Prova Segurança da Informação

Aluno(a).:____GABARITO P1_____27/04/2023

Professor.: Ronilson R. Pinho

1) Enumere as funções do Departamento de segurança de Informação de uma Empresa
criação, implementação, controle e monitoramento de políticas que almejam assegurar os ativos de informação
2) Conforme descrição feita pela ISO/IEC 17799, a proteção da Informação é vital, sendo caracterizada pela Trilogia CID. Descreva sucintamente a CID e os itens acrescentados pela Sêmola em 2003.
Confidencialidade
Garante que somente pessoas autorizadas poderão acessar as informações. Trata-se da não permissão da divulgação de uma informação sem prévia autorização.
• **Disponibilidade**
Garante acesso a uma informação no momento desejado. Isso implica no perfeito funcionamento da rede e do sistema. Imagine você necessitando de umas informações para concluir um relatório e o sistema não está funcionando!
• **Integridade**
Garante que a exatidão e completeza das informações não sejam alteradas ou violadas. Um exemplo, vamos supor que um gerente de uma empresa determina aumento de salário de 2% aos funcionários, para isso, utilizou seu e-mail para o departamento financeiro. Alguém interceptou e alterou de 2% para 20% o aumento
Legalidade: Garantia de que a informação foi produzida em conformidade com a lei;
Autenticidade: garantia de que num processo de comunicação os remetentes sejam exatamente o que dizem ser e que a mensagem ou informação não foi alterada após o seu envio ou validação.

3) As vulnerabilidades estão presentes no dia a dia das empresas e se apresentam nas mais diversas áreas de uma organização, a todo instante os negócios, seus processos e ativos físicos, tecnológicos e humanos são alvos de investidas de ameaças de toda ordem. Qual das opções abaixo descreve o melhor conceito de Vulnerabilidade na ótica da Segurança da Informação?

( ) Fragilidade presente ou associada a ativos que exploram ou processam informações.
( ) Impacto presente ou associada a ativos que manipulam ou processam informações.
( ) Fragilidade presente ou associada a ameaças que manipulam ou processam informações .
( ) Ameaça presente ou associada a ativos que manipulam ou processam informações.
(X) Fragilidade presente ou associada a ativos que manipulam ou processam informações.

4) Corrigir pontos vulneráveis ou pontos fracos que circulam em um setor que trabalha com a informação, não acabará, mas reduzirá em muito os riscos em que ela estará envolvida. Logo estará evitando como também prevenindo a concretização de possíveis ameaças. Baseado neste fato podemos denominar como Vulnerabilidade Física:

( ) Problemas nos equipamentos de apoio (acúmulo de poeira, aumento de umidade e de temperatura).

( ) Acessos não autorizados ou perda de comunicação e a ausência de sistemas de criptografia nas comunicações.
( ) Terrorismo ou vandalismo (ameaça de bomba, sabotagem, distúrbios civis, greves, roubo, furto, assalto, destruição de propriedades ou de dados, invasões, guerras, etc.).
(X) Instalações prediais fora dos padrões de engenharia e salas de servidores mal planejadas.
( ) Possibilidade de desastres naturais (incêndios, enchentes, terremotos, tempestades, falta de energia).

5) "Neste algoritmo, os dados são codificados em blocos de 64 bits usando uma chave de 56 *bits*. O algoritmo transforma a entrada de 64 *bits* em uma série de etapas em uma saída de 64 *bits*. As mesmas etapas, com a mesma chave, são empregadas para reverter a criptografia. Uma de suas desvantagens é que pode ser decifrado com a técnica de força bruta." As informações se referem ao seguinte tipo algoritmo de criptografia:

(X) DES
( ) AES
( ) RSA
( ) IDEA
( ) CAMELLIA

6) Computadores e redes de computadores sempre foram alvos de ataques, tais como os vírus, worms, entre outros, que tinham a finalidade de causar danos nas máquinas, ou para causar prejuízos ou apenas como diversão. Mas esse conceito tem mudado, a internet está sendo cada vez mais usada para fins lucrativos e maliciosos, como roubo de senhas, números de contas bancárias e de cartões de crédito, o que a torna bastante perigosa. Com relação aos tipos de ataques, julgue as afirmações abaixo:
I. Um ataque DoS (*Denial-of-Service*) torna uma rede, hospedeiro ou outra parte da infraestrutura inutilizável por usuários verdadeiros. A maioria dos ataques DoS na Internet pode ser dividida em três categorias: Ataque de vulnerabilidade, Inundação na largura de banda e Inundação na conexão.
II. Um ataque de Sniffing, ou ataque de Sniffer, são caracterizados pelo uso de ferramentas que rodam em Background e em modo promiscuo, ou seja, analisam todos os pacotes que estão trafegando pela rede no momento.
III. Os ataques do tipo *man-in-the-middle* (MITM) também são usados em sistemas de segurança baseados em token. Consistem em interceptar o tráfego entre dois computadores, e, para ambos, continuar parecendo que a comunicação é direta. Contudo, a entidade que intercepta o tráfego também o altera, de forma que a requisição de rede pareça original e autêntica.
É correto o que consta:

( ) na afirmativa I, apenas.
( ) na afirmativa II, apenas.
( ) na afirmativa III, apenas.
( ) nas afirmativas I e III, apenas.
(X) nas afirmativas I, II e III.

7) Diferencie Criptografia Simétrica da Assimétrica

Criptografia Simétrica	Criptografia assimétrica
Utiliza uma única chave para criptografar e descriptografar informações	Utiliza duas chaves diferentes para criptografar e descriptografar informações
Processo de criptografia mais rápido	Processo de criptografia mais lento
Chaves de 128 a 256 bits	Chaves de 2048 bits ou mais
Não utiliza muitos recursos	Utiliza mais recursos
O texto cifrado é menor ou do mesmo tamanho que o texto simples original	O texto cifrado é maior ou do mesmo tamanho que o texto cifrado original
Oferece autenticidade	Oferece autenticidade e irretratabilidade
Exemplo de algoritmos incluem AES, DES, 3DES, IDEA e Blowfish	Exemplo de algoritmos incluem RSA, ECC, DSA e El Gamal
Melhor para lidar com grandes quantidades de dados	Melhor para lidar com quantidades menores de dados
A chave pode ser roubada se não for armazenada de forma segura	A chave privada não pode ser recuperada se for perdida

8) Para verificar a autenticidade e a integridade de um certificado digital são usados os campos de Alternativas

(X) identificação e a assinatura digital da entidade (AC) que o emitiu.

( ) chave pública e chave privada do certificado.

( ) assinatura do emissor e do receptor do certificado.

( ) chave privada e *hash* do certificado.

( ) assinatura, período de validade e número de série do certificado.