

RESOLUÇÃO Nº 69, DE 13 DE OUTUBRO DE 2009.

APROVA A VERSÃO 1.1 DOS DOCUMENTOS QUE REGULAMENTAM A GERAÇÃO E USO DE CARIMBO DO TEMPO NO ÂMBITO DA INFRA-ESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA ICP-BRASIL: DOC-ICP-11, DOC-ICP-12, DOC-ICP-13 E DOC-ICP-14.

O SECRETÁRIO EXECUTIVO DO COMITÊ GESTOR DA INFRA-ESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA – ICP-BRASIL, no exercício do cargo do referido Comitê, no uso das atribuições legais previstas nos incisos I, V e VI do art. 4º da Medida Provisória nº 2.200-2, de 24 de agosto de 2001,

CONSIDERANDO o Decreto nº 6.605, de 14 de outubro de 2008, que dispõe sobre o Comitê Gestor da Infra-Estrutura de Chaves Públicas Brasileira – CG ICP-Brasil e fixa a competência, prevista no § 6º art. 2º, do Secretário Executivo para coordená-lo na hipótese de ausência do Coordenador titular e suplente; e

CONSIDERANDO a necessidade de revisão dos normativos relacionados ao Sistema de Carimbo de Tempo da ICP-Brasil;

RESOLVE:

Art. 1º Ao item 3.2.1 do DOC-ICP-11, versão 1.0, acrescenta-se a alínea “i” com a redação que segue:

- i) dispor no mínimo de duas linhas de comunicação com a Internet, providas por diferentes sistemas autônomos (AS).

Art. 2º O item 6 do DOC-ICP-11, versão 1.0, passa a integrar o Glossário ICP-Brasil.

Art. 3º Todas as demais cláusulas do DOC-ICP-11, versão 1.0, em sua ordem originária, integram a presente versão 1.1 e mantêm-se válidas.

Art. 4º O item 6.10.1 do DOC-ICP-12, versão 1.0, passa a vigorar com a seguinte redação:

6.10.1 Diretrizes Gerais

6.10.1.1 Neste item da DPCT devem ser descritos os controles relativos à segurança da rede da ACT responsável, incluindo *firewall* e recursos similares, observado o disposto no item 9.3.3 da POLÍTICA DE SEGURANÇA DA ICP-BRASIL [4].

6.10.1.2 Todos os servidores e elementos de infra-estrutura e proteção de rede, tais como: roteadores, *hubs*, *switches*, *firewall* e sistemas de detecção de intrusão (IDS), localizados no segmento de rede que hospeda os SCT, deverão estar localizados e operar em ambiente de, no mínimo, nível 3.

6.10.1.3 As versões mais recentes dos sistemas operacionais e dos aplicativos servidores, bem como as eventuais correções (*patches*), disponibilizadas pelos respectivos fabricantes deverão ser implantadas imediatamente após testes em ambiente de desenvolvimento ou homologação.

6.10.1.4 O acesso lógico aos elementos de infra-estrutura e proteção de rede deverá ser restrito, por meio de sistema de autenticação e autorização de acesso. Os roteadores conectados a redes externas deverão implementar filtros de pacotes de dados, que permitam somente as conexões aos serviços e servidores previamente definidos como passíveis de acesso externo.

- 6.10.1.5 O acesso à Internet deverá ser provido por no mínimo duas linhas de comunicação de sistemas autônomos (AS) distintos.
- 6.10.1.6 O acesso via rede aos SCTs e sistemas de gestão da ACT deverá ser permitido somente para os seguintes serviços:
- pela EAT da ICP-Brasil, para o sincronismo e auditoria de relógios dos SCTs;
 - pela ACT, para a administração dos SCTs e sistemas de gestão a partir de equipamento conectado por rede interna ou por VPN estabelecida mediante endereçamento IP fixo previamente cadastrado junto à EAT;
 - pelo PSS da ACT, para a administração dos SCTs e sistemas de gestão a partir de equipamento conectado por rede interna ou por VPN estabelecida mediante endereçamento IP fixo previamente cadastrado junto à EAT;
 - pelo subscritor, para a solicitação e recebimento de carimbos do tempo.

Art. 5º Acrescenta-se o item 6.10.5.3 ao DOC-ICP-12 com a redação que segue:

6.10.5.3 Os relógios dos SCTs devem estar protegidos contra ataques, incluindo violações e imprecisões causadas por sinais elétricos ou sinais de rádio, para evitar que sejam descalibrados. Qualquer modificação ocorrida nestes relógios deverá ser registrada e detectada.

Art. 6º O item 11 do DOC-ICP-12, versão 1.0, passa a integrar o Glossário ICP-Brasil.

Art. 7º Todas as demais cláusulas do DOC-ICP-12, versão 1.0, em sua ordem originária, integram a presente versão 1.1 e mantêm-se válidas.

Art. 8º O item 6 do DOC-ICP-13, versão 1.0, passa a integrar o Glossário ICP-Brasil.

Art. 9º Todas as demais cláusulas do DOC-ICP-13, versão 1.0, em sua ordem originária, integram a presente versão 1.1 e mantêm-se válidas.

Art. 10º O item 2.2 do DOC-ICP-14, versão 1.0, passa a vigorar com a seguinte redação:

2.2 Procedimentos da AC Raiz

2.2.1 Nesta seção são apresentados os procedimentos realizados pela AC Raiz para a auditoria e sincronismo dos relógios dos SCTs.

2.2.2 A AC Raiz disponibilizará às ACTs cópia dos certificados digitais de seus SAS, para permitir a autenticação mútua SAS-SCT.

2.2.3 Após a colocação do SCT em operação, a AC Raiz deverá:

- auditar periodicamente o relógio dos SCTs, em período tal que o erro máximo acumulado não ultrapasse o valor especificado na PCT correspondente;
- emitir alvarás, respeitando o período descrito no item a) habilitando o funcionamento dos SCTs;
- informar à ACT, através de mensagem eletrônica, o motivo da impossibilidade da emissão de um alvará para um SCT;
- analisar e emitir relatórios dos registros de auditoria e sincronismo do relógio do SCT, usando os dados registrados no SAS;
- pelo menos 2 (dois) dias úteis antes da expiração do certificado do SAS, providenciar novo certificado e disponibilizá-lo às ACTs.

Art. 11º O item 2.3.2 do DOC-ICP-14, versão 1.0, passa a vigorar com a seguinte redação:

2.3.2 Antes de colocar em operação seus SCTs, a ACT deve:

- solicitar os serviços da Rede de Carimbo do Tempo da ICP-Brasil para cada relógio de SCT que emita carimbos de tempo no âmbito da ICP-Brasil;

- b) contratar o fornecimento dos meios de comunicação e dos equipamentos necessários para ligar seus SCTs à rede Rede de Carimbo do Tempo da ICP-Brasil;
- c) utilizar somente equipamentos homologados pela ICP-Brasil ou por entidades por ela autorizadas;
- d) enviar à AC Raiz cópia dos certificados digitais de seus SCTs, para permitir a autenticação mútua SAS-SCT.

Art. 12º O item 3 do DOC-ICP-14, versão 1.0, passa a vigorar com a seguinte redação:

3. REQUISITOS OPERACIONAIS

Esta seção trata do conteúdo dos arquivos que serão gerados durante as auditorias na Rede de Carimbo do Tempo da ICP-Brasil

3.1 Arquivos Gerados nas Auditorias

As operações de autenticação mútua e sincronismo gerarão arquivos codificados em UTF-8 (ou ASCII) nos SASs e SCTs, contendo dados resultantes destas operações.

3.1.1 Dados Referentes à Autenticação Mútua

3.1.1.1 Os arquivos de registro do SAS devem conter no mínimo as seguintes informações:

- a) data e hora de realização da autenticação;
- b) endereço de rede do SAS;
- c) endereço de rede do SCT;
- d) identificação do certificado digital do SCT;
- e) identificação do alvará;
- f) mensagem de aviso ou de erro.

3.1.1.2 Os arquivos de registro do SCT devem conter as seguintes informações:

- a) data e hora de realização da autenticação;
- b) endereço de rede do SAS;
- c) endereço de rede do SCT;
- d) identificação do certificado digital do SAS;
- e) identificação do alvará;
- f) mensagem de aviso ou de erro.

3.1.2 Dados Referentes ao Sincronismo

3.1.2.1 Os arquivos de registro do SAS e do SCT devem conter no mínimo as seguintes informações:

- a) data e hora de realização do sincronismo;
- b) erro do relógio do SCT;
- c) retardo;
- d) endereço de rede do SAS;
- e) endereço de rede do SCT.

Art. 13º O item 6 do DOC-ICP-14, versão 1.0, passa a integrar o Glossário ICP-Brasil.

Art. 14º Todas as demais cláusulas do DOC-ICP-14, versão 1.0, em sua ordem originária, integram a presente versão 1.1 e mantêm-se válidas.

Art. 15º Esta Resolução entra em vigor na data de sua publicação.

RENATO DA SILVEIRA MARTINI