

## Questão 1

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. ☐ spyware.

B. ☐ keylogger.

C. ☒ botnet.

D. ☐ adware.

E. ☐ backdoor.

## Questão 2

A Criptografia tem como definição que é a arte de escrever ou resolver códigos. A criptografia deriva de duas palavras gregas: kryptos, que significa oculto, e graphien, que significa escrever. Seu objetivo não é esconder a existência da mensagem, mas sim de apenas ocultar o seu significado.

Ano: 2018 Banca: FCC Órgão: SEFAZ-SC Prova: FCC - 2018 - SEFAZ-SC - Auditor-Fiscal da Receita Estadual - Tecnologia da Informação (Prova 3)

A Assinatura Digital tem como objetivo principal garantir que o documento recebido é o mesmo que o remetente enviou, que não foi alterado durante o transporte e que o emissor não poderá negar que assinou e enviou tal documento. No processo da Assinatura Digital, após a geração do hash sobre o documento original, é aplicada, sobre esse hash, a criptografia utilizando a chave:

A. ☐ privada do receptor.

B. ☐ pública do receptor.

C. ☒ privada do emissor.

D. ☐ simétrica compartilhada.

E. ☐ pública do emissor.

### Questão 3

As ferramentas de segurança visam à prevenção, detecção e resposta a ataques, protegendo os ativos contra ataques que comprometam uma das propriedades básicas de segurança da informação.

Ano: 2019 Banca: FGV Órgão: DPE-RJ Prova: FGV - 2019 - DPE-RJ - Técnico Superior Especializado - Tecnologia da Informação

De acordo com a norma ABNT NBR ISO/IEC 27001:2013, uma organização deve programar auditorias internas a fim de verificar a aderência da conformidade do sistema de gestão da segurança da informação aos seus requisitos e à legislação vigente.

Sobre a realização da auditoria interna, é correto afirmar que:

- A. ☐ os auditores devem ser do próprio setor auditado a fim de possibilitar o aproveitamento de seu conhecimento acerca das atividades desenvolvidas;
- B. ☐ os auditores não devem conhecer e considerar os resultados das auditorias anteriores para não influenciarem o trabalho de verificação;
- C. ☒ os resultados das auditorias devem ser de conhecimento da direção responsável pelo setor auditado;
- D. ☐ os relatórios das auditorias podem ser descartados na ausência de inconformidades.
- E. ☐ os critérios de verificação devem ser sempre os mesmos, independentemente do escopo ou do processo da organização a ser auditado;

### Questão 4

Os controles têm objetivos diversos, como para o processo de aquisição, desenvolvimento e manutenção de sistemas, ou para o controle de acesso lógico e físico.

Quando nos referimos esses controles, o que completa corretamente a lacuna é:

Os controles \_\_\_\_\_ tem como exemplo firewall e VPN.

- A. ☐ Lógicos
- B. ☐ Físicos
- C. ☐ Processuais
- D. ☐ Laboratoriais
- E. ☒ Tecnológicos

### Questão 5

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

Banca: FCC, Órgão: MPE-RN Prova: [Analista de Tecnologia da Informação - Redes-Segurança-Conectividade](#)

Instrumento que define as normas a serem aplicadas na empresa e praticadas por seus funcionários, colaboradores, prestadores de serviço, clientes e fornecedores, com o objetivo de preservar os ativos de informação livres de risco, assegurando a continuidade dos negócios. É a definição de:

- A. ☐ Informação.
- B. ☒ Política de Segurança da Informação.
- C. ☐ Infraestrutura de Tecnologia da Informação.
- D. ☐ Gerência de Relacionamento de Clientes.
- E. ☐ Gestão de Tecnologia da Informação.

### Questão 6

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 lidar 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. ☒ a identificação e a estimativa de riscos.
- B. ☐ o tratamento e a aceitação de riscos.
- C. ☐ a comunicação e a avaliação de riscos.
- D. ☐ a avaliação e o tratamento de riscos.
- E. ☐ a estimativa e o tratamento de riscos.

### Questão 7

O objetivo e o escopo da auditoria podem estar relacionados com a conformidade com normas, padrões, frameworks, leis e requisitos de negócios.

Analise as técnicas e ferramentas que envolvem interação com pessoas, então assinale o que preenche corretamente a lacuna (BENETON, 2017) (ISACA, 2016) (ISACA, 2017) (KAMAL, 2020) (LIMA, 2020):

\_\_\_\_\_ são a obtenção de dados via perguntas individuais ou para grupos.

- A. ☐ Entrevistas
- B. ☐ Perguntas e observação
- C. ☒ Pesquisas
- D. ☐ Questionários
- E. ☐ Dinâmicas em grupo

### Questão 8

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. ☐ Usa firewall.
- B. ☐ A utilização de certificados digitais A3 é mais adequada que certificados A1.
- C. ☐ A instalação de softwares detectores de 'phishing' é uma estratégia para evitar ataques de um engenheiro social.
- D. ☒ Um 'ataque' de engenharia social pode utilizar estratégias de relacionamento pessoal para obtenção de informações sigilosas.
- E. ☐ Algoritmos de 'força bruta' são um instrumento comumente utilizados para descoberta de informações.

### Questão 9

O objetivo e o escopo da auditoria podem estar relacionados com a conformidade com normas, padrões, frameworks, leis e requisitos de negócios.

Analisar as técnicas e ferramentas que envolvem interação com pessoas, então assinale o que preenche corretamente a lacuna (BENETON, 2017) (ISACA, 2016) (ISACA, 2017) (KAMAL, 2020) (LIMA, 2020):

\_\_\_\_\_ são reuniões com profissionais de áreas-chave para a auditoria.

- A. ☐ Dinâmicas em grupo
- B. ☒ Entrevistas
- C. ☐ Questionários
- D. ☐ Pesquisas
- E. ☐ Perguntas e observação

### Questão 10

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.

Ano: 2020 Banca: FCC Órgão: AL-AP Prova: FCC - 2020 - AL-AP - Analista Legislativo - Administrador de Rede e Telecomunicações

A equipe que administra a infraestrutura de tecnologia da informação precisa liberar acesso sem filtros de proteção para navegação na internet através de dispositivos móveis autenticados na rede como pertencentes aos visitantes que regularmente comparecem à empresa para reuniões executivas. Para isso, um conjunto de equipamentos servidores de domínio WEB (DNS), servidores FTP e um conjunto de switches WiFi serão mapeados nessa rede de visitantes que implementa:

- A. ☐ um IPS
- B. ☒ uma DMZ.
- C. ☐ uma criptografia.
- D. ☐ um IDS.
- E. ☐ um certificado digital.

### Questão 11

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: FGV, 2017, Órgão: MPE-BA, Prova: **Analista Técnico - Tecnologia**

Um ciber criminoso envia para sua vítima um e-mail falso, em que se passa por uma instituição conhecida, informando que seu cadastro está irregular e que, para regularizá-lo, é necessário clicar no link presente no corpo do e-mail.

Esse tipo de falsificação de uma comunicação por e-mail é uma técnica conhecida como:

A. ☐ Denial of Service;

B. ☐ MAC Spoof;

C. ☐ SQL Injection.

D. ☐ Sniffing;

E. ☒ Phishing;

### Questão 12

Entre os controles que convêm ser realizados prioritariamente com o objetivo de proteger a integridade do software e da informação contra códigos maliciosos e códigos móveis no gerenciamento das operações de TI e das comunicações em uma empresa, inclui-se a ação de:

A. ☐ estabelecer acordos de níveis de operação para responder a ameaças e vulnerabilidades na rede com eficiência.

B. ☐ colocar informações do sistema de emergência em local central na rede como endereços IP e regras para o firewall

C. ☒ realizar procedimentos para a conscientização dos usuários contra métodos de engenharia social.

D. ☐ garantir que a segurança da informação seja uma atividade restrita à área de TI.

E. ☐ evitar a instalação de novos patches para não introduzir modificações no ambiente

### Questão 13

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: FUNRIO Órgão: MPOG Prova: Analista de Tecnologia da

Informação <https://www.qconursos.com/questoes-de-concursos/disciplinas/tecnologia-da-informacao-seguranca-da-informacao/ataques-e-ameacas>

O que significa o tipo de ataque de DoS conhecido por "Inundação na conexão" ?

- A. ☐ O atacante executa um pequeno número de conexões TCP do tipo FIN em um alvo, tornando-o incapaz de responder a conexões legítimas.
- B. ☐ O atacante executa uma conexão do tipo FIN em um alvo, tornando-o incapaz de responder a conexões legítimas.
- C. ☒ O atacante executa um grande número de conexões TCP abertas ou semiabertas em um alvo, tornando-o incapaz de responder a conexões legítimas.
- D. ☐ O atacante executa um grande número de conexões UDP em um alvo, tornando-o incapaz de responder a conexões legítimas.

### Questão 14

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.

Um equipamento importante de rede utilizado para restringir o acesso a uma rede de computadores, evitando assim um ataque indesejado, é

A. ☒ **firewall.**

B. ☐ roteador.

C. ☐ chaveador.

D. ☐ gateway.

E. ☐ switch.

### Questão 15

O bem mais importante que as empresas possuem, sem dúvida, são as informações gerenciais, sendo muito importantes para a tomada de decisões. 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 lidar com tudo isso. É importante criar normas rígidas e principalmente treinar toda a equipe interna e externa.

Fonte: <http://analistati.com/politica-de-seguranca-da-informacao-como-fazer/> Acesso: 16 abril 21

Com relação aos controles e à política de segurança da informação de uma organização, analise:

I. A distribuição de diretrizes e normas sobre a política de segurança da informação para todos os gerentes, funcionários e outras partes envolvidas é um fator crítico para o sucesso da implementação da segurança da informação em uma organização.

II. A segurança da informação é obtida a partir da implementação de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de *software* e *hardware*.

III. Uma política de segurança da informação que reflita os objetivos do negócio, apesar de importante, não representa um fator crítico para o sucesso da implementação da segurança da informação dentro de uma organização.

IV. Um controle é uma forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal.

Está correto o que consta em :

- A. ☐ II, apenas.
- B. ☒ I, II e IV, apenas.

### Questão 16

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 de:

- A. ☐ plugin.
- B. ☐ browser.
- C. ☐ outlook.
- D. ☒ firewall.
- E. ☐ link.