D. não inclui processos.

E. não inclui estrutura organizacional.

< ANTERIOR PRÓXIMA >

Questão 9

Você já está ciente de alguns dos riscos relacionados ao uso de computadores e da Internet e que, apesar disso, reconhece que não é possível deixar de usar estes recursos, está no momento de aprender detalhadamente a se proteger. No seu dia a dia, há cuidados que você toma, muitas vezes de forma instintiva, para detectar e evitar riscos. Por exemplo: o contato pessoal e a apresentação de documentos possibilitam que você confirme a identidade de alguém, a presença na agência do seu banco garante que há um relacionamento com ele, os Cartórios podem reconhecer a veracidade da assinatura de alguém, etc. E como fazer isto na Internet, onde as ações são realizadas sem contato pessoal e por um meio de comunicação que, em princípio, é considerado inseguro?

https://cartilha.cert.br/mecanismos/ Acesso 14 mar 2021

Possuímos alguns recursos para minimizar os ataques temos medidas de segurança assinale a alternativa INCORRETA:

A. **Ausência de política de segurança e auditoria**

B. Classificação das informações e firewall

C. Proteção antivírus e sistema de backup

D. Palavra para usuários e sistema de detecção de intrusos

Questão 10

Em desenvolvimento de software seguro, para maior proteção dos acessos, é conveniente que o procedimento de log-on divulgue o mínimo de informações sobre o sistema, não fornecendo, assim, informações detalhadas a um usuário não autorizado.

A partir do contexto apresentado, analise as afirmativas I, II e III e assinale a alternativa que identifica de forma correta, procedimentos para um log-on eficiente:

I - Não ocultar senhas que estão sendo digitadas.

II - Não transmitir senhas com textos claros.

III - Mostrar um aviso de que a aplicação só pode ser acessada por pessoas autorizadas.

A. Somente a afirmativa II está correta.

B. Somente as afirmativas I e II estão corretas.

C. Somente a afirmativa I está correta.

D. **Somente as afirmativas II e III estão corretas.**

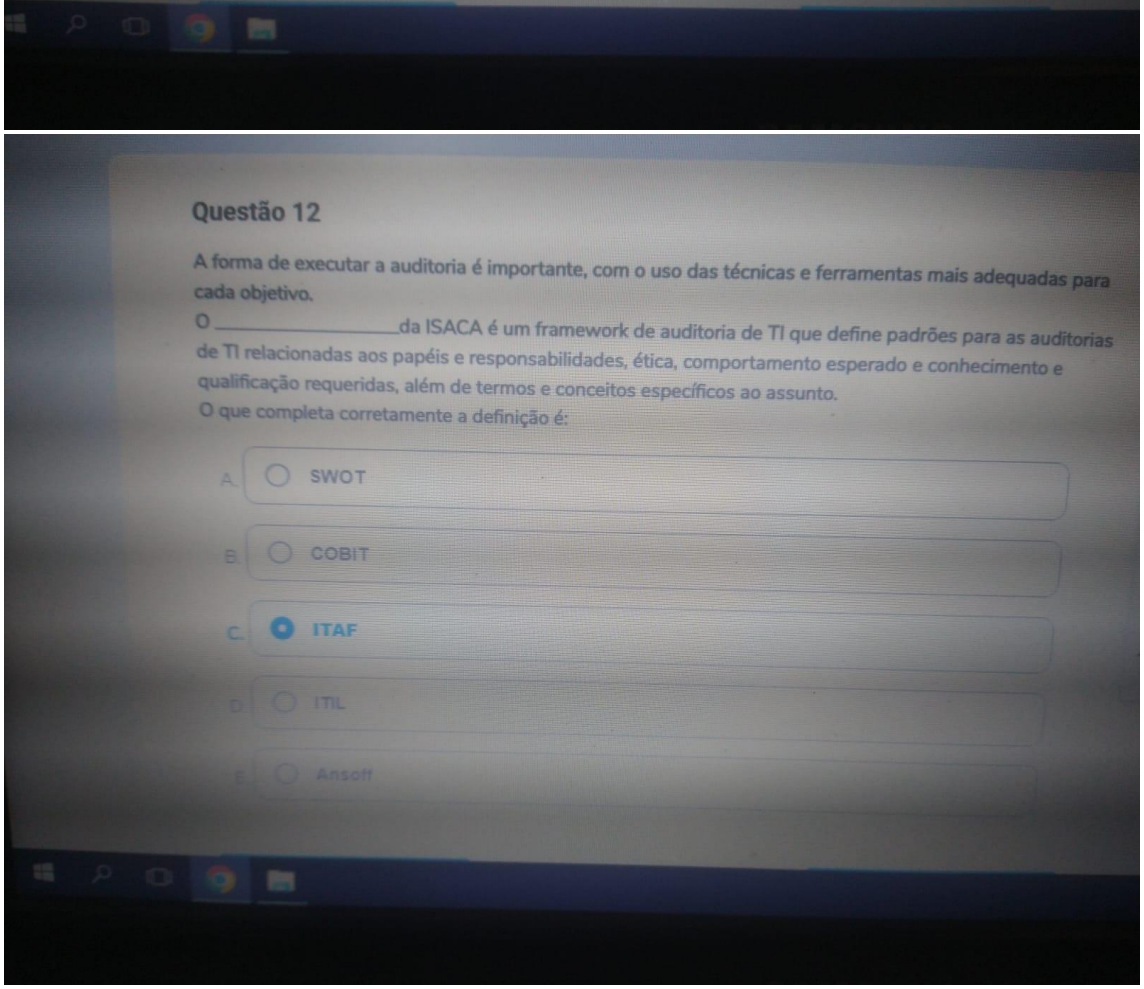
E. Somente a afirmativa III está correta.

Questão 11

As ameaças enfrentadas pela aplicação podem ser categorizadas com base nos objetivos e propósitos dos ataques. A Microsoft adota uma categoria de ameaças conhecida como STRIDE (MICROSOFT, 2004).
Aplicada em: 2017 **Banca:** CESPE **Órgão:** TRT - 7ª Região (CE) **Prova:** Analista Judiciário - Tecnologia da Informação

O ataque que amplia o número de acessos a um servidor, gerando indisponibilidade de recursos aos usuários, é denominado:

A. spoofing.
B. botnet
C. phishing
D. adware
E. DoS.



Questão 12

A forma de executar a auditoria é importante, com o uso das técnicas e ferramentas mais adequadas para cada objetivo.

O _____da ISACA é um framework de auditoria de TI que define padrões para as auditorias de TI relacionadas aos papéis e responsabilidades, ética, comportamento esperado e conhecimento e qualificação requeridas, além de termos e conceitos específicos ao assunto.

O que completa corretamente a definição é:

A. SWOT
B. COBIT
C. ITAF
D. ITIL
E. Ansoff

Questão 13

A proteção de uma empresa é feita com o uso de mecanismos de segurança tecnológicos, físicos, processuais e regulatórios. É com a sua implementação que as finalidades de prevenção, detecção e resposta a incidentes são cumpridas.
É uma combinação de hardware e software que isola a rede interna de uma organização da internet em geral, permitindo que alguns pacotes passem e bloqueando outros, trata-se do:

A. plugin.
B. browser.
C. link.
D. **firewall.**
E. outlook.

< ANTERIOR PRÓXIMA >

Questão 14

Os testes de penetração ou pentests, são também conhecidos como testes de intrusão e ethical hacking, e são realizados a partir do ambiente externo.
O teste de _____ é o teste em que alguma informação é provida para o profissional, como uma credencial de acesso, enquanto outras informações têm que ser descobertas.

A. **Red-Box**
B. **Black-Box.**
C. **Gray-Box.**
D. White-Box.
E. Yellow-Box

< ANTERIOR PRÓXIMA >

Questão 15

E os testes de segurança são uma das principais atividades de empresas especializadas em segurança e privacidade, com a oferta de serviços de análise de vulnerabilidades e pentests, por exemplo.
Vulnerabilidade é o (a)

A. efeito da incerteza quanto aos objetivos.

B. resultado de um evento que afetou um ativo.

C. potencial causa de um incidente não desejado que pode resultar em danos à organização.

D. processo de identificar, reconhecer e tratar riscos.

E. **ponto fraco de um ativo que pode ser explorado por uma ameaça.**

< ANTERIOR

PRÓXIMA >

Questão 16

O avanço dos ataques cibernéticos, que vitimam indivíduos, empresas e países, é motivado por uma série de fatores que tornam ainda mais desafiador o trabalho do profissional de segurança da informação. Quando *sites* de diversos sofrem ataques através da Internet com o objetivo de deixá-los inacessíveis. Este tipo de ataque é conhecido como:

A. *port scanning.*

B. *backdoor.*

C. ***denial of service.***

D. *cookie hijacking.*

E. *phishing.*

< ANTERIOR