REVOGADA EM 18.04.2006 PELA RESOLUÇÃO 42

COMITÊ GESTOR DA ICP-BRASIL

RESOLUÇÃO Nº 21, DE 29 DE AGOSTO DE 2003.

Altera a Declaração de Práticas de Certificação da AC Raiz da ICP-Brasil, os Critérios e Procedimentos para Credenciamento das Entidades Integrantes da ICP-Brasil, os Requisitos Mínimos para as Políticas de Certificado na ICP-Brasil e os Requisitos Mínimos para as Declarações de Práticas de Certificação das Autoridades Certificadoras da ICP-Brasil.

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 art. 4º da Medida Provisória Nº 2.200-2, de 24 de agosto de 2001,

RESOLVE:

Art. 1º A Declaração de Práticas de Certificação da AC Raiz da ICP-Brasil, aprovada pela Resolução Nº 1, de 25 de setembro de 2001, passa a vigorar com as seguintes alterações:

"1.4 Dados de Contato

Nome: Instituto Nacional de Tecnologia da Informação - ITI
Endereço: Palácio do Planalto, Anexo IV
Telefone: (550xx61) 4112080, 411 3204, 4112781
Fax: 2265636
Página Web: http://www.iti.gov.br
E-mail: acraiz@iti.gov.br"

"2.1.1 Obrigações da AC Raiz

Constituem obrigações da AC Raiz da ICP-Brasil:

- A geração e o gerenciamento do par de chaves criptográficas da AC Raiz;
- A emissão e distribuição do certificado da AC Raiz;
- A emissão, a expedição e a distribuição de certificados de AC de nível imediatamente subseqüente ao seu;
- A publicação de certificados por ela emitidos;
- A revogação de certificados por ela emitidos;
- A emissão, o gerenciamento e a publicação de sua Lista de Certificados Revogados (LCR);
- A fiscalização e a auditoria das AC, das AR e dos prestadores de serviço habilitados em conformidade com os critérios estabelecidos pelo CG da ICP-Brasil;
- A implementação de acordos de certificação cruzada, conforme as diretrizes estabelecidas pelo CG da ICP-Brasil.
- Adotar medidas de segurança e controle, previstas nesta DPC e na Política de Segurança da ICP-Brasil, envolvendo seus processos, procedimentos e atividades;
- Manter os processos, procedimentos e atividades em conformidade com a legislação vigente e com as normas, práticas e regras estabelecidas pelo CG da ICP-Brasil;
- Manter e garantir a integridade, o sigilo e a segurança da informação por ela tratada; e
- Manter e testar regularmente planos de continuidade de negócio e de recuperação de desastres."

“2.2.1 Responsabilidades da AC Raiz

A AC Raiz responde pelos danos a que der causa.”

“2.4.2 Forma de interpretação e notificação

Na hipótese de uma ou mais das disposições desta DPC ser, por qualquer razão, considerada inválida, ilegal, ou não aplicável por lei, tal inaplicabilidade não afetará as demais disposições, sendo esta DPC interpretada então como se não contivesse tal disposição, e na medida do possível, interpretada para manter a intenção original da DPC.

Os direitos e obrigações previstos nesta DPC são de ordem pública e indisponíveis.

As notificações, intimações, solicitações ou qualquer outra comunicação necessária sujeita às práticas descritas nesta DPC serão feitas, preferencialmente, por e-mail assinado digitalmente, ou, na sua impossibilidade, por ofício da autoridade competente ou publicação no Diário Oficial da União.”

“2.6.1 Publicação de informação da AC Raiz

O certificado da AC Raiz, sua LCR e os certificados das AC de nível imediatamente subseqüente ao seu são publicados em serviço de diretório e/ou em página *Web* da AC Raiz, obedecendo as regras e os critérios estabelecidos nesta DPC.

A lista das Autoridades Certificadoras que integram a ICP-Brasil também é encontrada na página *Web* da AC Raiz.

A disponibilidade das informações publicadas pela AC Raiz em serviço de diretório e/ou página *Web*, tais como certificados, sua LCR, sua DPC, entre outras, é de 99,99% (noventa e nove inteiros e noventa e nove décimos por cento) do tempo, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.

A AC Raiz inclui nos certificados emitidos a identificação da sua página *Web*.”

“2.7.5 Medidas a serem adotadas em caso de não conformidade

Cabe à entidade auditada cumprir, no prazo estipulado pela AC Raiz da ICP-Brasil, as recomendações dos auditores para corrigir os casos de não conformidade com a legislação ou com as políticas, normas, práticas e regras estabelecidas. O não cumprimento das recomendações, no prazo estipulado, acarretará o cancelamento do credenciamento da entidade auditada, salvo determinação contrária da AC Raiz da ICP-Brasil.

Cabe à AC Raiz tomar todas as medidas cabíveis a fim de garantir a segurança e a confiabilidade da ICP-Brasil, podendo cancelar imediatamente o credenciamento da AC e da AR auditada, mediante decisão motivada.

A AC Raiz, em casos de iminente dano irreparável ou de difícil reparação a terceiros, suspenderá cautelarmente, no todo ou em parte, a emissão de certificados pela AC de nível imediatamente subseqüente ao seu.”

“2.8.1 Tipos de informações sigilosas

Como princípio geral, todo documento, informação ou registro fornecido à AC Raiz será sigiloso.”

“2.8.2 Tipos de informações não sigilosas
Certificados, LCR, e informações corporativas ou pessoais que necessariamente façam parte deles ou de diretórios públicos são consideradas informações não sigilosas.

Os seguintes documentos da AC Raiz e das AC de nível imediatamente subseqüente ao seu também são considerados documentos não sigilosos:

- qualquer PC aplicável;
-
- qualquer DPC;
-
- versões públicas de Políticas de Segurança;

–
– a conclusão dos relatórios da auditoria.”

“3.2 Criação de novo par de chaves antes da expiração do atual

O processo de geração, pela AC Raiz, de um novo certificado para uma AC de nível imediatamente subseqüente ao seu pode ser feito de forma simplificada, antes da expiração do certificado vigente da AC. Para isto, um representante legal da AC deve preencher e assinar digitalmente o formulário eletrônico Revalidação dos Dados Cadastrais e Solicitação de Novo Certificado. Após o recebimento desse formulário, desde que a documentação esteja regularmente atualizada, a AC Raiz iniciará o processo de emissão do novo certificado.”

“3.3 Criação de novo par de chaves após revogação

A solicitação de novo certificado de AC após a revogação do certificado anterior deverá ser efetivada pelo preenchimento do formulário Revalidação dos Dados Cadastrais e Solicitação de Novo Certificado. Este formulário deverá ser assinado por representante legalmente constituído da AC e entregue junto à AC Raiz. Após o recebimento desse formulário, desde que a documentação esteja regularmente atualizada, a AC Raiz iniciará o processo de emissão do novo certificado.”

“4.4.1 Circunstâncias para revogação

Um certificado de AC de nível imediatamente subseqüente ao da AC Raiz pode ser revogado a qualquer instante, por solicitação da própria AC titular do certificado ou por decisão motivada da AC Raiz, resguardados os princípios do contraditório e da ampla defesa.

Um certificado deve obrigatoriamente ser revogado:

– quando constatada emissão imprópria ou defeituosa do mesmo;
–
– quando for necessária a alteração de qualquer informação constante no mesmo;
–
– no caso de dissolução da AC titular do certificado; ou
–
– no caso de comprometimento da chave privada da AC ou da sua mídia armazenadora.

A AC Raiz da ICP-Brasil pode revogar ou determinar a revogação do certificado ou da certificação cruzada, conforme o caso, da AC que deixar de cumprir a legislação vigente ou as políticas, normas, práticas e regras estabelecidas para a ICP-Brasil.

As chaves públicas dos certificados emitidos por AC dissolvida serão armazenadas por outra AC, após aprovação da AC Raiz.

Quando houver mais de uma AC interessada, assumirá a responsabilidade do armazenamento das chaves públicas, aquela indicada pela AC que encerra as suas atividades.

A AC que encerra as suas atividades transferirá, se for o caso, a documentação dos certificados digitais emitidos à AC que tenha assumido a guarda das respectivas chaves públicas.

Caso as chaves públicas não tenham sido assumidas por outra AC, os documentos referentes aos certificados digitais e as respectivas chaves públicas serão repassados à AC Raiz.”

Art. 2º Os Critérios e Procedimentos para Credenciamento das Entidades Integrantes da ICP-Brasil, aprovados pela Resolução Nº 6, de 22 de novembro de 2001, passam a vigorar com as seguintes alterações e inclusão de notas:

“ANEXO IV
(SEM VALIDADE POIS FOI DADA NOVA REDAÇÃO PELA RESOLUÇÃO Nº 26, DE 24 DE OUTUBRO DE 2003)

DOCUMENTOS PARA CREDENCIAMENTO DE AUTORIDADE CERTIFICADORA

O candidato a desenvolver as atividades de Autoridade Certificadora - AC deve entregar ao Instituto Nacional de Tecnologia da Informação - ITI, os seguintes documentos atualizados: ”

“NOTA 1: Na hipótese de o candidato já estar credenciado como AC em relação a outra Política de Certificado, o documento a apresentar fica restrito àquele descrito no item 4b. Nessa mesma hipótese, todos os demais documentos deverão ser reapresentados apenas se modificados em relação às versões anteriormente entregues.

NOTA 2: Na hipótese de o candidato a AC ser pessoa jurídica de direito público deverá apresentar a seguinte documentação, se aplicável:

a) prova de inscrição no Cadastro Nacional de Pessoas Jurídicas – CNPJ;

b) ato constitutivo;

c) prova de regularidade junto às Fazendas Públicas Federal, Estaduais e Municipais do domicílio ou sede do candidato, ou outra equivalente, na forma da lei; e

d) prova de regularidade junto à Seguridade Social, demonstrando situação regular no cumprimento dos encargos sociais instituídos por lei.”

“ANEXO V
(SEM VALIDADE POIS FOI DADA NOVA REDAÇÃO PELA RESOLUÇÃO Nº 26, DE 24 DE OUTUBRO DE 2003)

DOCUMENTOS PARA CREDENCIAMENTO DE AUTORIDADE DE REGISTRO

O candidato a desenvolver as atividades de Autoridade de Registro - AR deve entregar, por intermédio da Autoridade Certificadora - AC ou candidato a AC a que esteja operacionalmente vinculado, ao Instituto Nacional de Tecnologia da Informação - ITI, os seguintes documentos atualizados:”

“NOTA 1: Fica dispensado da entrega dos documentos descritos neste Anexo o candidato já credenciado como AR em relação a outras Políticas de Certificado, exceto quando houver modificação dos mesmos em relação às versões anteriormente entregues.

NOTA 2: Na hipótese de o candidato a AR ser pessoa jurídica de direito público deverá apresentar a seguinte documentação, se aplicável:

a) prova de inscrição no Cadastro Nacional de Pessoas Jurídicas – CNPJ;

b) ato constitutivo

c) prova de regularidade junto às Fazendas Públicas Federal, Estaduais e Municipais do domicílio ou sede do candidato, ou outra equivalente, na forma da lei; e
d) Prova de regularidade junto à Seguridade Social, demonstrando situação regular no cumprimento dos encargos sociais instituídos por lei.”

“ANEXO VI
(SEM VALIDADE POIS FOI DADA NOVA REDAÇÃO PELA RESOLUÇÃO Nº 26, DE 24 DE OUTUBRO DE 2003)

DOCUMENTOS PARA CREDENCIAMENTO DE PRESTADOR DE SERVIÇO DE SUPORTE

O candidato a desenvolver as atividades de prestador de serviço de suporte deve entregar, por intermédio da Autoridade Certificadora - AC ou candidato a AC a que esteja operacionalmente vinculado, ao Instituto Nacional de Tecnologia da Informação – ITI, os seguintes documentos atualizados:”

“NOTA 1: Fica dispensado da entrega dos documentos descritos neste Anexo o candidato já credenciado como prestador de serviço de suporte em relação a outras Políticas de Certificado, exceto quando houver modificação dos mesmos em relação às versões anteriormente entregues.

NOTA 2: Na hipótese de o candidato a Prestador de Serviço de Suporte ser pessoa jurídica de direito público deverá apresentar a seguinte documentação, se aplicável:

a) prova de inscrição no Cadastro Nacional de Pessoas Jurídicas – CNPJ;

b) ato constitutivo

c) prova de regularidade junto às Fazendas Públicas Federal, Estaduais e Municipais do domicílio ou sede do candidato, ou outra equivalente, na forma da lei; e

d) Prova de regularidade junto à Seguridade Social, demonstrando situação regular no cumprimento dos encargos sociais instituídos por lei."

Art. 3º Os Requisitos Mínimos para as Políticas de Certificado na ICP-Brasil aprovados pela Resolução Nº 7, de 12 de dezembro de 2001, passam a vigorar com as seguintes alterações e inclusão de notas:

"1.3.3. Titulares de Certificado

Neste item devem ser caracterizadas as entidades - pessoas físicas ou jurídicas - que poderão ser titulares dos certificados emitidos segundo a PC.

NOTA 1: Em sendo o titular do certificado pessoa jurídica, será designada pessoa física como responsável pelo certificado, que será a detentora da chave privada.

Preferencialmente, será designado como responsável pelo certificado, o representante legal da pessoa jurídica ou um de seus representantes legais.

NOTA 2: Em se tratando de certificado emitido para equipamento ou aplicação, o titular será a pessoa física ou jurídica solicitante do certificado, que deverá indicar o responsável pela chave privada."

"1.3.4. Aplicabilidade

Neste item devem ser relacionadas as aplicações para as quais são adequados os certificados definidos pela PC e, quando cabíveis, as aplicações para as quais existam restrições ou proibições para o uso desses certificados.

As aplicações e demais programas que admitirem o uso de certificado digital de um determinado tipo contemplado pela ICP-Brasil devem aceitar qualquer certificado de mesmo tipo, ou com requisitos de segurança mais rigorosos, emitido por qualquer Autoridade Certificadora credenciada pela AC Raiz.

Na definição das aplicações para o certificado definido pela PC, a AC responsável deve levar em conta o nível de segurança previsto para o tipo do certificado. Esse nível de segurança é caracterizado pelos requisitos mínimos definidos para aspectos como: tamanho da chave criptográfica, mídia armazenadora da chave, processo de geração do par de chaves, procedimentos de identificação do titular de certificado, freqüência de emissão da correspondente Lista de Certificados Revogados (LCR) e extensão do período de validade do certificado, apresentados na tabela constante do Anexo I.

Certificados de tipos A1, A2, A3 e A4 serão utilizados em aplicações como confirmação de identidade na Web, correio eletrônico, transações on-line, redes privadas virtuais, transações eletrônicas, informações eletrônicas, cifração de chaves de sessão e assinatura de documentos eletrônicos com verificação da integridade de suas informações.

Certificados de tipos S1, S2, S3 e S4 serão utilizados em aplicações como cifração de documentos, bases de dados, mensagens e outras informações eletrônicas, com a finalidade de garantir o seu sigilo."

"2.1.1. Obrigações da AC (SEM VALIDADE POIS FOI DADA NOVA REDAÇÃO PELA RESOLUÇÃO Nº 37, DE 21 DE OUTUBRO DE 2004)

Neste item devem ser incluídas as obrigações da AC responsável pela PC, contendo, no mínimo, as abaixo relacionadas:

- operar de acordo com a sua Declaração de Práticas de Certificação (DPC) e com as PC que implementa;
-
- tomar as medidas cabíveis para assegurar que usuários e demais entidades envolvidas tenham conhecimento de seus respectivos direitos e obrigações;

- gerar e gerenciar os seus pares de chaves criptográficas;

- assegurar a proteção de suas chaves privadas;

- notificar os seus usuários quando ocorrer: suspeita de comprometimento de sua chave, emissão de novo par de chaves e correspondente certificado ou o encerramento de suas atividades;

- distribuir o seu próprio certificado;

- emitir, expedir e distribuir os certificados de AC de nível imediatamente subseqüente ao seu ou os certificados de AR a ela vinculadas e os certificados de usuários finais;

- informar a emissão do certificado ao respectivo solicitante;

- revogar os certificados por ela emitidos;

- emitir, gerenciar e publicar sua Lista de Certificados Revogados (LCR) e, quando aplicável, disponibilizar consulta on-line de situação do certificado (OCSP - On-line Certificate Status Protocol);

- identificar e registrar todas as ações executadas, conforme as normas, práticas e regras estabelecidas pelo CG da ICP-Brasil;

- publicar em sua página Web sua DPC e suas PC aprovadas;
-
- adotar as medidas de segurança e controle previstas na PC, DPC e Política de Segurança que implementar, envolvendo seus processos, procedimentos e atividades, observadas as normas, critérios, práticas e procedimentos da ICP-Brasil;

- manter a conformidade dos seus processos, procedimentos e atividades com as normas, práticas e regras da ICP-Brasil e com a legislação vigente;

- manter e garantir a integridade, o sigilo e a segurança da informação por ela tratada;

- manter e testar regularmente seu Plano de Continuidade do Negócio;
-
- informar às terceiras partes e titulares de certificado acerca das garantias, coberturas, condicionantes e limitações estipuladas pela apólice de seguro de responsabilidade civil contratada pela AC; e

- não emitir certificado com prazo de validade que se estenda além do prazo de validade de seu próprio certificado".

"2.1.2. Obrigações das AR (SEM VALIDADE POIS FOI DADA NOVA REDAÇÃO PELA RESOLUÇÃO Nº 26, DE 24 DE OUTUBRO DE 2003)

Neste item devem ser incluídas as obrigações das AR vinculadas à AC responsável pela PC, contendo, no mínimo, as abaixo relacionadas:

- receber solicitações de emissão ou de revogação de certificados;
-
- confirmar a identidade do solicitante e a validade da solicitação, de acordo com os requisitos estabelecidos pelos itens 3 e 4 da PC;
-
- encaminhar a solicitação de emissão ou de revogação de certificado à AC responsável;
-
- informar aos respectivos titulares a emissão ou a revogação de seus certificados;

- disponibilizar os certificados emitidos pela AC aos seus respectivos solicitantes;

- identificar e registrar todas as ações executadas, conforme as normas, práticas e regras estabelecidas pelo CG da ICP-Brasil;
-
- manter a conformidade dos seus processos, procedimentos e atividades com as normas, critérios, práticas e regras estabelecidas pela AC vinculada; e

- manter e garantir a segurança da informação por elas tratada, de acordo com o estabelecido nas normas, critérios, práticas e procedimentos da ICP-Brasil."

"2.1.3. Obrigações do Titular do Certificado

Neste item devem ser incluídas as obrigações dos titulares de certificados emitidos de acordo com a PC,

que integrarão o contrato de que trata o item 4.1, contendo, no mínimo, as abaixo relacionadas:

- fornecer, de modo completo e preciso, todas as informações necessárias para sua identificação;
-
- garantir a proteção e o sigilo de suas chaves privadas, senhas e dispositivos criptográficos;
-
- utilizar os seus certificados e chaves privadas de modo apropriado, conforme o previsto na PC correspondente;

- conhecer os seus direitos e obrigações, contemplados pela PC, pela DPC da AC emitente e por outros documentos aplicáveis da ICP-Brasil;
-
- informar à AC emitente qualquer comprometimento de sua chave privada e solicitar a imediata revogação do certificado correspondente.

NOTA: Em se tratando de certificado emitido para pessoa jurídica, equipamento ou aplicação, estas obrigações se aplicam ao responsável pelo uso do certificado."

"2.2.1. Responsabilidades da AC".

A AC responde pelos danos a que der causa.

A AC responsável pela PC responderá solidariamente pelos atos das AC das cadeias a ela subordinadas."

"2.2.2. Responsabilidades das AR

A AR será responsável pelos danos a que der causa."

"2.3.2. Relações Fiduciárias

Neste item deve constar que a AC responsável ou AR vinculada indenizará integralmente os danos o que der causa. Em situações justificáveis, pode ocorrer limitação da indenização, quando o titular do certificado for pessoa jurídica."

"2.6.1. Publicação de informação da AC (SEM VALIDADE POIS FOI DADA NOVA REDAÇÃO PELA RESOLUÇÃO Nº 26, DE 24 DE OUTUBRO DE 2003)

Neste item devem ser definidas as informações a serem publicadas pela AC responsável, o modo pelo qual serão disponibilizadas e a sua disponibilidade, que deverá ser, no mínimo, de 99% (noventa e nove por cento) do tempo, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana."

As seguintes informações, no mínimo, deverão ser publicadas pela AC em serviço de diretório ou página *web*: (INCLUÍDO PELA RETIFICAÇÃO DE 29 DE AGOSTO DE 2003)

- seu próprio certificados;
-
- suas LCR;
-
- sua DPC;
-
- as PC que implementar.

"2.8. Sigilo

A chave privada de assinatura digital da AC credenciada será gerada e mantida pela própria AC, que será responsável pelo seu sigilo. A divulgação ou utilização indevida da chave privada de assinatura pela AC será de sua inteira responsabilidade.

A PC deve informar que os titulares de certificados emitidos para pessoas físicas ou os responsáveis pelo uso de certificados emitidos para pessoas jurídicas, equipamentos ou aplicações, terão as atribuições de geração, manutenção e sigilo de suas respectivas chaves privadas. Além, disso, responsabilizam-se pela divulgação ou utilização indevidas dessas mesmas chaves. A PC deve informar também as medidas necessárias para preservação do sigilo dessas chaves privadas.

No caso de PC referente a certificado de sigilo, devem ser delimitadas as responsabilidades pela manutenção e pela garantia do sigilo da respectiva chave privada."

"2.8.1. Tipos de informações sigilosas

Neste item devem ser identificados os tipos de informações consideradas sigilosas pela AC responsável pela PC e pelas AR a ela vinculadas, de acordo com as normas, critérios, práticas e procedimentos da ICP-Brasil.

Como princípio geral, todo documento, informação ou registro fornecido à AC ou às AR será sigiloso."

"2.8.3. Divulgação de informação de revogação e de suspensão de certificado

Neste item devem ser descritas as formas previstas pela AC para a divulgação de informação de revogação dos certificados por ela emitidos. O item deve informar também a política adotada pela AC para a divulgação ou não divulgação das razões para a revogação dos certificados para terceiros.

As razões para revogação do certificado sempre serão informadas para o seu titular, e serão tornadas públicas desde que haja autorização expressa deste.

A PC deve ainda informar que a suspensão de certificados não é admitida no âmbito da ICP-Brasil."

"3.1.1. Tipos de nomes

Neste item, devem ser descritos os tipos de nomes admitidos para os titulares de certificados emitidos segundo a PC, tais como nomes no padrão ITU X.500, endereços de correio eletrônico ou endereços de página Web (URL).

A PC deve estabelecer ainda que um certificado emitido para uma pessoa jurídica deverá incluir o nome da pessoa física responsável pelo seu uso."

"3.1.9. Autenticação da identidade de um indivíduo (SEM VALIDADE POIS FOI DADA NOVA REDAÇÃO PELA RESOLUÇÃO Nº 26, DE 24 DE OUTUBRO DE 2003)

Neste item devem ser definidos os procedimentos empregados pelas AR vinculadas para a confirmação da identidade de um indivíduo. Essa confirmação deverá ser realizada, mediante a presença física do interessado, com base em documentos de identificação legalmente aceitos. Devem ser apresentados, acompanhados de cópia, no mínimo, os seguintes documentos:

- Cédula de Identidade ou Passaporte, se estrangeiro;
- Cadastro de Pessoa Física;
- comprovante de residência;
- PIS/PASEP, se aplicável;
- título de eleitor, se aplicável;
- mais um documento oficial com fotografia, no caso de certificados de tipos A4 e S4;
- os documentos acima relacionados do responsável, caso o solicitante seja incapaz.

Quando o titular do certificado for pessoa física, deverá ser feita a confirmação de sua identidade, mediante apresentação dos documentos acima expostos. Neste caso o titular do certificado, assinará "termo de titularidade".

Quando o titular do certificado for pessoa jurídica, deverá ser feita a confirmação de sua identidade, na forma do item 3.1.8; e de seu representante legal, mediante apresentação dos documentos acima expostos. Neste caso, o representante legal da pessoa jurídica, assinará "termo de titularidade". Será feita ainda a confirmação da identidade da pessoa física responsável pelo uso do certificado, mediante apresentação dos documentos acima expostos. O responsável pelo certificado, assinará "termo de responsabilidade".

Quando o certificado for emitido para equipamento ou aplicação, deverá ser feita a confirmação da identidade do titular do certificado – pessoa física ou jurídica - e do responsável pela chave privada, na forma do que já foi disposto. Neste caso, também será assinado “termo de titularidade” e “termo de responsabilidade”.
A PC deve descrever como serão os procedimentos utilizados pelas AR para identificação e autenticação da identidade de um indivíduo.

A PC deve prever que serão mantidos arquivos com o tipo e os detalhes da identificação utilizada em cada caso.”

“3.2. Geração de novo par de chaves antes da expiração do atual

Neste item, a PC deve estabelecer o processo de identificação do solicitante exigido para a geração do novo par de chaves, e de seu correspondente certificado, antes da expiração do certificado vigente. Esse processo poderá ser conduzido segundo uma das seguintes possibilidades:

- adoção dos mesmos requisitos e procedimentos exigidos para a solicitação do certificado; ou
-
- solicitação por meio eletrônico, assinada digitalmente com uso de certificado vigente, que seja pelo menos do mesmo nível de segurança, limitada a 3 (três) ocorrências sucessivas.”

“4.3. Aceitação de Certificado

Neste item devem ser descritos todos os requisitos e procedimentos operacionais referentes à aceitação de um certificado por seu titular.

A PC deve garantir que a aceitação de todo certificado emitido seja declarada pelo respectivo titular. No caso de certificados emitidos para pessoas jurídicas, equipamentos ou aplicações, a declaração deverá ser feita pela pessoa física responsável por esses certificados.”

“4.9. Extinção da AC

Este item da PC deve descrever os requisitos e os procedimentos que deverão ser adotados nos casos de extinção dos serviços da AC responsável ou de uma AR a ela vinculada. Devem ser descritos os procedimentos para notificação dos usuários e para a transferência da guarda de seus dados e registros de arquivo.

O responsável pela guarda desses dados e registros deverá observar os mesmos requisitos de segurança exigidos para a AC extinta.

As chaves públicas dos certificados emitidos por AC dissolvida serão armazenadas por outra AC, após aprovação da AC Raiz.

Quando houver mais de uma AC interessada, assumirá a responsabilidade do armazenamento das chaves públicas, aquela indicada pela AC que encerra as suas atividades.

A AC que encerra as suas atividades transferirá, se for o caso, a documentação dos certificados digitais emitidos à AC que tenha assumido a guarda das respectivas chaves públicas.

Caso as chaves públicas não tenham sido assumidas por outra AC, os documentos referentes aos certificados digitais e as respectivas chaves públicas serão repassados à AC Raiz.”

“6.1.1. Geração do par de chaves

Quando o titular de certificado for uma pessoa física, esta será a responsável pela geração dos pares de chaves criptográficas. Quando o titular de certificado for uma pessoa jurídica, esta indicará por seu(s) representante(s) legal(s), a pessoa responsável pela geração dos pares de chaves criptográficas e pelo uso do certificado.

Neste item, a PC deve descrever todos os requisitos e procedimentos referentes ao processo de geração de chaves aplicável ao certificado que define.
Ao ser gerada, a chave privada da entidade titular deverá ser gravada cifrada, por algoritmo simétrico como 3-DES, IDEA, SAFER+ ou outros aprovados pelo CG da ICP-Brasil, no meio de armazenamento definido para cada tipo de certificado previsto pela ICP-Brasil, conforme a Tabela 4.

A chave privada deverá trafegar cifrada, empregando os mesmos algoritmos citados no parágrafo anterior, entre o dispositivo gerador e a mídia utilizada para o seu armazenamento.

O meio de armazenamento da chave privada deverá assegurar, por meios técnicos e procedimentais adequados, no mínimo, que:

- a chave privada é única e seu sigilo é suficientemente assegurado;
- a chave privada não pode, com uma segurança razoável, ser deduzida e deve estar protegida contra falsificações realizadas através das tecnologias atualmente disponíveis;
- a chave privada pode ser eficazmente protegida pelo legítimo titular contra a utilização por terceiros.

Esse meio de armazenamento não deve modificar os dados a serem assinados, nem impedir que esses dados sejam apresentados ao signatário antes do processo de assinatura.

Tipo de Certificado	Mídia Armazenadora de Chave Criptográfica (requisitos mínimos)
A1 e S1	Cartão Inteligente ou *Toke*n, ambos sem capacidade de geração de chave e protegidos por senha
A2 e S2	Cartão Inteligente ou *Toke*n, ambos sem capacidade de geração de chave e protegidos por senha
A3 e S3	Cartão Inteligente ou *Toke*n, ambos com capacidade de geração de chave e protegidos por senha, ou *hardware* criptográfico aprovado pelo CG da ICP-Brasil
A4 e S4	Cartão Inteligente ou *Toke*n, ambos com capacidade de geração de chave e protegidos por senha, ou *hardware* criptográfico aprovado pelo CG da ICP-Brasil

TABELA 4 – Mídias Armazenadoras de Chaves Criptográficas."

"7.1.4. Formatos de nome

O nome do titular do certificado, constante do campo "Subject", deverá adotar o "Distinguished Name" (DN) do padrão ITU X.500/ISO 9594, da seguinte forma:

C = BR
O = ICP-Brasil
CN = nome do titular do certificado em certificado de pessoa física; em um certificado de pessoa jurídica, deverá conter o nome empresarial constante do CNPJ (Cadastro Nacional de Pessoa Jurídica); em um certificado de equipamento ou aplicação, o identificador CN deverá conter o URL correspondente.

NOTA: Será escrito o nome até o limite do tamanho do campo disponível, vedada a abreviatura."

Art. 4º Os Requisitos Mínimos para as Declarações de Práticas de Certificação das Autoridades Certificadoras da ICP-Brasil aprovados pela Resolução Nº 8, de 12 de dezembro de 2001, passam a vigorar com as seguintes alterações e inclusão de notas:

"1.3.3. Titulares de Certificado

Neste item devem ser caracterizadas as entidades - pessoas físicas ou jurídicas - que poderão ser titulares dos certificados emitidos segundo a DPC.

Quando aplicável, devem ser caracterizadas as AC para as quais a AC em questão poderá emitir certificados.

NOTA 1: Em sendo o titular do certificado pessoa jurídica, será designada pessoa física como responsável pelo certificado, que será a detentora da chave privada.

Preferencialmente, será designado como responsável pelo certificado, o representante legal da pessoa jurídica ou um de seus representantes legais.

NOTA 2: Em se tratando de certificado emitido para equipamento ou aplicação, o titular será a pessoa física ou jurídica solicitante do certificado, que deverá indicar o responsável pela chave privada."

"2.1.1. Obrigações da AC (SEM VALIDADE POIS FOI DADA NOVA REDAÇ PELA RESOLUÇÃO Nº 37, DE 21 DE OUTUBRO DE 2004)

Neste item devem ser incluídas as obrigações da AC responsável pela DPC, contendo, no mínimo, as abaixo relacionadas:

- operar de acordo com a sua DPC e com as PC que implementa;
- gerar e gerenciar o seu par de chaves criptográficas;
- assegurar a proteção de suas chaves privadas;
- notificar a AC de nível superior, emitente do seu certificado, quando ocorrer comprometimento de sua chave privada e solicitar a imediata revogação desse certificado;
- notificar os seus usuários quando ocorrer suspeita de comprometimento de sua chave, emissão de novo par de chaves e correspondente certificado, ou o encerramento de suas atividades;
- distribuir o seu próprio certificado;
- emitir, expedir e distribuir os certificados de AC de nível imediatamente subseqüente ao seu ou os certificados de AR vinculadas e de usuários finais;
- informar a emissão do certificado ao respectivo solicitante;
- revogar os certificados por ela emitidos;
- emitir, gerenciar e publicar suas Listas de Certificados Revogados (LCR) e, quando aplicável, disponibilizar consulta on-line de situação do certificado (OCSP - On-line Certificate Status Protocol);
- publicar em sua página Web sua DPC e as PC aprovadas que implementa;
- identificar e registrar todas as ações executadas, conforme as normas, práticas e regras estabelecidas pelo CG da ICP-Brasil.
-
- adotar as medidas de segurança e controle previstas na DPC, PC e Política de Segurança que implementar, envolvendo seus processos, procedimentos e atividades, observadas as normas, critérios, práticas e procedimentos da ICP-Brasil;
- manter a conformidade dos seus processos, procedimentos e atividades com as normas, práticas e regras da ICP-Brasil e com a legislação vigente;
-
- manter e garantir a integridade, o sigilo e a segurança da informação por ela tratada;
- manter e testar regularmente seu Plano de Continuidade do Negócio;
-
- informar às terceiras partes e titulares de certificado acerca das garantias, coberturas, condicionantes e limitações estipuladas pela apólice de seguro de responsabilidade civil contratada pela AC;
- não emitir certificado com prazo de validade que se estenda além do prazo de validade de seu próprio certificado."

"2.1.2. Obrigações das AR (SEM VALIDADE POIS FOI DADA NOVA REDAÇÃO PELA RESOLUÇÃO Nº 26, DE 24 DE OUTUBRO DE 2003)

Neste item devem ser incluídas as obrigações das AR vinculadas à AC responsável pela DPC, contendo, no mínimo, as abaixo relacionadas:

- receber solicitações de emissão ou de revogação de certificados;
- confirmar a identidade do solicitante e a validade da solicitação;
- encaminhar a solicitação de emissão ou de revogação de certificado à AC responsável;
- informar aos respectivos titulares a emissão ou a revogação de seus certificados;
- disponibilizar os certificados emitidos pela AC aos seus respectivos solicitantes;
- identificar e registrar todas as ações executadas, conforme as normas, práticas e regras estabelecidas pelo CG da ICP-Brasil.
- manter a conformidade dos seus processos, procedimentos e atividades com as normas, práticas e regras estabelecidas pela AC a que se vincular;
- manter e garantir a segurança da informação por elas tratada, de acordo com o estabelecido nas normas, critérios, práticas e procedimentos da ICP-Brasil."

"2.1.3. Obrigações do Titular do Certificado

Neste item devem ser incluídas as obrigações dos titulares de certificados emitidos pela AC responsável pela DPC, que integrarão o contrato de que trata o item 4.1, contendo no mínimo as abaixo relacionadas:

- fornecer, de modo completo e preciso, todas as informações necessárias para sua identificação;
- garantir a proteção e o sigilo de suas chaves privadas, senhas e dispositivos criptográficos;
- utilizar os seus certificados e chaves privadas de modo apropriado, conforme o previsto na PC correspondente;
- conhecer os seus direitos e obrigações, contemplados pela PC, pela DPC da AC emitente e por outros documentos aplicáveis da ICP-Brasil;
- informar à AC emitente qualquer comprometimento de sua chave privada e solicitar a imediata revogação do certificado correspondente.

NOTA: Em se tratando de certificado emitido para pessoa jurídica, equipamento ou aplicação, estas obrigações se aplicam ao responsável pelo uso do certificado."

"2.2.1. Responsabilidades da AC
A AC responde pelos danos a que der causa.

A AC responsável pela DPC responderá solidariamente pelos atos das AC das cadeias a ela subordinadas."

"2.2.2. Responsabilidades das AR

A AR será responsável pelos danos a que der causa.

A AC responsável pela DPC responderá solidariamente pelos atos das AR a ela vinculadas."

"2.3.2. Relações Fiduciárias

Neste item deve constar que a AC responsável ou AR vinculada indenizará integralmente os danos o que der causa. Em situações justificáveis, pode ocorrer limitação da indenização, quando o titular do certificado for pessoa jurídica."

"2.6.1. Publicação de informação da AC (SEM VALIDADE POIS FOI DADA NOVA REDAÇÃO PELA RESOLUÇÃO Nº 26, DE 24 DE OUTUBRO DE 2003)

Neste item devem ser definidas as informações a serem publicadas pela AC responsável pela DPC, o modo pelo qual elas serão disponibilizadas e a sua disponibilidade, que deverá ser, no mínimo, de 99%

(noventa e nove por cento) do tempo, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana."

As seguintes informações, no mínimo, deverão ser publicadas pela AC em serviço de diretório ou página *web*: (INCLUÍDO PELA RETIFICAÇÃO DE 29 DE AGOSTO DE 2003)

- seu próprio certificados;
- suas LCR;
- sua DPC;
- as PC que implementar.

"2.7.2. Identidade e qualificações do auditor

Os relatórios de auditoria das AC de nível imediatamente subseqüente (AC Subseqüente) à AC responsável (AC Principal) deverão ser fornecidos por empresa de auditoria especializada e independente, contratada pela AC a ser auditada e autorizada pela AC Raiz.

Os relatórios de auditoria das AR e dos prestadores de serviço de suporte não precisam ser fornecidos por empresa de auditoria especializada e independente."

"2.8. Sigilo

A chave privada de assinatura digital da AC credenciada responsável pela DPC será gerada e mantida pela própria AC, que será responsável pelo seu sigilo. A divulgação ou utilização indevida da chave privada de assinatura pela AC será de sua inteira responsabilidade.

A DPC deve informar que os titulares de certificados ou os responsáveis pelo uso de certificados emitidos para pessoas jurídicas, equipamentos ou aplicações, terão as atribuições de geração, manutenção e sigilo de suas respectivas chaves privadas. Além, disso, responsabilizam-se pela divulgação ou utilização indevidas dessas mesmas chaves.

No caso de certificados de sigilo emitidos pela AC, a DPC deve se referir às PC correspondentes para delimitar as responsabilidades pela manutenção e pela garantia do sigilo das respectivas chaves privadas."
"2.8.3. Divulgação de informação de revogação ou suspensão de certificado

Neste item devem ser descritas as formas previstas pela AC responsável pela DPC para a divulgação de informação de revogação dos certificados por ela emitidos. O item deve informar também a política adotada pela AC para a divulgação ou não divulgação das razões para a revogação dos certificados para terceiros.

As razões para revogação do certificado sempre serão informadas para o seu titular, e serão tornadas públicas desde que haja autorização expressa deste.

A DPC deve ainda informar que a suspensão de certificados não é admitida no âmbito da ICP-Brasil."

"3.1.9. Autenticação da identidade de um indivíduo

Neste item da DPC devem ser descritos os procedimentos gerais empregados pelas AR vinculadas para a confirmação da identidade de um indivíduo. Essa confirmação deverá ser realizada, mediante a presença física do interessado, com base em documentos de identificação legalmente aceitos.

Cada PC implementada pela AC responsável deve definir os documentos de identificação exigidos, com base nos requisitos aplicáveis estabelecidos pelo documento Requisitos Mínimos para Políticas de Certificado na ICP-Brasil.

A DPC deve estabelecer que solicitações de certificados para AC deverão ser realizadas por pessoa física legalmente responsável. Caberá às AR vinculadas à AC responsável verificar a autorização atribuída ao solicitante, bem como a presença dos documentos exigidos. Os procedimentos utilizados pelas AR para identificação e verificação da autorização do solicitante devem ser descritos em detalhes nas PC implementadas.

A DPC deve estabelecer, ainda, que no caso de certificado emitido para pessoa física, o titular deste assinará “termo de titularidade”, a ser mantido junto à documentação exigida neste item, e será, para todos os efeitos legais responsável pela correta utilização do certificado conforme as normas da ICP-Brasil, assim como pelos danos a que der causa pelo uso indevido do certificado.

No caso de certificado emitido para pessoa jurídica, o seu representante legal assinará “termo de titularidade”, e a pessoa física indicada como responsável pelo certificado assinará “termo de responsabilidade”. Os termos de titularidade e de responsabilidade serão mantidos junto à documentação exigida neste item. Tanto a pessoa jurídica titular do certificado, como a pessoa física designada como responsável pelo certificado, serão responsáveis, pela correta utilização deste conforme as normas da ICP-Brasil, assim como pelos danos a que derem causa pelo uso indevido do certificado.

No caso de certificado emitido para equipamento ou aplicação, também serão assinados “termo de titularidade” e “termo de responsabilidade”, sendo o titular do certificado e a pessoa física designada, responsáveis pela correta utilização deste conforme as normas da ICP-Brasil, assim como pelos danos a que derem causa pelo uso indevido do certificado.

A DPC deve ainda prever que deverá ser mantido arquivo com o tipo e os detalhes do procedimento de identificação utilizado em cada caso.”

“4.3. Aceitação de Certificado

Neste item devem ser descritos todos os requisitos e procedimentos operacionais referentes à aceitação de um certificado por seu titular. Devem ser apontadas as implicações decorrentes dessa aceitação, ou não aceitação. Os procedimentos detalhados devem ser descritos nas PC implementadas.

A DPC deve garantir que a aceitação de todo certificado emitido seja declarada pelo respectivo titular. No caso de certificados emitidos para pessoas jurídicas, equipamentos ou aplicações, a declaração deverá ser feita pela pessoa física responsável por esses certificados.
Eventuais termos de acordo, ou instrumentos similares, requeridos devem ser descritos neste item da DPC.”

“4.9. Extinção da AC

Este item da DPC deve descrever os requisitos e os procedimentos que deverão ser adotados nos casos de extinção dos serviços da AC responsável ou de uma AR a ela vinculada. Devem ser descritos os procedimentos para notificação dos usuários e para a transferência da guarda de seus dados e registros de arquivo.

O responsável pela guarda desses dados e registros deverá observar os mesmos requisitos de segurança exigidos para a AC extinta.

As chaves públicas dos certificados emitidos por AC dissolvida serão armazenadas por outra AC, após aprovação da AC Raiz.

Quando houver mais de uma AC interessada, assumirá a responsabilidade do armazenamento das chaves públicas, aquela indicada pela AC que encerra as suas atividades.

A AC que encerra as suas atividades transferirá, se for o caso, a documentação dos certificados digitais emitidos à AC que tenha assumido a guarda das respectivas chaves públicas.

Caso as chaves públicas não tenham sido assumidas por outra AC, os documentos referentes aos certificados digitais e as respectivas chaves públicas serão repassados à AC Raiz.”

Art. 5º As Autoridades Certificadoras – AC devidamente credenciadas deverão apresentar, no prazo máximo de trinta dias contados da publicação desta Resolução, alteração na sua declaração de práticas de certificação e nas suas políticas de certificado, comprovando, sob pena de descredenciamento, a adequação de seus documentos às alterações procedidas por esta Resolução.

Parágrafo único. As AC em processo de credenciamento deverão apresentar imediatamente alteração na declaração de práticas de certificação e nas políticas de certificado apresentadas, adequando-as às modificações procedidas por esta Resolução.

Art. 6º Esta Resolução entra em vigor na data da sua publicação.

REVOGADA EM 18.04.2006 PELA RESOLUÇÃO 42