

PREFEITURA MUNICIPAL DE JOÃO PESSOA
CONTROLADORIA-GERAL DO MUNICÍPIO DE JOÃO PESSOA
CARGO 3: AUDITOR MUNICIPAL DE CONTROLE INTERNO –
ÁREA: TECNOLOGIA DA INFORMAÇÃO – CAMPO DE ATUAÇÃO:
DESENVOLVIMENTO DE SISTEMAS
PROVA DISCURSIVA

Aplicação: 28/1/2018

PADRÃO DE RESPOSTA DEFINITIVO

Autoridade certificadora não válida: é um tipo de erro relacionado a certificados digitais emitidos por autoridade certificadora que não é confiável pelo navegador na sua cadeia de certificação. A assinatura digital da autoridade certificadora que emitiu o certificado pode não ser verificada corretamente para evitar problemas na comunicação com o navegador. Prazo do certificado expirado havia pelo menos dois anos: o prazo de uso do certificado já não é mais válido dentro do limite de tempo estabelecido para o certificado em questão. As transações realizadas com esse certificado não podem ser consideradas válidas do ponto de vista de auditoria de validade do tempo, já que o certificado previa seu uso somente até uma determinada data.

Uso da função resumo MD5 na técnica de assinatura digital: a função de *hash* do certificado utiliza um padrão já não considerado seguro e que permite colisão de dados em determinados casos. O MD5 é uma função de resumo de mensagem que verifica a integridade de determinado dado. **Como alternativa, é possível o uso de algoritmos como o SHA2 ou o SHA512.**

Nome do sítio no certificado não correspondente ao nome DNS do sítio em uso: o certificado emitido não equivale ao seu nome correspondente no DNS, de tal forma que a URL do sítio não é confiável ou a URL constante no certificado não é confiável.

De maneira geral, a prefeitura necessita estabelecer processos de controle, de emissão e de revogação de certificados digitais oriundos de autoridades certificadoras confiáveis para seus serviços de Internet. Esse tipo de controle parte do pressuposto que a prefeitura controla seus sítios na Internet e mantém seus processos de certificação digital sob controle de validade e revogação, dando garantias de uso de seus serviços digitais aos cidadãos.