COMITÊ GESTOR DA ICP-BRASIL

RESOLUÇÃO Nº 5, DE 22 DE NOVEMBRO DE 2001.

O **SECRETÁRIO-EXECUTIVO DO COMITÊ GESTOR DA INFRA-ESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA - ICP-BRASIL** faz saber que aquele Comitê, no uso das atribuições previstas no inciso IV do art. 4º da Medida Provisória Nº 2.200-2, de 24 de agosto de 2001,

RESOLVE:

Aprovar o relatório de auditoria apresentado pela Comissão designada pela Resolução Nº 3, de 25 de setembro de 2001, em anexo, homologar a Autoridade Certificadora Raiz - AC Raiz e o Serviço Federal de Processamento de Dados - SERPRO como seu prestador de serviço, bem como autorizar à Autoridade Certificadora Raiz - AC Raiz a gerar seu par de chaves assimétricas e a emitir o seu certificado.

MURILO MARQUES BARBOZA

RELATÓRIO DE AUDITORIA DA AC RAIZ DA ICP-BRASIL

1 - Objeto de Auditoria

Instalações e procedimentos operacionais da AC Raiz para geração do seu par de chaves assimétricas e emissão do seu correspondente certificado digital.

2 - Período da Auditoria

15.10.2001 a 19.10.2001 e de 12.11.2001 a 14.11.2001

3 - Objetivo da Auditoria

Avaliar se a AC Raiz está tecnicamente habilitada a gerar seu par de chaves assimétricas e a emitir o seu certificado de maneira segura, em conformidade com os procedimentos preconizados na sua Declaração de Práticas de Certificação - DPC, na Política de Segurança - PS da ICP-Brasil, nas Diretrizes de Segurança da Informação - DSI da AC Raiz e em outros documentos técnicos normativos da AC Raiz.

4 - Escopo da Auditoria

O escopo da auditoria pré-operacional foi a análise da conformidade dos procedimentos da AC Raiz em relação aos controles ambientais, operacionais e administrativos, necessários para garantir a geração de seu par de chaves assimétricas e a emissão de seu certificado, de maneira segura.

Por se tratar de uma auditoria pré-operacional, isto é, em ambiente onde ainda não foram iniciadas efetivamente as atividades da AC Raiz, não havia registros históricos de diversos procedimentos. Assim, utilizou-se a simulação de eventos e a análise documental dos manuais operacionais, examinando a conveniência e exatidão dos procedimentos previstos.

Devido ao caráter pré-operacional da auditoria, não foram avaliados os procedimentos e os ambientes para:

- divulgação do diretório de certificados e da lista de certificados revogados (site web); e
- recepção, análise e encaminhamento de pedidos de credenciamento como Autoridade Certificadora de nível imediatamente subseqüente ao da AC Raiz.

5 - Visão Global

O ITI firmou contrato com o SERPRO para que o mesmo opere, inicialmente, o sistema de certificação da AC Raiz, tendo sido prevista a realização das seguintes atividades:

- “alocação do sistema de geração de pares de chaves criptográficas e de certificados e respectivos serviços de gerenciamento do ciclo de vida das chaves criptográficas e dos certificados gerados, no ambiente físico do SERPRO-RJ, no Rio de Janeiro, Horto, em Sala-Cofre, com toda a infra-estrutura de segurança necessária;
- prestação de serviços relativos à segurança física, segurança dos dados, segurança operacional (procedimentos executados de forma segura) e controle de pessoal;
- realização de cerimonial de geração de certificado da AC Raiz;
- realização de cerimonial de geração de certificado das Autoridades Certificadoras - AC, quando demandado pelo ITI;
- geração de chaves de ignição que dão acesso à chave da AC Raiz, a serem fornecidas aos servidores designados pelo ITI;
- confecção, hospedagem e manutenção da página Web da AC Raiz, em português e inglês, em ambiente seguro;
- consultoria de Infra-estrutura de Chaves Públicas – ICP;
- treinamento técnico-operacional especializado sobre infra-estrutura de chaves públicas;

–
– emissão de certificados digitais para equipamentos servidores Web e aplicações que atendam à ICP-Brasil;
–
– serviços de disponibilização de Lista de Certificados Revogados - LCR em conformidade com as Políticas de Certificação da AC Raiz;
–
– serviços de informática relacionados à ICP-Brasil, sobre os quais as partes se ponham de acordo, a serem incluídos no Contrato mediante Termo Aditivo."

Para realizar as atividades de geração de chaves e certificados, o SERPRO disponibilizou a infra-estrutura física, lógica e de pessoal que possui em suas instalações no Rio de Janeiro, inicialmente concebidas para abrigar a Autoridade Certificadora do próprio SERPRO.

Os equipamentos que gerarão o certificado da AC Raiz estão instalados em sala exclusiva na sala-cofre do SERPRO-RJ, sendo que o acesso à mesma é restrito aos técnicos responsáveis pelas atividades ligadas à geração do certificado da AC Raiz e das AC subseqüentes, bem como da emissão da LCR.

6 - Análise

Para proceder à auditoria, foram utilizadas as técnicas de observação direta das instalações e atividades, exame documental e simulação da cerimônia de geração de chaves e emissão do certificado da AC Raiz e da LCR.

Durante a auditoria foram analisados os seguintes aspectos:

Controles ambientais

Gerenciamento de Risco

- Existência e abrangência de análise de risco
- Implementação de controles
- Monitoração dos riscos

Plano de Continuidade de Negócios

- Existência e abrangência do Plano de Continuidade de Negócios

Segurança física

- Níveis de segurança
- Armazenamento externo
- Manutenção de equipamentos

Segurança lógica

- Controle de softwares
- Controle de acesso lógico
- *Backup* e *restore*

Segurança de Pessoal

- Designação
- Treinamento técnico operacional

Segurança da Documentação

- Classificação da informação
- Geração, guarda, manuseio e destruição de documentos

Controles operacionais

Gerenciamento de chaves criptográficas

- Geração de chaves
- Uso das chaves
- Guarda das chaves
- Arquivamento de chaves
- Cópia de segurança
- Destruição de chaves

Gerenciamento do ciclo de vida dos certificados

Emissão do certificado da AC Raiz

- Emissão da Lista de Certificados Revogados - LCR

A comissão de auditoria, após a análise dos processos, solicitou que os sistemas: operacional, de administração de banco de dados e de certificação digital, necessários à operacionalização da AC Raiz, fossem instalados na sua presença. Esse procedimento teve por objetivo garantir que os softwares residentes no conjunto de equipamentos envolvidos no processo de geração do certificado da AC Raiz sejam estritamente os necessários para a consecução do mesmo.

Foram gerados *logs* ao final do processo de instalação de modo que a comissão de auditoria tenha condições de detectar qualquer atividade não autorizada antes do evento da geração do certificado da AC Raiz.

7 - Conclusão

A comissão de auditoria conclui, com base nos testes e análises realizadas durante os períodos em que executou a auditoria nas instalações operacionais da AC Raiz, que a mesma apresenta-se tecnicamente habilitada a gerar seu par de chaves assimétricas, emitir o seu próprio certificado e os certificados das AC de nível imediatamente subseqüente, de maneira segura.

Otávio Carlos Cunha da Silva
membro titular

Adriana Maria Pessôa Léo
membro titular

Viviane Regina Lemos Bertol
membro titular

Ernandes Lopes Bezerra
membro titular

Roger Stiefelmann Leal
membro titular