



SOLUTI

Certificação Digital

**Declaração de Práticas de Certificação
da Autoridade Certificadora**

SOLUTI

(DPC AC SOLUTI)

OID 2.16.76.1.1.46

Versão 1.0 de 1 de novembro de 2012

Classificação: Ostensivo

www.acsoluti.com.br

Sumário

Controle de Versão.....	6
Tabela de Siglas.....	7
1 INTRODUÇÃO.....	9
1.1 Visão Geral.....	9
1.2 Identificação.....	9
1.3 Comunidade e Aplicabilidade.....	9
1.3.1 Autoridades Certificadoras.....	9
1.3.2 Autoridades de Registro.....	9
1.3.2.1 Endereço da página web (URL).....	9
1.3.2.2 Atualização.....	9
1.3.3 Prestador de Serviço de Suporte.....	9
1.3.3.1 Identificação.....	9
1.3.3.2 Definição e classificação.....	9
1.3.4 Titulares de Certificado.....	10
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 AC SOLUTI.....	10
2.1.2 Obrigações das ARs.....	11
2.1.3 Obrigações do Titular do Certificado.....	11
2.1.4 Direitos da Terceira Parte (Relying Party).....	12
2.1.4.1 Definição.....	12
2.1.4.2 Direitos.....	12
2.1.4.3 Não exercício dos direitos.....	12
2.1.5 Obrigações do Repositório.....	12
2.2 Responsabilidades.....	12
2.2.1 Responsabilidades da AC SOLUTI.....	12
2.2.1.1 Danos.....	12
2.2.1.2 Responsabilidade solidária.....	12
2.2.1.3 Da Ausência de Responsabilidade pelo RIC.....	12
2.2.2 Responsabilidades da AR.....	12
2.3 Responsabilidade Financeira.....	12
2.3.1 Indenizações devidas pela terceira parte usuária (Relying Party).....	12
2.3.2 Relações Fiduciárias.....	12
2.3.3 Processos Administrativos.....	12
2.4 Interpretação e Execução.....	13
2.4.1 Legislação.....	13
2.4.2 Forma de interpretação e notificação.....	13
2.4.3 Procedimentos de solução de disputa.....	13
2.5 Tarifas de Serviço.....	13
2.5.1 Tarifas de emissão e renovação de certificados.....	13
2.5.2 Tarifas de acesso ao certificado.....	13
2.5.3 Tarifas de revogação ou de acesso à informação de status.....	13
2.5.4 Tarifas para outros serviços.....	13
2.5.5 Política de reembolso.....	13
2.6 Publicação e Repositório.....	14
2.6.1 Publicação de informação da AC SOLUTI.....	14
2.6.2 Frequência de publicação.....	14
2.6.3 Controles de acesso.....	14
2.6.4 Repositórios.....	14
2.7 Fiscalização e Auditoria de conformidade.....	14
2.8 Sigilo.....	15
2.8.1 Disposições Gerais.....	15

2.8.2	Tipos de informações sigilosas.....	15
2.8.3	Tipos de informações não sigilosas.....	15
2.8.4	Divulgação de informação de revogação/suspensão de certificado.....	15
2.8.5	Quebra de sigilo por motivos legais.....	16
2.8.6	Informações a terceiros.....	16
2.8.7	Divulgação por solicitação do titular.....	16
2.8.8	Outras circunstâncias de divulgação de informação.....	16
2.9	Direitos de Propriedade Intelectual.....	16
3	IDENTIFICAÇÃO E AUTENTICAÇÃO.....	16
3.1	Registro Inicial.....	16
3.1.1	Disposições Gerais.....	16
3.1.2	Tipos de nomes.....	18
3.1.3	Necessidade de nomes significativos.....	18
3.1.4	Regras para interpretação de vários tipos de nomes.....	18
3.1.5	Unicidade de nomes.....	18
3.1.6	Procedimento para resolver disputa de nomes.....	18
3.1.7	Reconhecimento, autenticação e papel de marcas registradas.....	18
3.1.8	Método para comprovar a posse de chave privada.....	18
3.1.9	Autenticação da identidade de um indivíduo.....	18
3.1.9.1	Documentos para efeito de identificação de um indivíduo.....	18
3.1.9.2	Informações contidas no certificado emitido para um indivíduo.....	19
3.1.10	Autenticação da Identidade de uma organização.....	19
3.1.10.1	Disposições Gerais.....	19
3.1.10.2	Documentos para efeitos de identificação de uma organização.....	20
3.1.10.3	Informações contidas no certificado emitido para uma organização.....	20
3.1.11	Autenticação da Identidade de um equipamento ou aplicação.....	20
3.1.11.1	Disposições Gerais.....	20
3.1.11.2	Procedimentos para efeitos de identificação de um equipamento ou aplicação.....	20
3.1.11.3	Informações contidas no certificado emitido para um equipamento ou aplicação.....	21
3.2	Geração de novo par de chaves antes da expiração do atual.....	21
3.3	Geração de novo par de chaves após expiração ou revogação.....	21
3.4	Solicitação de Revogação.....	21
4	REQUISITOS OPERACIONAIS.....	21
4.1	Solicitação de Certificado.....	21
4.2	Emissão de Certificado.....	22
4.3	Aceitação de Certificado.....	22
4.4	Suspensão e Revogação de Certificado.....	22
4.4.1	Circunstâncias para revogação.....	22
4.4.2	Quem pode solicitar revogação.....	23
4.4.3	Procedimento para solicitação de revogação.....	23
4.4.4	Prazo para solicitação de revogação.....	23
4.4.5	Circunstâncias para suspensão.....	24
4.4.6	Quem pode solicitar suspensão.....	24
4.4.7	Procedimento para solicitação de suspensão.....	24
4.4.8	Limites no período de suspensão.....	24
4.4.9	Frequência de emissão de LCR.....	24
4.4.10	Requisitos para verificação de LCR.....	24
4.4.11	Disponibilidade para revogação/verificação de status on-line.....	24
4.4.12	Requisitos para verificação de revogação on-line.....	24
4.4.13	Outras formas disponíveis para divulgação de revogação.....	24
4.4.14	Requisitos para verificação de outras formas de divulgação de revogação.....	24
4.4.15	Requisitos especiais para o caso de comprometimento de chave.....	25
4.5	Procedimentos de Auditoria de Segurança.....	25
4.5.1	Tipos de Evento Registrados.....	25
4.5.2	Frequência de auditoria de registros (logs).....	26
4.5.3	Período de Retenção para registros (logs) de Auditoria.....	26
4.5.4	Proteção de registro (log) de Auditoria.....	26
4.5.5	Procedimentos para cópia de segurança (backup) de registro (log) de auditoria.....	26
4.5.6	Sistema de coleta de dados de auditoria.....	26

4.5.7	Notificação de agentes causadores de eventos.....	26
4.5.8	Avaliações de vulnerabilidade.....	27
4.6	Arquivamento de Registros.....	27
4.6.1	Tipos de registros arquivados.....	27
4.6.2	Período de retenção para arquivo.....	27
4.6.3	Proteção de arquivos.....	27
4.6.4	Procedimentos para cópia de segurança (backup) de arquivos.....	27
4.6.5	Requisitos para datação de registros.....	27
4.6.6	Sistema de coleta de dados de arquivo.....	27
4.6.7	Procedimentos para obter e verificar informação de arquivo.....	28
4.7	Troca de chave.....	28
4.8	Comprometimento e Recuperação de Desastre.....	28
4.8.1	Recursos computacionais, software e dados corrompidos.....	28
4.8.2	Certificado de entidade é revogado.....	28
4.8.3	Chave de entidade é comprometida.....	28
4.8.4	Segurança dos recursos após desastre natural ou de outra natureza.....	28
4.8.5	Atividades das Autoridades de Registro.....	28
4.9	Extinção dos serviços da AC, AR ou PSS.....	29
5	CONTROLES DE SEGURANÇA FÍSICA, PROCEDIMENTAL E DE PESSOAL.....	29
5.1	Controle Físico.....	29
5.1.1	Construção e localização das instalações de AC.....	29
5.1.2	Acesso físico nas instalações de AC SOLUTI.....	30
5.1.2.1	Níveis de Acesso.....	30
5.1.2.1.2	Nível 1.....	30
5.1.2.1.4	Nível 2.....	30
5.1.2.1.5	Nível 3.....	30
5.1.2.1.8	Nível 4.....	30
5.1.2.1.12	Nível 5.....	31
5.1.2.1.14	Nível 6.....	31
5.1.2.2	Sistema físico de detecção.....	31
5.1.2.3	Sistema de Controle de Acesso.....	32
5.1.2.4	Mecanismos de emergência.....	32
5.1.3	Energia e ar condicionado nas instalações da AC.....	32
5.1.4	Exposição à água nas instalações da AC.....	33
5.1.5	Prevenção e proteção contra incêndio nas instalações da AC.....	33
5.1.6	Armazenamento de mídia nas instalações da AC SOLUTI.....	33
5.1.7	Destruição de lixo nas instalações da AC SOLUTI.....	33
5.1.8	Instalações de segurança (backup) externas (off-site) para AC SOLUTI.....	33
5.1.9	Instalações técnicas de AR.....	33
5.2	Controles Procedimentais.....	33
5.2.1	Perfis qualificados.....	33
5.2.2	Número de pessoas necessário por tarefa.....	34
5.2.3	Identificação e autenticação para cada perfil.....	34
5.3	Controles de Pessoal.....	34
5.3.1	Antecedentes, qualificação, experiência e requisitos de idoneidade.....	35
5.3.2	Procedimentos de Verificação de Antecedentes.....	35
5.3.3	Requisitos de treinamento.....	35
5.3.4	Frequência e requisitos para reciclagem técnica.....	35
5.3.5	Frequência e sequência de rodízios de cargos.....	35
5.3.6	Sanções para ações não autorizadas.....	35
5.3.7	Requisitos para contratação de pessoal.....	36
5.3.8	Documentação fornecida ao pessoal.....	36
6	CONTROLES TÉCNICOS DE SEGURANÇA.....	36
6.1	Geração e Instalação do Par de chaves.....	36
6.1.1	Geração do Par de Chaves.....	36
6.1.2	Entrega da chave privada à entidade titular.....	36
6.1.3	Entrega da chave pública para emissor de certificado.....	37
6.1.4	Disponibilização de chave pública da AC SOLUTI para usuários.....	37
6.1.5	Tamanhos de chave.....	37
6.1.6	Geração de parâmetros de chaves assimétricas.....	37

6.1.7	Verificação da qualidade dos parâmetros.....	37
6.1.8	Geração de chave por hardware ou software.....	37
6.1.9	Propósitos de uso de chave (conforme campo "Key usage" na X.509 v3).....	37
6.2	Proteção da Chave Privada.....	37
6.2.1	Padrões para módulo criptográfico.....	38
6.2.2	Controle "n de m" para chave privada.....	38
6.2.3	Recuperação (escrow) de chave privada.....	38
6.2.4	Cópia de segurança (backup) de chave privada.....	38
6.2.5	Arquivamento de chave privada.....	38
6.2.6	Inserção de chave privada em módulo criptográfico.....	38
6.2.7	Método de ativação de chave privada.....	38
6.2.8	Método de desativação de chave privada.....	39
6.2.9	Método de destruição de chave privada.....	39
6.3	Outros Aspectos do Gerenciamento do Par de Chaves.....	39
6.3.1	Arquivamento de chave pública.....	39
6.3.2	Períodos de uso para as chaves pública e privada.....	39
6.4	Dados de ativação.....	39
6.4.1	Geração e instalação dos dados de ativação.....	39
6.4.2	Proteção dos dados de ativação.....	39
6.4.3	Outros aspectos dos dados de ativação.....	40
6.5	Controles de Segurança Computacional.....	40
6.5.1	Requisitos técnicos específicos de segurança computacional.....	40
6.5.2	Classificação da segurança computacional.....	40
6.5.3	Controle de segurança para as Autoridades de Registro.....	40
6.6	Controles Técnicos do Ciclo de Vida.....	41
6.6.1	Controles de desenvolvimento de sistemas.....	41
6.6.2	Controle de gerenciamento de segurança.....	41
6.6.3	Classificação de segurança de ciclo de vida.....	41
6.6.4	Controles na geração da LCR antes de publicadas.....	41
6.7	Controles de Segurança de Rede.....	41
6.7.1	Diretrizes Gerais.....	41
6.7.2	Firewall.....	42
6.7.3	Sistema de detecção de intrusão (IDS).....	42
6.7.4	Registro de acessos não autorizados à rede.....	42
6.8	Controles de Engenharia do Módulo Criptográfico.....	42
7	PERFIS DE CERTIFICADO E LCR.....	42
7.1	Diretrizes Gerais.....	42
7.2	Perfil do Certificado.....	43
7.2.1	Número(s) de versão.....	43
7.2.2	Extensões de certificados.....	43
7.2.3	Identificadores de algoritmos.....	43
7.2.4	Formatos de nome.....	43
7.2.5	Restrições de nome.....	43
7.2.6	OID (Object Identifier) de DPC.....	44
7.2.7	Uso da extensão "Policy Constraints".....	44
7.2.8	Sintaxe e semântica dos qualificadores de política.....	44
7.2.9	Semântica de processamento para extensões críticas.....	44
7.3	Perfil de LCR.....	44
7.3.1	Número (s) de versão.....	44
7.3.2	Extensões de LCR e de suas entradas.....	44
8	ADMINISTRAÇÃO DE ESPECIFICAÇÃO.....	45
8.1	Procedimentos de mudança de especificação.....	45
8.2	Políticas de publicação e de notificação.....	45
8.3	Procedimentos de aprovação.....	45
9	DOCUMENTOS REFERENCIADOS.....	45

Controle de Versão

Versão	Data	Descrição
1.0	01/11/2012	Versão inicial, a partir do DOC-ICP-05 versão 3.6.

Tabela de Siglas

SIGLA	DESCRIÇÃO
AC	Autoridade Certificadora
AC Raiz	Autoridade Certificadora Raiz da ICP-Brasil
ACT	Autoridade de Carimbo do Tempo
AGR	Agente de Registro
AR	Autoridade 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 Pessoa Jurídica
COBIT	Control Objectives for Information and related Technology
COSO	Comitee of Sponsoring Organizations
CPF	Cadastro de Pessoas Físicas
DMZ	Zona Desmilitarizada
DN	Distinguished Name
DPC	Declaração de Práticas de Certificação
ICP-BRASIL	Infraestrutura de Chaves Públicas Brasileira
IDS	Instrusion Detection System
IEC	International Eletrotechnical Commission
ISO	International Organization for Standardization
ITSEC	European Information Technology Security Evaluation Criteria
ITU	International Telecommunications Union
LCR	Lista de Certificados Revogados
NBR	Norma Brasileira
NIS	Número de Identificação Social

SIGLA	DESCRIÇÃO
NIST	National Institute of Standards and Technology
OCSP	On-line Certificate Status Protocol
OID	Object Identifier
OU	Organization Unit
PASEP	Programa de Formação do Patrimônio do Servidor Público
PC	Política de Certificado
PCN	Plano de Continuidade de Negócio
PIS	Programa de Integração Social
POP	Proof of Possession
PS	Política de Segurança
PSS	Prestadores de Serviço de Suporte
RIC	Registro de Identificação Civil
RFC	Request For Comments
RG	Registro Geral
SINRIC	Sistema Nacional de Registro de Identificação Civil
SNMP	Simple Network Management Protocol
TCSEC	Trusted System Evaluation Criteria
TSDM	Trusted Software Development Methodology
UF	Unidade da Federação
URL	Uniform Resource Locator

1 INTRODUÇÃO

1.1 Visão Geral

1.1.1

Esta DPC descreve as práticas e os procedimentos empregados pela Autoridade Certificadora da AC SOLUTI, AC integrante da Infra-Estrutura de Chaves Públicas Brasileira – ICP-Brasil, na execução dos seus serviços de certificação digital.

1.1.2

Esta DPC foi elaborada adotando a mesma estrutura empregada no documento DOC-ICP-05 do Comitê Gestor da ICP-Brasil.

1.2 Identificação

Esta DPC é chamada “Declaração de Práticas de Certificação da Autoridade Certificadora SOLUTI, integrante da ICP-Brasil”, e comumente referida como “DPC AC SOLUTI”. O Identificador de Objeto (OID) desta DPC, atribuído pela AC Raiz, é 2.16.76.1.1.46.

1.3 Comunidade e Aplicabilidade

1.3.1 Autoridades Certificadoras

Esta DPC refere-se unicamente à AC SOLUTI, integrante da ICP-Brasil.

1.3.2 Autoridades de Registro

1.3.2.1 Endereço da página web (URL)

O endereço da página web (URL) da AC SOLUTI é <https://ccd.acsoluti.com.br/>, onde estarão publicados os dados abaixo, referentes às Autoridades de Registro, responsáveis pelos processos de recebimento, validação e encaminhamento de solicitação de emissão ou de revogação de certificados digitais, e de identificação de seus solicitantes:

- a) relação de todas as AR credenciadas, com informações sobre as PC que implementam;
- b) para cada AR credenciada, os endereços de todas as instalações técnicas, autorizadas pela AC Raiz a funcionar;
- c) para cada AR credenciada, relação de eventuais postos provisórios autorizados pela AC Raiz a funcionar, com data de criação e encerramento de atividades;
- d) relação de AR que tenham se descredenciado da cadeia da AC, com respectiva data do descredenciamento;
- e) relação de instalações técnicas de AR credenciada que tenham deixado de operar, com respectiva data 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 Atualização

A AC SOLUTI mantém as informações acima atualizadas.

1.3.3 Prestador de Serviço de Suporte

1.3.3.1 Identificação

A relação de todos os Prestadores de Serviço de Suporte – PSS – vinculados diretamente à AC SOLUTI e/ou por intermédio de suas ARs é publicada em sua página web (<https://ccd.acsoluti.com.br/>).

1.3.3.2 Definição e classificação

PSS são entidades utilizadas pela AC e/ou suas ARs para desempenhar as atividades descritas nesta DPC ou nas PCs e são classificadas de acordo com o tipo de atividade prestada:

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

1.3.3.3

A AC SOLUTI mantém as informações acima atualizadas.

1.3.4 Titulares de Certificado

Somente pessoas jurídicas podem ser titulares de certificados emitidos pela AC SOLUTI.

1.3.5 Aplicabilidade

A AC SOLUTI emite certificados digitais para Autoridades Certificadoras de nível imediatamente subsequente ao seu (AC Subsequente), e essas ACs Subsequentes definirão em suas DPCs a aplicabilidade de seus certificados.

1.4 Dados de Contato

SOLUTI – Certificação Digital

Rua 260, número 288, Sala 6, Setor Leste Universitário

74.610-240 – Goiânia – Goiás

A/C: Vinicius Vieira de Sousa

Telefones: (62) 3941-6088 / 3999-6000 – Fax: (62) 3999-6097

E-mail: acsoluti@acsoluti.com.br

2 DISPOSIÇÕES GERAIS

2.1 Obrigações e Direitos

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

2.1.1 Obrigações da AC SOLUTI

São obrigações da AC SOLUTI:

- a) operar de acordo com DPC da AC SOLUTI;
- 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 do correspondente certificado;
- e) notificar os seus usuários quando ocorrer: suspeita de comprometimento de sua chave privada, emissão de novo par de chaves e correspondente certificado ou o encerramento de suas atividades;
- f) distribuir o seu próprio certificado;
- g) emitir, expedir e distribuir os certificados de ACs de nível imediatamente subsequente ao seu;
- h) informar a emissão do certificado ao respectivo solicitante;
- i) revogar os certificados por ela emitidos;
- j) emitir, gerenciar e publicar suas LCRs;
- k) publicar na página web (<https://ccd.acsoluti.com.br/>) esta DPC;
- l) publicar, na página web (<https://ccd.acsoluti.com.br/>), as informações definidas no item 2.6.1.2 deste documento;
- m) publicar, na 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 CG da ICP-Brasil;
- p) adotar as medidas de segurança e controle previstas na DPC 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 e com a legislação vigente;
- 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, de acordo com as normas do CG da ICP-Brasil;
- u) informar às terceiras partes e titulares de certificado acerca das garantias, coberturas, condicionantes e limitações estipuladas pela apólice de seguro de responsabilidade civil contratada nos termos acima;
- v) não emitir certificado com prazo de validade que se estenda além do prazo de validade de seu próprio certificado.

2.1.2 Obrigações das ARs

As obrigações das ARs vinculadas à AC SOLUTI 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 SOLUTI utilizando protocolo de comunicação seguro, conforme padrão definido no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS ARs DA ICP-BRASIL[1];
- d) informar aos respectivos titulares a emissão ou a revogação de seus certificados;
- e) disponibilizar os certificados emitidos pela AC 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 SOLUTI 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 elas 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 o 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 AR vinculadas credenciadas.

2.1.3 Obrigações do Titular do Certificado

As obrigações do titular de certificado emitido de acordo com esta DPC AC SOLUTI são as abaixo relacionadas:

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

2.1.4 Direitos da Terceira Parte (Relying Party)

2.1.4.1 Definição

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

2.1.4.2 Direitos

Constituem direitos da terceira parte:

- a) recusar a utilização do certificado para fins diversos dos previstos nesta DPC;
- 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 SOLUTI;
 - ii. não estiver expirado; e
 - iii. puder ser verificado com o uso de certificado válido da AC SOLUTI;

2.1.4.3 Não exercício dos direitos

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

2.1.5 Obrigações do Repositório

Estas são as obrigações do repositório:

- a) disponibilizar, logo após a sua emissão, os certificados emitidos pela AC e sua Lista de Certificados Revogados (LCR);
- b) estar disponível para consulta durante 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana; e
- c) implementar os recursos necessários para a garantia da segurança dos dados nele armazenados.

2.2 Responsabilidades

2.2.1 Responsabilidades da AC SOLUTI

2.2.1.1 Danos

A Autoridade Certificadora da AC SOLUTI responde pelos danos a que der causa.

2.2.1.2 Responsabilidade solidária

A AC SOLUTI responde solidariamente pelos atos das entidades de sua cadeia de certificação: AR e PSS (se houver a sua adoção).

2.2.1.3 Da Ausência de Responsabilidade pelo RIC

Quando da emissão de certificado que integra o Documento RIC, as entidades integrantes da ICP-Brasil, não possuirão qualquer espécie de responsabilidade por eventuais danos gerados na identificação presencial do cidadão, a cargo do Estado (CF / 88, art. 37 & 6).

2.2.2 Responsabilidades da AR

A AR será responsável pelos danos a que der causa.

2.3 Responsabilidade Financeira

2.3.1 Indenizações devidas pela terceira parte usuária (Relying Party)

Não existe responsabilidade da terceira parte (Relying Party – 2.1.4) perante a AC ou AR a ela vinculada, que requeira prática de indenização, exceto na hipótese de prática de ato ilícito pela terceira parte.

2.3.2 Relações Fiduciárias

A AC SOLUTI ou AR a ela vinculada indenizará integralmente os danos a que der causa. Em situações justificáveis, pode ocorrer limitação da indenização, quando o titular do certificado for pessoa jurídica.

2.3.3 Processos Administrativos

Os processos administrativos cabíveis, relativos às operações da AC SOLUTI e das ARs vinculadas à AC SOLUTI, seguirão a legislação específica na qual os procedimentos questionados se enquadrarem.

2.4 Interpretação e Execução

2.4.1 Legislação

A DPC AC SOLUTI obedece às leis da República Federativa do Brasil e atende aos requisitos da legislação em vigor, incluindo a Medida Provisória nº 2.200-2, de 24 de agosto de 2001, bem como as Resoluções do CG da ICP-Brasil. Além disto, é apoiada em uma estrutura contratual entre AC SOLUTI e Titulares de Certificados.

2.4.2 Forma de interpretação e notificação

2.4.2.1

Caso uma ou mais disposições desta DPC, por qualquer razão, sejam consideradas inválidas, ilegais, ou não aplicáveis, somente essas disposições serão afetadas. Todas as demais permanecem válidas dentro do escopo de abrangência deste documento. Nesse caso, o corpo técnico, da AC SOLUTI, examinará a disposição inválida e proporá à Comissão Técnica, no prazo máximo de 90 (noventa) dias, nova redação ou retirada da disposição afetada. As práticas descritas nesta DPC não prevalecerão sobre as normas, critérios, práticas e procedimentos determinados em instrução expressa da ICP-Brasil.

2.4.2.2

Todas solicitações, notificações ou quaisquer outras comunicações necessárias sujeitas às práticas descritas nessa DPC serão realizadas por iniciativa da AC SOLUTI por intermédio de seus responsáveis, e enviadas formalmente ao CG da ICP-Brasil via e-mail oficial das pessoas, dos órgãos e instituições envolvidos, ficando sob o crivo da AC SOLUTI a adoção de via postal, quando conveniente ou o meio se mostrar mais adequado.

2.4.3 Procedimentos de solução de disputa

2.4.3.1

Em caso de conflito entre a DPC e outras declarações, políticas, planos, acordos, contratos ou documentos que a AC SOLUTI adotar, prevalecerão as práticas e procedimentos determinados pela ICP-Brasil, devendo as normas conflitantes serem modificadas para a adequação necessária aos preceitos do ICP-Brasil.

2.4.3.2

No caso de um conflito entre esta DPC e as resoluções do Comitê Gestor da ICP-Brasil, prevalecerão sempre as normas, critérios, práticas e procedimentos estabelecidos pela ICP-Brasil. Nesta situação esta DPC será alterada para a solução da disputa.

2.4.3.3

Os casos omissos serão encaminhados para a apreciação da AC Raiz.

2.5 Tarifas de Serviço

Nos itens a seguir, são especificadas as políticas tarifárias e de reembolso aplicáveis.

2.5.1 Tarifas de emissão e renovação de certificados

As tarifas referentes aos serviços de emissão e renovação de certificados serão definidas internamente pela AC SOLUTI.

2.5.2 Tarifas de acesso ao certificado

Não há tarifa que incida sobre este serviço.

2.5.3 Tarifas de revogação ou de acesso à informação de status

As tarifas serão definidas internamente pela AC SOLUTI.

2.5.4 Tarifas para outros serviços

As tarifas serão definidas internamente pela AC SOLUTI.

2.5.5 Política de reembolso

Variável, definida internamente pela AC SOLUTI.

2.6 Publicação e Repositório

2.6.1 Publicação de informação da AC SOLUTI

2.6.1.1

A AC SOLUTI publica e mantém disponível em sua página web as informações descritas no item 2.6.1.2 no endereço <https://ccd.acsoluti.com.br/>. A disponibilidade da página é de no mínimo 99,5% (noventa e nove virgula cinco por cento) do mês, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.

2.6.1.2

As seguintes informações são publicadas na página web:

- a) seu próprio certificado;
- b) suas LCR;
- c) sua DPC;
- d) relação atualizada contendo as ARs vinculadas e seus respectivos endereços de instalação técnica em funcionamento;
- e) 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 PSSs vinculados.

2.6.2 Frequência de publicação

As informações mencionadas no item 2.6.1 serão publicadas sempre que sofrerem alterações.

As LCRs são publicadas conforme descrito no item 4.4.9 desta DPC.

2.6.3 Controles de acesso

Não há qualquer restrição ao acesso para consulta a esta DPC, às suas PCs, aos certificados emitidos e à LCR da AC SOLUTI.

Acessos para escrita nos locais de armazenamento (repositório) e publicação são permitidos apenas às pessoas responsáveis designadas especificamente para esse fim. Os controles de acesso incluem identificação pessoal para acesso aos equipamentos e utilização de senhas.

2.6.4 Repositórios

A AC SOLUTI adota como repositório de LCR os seguintes endereços:

- a) <http://ccd.acsoluti.com.br/lcr/ac-soluti-v1.crl>
- b) <http://ccd2.acsoluti.com.br/lcr/ac-soluti-v1.crl>
- c) <http://repositorio.icpbrasil.gov.br/lcr/ACSOLUTI/ac-soluti-v1.crl>

O repositório de LCR atende os seguintes requisitos:

- a) Disponibilidade – aquela definida no item 2.6.1;
- b) Protocolos de acesso – HTTP e HTTPS;
- c) Requisitos de segurança – obedece aos requisitos definidos no item 5.

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 da AC SOLUTI estão em conformidade com suas respectivas DPC, PC, PS e demais normas e procedimentos estabelecidos pela ICP-Brasil.

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, observando 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 CG da ICP-Brasil, a auditoria da AC SOLUTI é realizada pela AC Raiz, por meio de servidores de seu quadro próprio, ou por terceiros por ela autorizados, observando o disposto no documento CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL[3].

2.7.4

A AC SOLUTI informa que recebeu auditoria prévia da AC Raiz para fins de credenciamento na ICP-Brasil e que 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 SOLUTI informa que as entidades da ICP-Brasil a ela diretamente vinculadas, AR, também receberam auditoria prévia, para fins de credenciamento, e que a AC SOLUTI é 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 SOLUTI foi gerada e é mantida pela própria AC SOLUTI, que é responsável pelo seu sigilo. A divulgação ou utilização indevida de sua chave privada de assinatura é de sua inteira responsabilidade.

2.8.1.2

Não se aplica.

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 SOLUTI e a AR vinculada são consideradas sigilosas, exceto aquelas informações citadas no item 2.8.3.

2.8.2.2

Como princípio geral, nenhum documento, informação ou registro fornecido à AC SOLUTI ou AR vinculada deverá ser divulgado.

2.8.3 Tipos de informações não sigilosas

Os seguintes documentos da AC SOLUTI e AR vinculada são considerados documentos não sigilosos:

- a) os certificados e as LCR emitidos;
- b) informações corporativas que façam parte de certificados ou de diretórios públicos;
- c) esta DPC;
- d) versões públicas de Políticas de Segurança; e
- e) a conclusão dos relatórios de auditoria.

2.8.4 Divulgação de informação de revogação/suspensão de certificado

2.8.4.1

A AC SOLUTI divulga informações de revogação de certificados por ela emitidos, na sua página web descrita no item 2.6.1 desta DPC, através de sua lista de certificados revogados.

2.8.4.2

A razões para revogação do certificado sempre serão informadas para o seu titular.

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

Como princípio geral, nenhum documento, informação ou registro que pertençam ou estejam sob a guarda da AC SOLUTI e suas ARs vinculadas é divulgado a entidades legais ou seus funcionários, exceto quando:

- a) exista uma ordem judicial corretamente constituída; e
- b) estejam corretamente identificados o processo onde foi determinada e a autoridade judicial que determinou a quebra de sigilo.

2.8.6 Informações a terceiros

Como diretriz geral nenhum documento, informação ou registro, sob a guarda da AC SOLUTI ou AR vinculada, será fornecido a terceiros, exceto quando o requerente o solicite através 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

O titular de certificado e seu representante legal, constituído na forma da lei, terão amplo acesso a quaisquer dos seus próprios dados e identificações, e poderão autorizar a divulgação de seus registros a outras pessoas.

2.8.7.2

Qualquer liberação de informação pela AC SOLUTI ou AR vinculada, a terceiros somente será permitida mediante autorização formal do titular do certificado. As formas de autorização são as seguintes:

- a) por meio eletrônico, contendo assinatura válida garantida por certificado do titular, reconhecido pela AC SOLUTI; ou
- b) por meio de pedido escrito com firma reconhecida.

2.8.8 Outras circunstâncias de divulgação de informação

Nenhuma outra liberação de informação, que não as expressamente descritas nesta DPC, é permitida.

2.9 Direitos de Propriedade Intelectual

Todos os direitos de propriedade intelectual de certificados, políticas, especificações de práticas e procedimentos, nomes e chaves criptográficas, e todos os documentos gerados para a AC SOLUTI (eletrônicos ou não), de acordo com a legislação vigente, pertencem e continuarão sendo propriedade da Soluti – Soluções em Negócios Inteligentes.

3 IDENTIFICAÇÃO E AUTENTICAÇÃO

3.1 Registro Inicial

3.1.1 Disposições Gerais

3.1.1.1

Neste item e nos seguintes a DPC descreve os requisitos e os procedimentos gerais utilizados pela AR vinculada à AC SOLUTI, responsável 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 ou responsável pelo certificado ou como representante legal de uma pessoa jurídica é realmente aquela cujos dados constam na documentação apresentada;

NOTA 1: nos casos que envolver certificado para titular pessoa física, fica vedado qualquer espécie de procuração;

NOTA 2: nos casos em que envolver certificado para titular pessoa jurídica, admite-se

procuração apenas se o ato constitutivo prever expressamente a autorização para constituir procurador, devendo-se, para tanto, revestir-se da forma pública com poderes específicos para atuar perante a ICP- Brasil;

NOTA 3: nos casos de falecimento de um ou dos responsáveis legais por quaisquer empresas de um modo geral, desde que haja decisão judicial com nomeação de inventariante e termo de compromisso de inventariante assinado, e nomeação expressa deste como administrador, será admitida a pessoa nomeada na qualidade de responsável legal do Certificado Digital para todos os fins legais e administrativos.

- 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 de certificado com os constantes dos documentos apresentados e liberação da emissão do certificado no sistema da AC;
 - iv. as etapas descritas acima podem ser realizadas por um ou mais agentes de validação.
- b) VERIFICAÇÃO DA SOLICITAÇÃO DE CERTIFICADO - confirmação da validação realizada, observando que são executados, 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.

NOTA: Não será emitido qualquer certificado sem antes da verificação da solicitação de certificado.

3.1.1.2

O processo de validação poderá ser realizado pelo agente de registro fora do ambiente físico da AR, desde que utilizado ambiente computacional auditável e devidamente registrado no inventário de hardware e softwares da AR.

3.1.1.3

Todas as etapas dos processos de validação e verificação da solicitação de certificado são registradas e assinadas digitalmente pelos executantes, na solução de certificação disponibilizada pela AC SOLUTI, com a utilização de certificado digital ICP-Brasil do tipo A3. Tais registros são feitos de forma a permitir a reconstituição completa dos processos executados, para fins de auditoria.

3.1.1.4

São mantidos arquivos com as cópias de todos os documentos utilizados para confirmação da identidade de uma organização e/ou de um indivíduo. Tais cópias são mantidas em papel e/ou em forma digitalizada, observadas as condições definidas no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP-BRASIL[1].

3.1.1.5

Nos casos de certificado digital emitido para Servidores do Serviço Exterior Brasileiro, em missão permanente no exterior, assim caracterizados conforme a Lei nº 11.440, de 29 de dezembro de 2006, se houver impedimentos para a identificação conforme o disposto no subitem 3.1.1.1 deste anexo, é facultada a remessa da documentação pela mala diplomática e a realização da identificação por outros meios seguros, a serem definidos e aprovados pela AC-Raiz da ICP-Brasil.

3.1.1.6

A solicitação de certificado que integra o Documento RIC, realizada por Órgão de Identificação integrante do SINRIC, conforme Lei 12.058 de 13 de outubro de 2009 deverá:

- a) realizar a validação do registro inicial por meio de processo de individualização unívoca do cidadão com a consequente atribuição de número RIC, conforme as Leis nº 9.454 de 07 de abril de 1997, 12.058 de 13 de outubro de 2009 e Decreto nº 7.166 de 05 de maio de 2010, bem como demais resoluções do Comitê-Gestor do Registro de Identidade Civil – CG – RIC;

- b) realizar a verificação da solicitação de certificado mediante autenticação biométrica automatizada da pessoa que se apresenta como titular do certificado de pessoa física, feita na presença de funcionário do Órgão de Identificação, formalmente autorizado por autoridade competente para ser cadastrado no sistema da AC;
- c) obter os dados, enviados para que a AC emita o certificado digital, da memória do Cartão RIC, sem que haja possibilidade de alteração destes por parte do agente de AR, após autenticação biométrica utilizando os recursos do Cartão RIC (match-on-card).

3.1.2 Tipos de nomes

3.1.2.1

Os tipos de nomes admitidos para os titulares de certificados da AC SOLUTI são:

- a) Certificados de pessoa física, o campo "Common Name" (CN) é composto do nome do Titular do Certificado;
- b) Certificados de pessoa jurídica, o campo "Common Name" (CN) é composto do nome empresarial da pessoa jurídica;
- c) Certificados de equipamento, o campo "Common Name" (CN) é composto do "Domain Name System" (DNS) do site;
- d) Certificados para assinatura de código, o campo "Common Name" (CN) é composto do nome empresarial da pessoa jurídica mais a área responsável pelo certificado;
- e) Certificados de Aplicação, o campo "Common Name" (CN) é composto do nome da Aplicação.

3.1.2.2

Certificados emitidos para ACs subsequentes ao da AC SOLUTI não deverão incluir o nome da pessoa responsável.

3.1.3 Necessidade de nomes significativos

Para identificação dos titulares dos certificados emitidos, a AC SOLUTI faz uso de nomes significativos que possibilitam determinar a identidade da pessoa ou organização a que se referem.

3.1.4 Regras para interpretação de vários tipos de nomes

Os requisitos e procedimentos específicos, quando aplicáveis, estão detalhados nas PCs implementadas.

3.1.5 Unicidade de nomes

No campo "Distinguished Name" (DN) devem ser únicos e não ambíguos, para cada titular de certificado, no âmbito da AC emitente. Números ou letras adicionais poderão ser incluídos ao nome de cada entidade para assegurar a unicidade do campo.

3.1.6 Procedimento para resolver disputa de nomes

A AC SOLUTI reserva-se o direito de tomar todas as decisões referentes a disputas decorrentes da igualdade de nomes das AC de nível imediatamente subsequente ao seu. Durante o processo de confirmação de identidade, a AC solicitante deve provar o seu direito de uso de um nome específico (DN) em seu certificado.

3.1.7 Reconhecimento, autenticação e papel de marcas registradas

Os processos de tratamento, reconhecimento e confirmação de autenticidade de marcas registradas serão executados de acordo com a legislação em vigor.

3.1.8 Método para comprovar a posse de chave privada

A AC SOLUTI verifica se a entidade possui a chave privada correspondente à chave pública apresentada na solicitação de certificado digital. A AC SOLUTI segue padrão RFC 2510, aplicando como método de verificação o POP (Proof of Possession).

3.1.9 Autenticação da identidade de um indivíduo

A confirmação da identidade de um indivíduo é realizada pelas ARs vinculadas à AC SOLUTI mediante a presença física do interessado, com base em documentos legalmente aceitos.

3.1.9.1 Documentos para efeito 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) Caso os documentos acima tenham sido expedidos há mais de 5 (cinco) anos, ou não possuam fotografia, uma foto colorida recente ou documento de identidade com foto colorida, emitido há no máximo 5 (cinco) anos da data de validação presencial;
- e) Comprovante de residência ou domicílio, emitido há no máximo 3 (três) meses da data de validação presencial;
- f) mais um documento oficial com fotografia, no caso de certificados de tipos A4.

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: Para a identificação de indivíduo na emissão de certificado que integra o Documento RIC, deverá ser observado o disposto no item 3.1.1.6.

NOTA 5: Caso não haja suficiente clareza no documento apresentado, a AR deve solicitar outro documento, preferencialmente a CNH - Carteira Nacional de Habilitação ou o Passaporte Brasileiro.

NOTA 6: 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 7: 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.

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.

NOTA 1: É permitida a substituição dos documentos elencados acima por documento único, desde que este seja oficial e contenha as informações constantes daqueles.

NOTA 2: O cartão CPF poderá ser substituído por consulta à página da Receita Federal, devendo a cópia da mesma ser arquivada junto à documentação, para fins de auditoria.

3.1.10 Autenticação da Identidade de uma organização

3.1.10.1 Disposições Gerais

3.1.10.1.1

Os procedimentos empregados pelas ARs vinculadas para a confirmação da identidade de uma pessoa jurídica é feita mediante a presença física do responsável legal, com base em documentos de identificação legalmente aceitos.

3.1.10.1.2

Sendo titular do certificado pessoa jurídica, será designado 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

Será 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 do responsável pelo uso do certificado e assinatura do termo de responsabilidade de que trata o item 4.1.1; e
- d) presença física do(s) representante(s) legal(is) da pessoa jurídica 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;
 - iii. ato constitutivo, devidamente registrado no órgão competente; e
 - iv. documentos da eleição de seus administradores, quando aplicável;
- b) Relativos à 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.

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 um equipamento ou aplicação

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 ou aplicação

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 ou aplicação.

3.1.11.3.1

Não se aplica.

3.1.11.3.2

Não se aplica.

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

Antes da expiração do certificado o solicitante pode solicitar um novo certificado devendo ser observados os mesmos requisitos e procedimentos exigidos para a solicitação inicial do certificado, na forma e no prazo estabelecidos nesta DPC.

3.3 Geração de novo par de chaves após expiração ou revogação

3.3.1

O processo de identificação do solicitante quando da geração de novo par de chaves e emissão pela AC SOLUTI de novo certificado, após expiração ou revogação do anterior, será o mesmo da primeira emissão.

3.3.2

Após expiração ou revogação de certificado de AC Subsequente à AC SOLUTI, a AC Subsequente executa o processo padrão para geração de seu novo par de chaves.

3.4 Solicitação de Revogação

A solicitação de revogação de certificado de AC Subsequente é realizada através de solicitação formal assinada pelos representantes legais da entidade.

A confirmação da identidade do Titular do Certificado, e dos seus representantes legais, deve ser feita com base em um dos documentos de identidade descritos nos itens 3.1.9 e 3.1.10.

4 REQUISITOS OPERACIONAIS

4.1 Solicitação de Certificado

4.1.1

Os requisitos e procedimentos mínimos necessários para a solicitação de emissão de certificado pela AC SOLUTI são:

- 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 do tipo A3, inclusive quando da emissão de certificado que integra o RIC, de funcionário de Órgão de Identificação integrante do SINRIC, conforme Lei 12.058 de 3 de outubro de 2009; e
- c) assinatura do Termo de Titularidade e de Responsabilidade pelo titular ou responsável legal pelo uso do certificado; ou
- d) assinatura de Guia Informativo entregue ao titular do certificado, quando da emissão de certificado que integra o RIC, de funcionário de Órgão de Identificação integrante do SINRIC, conforme Lei 12.058 de 3 de outubro de 2009.

4.1.2

A solicitação de certificado para AC Subsequente à AC SOLUTI somente será possível após o processo de credenciamento e a autorização de funcionamento da AC em questão, conforme disposto no documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL[6].

4.1.3

Não se aplica.

4.1.4

A AC subsequente deverá encaminhar a solicitação de certificado à AC SOLUTI por meio de seus representantes legais, utilizando o padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[9].

4.2 Emissão de Certificado

4.2.1

Os certificados são emitidos pela AC SOLUTI após o completo e correto preenchimento da solicitação do certificado, e apresentação da documentação do solicitante. Após o processo de validação das informações fornecidas, o certificado será emitido e o titular notificado, por e-mail.

4.2.2

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

4.3 Aceitação de Certificado

4.3.1

O recebimento de um certificado pelo Titular de Certificado e o uso subsequente das chaves, constitui aceitação do certificado por parte do Titular. Aceitando um certificado, o Titular deste:

- a) manifesta expressamente estar de acordo com as responsabilidades contínuas, obrigações e deveres impostas a ele pelo Termo de Responsabilidade e esta DPC da AC SOLUTI;
- b) toma conhecimento e atesta que, para sua segurança, nenhuma pessoa deve ter acesso à chave privada e senhas associadas com o certificado;
- c) afirma que as informações fornecidas durante o processo de solicitação são verdadeiras e foram publicadas dentro do certificado com precisão.

4.3.2

A aceitação do certificado é feita pela pessoa física responsável pela entidade.

4.3.3

Não há termos de acordo ou instrumentos similares requeridos pela AC SOLUTI.

4.4 Suspensão e Revogação de Certificado

4.4.1 Circunstâncias para revogação

4.4.1.1

A AC SOLUTI pode revogar um certificado por ela emitido pelos seguintes motivos:

- a) solicitação de revogação corretamente preenchido pelo Titular do Certificado;
- b) solicitação de revogação é feita por uma pessoa com procuração do Titular do Certificado;
- c) solicitação de revogação enviada à AC SOLUTI por um terceiro autorizado:
 - i. determinação judicial, sob qualquer fundamento;
 - ii. familiares do Titular do Certificado, face ao seu falecimento;
 - iii. responsável legal da empresa, quando o Titular do Certificado organizacional deixa o emprego;

4.4.1.2

Um certificado é revogado obrigatoriamente pelos seguintes motivos:

- 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 dissolução da AC SOLUTI; ou
- d) no caso de comprometimento da chave privada correspondente ou da sua mídia armazenadora.

4.4.1.3

Em relação à revogação, deve ainda ser observado que:

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

Brasil.

4.4.2 Quem pode solicitar revogação

A solicitação para a revogação de um certificado somente poderá ser feita

- a) por solicitação do titular do certificado;
- b) por solicitação do responsável pelo certificado;
- c) pela AC SOLUTI;
- d) por uma AR vinculada; ou
- e) por determinação do CG da ICP-Brasil ou da AC Raiz.

4.4.3 Procedimento para solicitação de revogação

4.4.3.1

O procedimento para a solicitação de uma revogação varia dependendo de quem a origina:

4.4.3.1.1

A solicitação de revogação de certificado deve ser realizada através do envio de formulário específico disponível na página web da AC SOLUTI. O formulário deverá ser encaminhado devidamente preenchido e assinado.

4.4.3.1.2

Esse procedimento garante aos agentes habilitados, conforme o item 4.4.2, acessibilidade e facilidade para solicitar a qualquer tempo revogação de seus respectivos certificados.

4.4.3.2

Fica estabelecido como diretrizes gerais que:

- a) o solicitante da revogação de um certificado deve ser identificado;
- b) as solicitações de revogação, bem como as ações delas decorrentes deverão ser registradas e armazenadas;
- c) as justificativas para a revogação de um certificado são documentadas; e
- d) o processo de revogação de um certificado terminará com a geração e a publicação de uma LCR que contenha o certificado revogado.

4.4.3.3

Não se aplica.

4.4.3.4

O prazo máximo admitido para a conclusão do processo de revogação de certificado de AC, após o recebimento da respectiva solicitação, é de 12 (doze) horas.

4.4.3.5

A AC SOLUTI 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. A AC SOLUTI estabelece o prazo de 2 (dois) dias para a aceitação do certificado solicitado por seu titular, dentro dos quais a revogação do certificado poderá ser solicitada sem cobrança de tarifa pela AC SOLUTI.

4.4.4.2

Não se aplica.

4.4.5 Circunstâncias para suspensão

A suspensão de certificados não é admitida no âmbito da ICP-Brasil, não sendo, portanto, admitida no âmbito da AC SOLUTI.

4.4.6 Quem pode solicitar suspensão

A suspensão de certificados não é admitida no âmbito da ICP-Brasil, não sendo, portanto, admitida no âmbito da AC SOLUTI.

4.4.7 Procedimento para solicitação de suspensão

A suspensão de certificados não é admitida no âmbito da ICP-Brasil, não sendo, portanto, admitida no âmbito da AC SOLUTI.

4.4.8 Limites no período de suspensão

A suspensão de certificados não é admitida no âmbito da ICP-Brasil, não sendo, portanto, admitida no âmbito da AC SOLUTI.

4.4.9 Frequência de emissão de LCR

4.4.9.1

A AC SOLUTI emite uma nova LCR referentes a certificados de ACs Subsequentes a cada 30 (trinta) dias.

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 é de 45 (quarenta e cinco) dias. Em caso de revogação de certificado de AC Subsequente, a AC SOLUTI deverá emitir nova LCR no prazo previsto no item 4.4.3 e notificar todas as ACs 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 também ser confirmada por meio da verificação da assinatura da AC SOLUTI e do período de validade da LCR.

4.4.11 Disponibilidade para revogação/verificação de status on-line

A AC SOLUTI não suporta o processo de verificação da situação de estado de certificados de forma on-line (OCSP). O processo de revogação on-line está disponível ao Titular do Certificado, conforme descrito no item 3.4.

4.4.12 Requisitos para verificação de revogação on-line

A AC SOLUTI não disponibiliza diretório on-line ou um servidor de OCSP para verificar o estado dos certificados emitidos pela AC SOLUTI.

4.4.13 Outras formas disponíveis para divulgação de revogação

A AC SOLUTI não suporta outras formas para divulgação da revogação que não através da publicação de LCR.

4.4.14 Requisitos para verificação de outras formas de divulgação de revogação

Como definido no item 4.4.11, a AC SOLUTI não suporta o processo de verificação da situação de estado de certificados de forma on-line (OCSP).

4.4.15 Requisitos especiais para o caso de comprometimento de chave

4.4.15.1

Quando houver comprometimento ou suspeita de comprometimento da chave privada, o Titular do Certificado deverá comunicar imediatamente a AC SOLUTI.

4.4.15.2

A comunicação a AC SOLUTI deverá ser através de formulário específico disponibilizado na página da AC SOLUTI.

4.5 Procedimentos de Auditoria de Segurança

4.5.1 Tipos de Evento Registrados

4.5.1.1

Todas as ações executadas pelo pessoal da AC SOLUTI, no desempenho de suas atribuições, são registradas de modo que cada ação esteja associada à pessoa que a realizou. A AC SOLUTI registra em arquivos para fins de auditoria todos os eventos relacionados à segurança do seu sistema de certificação, quais sejam:

- a) iniciação e desligamento do sistema de certificação;
- b) tentativas de criar, remover, definir senhas ou mudar privilégios de sistema dos operadores da AC SOLUTI;
- c) mudanças na configuração da AC SOLUTI 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 SOLUTI ou de chaves de Titulares de Certificados;
- 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

A AC SOLUTI registra, eletrônica ou manualmente, informações de segurança não geradas diretamente pelo seu sistema de certificação, quais sejam:

- 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

As informações registradas pela AC SOLUTI são todas as descritas nos itens acima.

4.5.1.4

Todos 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 SOLUTI é armazenada, eletrônica ou manualmente, em local único, conforme a POLÍTICA DE SEGURANÇA DA ICP-

BRASIL[8].

4.5.1.6

A AR vinculada à AC SOLUTI, responsável pela DPC, registrará eletronicamente em arquivos de auditoria todos os eventos relacionados à validação e aprovação da solicitação, bem como, à revogação de certificados. Os seguintes eventos deverão obrigatoriamente estar 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 SOLUTI define que o local de arquivamento das cópias dos documentos para identificação, apresentadas no momento da solicitação e revogação de certificados e dos termos de titularidade e responsabilidade, é o mesmo das instalações técnicas da AC SOLUTI.

4.5.2 Frequência de auditoria de registros (logs)

Os registros de auditoria da AC SOLUTI serão analisados semanalmente pelo pessoal operacional da AC SOLUTI.

Todos os eventos significativos serão explicados em relatório de auditoria de registros. Tal análise envolverá uma inspeção breve de todos os registros verificando-se que não foram alterados, em seguida proceder-se-á a uma investigação mais detalhada de quaisquer alertas ou irregularidades nesses registros. Todas as ações tomadas em decorrência dessa análise serão documentadas.

4.5.3 Período de Retenção para registros (logs) de Auditoria

A AC SOLUTI manterá nas instalações da AC SOLUTI os seus registros de auditoria pelo prazo de 2 (dois) meses e, subsequentemente, fará o armazenamento da maneira descrita no item 4.6.

4.5.4 Proteção de registro (log) de Auditoria

4.5.4.1

Os registros de auditoria gerados eletronicamente são obrigatoriamente protegidos contra leitura não autorizada, modificação e remoção. Estes registros são classificados e mantidos conforme sua classificação, segundo os requisitos da POLÍTICA DE SEGURANÇA DA ICP-BRASIL[8].

4.5.4.2

As informações de auditoria geradas manualmente são obrigatoriamente protegidas contra leitura não autorizada, modificação e remoção. Estes registros são classificados e mantidos conforme sua classificação, segundo os requisitos da POLÍTICA DE SEGURANÇA DA ICP-BRASIL[8].

4.5.4.3

Os mecanismos de proteção descritos neste item obedecem a POLÍTICA DE SEGURANÇA DA ICP-BRASIL[8].

4.5.5 Procedimentos para cópia de segurança (backup) de registro (log) de auditoria

A AC SOLUTI executa procedimentos de backup, de todo o sistema de certificação (SISTEMA OPERACIONAL + APLICAÇÃO DE AC + BANCO DE DADOS) de duas formas:

- a) diariamente: cópia de segurança; e
- b) semanalmente: cópia armazenada para processos de auditoria.

4.5.6 Sistema de coleta de dados de auditoria

O sistema de coleta de dados de auditoria da AC SOLUTI é uma combinação de processos automatizados e manuais, executada por seus sistemas ou por seu pessoal operacional.

4.5.7 Notificação de agentes causadores de eventos

Eventos registrados pelo conjunto de sistemas de auditoria da AC SOLUTI não serão notificados à pessoa, organização, dispositivo ou aplicação que causou o evento.

4.5.8 Avaliações de vulnerabilidade

Eventos que indiquem possível vulnerabilidade, detectados na análise periódica dos registros de auditoria da AC SOLUTI, serão analisados detalhadamente e, dependendo de sua gravidade, registrados em separado. Ações corretivas decorrentes são implementadas e registradas para fins de auditoria.

4.6 Arquivamento de Registros

Essa DPC descreve nestes tópicos a Política Geral de Arquivamento de Registros, para uso futuro, implementada pela AC SOLUTI e pelas suas ARs vinculadas.

4.6.1 Tipos de registros arquivados

A AC SOLUTI registrada e arquivada informações a respeito de :

- 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 SOLUTI;
- g) informações de auditoria previstas no item 4.5.1.

4.6.2 Período de retenção para arquivo

Os períodos de retenção para cada registro arquivado são (de):

- a) PERMANENTEMENTE: as LCR referentes a certificados de assinatura digital, para fins de consulta histórica;
- b) DEZ ANOS: para as cópias dos documentos para identificação apresentadas no momento da solicitação e da revogação de certificados, e os termos de titularidade e responsabilidade, a contar da data da expiração ou revogação do certificado;
- c) SEIS ANOS: as demais informações, inclusive arquivos de auditoria.

4.6.3 Proteção de arquivos

Todos os registros arquivados são classificados e armazenados com requisitos de segurança compatíveis com sua classificação, conforme a POLÍTICA DE SEGURANÇA DA ICP-BRASIL[8].

4.6.4 Procedimentos para cópia de segurança (backup) de arquivos

4.6.4.1

Uma segunda cópia de todo o material arquivado é armazenada em ambiente externo ao sistema de certificação da AC SOLUTI, e recebem 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

É feita a verificação da integridade dessas cópias de segurança, periodicamente a cada 6 (seis) meses.

4.6.5 Requisitos para datação de registros

Os servidores da AC SOLUTI são sincronizados com a hora GMT fornecida pelo Observatório Nacional. 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, estes contêm a Hora Oficial do Brasil.

4.6.6 Sistema de coleta de dados de arquivo

O sistema de coleta de dados de arquivos da AC SOLUTI é uma combinação de processos automatizados e manuais executados pelo sistema operacional, pelos sistemas de certificação de AC e pelo pessoal operacional.

4.6.7 Procedimentos para obter e verificar informação de arquivo

A verificação de informação de arquivo deve ser solicitada formalmente à AC SOLUTI, ou a uma AR a ela vinculada, identificando de forma precisa o tipo e o período da informação a ser verificada. O solicitante da verificação de informação é devidamente identificado.

4.7 Troca de chave

4.7.1

A AC SOLUTI comunica a AC Subsequente, por E-mail, da necessidade de renovação do certificado, com antecedência de 13 (treze) meses.

4.7.2

Não se aplica.

4.8 Comprometimento e Recuperação de Desastre

Os requisitos relacionados aos procedimentos de notificação e de recuperação de desastres estão descritos no PCN da AC SOLUTI, conforme estabelecido na POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8], para garantir a continuidade dos seus serviços críticos.

4.8.1 Recursos computacionais, software e dados corrompidos

A AC SOLUTI possui um Plano de Continuidade de Negócio que especifica as ações a serem tomadas no caso em que recursos computacionais, software e/ou dados são corrompidos, e que podem ser resumidas no seguinte:

- a) é feita a identificação de todos os elementos corrompidos;
- b) o instante do comprometimento é determinado e é crítico para invalidar as transações executadas após aquele instante;
- c) é feita uma análise do nível do comprometimento para a determinação das ações a serem executadas, que podem variar de uma simples restauração de um backup de segurança até a revogação do certificado da AC SOLUTI.

4.8.2 Certificado de entidade é revogado

A AC SOLUTI possui um Plano de Continuidade de Negócio que especifica as ações a serem tomadas no caso em que o certificado da AC SOLUTI é revogado, e que podem ser resumidas da seguinte forma:

- a) A AC Raiz e os Titulares de Certificados serão notificadas por comunicação segura;
- b) A AC SOLUTI revoga os certificados por ela emitidos;
- c) A AC SOLUTI solicita um novo certificado à AC Raiz;
- d) Iniciam-se os procedimentos para emissão dos novos certificados de usuários.

4.8.3 Chave de entidade é comprometida

A AC SOLUTI possui um Plano de Continuidade de Negócio que especifica as ações a serem tomadas no caso de comprometimento de sua chave privada após a identificação da crise são notificados os gestores do processo de certificação digital que acionam as equipes envolvidas, para ativar o site de contingência.

4.8.4 Segurança dos recursos após desastre natural ou de outra natureza

A AC SOLUTI possui um Plano de Continuidade de Negócio que especifica as ações a serem tomadas no caso de desastre natural ou de outra natureza.

O propósito deste plano é restabelecer as principais operações da AC SOLUTI quando a operação de sistemas é significativamente e adversamente abalada por fogo, greves, etc. O plano garante que qualquer impacto em operações de sistema não causará um impacto operacional direto e imediato dentro da ICP-Brasil da qual a AC SOLUTI faz parte.

Isto significa que o plano tem como meta primária, restabelecer a AC SOLUTI para tornar acessível os registros lógicos mantidos dentro do software. Serão tomadas as ações de recuperação aprovadas dentro do plano, segundo uma ordem de prioridade.

4.8.5 Atividades das Autoridades de Registro

Os procedimentos no PCN das ARs vinculadas para recuperação, total ou parcial das atividades das ARs, estão abaixo descrito:

- 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 será 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 da AC, AR ou PSS

4.9.1

Caso seja necessária a extinção dos serviços de AC, AR ou PSS, a AC SOLUTI executará os procedimentos aplicáveis descritos no documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL[6].

4.9.2

Os procedimentos para notificação dos usuários e para a transferência da guarda de seus dados e registros de arquivos incluem:

- a) notificação para o e-mail do titular do certificado;
- b) transferência progressiva do serviço e dos registros operacionais para um sucessor que tenha os mesmos requisitos de segurança da entidade extinta;
- c) preservação de quaisquer registros não transferidos a um sucessor;
- d) as chaves públicas dos certificados emitidos pela AC dissolvida serão armazenadas por outra AC após aprovação da AC Raiz;
- e) quando houver mais de uma AC interessada, assumirá a responsabilidade do armazenamento das chaves públicas, aquela indicada pela AC SOLUTI;
- f) a AC SOLUTI, ao encerrar as suas atividades transferirá, se for o caso, a documentação dos certificados digitais emitidos à AC que tenha assumido a guarda das respectivas chaves públicas;
- g) caso as chaves públicas não tenham sido assumidas por outra AC, os documentos referentes aos certificados digitais e as respectivas chaves públicas serão repassados à AC Raiz.

5 CONTROLES DE SEGURANÇA FÍSICA, PROCEDIMENTAL E DE PESSOAL

Nos itens seguintes estão descritos os controles de segurança implementados pela AC SOLUTI, responsável pela DPC e pelas ARs a ela vinculadas, para executar de modo seguro suas funções de geração de chaves, identificação, certificação, auditoria e arquivamento de registros.

5.1 Controle Físico

5.1.1 Construção e localização das instalações de AC

5.1.1.1

A localização e o sistema de certificação utilizado para a operação da AC SOLUTI não são publicamente identificados, nem há identificação pública externa das instalações. Internamente, não são admitidos ambientes compartilhados que permitam visibilidade nas operações de emissão e revogação de certificados. Essas operações são segregadas em compartimentos fechados e fisicamente protegidos.

5.1.1.2

Todos os aspectos de construção das instalações da AC SOLUTI, relevantes para os controles de segurança física, foram executadas por técnicos especializados e compreendem, entre outros, os descritos abaixo:

- a) instalações para equipamentos de apoio: máquinas de ar condicionado, grupos geradores, no-

breaks, baterias, quadros de distribuição de energia e de telefonia, retificadores e estabilizadores e similares;

- b) instalações para sistemas de telecomunicações;
- c) sistema de aterramento e de proteção contra descargas atmosféricas; e
- d) iluminação de emergência.

5.1.2 Acesso físico nas instalações de AC SOLUTI

O acesso físico às dependências da AC SOLUTI é gerenciado e controlado internamente conforme o previsto na POLÍTICA DE SEGURANÇA DA ICP-BRASIL[8].

5.1.2.1 Níveis de Acesso

5.1.2.1.1

São implementados 4 (quatro) níveis de acesso físico aos diversos ambientes onde estão instalados os equipamentos utilizados na operação da AC SOLUTI, e mais 2 (dois) níveis relativos à proteção da chave privada de AC.

5.1.2.1.2 Nível 1

O primeiro nível – ou nível 1 – situa-se após a primeira barreira de acesso às instalações da AC SOLUTI. Para entrar em uma área de nível 1, cada indivíduo é identificado e registrado por segurança armada. A partir desse nível, pessoas estranhas à operação da AC SOLUTI transitam apenas devidamente identificadas e acompanhadas. Nenhum tipo de processo operacional ou administrativo da AC SOLUTI é executado nesse nível.

5.1.2.1.3

Excetuados os casos previstos em lei, o porte de armas não é admitido nas instalações do ambiente onde estão instalados os equipamentos utilizados na operação da AC SOLUTI, em níveis superiores ao nível 1. A partir desse nível, equipamentos de gravação, fotografia, vídeo, som ou similares, bem como computadores portáteis, tem sua entrada controlada e somente podem ser utilizados mediante autorização formal e supervisão.

5.1.2.1.4 Nível 2

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

5.1.2.1.5 Nível 3

O terceiro nível – ou nível 3 – é interno ao segundo nível e é o primeiro nível a abrigar material e atividades sensíveis da operação da AC SOLUTI. Qualquer atividade relativa ao ciclo de vida dos certificados digitais está localizada a partir desse nível. Pessoas que não estejam envolvidas com essas atividades não têm permissão para acesso a esse nível. Pessoas que não possuem permissão de acesso não podem permanecer nesse nível se não estiverem devidamente autorizadas, identificadas e acompanhadas por pelo menos um funcionário que tenha esta permissão.

5.1.2.1.6

No terceiro nível 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: a identificação individual, com cartão eletrônico e a identificação biométrica.

5.1.2.1.7

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

5.1.2.1.8 Nível 4

O quarto nível - ou nível 4 – é interno ao terceiro nível, é aquele no qual ocorrem atividades especialmente sensíveis de operação da AC SOLUTI, 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 dessas pessoas é exigida enquanto o ambiente estiver ocupado.

5.1.2.1.9

No quarto nível todas as paredes, o piso e o teto são revestidos de aço e concreto. As paredes, piso e o teto são inteiriços, constituindo uma célula estanque contra ameaças de acesso indevido, água, vapor, gases e fogo. 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 – que constituem a chamada sala cofre - possuem proteção contra interferência eletromagnética externa.

5.1.2.1.10

A sala cofre é construída segundo as normas brasileiras aplicáveis. Eventuais omissões dessas normas devem ser sanadas por normas internacionais pertinentes.

5.1.2.1.11

A AC SOLUTI possui um único ambiente de nível 4.

5.1.2.1.12 Nível 5

O quinto nível – ou nível 5 – é interno aos ambientes de nível 4, e compreende cofres e gabinetes reforçados trancados. Materiais criptográficos tais como chaves, dados de ativação, suas cópias e equipamentos criptográficos são 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; e
- b) possui tranca com chave.

5.1.2.1.14 Nível 6

O sexto nível – ou nível 6 – consiste de pequenos depósitos localizados no interior do cofre ou gabinete de quinto nível. Cada um desses depósitos dispõe de fechadura individual. Os dados de ativação da AC SOLUTI estão armazenados em um desses depósitos.

5.1.2.2 Sistema físico 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 câmaras de vídeo ligadas a um sistema de gravação 24x7. O posicionamento e a capacidade dessas câmaras não permitem a recuperação de senhas digitadas nos controles de acesso.

5.1.2.2.2

As fitas de vídeo resultantes da gravação 24x7 são armazenadas por 1 (um) ano. Elas são testadas (verificação de trechos aleatórios no início, meio e final da fita) pelo menos a cada 3 (três) meses, com a escolha de, no mínimo, uma fita referente a cada semana. Essas fitas 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. A partir do nível 2 não há vidros separando os níveis de acesso.

5.1.2.2.4

Em todos os ambientes de quarto nível, um alarme de detecção de movimentos permanece ativo enquanto não for satisfeito o critério de acesso ao ambiente. Assim que, devido à saída de um ou mais funcionários de confiança, o critério mínimo de ocupação deixar 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 câmaras de vídeo cujo posicionamento permite o acompanhamento das ações do guarda.

5.1.2.3 Sistema de Controle de Acesso

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

5.1.2.4 Mecanismos de emergência

5.1.2.4.1

Mecanismos específicos foram implantados para garantir a segurança do pessoal e dos equipamentos da AC SOLUTI 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 estão 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 da AC

5.1.3.1

A infra-estrutura do ambiente de certificação da AC SOLUTI é 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 SOLUTI e seus respectivos serviços. Há sistema de aterramento implantado.

5.1.3.2

Todos os cabos elétricos são protegidos por tubulações e dutos apropriados.

5.1.3.3

São utilizadas tubulações, dutos, calhas, quadros e caixas de passagem, de distribuição e de terminação, projetados e construídos de forma a facilitar vistorias e a detecção de tentativas de violação. São utilizados dutos para os cabos de energia separados dos dutos para cabos de telefonia e de dados.

5.1.3.4

Todos os cabos são catalogados, identificados e periodicamente vistoriados, 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 aos 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 é independente 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 dos ambientes de nível 4 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 SOLUTI é garantida por meio de:

- a) geradores de porte compatível;
- b) geradores de reserva;
- c) sistemas de no-breaks redundantes;
- d) sistemas redundantes de ar condicionado.

5.1.4 Exposição à água nas instalações da AC

A estrutura inteira do ambiente de nível 4, construído na forma de célula estanque, prevê proteção física contra exposição à água, infiltrações e inundações, provenientes de qualquer fonte externa.

5.1.5 Prevenção e proteção contra incêndio nas instalações da AC

5.1.5.1

Os sistemas de prevenção contra incêndios das áreas de nível 4 possibilitam alarmes preventivos antes de fumaça visível, disparando alarmes com a presença de partículas que caracterizam o superaquecimento de materiais elétricos e outros materiais combustíveis presentes nas instalações.

5.1.5.2

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

5.1.5.3

A sala cofre possui sistema para detecção precoce de fumaça e sistema de extinção de incêndio por gás. As portas de acesso à sala cofre são eclusas, uma porta só se abre quando a anterior está fechada.

5.1.5.4

Em caso de incêndio nas instalações da AC SOLUTI, a temperatura interna da sala cofre não excede 50 graus Celsius, e a sala suporta esta condição por, no mínimo, uma hora.

5.1.6 Armazenamento de mídia nas instalações da AC SOLUTI

A AC SOLUTI atende a norma brasileira NBR 11.515/NB 1334 ("Critérios de Segurança Física Relativos ao Armazenamento de Dados").

5.1.7 Destruição de lixo nas instalações da AC SOLUTI

5.1.7.1

Todos os documentos em papel que contenham 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 SOLUTI

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 de AR atendem aos requisitos estabelecidos no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS ARs DA ICP-BRASIL[1].

5.2 Controles Procedimentais

Nos itens seguintes estão descritos os requisitos para a caracterização e o reconhecimento de perfis qualificados na AC SOLUTI, juntamente com as responsabilidades definidas para cada perfil. Para cada tarefa associada aos perfis definidos, é estabelecido o número de pessoas requerido para sua execução.

5.2.1 Perfis qualificados

5.2.1.1

A separação das tarefas para funções críticas é uma prática adotada, com o intuito de evitar que um funcionário utilize indevidamente o sistema de certificação sem ser detectado. As ações de cada

empregado estão limitadas de acordo com o seu perfil.

5.2.1.2

A AC SOLUTI estabelece um mínimo de 3 (três) 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.

5.2.1.3

Todos os operadores do sistema de certificação da AC SOLUTI 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 desliga da AC SOLUTI, suas permissões de acesso são revogadas imediatamente. Quando há mudança na posição ou função que o empregado ocupa dentro da AC, são revistas suas permissões de acesso. Existe uma lista de revogação, com todos os recursos, antes disponibilizados, que o empregado deverá devolver à AC no ato de seu desligamento.

5.2.2 Número de pessoas necessário por tarefa

5.2.2.1

Controle multiusuário é requerido para a geração e a utilização da chave privada da AC SOLUTI, conforme o descrito em 6.2.2.

5.2.2.2

Todas as tarefas executadas no ambiente onde está localizado o equipamento de certificação da AC SOLUTI necessitam da presença de no mínimo 2 (dois) operadores (funcionários) da AC SOLUTI. As demais tarefas da AC SOLUTI podem ser executadas por um único operador.

5.2.3 Identificação e autenticação para cada perfil

5.2.3.1

Pessoas que ocupam os perfis designados pela AC SOLUTI passam por um processo rigoroso de seleção. Todo funcionário da AC SOLUTI tem sua identidade e perfil verificados antes de:

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

5.2.3.2

Os certificados, contas e senhas utilizados para identificação e autenticação dos são:

- a) diretamente atribuídos a um único operador, funcionário da AC SOLUTI devidamente qualificado;
- b) não compartilhados;
- c) restritos às ações associadas ao perfil para o qual foram criados.

5.2.3.3

A AC SOLUTI implementa um padrão de utilização de "senhas fortes", definido em seu Manual de Segurança 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 SOLUTI e das AR e PSS vinculados, encarregados de tarefas operacionais, têm registrado em contrato ou termo de responsabilidade:

- a) Os termos e as condições do perfil que ocupam;
- b) O compromisso de observar as normas, políticas e regras aplicáveis da AC SOLUTI;
- c) O compromisso de observar as normas, políticas e regras aplicáveis da ICP-Brasil;

- d) 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 SOLUTI e AR vinculada 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 AC SOLUTI e na POLÍTICA DE SEGURANÇA DA ICP-BRASIL[8].

5.3.2 Procedimentos de Verificação de Antecedentes

5.3.2.1

Com o propósito de resguardar a segurança e a credibilidade da AC SOLUTI, todo o pessoal envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados, é submetido aos seguintes processos, antes do começo das atividades de:

- Verificação de antecedentes criminais;
- Verificação de situação de crédito;
- Verificação de histórico de empregos anteriores;
- Comprovação de escolaridade e de residência.

5.3.2.2

A AC SOLUTI poderá definir requisitos adicionais para a verificação de antecedentes.

5.3.3 Requisitos de treinamento

Todo o pessoal da AC SOLUTI 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:

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

5.3.4 Frequência e requisitos para reciclagem técnica

Todo o pessoal da AC SOLUTI 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 no sistema de certificação da AC SOLUTI. Treinamentos de reciclagem são realizados pela AC SOLUTI sempre que necessário.

5.3.5 Frequência e sequência de rodízios de cargos

A AC SOLUTI não implementa rodízio de cargos.

5.3.6 Sanções para ações não autorizadas

5.3.6.1

A AC SOLUTI, na eventualidade de uma ação não autorizada, real ou suspeita, ser realizada por pessoa encarregada de processo operacional da AC SOLUTI ou de uma AR vinculada, suspenderá, de imediato, o acesso dessa pessoa ao seu sistema de certificação, instaurará processo administrativo para apurar os fatos e, se for o caso, adotar as medidas legais cabíveis.

5.3.6.2

O processo administrativo referido acima conterà, no mínimo, os seguintes itens:

- relato da ocorrência com "modus operandis";
- identificação dos envolvidos;
- eventuais prejuízos causados;

- d) punições aplicadas, se for o caso;
- e) conclusões.

5.3.6.3

Concluído o processo administrativo, a AC SOLUTI encaminhará 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

O pessoal da AC SOLUTI e das ARs vinculadas, no exercício de 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].

5.3.8 Documentação fornecida ao pessoal

5.3.8.1

A AC SOLUTI disponibiliza para todo o seu pessoal e para as ARs vinculadas:

- a) Esta DPC;
- b) POLÍTICA DE SEGURANÇA DA ICP-BRASIL[8];
- c) A Política de Segurança da AC SOLUTI;
- d) Documentação operacional relativa às suas atividades;
- e) Contratos, normas e políticas relevantes para suas atividades.

5.3.8.2

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

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 da AC SOLUTI é gerado pela própria AC SOLUTI, em módulo criptográfico que implementa as características de segurança definidas no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[9], após o deferimento do pedido de credenciamento da mesma e a consequente autorização de funcionamento no âmbito da ICP-Brasil.

6.1.1.2

Pares de chaves são gerados somente pelo Titular do Certificado correspondente.

6.1.1.3

As PCs implementadas pela AC SOLUTI definem o meio utilizado para armazenamento das respectivas chaves privadas, com base nos requisitos aplicáveis estabelecidos pelo documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL[7].

6.1.2 Entrega da chave privada à entidade titular.

Não se aplica. É responsabilidade exclusiva do titular do certificado a geração e a guarda da sua chave privada.

6.1.3 Entrega da chave pública para emissor de certificado

6.1.3.1

A AC SOLUTI entregará à AC SOLUTI cópia de sua chave pública, em formato PKCS#10..

6.1.3.2

O representante legal da AC Subsequente entregará a chave pública da AC, em cerimônia específica, em data e hora previamente estabelecidas pela AC SOLUTI. Os detalhes da cerimônia serão registrados para fins de auditoria.

6.1.4 Disponibilização de chave pública da AC SOLUTI para usuários

As formas para a disponibilização do certificado da AC SOLUTI, e de todos os certificados da cadeia de certificação, para os usuários da AC SOLUTI, compreendem:

- no momento da disponibilização de um certificado para seu titular, será utilizado o formato definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[9];
- página web da AC SOLUTI (<https://ccd.acsoluti.com.br/>);
- outros meios seguros 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 ao certificado de AC Subsequente é de RSA 4096 bits (V2) e ECDSA 512 bits (V3), conforme definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[9].

6.1.6 Geração de parâmetros de chaves assimétricas

Os parâmetros de geração de chaves assimétricas da AC SOLUTI seguem o padrão FIPS (Federal Information Processing Standards) 140-2 nível 3, uma vez que utilizam hardware criptográfico com esta certificação. Este padrão é definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[9].

6.1.7 Verificação da qualidade dos parâmetros

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

O processo de geração do par de chaves da AC SOLUTI é feito por hardware padrão FIPS (Federal Information Processing Standards) 140-2, nível 3.

6.1.8.2

O processo utilizado para a geração de chaves criptográficas dos titulares de certificados segue os requisitos aplicáveis estabelecidos pelo documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL[7].

6.1.9 Propósitos de uso de chave (conforme campo “Key usage” na X.509 v3)

6.1.9.1

A chave privada de AC Subsequente pode ser utilizada apenas para assinatura dos certificados por ela emitidos e para assinatura de sua LCR.

6.1.9.2

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

6.2 Proteção da Chave Privada

A chave privada da AC SOLUTI é gerada, armazenada e utilizada apenas em hardware criptográfico,

classificado como FIPS 140-2 nível 3. O acesso a esse hardware 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 SOLUTI utiliza hardware criptográfico, classificado como FIPS 140-2 nível 3. Este padrão está definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[9].

6.2.1.2

Os módulos de geração de chaves criptográficas dos Titulares de Certificados são aqueles definidos no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[9].

6.2.2 Controle “n de m” para chave privada

6.2.2.1

A AC SOLUTI implementa o controle múltiplo para a ativação e desativação da sua chave privada através de controles de acesso físico e do software de certificação.

6.2.2.2

É exigido a presença no mínimo de 2 (dois) detentores da chave de ativação (“n”) de um grupo de 10 (dez) (“m”) para a ativação da chave da AC SOLUTI.

6.2.3 Recuperação (escrow) de chave privada

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

Como diretriz geral, qualquer entidade titular de certificado poderá, a seu critério, manter cópia de segurança de sua própria chave privada.

6.2.4.2

A AC SOLUTI mantém cópia de segurança de sua própria chave privada. Esta cópia é armazenada cifrada e protegida com um nível de segurança não inferior àquele definido para a versão original da chave e aprovado pelo CG da ICP-Brasil, e mantida pelo prazo de validade do certificado correspondente.

6.2.4.3

A AC SOLUTI não mantém cópia de segurança da chave privada de Titular de Certificado de assinatura digital por ela emitido.

6.2.4.4

Em qualquer caso, a cópia de segurança deve ser 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

As chaves privadas dos titulares de certificados emitidos pela AC SOLUTI não são arquivadas.

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

A AC SOLUTI 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

A ativação da chave privada da AC SOLUTI é implementada por meio de token criptográfico, protegido com senha, após a identificação de 2 dos detentores da chave de ativação da chave criptográfica. Os

detentores da chave de ativação são os Administradores da Soluti, seus sócios, diretores ou funcionários designados para essa função.. As senhas utilizadas obedecem à política de senhas estabelecida pela AC SOLUTI.

6.2.8 Método de desativação de chave privada

A chave privada da AC SOLUTI, armazenada em módulo criptográfico, é desativada quando não mais é necessária através de mecanismo disponibilizado pelo software de certificação que permite o apagamento de todas as informações contidas no módulo criptográfico. Este procedimento é implementado por meio de tokens criptográficos, protegidos com senha, após a identificação de 2 dos detentores da chave de ativação da chave criptográfica. Os detentores da chave de ativação são os Administradores do Sistema de Certificação da AC SOLUTI. As senhas utilizadas obedecem à política de senhas estabelecida pela AC SOLUTI.

6.2.9 Método de destruição de chave privada

Quando a chave privada da AC SOLUTI for desativada, em decorrência de expiração ou revogação, esta deve ser eliminada da memória do módulo criptográfico. Todas as cópias de segurança da chave privada da AC SOLUTI e os tokens criptográficos dos custodiantes serão eliminados. Os agentes autorizados para realizar estas operações são os administradores e os custodiantes das chaves de ativação da AC SOLUTI.

6.3 Outros Aspectos do Gerenciamento do Par de Chaves

6.3.1 Arquivamento de chave pública

A AC SOLUTI armazena as chaves públicas da própria AC SOLUTI e dos titulares de certificados, bem como as LCRs emitidas, após a expiração dos certificados correspondentes, permanentemente, para verificação de assinaturas geradas durante seu período de validade.

6.3.2 Períodos de uso para as chaves pública e privada

6.3.2.1

A chave privada da AC SOLUTI e dos titulares de certificados por ela emitidos, são utilizadas apenas durante o período de validade dos certificados correspondentes. A chave pública da AC SOLUTI pode ser utilizada durante todo o período de tempo determinado pela legislação aplicável, para verificação de assinaturas geradas durante o prazo de validade dos certificados correspondentes.

6.3.2.2

Não se aplica.

6.3.2.3

Não se aplica.

6.3.2.4

O período máximo de validade admitido para o certificado da AC SOLUTI é limitada à validade do certificado da AC que o emitiu.

6.4 Dados de ativação

Os dados de ativação, distintos das chaves criptográficas, são aqueles requeridos para a operação de alguns módulos criptográficos.

6.4.1 Geração e instalação dos dados de ativação

6.4.1.1

Os dados de ativação da chave privada da AC SOLUTI são únicos e aleatórios.

6.4.1.2

Não se aplica.

6.4.2 Proteção dos dados de ativação.

6.4.2.1

Os dados de ativação da AC SOLUTI são protegidos contra o uso não autorizado, por tokens criptográficos individuais com senha e pelo armazenamento em ambiente de nível 6 de segurança.

6.4.2.2

Os dados de ativação da chave privada da entidade titular do certificado são protegidos contra uso não autorizado.

6.4.3 Outros aspectos dos dados de ativação

Todos os aspectos acerca dos dados de ativação já foram tratados nos itens anteriores.

6.5 Controles de Segurança Computacional

6.5.1 Requisitos técnicos específicos de segurança computacional

6.5.1.1

A AC SOLUTI garante que a geração de seu par de chaves é realizada em ambiente off-line, para impedir o acesso remoto não autorizado durante o processo.

6.5.1.2

Os requisitos gerais de segurança computacional do equipamento onde são gerados os pares de chaves criptográficas dos titulares de certificados emitidos pela AC SOLUTI estão descritos desta DPC.

6.5.1.3

Os computadores servidores, utilizados pela AC SOLUTI, relacionados 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 SOLUTI;
- b) clara separação das tarefas e atribuições relacionadas a cada perfil qualificado da AC SOLUTI;
- c) acesso restrito aos bancos de dados da AC SOLUTI;
- d) uso de criptografia para segurança de base de dados, quando exigido pela classificação de suas informações;
- e) geração e armazenamento de registros de auditoria da AC SOLUTI;
- f) mecanismos internos de segurança para garantia da integridade de dados e processos críticos;
- g) 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 as informações sensíveis nele contidas apagadas e é efetuado controle de entrada e saída, registrando número de série e as datas de envio e de recebimento. Ao retornar às instalações onde residem os equipamentos utilizados para operação da AC SOLUTI, o equipamento que passou por manutenção é inspecionado. Em todo equipamento que deixar de ser utilizado em caráter permanente, são destruídas de maneira definitiva todas as informações sensíveis armazenadas, relativas à atividade da AC SOLUTI. Todos esses eventos são registrados para fins de auditoria.

6.5.1.6

Qualquer equipamento incorporado à AC SOLUTI, é preparado e configurado como previsto na Política de Segurança implementada ou em outro documento aplicável, de forma a apresentar o nível de segurança necessário à sua finalidade.

6.5.2 Classificação da segurança computacional

A segurança computacional da AC SOLUTI segue as recomendações Common Criteria.

6.5.3 Controle de segurança para as Autoridades de Registro

6.5.3.1

Os requisitos de segurança computacional das estações de trabalho e dos computadores portáteis utilizados pela ARs para os processos de validação e aprovação de certificados são os estabelecidos no documento CARACTERÍSTICAS MINIMAS DE SEGURANÇA PARA ARs DA ICP-BRASIL[1].

6.5.3.2

Nas PSs adotadas foram atendidos os requisitos mínimos estabelecidos no documento CARACTERÍSTICAS MINIMAS DE SEGURANÇA PARA ARs DA ICP-BRASIL[1], no item 6.5.32 "Estações de Trabalho".

6.6 Controles Técnicos do Ciclo de Vida

6.6.1 Controles de desenvolvimento de sistemas

6.6.1.1

A AC SOLUTI adota o Sistema de Certificação Digital da AC SOLUTI, desenvolvido em código aberto. Todas as customizações são realizadas inicialmente em um ambiente de desenvolvimento e após conclusão dos testes é colocado em um ambiente de homologação. Finalizando o processo de homologação das customizações, o Gerente do CCD avalia e decide quando será a implementação no ambiente de produção.

6.6.1.2

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

6.6.2 Controle de gerenciamento de segurança

6.6.2.1

As ferramentas e os procedimentos empregados pela AC SOLUTI para garantir que os seus sistemas implementem os níveis configurados de segurança são a administração de segurança de sistema que é controlada pelos privilégios nomeados a contas de sistema operacional, e pelos papéis confiados descritos no item 5.2.1.

6.6.2.2

O gerenciamento de configuração, para a instalação e a contínua manutenção do sistema de certificação utilizado pela AC SOLUTI, envolve o teste de mudanças planejadas no Ambiente de Desenvolvimento e Homologação isolados antes de sua implantação no ambiente de Produção, incluindo as seguintes atividades:

- a) instalação de novas versões ou de atualizações nos produtos que constituem a plataforma do sistema de certificação;
- b) implantação ou modificação de Autoridades Certificadoras com customizações a nível de certificados, páginas web, scripts, etc.;
- c) implantação de novos procedimentos operacionais relacionados com a plataforma de processamento incluindo módulos criptográficos;
- d) instalação de novos serviços na plataforma de processamento.

6.6.3 Classificação de segurança de ciclo de vida

Não se aplica.

6.6.4 Controles na geração da LCR antes de publicadas

Todas as LCRs geradas pela AC SOLUTI, antes de publicadas, são cheçadas 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 SOLUTI, incluindo firewalls e recursos similares.

6.7.1.2

Nos servidores e elementos de infra-estrutura e proteção de rede utilizados pela AC SOLUTI, somente os serviços estritamente necessários são habilitados.

6.7.1.3

Os servidores e elementos de infra-estrutura e proteção de rede tais como roteadores, hubs, switches, firewalls localizados no segmento de rede que hospeda o sistema de certificação da AC SOLUTI, 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 e homologação.

6.7.1.5

Acesso lógico aos elementos de infra-estrutura 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 permitam 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 estão implementados em equipamentos de utilização específica, configurados exclusivamente para tal função. O firewall promove o isolamento, em sub-redes específicas, dos equipamentos servidores com acesso externo – a conhecida "zona desmilitarizada" (ZDM) – em relação aos equipamentos com acesso exclusivamente interno à AC SOLUTI.

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 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 ao firewall ou ao terminal de gerenciamento, promover a desconexão automática de conexões suspeitas, ou ainda a reconfiguração do firewall.

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

As tentativas de acesso não autorizado – em roteadores, firewalls ou IDS – são registradas em arquivos para posterior análise, que poderá ser automatizada. O exame dos arquivos de registro é realizado diariamente e todas as ações tomadas em decorrência desse exame são documentadas.

6.8 Controles de Engenharia do Módulo Criptográfico

O módulo criptográfico utilizado pela AC SOLUTI para o armazenamento de sua chave privada é certificado como FIPS (Federal Information Processing Standards) 140-2, nível 3.

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 SOLUTI.

7.1.2

Não se aplica.

7.1.3

Nos itens seguintes é especificado o formato do certificado emitido para AC Subsequente.

7.2 Perfil do Certificado

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

7.2.1 Número(s) de versão

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

7.2.2 Extensões de certificados

Os certificados emitidos pela AC SOLUTI apresentam obrigatoriamente as seguintes extensões:

- a) **Authority Key Identifier**, não crítica: o campo **keyIdentifier** contém o hash SHA-1 da chave pública da AC SOLUTI;
- b) **Subject Key Identifier**, não crítica: contém o hash SHA-1 da chave pública da AC titular do certificado (AC Subsequente);
- c) **Key Usage**, crítica: somente os bits **keyCertSign** e **CRLSign** estão ativados;
- d) **Certificate Policies**, não crítica:
 1. o campo **policyIdentifier** deve conter os OIDs das PCs que a AC Subsequente, titular do certificado, implementa;
 2. o campo **policyQualifiers** deve conter o endereço Web da DPC da AC SOLUTI: <https://ccd.acsoluti.com.br/docs/dpc-ac-soluti.pdf>;
- e) **basicConstraints**, crítica: contém o campo **CA=True**; e
- f) **CRL Distribution Points**, não crítica: contém o endereço Web onde se obtém a LCR da AC SOLUTI:
 1. <http://ccd.acsoluti.com.br/lcr/ac-soluti-v1.crl>
 2. <http://ccd2.acsoluti.com.br/lcr/ac-soluti-v1.crl>
 3. <http://repositorio.icpbrasil.gov.br/lcr/ACSOLUTI/ac-soluti-v1.crl>

7.2.3 Identificadores de algoritmos

Os certificados de AC deverão ser assinados com o uso do algoritmo **sha512WithRSAEncryption**, definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[9].

7.2.4 Formatos de nome

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

C = BR
O = ICP-Brasil
OU = Autoridade Certificadora Raiz Brasileira v2
OU = AC SOLUTI
CN = nome da AC Subsequente

7.2.5 Restrições de nome

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

- a) Não são admitidos sinais de acentuação, trema ou cedilhas;
 - i. caracteres acentuados devem ser substituídos por seu correspondente sem acento;
 - ii. o cedilha deve ser substituído pelo caractere 'c';

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

Caractere	Código NBR9611 (hexadecimal)	Caractere	Código NBR9611 (hexadecimal)
(branco)	20	+	2B
!	21	,	2C
“	22	-	2D
#	23	.	2E
\$	24	/	2F
%	25	:	3A
&	26	;	3B
'	27	=	3D
(28	?	3F
)	29	@	40
*	2A	\	5C

7.2.6 OID (Object Identifier) de DPC

O Identificador de Objeto (OID) desta DPC, atribuído pela ICP-Brasil após a conclusão do processo de credenciamento, é 2.16.76.1.1.46.

7.2.7 Uso da extensão “Policy Constraints”

Extensão não utilizada.

7.2.8 Sintaxe e semântica dos qualificadores de política

O campo **policyQualifiers** da extensão “Certificate Policies” deverá conter o endereço web (URL) da DPC da AC SOLUTI: <https://ccd.acsoluti.com.br/docs/dpc-ac-soluti.pdf>.

7.2.9 Semântica de processamento para extensões críticas

Extensões críticas são interpretadas conforme a RFC 5280.

7.3 Perfil de LCR

7.3.1 Número (s) de versão

As LCR geradas pela AC SOLUTI 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

A AC SOLUTI adota as seguintes extensões de LCR definidas como obrigatórias pela ICP-Brasil:

- “Authority Key Identifier”, não crítica: contém o resumo SHA-1 da chave pública da AC SOLUTI;
- “CRL Number”, não crítica: contém número sequencial para cada LCR emitida.

7.3.2.2

A ICP-Brasil define como obrigatórias as seguintes extensões de LCR:

- “Authority Key Identifier”, não crítica: contém o resumo SHA-1 da chave pública da AC SOLUTI;
- “CRL Number”, não crítica: contém número sequencial para cada LCR emitida.

8 ADMINISTRAÇÃO DE ESPECIFICAÇÃO

8.1 Procedimentos de mudança de especificação

Qualquer alteração nesta DPC da AC SOLUTI será submetida previamente à aprovação do CG da ICP-Brasil.

8.2 Políticas de publicação e de notificação

A AC SOLUTI publica esta DPC, em sua página web acessível pela URL <https://ccd.acsoluti.com.br/docs/dpc-ac-soluti.pdf>. Sempre que esta DPC for atualizada será alterado o arquivo disponibilizado na web.

8.3 Procedimentos de aprovação

Essa DPC foi submetida à aprovação, durante o processo de credenciamento da AC SOLUTI, conforme o estabelecido no documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL[6].

Novas versões serão igualmente submetidas à aprovação da AC Raiz.

9 DOCUMENTOS REFERENCIADOS

9.1

Os documentos abaixo são aprovados por Resoluções do Comitê-Gestor da ICPBrasil, podendo ser alterados, quando necessário, pelo mesmo tipo de dispositivo legal. O site <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

9.2

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

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

Os documentos abaixo são aprovados pela AC Raiz, podendo ser alterados, quando necessário, mediante publicação de uma nova versão no sítio <http://www.iti.gov.br/>.

Ref.	Nome do documento	Código
[4]	MODELO DE TERMO DE TITULARIDADE	DOC-ICP-05.A
[5]	MODELO DE TERMO DE RESPONSABILIDADE	DOC-ICP-05.B