Questão 1

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) link.
B) browser.
C) outlook.
D) firewall.
E) plug in.

Questão 2

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, cliente s 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) Gestão de Tecnologia da Informação.
C) Infraestrutura de Tecnologia da Informação.
D) Gerência de Relacionamento de Clientes.
E) Política de Segurança da Informação.

Questão 3

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: 2019 Banca: UFGD Órgão: UFGD Uma séria ameaça à lojas virtuais, serviços de armazenamento de arquivos na nuvem, serviços de e-mail, provedores d e Internet, dentre outros, é um tipo de ataque que visa a impedir usuários legítimos de acessarem determinado serviço. Esse tipo de ataque torna os sistemas d e computador inacessíveis , inundando servidores, redes e inclusive sistema s de usuário final com tráfego basicamente inútil, provindos de um ou diferentes hosts contami nados reunidos para esse fim, causando indisponibilidade do alvo, fazendo com que os usuários reais não consigam acessar o recurso pretendido. Essa ameaça é conhecida com o:

A) interceptação de tráfego (Sniffing).
B) força bruta (Brute force).
C) desfiguração de página (Defacement).
D) falsificação de e-mail (E-mail spoofing).
E) negação de serviço (DoS e DDoS).

Questão 4

Com o crescimento da internet e o uso de dispositivos móveis nas empresas é inevitável a ocorrência de problemas d e 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. Concurso TJ PA Analista Judiciário - Analista d e Sistemas - Desenvolvimento 2019 . Centro de Seleção e de Promoção de Evento s UnB (CESPE/CEBRAS PE) Nas questões que avaliarem conhecimentos de informática e(ou) tecnologia da informação, a menos que seja explicitamente informado o contrário, considere que todos os programas mencionados estão e m configuração-padrão e que não há restrições de proteção, de funcionamento e de uso em relação aos programas, arquivos, diretórios, recursos e equipamentos mencionados. A Lei n.º 13.709/201 8 (Lei Geral de Proteção de Dados Pessoais) prevê a realização do tratamento de dados pessoais, mediante o consentimento do titular dos dado s, para o cumprimento de obrigação legal o u regulatória e para a realização de estudos ou execução de contratos a pedido do titular.
As hipótese s em questão são exemplos de:
A) requisitos para o tratamento de dados pessoais sensíveis.
B) tratamento de dados pessoais de crianças e adolescentes.
C) princípios das atividades de tratamento de dados pessoais.
D) requisitos para o tratamento de dados pessoais.
E) direitos do titular dos dados.

Questão 5

A análise de segurança física se inicia com a visita técnica nos ambientes onde são realizadas as atividades relacionadas direta ou indiretamente com os processos de negócio que estão sendo analisados. Esses ambientes devem ser observados com relação a diversos aspectos, sendo que a principal premissa para garantir o controle de acesso é:
A) Tudo é permitido, menos o que é expressamente proibido .
B) Liberar apenas o estritamente necessário para o uso do usuário.
C) Liberar tudo para o uso do usuário, mas com senha.
D) Tudo é proibido, desde que expressamente declarado.
E) Tudo é permitido, desde que expressamente declarado.

Questão 6

O avanço dos ataques cibernético s, que vitimam indivíduos, empresa s e países, é motivado por uma série de
fatores que tornam ainda mais desafiador o trabalho do profissional de segurança da informação. Ano: 2017 Banca: CIEE Órgão: TJ-DF T Prova: CIEE - 20 17 - TJ-DFT - (adaptada) É um tipo de código malicioso que torna inacessíveis os dados armazenados em um equipamento, geralmente usando criptografia, e que exige pagamento de resgate para restabelecer o acesso.

A) DDOS
B) Cavalo de Troia
C) Cookie
D) Ransonware
E) Spam

Questão 7

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 T I 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 control es e à política de segurança da informação de uma organização, análise:
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 d e 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) I, II e IV , apenas.
B) I, II, III e IV.
C) II, apenas.
D) II e III, apenas.

Questão 8

Um ataque só acontece porque vulnerabilidades são exploradas pelos atacantes. Temos que eliminar todos os pontos fracos de nosso ambiente, em todos os níveis. Analise as afirmativas dentre as principais vulnerabilidades que devem ser evitadas, e assinale a alternativa correta:

I. Falhas de Injeção

II. Autenticação quebrada

III. Exposição de dados sensívei s

Estão corretas as afirmativas:

A) Apenas I e III

B) Apenas II e III

C) Apenas I e II

D) Apenas I

E) I, II e II I

Questão 9

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 d a mensagem , mas sim de apenas ocultar o seu significado. Possuímos diversas propriedades fundamentais na segurança da informação Qual delas NÃO é baseada em métodos de criptografia?

A) Integridade.

B) Confidencialidade.

C) Disponibilidade.

D) Autenticidade.

E) Irretratabilidade.

Questão 10

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 d a mensagem , mas sim de apenas ocultar o seu significado. Um certificado digital é um arquivo de dados contendo segmentos ou seções que possuem informações obrigatórias e adicionais armazenadas em extensões. A utilização de certificados digitais permite que sejam agregados requisitos de segurança n a tramitação de informações. Dentre esses requisitos, está a garantia da impossibilidade de que o autor recuse a autoria . Esse é o requisito de:

A) privacidade.

B) não-repúdio.

C) autenticidade.

D) integridade.
E) sigilo.

Questão 11

Assinale a alternativa que identifica de forma correta, somente princípios relacionados de forma direta ao contexto d e segurança à interconexão dos sistemas.

A) Confiabilidade, integridade, disponibilidade, autenticação e repúdio.
B) Confidencialidade, integridade, disponibilidade, programação e configuração.
C) Confiabilidade, integridade, disponibilidade, autenticação e não repúdio.
D) Confidencialidade, integridade, disponibilidade, autenticação e configuração.
E) Confiabilidade, integridade, disponibilidade, autenticação e confidencialidade.

Questão 12

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 switch es WiFi serão mapeados nessa rede de visitantes que implementa:

A) um IDS .
B) um certificado digital .
C) um IPS
D) uma DMZ.
E) uma criptografia.

Questão 13

Para os desenvolvedores de aplicativos móveis há uma série de cuidados d e segurança e privacidade que precisam ser tomados para que vulnerabilidades não sejam introduzidas. Ano: 2019 Banca: UFMT Órgão: COREN-MT Prova: UFMT - 2019 - COREN- MT - adaptada Sobre segurança da informação a o utilizar dispositivos móveis, assinale a afirmativa correta.

A) Recomenda -se manter interfaces de comunicação, com o bluetooth, infravermelho e Wi-Fi sempre ativadas, mesmo quando não utilizadas.

B) Ao baixar e instalar aplicativos, é aconselhado obtê-los d e lojas oficiais ou de sites dos fabricantes.

C) Ao adquirir um dispositivo móvel usado, não é recomendado restaurar as configurações originais de fábrica.

D) Por se tratar de equipamentos de baixa vulnerabilidade, não é necessária a instalação de um programa antivírus.

E) Coloque sempre senhas fáceis de lembrar.

Questão 14

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 estimativa e o tratamento de riscos.

B) a identificação e a estimativa de riscos.

C) a comunicação e a avaliação de riscos.

D) a avaliação e o tratamento de riscos.

E) o tratamento e a aceitação de riscos.

Questão 15

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 ass inale 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) Criptografia
B) Política da Segurança
C) Segurança da Informação
D) Integridade
E) Disponibilidade

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. Técnico d e Nível Superior - Análise de Sistemas
https://www.qconcursos.com/questoes-de-concursos/disciplinas/tecnologia-da-informacao-seguranca-da-informacao/ataques-e-ameacas
Considere que um hacker comprometa milhares de hosts ao redor do mundo, criando uma botnet com intenção maliciosa. Em determinada ocasião , comandados por um computador mestre, estes hosts executam um ataque conjunto a um determinado servidor web ou DNS, consumindo a largura de banda do servidor e comprometendo seu funcionamento.
O cenário descrito é típico de um ataque denominado:
A) DoS.
B) worms.
C) phishing.
D) spoofing.
E) DDoS