SEGURANÇA INFORMÁTICA E DAS COMUNICAÇÕES

CAPÍTULO 1. FUNDAMENTOS DE SEGURANÇA DA INFORMAÇÃO

Exercícios Práticos – Capitulo 1

Esta ficha tem como o objectivo de consolidar todos os conceitos apreendidos nas aulas Teóricas.

1. Em relação à segurança da informação, é correcto afirmar que:

   Selecione a afirmação correcta:

   A) a confidencialidade é a garantia de que os dados chegarão exactamente como foram enviados.

   B) a integridade é a verificação da entidade ou do usuário emissor antes do acesso a um sistema computacional qualquer.

   C) os detectores de intrusão, *software* antivírus, firewalls e engenharia social fornecem segurança a um sistema corporativo.

   D) o hashing, dentre os controlos lógicos para a garantia da integridade da informação, é a comunicação sem alterações por intrusos.

   E) o Sistema de Gestão de Segurança da Informação é um modelo de abordagem à segurança independente de fabricantes que envolve temas, como telecomunicações, segurança e proteção do meio físico.

2. Sobre o princípio da autenticidade, pode-se afirmar que:

   Selecione a afirmação correcta:
   A) garante que apenas pessoas autorizadas terão acesso à informação.
   B) garante um tratamento igual entre todas as pessoas.
   C) garante que apenas pessoas autorizadas poderão alterar a informação.
   D) garante que a informação estará disponível sempre que um usuário autorizado quiser acede-la.
   E) garante a veracidade da autoria da informação, além de o não-repúdio.

3. Em aplicações que utilizam certificados digitais no padrão de uma PKI, é muito importante estabelecer a validade de um certificado digital. Sobre o tema, analise as afirmações abaixo e assinale a alternativa correcta.

   I. Qualquer certificado da PKI contém todas as informações necessárias para verificar a sua validade, não necessitando de quaisquer artefactos externos para ser validado.

   II. As autoridades certificadoras (CAs) publicam informações, periodicamente actualizadas, sobre a validade dos certificados que emitiram.

   III. Um dos critérios sobre a validade de um certificado é seu período de validade, composto por duas datas: inicial e final.

   IV. Uma etapa da validação é a conferência da validade de toda a cadeia de certificação, partindo da Autoridade Raiz, passando pelas Autoridades Certificadoras (CAs) até o certificado final.

   Selecione a afirmação correcta:

   A) Todas estão incorrectas;

B) Todas estão correctas;

C) Apenas I e III estão correctas;

D) Apenas II e IV estão correctas;

E) Apenas II, III e IV estão correctas.

4. A segurança de um sistema de computação pode ser expressa através de algumas propriedades fundamentais.

   Assinale a alternativa que indica corretamente a propriedade na qual todas as ações realizadas no sistema são conhecidas e não podem ser escondidas ou negadas por seus autores; esta propriedade também é conhecida como irrefutabilidade ou não-repúdio.

   Esta correcta a afirmação:

   A) Irretratabilidade

   B) Autenticidade

   C) Confidencialidade

   D) Disponibilidade

   E) Integridade

5. Escolha uma das opções e justifique. A criptografia é utilizada com o objectivo de aumentar alguns dos aspectos de segurança na transmissão da informação entre o transmissor e o destinatário. Por exemplo, a criptografia *Data Encryption Standard* (DES) tem como objectivo principal…

   a) Não-repúdio.
   b) Confidencialidade.
   c) Autenticação.
   d) Integridade.

6. Os certificados digitais estão sendo cada vez mais utilizados, tanto por pessoas físicas quanto jurídicas, como meios de garantir a autenticidade, confidencialidade e integridade das operações que são realizadas. Assinale a alternativa correta, a respeito dos certificados digitais.

   Esta correcta a afirmação:

   A) As operações realizadas com certificação digital pelas empresas são consideradas sempre como autênticas, pois envolve pelo menos uma pessoa jurídica. Já as operações realizadas com um certificado digital de pessoa física, só terá validade se uma das partes for uma pessoa jurídica;

   B) Qualquer operação feita com certificado digital poderá ser contestada, pois não é uma assinatura física;

   C) As operações realizadas com certificação digital não podem ser repudiadas;

   D) As operações realizadas com certificação digital só serão consideradas válidas se forem posteriormente firmadas em contrato físico.

7. Uma entidade P precisa fazer várias verificações para validar um certificado digital de uma entidade Q emitido por uma Autoridade Certificadora (AC). Uma verificação das mais importantes visa à integridade e à autenticidade do certificado digital da entidade Q. Para isso, a entidade P precisa ter:

   Alternativas

   A) a chave privada da AC que emitiu o certificado digital da entidade Q;

B) a chave privada e a lista de certificados revogados da AC que emitiu o certificado digital da entidade Q;

C) a chave pública da entidade Q e a lista de certificados revogados da AC que emitiu o certificado digital da entidade Q;

D) o certificado digital da AC que emitiu o certificado digital da entidade Q;

E) a chave pública da entidade Q e a chave privada da AC que emitiu o certificado digital da entidade Q.

8. Um analista entrou em um *site* e desejava saber se este utilizava conexão segura. Para isto clicou em um ícone de cadeado ao lado da URL no navegador, a partir do qual obteve informações sobre:

Selecione a afirmação correcta:

A) a assinatura digital, tais como chave pública, chave privada e autorização de acesso;

B) o certificado digital, tais como chave secreta, hash público e período de validade;

C) a assinatura eletrônica, tais como assinaturas digitais, contraprova e autorização de acesso;

D) o hash criptográfico, tais como validade do certificado digital, redirecionamentos seguros e hash público.

E) o certificado digital, tais como emissão (para e por quem), período de validade e assinaturas digitais;

9. O auditor Gerson recebeu o arquivo AnexoJ em formato digital. Antes de proceder com a abertura do AnexoJ, Gerson determinou a fidedignidade do referido arquivo, avaliando a conformidade dos dados do AnexoJ por ele recebido com os dados do AnexoJ transmitido pelo emissor.

Essa avaliação feita por Gerson em AnexoJ está directamente relacionada com o seguinte princípio da segurança de informações:

Selecione a afirmação correcta:

A) integridade;

B) confidencialidade;

C) autenticidade;

D) disponibilidade;

E) não-repudio.

10. O certificado digital de um site é …

A) um código de 12 *bits* que garante a segurança de um *site* na internet;

B) D) um arquivo digital que contém informações sobre uma entidade de confiança, como uma empresa ou um indivíduo;

B) uma senha privada emitida por uma autoridade de certificação (CA), que protege o acesso a um site ou aplicativo;

C) um dispositivo físico (*token*) que protege o acesso a um site ou aplicativo;

E) um *software* que protege o acesso ao sistema operativo de um computador.

11. Uma infra-estrutura de chave pública (PKI) é frequentemente gerida por uma autoridade independente e confiável. Indique e descreva a entidade mais importante da infra-estrutura de chave pública?

12. Nos meios eletrônicos, ainda não existe recurso de segurança que consiga ser mais viável do que as senhas (*password*). Os bancos, cartões de crédito, contas de *e-mail*, redes sociais e lojas *on-line* estão entre as numerosas aplicações que dependem dessas combinações.

    Quais são os golpes mais frequentes relacionados com e-mails ou páginas de internet falsas?

13. A função *Hash* é qualquer algoritmo que mapeie dados grandes e de tamanho variável para pequenos dados de tamanho fixo. Por esse motivo, as funções *Hash* são conhecidas por resumirem os dados.

    a) Para ter utilidade criptográfica, quais são as características que a função de *hashing* deve ter?

    b) Quais são os princípios deste algoritmo?

Bom Trabalho!