

PROVA DISCURSIVA

- Nesta prova, faça o que se pede, utilizando, caso deseje, o espaço para rascunho indicado no presente caderno. Em seguida, transcreva o texto para a **FOLHA DE TEXTO DEFINITIVO DA PROVA DISCURSIVA**, no local apropriado, pois **não será avaliado fragmento de texto escrito em local indevido**.
- Qualquer fragmento de texto que ultrapassar a extensão máxima de linhas disponibilizadas será desconsiderado.
- Na **Folha de Texto Definitivo**, identifique-se apenas no cabeçalho da primeira página, pois **não será avaliado** texto que tenha qualquer assinatura ou marca identificadora fora do local apropriado.
- Ao domínio do conteúdo serão atribuídos até **40,00 pontos**, dos quais até **2,00 pontos** serão atribuídos ao quesito apresentação (legibilidade, respeito às margens e indicação de parágrafos) e estrutura textual (organização das ideias em texto estruturado).

A Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) é uma cadeia hierárquica de confiança que viabiliza a emissão de certificados digitais para identificação virtual do cidadão. O modelo adotado pelo Brasil foi o de certificação com raiz única, e o Instituto de Tecnologia da Informação (ITI), além de desempenhar o papel de Autoridade Certificadora Raiz (AC-Raiz), também credencia e descredencia os demais participantes da cadeia e supervisiona e faz auditoria dos processos.

Na prática, o certificado digital ICP-Brasil funciona como uma identidade virtual que permite a identificação segura e inequívoca do autor de uma mensagem ou de uma transação feita em meios eletrônicos, como a Web. Esse documento eletrônico é gerado e assinado por uma terceira parte confiável, ou seja, uma autoridade certificadora que, seguindo regras estabelecidas pelo Comitê Gestor da ICP-Brasil, associa uma entidade (pessoa, processo, servidor) a um par de chaves criptográficas.

O certificado digital da ICP-Brasil, além de personificar o cidadão na rede mundial de computadores, garante, por força da legislação atual, validade jurídica aos atos praticados mediante o seu uso. A certificação digital é uma ferramenta que permite que aplicações como comércio eletrônico, assinatura de contratos digitais, operações bancárias virtuais, iniciativas de governo eletrônico, entre outras, sejam realizadas. São transações feitas de forma virtual, ou seja, sem a presença física do interessado, mas que demandam identificação clara da pessoa que as realiza pela Internet.

Internet: <www.iti.gov.br> (com adaptações).

Considere a seguinte situação hipotética.

Na realização de uma auditoria em um sistema *web* de oferta de prestação de serviços de informação para os cidadãos de uma prefeitura, constatou-se o uso de certificado digital emitido por órgão não oficial ou autoridade não acreditada. Na ocasião, um navegador do tipo Firefox atualizado em relação ao uso do certificado identificou alguns problemas gerais, entre eles:

- autoridade certificadora não válida;
- prazo do certificado expirado havia pelo menos dois anos;
- uso da função resumo MD5 na técnica de assinatura digital;
- nome do sítio no certificado não correspondente ao nome DNS do sítio em uso.

Tendo o texto inicial como meramente motivador e considerando a situação hipotética apresentada, discorra sobre as consequências de cada um dos problemas citados para o sistema da prefeitura em relação ao uso de certificados digitais [**valor: 28,00 pontos**] e proponha uma solução que possa ser adotada pela prefeitura para saná-los [**valor: 10,00 pontos**].

RASCUNHO

1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	
17	
18	
19	
20	