

Declaração de Práticas de Certificação da Autoridade Certificadora Safeweb

DPC - AC SAFEWEB

**Versão 1.0
Outubro 2017**

DECLARAÇÃO DE PRÁTICAS DE CERTIFICAÇÃO

SUMÁRIO

1	INTRODUÇÃO	08
1.1	VISÃO GERAL	08
1.2	IDENTIFICAÇÃO	08
1.3	COMUNIDADE E APLICABILIDADE	08
1.3.1	AUTORIDADE CERTIFICADORA - AC	08
1.3.2.	AUTORIDADE DE REGISTRO - AR	09
1.3.3	PRESTADOR DE SERVIÇOS DE SUPORTE – PSS	09
1.3.4	TITULARES DE CERTIFICADO	9
1.3.5	APLICABILIDADE	10
1.4	DADOS DE CONTATO.....	10
2	DISPOSIÇÕES GERAIS.....	10
2.1	OBRIGAÇÕES E DIREITOS.....	10
2.1.1	OBRIGAÇÕES DA AUTORIDADE CERTIFICADORA SAFEWEB	10
2.1.2	OBRIGAÇÕES DAS AUTORIDADES DE REGISTRO – AR.....	12
2.1.3	OBRIGAÇÕES DO TITULAR DO CERTIFICADO	12
2.1.4	DIREITOS DA TERCEIRA PARTE - <i>Relying Party</i>	13
2.1.5	OBRIGAÇÕES DO REPOSITÓRIO DA AC SAFEWEB	14
2.2	RESPONSABILIDADES	14
2.2.1	RESPONSABILIDADES DA AC SAFEWEB	14
2.2.2	RESPONSABILIDADES DAS AUTORIDADES DE REGISTRO VINCULADAS	14
2.3	RESPONSABILIDADE FINANCEIRA	14
2.3.1	INDENIZAÇÕES DEVIDAS PELA TERCEIRA PARTE - <i>Relying Party</i>	14
2.3.2	RELAÇÕES FIDUCIÁRIAS	14
2.3.3	PROCESSOS ADMINISTRATIVOS.....	15
2.4	INTERPRETAÇÃO E EXECUÇÃO	15
2.4.1	LEGISLAÇÃO.....	15
2.4.2	FORMA DE INTERPRETAÇÃO E NOTIFICAÇÃO	15
2.4.3	PROCEDIMENTO DE SOLUÇÃO DE DISPUTA	16
2.5	TARIFAS DE SERVIÇOS	16
2.5.1	TARIFAS DE EMISSÃO E RENOVAÇÃO DE CERTIFICADOS.....	16
2.5.2	TARIFAS DE ACESSO AO CERTIFICADO	16
2.5.3	TARIFAS DE REVOGAÇÃO OU DE ACESSO A INFORMAÇÃO DE STATUS	16
2.5.4	TARIFAS PARA OUTROS SERVIÇOS	16
2.5.5	POLÍTICA DE REEMBOLSO	16
2.6	PUBLICAÇÃO E REPOSITÓRIO	16
2.6.1	PUBLICAÇÃO DE INFORMAÇÃO DA AC SAFEWEB	17
2.6.2	FREQUÊNCIA DE PUBLICAÇÃO	17
2.6.3	CONTROLES DE ACESSO	17
2.6.4	REPOSITÓRIOS.....	17
2.7	FISCALIZAÇÃO E AUDITORIA DE CONFORMIDADE	18
2.8	SIGILO	18

2.8.1	DISPOSIÇÕES GERAIS.....	18
2.8.2	TIPOS DE INFORMAÇÕES SIGILOSAS	19
2.8.3	TIPOS DE INFORMAÇÕES NÃO SIGILOSAS.....	19
2.8.4	DIVULGAÇÃO DE INFORMAÇÃO DE REVOGAÇÃO DE CERTIFICADO	20
2.8.5	QUEBRA DE SIGILO POR MOTIVOS LEGAIS	20
2.8.6	INFORMAÇÕES A TERCEIROS	20
2.8.7	DIVULGAÇÃO POR SOLICITAÇÃO DO TITULAR	20
2.8.8	OUTRAS CIRCUNSTÂNCIAS DE DIVULGAÇÃO DE INFORMAÇÃO.....	21
2.9	DIREITOS DE PROPRIEDADE INTELECTUAL.....	21
3	IDENTIFICAÇÃO E AUTENTICAÇÃO	21
3.1	REGISTRO INICIAL	21
3.1.1	DISPOSIÇÕES GERAIS.....	21
3.1.2	TIPOS DE NOMES.....	22
3.1.3	NECESSIDADE DE NOMES SIGNIFICATIVOS.....	23
3.1.4	REGRAS PARA INTERPRETAÇÃO DE VÁRIOS TIPOS DE NOMES.....	23
3.1.5	UNICIDADE DE NOMES.....	23
3.1.6	PROCEDIMENTO PARA RESOLVER DISPUTA DE NOMES.....	23
3.1.7	RECONHECIMENTO, AUTENTICAÇÃO E PAPEL DE MARCAS REGISTRADAS.....	23
3.1.8	MÉTODO PARA COMPROVAR A POSSE DE CHAVE PRIVADA	23
3.1.9	AUTENTICAÇÃO DA IDENTIDADE DE UM INDIVÍDUO	23
3.1.10	AUTENTICAÇÃO DA IDENTIDADE DE UMA ORGANIZAÇÃO	25
3.1.11	AUTENTICAÇÃO DA IDENTIDADE DE EQUIPAMENTO, APLICAÇÃO OU CÓDIGO	26
3.2	GERAÇÃO DE NOVO PAR DE CHAVES ANTES DA EXPIRAÇÃO DO ATUAL	26
3.3	GERAÇÃO DE NOVO PAR DE CHAVES APÓS REVOGAÇÃO OU EXPIRAÇÃO.....	27
3.4	SOLICITAÇÃO DE REVOGAÇÃO	27
4	REQUISITOS OPERACIONAIS.....	27
4.1	SOLICITAÇÃO DE CERTIFICADO	27
4.2	EMISSÃO DE CERTIFICADO	28
4.3	ACEITAÇÃO DO CERTIFICADO	28
4.4	REVOGAÇÃO DE CERTIFICADO	28
4.4.1	CIRCUNSTÂNCIAS PARA REVOGAÇÃO.....	28
4.4.2	QUEM PODE SOLICITAR A REVOGAÇÃO	29
4.4.3	PROCEDIMENTO PARA SOLICITAÇÃO DE REVOGAÇÃO	29
4.4.4	PRAZO PARA SOLICITAÇÃO DE REVOGAÇÃO	30
4.4.5	CIRCUNSTÂNCIAS PARA SUSPENSÃO	30
4.4.6	QUEM PODE SOLICITAR SUSPENSÃO	30
4.4.7	PROCEDIMENTO PARA SOLICITAÇÃO DE SUSPENSÃO.....	30
4.4.8	LIMITES NO PERÍODO DE SUSPENSÃO	31
4.4.9	FREQUÊNCIA DE EMISSÃO DE LCR	31
4.4.10	REQUISITOS PARA VERIFICAÇÃO DE LCR.....	31
4.4.11	DISPONIBILIDADE PARA REVOGAÇÃO/VERIFICAÇÃO DE STATUS ON-LINE	31
4.4.12	REQUISITOS PARA VERIFICAÇÃO DE REVOGAÇÃO ON-LINE	31
4.4.13	OUTRAS FORMAS DISPONÍVEIS PARA DIVULGAÇÃO DE REVOGAÇÃO	31
4.4.14	REQUISITOS PARA VERIFICAÇÃO DE OUTRAS FORMAS DE DIVULGAÇÃO DE REVOGAÇÃO.....	31
4.4.15	REQUISITOS ESPECIAIS PARA O CASO DE COMPROMETIMENTO DE CHAVE.....	31
4.5	PROCEDIMENTOS DE AUDITORIA DE SEGURANÇA.....	32
4.5.1	TIPOS DE EVENTO REGISTRADOS.....	32
4.5.2	FREQUÊNCIA DE AUDITORIA DE REGISTROS (LOGS).....	33
4.5.3	PERÍODO DE RETENÇÃO PARA REGISTROS (LOGS) DE AUDITORIA.....	33

4.5.4	PROTEÇÃO DE REGISTRO (LOGS) DE AUDITORIA.....	34
4.5.5	PROCEDIMENTO PARA CÓPIA DE SEGURANÇA (BACKUP) DE REGISTRO (LOG) DE AUDITORIA....	34
4.5.6	SISTEMA DE COLETA DE DADOS DE AUDITORIA	34
4.5.7	NOTIFICAÇÃO DE AGENTES CAUSADORES DE EVENTOS	34
4.5.8	AVALIAÇÕES DE VULNERABILIDADE.....	34
4.6	ARQUIVAMENTO DE REGISTRO	35
4.6.1	TIPOS DE EVENTOS REGISTRADOS	35
4.6.2	PERÍODO DE RETENÇÃO PARA ARQUIVO.....	35
4.6.3	PROTEÇÃO DE ARQUIVO	35
4.6.4	PROCEDIMENTOS PARA CÓPIA DE SEGURANÇA (BACKUP) DE ARQUIVO	35
4.6.5	REQUISITOS PARA DATAÇÃO DE REGISTROS (time-stamping)	36
4.6.6	SISTEMA DE COLETA DE DADOS DE ARQUIVO	36
4.6.7	PROCEDIMENTOS PARA OBTER E VERIFICAR INFORMAÇÃO DE ARQUIVO	36
4.7	TROCA DE CHAVE	36
4.8	COMPROMETIMENTO E RECUPERAÇÃO DE DESASTRE	36
4.8.1	RECURSOS COMPUTACIONAIS, SOFTWARE E DADOS CORROMPIDOS	37
4.8.2	CERTIFICADO DE ENTIDADE É REVOGADO.....	37
4.8.3	CHAVE DE ENTIDADE É COMPROMETIDA.....	38
4.8.4	SEGURANÇA DOS RECURSOS APÓS DESASTRE NATURAL OU DE OUTRA NATUREZA	38
4.8.5	ATIVIDADES DAS AUTORIDADES DE REGISTRO.....	38
4.9	EXTINÇÃO DOS SERVIÇOS DE AC, AR ou PSS.....	39
5	CONTROLES DE SEGURANÇA FÍSICA, PROCEDIMENTAL E DE PESSOAL	40
5.1	CONTROLES FÍSICOS	40
5.1.1	CONSTRUÇÃO E LOCALIZAÇÃO DAS INSTALAÇÕES DE AC	40
5.1.2	ACESSO FÍSICO NAS INSTALAÇÕES DA AC SAFEWEB	40
5.1.3	ENERGIA E AR CONDICIONADO NAS INSTALAÇÕES DE AC	43
5.1.4	EXPOSIÇÃO À ÁGUA NAS INSTALAÇÕES DE AC.....	44
5.1.5	PREVENÇÃO E PROTEÇÃO CONTRA INCÊNDIO NAS INSTALAÇÕES DE AC.....	44
5.1.6	ARMAZENAMENTO DE MÍDIA NAS INSTALAÇÕES DE AC.....	45
5.1.7	DESTRUIÇÃO DE LIXO NAS INSTALAÇÕES DE AC.....	45
5.1.8	INSTALAÇÕES DE SEGURANÇA (BACKUP) EXTERNAS (OFF-SITE) PARA AC	45
5.1.9	INSTALAÇÕES TÉCNICAS DE AR	45
5.2	CONTROLES PROCEDIMENTAIS.....	45
5.2.1	PERFIS QUALIFICADOS	46
5.2.2	NÚMERO DE PESSOAS NECESSÁRIO POR TAREFA	46
5.2.3	IDENTIFICAÇÃO E AUTENTICAÇÃO PARA CADA PERFIL	46
5.3	CONTROLES DE PESSOAL.....	47
5.3.1	ANTECEDENTES, QUALIFICAÇÃO, EXPERIÊNCIA E REQUISITOS DE IDONEIDADE	47
5.3.2	PROCEDIMENTOS DE VERIFICAÇÃO DE ANTECEDENTES	47
5.3.3	REQUISITOS DE TREINAMENTO	48
5.3.4	FREQUÊNCIA E REQUISITOS PARA RECICLAGEM TÉCNICA	48
5.3.5	FREQUÊNCIA E SEQUÊNCIA DE RODÍZIO DE CARGOS	48
5.3.6	SANÇÕES PARA AÇÕES NÃO AUTORIZADAS	48
5.3.7	REQUISITOS PARA CONTRATAÇÃO DE PESSOAL.....	49
5.3.8	DOCUMENTAÇÃO FORNECIDA AO PESSOAL.....	49
6	CONTROLES TÉCNICOS DE SEGURANÇA	49
6.1	GERAÇÃO E INSTALAÇÃO DO PAR DE CHAVES.....	49
6.1.1	GERAÇÃO DO PAR DE CHAVES	49
6.1.2	ENTREGA DA CHAVE PRIVADA À ENTIDADE TITULAR.....	50

6.1.3	ENTREGA DA CHAVE PÚBLICA PARA EMISSOR DE CERTIFICADO.....	50
6.1.4	DISPONIBILIZAÇÃO DE CHAVE PÚBLICA DA AC SAFEWEB PARA USUÁRIOS.....	50
6.1.5	TAMANHOS DE CHAVE.....	51
6.1.6	GERAÇÃO DE PARÂMETROS DE CHAVES ASSIMÉTRICAS.....	51
6.1.7	VERIFICAÇÃO DE QUALIDADE DOS PARÂMETROS.....	51
6.1.8	GERAÇÃO DE CHAVE POR HARDWARE OU SOFTWARE.....	51
6.1.9	PROPÓSITO DE USO DE CHAVE (conforme o campo "key usage" na X.509 v3).....	51
6.2	PROTEÇÃO DA CHAVE PRIVADA.....	51
6.2.1	PADRÕES PARA MÓDULO CRIPTOGRÁFICO.....	52
6.2.2	CONTROLE "N de M" PARA CHAVE PRIVADA.....	52
6.2.3	RECUPERAÇÃO (escrow) DE CHAVE PRIVADA.....	52
6.2.4	CÓPIA DE SEGURANÇA (backup) DE CHAVE PRIVADA.....	52
6.2.5	ARQUIVAMENTO DE CHAVE PRIVADA.....	53
6.2.6	INSERÇÃO DE CHAVE PRIVADA EM MÓDULO CRIPTOGRÁFICO.....	53
6.2.7	MÉTODO DE ATIVAÇÃO DE CHAVE PRIVADA.....	53
6.2.8	MÉTODO DE DESATIVAÇÃO DE CHAVE PRIVADA.....	53
6.2.9	MÉTODO DE DESTRUIÇÃO DE CHAVE PRIVADA.....	53
6.3	OUTROS ASPECTOS DO GERENCIAMENTO DO PAR DE CHAVES.....	53
6.3.1	ARQUIVAMENTO DE CHAVE PÚBLICA.....	53
6.3.2	PERÍODOS DE USO PARA CHAVES PÚBLICAS E PRIVADAS.....	54
6.4	DADOS DE ATIVAÇÃO.....	54
6.4.1	GERAÇÃO E INSTALAÇÃO DOS DADOS DE ATIVAÇÃO.....	54
6.4.2	PROTEÇÃO DOS DADOS DE ATIVAÇÃO.....	54
6.4.3	OUTROS ASPECTOS DOS DADOS DE ATIVAÇÃO.....	54
6.5	CONTROLES DE SEGURANÇA COMPUTACIONAL.....	55
6.5.1	REQUISITOS TÉCNICOS ESPECÍFICOS DE SEGURANÇA COMPUTACIONAL.....	55
6.5.2	CLASSIFICAÇÃO DA SEGURANÇA COMPUTACIONAL.....	55
6.5.3	CONTROLES DE SEGURANÇA PARA AS AUTORIDADES DE REGISTRO.....	56
6.6	CONTROLES TÉCNICOS DO CICLO DE VIDA.....	58
6.6.1	CONTROLES DE DESENVOLVIMENTO DE SISTEMA.....	58
6.6.2	CONTROLES DE GERENCIAMENTO DE SEGURANÇA.....	58
6.6.3	CLASSIFICAÇÕES DE SEGURANÇA DE CICLO DE VIDA.....	58
6.6.4	CONTROLES NA GERAÇÃO DE LCR.....	59
6.7	CONTROLES DE SEGURANÇA DE REDE.....	59
6.7.1	DIRETRIZES GERAIS.....	59
6.7.2	FIREWALL.....	59
6.7.3	SISTEMA DE DETECÇÃO DE INTRUSÃO – IDS.....	60
6.7.4	REGISTRO DE ACESSOS NÃO AUTORIZADOS À REDE.....	60
6.8	CONTROLES DE ENGENHARIA DO MÓDULO CRIPTOGRÁFICO.....	60
7	PERFIS DE CERTIFICADO E LCR.....	60
7.1	DIRETRIZES GERAIS.....	60
7.2	PERFIL DO CERTIFICADO.....	60
7.2.1	NÚMERO (S) DE VERSÃO.....	61
7.2.2	EXTENSÕES DE CERTIFICADO.....	61
7.2.3	IDENTIFICADORES DE ALGORITMO.....	61
7.2.4	FORMATOS DE NOME.....	62
7.2.5	RESTRIÇÕES DE NOME.....	62
7.2.6	OID (OBJECT IDENTIFIER) DE DPC.....	63
7.2.7	USO DA EXTENSÃO "Policy Constraints".....	63

7.2.8	SINTAXE E SEMÂNTICA DOS QUALIFICADORES DE POLÍTICA.....	63
7.2.9	SEMÂNTICA DE PROCESSAMENTO PARA EXTENSÕES CRÍTICAS.....	63
7.3	PERFIL DE LCR.....	63
7.3.1	NÚMERO (s) DE VERSÃO	63
7.3.2	EXTENSÕES DE LCR E DE SUAS ENTRADAS.....	63
8	ADMINISTRAÇÃO DE ESPECIFICAÇÃO	64
8.1	PROCEDIMENTOS DE MUDANÇA DE ESPECIFICAÇÃO	64
8.2	POLÍTICAS DE PUBLICAÇÃO E NOTIFICAÇÃO.....	64
8.3	PROCEDIMENTOS DE APROVAÇÃO	64
9	DOCUMENTOS REFERENCIADOS	64
9.1	RESOLUÇÕES DO COMITÊ-GESTOR DA ICP-Brasil	64
9.2	INSTRUÇÕES NORMATIVAS DA AC RAIZ	65
9.3	DOCUMENTOS DA AC RAIZ	65
10	LISTA DE ACRÔNIMOS.....	65

CONTROLE DE ALTERAÇÕES

Versão	Data	Resolução que aprovou a alteração	Item Alterado
1.0	10/10/2017	N/A	Versão inicial

1 INTRODUÇÃO

1.1 VISÃO GERAL

1.1.1 Esta Declaração de Práticas de Certificação – DPC, constitui os requisitos mínimos, obrigatoriamente observados pela Autoridade Certificadora - AC Safeweb, integrante da Infraestrutura de Chaves Públicas Brasileira (ICP Brasil) e descreve as práticas e os procedimentos utilizados pela AC Safeweb na execução de seus serviços de certificação digital.

1.1.2 Esta DPC adota a mesma estrutura utilizada no DOC-ICP-05, do Comitê Gestor da ICP-Brasil, que estabelece os REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DE CERTIFICAÇÃO DAS AUTORIDADES CERTIFICADORAS DA ICP-BRASIL [10].

1.1.3 A AC Safeweb está credenciada em nível imediatamente subsequente ao da AC Raiz da ICP-Brasil. O certificado da AC Safeweb contém a chave pública correspondente à sua chave privada, utilizada para assinar sua Lista de Certificados Revogados (LCR) e para assinar os certificados de AC de nível imediatamente subsequente (AC Subsequente).

1.1.4 O certificado da AC Safeweb é usado na emissão de certificados digitais de AC Subsequentes, com o objetivo de identificar as AC de nível imediatamente subsequente ao seu, referidas neste documento como AC Subsequente. Para regulamentar uso específico dos certificados emitidos pela AC Safeweb são publicadas Políticas de Certificado disponíveis em página web: <http://www.safeweb.com.br/ac/repositorio>.

1.2 IDENTIFICAÇÃO

1.2.1 Este documento é chamado “Declaração de Práticas de Certificação da Autoridade Certificadora Safeweb”, referido a seguir simplesmente como "DPC - AC Safeweb " e descreve as práticas e os procedimentos empregados por essa AC no âmbito da ICP-Brasil.

1.2.2 O OID da DPC - AC Safeweb, atribuído pela AC Raiz após conclusão do seu processo de credenciamento, é **2.16.76.1.1.84**.

1.3 COMUNIDADE E APLICABILIDADE

1.3.1 AUTORIDADE CERTIFICADORA - AC

Esta DPC se refere à AC Safeweb e encontra-se publicada em sua página web www.safeweb.com.br. A AC Safeweb está no nível imediatamente subsequente ao da Autoridade Certificadora Raiz da ICP-Brasil (AC Raiz).

1.3.2 AUTORIDADE DE REGISTRO - AR

1.3.2.1 Os dados a seguir, referentes às Autoridades de Registro – AR, utilizadas pela AC Safeweb para os processos de recebimento, validação e encaminhamento de solicitações de emissão ou de revogação de certificados digitais de Autoridades Certificadoras Subsequentes – AC Subsequente e identificação das organizações solicitantes, estão relacionadas na página da AC Safeweb www.safeweb.com.br que contém as seguintes informações:

- a) relação de todas as ARs credenciadas, com informações sobre as PCs que praticam;
- b) para cada AR credenciada, relação dos endereços de todas as instalações técnicas, autorizadas a funcionar pela AC Raiz;
- c) para cada AR credenciada, relação de eventuais postos provisórios autorizados a funcionar pela AC Raiz, com data de criação e encerramento de atividades;
- d) relação de AR que tenha se descredenciado da cadeia da AC, com respectivas datas do descredenciamento;
- e) relação de instalações técnicas de AR credenciada, que tenham deixado de operar, com respectivas datas de encerramento das atividades;
- f) acordos operacionais celebrados pelas ARs vinculadas com outras ARs da ICP-Brasil, se for o caso.

1.3.2.2. A AC Safeweb mantém as informações acima sempre atualizadas.

1.3.3 PRESTADOR DE SERVIÇOS DE SUPORTE – PSS

1.3.3.1 Os Prestadores de Serviços de Suporte vinculados à AC Safeweb estão relacionados na página www.safeweb.com.br.

1.3.3.2 PSS são entidades utilizadas pela AC Safeweb ou pelas AR Vinculadas para desempenhar atividade descrita nesta DPC e se classificam em três categorias, conforme o tipo de atividade prestada:

- a) disponibilização de infraestrutura física e lógica;
- b) disponibilização de recursos humanos especializados; ou
- c) disponibilização de infraestrutura física e lógica e de recursos humanos especializados.

1.3.3.3 AC Safeweb mantém as informações acima sempre atualizadas.

1.3.4 TITULARES DE CERTIFICADO

Apenas pessoas jurídicas podem ser titulares de certificados de AC Subsequente emitidos pela AC Safeweb.

1.3.5 APLICABILIDADE

Os certificados emitidos pela AC Safeweb tem sua utilização exclusiva para assinatura de certificados digitais de AC de nível imediatamente subsequente - AC Subsequente - ao seu e de sua Lista de Certificados Revogados (LCR).

1.4 DADOS DE CONTATO

Dúvidas decorrentes da leitura desta DPC - AC Safeweb e que não sejam respondidas mediante a leitura da página www.safeweb.com.br podem ser esclarecidas contatando:

Contato: Setor de Compliance

Telefone: + 55 51 3018-0300

E-mail: compliance@safeweb.com.br

Safeweb Segurança da Informação Ltda.

Endereço: Av. Princesa Isabel, 828 – Porto Alegre/RS – CEP 90620-000

2 DISPOSIÇÕES GERAIS

2.1 OBRIGAÇÕES E DIREITOS

Nos itens a seguir estão descritas as obrigações e direitos gerais das entidades envolvidas.

2.1.1 OBRIGAÇÕES DA AUTORIDADE CERTIFICADORA

As obrigações da AC Safeweb são as abaixo relacionadas:

- a) operar de acordo com esta DPC - AC Safeweb;
- b) gerar e gerenciar os seus pares de chaves criptográficas;
- c) assegurar a proteção de suas chaves privadas;
- d) notificar a AC Raiz, emitente do seu certificado, quando ocorrer comprometimento de sua chave privada e solicitar a imediata revogação desse certificado;

- e) notificar os seus usuários quando ocorrer: suspeita de comprometimento de sua chave, emissão de novo par de chaves e correspondente certificado, ou encerramento de suas atividades;
- f) distribuir o seu próprio certificado;
- g) emitir, expedir e distribuir os certificados de AC de nível imediatamente subsequente;
- h) informar a emissão do certificado ao respectivo solicitante;
- i) revogar os certificados por ela emitidos;
- j) emitir, gerenciar e publicar sua LCR e quando aplicável, disponibilizar consulta *online* de situação do certificado (OCSP - *Online Certificate Status Protocol*), quando aplicável;
- k) publicar em sua página web esta DPC - AC Safeweb;
- l) publicar, em sua página web, as informações definidas no item 2.6.1.2 deste documento;
- m) publicar, em sua página web, informações sobre o descredenciamento de AR bem como sobre extinção de instalação técnica;
- n) utilizar protocolo de comunicação seguro ao disponibilizar serviços para os solicitantes ou usuários de certificados digitais via web;
- o) identificar e registrar todas as ações executadas, conforme as normas, práticas e regras estabelecidas pelo Comitê Gestor da ICP-Brasil;
- p) adotar as medidas de segurança e controle previstas na DPC - AC Safeweb e Política de Segurança (PS) implementadas, envolvendo seus processos, procedimentos e atividades, observadas as normas, critérios, práticas e procedimentos da ICP-Brasil;
- q) manter a conformidade dos seus processos, procedimentos e atividades com as normas, práticas e regras da ICP-Brasil;
- r) manter e garantir a integridade, o sigilo e a segurança da informação por ela tratada;
- s) manter e testar anualmente seu Plano de Continuidade do Negócio (PCN);
- t) manter contrato de seguro de cobertura de responsabilidade civil decorrente das atividades de certificação digital e de registro, com cobertura suficiente e compatível com o risco dessas atividades, e exigir sua manutenção pelas ACs de nível subsequente ao seu, quando estas estiverem obrigadas a contratá-lo, de acordo com as normas do Comitê Gestor da ICP-Brasil;
- u) informar as terceiras parte e titulares de certificado acerca das garantias, coberturas, condicionantes e limitações estipuladas pela apólice de seguro de responsabilidade civil contratada pela AC Safeweb;
- v) informar à AC Raiz, mensalmente, a quantidade de certificados digitais emitidos;
- w) não emitir certificado com prazo de validade que se estenda além do prazo de validade de seu

próprio certificado.

- x) tomar as medidas cabíveis para assegurar que usuários e demais entidades envolvidas tenham conhecimento de seus respectivos direitos e obrigações;
- y) fiscalizar e auditar as ARs vinculadas e os prestadores de serviço que lhe sejam vinculados, em conformidade com as políticas, normas e procedimentos da ICP-Brasil.

2.1.2 OBRIGAÇÕES DAS AUTORIDADES DE REGISTRO – AR

As obrigações das ARs vinculadas são as abaixo relacionadas:

- a) receber solicitações de emissão ou de revogação de certificados;
- b) confirmar a identidade do solicitante e a validade da solicitação;
- c) encaminhar a solicitação de emissão ou de revogação de certificado à AC Safeweb utilizando protocolo de comunicação seguro, conforme padrão definido no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP BRASIL [1];
- d) informar aos respectivos titulares a emissão ou a revogação de seus certificados;
- e) disponibilizar os certificados emitidos pela AC Safeweb aos seus respectivos solicitantes;
- f) identificar e registrar todas as ações executadas, conforme as normas, práticas e regras estabelecidas pelo CG da ICP-Brasil;
- g) manter a conformidade dos seus processos, procedimentos e atividades com as normas, critérios, práticas e regras estabelecidas pela AC Safeweb e pela ICP-Brasil, em especial com o contido no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS ARs DA ICP-BRASIL [1];
- h) manter e garantir a segurança da informação por ela tratada, de acordo com o estabelecido nas normas, critérios, práticas e procedimentos da ICP-Brasil;
- i) manter e testar anualmente seu Plano de Continuidade do Negócio - PCN;
- j) proceder ao reconhecimento das assinaturas e da validade dos documentos apresentados na forma dos itens 3.1.9, 3.1.10 e 3.1.11;
- k) garantir que todas as aprovações de solicitação de certificados sejam realizadas em instalações técnicas autorizadas a funcionar como ARs vinculadas credenciadas;
- l) obedecer estritamente a esta DCP e, bem como respeitar a legislação aplicável, incluindo as regras definidas pelo CG da ICP-Brasil.

2.1.3 OBRIGAÇÕES DO TITULAR DO CERTIFICADO

Constituem-se obrigações do titular de certificado emitido pela AC Safeweb:

- a) fornecer, de modo completo e preciso, todas as informações necessárias para sua identificação;
- b) garantir a proteção e o sigilo de suas chaves privadas, senhas e dispositivos criptográficos;
- c) utilizar os seus certificados e chaves privadas de modo apropriado;
- d) conhecer os seus direitos e obrigações, contemplados pela DPC - AC Safeweb e por outros documentos aplicáveis da ICP-Brasil;
- e) informar à AC Safeweb qualquer comprometimento de sua chave privada e solicitar a imediata revogação do certificado correspondente;
- f) apresentação dos originais e fornecimento de cópias autênticas dos documentos que forem exigidos para emissão do certificado;
- g) responsabilizar-se por todos os atos praticados com utilização do referido certificado e sua correspondente chave privada;
- h) utilizar obrigatoriamente senha para proteção da chave privativa;
- i) obedecer estritamente a esta DPC - AC Safeweb bem como respeitar a legislação vigente, incluindo, mas não se limitando, as regras definidas pelo CG da ICP-Brasil e as obrigações contratuais assumidas perante a AC Safeweb e a AR que esteja vinculada.

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

2.1.4 DIREITOS DA TERCEIRA PARTE - RELYING PARTY

2.1.4.1 Considera-se terceira parte, a parte que confia no teor, validade e aplicabilidade do certificado digital.

2.1.4.2 Constituem direitos da terceira parte:

- a) recusar a utilização do certificado para fins diversos dos previstos nesta DPC correspondente;
- b) verificar, a qualquer tempo, a validade do certificado. Um certificado emitido por AC integrante da ICP-Brasil é considerado válido quando:
 - i. não constar da LCR da AC emitente;
 - ii. não estiver expirado; e
 - iii. puder ser verificado com o uso de certificado válido da AC emitente.

2.1.4.3 O não exercício desses direitos não afasta a responsabilidade da AC Safeweb e do titular do certificado.

2.1.5 OBRIGAÇÕES DO REPOSITÓRIO DA AC SAFEWEB

As obrigações da AC Safeweb em relação ao seu repositório são:

- a) disponibilizar, logo após a sua emissão, os certificados emitidos pela AC Safeweb e a sua LCR;
- b) estar disponível para consulta durante 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana;
- c) implementar os recursos necessários para a garantia da segurança dos dados nele armazenados; e
- d) disponibilizar verificação on-line do status do certificado ou outro mecanismo de atualização de status aprovado pela ICP-Brasil, quando aplicável por força ou contratação específica.

2.2 RESPONSABILIDADES

2.2.1 RESPONSABILIDADES DA AC SAFEWEB

2.2.1.1 A AC Safeweb responde pelos danos a que der causa.

2.2.1.2 A AC Safeweb responde solidariamente pelos atos das entidades de sua cadeia de certificação: AR e PSS.

2.2.1.3 Não se aplica.

2.2.2 RESPONSABILIDADES DAS AUTORIDADES DE REGISTRO VINCULADAS

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

2.3 RESPONSABILIDADE FINANCEIRA

2.3.1 INDENIZAÇÕES DEVIDAS PELA TERCEIRA PARTE - *RELYING PARTY*

A terceira parte - *Relying Party* - não é responsável perante a AC Safeweb e AR Vinculada, exceto na hipótese de prática de ato ilícito. Nesse caso, essa terceira parte responderá em quaisquer esferas de direito, e deverá indenizar a AC Safeweb e/ou os titulares de seus certificados pelos danos a que der causa em decorrência de omissão ou ação não conforme com a legislação aplicável.

2.3.2 RELAÇÕES FIDUCIÁRIAS

2.3.2.1 A AC Safeweb ou AR vinculada indenizará integralmente os danos a que comprovadamente der causa. Em situações justificáveis, pode ocorrer limitação da indenização,

quando o titular do certificado for pessoa jurídica.

2.3.2.2 Os detalhes das condições de aplicação da Política de Garantia estão disponíveis na página web www.safeweb.com.br.

2.3.3 PROCESSOS ADMINISTRATIVOS

O titular do certificado que julgar-se prejudicado em decorrência do uso do certificado digital terá o direito de comunicar à AC Safeweb que deseja a indenização prevista no documento Política de Garantia. Serão observadas as seguintes condições:

- a) nos casos de perdas e danos decorrentes de comprometimento da chave privada da AC Safeweb, tal comprometimento deverá ter sido provado por perícia realizada por perito especializado e independente, escolhido em consenso;
- b) nos casos de erro na transcrição, o titular do certificado não poderá requerer qualquer indenização quando houver aceitado o certificado.

2.4 INTERPRETAÇÃO E EXECUÇÃO

2.4.1 LEGISLAÇÃO

Esta DPC - AC Safeweb obedece às leis da República Federativa do Brasil e atende aos requisitos da legislação em vigor, incluindo, mas não se limitando, a Medida Provisória nº 2200-2, de 24 de agosto de 2001, pelas resoluções do Comitê Gestor da ICP-Brasil, bem como as demais leis em vigor no Brasil.

2.4.2 FORMA DE INTERPRETAÇÃO E NOTIFICAÇÃO

2.4.2.1 Caso esta DPC - AC Safeweb ou alguma de suas disposições venha a ser considerada ou declarada inválida, ilegal ou não aplicável por lei, a AC Safeweb tomará de imediato às medidas necessárias para adequar esta DPC ou a disposição em questão às exigências legais.

2.4.2.2 As notificações, solicitações ou quaisquer outras comunicações necessárias serão realizadas pela AC Safeweb vinculadas por mensagem eletrônica (*e-mail*) a ser enviada para o endereço eletrônico fornecido pelo solicitante no formulário de solicitação. A mensagem eletrônica (*e-mail*) será considerada como recebida quando enviado a esse endereço.

2.4.2.3 A DPC da AC Safeweb na ICP-Brasil, não prevalece sobre as normas, critérios, práticas e procedimentos da ICP-Brasil.

2.4.3 PROCEDIMENTO DE SOLUÇÃO DE DISPUTA

2.4.3.1 Em caso de conflito entre esta DPC - AC Safeweb e outras declarações, políticas, planos, acordos, contratos ou documentos, esta DPC prevalecerá.

2.4.3.2 Esta DPC - AC Safeweb não prevalecerá sobre as normas, critérios, práticas e procedimentos da ICP-Brasil.

2.4.3.3 Os casos omissos deverão ser encaminhados para apreciação da AC Raiz.

2.5 TARIFAS DE SERVIÇOS

Pelo certificado emitido será cobrado o valor estabelecido contratualmente.

2.5.1 TARIFAS DE EMISSÃO E RENOVAÇÃO DE CERTIFICADOS

Pela emissão e renovação do certificado será cobrado o valor estabelecido contratualmente.

2.5.2 TARIFAS DE ACESSO AO CERTIFICADO

Pelo acesso ao certificado será cobrado o valor estabelecido contratualmente.

2.5.3 TARIFAS DE REVOGAÇÃO OU DE ACESSO A INFORMAÇÃO DE STATUS

Não há tarifas previstas pela AC Safeweb para a revogação. Pelo acesso a informação de status a tarifa é variável conforme definição interna da AC Safeweb.

2.5.4 TARIFAS PARA OUTROS SERVIÇOS

Para outros serviços será cobrado o valor estabelecido contratualmente.

2.5.5 POLÍTICA DE REEMBOLSO

Na hipótese de necessidade de o certificado ser revogado por motivo de comprometimento da chave privada da AC Safeweb ou da mídia armazenadora da chave privada da AC Safeweb, ou ainda quando constatada a emissão imprópria ou defeituosa, com culpa da AC Safeweb, será emitido outro certificado em substituição, sem cobrança ao titular do mesmo. Não haverá reembolso no caso de emissão sem custo de outro certificado em substituição.

2.6 PUBLICAÇÃO E REPOSITÓRIO

2.6.1 PUBLICAÇÃO DE INFORMAÇÃO DA AC SAFEWEB

2.6.1.1 A AC Safeweb publica e mantém disponível em seu site www.safeweb.com.br informações com disponibilidade mínima de 99,5% (noventa e nove vírgula cinco por cento) do mês, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.

2.6.1.2 As seguintes informações, no mínimo, são publicadas pela AC Safeweb em página web:

- a) Seu próprio certificado;
- b) Suas LCRs;
- c) Sua DPC;
- d) Uma relação, regularmente atualizada, contendo as ARs vinculadas e seus respectivos endereços de instalações técnicas em funcionamento;
- e) Uma relação, regularmente atualizada, das ARs vinculadas que tenham celebrado acordos operacionais com outras ARs da ICP-Brasil, contendo informações sobre os pontos do acordo que sejam de interesse dos titulares e solicitantes de certificado; e
- f) Uma relação, regularmente atualizada, dos PSS vinculados.

2.6.2 FREQUÊNCIA DE PUBLICAÇÃO

Certificados da AC Safeweb são publicados imediatamente após sua emissão. A publicação da LCR se dá conforme determinado na PC correspondente. As versões ou alterações desta DPC, assim como os endereços das instalações técnicas das ARs vinculadas, são atualizados no web site da AC Safeweb após aprovação da AC Raiz da ICP-Brasil.

2.6.3 CONTROLES DE ACESSO

Somente os funcionários competentes e designados especialmente para esse fim poderão alterar as informações constantes nesta DPC. Somente a AC Safeweb, por seus funcionários competentes e designados especialmente para esse fim, pode efetuar as necessárias atualizações de sua LCR. Caso se faça necessário modificar os dados contidos nos certificados, será necessária a revogação dos certificados. Não há restrições para leitura desta DPC e das LCRs.

Todas as informações disponibilizadas pela AC Safeweb, conforme o item 2.6.1 desta DPC, estão disponíveis para leitura sem restrições.

2.6.4 REPOSITÓRIOS

2.6.4.1 A AC responsável deve disponibilizar 02 (dois) repositórios, em infraestruturas de rede

segregadas, para distribuição de LCR.

2.6.4.2 O repositório da AC Safeweb pode ser acessado utilizando o protocolo de acesso http ou https, através da página www.safeweb.com.br. Os repositórios estão disponíveis em no mínimo 99,5% (noventa e nove vírgula cinco por cento) do mês, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana. Além disso, obedecem aos requisitos de segurança estabelecidos no item 5 desta DPC.

2.7 FISCALIZAÇÃO E AUDITORIA DE CONFORMIDADE

2.7.1 As fiscalizações e auditorias realizadas no âmbito da ICP-Brasil têm por objetivo verificar se os processos, procedimentos e atividades das entidades integrantes da ICP-Brasil estão em conformidade com suas respectivas DPC, PS e demais normas e procedimentos estabelecidos pela ICP-Brasil e com os princípios e critérios definidos pelo WebTrust.

2.7.2 As fiscalizações das entidades integrantes da ICP-Brasil são realizadas pela AC Raiz, por meio de servidores de seu quadro próprio, a qualquer tempo, sem aviso prévio, observado o disposto no documento CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [2].

2.7.3 Com exceção da auditoria da própria AC Raiz, que é de responsabilidade do Comitê Gestor da ICP-Brasil, as auditorias das entidades integrantes da ICP-Brasil são realizadas pela AC Raiz, por meio de servidores de seu quadro próprio, ou por terceiros por ela autorizados, observado o disposto no documento CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL [3].

2.7.4 A AC Safeweb recebeu auditoria prévia da AC Raiz para fins de credenciamento na ICP-Brasil e é auditada anualmente, para fins de manutenção do credenciamento, com base no disposto no documento CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL [3]. Esse documento trata do objetivo, frequência e abrangência das auditorias, da identidade e qualificação do auditor e demais temas correlacionados.

2.7.5 A AC Safeweb e as entidades da ICP-Brasil a ela diretamente vinculadas – AR Vinculadas e PSS, receberam auditoria prévia, para fins de credenciamento, sendo a AC Safeweb responsável pela realização de auditorias anuais nessas entidades, para fins de manutenção de credenciamento, conforme disposto no documento citado no parágrafo anterior.

2.8 SIGILO

2.8.1 DISPOSIÇÕES GERAIS

2.8.1.1 A chave privada de assinatura digital da AC Safeweb foi gerada e é mantida pela própria AC Safeweb, que assegura o seu sigilo. A divulgação ou utilização indevida da chave privada de assinatura pela AC é de sua inteira responsabilidade.

2.8.1.2 Os responsáveis pelo uso de certificados emitidos para pessoas jurídicas, na figura de AC Subsequente, terão as atribuições de geração, manutenção e sigilo de suas respectivas chaves privadas, correspondente à chave pública contida no certificado, bem como, pela divulgação ou utilização indevidas dessas mesmas chaves.

2.8.1.3 Não se aplica.

2.8.2 TIPOS DE INFORMAÇÕES SIGILOSAS

2.8.2.1 Todas as informações coletadas, geradas, transmitidas e mantidas pela AC Safeweb e pelas ARs vinculadas são consideradas sigilosas.

2.8.2.2 Como princípio geral, nenhum documento, informação ou registro fornecido à AC Safeweb será divulgado.

2.8.3 TIPOS DE INFORMAÇÕES NÃO SIGILOSAS

Não são consideradas como informações sigilosas pela AC Safeweb e pela AR Vinculada:

- a) os certificados e as LCR emitidos pela AC Safeweb;
- b) as informações corporativas ou pessoais que façam parte de certificados ou de diretórios públicos;
- c) esta DPC;
- d) versões públicas de Políticas de Segurança;
- e) resultados finais de auditoria; e
- f) Termo de Titularidade ou solicitação de emissão de certificado.

A AC Safeweb e a AR Vinculada julgam confidenciais os dados fornecidos pelo solicitante que não constem no certificado. Contudo, tais dados não são considerados confidenciais quando:

- a) o solicitante autorize formalmente a sua divulgação;
- b) depois de entregue pelo solicitante, os dados sejam obtidos ou possam ter sido obtidos legalmente de terceiro (s) sem quaisquer restrições;
- c) tenham a exibição ordenada por determinação judicial ou autoridade competente com poder de polícia; se possível, a exigência poderá ser comunicada de imediato ao solicitante.

Os motivos que justificaram a não emissão de um certificado poderão ser mantidos confidenciais pela AC Safeweb e pela AR Vinculada, salvo na hipótese da alínea "c".

2.8.4 DIVULGAÇÃO DE INFORMAÇÃO DE REVOGAÇÃO DE CERTIFICADO

2.8.4.1 A AC Safeweb disponibiliza permanentemente em seu site www.safeweb.com.br informações sobre revogação de certificados através de sua LCR.

2.8.4.2 Os motivos que justificaram a revogação são sempre informados ao titular ou responsável pelo certificado e mantidos confidenciais pela AC Safeweb, exceto quando o titular do certificado revogado solicitar ou autorizar expressamente a sua divulgação a terceiros, ou quando tais motivos sejam requisitados por determinação judicial ou de autoridade competente, caso em que a AC Safeweb estiver obrigada a divulgá-los, poderá comunicar previamente ao titular do certificado a existência de tal determinação.

2.8.4.3 A suspensão de certificados não é admitida no âmbito da ICP-Brasil.

2.8.5 QUEBRA DE SIGILO POR MOTIVOS LEGAIS

2.8.5.1 As informações fornecidas pelo solicitante ou titular do certificado, bem como os documentos e registros relativos ao solicitante, ao titular do certificado, à solicitação ou ao certificado emitido não são mantidos sob sigilo pela AC Safeweb quando a lei prevê a sua publicidade e/ou divulgação ou por ordem judicial ou de autoridade competente.

2.8.6 INFORMAÇÕES A TERCEIROS

2.8.6.1 Como diretriz geral, nenhum documento, informação ou registro sob a guarda da AC Safeweb será fornecido a terceiros, exceto quando o requerente o solicite por meio de instrumento devidamente constituído, seja autorizado para fazê-lo e esteja corretamente identificado.

2.8.7 DIVULGAÇÃO POR SOLICITAÇÃO DO TITULAR

2.8.7.1 A qualquer tempo o titular do certificado, ou seu mandatário, terá acesso aos dados que lhe dizem respeito e que estejam sob a guarda da AC.

2.8.7.2 Qualquer liberação de informação pela AC Safeweb somente será permitida mediante autorização formal do titular do certificado. Essa autorização pode ser feita no ato da solicitação do certificado, no próprio formulário de solicitação, ou posteriormente, por documento legalmente aceito.

2.8.8 OUTRAS CIRCUNSTÂNCIAS DE DIVULGAÇÃO DE INFORMAÇÃO

2.8.8.1 Não se aplica.

2.9 DIREITOS DE PROPRIEDADE INTELECTUAL

2.9.1 A Safeweb Segurança da Informação Ltda. detém todos os direitos de propriedade intelectual sobre ideias, conceitos, técnicas e invenções, processos e/ou obras, incluídas ou utilizadas nos produtos e serviços fornecidos por AC Safeweb nos termos dessa DPC.

3 IDENTIFICAÇÃO E AUTENTICAÇÃO

3.1 REGISTRO INICIAL

3.1.1 DISPOSIÇÕES GERAIS

3.1.1.1 Neste item e nos itens seguintes estão descritos em detalhes os requisitos e procedimentos utilizados pelas ARs vinculadas a AC Safeweb para a realização dos seguintes processos:

a) VALIDAÇÃO DA SOLICITAÇÃO DE CERTIFICADO: compreende as etapas abaixo, realizadas mediante a presença física do interessado, com base nos documentos de identificação citados nos itens 3.1.9, 3.1.10 e 3.1.11:

i. Confirmação da identidade de um indivíduo: comprovação de que a pessoa que se apresenta como titular do certificado de pessoa física é realmente aquela cujos dados constam na documentação e/ou biometria apresentada vedada qualquer espécie de procuração para tal fim. No caso de pessoa jurídica, comprovar que a pessoa física que se apresenta como a sua representante é realmente aquela cujos dados constam na documentação apresentada, admitida a procuração apenas se o ato constitutivo previr expressamente tal possibilidade, devendo-se, para tanto, revestir-se da forma pública, com poderes específicos para atuar perante a ICP-Brasil e com prazo de validade de até 90 (noventa) dias. O responsável pela utilização do certificado digital de pessoa jurídica deve comparecer presencialmente, vedada qualquer espécie de procuração para tal fim.

ii. Confirmação da identidade de uma organização: comprovação de que os documentos apresentados referem-se, efetivamente à pessoa jurídica titular do certificado e de que a pessoa que se apresenta como representante legal da pessoa jurídica realmente possui tal atribuição;

iii. Emissão do certificado: conferência dos dados da solicitação do certificado com os constantes nos documentos apresentados e liberação da emissão do certificado no sistema da AC.

b) VERIFICAÇÃO DA SOLICITAÇÃO DE CERTIFICADO: confirmação da validação realizada observando que deve ser executada, obrigatoriamente:

- i. Por agente de registro distinto do que executou a etapa de validação;
- ii. Em uma das instalações técnicas da AR devidamente autorizadas a funcionar pela AC Raiz;
- iii. Somente após o recebimento, na instalação técnica da AR, de cópia da documentação apresentada na etapa de validação;
- iv. Antes do início da validade do certificado, devendo esse ser revogado automaticamente caso a verificação não tenha ocorrido até o início de sua validade.

3.1.1.2 O processo de validação ao ser realizado pelo agente de registro fora do ambiente físico da AR, deverá utilizar ambiente computacional auditável e devidamente registrado no inventário de hardware e softwares da AR.

3.1.1.3 Não se aplica.

3.1.1.4 Deve ser mantido arquivo com as cópias de todos os documentos utilizados para confirmação da identidade de uma organização e/ou de um indivíduo. Tais cópias poderão ser mantidas em papel ou em forma digitalizada, observadas as condições definidas no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS ARs DA ICP-BRASIL [1].

3.1.1.4.1 Não se aplica.

3.1.1.5 Não se aplica.

3.1.1.6 Não se aplica.

3.1.1.7 Não se aplica.

3.1.1.8 Não se aplica.

3.1.2 TIPOS DE NOMES

3.1.2.1 A AC Safeweb emite certificados com nomes que possibilitam determinar a identidade da pessoa ou organização a que se referem. Para tanto utiliza o "*distinguished name*" do padrão ITU X.500, endereços de correio eletrônico ou endereços de página Web (URL).

3.1.2.2 Um certificado emitido para uma AC Subsequente não inclui o nome da pessoa responsável.

3.1.3 NECESSIDADE DE NOMES SIGNIFICATIVOS

3.1.3.1 Os certificados emitidos pela AC Safeweb exigem o uso de nomes significativos que possibilitam determinar univocamente a identidade da pessoa ou da organização titular do certificado a que se referem.

3.1.4 REGRAS PARA INTERPRETAÇÃO DE VÁRIOS TIPOS DE NOMES

3.1.4.1 Não se aplica.

3.1.5 UNICIDADE DE NOMES

3.1.5.1 Os identificadores do tipo "*Distinguished Name*" (DN) são únicos para cada entidade titular de certificado, no âmbito da AC Safeweb. Números ou letras adicionais podem ser incluídos ao nome de cada entidade para assegurar a unicidade do campo DN.

3.1.6 PROCEDIMENTO PARA RESOLVER DISPUTA DE NOMES

3.1.6.1 A AC Safeweb reserva-se no direito de tomar todas as decisões na hipótese de haver disputa de nomes decorrente da igualdade de nomes entre os solicitantes diversos de certificados. Durante o processo de confirmação de identidade, cabe a entidade solicitante do certificado provar o seu direito de uso de um nome específico.

3.1.7 RECONHECIMENTO, AUTENTICAÇÃO E PAPEL DE MARCAS REGISTRADAS

3.1.7.1 Os processos de tratamento, reconhecimento e confirmações de autenticidade de marcas registradas são executados de acordo com a legislação em vigor.

3.1.8 MÉTODO PARA COMPROVAR A POSSE DE CHAVE PRIVADA

3.1.8.1 A confirmação de que a entidade solicitante possui a chave privada correspondente à chave pública para a qual está sendo solicitado o certificado digital é realizada seguindo o padrão RFC 2510, relativos à POP (*Proof of Possession*).

3.1.9 AUTENTICAÇÃO DA IDENTIDADE DE UM INDIVÍDUO

A confirmação da identidade é realizada mediante a presença física do interessado, com base em documentos de identificação legalmente aceitos e pelo processo de identificação biométrica da ICP-Brasil.

3.1.9.1 DOCUMENTOS PARA EFEITOS DE IDENTIFICAÇÃO DE UM INDIVÍDUO

Deverá ser apresentada a seguinte documentação, em sua versão original, para fins de identificação de um indivíduo solicitante de certificado:

- a) Cédula de Identidade ou Passaporte, se brasileiro;
- b) Carteira Nacional de Estrangeiro – CNE, se estrangeiro domiciliado no Brasil;
- c) Passaporte, se estrangeiro não domiciliado no Brasil;
- d) Comprovante de residência ou domicílio, emitido há no máximo 3 (três) meses da data da validação presencial;
- e) Ata ou procuração conferindo poderes ao responsável, quando aplicável;
- f) Fotografia da face do requerente de um certificado digital ICP-Brasil, conforme disposto no DOC-ICP-05.03 [11] e;
- g) Impressões digitais do requerente de um certificado digital ICP-Brasil, conforme disposto no DOC-ICP-05.03 [11].

NOTA 1: Entende-se como cédula de identidade os documentos emitidos pelas Secretarias de Segurança Pública bem como os que, por força de lei, equivalem a documento de identidade em todo o território nacional, desde que contenham fotografia.

NOTA 2: Entende-se como comprovante de residência ou de domicílio contas de concessionárias de serviços públicos, extratos bancários ou contrato de aluguel onde conste o nome do titular; na falta desses, declaração emitida pelo titular ou seu empregador.

NOTA 3: A emissão de certificados em nome dos absolutamente incapazes e dos relativamente incapazes observará o disposto na lei vigente.

NOTA 4: Caso não haja suficiente clareza no documento apresentado, a AR deve solicitar outro documento, preferencialmente a Carteira Nacional de Habilitação (CNH) ou o Passaporte Brasileiro.

NOTA 5: Deverão ser consultadas as bases de dados dos órgãos emissores da Carteira Nacional de Habilitação, e outras verificações documentais expressas no item 7 do documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP BRASIL [1].

NOTA 6: Caso haja divergência dos dados constantes do documento de identidade, a emissão do certificado digital deverá ser suspensa e o solicitante orientado a regularizar sua situação junto ao órgão responsável.

NOTA 7: Os documentos que possuem data de validade devem estar no prazo.

3.1.9.2 INFORMAÇÕES CONTIDAS NO CERTIFICADO EMITIDO PARA UM INDIVÍDUO

3.1.9.2.1 Não se aplica.

3.1.9.2.2 Não se aplica.

3.1.9.2.3 Não se aplica.

3.1.10 AUTENTICAÇÃO DA IDENTIDADE DE UMA ORGANIZAÇÃO

3.1.10.1 DISPOSIÇÕES GERAIS

3.1.10.1.1 Neste item são definidos os procedimentos empregados pelas ARs vinculadas para a confirmação da identidade de uma pessoa jurídica.

3.1.10.1.2 Em sendo o titular do certificado pessoa jurídica, é 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.

3.1.10.1.3 Deverá ser feita a confirmação da identidade da organização e das pessoas físicas, nos seguintes termos:

- a) apresentação do rol de documentos elencados no item 3.1.10.2;
- b) apresentação do rol de documentos elencados no item 3.1.9.1 do(s) representante(s) legal(is) da pessoa jurídica e do responsável pelo uso do certificado;
- c) presença física dos representantes legais e do responsável pelo uso do certificado, e assinatura do termo de titularidade de que trata o item 4.1.1.

3.1.10.2 DOCUMENTOS PARA EFEITOS DE IDENTIFICAÇÃO DE UMA ORGANIZAÇÃO

A confirmação da identidade de uma pessoa jurídica deverá ser feita mediante a apresentação de, no mínimo, os seguintes documentos:

- a) Relativos a sua habilitação jurídica:
 - i. se pessoa jurídica criada ou autorizada a sua criação por lei, cópia do ato constitutivo e CNPJ;
 - ii. se entidade privada:
 - 1. ato constitutivo, devidamente registrado no órgão competente; e
 - 2. documentos da eleição de seus administradores, quando aplicável, registrado no órgão competente;
- b) Relativos a sua habilitação fiscal:

- i. prova de inscrição no Cadastro Nacional de Pessoas Jurídicas – CNPJ; ou
- ii. prova de inscrição no Cadastro Específico do INSS – CEI.

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

3.1.10.3 INFORMAÇÕES CONTIDAS NO CERTIFICADO EMITIDO PARA UMA ORGANIZAÇÃO

3.1.10.3.1 Não se aplica.

3.1.10.3.2 Não se aplica.

3.1.11 AUTENTICAÇÃO DA IDENTIDADE DE EQUIPAMENTO, APLICAÇÃO OU CÓDIGO

3.1.11.1 DISPOSIÇÕES GERAIS

3.1.11.1.1 Não se aplica.

3.1.11.1.2 Não se aplica.

3.1.11.1.3 Não se aplica.

3.1.11.2 PROCEDIMENTOS PARA EFEITOS DE IDENTIFICAÇÃO DE UM EQUIPAMENTO, APLICAÇÃO OU CÓDIGO

3.1.11.2.1 Não se aplica

3.1.11.2.2 Não se aplica.

3.1.11.3 INFORMAÇÕES CONTIDAS NO CERTIFICADO EMITIDO PARA UM EQUIPAMENTO, APLICAÇÃO OU CÓDIGO

3.1.11.3.1 Não se aplica.

3.1.11.3.2 Não se aplica.

3.1.12. AUTENTICAÇÃO DE IDENTIFICAÇÃO DE EQUIPAMENTO PARA CERTIFICADO CFE-SAT

3.1.12.1 Não se aplica.

3.2 GERAÇÃO DE NOVO PAR DE CHAVES ANTES DA EXPIRAÇÃO DO ATUAL

3.2.1 No item seguinte estão estabelecidos os processos de identificação do solicitante pela AC Safeweb para a geração de novo par de chaves, e de seu correspondente certificado, antes da expiração do certificado vigente.

3.2.2 O processo descrito acima é conduzido através da adoção dos mesmos requisitos e procedimentos exigidos para a solicitação do certificado.

3.2.3 Não se aplica.

3.3 GERAÇÃO DE NOVO PAR DE CHAVES APÓS REVOGAÇÃO OU EXPIRAÇÃO

3.3.1 Após a revogação ou expiração do certificado, os procedimentos utilizados para confirmação da identidade do solicitante de novo certificado são os mesmos exigidos na solicitação inicial do certificado, na forma e prazo descritos nesta DPC.

3.3.2 Após a expiração ou revogação de certificado de AC de nível imediatamente subsequente ao da AC Safeweb, a AC Subsequente executa os processos regulares de geração de seu novo par de chaves.

3.4 SOLICITAÇÃO DE REVOGAÇÃO

3.4.1 A solicitação de revogação de certificado é realizada através de formulário específico, permitindo a identificação inequívoca do solicitante. A confirmação da identidade do solicitante é feita com base na confrontação de dados fornecidos na solicitação de revogação e os dados previamente cadastrados na AR. As solicitações de revogação de certificado são registradas.

4 REQUISITOS OPERACIONAIS

4.1 SOLICITAÇÃO DE CERTIFICADO

4.1.1 A solicitação de emissão de um Certificado Digital é feita mediante o preenchimento de formulário colocado à disposição do solicitante pela AR Vinculada. Toda referência a formulário deverá ser entendida também como referência a outras formas que a AR Vinculada possa vir a adotar. Dentre os requisitos e procedimentos operacionais estabelecidos pela AC Safeweb para as solicitações de emissão de certificado, estão:

- a) A comprovação de atributos de identificação constantes do certificado, conforme item 3.1;
- b) A autenticação do agente de registro responsável pelas solicitações de emissão e de revogação de certificados mediante o uso de certificado digital que tenha requisitos de segurança, no mínimo, equivalentes a de um certificado de tipo A3; e

c) Um termo de titularidade assinado pelo titular do certificado e um termo de responsabilidade assinado pelo responsável pelo uso do certificado, elaborados conforme o documento MODELO DE TERMO DE TITULARIDADE [4].

4.1.2. A solicitação de certificado para AC de nível imediatamente subsequente a AC Safeweb somente é possível após o processo de credenciamento e autorização de funcionamento da AC em questão, conforme documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6].

4.1.3. Não se aplica.

4.1.4. Nos casos do item 4.1.2, a AC Subsequente encaminha a solicitação de seu certificado à AC Safeweb por meio de seu(s) representante(s) legal(is), utilizando protocolo definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

4.2 EMISSÃO DE CERTIFICADO

4.2.1 Depois da validação da solicitação do certificado, de que trata o item 3.1.1.1, a AC Safeweb procede à emissão do certificado. O certificado emitido é inserido na relação de certificados emitidos pela AC Safeweb e cópia do certificado é entregue ao representante da AC.

4.2.2 Um certificado é considerado válido a partir do momento de sua emissão.

4.3 ACEITAÇÃO DO CERTIFICADO

4.3.1 O certificado é considerado aceito assim que for utilizado. A aceitação implica que a pessoa física responsável pelo certificado reconhece a veracidade dos dados contidos nele.

4.3.2 A aceitação de todo certificado emitido é declarada implicitamente pelo respectivo titular assim que for utilizado. No caso de certificados emitidos para pessoas jurídicas, equipamentos, aplicações ou assinaturas de códigos, a declaração deverá ser feita pela pessoa física responsável por esses certificados.

4.4 SUSPENSÃO E REVOGAÇÃO DE CERTIFICADO

4.4.1 CIRCUNSTÂNCIAS PARA REVOGAÇÃO

4.4.1.1 Neste item, a DPC caracteriza as circunstâncias nas quais um certificado poderá ser revogado.

4.4.1.2 Um certificado é obrigatoriamente revogado nas seguintes circunstâncias:

- a) Quando constatada emissão imprópria ou defeituosa do mesmo;
- b) Quando for necessária a alteração de qualquer informação constante no mesmo;
- c) No caso de extinção, dissolução ou transformação do titular do certificado.
- d) No caso de perda, roubo, modificação, acesso indevido ou comprometimento da chave privada correspondente ou da sua mídia armazenadora;
- e) No caso de perda, roubo, acesso indevido, comprometimento ou suspeita de comprometimento da chave privada correspondente à pública contida no certificado ou da sua mídia armazenadora;

4.4.1.3 Deve-se observar ainda que:

- a) A AC Safeweb revogará, no prazo definido no item 4.4.3, o certificado da entidade que deixar de cumprir as políticas, normas e regras estabelecidas para a ICP-Brasil;
- b) O CG da ICP-Brasil determinará a revogação do certificado da AC que deixar de cumprir a legislação vigente ou as políticas, normas, práticas e regras estabelecidas para a ICP-Brasil.

4.4.2 QUEM PODE SOLICITAR A REVOGAÇÃO

A revogação de um certificado somente pode ser solicitada:

- a) Pelo titular do certificado;
- b) Pelo responsável pelo certificado, no caso de certificado de equipamentos, aplicações, assinaturas de códigos e pessoas jurídicas;
- c) Por empresa ou órgão, quando o titular do certificado fornecido por essa empresa ou órgão for seu empregado, funcionário ou servidor;
- d) Pela AC Safeweb;
- e) Pela AR Vinculada; ou
- f) Por determinação do CG da ICP-Brasil ou da AC Raiz.

4.4.3 PROCEDIMENTO PARA SOLICITAÇÃO DE REVOGAÇÃO

4.4.3.1 Para solicitar a revogação é necessário o envio à AC Safeweb ou à AR vinculada de um formulário disponibilizado pela AC Safeweb no site www.safeweb.com.br, preenchido com os dados do solicitante, o número de série do certificado e a indicação do motivo da solicitação. A AC Safeweb garante que todos agentes habilitados podem, facilmente e a qualquer tempo, solicitar a revogação de seus respectivos certificados conforme o item 4.4.2.

4.4.3.2 Como diretrizes gerais:

- a) O solicitante da revogação de um certificado é identificado;
- b) As solicitações de revogação, bem como as ações delas decorrentes são registradas e armazenadas;
- c) As justificativas para a revogação de um certificado são documentadas;
- d) O processo de revogação de um certificado termina com a geração e a publicação de uma LCR que contém o certificado revogado e com a atualização da situação do certificado nas bases de dados da AC Safeweb de consulta OCSP, quando aplicável.

4.4.3.3 Não se aplica.

4.4.3.4 O prazo máximo admitido para a conclusão do processo de revogação de certificado, após o recebimento da respectiva solicitação, para todos os tipos de certificado previstos pela ICP-Brasil é de 12 (doze) horas.

4.4.3.5 A AC Safeweb responde plenamente por todos os danos causados pelo uso de um certificado no período compreendido entre a solicitação de sua revogação e a emissão da correspondente LCR.

4.4.3.6 Não se aplica.

4.4.4 PRAZO PARA SOLICITAÇÃO DE REVOGAÇÃO

4.4.4.1 A solicitação de revogação deve ser imediata quando configuradas as circunstâncias definidas no item 4.4.1.

4.4.4.2 O prazo máximo para a aceitação do certificado por seu titular, dentro do qual a revogação desse certificado pode ser solicitada sem cobrança de tarifa pela AC Safeweb é de 3 (três) dias.

4.4.5 CIRCUNSTÂNCIAS PARA SUSPENSÃO

4.4.5.1 A suspensão de certificados não é admitida no âmbito da ICP-Brasil.

4.4.6 QUEM PODE SOLICITAR SUSPENSÃO

4.4.6.1 A suspensão de certificados não é admitida no âmbito da ICP-Brasil.

4.4.7 PROCEDIMENTO PARA SOLICITAÇÃO DE SUSPENSÃO

4.4.7.1 A suspensão de certificados não é admitida no âmbito da ICP-Brasil.

4.4.8 LIMITES NO PERÍODO DE SUSPENSÃO

4.4.8.1 A suspensão de certificados não é admitida no âmbito da ICP-Brasil.

4.4.9 FREQUÊNCIA DE EMISSÃO DE LCR

4.4.9.1 Neste item é definida a frequência de emissão da LCR referente a certificados de AC de nível imediatamente subsequente a AC Safeweb.

4.4.9.2 Não se aplica.

4.4.9.3 A frequência máxima admitida para a emissão de LCR referente a certificados de AC Subsequente é de 45 (quarenta e cinco) dias. Em caso de revogação de certificado de AC de nível imediatamente subsequente a AC Safeweb, é emitida nova LCR no prazo previsto no item 4.4.3 e notificada a todas as AC de nível imediatamente subsequente ao seu.

4.4.9.4 Não se aplica.

4.4.10 REQUISITOS PARA VERIFICAÇÃO DE LCR

4.4.10.1 Todo certificado deve ter a sua validade verificada, na respectiva LCR, antes de ser utilizado.

4.4.10.2 A autenticidade da LCR deve ser confirmada por meio das verificações da assinatura da AC Safeweb e do período de validade da LCR.

4.4.11 DISPONIBILIDADE PARA REVOGAÇÃO/VERIFICAÇÃO DE STATUS ON-LINE

4.4.11.1 Não se aplica

4.4.12 REQUISITOS PARA VERIFICAÇÃO DE REVOGAÇÃO ON-LINE

4.4.12.1 Não se aplica.

4.4.13 OUTRAS FORMAS DISPONÍVEIS PARA DIVULGAÇÃO DE REVOGAÇÃO

4.4.13.1 Não se aplica.

4.4.14 REQUISITOS PARA VERIFICAÇÃO DE OUTRAS FORMAS DE DIVULGAÇÃO DE REVOGAÇÃO

4.4.14.1 Não se aplica.

4.4.15 REQUISITOS ESPECIAIS PARA O CASO DE COMPROMETIMENTO DE CHAVE

4.4.15.1 Havendo roubo, perda, modificação, acesso indevido ou qualquer forma de comprometimento da chave privada ou de sua mídia, o titular do certificado deve comunicar imediatamente a AC Safeweb. Serão registradas as circunstâncias de comprometimento, observando o disposto no item 4.4.3.

4.4.15.2 O comprometimento ou suspeita de comprometimento de chave deve ser comunicado à AC Safeweb ou através de AR responsável, utilizando formulário específico para tal fim, observado o disposto no item 4.4.3 desta DPC.

4.5 PROCEDIMENTOS DE AUDITORIA DE SEGURANÇA

4.5.1 TIPOS DE EVENTO REGISTRADOS

4.5.1.1 EVENTOS OBRIGATÓRIOS RELACIONADOS AO SISTEMA DE CERTIFICAÇÃO QUE DEVERÃO SER INCLUÍDOS EM ARQUIVOS DE AUDITORIA

- a) Iniciação e desligamento do sistema de certificação;
- b) Tentativas de criar, remover, definir senhas ou mudar privilégios de sistema dos operadores da AC Safeweb;
- c) Mudanças na configuração da AC Safeweb ou nas suas chaves;
- d) Mudanças nas políticas de criação de certificados;
- e) Tentativas de acesso (login) e de saída do sistema (logout);
- f) Tentativas não autorizadas de acesso aos arquivos de sistema;
- g) Geração de chaves próprias da AC Safeweb ou de chaves das ACs subsequentes;
- h) Emissão e revogação de certificados;
- i) Geração de LCR;
- j) Tentativas de iniciar, remover, habilitar e desabilitar usuários de sistemas, e de atualizar e recuperar suas chaves;
- k) Operações falhas de escrita ou leitura no repositório de certificados e da LCR, quando aplicável;
- l) Operações de escrita nesse repositório, quando aplicável.

4.5.1.2 EVENTOS NÃO DIRETAMENTE RELACIONADOS AO SISTEMA DE CERTIFICAÇÃO

A AC Safeweb registra, eletrônica ou manualmente, informações de segurança não geradas diretamente pelo seu sistema de certificação, tais como:

- a) Registros de acessos físicos;
- b) Manutenção e mudanças na configuração de seus sistemas;
- c) Mudanças de pessoal e de perfis qualificados;
- d) Relatórios de discrepância e comprometimento; e
- e) Registros de destruição de mídias de armazenamento contendo chaves criptográficas, dados de ativação de certificados ou informação pessoal de usuários.

4.5.1.3 A AC Safeweb não registra outras informações.

4.5.1.4 Os registros de auditoria, eletrônicos ou manuais, contém a data e a hora do evento registrado e a identidade do agente que o causou.

4.5.1.5 Para facilitar os processos de auditoria, toda a documentação relacionada aos serviços da AC Safeweb é armazenada, eletrônica ou manualmente, em local único, conforme a POLÍTICA DE SEGURANÇA DA ICP-BRASIL[8].

4.5.1.6 A AR vinculada registra eletronicamente em arquivos de auditoria todos os eventos relacionados à validação e aprovação da solicitação, bem como, à revogação de certificados. Os seguintes eventos estão obrigatoriamente incluídos em arquivos de auditoria:

- a) Os agentes de registro que realizaram as operações;
- b) Data e hora das operações;
- c) A associação entre os agentes que realizaram a validação e aprovação e o certificado gerado;
- d) A assinatura digital do executante.

4.5.1.7 A AC Safeweb define, em documento disponível nas auditorias de conformidade, o local de arquivamento das cópias dos documentos para identificação, apresentadas no momento da solicitação e revogação de certificados e do termo de titularidade.

4.5.2 FREQUÊNCIA DE AUDITORIA DE REGISTROS (LOGS)

4.5.2.1 AC Safeweb examina os registros de auditoria uma vez por semana. Todos os eventos significativos são analisados e explicados em relatório de auditoria de registros. Tal análise envolve uma inspeção breve de todos os registros, com a verificação de que não foram alterados, seguida de uma investigação mais detalhada de quaisquer alertas ou irregularidades nesses registros. Todas as ações tomadas em decorrência dessa análise são documentadas.

4.5.3 PERÍODO DE RETENÇÃO PARA REGISTROS (LOGS) DE AUDITORIA

A AC Safeweb mantém localmente seus registros de auditoria por pelo menos 2 (dois) meses e,

subseqüentemente, armazena os seus registros de auditoria da maneira descrita no item 4.6.

4.5.4 PROTEÇÃO DE REGISTRO (LOGS) DE AUDITORIA

4.5.4.1 O sistema de registro de eventos de auditoria inclui mecanismos para proteger os arquivos de auditoria contra leitura não autorizada, modificação e remoção, através das funcionalidades nativas dos sistemas operacionais.

4.5.4.2 Mecanismos de proteção utilizados:

- a) Os acessos lógicos são liberados através da ferramenta nativa do sistema operacional de modo a assegurar o uso apenas a usuários ou processos autorizados;
- b) Os acessos lógicos aos registros de eventos de auditoria são registrados em *logs* do próprio sistema operacional;
- c) Informações manuais de auditoria também são protegidas contra a leitura não autorizada, modificação e remoção.

4.5.4.3 Os mecanismos de proteção descritos neste item obedecem à Política de Segurança implementada, de conformidade com a POLÍTICA DE SEGURANÇA DA ICP-BRASIL[8].

4.5.5 PROCEDIMENTO PARA CÓPIA DE SEGURANÇA (BACKUP) DE REGISTRO (LOG) DE AUDITORIA

A AC Safeweb gera a cada semana cópia de *backup* de seus registros de auditoria, através de procedimentos utilizando conexão segura.

4.5.6 SISTEMA DE COLETA DE DADOS DE AUDITORIA

O sistema de coleta de dados de auditoria é interno à AC Safeweb e utiliza processos automatizados e manuais.

4.5.7 NOTIFICAÇÃO DE AGENTES CAUSADORES DE EVENTOS

Quando um evento é registrado pelo conjunto de sistemas de auditoria da AC Safeweb, nenhuma notificação é enviada à pessoa, organização, dispositivo ou aplicação que causou o evento.

4.5.8 AVALIAÇÕES DE VULNERABILIDADE

Os eventos que indicam possível vulnerabilidade, detectados na análise periódica dos registros de auditoria da AC Safeweb, são analisados detalhadamente e, dependendo de sua gravidade,

registrados em separado. Ações corretivas decorrentes são implementadas pela AC Safeweb e registradas para fins de auditoria.

4.6 ARQUIVAMENTO DE REGISTRO

4.6.1 TIPOS DE EVENTOS REGISTRADOS

Os tipos de eventos arquivados pela AC Safeweb , são:

- a) Solicitações de certificados;
- b) Solicitações de revogação de certificados;
- c) Notificações de comprometimento de chaves privadas;
- d) Emissões e revogações de certificados;
- e) Emissões de LCR;
- f) Trocas de chaves criptográficas da AC Safeweb ;
- g) Informações de auditoria previstas no item 4.5.1.

4.6.2 PERÍODO DE RETENÇÃO PARA ARQUIVO

Os períodos de retenção para cada evento arquivado, são:

- a) As LCRs e os certificados de assinatura digital são retidos permanentemente, para fins de consulta histórica;
- b) As cópias dos documentos para identificação apresentadas no momento da solicitação e da revogação de certificados, e os termos de titularidade e responsabilidade devem ser retidos, no mínimo, por 10 (dez) anos, a contar da data de expiração ou revogação do certificado; e
- c) As demais informações, inclusive arquivos de auditoria, são retidas por, no mínimo, 6 (seis) anos.

4.6.3 PROTEÇÃO DE ARQUIVO

Os registros arquivados da AC Safeweb são classificados e armazenados com requisitos de segurança compatíveis com essa classificação e com a POLÍTICA DE SEGURANÇA DA ICP-BRASIL[8].

4.6.4 PROCEDIMENTOS PARA CÓPIA DE SEGURANÇA (BACKUP) DE ARQUIVO

- 4.6.4.1 Uma segunda cópia de todo o material arquivado será armazenada no site *backup*,

recebendo o mesmo tipo de proteção utilizada por ela no arquivo principal.

4.6.4.2 As cópias de segurança seguem os períodos de retenção definidos para os registros dos quais são cópias.

4.6.4.3 A AC Safeweb verifica a integridade dessas cópias de segurança, no mínimo, a cada 6 (seis) meses.

4.6.5 REQUISITOS PARA DATAÇÃO DE REGISTROS (TIME-STAMPING)

Os servidores estão sincronizados com a hora Greenwich Mean Time – GMT. Todas as informações geradas que possuam alguma identificação de horário recebem o horário em GMT, inclusive os certificados emitidos por esses equipamentos. No caso dos registros feitos manualmente e formulários de requisição de certificados, estes contêm a Hora Oficial do Brasil.

4.6.6 SISTEMA DE COLETA DE DADOS DE ARQUIVO

Todos os sistemas de coleta de dados de arquivo utilizados pela AC Safeweb em seus procedimentos operacionais são automatizados, manuais e internos.

4.6.7 PROCEDIMENTOS PARA OBTER E VERIFICAR INFORMAÇÃO DE ARQUIVO

A verificação de informação de arquivo deve ser solicitada formalmente à AC Safeweb, identificando de forma precisa o tipo e o período da informação a ser verificada. O solicitante da verificação de informação deve ser devidamente identificado.

4.7 TROCA DE CHAVE

4.7.1 A AC Safeweb fornece novo certificado a AC Subsequente utilizando o mesmo procedimento utilizado para emissão de certificado inicial. A AC Safeweb comunica o titular do certificado trinta dias (30) antes da data de expiração do certificado digital, junto com informações para a solicitação de um novo certificado. A comunicação de expiração e solicitação de renovação é realizada através de e-mail.

4.7.2 Não se aplica.

4.8 COMPROMETIMENTO E RECUPERAÇÃO DE DESASTRE

A AC Safeweb possui um Plano de Continuidade de Negócio (PCN), estabelecido conforme a POLÍTICA DE SEGURANÇA DA ICP-BRASIL[8] e testado pelo menos uma vez por ano, para garantir a

continuidade dos seus serviços críticos.

O plano estabelecido conforme a PS da ICP-Brasil governa as situações de crise através da:

- i. Identificação do motivo da crise;
- ii. Identificação dos responsáveis pelo processo de certificação digital;
- iii. Ativação das equipes envolvidas na solução do imprevisto;
- iv. Definição da ação para impedir a continuidade do problema;
- v. Avaliação da expansão da crise;
- vi. Identificação das ações de recuperação propriamente ditas;
- vii. Notificações à AC Raiz da evolução corretiva e solução, registro da crise e análise para melhoria.

4.8.1 RECURSOS COMPUTACIONAIS, SOFTWARE E DADOS CORROMPIDOS

4.8.1.1 Os procedimentos de recuperação utilizados pela AC Safeweb quando recursos computacionais, softwares ou dados estiverem corrompidos ou houver suspeita de corrupção, incluem, mas não se limitam a somente estes: a identificação da crise, acionamento dos principais gestores, ativação das equipes, contenção da crise, estimativa do alargamento da crise, declaração do início das atividades de ativação da situação de recuperação, notificação da crise, registro da crise, crítica para melhoria.

4.8.1.2 Nas circunstâncias de crise relacionadas aos recursos computacionais, softwares e dados corrompidos ou quando houver suspeita de corrupção desses componentes, após a identificação da crise ou confirmação da suspeita de corrupção, são comunicados os gestores de certificação digital, que acionam as equipes, de forma a identificar o grau de corrupção.

4.8.1.3 Os métodos de recuperação dos recursos computacionais, softwares e dados corrompidos envolvem: identificação da necessidade de recurso computacional alternativo e, em caso de necessidade, disponibilização de outro recurso computacional equivalente, instalação dos softwares necessários e recuperação dos dados através do arquivo de backup, conforme detalhado no Plano de Continuidade de Negócios da AC Safeweb e no Plano de Migração e Fluxo de Ativação do Ambiente Backup.

4.8.2 CERTIFICADO DE ENTIDADE É REVOGADO

Em caso de revogação do certificado da AC Safeweb, após a identificação do incidente, são notificados os gestores do processo de certificação digital, que acionam as equipes envolvidas, de forma a indisponibilizar temporariamente os serviços de autoridade certificadora. Na confirmação do

incidente, são revogados os certificados das AC de nível imediatamente subsequente, é gerado um novo par de chaves da AC Safeweb, emitido certificado associado ao novo par de chaves gerado e emitidos novos certificados digitais para as AC de nível imediatamente subsequente.

4.8.3 CHAVE DE ENTIDADE É COMPROMETIDA

Em caso de comprometimento da chave da AC Safeweb, após a identificação da crise são notificados os gestores do processo de certificação digital, que acionam as equipes envolvidas, de forma a indisponibilizar temporariamente os serviços de autoridade certificadora. Na confirmação do incidente, são revogados os certificados da AC Safeweb e das AC de nível imediatamente subsequente, é gerado um novo par de chaves, emitido certificado associado ao novo par de chaves gerado e emitidos novos certificados digitais para as AC de nível imediatamente subsequente.

4.8.4 SEGURANÇA DOS RECURSOS APÓS DESASTRE NATURAL OU DE OUTRA NATUREZA

Em caso de desastre natural ou de outra natureza, depois da identificação da crise são comunicados os gestores do processo de certificação digital, que acionam as equipes envolvidas, de forma a identificar o grau de exposição e comprometimento do ambiente. Na confirmação do desastre e constatado impossibilidade de operação no site, as atividades são transferidas para o site de recuperação de desastre.

4.8.5 ATIVIDADES DAS AUTORIDADES DE REGISTRO

Procedimentos descritos no Plano de Continuidade do Negócio da(s) AR(s) Vinculada(s) contemplam a recuperação, total ou parcial das atividades das ARs, contendo, no mínimo as seguintes informações:

- a) Identificação dos eventos que podem causar interrupções nos processos do negócio, por exemplo falha de equipamentos, inundações e incêndios;
- b) Identificação e concordância de todas as responsabilidades e procedimentos de emergência;
- c) Implementação dos procedimentos de emergência que permitam a recuperação e restauração nos prazos necessários. Atenção especial deve ser dada à avaliação da recuperação das documentações armazenadas nas instalações técnicas atingidas pelo desastre;
- d) Documentação dos processos e procedimentos acordados;
- e) Treinamento adequado do pessoal nos procedimentos e processos de emergência definidos, incluindo o gerenciamento de crise;
- f) Teste e atualização dos planos.

4.9 EXTINÇÃO DOS SERVIÇOS DE AC, AR OU PSS

4.9.1 Em caso de extinção da AC Safeweb, ou de uma AR ou PSS a ela vinculados serão tomadas as providências preconizadas no documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6], que incluem a divulgação da decisão do encerramento de atividades, prazos para essa divulgação, atividades relacionadas à geração de novos certificados, revogação de certificados, transferência da guarda de bases de dados e registros de arquivo.

4.9.2 Quando for necessário encerrar as atividades da AC Safeweb, o impacto deste término deve ser minimizado da melhor forma possível tendo em vista as circunstâncias prevalecentes, inclusive:

- a) Notificar a AC Raiz da ICP-Brasil;
- b) Extinguir a emissão, revogação e publicação de LCR e/ou dos serviços de status on-line, após a revogação de todos os certificados emitidos;
- c) Providenciar a transferência de chaves públicas, dos certificados e respectiva documentação para serem armazenados por outra AC, após aprovação da AC Raiz;
- d) Transferir progressivamente o serviço e os registros operacionais para um sucessor, que deverá observar os mesmos requisitos de segurança exigidos para a AC Safeweb;
- e) Preservar qualquer registro não transferido a um sucessor;
- f) Transferir, se for o caso, a documentação dos certificados digitais emitidos à AC que tenha assumido a guarda das respectivas chaves públicas; e
- g) Repassar à AC Raiz os documentos referentes aos certificados digitais e as respectivas chaves públicas, caso essas não sejam assumidas por outra AC.

4.9.3 No caso de encerramento das atividades como AR vinculada à AC Safeweb a AR deverá seguir os seguintes requisitos e procedimentos :

- a) Comunicará publicamente a extinção dos serviços de AR vinculada AC Safeweb, através de publicação em jornal de grande circulação;
- b) Extinguirá os serviços de recebimento e validação de pedidos de emissão de certificados;
- c) Ficará responsável pela guarda dos documentos, dados e registros relativos aos pedidos de emissão de certificados para a AC Safeweb, devendo fornecê-los sempre que solicitada pelo Titular, ou pela AC Safeweb. O período no qual os mesmos ficarão armazenados está descrito na DPC item 4.6.

4.9.4 Em caso de falência ou extinção da AR a documentação e registros relativos à emissão de certificados deverá ser entregue para guarda da AC Safeweb.

4.9.5 No caso de encerramento das atividades como PSS vinculada a AC Safeweb, a AC, diretamente ou por intermédio da AR, deverá seguir os seguintes requisitos e procedimentos :

- a) Publicará, em sua página web, informação sobre o descredenciamento do PSS e o credenciamento de novo PSS, se for o caso;
- b) Manterá a guarda de toda a documentação comprobatória em seu poder.

5 CONTROLES DE SEGURANÇA FÍSICA, PROCEDIMENTAL E DE PESSOAL

Os controles descritos a seguir são implementados pela AC Safeweb para executar de modo seguro suas funções de geração de chaves, identificação, certificação, auditoria e arquivamento de registros.

5.1 CONTROLES FÍSICOS

Nos itens seguintes estão descritos os controles físicos referentes às instalações que abrigam os sistemas da AC Safeweb.

5.1.1 CONSTRUÇÃO E LOCALIZAÇÃO DAS INSTALAÇÕES DE AC

5.1.1.1 A localização e o sistema de certificação AC Safeweb não são publicamente identificados. Não há identificação pública externa das instalações e, internamente, não são admitidos ambientes compartilhados que permitam visibilidade das operações de emissão e revogação de certificados. Essas operações são segregadas em compartimentos fechados e fisicamente protegidos.

5.1.1.2 Na construção das instalações da AC Safeweb foram considerados, entre outros, os seguintes aspectos relevantes para os controles de segurança física:

- a) Instalações para equipamentos de apoio, tais como: máquinas de ar condicionado, grupos geradores, nobreaks, baterias, quadros de distribuição de energia e de telefonia, subestações, retificadores, estabilizadores e similares;
- b) Instalações para sistemas de telecomunicações;
- c) Sistemas de aterramento e de proteção contra descargas atmosféricas;
- d) Iluminação de emergência.

5.1.2 ACESSO FÍSICO NAS INSTALAÇÕES DA AC

A AC Safeweb inseriu um sistema de controle de acesso físico que garante a segurança de suas

instalações, conforme a Política de Segurança implementada.

5.1.2.1 NÍVEIS DE ACESSO

5.1.2.1.1 A AC Safeweb definiu 4 (quatro) níveis de acesso físico aos diversos ambientes da AC e 2 (dois) níveis relativos à proteção de sua chave privada.

5.1.2.1.2 O primeiro nível (nível 1) situa-se após a primeira barreira de acesso às instalações da AC Safeweb . Para entrar em uma área de nível 1, cada indivíduo deve ser identificado e registrado por segurança armado. A partir desse nível, pessoas estranhas à operação da AC devem transitar devidamente identificadas e acompanhadas. Nenhum tipo de processo operacional ou administrativo da AC é executado nesse nível.

5.1.2.1.3 Excetuados os casos previstos em lei, o porte de armas não é admitido nas instalações da AC Safeweb, a partir do nível 1. A partir desse nível, equipamentos de gravação, fotografia, vídeo, som ou similares, bem como computadores portáteis, têm sua entrada controlada e somente podem ser utilizados mediante autorização formal e supervisão.

5.1.2.1.4 O segundo nível (nível 2) é interno ao primeiro e requer, da mesma forma que o primeiro, a identificação individual das pessoas que nele entram. A passagem do primeiro para o segundo nível exige identificação por meio eletrônico e o uso de crachá. Esse é o nível mínimo de segurança requerido para a execução de qualquer processo operacional ou administrativo da AC Safeweb .

5.1.2.1.5 O terceiro nível (nível 3) situa-se dentro do segundo e é o primeiro nível a abrigar material e atividades sensíveis da operação da AC Safeweb . As atividades relativas ao ciclo de vida dos certificados digitais estão localizadas a partir desse nível. Pessoas que não estejam envolvidas com essas atividades não têm permissão para acesso a esse nível. Pessoas que não possuam permissão de acesso não podem permanecer nesse nível se não estiverem acompanhadas por alguém que tenha essa permissão.

5.1.2.1.6 No nível 3 são controladas tanto as entradas quanto as saídas de cada pessoa autorizada. Dois tipos de mecanismos de controle são requeridos para a entrada nesse nível: senha individual e identificação biométrica.

5.1.2.1.7 Telefones celulares, bem como outros equipamentos portáteis de comunicação, exceto aqueles exigidos para a operação da AC Safeweb, não são admitidos a partir do nível 3.

5.1.2.1.8 No quarto nível (nível 4), interior ao terceiro, é onde ocorrem atividades especialmente sensíveis da operação da AC Safeweb, tais como emissão e revogação de certificados, e emissão de LCR. Todos os sistemas e equipamentos necessários a estas atividades estão localizados a partir desse nível. O nível 4 possui os mesmos controles de acesso do nível 3 e, adicionalmente, exige, em cada acesso ao seu ambiente, a identificação de, no mínimo, 2 (duas) pessoas autorizadas.

Nesse nível, a permanência no mínimo de duas pessoas autorizadas é exigida enquanto o ambiente estiver ocupado.

5.1.2.1.9 No quarto nível todas as paredes, piso e teto são revestidos de aço e concreto ou de outro material de resistência equivalente. As paredes, piso e o teto são inteiriços, constituindo uma célula estanque contra ameaças de acesso indevido, água, vapor, gases e fogo. No quarto nível, os dutos de refrigeração e de energia, bem como os dutos de comunicação, não permitem a invasão física das áreas de quarto nível. Adicionalmente, esses ambientes de nível 4 possuem proteção contra interferência eletromagnética externa.

5.1.2.1.10 As salas-cofre foram construídas segundo as normas brasileiras aplicáveis. Eventuais omissões dessas normas deverão ser sanadas por normas internacionais pertinentes.

5.1.2.1.11 Na AC Safeweb há ambientes de quarto nível para abrigar e segregar, respectivamente:

- a) Equipamentos de produção on-line;
- b) Equipamentos de produção off-line e cofre de armazenamento.

5.1.2.1.12 O quinto nível (nível 5), interior aos ambientes de nível 4, compreende um cofre ou gabinete reforçado trancado. Materiais criptográficos tais como chaves, dados de ativação, suas cópias e equipamentos criptográficos estão armazenados em ambiente de nível 5 ou superior.

5.1.2.1.13 Para garantir a segurança do material armazenado, o cofre ou o gabinete obedecem às seguintes especificações mínimas:

- a) É feito em aço ou material de resistência equivalente;
- b) Possui tranca com chave e segredo.

5.1.2.1.14 O sexto nível (nível 6), consiste de pequenos depósitos localizados no interior do cofre de quinto nível. Cada um desses depósitos dispõe de uma fechadura comum, com duas cópias de chave. Os dados de ativação da chave privada da AC Safeweb são armazenados nesses depósitos.

5.1.2.2 SISTEMAS FÍSICOS DE DETECÇÃO

5.1.2.2.1 Todas as passagens entre os níveis de acesso, bem como as salas de operação de nível 4, são monitoradas por câmeras de vídeo ligadas a um sistema de gravação 24x7. O posicionamento e a capacidade dessas câmeras não permitem a recuperação de senhas digitadas nos controles de acesso.

5.1.2.2.2 Os arquivos de imagens ou as fitas de vídeo resultantes da gravação 24x7 são armazenadas por, no mínimo, um ano. Essas gravações são testadas (verificação de trechos aleatórios no início, meio e final do arquivo) pelo menos a cada 3 (três) meses, com a escolha de, no mínimo, um arquivo referente a cada semana. Essas gravações são armazenadas em ambiente de terceiro nível.

5.1.2.2.3 Todas as portas de passagem entre os níveis de acesso 3 e 4 do ambiente são monitoradas por sistema de notificação de alarmes. Onde há, a partir do nível 2, vidros separando níveis de acesso foi implantado um mecanismo de alarme de quebra de vidros, que permanece ligado ininterruptamente.

5.1.2.2.4 Em todos os ambientes de quarto nível, um alarme de detecção de movimentos permanece ativo enquanto não é satisfeito o critério de acesso ao ambiente. Assim que, devido à saída de um ou mais empregados, o critério mínimo de ocupação deixa de ser satisfeito, ocorre a reativação automática dos sensores de presença.

5.1.2.2.5 O sistema de notificação de alarmes utiliza 2 (dois) meios de notificação: sonoro e visual.

5.1.2.2.6 O sistema de monitoramento das câmeras de vídeo, bem como o sistema de notificação de alarmes, são permanentemente monitorados por guarda, armado, e estão localizados em ambiente de nível 3. As instalações do sistema de monitoramento, por sua vez, são monitoradas por câmeras de vídeo cujo posicionamento permite o acompanhamento das ações do guarda.

5.1.2.3 SISTEMA DE CONTROLE DE ACESSO

5.1.2.3.1 O sistema de controle de acesso está baseado em um ambiente de nível 4.

5.1.2.4 MECANISMO DE EMERGÊNCIA

5.1.2.4.1 Mecanismos específicos foram implantados pela AC Safeweb para garantir a segurança de seu pessoal e de seus equipamentos em situações de emergência. Esses mecanismos permitem o destravamento de portas por meio de acionamento mecânico, para a saída de emergência de todos os ambientes com controle de acesso. A saída efetuada por meio desses mecanismos aciona imediatamente os alarmes de abertura de portas.

5.1.2.4.2 Todos os procedimentos referentes aos mecanismos de emergência são documentados. Os mecanismos e procedimentos de emergência são verificados semestralmente, por meio de simulação de situações de emergência.

5.1.3 ENERGIA E AR CONDICIONADO NAS INSTALAÇÕES DE AC

5.1.3.1 A infraestrutura do ambiente de certificação da AC Safeweb foi dimensionada com sistemas e dispositivos que garantem o fornecimento ininterrupto de energia elétrica às instalações. As condições de fornecimento de energia são mantidas de forma a atender os requisitos de disponibilidade dos sistemas da AC Safeweb e seus respectivos serviços. Um sistema de aterramento foi implantado.

- 5.1.3.2 Todos os cabos elétricos estão protegidos por tubulações ou dutos apropriados.
- 5.1.3.3 Foram utilizados tubulações, dutos, calhas, quadros e caixas de passagem, distribuição e terminação - projetados e construídos de forma a facilitar vistorias e a detecção de tentativas de violação. Foram utilizados dutos separados para os cabos de energia, de telefonia e de dados.
- 5.1.3.4 Todos os cabos são catalogados, identificados e periodicamente vistoriados, no mínimo a cada 6 meses, na busca de evidências de violação ou de outras anormalidades.
- 5.1.3.5 São mantidos atualizados os registros sobre a topologia da rede de cabos, observados os requisitos de sigilo estabelecidos pela POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8]. Qualquer modificação nessa rede é previamente documentada.
- 5.1.3.6 Não são admitidas instalações provisórias, fiações expostas ou diretamente conectadas às tomadas sem a utilização de conectores adequados.
- 5.1.3.7 O sistema de climatização atende os requisitos de temperatura e umidade exigidos pelos equipamentos utilizados no ambiente e dispõe de filtros de poeira. Nos ambientes de nível 4, o sistema de climatização independente, redundante e tolerante a falhas.
- 5.1.3.8 A temperatura dos ambientes atendidos pelo sistema de climatização é permanentemente monitorada pelo sistema de notificação de alarmes.
- 5.1.3.9 O sistema de ar condicionado é interno, com troca de ar realizada apenas por abertura da porta.
- 5.1.3.10 A capacidade de redundância de toda a estrutura de energia e ar condicionado da AC Safeweb é garantida, por meio de:
- a) Geradores de porte compatível;
 - b) Geradores de reserva;
 - c) Sistemas de nobreaks redundantes;
 - d) Sistemas redundantes de ar condicionado.

5.1.4 EXPOSIÇÃO À ÁGUA NAS INSTALAÇÕES DE AC

O ambiente de nível 4 encontra-se fisicamente protegido contra exposição à água, infiltrações e inundações, provenientes de qualquer fonte externa.

5.1.5 PREVENÇÃO E PROTEÇÃO CONTRA INCÊNDIO NAS INSTALAÇÕES DE AC

5.1.5.1 Os sistemas de prevenção contra incêndios, internos aos ambientes, possibilitam alarmes preventivos antes de fumaça visível, disparados somente com a presença de partículas

que caracterizam o sobreaquecimento de materiais elétricos e outros materiais combustíveis presentes nas instalações.

5.1.5.2 Nas instalações da AC Safeweb não é permitido fumar ou portar objetos que produzam fogo ou faísca.

5.1.5.3 O ambiente de nível 4 possui sistema para detecção precoce de fumaça e sistema de extinção de incêndio por gás. As portas de acesso ao ambiente de nível 4 constituem eclusas, onde uma porta só se abre quando a anterior estiver fechada.

5.1.5.4 Em caso de incêndio nas instalações da AC Safeweb, o aumento da temperatura interna da sala-cofre de nível 4 não excede 50 graus Celsius, e a sala suporta esta condição por, no mínimo, 1 (uma) hora.

5.1.6 ARMAZENAMENTO DE MÍDIA NAS INSTALAÇÕES DE AC

São observados os critérios estabelecidos na norma brasileira NBR 11.515/NB 1334 ("Critérios de Segurança Física Relativos ao Armazenamento de Dados").

5.1.7. DESTRUIÇÃO DE LIXO NAS INSTALAÇÕES DE AC

5.1.7.1 Todos os documentos em papel que contém informações classificadas como sensíveis são triturados antes de ir para o lixo.

5.1.7.2 Todos os dispositivos eletrônicos não mais utilizáveis, e que tenham sido anteriormente utilizados para o armazenamento de informações sensíveis, são fisicamente destruídos.

5.1.8 INSTALAÇÕES DE SEGURANÇA (BACKUP) EXTERNAS (OFF-SITE) PARA AC

As instalações de backup atendem os requisitos mínimos estabelecidos por este documento. Sua localização é tal que, em caso de sinistro que torne inoperantes as instalações principais, as instalações de backup não serão atingidas e tornar-se-ão totalmente operacionais em, no máximo, 48 (quarenta e oito) horas.

5.1.9 INSTALAÇÕES TÉCNICAS DE AR

As instalações técnicas da(s) AR(s) Vinculada(s) atendem aos requisitos estabelecidos no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP-BRASIL [1].

5.2 CONTROLES PROCEDIMENTAIS

5.2.1 PERFIS QUALIFICADOS

5.2.1.1 A AC Safeweb efetua separação das tarefas para funções críticas, com o intuito de evitar que um empregado utilize o seu sistema de certificação sem ser detectado. As ações de cada empregado estão limitadas de acordo com seu perfil.

5.2.1.2 A AC Safeweb estabelece perfis distintos para sua operação, distinguindo as operações do dia-a-dia do sistema, o gerenciamento e a auditoria dessas operações, bem como o gerenciamento de mudanças substanciais no sistema.

O detalhamento dos perfis encontra-se em documento interno normativo.

5.2.1.3 Todos os operadores do sistema de certificação da AC Safeweb recebem treinamento específico antes de obter qualquer tipo de acesso. O tipo e o nível de acesso são determinados, em documento formal, com base nas necessidades de cada perfil.

5.2.1.4 Quando um empregado se desligar da AC Safeweb, suas permissões de acesso são revogadas imediatamente. Quando houver mudança na posição ou função que o empregado ocupa dentro da AC Safeweb, suas permissões de acesso são revistas.

Há uma lista de revogação, com todos os recursos, antes disponibilizados, que o empregado deve devolver à AC no ato de seu desligamento.

5.2.2 NÚMERO DE PESSOAS NECESSÁRIO POR TAREFA

5.2.2.1 A AC Safeweb utiliza o requisito de controle multiusuário para a geração e a utilização da sua chave privada, na forma definida no item 6.2.2.

5.2.2.2 Todas as tarefas executadas no ambiente onde está localizado o equipamento de certificação da AC Safeweb requerem a presença de, no mínimo, 2 (dois) de seus empregados com perfis qualificados. As demais tarefas da AC Safeweb podem ser executadas por um único empregado.

5.2.3 IDENTIFICAÇÃO E AUTENTICAÇÃO PARA CADA PERFIL

5.2.3.1 Todo empregado da AC Safeweb tem sua identidade e perfil verificados antes de:

- a) Ser incluído em uma lista de acesso às instalações da AC;
- b) Ser incluído em uma lista para acesso físico ao sistema de certificação da AC;
- c) Receber um certificado para executar suas atividades operacionais na AC;
- d) Receber uma conta no sistema de certificação da AC;

5.2.3.2 Os certificados, contas e senhas utilizados para identificação e autenticação dos

empregados:

- a) São diretamente atribuídos a um único empregado;
- b) Não são compartilhados;
- c) São restritos às ações associadas ao perfil para o qual foram criados.

5.2.3.3 AC Safeweb implementa um padrão de utilização de "senhas fortes", definido na Política de Segurança implementada e em conformidade com a POLÍTICA DE SEGURANÇA DA ICP-BRASIL[8], juntamente com procedimentos de validação dessas senhas.

5.3 CONTROLES DE PESSOAL

Todos os empregados da AC Safeweb, das ARs e PSS vinculados encarregados de tarefas operacionais têm registrado em contrato ou termo de responsabilidade:

- a) Os termos e as condições do perfil que ocuparão;
- b) O compromisso de observar as normas, políticas e regras aplicáveis da ICP-Brasil;
- c) O compromisso de não divulgar informações sigilosas a que tenham acesso.

5.3.1 ANTECEDENTES, QUALIFICAÇÃO, EXPERIÊNCIA E REQUISITOS DE IDONEIDADE

Todo o pessoal da AC Safeweb e das ARs Vinculadas envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados é admitido conforme o estabelecido na POLÍTICA DE SEGURANÇA DA ICP-BRASIL[8] e na Política de Segurança implementada.

5.3.2 PROCEDIMENTOS DE VERIFICAÇÃO DE ANTECEDENTES

5.3.2.1 Com o propósito de resguardar a segurança e a credibilidade das entidades, todo o pessoal da AC Safeweb e da ARs Vinculadas envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados é submetido a:

- a) Verificação de antecedentes criminais;
- b) Verificação de situação de crédito;
- c) Verificação de histórico de empregos anteriores;
- d) Comprovação de escolaridade e de residência.

5.3.2.2 A AC Safeweb não define requisitos adicionais para a verificação de antecedentes.

5.3.3 REQUISITOS DE TREINAMENTO

5.3.3.1 Todo o pessoal da AC Safeweb e das ARs Vinculadas envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados recebe treinamento documentado, suficiente para o domínio dos seguintes temas:

- a) Princípios e mecanismos de segurança da AC Safeweb e das AR vinculadas;
- b) Sistema de certificação em uso na AC Safeweb;
- c) Procedimentos de recuperação de desastres e de continuidade do negócio;
- d) Reconhecimento de assinaturas e validade dos documentos apresentados, na forma do item 3.1.9 e 3.1.10 e 3.1.11; e
- e) Outros assuntos relativos a atividades sob sua responsabilidade.

5.3.4 FREQUÊNCIA E REQUISITOS PARA RECICLAGEM TÉCNICA

5.3.4.1 Todo o pessoal da AC Safeweb e das ARs Vinculadas envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados é mantido atualizado sobre eventuais mudanças tecnológicas nos sistemas da AC Safeweb .

5.3.5 FREQUÊNCIA E SEQUÊNCIA DE RODÍZIO DE CARGOS

5.3.5.1 A AC Safeweb e as ARs Vinculadas possuem pessoal e efetivo de contingência devidamente treinado, não fazendo uso de rodízio de pessoal.

5.3.6 SANÇÕES PARA AÇÕES NÃO AUTORIZADAS

5.3.6.1 Na eventualidade de uma ação não autorizada, real ou suspeita, ser realizada por pessoa encarregada de processo operacional da AC Safeweb e das ARs Vinculadas a AC Safeweb ou a AR Vinculada suspenderá o acesso dessa pessoa ao seu sistema de certificação e tomará as medidas administrativas e legais cabíveis.

5.3.6.2 O processo administrativo referido acima contem os seguintes itens:

- a) Relato da ocorrência com “modus operandis”;
- b) Identificação dos envolvidos;
- c) Eventuais prejuízos causados;
- d) Punições aplicadas, se for o caso; e

e) Conclusões.

5.3.6.3 Concluído o processo administrativo, a AC Safeweb encaminha suas conclusões à AC Raiz.

5.3.6.4 As punições passíveis de aplicação, em decorrência de processo administrativo, são:

- a) Advertência;
- b) Suspensão por prazo determinado; ou
- c) Impedimento definitivo de exercer funções no âmbito da ICP-Brasil.

5.3.7 REQUISITOS PARA CONTRATAÇÃO DE PESSOAL

5.3.7.1 Todo o pessoal da AC Safeweb e das ARs Vinculadas envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados é contratado conforme o estabelecido na POLÍTICA DE SEGURANÇA DA ICP-BRASIL[8] e na Política de Segurança implementada pela AC Safeweb .

5.3.8 DOCUMENTAÇÃO FORNECIDA AO PESSOAL

5.3.8.1 A AC Safeweb torna disponível para todo o seu pessoal e para o pessoal das ARs Vinculadas:

- a) Sua DPC;
- b) As PCs que implementa;
- c) A POLÍTICA DE SEGURANÇA DA ICP-BRASIL[8] e a sua Política de Segurança;
- d) Documentação operacional relativa a suas atividades;
- e) Contratos, normas e políticas relevantes para suas atividades.

5.3.8.2 Toda a documentação fornecida ao pessoal é classificada segundo a política de classificação de informação definida pela AC Safeweb e é mantida atualizada.

6 CONTROLES TÉCNICOS DE SEGURANÇA

6.1 GERAÇÃO E INSTALAÇÃO DO PAR DE CHAVES

6.1.1 GERAÇÃO DO PAR DE CHAVES

6.1.1.1 O par de chaves criptográficos da AC Safeweb é gerado pela própria AC Safeweb, após o deferimento do seu pedido de credenciamento e a consequente autorização de funcionamento no âmbito da ICP-Brasil, em módulos criptográficos de hardware, conforme definido no DOC-ICP-

01.01, com padrão de segurança obrigatório (Homologação da ICP-Brasil NSH-2 - para a cadeia de certificação V5) definido no DOC-ICP-01.

6.1.1.2 Pares de chaves das AC Subsequente são gerados somente pelas AC Subsequente, titulares do certificado correspondente, que indicarão, por seu(s) representante(s) legal(s), a pessoa responsável pela geração do par de chaves criptográficas. A geração do par de chaves de AC Subsequente é realizada em processo verificável, obrigatoriamente na presença de funcionários de confiança da AC Subsequente treinados para a função. A geração destas chaves obedece a procedimento formalizado, controlado e passível de auditoria. O par de chaves das AC Subsequente é gerado e armazenado em módulo criptográfico de hardware, conforme definido no DOC-ICP-01.01, com padrão de segurança obrigatório (Homologação da ICP-Brasil NSH-2 - para a cadeia de certificação V5) definido no DOC-ICP-01.

6.1.1.3 Não se aplica.

6.1.2 ENTREGA DA CHAVE PRIVADA À ENTIDADE TITULAR

6.1.2.1 A geração e a guarda de uma chave privada é de responsabilidade exclusiva do titular do certificado correspondente.

6.1.3 ENTREGA DA CHAVE PÚBLICA PARA EMISSOR DE CERTIFICADO

6.1.3.1 Para a entrega de sua chave pública à AC Raiz, encarregada da emissão de seu certificado, a AC Safeweb fará uso do padrão PKCS#10.

6.1.3.2 A chave pública de uma AC Subsequente é entregue pelo representante legal da AC Subsequente, em cerimônia específica, em data e hora previamente estabelecidas pela AC Safeweb. Todos os eventos ocorridos nessa cerimônia são registrados para fins de auditoria.

6.1.4 DISPONIBILIZAÇÃO DE CHAVE PÚBLICA DA AC SAFEWEB PARA USUÁRIOS

As formas para a disponibilização do certificado da AC Safeweb, e de todos os certificados da cadeia de certificação, para os usuários da ICP-Brasil, compreendem, entre outras:

- a) Formato PKCS#7 (RFC 2315), que inclui toda a cadeia de certificação, no momento da disponibilização de um certificado para seu titular;
- b) Diretório;
- c) Página Web da AC Safeweb www.safeweb.com.br;
- d) Outros meios seguros a serem aprovados pelo CG da ICP-Brasil.

6.1.5 TAMANHOS DE CHAVE

6.1.5.1 Não se aplica.

6.1.5.2 O tamanho mínimo das chaves criptográficas associadas aos certificados da AC Safeweb é de RSA 4096 bits (V5), conforme definido no DOC-ICP-01.01.

6.1.6 GERAÇÃO DE PARÂMETROS DE CHAVES ASSIMÉTRICAS

6.1.6.1 Os parâmetros de geração de chaves assimétricas da AC Safeweb adotam o padrão obrigatório (Homologação da ICP-Brasil NSH-2 - para a cadeia de certificação V5), conforme definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9]

6.1.7 VERIFICAÇÃO DE QUALIDADE DOS PARÂMETROS

6.1.7.1 Os parâmetros são verificados de acordo com as normas estabelecidas pelo padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

6.1.8 GERAÇÃO DE CHAVE POR HARDWARE OU SOFTWARE

6.1.8.1. As chaves da AC Safeweb são geradas, armazenadas e utilizadas dentro de hardware específico, compatíveis com as normas estabelecidas pelo padrão obrigatório (Homologação da ICP-Brasil NSH-2 - para a cadeia de certificação V5), conforme definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

6.1.8.2. As chaves criptográficas das AC Subsequentes são geradas, armazenadas e utilizadas dentro de hardware específico, compatível com os requisitos no padrão obrigatório (Homologação da ICP-Brasil NSH-2 - para a cadeia de certificação V5), conforme definido no DOC-ICP-01.01, baseado nos requisitos aplicáveis estabelecidos pelo documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [7].

6.1.9 PROPÓSITO DE USO DE CHAVE (CONFORME O CAMPO "KEY USAGE" NA X.509 V3)

6.1.9.1 A chave privada das AC Subsequentes é utilizada apenas para a assinatura dos certificados por ela emitidos e para assinatura de sua LCR.

6.1.9.2 A chave privada da AC Safeweb é utilizada apenas para a assinatura dos certificados por ela emitidos e de sua LCR.

6.2 PROTEÇÃO DA CHAVE PRIVADA

As chaves privadas da AC Safeweb são armazenadas de forma cifrada nos mesmos componentes seguros de hardware utilizados para sua geração. O acesso a esses componentes é controlado por meio de chave criptográfica de ativação.

6.2.1 PADRÕES PARA MÓDULO CRIPTOGRÁFICO

6.2.1.1. O módulo criptográfico de geração de chaves assimétricas da AC Safeweb adota o padrão obrigatório (Homologação da ICP-Brasil NSH-2 - para a cadeia de certificação V5), conforme definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

6.2.1.2 Não se aplica.

6.2.2 CONTROLE "N de M" PARA CHAVE PRIVADA

6.2.2.1 Para a utilização das suas chaves privadas, a AC Safeweb define a forma de controle múltiplo, do tipo “n” pessoas de um grupo de “m”.

6.2.2.2 A AC Safeweb estabelece como exigência de controle múltiplo para a utilização das suas chaves privadas:

a) Número mínimo de 2 ("n") (duas) pessoas de um grupo de 8 ("m") (oito) pessoas para utilização das suas chaves privadas.

6.2.3 RECUPERAÇÃO (ESCROW) DE CHAVE PRIVADA

6.2.3.1 Não é permitida, no âmbito da ICP-Brasil, a recuperação (*escrow*) de chaves privadas, isto é, não se permite que terceiros possam legalmente obter uma chave privada sem o consentimento de seu titular.

6.2.4 CÓPIA DE SEGURANÇA (BACKUP) DE CHAVE PRIVADA

6.2.4.1 Qualquer entidade titular de certificado pode, a seu critério, manter cópia de segurança de sua própria chave privada.

6.2.4.2 A AC Safeweb mantém cópia de segurança de sua própria chave privada.

6.2.4.3 Não se aplica.

6.2.4.4. Em qualquer caso, a cópia de segurança é armazenada, cifrada, por algoritmo simétrico definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9], e protegida com um nível de segurança não inferior àquele definido para a chave original.

6.2.5 ARQUIVAMENTO DE CHAVE PRIVADA

6.2.5.1 A AC Safeweb não emite certificados de sigilo. Não são arquivadas chaves privadas de assinatura digital.

6.2.5.2 Define-se arquivamento como o armazenamento da chave privada para seu uso futuro, após o período de validade do certificado correspondente.

6.2.6 INSERÇÃO DE CHAVE PRIVADA EM MÓDULO CRIPTOGRÁFICO

6.2.6.1 A AC Safeweb gera seus pares de chaves diretamente, sem inserções, em módulos de hardware criptográfico onde as chaves serão utilizadas.

6.2.7 MÉTODO DE ATIVAÇÃO DE CHAVE PRIVADA

6.2.7.1 Para a ativação das chaves privadas da AC Safeweb exige-se o número mínimo de 2 ("n") (duas) pessoas de um grupo de 8 ("m") (oito). A confirmação da identidade desses agentes é feita através de senhas, só lhes sendo permitido o acesso ao ambiente em duplas devidamente autorizadas.

6.2.8 MÉTODO DE DESATIVAÇÃO DE CHAVE PRIVADA

6.2.8.1 Para a desativação das chaves privadas da AC Safeweb exige-se o número mínimo de 2 ("n") (duas) pessoas de um grupo de 8 ("m") (oito). A confirmação da identidade desses agentes é feita através de senhas, só lhes sendo permitido o acesso ao ambiente em duplas devidamente autorizadas.

6.2.9 MÉTODO DE DESTRUIÇÃO DE CHAVE PRIVADA

6.2.9.1 Para a destruição das chaves privadas da AC Safeweb exige-se o número mínimo de 2 ("n") (duas) pessoas de um grupo de 8 ("m") (oito). A confirmação da identidade desses agentes é feita através de senhas, só lhes sendo permitido o acesso ao ambiente em duplas devidamente autorizadas. As mídias de armazenamento das chaves privadas são reinicializadas de forma a não restarem nelas informações sensíveis.

6.3 OUTROS ASPECTOS DO GERENCIAMENTO DO PAR DE CHAVES

6.3.1 ARQUIVAMENTO DE CHAVE PÚBLICA

6.3.1.1 As chaves públicas da AC Safeweb e dos titulares de certificados das ACs Subsequentes por

ela emitidos, bem como as LCR emitidas permanecem armazenadas após a expiração dos certificados correspondentes, permanentemente, para verificação de assinaturas geradas durante seu período de validade.

6.3.2 PERÍODOS DE USO PARA CHAVES PÚBLICAS E PRIVADAS

6.3.2.1. As chaves privadas dos titulares dos certificados das ACs subsequentes emitidos pela AC Safeweb são utilizadas apenas durante o período de validade dos certificados correspondentes. As correspondentes chaves públicas podem ser utilizadas durante todo período de tempo determinado pela legislação aplicável, para verificação de assinaturas geradas durante o prazo de validade dos respectivos certificados.

6.3.2.2. Não se aplica.

6.3.2.3. Não se aplica.

6.3.2.4. A validade admitida para certificados da AC Safeweb é limitada à validade do certificado da AC que o emitiu, desde que mantido o mesmo padrão de algoritmo para a geração de chaves assimétricas implementado pela AC hierarquicamente superior.

6.4 DADOS DE ATIVAÇÃO

6.4.1 GERAÇÃO E INSTALAÇÃO DOS DADOS DE ATIVAÇÃO

6.4.1.1. Os dados de ativação do equipamento de criptografia que armazena as chaves privadas da AC Safeweb são únicos e aleatórios.

6.4.1.2. Não se aplica

6.4.2 PROTEÇÃO DOS DADOS DE ATIVAÇÃO

6.4.2.1. A AC Safeweb garante que os dados de ativação de sua chave privada são protegidos contra uso não autorizado, por meio de mecanismo de criptografia e de controle de acesso físico.

6.4.2.2. Os dados de ativação da chave privada da entidade titular do certificado, se utilizados, são protegidos contra o uso não autorizado.

6.4.3 OUTROS ASPECTOS DOS DADOS DE ATIVAÇÃO

6.4.3.1 Não se aplica.

6.5 CONTROLES DE SEGURANÇA COMPUTACIONAL

6.5.1 REQUISITOS TÉCNICOS ESPECÍFICOS DE SEGURANÇA COMPUTACIONAL

6.5.1.1 A geração do par de chaves da AC Safeweb é realizada off-line, para impedir o acesso remoto não autorizado.

6.5.1.2 A geração dos pares de chaves das AC Subsequentes é realizada em ambiente próprio, protegido de modo a minimizar os riscos potenciais inerentes desta operação. O ambiente computacional é mantido off-line para impedir o acesso remoto não autorizado.

6.5.1.3 Cada computador servidor da AC Safeweb, relacionado diretamente com os processos de emissão, expedição, distribuição, revogação ou gerenciamento de certificados, implementam, entre outras, as seguintes características:

- a) Controle de acesso aos serviços e perfis da AC Safeweb;
- b) Clara separação das tarefas e atribuições relacionadas a cada perfil qualificado da AC Safeweb;
- c) Uso de criptografia para segurança de base de dados, quando exigido pela classificação de suas informações;
- d) Geração e armazenamento de registros de auditoria da AC Safeweb;
- e) Mecanismos internos de segurança para garantia da integridade de dados e processos críticos;
- f) Mecanismos para cópias de segurança (backup).

6.5.1.4 Essas características são implementadas pelo sistema operacional ou por meio da combinação deste com o sistema de certificação e com mecanismos de segurança física.

6.5.1.5 Qualquer equipamento, ou parte deste, ao ser enviado para manutenção tem apagadas as informações sensíveis nele contidas e controlados seu número de série e as datas de envio e de recebimento. Ao retornar às instalações da AC Safeweb, o equipamento que passou por manutenção é inspecionado. Em todo equipamento que deixa de ser utilizado em caráter permanente, serão destruídas de maneira definitiva todas as informações sensíveis armazenadas, relativas à atividade da AC Safeweb. Todos esses eventos são registrados para fins de auditoria.

6.5.1.6 Qualquer equipamento incorporado à AC Safeweb é preparado e configurado como previsto na Política de Segurança, implementada de forma a apresentar o nível de segurança necessário à sua finalidade.

6.5.2 CLASSIFICAÇÃO DA SEGURANÇA COMPUTACIONAL

6.5.2.1 A AC Safeweb aplica configurações de segurança computacional baseadas no *Common Criteria* e desenvolvidas para o sistema operacional Windows Server 2012 R2. O fabricante

disponibiliza as atualizações do sistema operacional utilizado nos servidores do Sistema de Certificação Digital da AC Safeweb.

6.5.3 CONTROLES DE SEGURANÇA PARA AS AUTORIDADES DE REGISTRO

6.5.3.1 A AC Safeweb implementa requisitos de segurança computacional das estações de trabalho e dos computadores portáteis utilizados pela AR Vinculada para os processos de validação e aprovação de certificados.

6.5.3.2 São incluídos os seguintes requisitos especificados no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP-BRASIL [1]:

As estações de trabalho da AR, incluindo equipamentos portáteis, estão protegidas contra ameaças e ações não-autorizadas, bem como contra o acesso, uso ou exposição indevidos.

As estações de trabalho da AR, incluindo equipamentos portáteis, recebem as seguintes configurações de segurança:

- a) Controle de acesso lógico ao sistema operacional;
- b) Exigência de uso de senhas fortes;
- c) Diretivas de senha e de bloqueio de conta;
- d) Logs de auditoria do sistema operacional ativados, registrando:
 - i. Iniciação e desligamento do sistema;
 - ii. Tentativas de criar, remover, definir senhas ou mudar privilégios de sistema dos operadores da AR;
 - iii. Mudanças na configuração da estação;
 - iv. Tentativas de acesso (*login*) e de saída do sistema (*logoff*);
 - v. Tentativas não-autorizadas de acesso aos arquivos de sistema;
 - vi. Tentativas de iniciar, remover, habilitar e desabilitar usuários e de atualizar e recuperar suas chaves.
- e) Antivírus, *antitrojan* e *antispyware*, instalados, atualizados e habilitados;
- f) *Firewall* pessoal ativado, com permissões de acesso mínimas necessárias às atividades, podendo esse ser substituído por *firewall* corporativo, para equipamentos instalados em redes que possuam esse dispositivo;
- g) Proteção de tela acionada no máximo após dois minutos de inatividade e exigindo senha do usuário para desbloqueio;

- h) Sistema operacional mantido atualizado, com aplicação de correções necessárias (*patches*, *hotfix*, etc.);
- i) Utilização apenas de *softwares* licenciados e necessários para a realização das atividades do usuário;
- j) Impedimento de *login* remoto, via outro equipamento ligado à rede de computadores utilizada pela AR, exceto para as atividades de suporte remoto;
- k) Utilização da data e Hora Legal Brasileira.

Os *logs* de auditoria do sistema operacional registram os acessos aos equipamentos e ficam armazenados localmente por um período mínimo de 60 dias.

A análise desses *logs* somente é realizada em caso de suspeitas quanto a acessos não autorizados ou para dirimir outros tipos de dúvidas que possam surgir sobre a utilização dos equipamentos.

O Agente de Registro não possui perfil de administrador ou senha de *root* dos equipamentos, ficando essa tarefa delegada a terceiros da própria organização, para permitir segregação de funções.

O aplicativo que faz interface entre a AR e o sistema de certificação da AC possui as seguintes características de segurança:

- a) Acesso permitido somente mediante autenticação por meio do certificado do tipo A3 de Agente de Registro;
- b) Acesso permitido somente a partir de equipamentos autenticados no sistema (ex. usando cadastramento prévio de endereço IP, certificado digital de equipamento ou outra solução que permita ao sistema identificar de forma unívoca o equipamento);
- c) *Timeout* de sessão de acordo com a análise de risco da AC;
- d) Registro em *log* de auditoria dos eventos citados no item 4.5.1 do DOC-ICP-05 [1];
- e) Histórico da inclusão e exclusão dos Agentes de Registro no sistema e das permissões concedidas ou revogadas;
- f) Registro em *log*, para em cada certificado emitido, informando se a validação da solicitação de certificados foi executada interna ou externamente ao ambiente da AR;
- g) Mecanismo para revogação automática dos certificados digitais emitidos fora do ambiente da AR e que não tenham sido verificados pelo segundo Agente de Registro, mediante cópia da documentação apresentada na etapa de validação, até o momento do início da validade do certificado.

O aplicativo da AR:

- a) Foi desenvolvido com documentação formal;

- b) Possui mecanismos para controle de versões;
- c) Possui documentação dos testes realizados em cada versão;
- d) Possui documentação comprovando a homologação de cada versão em ambiente com as mesmas características do que será usado em produção, sendo esses ambientes, porém, obrigatoriamente apartados entre si;
- e) Possui aprovação documentada do gerente da AC, ou responsável designado, para colocar cada versão em ambiente de produção.

Os logs gerados por esse aplicativo são armazenados na AC pelo prazo de 6 (seis) anos, conforme previsto no item 4.6.2. do DOC-ICP-05.

6.6 CONTROLES TÉCNICOS DO CICLO DE VIDA

6.6.1 CONTROLES DE DESENVOLVIMENTO DE SISTEMA

6.6.1.1 A AC Safeweb adota tecnologias de certificação digital e efetua as devidas customizações para adequar as necessidades do ambiente da AC, as quais são desenvolvidas por empregados da AC Safeweb. Essas customizações são realizadas inicialmente em um ambiente de desenvolvimento e após concluídas são colocadas em um ambiente de homologação. Finalizado o processo de homologação é encaminhado um pedido para o Coordenador da AC, que avalia e decide quanto à sua implementação.

6.6.1.2 Os processos de projeto e desenvolvimento conduzidos pela AC Safeweb proveem documentação suficiente para suportar avaliações externas de segurança dos componentes da AC.

6.6.2 CONTROLES DE GERENCIAMENTO DE SEGURANÇA

6.6.2.1 A AC Safeweb utiliza metodologia formal de gerenciamento de configuração para a instalação e a contínua manutenção do seu sistema de certificação.

6.6.2.2 A AC Safeweb verifica os níveis configurados de segurança através de ferramentas do próprio sistema operacional. As verificações são feitas através da emissão de comandos de sistema comparando-se com as configurações aprovadas. Em caso de divergência, são tomadas as medidas para recuperação da situação, conforme a natureza do problema, e, posteriormente, é realizada a averiguação do fato gerador para evitar sua recorrência.

6.6.3 CLASSIFICAÇÕES DE SEGURANÇA DE CICLO DE VIDA

6.6.3.1 Não se aplica.

6.6.4 CONTROLES NA GERAÇÃO DE LCR

6.6.4.1 Antes de publicadas, todas as LCRs geradas pela AC Safeweb são checadas quanto à consistência de seu conteúdo, comparando-o com o conteúdo esperado em relação a número da LCR, data/hora de emissão e outras informações relevantes.

6.7 CONTROLES DE SEGURANÇA DE REDE

6.7.1 DIRETRIZES GERAIS

6.7.1.1 Neste item são descritos os controles relativos à segurança da rede da AC Safeweb, incluindo *firewalls* e recursos similares.

6.7.1.2 Nos servidores do sistema de certificação da AC Safeweb, somente os serviços estritamente necessários para o funcionamento da aplicação são habilitados.

6.7.1.3 Todos os servidores e elementos de infraestrutura e proteção de rede, tais como roteadores, *hubs*, *switches*, *firewalls* e sistemas de detecção de intrusão - IDS, localizados no segmento de rede que hospeda o sistema de certificação da AC Safeweb, estão localizados e operam em ambiente de nível 4.

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

6.7.1.5 O acesso lógico aos elementos de infraestrutura e proteção de rede é restrito por meio de sistema de autenticação e autorização de acesso. Os roteadores conectados a redes externas implementam filtros de pacotes de dados, que permitem somente as conexões aos serviços e servidores previamente definidos como passíveis de acesso externo.

6.7.2 FIREWALL

6.7.2.1 Mecanismos de *firewall* são implementados em equipamentos de utilização específica configurados exclusivamente para tal função. *Firewalls* promovem o isolamento, em sub-redes específicas, dos equipamentos servidores com acesso externo - a conhecida "zona desmilitarizada" (DMZ) - em relação aos equipamentos com acesso exclusivamente interno à AC Safeweb.

6.7.2.2 O software de *firewall*, entre outras características, implementa registros de auditoria.

6.7.3 SISTEMA DE DETECÇÃO DE INTRUSÃO – IDS

6.7.3.1 O sistema de detecção de intrusão tem capacidade de ser configurado para reconhecer ataques em tempo real e respondê-los automaticamente, com medidas tais como: enviar *traps* SNMP, executar programas definidos pela administração da rede, enviar e-mail aos administradores, enviar mensagens de alerta aos *firewalls* ou ao terminal de gerenciamento, promover a desconexão automática de conexões suspeitas, ou ainda a reconfiguração dos *firewalls*.

6.7.3.2 O sistema de detecção de intrusão tem capacidade de reconhecer diferentes padrões de ataques, inclusive contra o próprio sistema, apresentando a possibilidade de atualização da sua base de reconhecimento.

6.7.3.3 O sistema de detecção de intrusão provê o registro dos eventos em *logs*, recuperáveis em arquivos do tipo texto, além de implementar uma gerência de configuração.

6.7.4 REGISTRO DE ACESSOS NÃO AUTORIZADOS À REDE

6.7.4.1 As tentativas de acesso não autorizado - em roteadores, *firewalls* ou IDS - são registradas em arquivos para posterior análise. A frequência de exame dos arquivos de registro é, no mínimo, diária e todas as ações tomadas em decorrência desse exame são documentadas.

6.8 CONTROLES DE ENGENHARIA DO MÓDULO CRIPTOGRÁFICO

6.8.1 O módulo criptográfico utilizado para armazenamento da chave privada da AC Safeweb adota o padrão padrão obrigatório (Homologação da ICP-Brasil NSH-2 - para a cadeia de certificação V5), conforme definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

7 PERFIS DE CERTIFICADO E LCR

7.1 DIRETRIZES GERAIS

7.1.1. Nos seguintes itens desta DPC são descritos os aspectos dos certificados e LCR emitidos pela AC Safeweb.

7.1.2. Não se aplica.

7.1.3. Nos itens seguintes também são especificados o formato dos certificados emitidos pela AC Safeweb.

7.2 PERFIL DO CERTIFICADO

7.2.1 Os certificados emitidos pela AC Safeweb estão em conformidade com o formato definido pelo padrão ITU X.509 ou ISO/IEC 9594-8.

7.2.1 NÚMERO (S) DE VERSÃO

7.2.1.1 Todos os certificados emitidos pela AC Safeweb implementam a versão 3 do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 5280.

7.2.2 EXTENSÕES DE CERTIFICADO

7.2.2.1 Para os certificados emitidos sob a cadeia da Autoridade Certificadora Raiz da ICP-Brasil:
Os certificados emitidos pela AC Safeweb obedecem a ICP-Brasil, que define como obrigatórias as seguintes extensões:

- a) **Authority Key Identifier**, não crítica: o campo keyIdentifier contém o hash SHA-1 da chave pública da AC Safeweb;
- b) **Subject Key Identifier**, não crítica: contém o hash SHA-1 da chave pública da AC titular do certificado;
- c) **Key Usage**, crítica: somente os bits keyCertSign e CRLSign estão ativados;
- d) **Certificate Policies**, não crítica:
 - d.1) o campo policyIdentifier contém o OID desta DPC (OID = 2.16.76.1.1.84);
 - d.2) o campo policyQualifiers contém o endereço Web da DPC da AC Safeweb (<http://repositorio.acsafeweb.com.br/ac-safeweb/dpc-acsafeweb.pdf>)
- e) **BasicConstraints**, não crítica: contém o campo cA=True.
- f) **CRL Distribution Points**, não crítica: contém o endereço Web onde se obtém a LCR da AC Safeweb:

Para certificados emitidos na V5:

- f.1) <http://repositorio.acsafeweb.com.br/ac-safeweb/lcr-ac-safeweb.crl>
- f.2) <http://repositorio2.acsafeweb.com.br/ac-safeweb/lcr-ac-safeweb.crl>

7.2.3 IDENTIFICADORES DE ALGORITMO

7.2.3.1 Os certificados emitidos pela AC Safeweb são assinados com algoritmo RSA com SHA-512

como função de hash (OID = 1.2.840.113549.1.1.13) nas hierarquias V5 conforme o padrão PKCS#1.

7.2.4 FORMATOS DE NOME

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

C = BR

O = ICP-Brasil

OU = Razão Social da AC Subsequente

CN = nome da AC Subsequente

7.2.5 RESTRIÇÕES DE NOME

7.2.5.1. Neste item são descritas as restrições aplicáveis para os nomes dos titulares de certificados.

7.2.5.2. As restrições aplicáveis para os nomes dos titulares de certificado emitidos pela AC Safeweb são as seguintes:

Não são admitidos sinais de acentuação, trema ou cedilhas;

Apenas são admitidos sinais alfanuméricos e os caracteres especiais descritos na tabela abaixo:

Caractere	Código NBR9611 (hexadecimal)
Branco	20
!	21
"	22
#	23
\$	24
%	25
&	26
'	27
(28
)	29
*	2A
+	2B
,	2C
-	2D
.	2E
/	2F
:	3A

;	3B
=	3D
?	3F
@	40
\	5C

7.2.6 OID (OBJECT IDENTIFIER) DE DPC

7.2.6.1 O OID desta DPC AC Safeweb é **2.16.76.1.1.84**.

7.2.7 USO DA EXTENSÃO "POLICY CONSTRAINTS"

7.2.7.1 Não se aplica.

7.2.8 SINTAXE E SEMÂNTICA DOS QUALIFICADORES DE POLÍTICA

7.2.8.1 O campo policyQualifiers da extensão "Certificate Policies" contém o endereço web da DPC da AC Safeweb <http://repositorio.acsafeweb.com.br/ac-safeweb/dpc-acsafeweb.pdf>.

7.2.9 SEMÂNTICA DE PROCESSAMENTO PARA EXTENSÕES CRÍTICAS

7.2.9.1 Extensões críticas são interpretadas conforme a RFC 5280.

7.3 PERFIL DE LCR

7.3.1 NÚMERO (S) DE VERSÃO

7.3.1.1 As LCRS geradas pela AC Safeweb implementam a versão 2 do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 5280.

7.3.2 EXTENSÕES DE LCR E DE SUAS ENTRADAS

7.3.2.1 Neste item são descritas todas as extensões de LCR utilizadas pela AC Safeweb e sua criticidade.

7.3.2.2 As LCRs da AC Safeweb obedecem a ICP-Brasil que define como obrigatórias as seguintes extensões:

- a) "**Authority Key Identifier**": contém o hash SHA-1 da chave pública da AC que assina a LCR;
- b) "**CRL Number**", não crítica: contém um número sequencial para cada LCR emitida pela AC

Safeweb;

8 ADMINISTRAÇÃO DE ESPECIFICAÇÃO

8.1 PROCEDIMENTOS DE MUDANÇA DE ESPECIFICAÇÃO

8.1.1 Qualquer alteração nesta DPC AC Safeweb é submetida à aprovação do CG da ICP-Brasil. Esta DPC - AC Safeweb é atualizada sempre que uma nova PC implementada pela AC Safeweb o exigir.

8.2 POLÍTICAS DE PUBLICAÇÃO E NOTIFICAÇÃO

8.2.1 Esta DPC AC Safeweb está disponível para a comunidade no endereço web: <http://www.safeweb.com.br/ac/repositorio>.

8.3 PROCEDIMENTOS DE APROVAÇÃO

8.3.1 Esta DPC AC Safeweb foi submetida à aprovação, durante o processo de credenciamento da AC Safeweb, conforme o determinado pelo documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6].

9 DOCUMENTOS REFERENCIADOS

9.1 RESOLUÇÕES DO COMITÊ-GESTOR DA ICP-Brasil

9.1.1 Os documentos abaixo são aprovados por Resoluções do Comitê-Gestor da ICP-Brasil, podendo ser alterados, quando necessário, pelo mesmo tipo de dispositivo legal. O sítio <http://www.iti.gov.br> publica a versão mais atualizada desses documentos e as Resoluções que os aprovaram.

Ref.	Nome do documento	Código
[2]	CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-09
[3]	CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-08
[6]	CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-03

[7]	REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL	DOC-ICP-04
[8]	POLÍTICA DE SEGURANÇA DA ICP-BRASIL	DOC-ICP-02
[10]	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DE CERTIFICAÇÃO DAS AUTORIDADES CERTIFICADORAS DA ICP-BRASIL	DOC-ICP-05

9.2 INSTRUÇÕES NORMATIVAS DA AC RAIZ

9.2.1 Os documentos abaixo são aprovados por Instrução Normativa da AC Raiz, podendo ser alterados, quando necessário, pelo mesmo tipo de dispositivo legal. O sítio <http://www.it.gov.br> publica a versão mais atualizada desses documentos e as Instruções Normativas que os aprovaram.

Ref.	Nome do documento	Código
[1]	CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP-BRASIL	DOC-ICP-03.01
[9]	PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL	DOC-ICP-01.01

9.3 DOCUMENTOS DA AC RAIZ

Ref.	Nome do documento	Código
[4]	MODELO DE TERMO DE TITULARIDADE	ADE-ICP-05.A

10 LISTA DE ACRÔNIMOS

AC	Autoridade Certificadora
AC Raiz	Autoridade Certificadora Raiz da ICP-Brasil
AR	Autoridades de Registro
CEI	Cadastro Específico do INSS
CG	Comitê Gestor
CMM-SEI	Capability Maturity Model do Software Engineering Institute
CMVP	Cryptographic Module Validation Program
CN	Common Name

CNE	Carteira Nacional de Estrangeiro
CNPJ	Cadastro Nacional de Pessoas Jurídicas -
COBIT	<i>Control Objectives for Information and related Technology</i>
COSO	<i>Comitee of Sponsoring Organizations</i>
CPF	Cadastro de Pessoas Físicas
DMZ	Zona Desmilitarizada
DN	<i>Distinguished Name</i>
DPC	Declaração de Práticas de Certificação
ICP-Brasil	Infra-Estrutura de Chaves Públicas Brasileira
IDS	Sistemas de Detecção de Intrusão
IEC	<i>International Electrotechnical Commission</i>
ISO	<i>International Organization for Standardization</i>
ITSEC	<i>European Information Technology Security Evaluation Criteria</i>
ITU	<i>International Telecommunications Union</i>
LCR	Lista de Certificados Revogados
NBR	Norma Brasileira
NIS	Número de Identificação Social
NIST	<i>National Institute of Standards and Technology</i>
OCSP	<i>Online Certificate Status Protocol</i>
OID	<i>Object Identifier</i>
OU	<i>Organization Unit</i>
PASEP	Programa de Formação do Patrimônio do Servidor Público
PC	Políticas de Certificado
PCN	Plano de Continuidade de Negócio
PIS	Programa de Integração Social
POP	<i>Proof of Possession</i>
PS	Política de Segurança
PSS	Prestadores de Serviço de Suporte
RFC	<i>Request For Comments</i>
RG	Registro Geral
SNMP	<i>Simple Network Management Protocol</i>
TCSEC	<i>Trusted System Evaluation Criteria</i>
TSDM	<i>Trusted Software Development Methodology</i>
UF	Unidade de Federação
URL	<i>Uniform Resource Location</i>