PRESIDÊNCIA DA REPÚBLICA
CASA CIVIL
INFRAESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA
COMITÊ GESTOR

ATA DA REUNIÃO ORDINÁRIA DO COMITÊ GESTOR DA ICP-BRASIL, EM 09 DE DEZEMBRO DE 2015.

Aos nove dias do mês de dezembro do ano de 2015, nas dependências da sala de reuniões do Instituto Nacional de Tecnologia da Informação – ITI, situado no endereço SCN Qd. 02 Bl. E, na cidade de Brasília/DF, com horário de início às 14h30, reuniram-se os membros Titulares e Suplentes do Comitê Gestor da ICP-Brasil – CG ICP-Brasil, servidores do Instituto Nacional de Tecnologia da Informação – ITI, representantes por procuração e alguns ouvintes para participar da Reunião ordinária do Comitê Gestor da ICP-Brasil. Estavam presentes: Renato da Silveira Martini (Secretário-Executivo do CG ICP-Brasil), Maurício Augusto Coelho (Diretor da DINFRA/ITI – Diretoria de Infraestrutura de Chaves Públicas do ITI), Adriana Fetter Dias da Costa (Chefe de Gabinete do ITI/PR), Pedro Paulo Lemos Machado (Diretor da DAFN/ITI – Diretoria de Auditoria, Fiscalização e Normalização do ITI), André Pinto Garcia (Procurador-Chefe da Procuradoria Especializada do ITI), Fernando Nascimento Barbosa (Titular do Ministério da Fazenda – MF), Fernando Antônio Braga da Siqueira Júnior (Titular do Ministério do Planejamento, Orçamento e Gestão – MPOG), Júlio César Rogério Cosentino (Titular da ANCD – Associação Nacional de Certificação Digital), Nivaldo Cleto (Titular da AARB – Associação das Autoridades de Registro do Brasil), Manuel Dantas Matos (Titular da Camara-e.Net), Marcos Vinícius Amorim Ferreira Guimarães (Suplente do Ministério da Ciência, Tecnologia e Inovação), Paulo Lício de Geus (representante por procuração da Sociedade Brasileira de Computação – SBC), Patrícia Paiva (Suplente da Camara-e.Net), Antônio Sérgio Borba Cangiano (Suplente da ANCD – Associação Nacional de Certificação Digital), João Rufino (Representante por procuração do GSI/PR-Gabinete de Segurança Institucional), Marcelo de A. Maymore (Representante por procuração do GSI/PR-Gabinete de Segurança Institucional), Wander Blanco Nunes (Membro da COTEC pelo Ministério da Fazenda), Patrícia Leite (Membro da COTEC pela Camara-e.Net), Eduardo de Magalhães Lacerda (Assessor Especial do Diretor Presidente do ITI), Ruy César Ramos Filho (Assessor da Diretoria de Infraestrutura de Chaves Públicas do ITI), Edmar da Silva Araújo (Assessoria de Comunicação do ITI), Alexandre Menezes Ribeiro (Coordenador-Geral da Auditoria e Fiscalização do ITI, Substituto), Wilson Roberto Hirata (Coordenador-Geral de Normalização e Pesquisa do ITI), José Rodrigues Gonçalves Júnior (Coordenador-Geral de Segurança da Informação do ITI),

André Machado Caricatti (Coordenador-Geral de Operações do ITI), Angela Maia (Ouvinte da SAFEWEB), Luiz Zancanella Júnior (Ouvinte da SAFEWEB), Marta Santos (Ouvinte da CNDL), Eduardo Oliveira (Ouvinte da CNDL), Marcia R. Moratona (Ouvinte da BVS), Rodrigo Guimarães (Ouvinte da Camara-e.Net), Francisco (Ouvinte da Serasa), André (Ouvinte da Serasa), Vinicius (Ouvinte da Soluti), conforme lista de presença, para tratar da pauta a seguir:

PAUTA

1. Regulamentação de prazo diferenciado para LCRs de certificados da AC Raiz revogados;
2. Prazo para a AC Raiz revogar certificado de AC de nível imediatamente subsequente;
3. Aprovar os Relatórios de Auditoria da AC Raiz;
4. Atualizar o normativo referente às obrigações de repositórios de ACs;
5. Retirar o campo AIA das LCRs da ICP-Brasil;
6. Emissão da Cadeia V5 da AC Raiz da ICP-Brasil.

Iniciada a reunião Dr. Renato Martini deu boas vindas a todos e comunicou que esta é a última reunião do ano.

Propôs inversão de pauta, começando com o item 3, para aprovar os Relatórios de Auditoria da AC Raiz, passando a palavra para o Gonçalves que fez uma apresentação sobre o assunto. Expôs que o relatório é sigiloso, mas que, evidentemente, poderia se prover vistas ao relatório aos membros do Comitê Gestor interessados. Gonçalves fez um resumo do relatório para apresentação aos presentes. Destacou que além da conformidade aos normativos da ICP-Brasil, buscou-se também conformidade às normativas Webtrust, para que os certificados raízes da ICP-Brasil possam integrar com maior facilidade os repositórios dos browsers (navegadores). Foi realizada licitação sendo vencedora a *Ernest Young*. O edital previa auditoria nos 12 meses imediatamente anteriores a assinatura do contrato e, caso necessário, período anterior a este prazo inicial seria também auditado. Foi encontrada apenas uma não conformidade, já tratada, e sugerida uma possibilidade de melhoria no sistema de gerenciamento de certificado *Ywapa. D*iante do quadro de aplicação de conceito da *Ernest Young* a avaliação a ICP-Brasil foi 2, aceitável.

Após apresentação, Dr. Maurício falou do trabalho exitoso da ICP-Brasil, desde a última auditoria para esta, e que as auditorias serão realizadas anualmente. Professor Paulo Lício perguntou o que falta para os certificados da ICP-Brasil serem aceitos no *browsers*. Dr. Maurício respondeu que, de

forma geral, o requisito principal é ter relatórios anuais de auditoria que demonstrem conformidade aos requisitos *Webtrust*. Por vezes, porém, requisitos específicos são apresentados. Falou do caso com a *Mozilla,* que tem um entendimento diferenciado das outras empresas como *Microsoft e Adobe,* por exemplo. A *Mozillla* não quer incluir a raiz, mas sim todas as ACs emissoras de certificados de usuários finais. Dr. Renato complementou que o modelo da *Mozilla* é diferente, não seguem as orientações padrões. Como trata-se de uma fundação privada, segue seus próprios requisitos. A *Mozilla* cobra por AC inserida, por exemplo. Professor Lício pergunta ainda se a auditoria é só sobre documentos. Gonçalves respondeu que a auditoria é sobre documentos e processos. Que o apontamento da auditoria era no sentido de um melhor registro dos procedimento sem conformidade com o manual. O Conselheiro Manuel Matos registrou o agradecimento ao Gonçalves pelo atendimento que teve no dia anterior pelo mesmo, destacando que o controle está rigorosamente rígido e adequado as expectativas do Comitê Gestor. Dr. Renato salientou a importância do trabalho de uma auditoria para melhoria contínua dos processos. Dr. Maurício propôs que a aprovação dos relatórios de auditoria da AC Raiz se dessem sempre por meio de resolução do CG ICP-Brasil, Portanto, se acatada a proposta, o CG ICP-Brasil editaria uma resolução para aprovar esta auditoria. Dr. Pedro Paulo informou a necessidade de uma auditoria independente para a AC-Raiz. O Conselheiro Nivaldo Cleto, acrescentou a importância da AC-Raiz ser auditada por uma empresa deste porte, ratificando as palavras do Conselheiro Manuel Matos. Aprovado o relatório de auditoria por unanimidade.

Item de pauta 1. Regulamentação de prazo diferenciado para LCRs de certificados da AC Raiz revogados

André Caricatti apresentou o tema, fazendo a síntese do problema: "As LCRs da AC Raiz, embora geradas periodicamente, podem ser emitidas em razão de situações extraordinárias, como quando da revogação de certificados de AC de 1º nível. Notadamente, estes períodos podem ser adequados para atender ao agendamento de cerimônias, pois a presença de detentores externos ao ITI muitas vezes exige tal flexibilidade. Os normativos determinam a publicação de LCR em intervalos de tempo fixos e, à exceção dos casos que envolvam revogação de certificados, não consideram as eventuais alterações de prazo. Por fim, ao revogar um certificado da própria AC Raiz, deve-se emitir apenas uma última LCR, pois nas demais emissões a Lista será assinada com um certificado já revogado." Por fim, falou das alterações propostas, tendo como texto atual "4.4.9. Frequência de emissão de LCR: A LCR da AC Raiz é atualizada a cada 90 (noventa) dias. Em caso de revogação de certificado de AC de nível imediatamente ao seu, a AC Raiz emite nova LCR no prazo previsto no item 4.4.3 e notifica todas as ACs de nível imediatamente subsequente ao seu". E o texto proposto "4.4.9.

Frequência de emissão de LCR: A LCR da AC Raiz é atualizada, no máximo, a cada 90 (noventa) dias. Em caso de revogação de certificado de AC de nível imediatamente ao seu, a AC Raiz emite nova LCR no prazo previsto no item 4.4.3 e notifica todas as ACs de nível imediatamente subsequente ao seu. Quando da revogação de certificado da própria AC Raiz, deverá ser emitida LCR com período de validade igual ao do certificado revogado, encerrando a emissão de LCR por esta Autoridade Certificadora." Dr. Renato perguntou se há aprovação das medidas, sendo as mesmas aprovadas por unanimidade.

Os itens de pauta 4. Atualizar o normativo referente às obrigações de repositórios de ACs e 5. Retirar o campo AIA das LCRs da ICP-Brasil foram tratados em bloco.

Quanto ao item 4.Atualizar o normativo referente às obrigações de repositórios de ACs, o ITI recebeu uma sugestão da ANCD se manifestando negativamente sobre o fim de um 3º repositório de LCRs na AC Raiz. Gonçalves apresentou o tema fazendo uma síntese do problema: "Atualmente constam nos certificados emitidos na ICP-Brasil 03 (três) repositórios (URLs) de LCRs, sendo os 02 (dois) primeiros na infraestrutura da própria AC emitente do certificado e um terceiro na AC Raiz. Os normativos atuais não especificam a utilização desses três repositórios, de forma que se faz necessária a atualização das normas. A qualidade da infraestrutura de repositórios das ACs para a disponibilização de LCRs não justifica, atualmente, um terceiro ponto de distribuição de LCRs de ACs na AC Raiz e, além disso, uma eventual indisponibilidade na AC implica, consequentemente, na impossibilidade de atualização de suas LCRs no repositório da AC Raiz, uma vez que estas são copiadas a partir dos pontos de distribuição da respectiva AC." Apresentou ainda as soluções e providências contidas no ato normativo. "No DOC-ICP-5, em seu item 2.6.4, constam os requisitos aplicáveis aos repositórios utilizados pela AC. No DOC-ICP-4, em seu item 7.1.2.2, alínea 'd', consta a obrigatoriedade do endereço Web onde se obtém a LCR respectiva de cada certificado emitido. Assim, sugere-se a inserção da obrigatoriedade de dois repositórios, em infraestruturas de rede segregadas, para distribuição de LCRs pelas ACs em um subitem (2.6.4.1) do DOC-ICP-05; a previsão de dois endereços Web para obtenção de LCRs na alínea 'd' do item 7.1.2.2. do DOC-ICP-04 e, para que não haja impacto imediato nas atuais Políticas de Certificados, as ACs devem proceder as adequações necessárias para os certificados a serem emitidos sob a nova cadeia de certificação, cuja emissão da raiz (v5) está prevista para março/2015." Texto proposto:

"DOC-ICP-5:

2.6.4. Repositórios
Neste item devem ser descritos os requisitos aplicáveis aos repositórios utilizados pela AC responsável pela DPC, tais como:

a) localizações **física e** lógica;

b) disponibilidade;

c) protocolos de acesso; e

d) requisitos de segurança.

2.6.4.1 A AC responsável deve disponibilizar 02 (dois) repositórios, em infraestruturas de rede segregadas, para distribuição de LCRs.

DOC-ICP-4:

"7.1.2.2. A ICP-Brasil define como obrigatórias as seguintes extensões:
...
d) "CRL Distribution Points", não crítica: deve conter 02 (dois) endereços na Web onde se obtém a LCR correspondente;"

Diante do exposto chegamos a conclusão que o 3º repositório traz mais problemas do que benefícios. É responsabilidade das ACs apresentar 2 repositórios segregados. Dr. Maurício esclareceu que esta prática já está estabelecida pelas ACs. O 3º repositório (AC Raiz) continuará operacional até que todos certificados de usuários finais expirem. O Conselheiro Júlio Cosentino falou que o terceiro repositório cumpriu o seu papel, que é prudente analisar com mais detalhe a sua extinção. Dr. Renato falou que a filosofia do PKI é que a AC é responsável por sua LCR, numa emergência foi disponibilizado um terceiro, que é copiado e armazenado pela AC-Raiz. Manuel Matos falou que a análise feita na Câmara-e.net foi política, de que não é fatal para o ITI a manutenção do 3º repositório, perceberam que será mais prejudicial a retirada deste repositório do que mantê-lo, portanto o voto da Camara-e.net é pela regularização do mesmo e uma resolução para essa manutenção.

Dr. Renato, como proposta de encaminhamento, colocou o item 5 (Retirar o campo AIA das LCRs da ICP-Brasil) em aprovação. Os conselheiros do CGICP-Brasil manifestaram pela sua aprovação unânime. Quanto ao item 4 (Atualizar o normativo referentes às obrigações de repositórios de ACs), Dr. Renato falou que o tema fere um pouco o desenho do que é uma PKI, mas o tema não é polêmico para o ITI, então pode-se estudar aqui no comitê a proposta do Conselheiro Manuel Matos. "Não se trata de uma contextualização técnica, nem jurídica, mas de credibilidade da ICP-Brasil, que se mantém por sua confiabilidade." Dr. Maurício acrescentou que a confiabilidade do sistema corre risco, uma vez que há um interregno de tempo diferencial entre a disponibilização das LCRs pelas ACs e a disponibilização das mesmas no 3º repositório (AC-Raiz). O ideal seria adoção de OCSP pelas ACs da ICP-Brasil, assunto a ser discutido em grupo de trabalho na COTEC. Gonçalves falou que esse repositório consome mais recursos do que a manutenção de nossa própria LCR, que um ataque a esse 3º repositório poderia ser mais prejudicial para a credibilidade da ICP-Brasil do que a

extinção dele. Júlio Cosentino sugeriu mais tempo para estudar esse item, para detalhar esse quesito. Dr. Renato perguntou ao Conselheiro Manuel Matos que se colocou favorável a essa proposta de estudo mais detalhado. Professor Paulo falou que manter o 3º repositório vai contra todos os princípios de segurança da AC Raiz, colocando que já houve ataques dessa natureza mundo afora, e que a grande massa de clientes jamais chegam perto das raízes, que devem ser tratados pelos espelhos das raízes, para resguardar as raízes. Não é o caso aqui, mas o conceito de servidores de raiz deve ser preservado de ataques, como os do início dos anos 2000 e 2007. Este ano teve mais um, e tecnicamente ele recomenda blindar a raiz de todas as formas possíveis. Dr. Renato explicou que ele é um facilitador do debate e faz os encaminhamentos. O Conselheiro Manuel Matos falou inicialmente de consolidar o 3º repositório e acha pertinente estudar e retornar o tema numa próxima reunião. O Conselheiro Júlio Cosentino solicitou um tempo para estudar o assunto, falou ainda que tem janeiro e fevereiro para retomarmos esse tema. Conselheiro Fernando falou que temos aqui uma questão de ordem política e questão de ordem técnica, se fosse deliberar hoje ele deliberaria pela exclusão do 3º repositório, mas ouvindo o conselheiro Manuel Matos, sugere estabelecer uma política de comunicação para a exclusão do repositório. Dr. Renato concluiu que o Comitê decidiu por retomar o assunto para uma avaliação melhor antes da emissão de um novo certificado raiz (v5).

Item de pauta 6. Emissão da Cadeia V5 da AC Raiz da ICP-Brasil

Dr. Maurício apresentou a necessidade da AC Raiz emitir uma nova cadeia de certificação na primeira semana de março de 2016. Conforme demandam os normativos da ICP-Brasil, apresentou proposta de resolução que promove ajustes à DPC da AC Raiz para contemplar a nova raiz v5. O comitê aprovou por unanimidade.

Item de pauta 2. Prazo para a AC Raiz revogar certificado de AC de nível imediatamente subsequente;

Dr. Maurício chamou atenção para a necessidade de se analisar de forma mais atenta o pedido de revogação de um certificado de AC. Há casos críticos que demandam revogação o mais rapidamente possível (comprometimento de chave, por exemplo), e os não críticos (algum erro de codificação, por exemplo), cujo prazo de atual de 02 horas não é factível, nem recomendável. Apresentou proposta de atualização do texto com a diferenciação de caso crítico ou não, com prazos diferenciados para a revogação por parte da AC Raiz. Não havendo criticidade, o prazo para revogação seria mais amplo. Proposta aprovada por unanimidade.

Temas gerais

O conselheiro Nivaldo falou que os cartórios e juntas comerciais estão aceitando contratos 100% digitais, porém, como vamos conferir o documento original? Sugeriu uma resolução para regulamentar o pleito. Dr. Renato respondeu que já existe um grupo estudando isso na COTEC, com a coordenação do Hirata, mas é importante termos claro a governança do ITI e da ICP-Brasil em relação às juntas comerciais. Pode haver um canal de comunicação e o Sr. Nivaldo Cleto pode nos ajudar nisso a título de cooperação, como se faz em outras áreas como o Conselho Federal de Medicina. Hirata falou que o grupo recebeu indicação de 3 membros para sua composição. Nivaldo se coloca no grupo. Dr. Maurício pede a indicação formal por e-mail ao CGICP-Brasil. Júlio Cosentino acrescenta que é uma questão de aculturamento. Manuel Matos falou que os cartórios estão regulamentados, o fórum é dos tribunais de justiça e suas corregedorias, acho que se limita apenas as juntas comerciais. Os cartórios participaram ativamente dos grupos de Xades, Pades. Dr. Pedro Paulo falou dos portais de assinatura hoje vigentes tem a assinatura ICP-Brasil, um selo nosso, o reconhecimento jurídico que a ICP-Brasil confere. Dr. Renato falou que podemos influenciar mas não podemos determinar, o ITI está a disposição para cooperar.

Então, deu por encerrada a reunião, agradecendo a presença de todos.

RENATO DA SILVEIRA MARTINI
Secretário-Executivo do CG ICP-Brasil
Instituto Nacional de Tecnologia da Informação