RNP
ORGANIZAÇÃO SOCIAL DO MCTI

Educação, Pesquisa
e Inovação em Rede

ICPEdu
CERTIFICADO
PESSOAL

Política de certificado e Declaração de práticas de certificação da AC raiz da ICPEdu

DAGSER | REDE NACIONAL
DE ENSINO E PESQUISA

PRESIDÊNCIA DA REPÚBLICA

Jair Messias Bolsonaro
Presidente da República

Hamilton Mourão
Vice-Presidente da República

MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÕES

Paulo César Rezende de Carvalho Alvim
Ministro da Ciência, Tecnologia e Inovações

REDE NACIONAL DE ENSINO E PESQUISA

Nelson Simões
Diretor-geral

Michael Stanton
Representante da Diretoria Executiva da RNP

Política de certificado e Declaração de práticas de certificação da AC raiz da ICPEdu

DAGSER | REDE NACIONAL DE
ENSINO E PESQUISA

RNP
ORGANIZAÇÃO SOCIAL DO MCTI

Educação, Pesquisa
e Inovação em Rede

BRASÍLIA
2022

© 2022 Rede nacional de Ensino e Pesquisa
Esta obra é licenciada sob licença Creative Commons Attribution 4.0 (CC-BY 4.0), sendo permitida a reprodução parcial ou total, desde que mencionada a fonte.

Os autores são responsáveis pela apresentação dos fatos contidos e opiniões expressas nesta obra.

Autores
Rede Nacional de Ensino e Pesquisa

Revisão gramatical e ortográfica
Nayara Oliveira

Normalização
Larissa Alves
Graziela Gomes

Design gráfico, diagramação e capa
Alisson Eugênio

Dados Internacionais de Catalogação na Publicação (CIP)

P769	Política de certificado e declaração de práticas de certificação da AC raiz da ICPedu / Rede nacional de Ensino e Pesquisa. – Brasília, DF: RNP, 2022. 56 p. ISBN 978-65-89167-49-5 1.Infraestrutura de Chaves Públicas. 2. Certificado digital. I.Rede nacional de ensino e pesquisa . II. Título CDU

Ficha catalográfica elaborada por Larissa de Araújo Alves - CRB1/3462

RNP Educação, Pesquisa e Inovação em Rede
ORGANIZAÇÃO SOCIAL DO MCTI

https://www.rnp.br/

RNP Brasília
SAUS Quadra 5 - Lote 6, Bloco H, Brasília
7º andar - Edifício IBICT
Brasília - DF - 70070-914
tel: 55 61 3243-4300
fax: 55 61 3226-5303

CAMPINAS
Prédio da Embrapa/Unicamp Av. André Tosello, 209 – Cidade Universitária Zeferino Vaz
Campinas - SP - 13083-886
tel: 55 19 3787-3300

RIO DE JANEIRO
Rua Lauro Müller, 116
sala 1103 - Botafogo
Rio de Janeiro - RJ - 22290-906
tel: 55 21 2102-9660
fax: 55 21 2279-3731

RESUMO

Nesta política e declaração de certificação são descritas as práticas e os procedimentos empregados pela Diretoria Adjunta de Gestão de Serviços (DAGSer) na execução dos seus serviços como Autoridade Certificadora Raiz (AC Raiz) da Infraestrutura de Chaves Públicas para Ensino e Pesquisa (ICPEdu). No documento são explicitadas orientações para o uso do certificado, a política de administração, os requisitos operacionais do ciclo de vida do certificado, os controles técnicos de segurança, entre outros.

Código de barras:
ISBN: 978-65-89167-49-5

Apoio:

ibict

MINISTÉRIO DA CIÊNCIA, TECNOLOGIA, E INOVAÇÕES

Realização:

RNP
ORGANIZAÇÃO SOCIAL DO MCTI

Educação, Pesquisa e Inovação em Rede

Sumário

1 Introdução 12

1.1 Visão Geral 12

1.2 NOME DO DOCUMENTO E IDENTIFICAÇÃO 13

1.3 PARTICIPANTES DA ICPEDU 13

1.3.1 Autoridades certificadoras 13

1.3.2 Autoridades de registro 13

1.3.3 Entidades confiáveis 13

1.4 USO DO CERTIFICADO 13

1.4.1 Uso apropriado do certificado 13

1.4.2 Uso proibitivo do certificado 13

1.5 POLÍTICA DE ADMINISTRAÇÃO 13

1.5.1 Organização administrativa do documento 13

1.5.2 Contatos 14

1.5.3 Responsável pela adequabilidade da DPC com a PC 14

1.5.4 Procedimento de aprovação da DPC 14

1.6 DEFINIÇÕES E ACRÔNIMOS 14

2 REPOSITÓRIOS 16

2.1 RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO 16

2.1.1 O repositório da AC Raiz da ICPEdu é acessível através do endereço https://repositorio.icpedu.rnp.br. 16

2.2 PUBLICAÇÕES DE INFORMAÇÕES ... 16

2.2.1 A ICPEdu mantém disponível repositório atendendo os seguintes requisitos: ... 16

2.2.2 No repositório, são publicadas as versões atuais e todas as anteriores de LCRs, DPCs, PCs, certificados de ACs e ARs credenciadas e dados para contato. 16

2.3 FREQUÊNCIA DE PUBLICAÇÕES 16

2.3.1 O repositório é atualizado no prazo máximo de até 8 horas sempre que houver mudança nas informações listadas na Seção 2.2. 16

2.4 CONTROLES DE ACESSO AOS REPOSITÓRIOS 16

2.4.1 Todas as informações do repositório são públicas e podem ser acessadas para consulta em modo somente leitura e de forma anônima 16

2.4.2 São utilizados controles de acesso físico e lógico para restringir a possibilidade de escrita ou modificação dos documentos publicados no repositório por pessoas não autorizadas.
O servidor que armazena as informações acima se encontra em nível adequado de segurança física e requer credenciais de acesso.. 16

3 IDENTIFICAÇÃO E AUTENTICAÇÃO 17

3.1 ATRIBUIÇÃO DE NOMES 17

3.1.1 Tipos de nomes 17

3.1.2 Necessidade dos nomes serem significativos 17

3.1.3 Anonimato dos titulares de certificado 17

3.1.4 Regras para interpretação dos diversos formatos de nomes 17

3.1.5 Unicidade dos nomes 17

3.2 VALIDAÇÃO INICIAL DE IDENTIDADE 17

3.2.1 Método para prova da posse de chave privada 18

3.2.2 Autenticação da identificação da organização 18

3.2.3 Validação de autoridade 18

3.2.4 Autenticação da identidade de equipamento ou aplicação 18

3.2.5 Procedimentos complementares 18

3.3 IDENTIFICAÇÃO E AUTENTICAÇÃO PARA PEDIDOS DE NOVAS CHAVES 18

3.3.1 Estabelecer processos 18

3.3.2 Procedimentos específicos 19

3.3.3 Procedimentos específicos de expiração ou revogação 19

4 REQUISITOS OPERACIONAIS DO CICLO DE VIDA DO CERTIFICADO . 20

4.1 PROCEDIMENTOS DO REQUERENTE PARA SOLICITAR O CERTIFICADO 20

4.1.1 Quem pode submeter uma solicitação de certificado 20

4.1.2 Processo de registro e responsabilidades ... 20

4.2 PROCESSAMENTO DE SOLICITAÇÃO DE CERTIFICADO 21

4.2.1 Execução das funções de identificação e autenticação 21

4.2.2 Aprovação ou rejeição das solicitações de certificado 21

4.2.3 Tempo para processamento das solicitações 21

4.3 PROCESSAMENTO DE EMISSÃO DE CERTIFICADO 21

4.3.1 Ações da AC durante a emissão de certificado 21

4.3.2 Notificação do solicitante pela AC sobre a emissão de certificado 22

4.4 ACEITAÇÃO DO CERTIFICADO 22

4.4.1 Conduta que constitui a aceitação de certificado 22

4.4.2 Publicação do certificado pela AC 22

4.4.3 Notificação da emissão de certificado pela AC para outras entidades 22

4.5 USABILIDADE DO PAR DE CHAVES E DO CERTIFICADO 22

4.5.1 Responsabilidade pela utilização das chaves privadas e dos certificados por parte dos titulares 22

4.5.2 Responsabilidade pela utilização das chaves públicas e dos certificados das partes confiáveis 23

4.6 RENOVAÇÃO DE CERTIFICADOS 23

4.7 REEMISSÃO DE CERTIFICADOS POR TROCA DE CHAVES 23

4.8 REEMISSÃO DE CERTIFICADOS POR TROCA DE DADOS 23

4.9 SUSPENSÃO E REVOGAÇÃO DE CERTIFICADO 23

4.9.1 Circunstâncias para revogação 23

4.9.2 Quem pode solicitar revogação 24

4.9.3 Procedimento para solicitação de revogação 24

4.9.4 Prazo para a solicitação de revogação 24

4.9.5 Prazo para a AC processar a solicitação de revogação 24

4.9.6 Requisitos para verificação de revogação para as partes confiáveis 25

4.9.7 Frequência de emissão de LCRs 25

4.9.8 Latência máxima para LCRs 25

4.9.9 Procedimentos adicionais no caso de comprometimento da chave privada 25

4.9.10 Circunstâncias para suspensão 25

4.10 SERVIÇOS DE STATUS DE CERTIFICADO 25

4.10.1 Características operacionais 25

4.11 ENCERRAMENTO DO VÍNCULO COM A AC 26

4.11.1 Prazo de solicitação 26

4.12 CUSTÓDIA E RECUPERAÇÃO DE CHAVES 26

5 CONTROLES OPERACIONAIS, GERENCIAMENTO E DE INSTALAÇÕES 27

5.1 CONTROLES FÍSICOS 27

5.1.1 Construção e localização das instalações da AC 27

5.1.2 Acesso físico 27

5.1.3 Energia e ar-condicionado 29

5.1.4 Exposição à água 30

5.1.5 Prevenção e proteção contra incêndio 30

5.1.6 Armazenamento de mídia 30

5.1.7 Descarte de lixo 30

5.1.8 Instalações de segurança (*backup*) externas (off-site) para AC 30

5.2 CONTROLES PROCEDIMENTAIS 30

5.2.1 Perfis qualificados 30

5.2.2 Número de pessoas necessárias por tarefa 32

5.2.3 Identificação e autenticação para cada papel 32

5.2.4 Funções que requerem separação de deveres 32

5.3 CONTROLES DE PESSOAL 32

5.3.1 Antecedentes, qualificação, experiência e requisitos de idoneidade 32

5.3.2 Procedimentos de verificação de antecedentes 33

5.3.3 Requisitos de treinamento 33

5.3.4 Sanções para ações não autorizadas 33

5.3.5 Requisitos para prestadores de serviço independentes 33

5.3.6 Documentação fornecida aos funcionários 33

5.4 PROCEDIMENTOS DE LOG DE AUDITORIA 34

5.4.1 Tipos de eventos registrados 34

5.4.2 Frequência de auditoria de registros 35

5.4.3 Período de retenção para registros de auditoria 35

5.4.4 Proteção de registros de auditoria 35

5.4.5 Procedimentos para cópia de segurança (backup) de registros de auditoria 35

5.4.6 Sistema de coleta de dados de auditoría 36

5.4.7 Notificação de agentes causadores de eventos 36

5.4.8 Avaliações de vulnerabilidades 36

5.5 ARQUIVAMENTO DE REGISTROS 36

5.5.1 Tipos de registros arquivados 36

5.5.2 Período de retenção para arquivo 36

5.5.3 Requisitos para datação dos registros 36

5.5.4 Sistema de recolhimento de registros (interno ou externo) 36

5.5.5 Procedimentos para obtenção e verificação dos registros armazenados 37

5.6 TROCA DE CHAVE 37

5.6.1 Prazos específicos 37

5.7 COMPROMETIMENTO E RECUPERAÇÃO DE DESASTRE 37

5.8 EXTINÇÃO DA AC OU AR 37

5.8.1 Providências mínimas a serem tomadas em caso de extinção 37

6 CONTROLES TÉCNICOS DE SEGURANÇA 38

6.1 GERAÇÃO E INSTALAÇÃO DE PARES DE CHAVES 38

6.1.1 Geração de pares de chaves 38

6.1.2 Entrega pública para emissor de certificado 38

6.1.3 Divulgação da chave pública da AC 38

6.1.4 Tamanhos de chaves 39

6.1.5 Geração dos parâmetros de chave pública e verificação de qualidade 39

6.1.6 Propósitos de uso de chaves 39

6.2 PROTEÇÃO DA CHAVE PRIVADA E CONTROLE DE ENGENHARIA DO MÓDULO CRIPTOGRÁFICO 39

6.2.1 Padrões e controle para módulo criptográfico 39

6.2.2 Controle “n de m” para chave privada 39
6.2.3 Custódia (scrow) de chave privada 39
6.2.4 Cópia de segurança de chave privada 40
6.2.5 Arquivamento de chave privada 40
6.2.6 Inserção de chave privada em módulo criptográfico 40
6.2.7 Armazenamento de chave privada em módulo criptográfico 40
6.2.8 Método de ativação de chave primária 40
6.2.9 Método de desativação de chave primária 40
6.2.10 Método de destruição da chave privada 40

6.3 OUTROS ASPECTOS DO GERENCIAMENTO DO PAR DE CHAVES 40

6.3.1 Arquivamento de chave pública 40
6.3.2 Períodos de operação do certificado e períodos de uso para as chaves pública e privada 41

6.4 DADOS DE ATIVAÇÃO 41

6.4.1 Geração e instalação dos dados de ativação 41
6.4.2 Proteção de dados de ativação 41

6.5 CONTROLES DE SEGURANÇA COMPUTACIONAL 41

6.5.1 Requisitos técnicos 41

6.6 CONTROLES TÉCNICOS DO CICLO DE VIDA 42

6.6.1 Controles de desenvolvimento de sistemas 42
6.6.2 Controles de gerenciamento de segurança 42

6.7 CONTROLES DE SEGURANÇA DE REDE 42

6.7.1 Diretrizes gerais 42
6.7.2 *Firewall* 43
6.7.3 Sistema de detecção de intrusão (IDS) 43
6.7.4 Registro de acessos não autorizados à rede 43

6.8 CARIMBO DE TEMPO 43

6.8.1 Data e hora 43
6.8.2 Atualização off-line 43

7 PERFIS DE CERTIFICADO, LCR E OCSP 44

7.1 PERFIL DO CERTIFICADO 44

7.1.1 Número de versão 44
7.1.2 Extensões de certificado 44
7.1.3 Identificadores de algoritmo 44
7.1.4 Formatos de nome 44
7.1.5 Restrições de nome 44
7.1.6 OID (Object Identifier) da DPC 44
7.1.7 Sintaxe e semântica dos qualificadores de política 44

7.2 7.2 PERFIL DE LCR 45

7.2.1 Número(s) da versão 45
7.2.2 Extensões de LCR e de suas entradas 45

7.3 PERFIL DE OCSP 45

8 AUDITORIA DE CONFORMIDADE E OUTROS PADRÕES 46

8.1 FREQUÊNCIA E CIRCUNSTÂNCIAS DAS AVALIAÇÕES 46

8.1.1 Frequência 46

8.2 IDENTIFICAÇÃO/QUALIFICAÇÃO DO AVALIADOR 46

8.2.1 Identificação dos avaliadores 46
8.2.2 Avaliações 46

8.3 RELAÇÃO DO AVALIADOR COM A ENTIDADE AVALIADA 46

8.3.1 Avaliação da AC Raiz da ICPEdu 46
8.3.2 Avaliação das ACs vinculadas 46

8.4 TÓPICOS COBERTOS PELA AVALIAÇÃO....47

8.4.1 Verificação da conformidade da AC Raiz com esta PC/DPC e com as políticas e regras estabelecidas no contexto da ICPEdu. Aspectos como gerência das chaves e gerência do ciclo de vida do Certificado devem ser avaliados com especial cuidado....47

8.4.2 Declaração de auditoria da AC-Raiz....47

8.4.3 Declaração de auditoria de AC vinculada ...47

8.5 AÇÕES TOMADAS COM RESULTADO DE UMA INEFICIÊNCIA....47

8.5.1 Notificações à DAGSer....47

8.6 COMUNICAÇÃO DOS RESULTADOS....47

8.6.1 Encaminhamento....47

9 OUTROS NEGÓCIOS E ASSUNTOS JURÍDICOS....48

9.1 TARIFAS....48

9.1.1 Tarifas de emissão e renovação de certificados....48

9.1.2 Tarifas de acesso ao certificado 48

9.1.3 Tarifas de revogação ou de acesso à informação de status....48

9.1.4 Tarifas de outros serviços....48

9.2 RESPONSABILIDADE FINANCEIRA....48

9.3 CONFIDENCIALIDADE DA INFORMAÇÃO DO NEGÓCIO....48

9.3.1 Escopo de informações confidenciais:....48

9.3.2 Informações fora do escopo de informações confidenciais....49

9.3.3 Responsabilidade em proteger a informação confidencial....49

9.4 PRIVACIDADE DA INFORMAÇÃO PESSOAL....49

9.5 DIREITOS DE PROPRIEDADE INTELECTUAL....49

9.5.1 Critério de proteção....49

9.6 LIMITAÇÕES DE RESPONSABILIDADES....49

9.6.1 Danos 49

9.7 INDENIZAÇÕES....49

9.7.1 Responsabilização 49

9.8 PRAZO E RESCISÃO 49

9.8.1 Prazo....49

9.8.2 Término 49

9.8.3 Efeito da rescisão e sobrevivência....50

9.9 AVISOS INDIVIDUAIS E COMUNICAÇÕES COM OS PARTICIPANTES....50

9.9.1 Meio de comunicação 50

9.10 ALTERAÇÕES 50

9.10.1 Procedimentos para emendas....50

9.11 SOLUÇÃO DE CONFLITOS 50

9.11.1 Instâncias 50

9.12 LEI APLICÁVEL....50

9.12.1 Legislação....50

9.13 COM A LEI APLICÁVEL....50

9.13.1 Instâncias e cumprimento 50

REFERÊNCIAS BIBLIOGRÁFICAS....51

APÊNDICE A....52

Controle de versões

Versão	Data	Responsável	Natureza das Modificações
2.0	10/11/2008	Vinod Rebello	Criação do documento
3.0	20/06/2011	André Landim Leandro Guimarães	Atualização para o lançamento da AC Raiz da ICPEdu V2, com uso de SHA2 e RSA 4096
3.1.	01/05/2012	Anderson Silvério Ricardo Custódio	Correção dos itens levantados na auditoria
3.2	11/11/2020	Rick Lopes de Souza	Adaptação dos novos grupos que administram a ICPEdu
3.3	30/11/2021	Luciano Rocha Rick Lopes de Souza Yuri Alexandro	Revisão do texto

CORPORATIVO:
Documento para uso interno. A impressão deste documento torna a cópia não controlada

1 INTRODUÇÃO

A ICPEdu – Infraestrutura de Chaves Públicas para Ensino e Pesquisa, é o serviço de certificação digital oferecido pela Rede Nacional de Ensino e Pesquisa – RNP, que provê infraestrutura para a emissão de certificados digitais e chaves de segurança. O ICPEdu certificado Pessoal permite a emissão de certificados para identificação pessoal de alunos, professores e servidores das instituições que aderem ao serviço para validação de variados procedimentos digitais, como assinaturas eletrônicas, cifragem de documentos e autenticação em sistemas eletrônicos específicos.

1.1 VISÃO GERAL

Esta Declaração de Políticas e Práticas de Certificação (PC/DPC) descreve as práticas e os procedimentos empregados pela Diretoria Adjunta de Gestão de Serviços – DAGSer – na execução dos seus serviços como Autoridade certificadora Raiz (AC Raiz da ICPEdu) da Infraestrutura de Chaves Públicas para Ensino e Pesquisa (ICPEdu).

A governança do serviço ICPEdu é realizada pela DAGSer, no papel de Grupo de Operação Autoridade de Registro, sendo responsável pela mobilização e gestão dos grupos envolvidos na sua operação, assim como também é responsável pelas ações que envolvem a administração dos certificados de mais alto nível da cadeia de certificação da ICPEdu, pelo primeiro atendimento das instituições que desejam aderir ao serviço, pela execução dos procedimentos administrativos exigidos para aceitação de uma instituição como futuro membro da ICPEdu, pela administração das políticas relacionadas às operações da ICPEdu, incluindo análise e emissão de parecer de aprovação para criação de Autoridades certificadoras Intermediárias (ACs) e Autoridades de Registro (ARs), estabelecendo relação de confiança entre as organizações que aderem ao serviço ICPEdu e suas entidades integrantes.

Os certificados da AC Raiz da ICPEdu são autoassinados e são utilizados para assinar os certificados de autoridades certificadoras credenciadas, o certificado da AR Raiz e as listas de certificados revogados (LCR).

Existem dois comitês que apoiam a RNP na administração e manutenção da ICPEdu, ambos os comitês são entidades externas à RNP, sendo a sua composição aprovada pela Diretoria Executiva da RNP.

a) Comitê Assessor de Gestão de Identidade (CA-GId), representa as entidades usuárias da RNP e é responsável por aprovar os relatórios gerenciais dos serviços ICPEdu. Este comitê é responsável por balizar a priorização de projetos e melhorias a serem executadas na ICPEdu, com finalidade de justificar perante à Diretoria Executiva da RNP a prioridade das ações. Este comitê possui autonomia para solicitar auditoria nos afiliados para verificação da adequação com a política de uso.

b) Comitê Técnico de Gestão de Identidades (CT-GId), com membros eleitos pela Diretoria Executiva da RNP com o balizamento do CA-GId com a finalidade de apontar caminhos para a inovação tecnológica da ICPEdu.

A estrutura desta DPC é baseada no documento DOC-ICP-05.

Versão: 2.0

CORPORATIVO:
Documento para uso interno. A impressão deste documento torna a cópia não controlada

1.2 NOME DO DOCUMENTO E IDENTIFICAÇÃO

Esta Política de certificado e Declaração de Práticas de Certificação da Autoridade certificadora Raiz da ICPEdu é comumente referida como "PC/DPC da AC Raiz da ICPEdu".

O *Object Identifier* - OID desta PC/DPC é 1.3.6.1.4.1.15996.1.1.1.2, onde:

- 1.3.6.1.4.1 - Prefixo para *private enterprises* (IANA);
- 15996 - Prefixo RNP;
- 1 – ICPEdu;
- 1 - AC Raiz da ICPEdu;
- 1 - PC/DPC;
- 2 - Versão do documento.

1.3 PARTICIPANTES DA ICPEDU

1.3.1 Autoridades certificadoras

Esta DPC refere-se unicamente à Autoridade certificadora Raiz da ICPEdu.

1.3.2 Autoridades de registro

A atividade de identificação e cadastramento das AC externas e internas de nível imediatamente subsequente ao da AC Raiz da ICPEdu é realizada através da AR Raiz, operada pela DAGSer.

1.3.3 Entidades confiáveis

As autoridades certificadoras (AC) e de registro (AR) intermediárias imediatamente subordinadas à AC Raiz da ICPEdu;

1.4 USO DO CERTIFICADO

Esta seção descreve as aplicações apropriadas para o uso dos certificados digitais emitidos pela AC Raiz da ICPEdu.

1.4.1 Uso apropriado do certificado

Os certificados emitidos pela AC Raiz da ICPEdu têm como objetivo único identificar a própria AC Raiz, as ACs de nível imediatamente subsequente e a AR Raiz.

1.4.2 Uso proibitivo do certificado

Todas as aplicações não listadas na Seção 1.4.1.

1.5 POLÍTICA DE ADMINISTRAÇÃO

Esta seção apresenta os dados para contatar a AC Raiz da ICPEdu.

1.5.1 Organização administrativa do documento

Diretoria Adjunta de Gestão de Serviços da RNP.

CORPORATIVO:
Documento para uso interno. A impressão deste documento torna a cópia não controlada

1.5.2 Contatos

Nome: DAGSer / Rede Nacional de Ensino e Pesquisa (RNP)
Endereço: SAS, Quadra 5, Lote 6, bloco H, 7º andar, Edifício IBICT, Brasília, DF
Telefone: (61) 3243-4300 fax: (61) 3226-5303
Página web: http://ajuda.rnp.br/icpedu
E-mail: atendimento@rnp.br

1.5.3 Responsável pela adequabilidade da DPC com a PC

Nome: Luciano Fernandes da Rocha
Telefone: (61) 3243-4300
E-mail: atendimento@rnp.br

1.5.4 Procedimento de aprovação da DPC

Esta DPC é analisada e aprovada pelo CA-GID.
Os procedimentos de aprovação da DPC da ICPEdu são avaliados e aprovados pela CA-GId.

1.6 DEFINIÇÕES E ACRÔNIMOS

Sigla	Descrição
AC	Autoridade certificadora
AC Raiz da ICPEdu	Autoridade certificadora Raiz da ICPEdu
Administrador do SGCI	Grupo responsável pela administração do SGCI
AES	*Advanced Encryption Algorithm* (Algoritmo de Cifragem Avançada)
AR	Autoridade de Registro
Backup	Cópia de segurança
CA-GId	Comitê Assessor de Gestão de Identidade
CC	*Common Criteria* (Critérios Comuns)
COBIT	*Control Objectives for Information and related Technology*
COSO	Committee of Sponsoring Organizations
Criador do SGCI	Usuário responsável pela criação e inicialização do SGCI
CT-GId	Comitê Técnico de Gestão de Identidade
DN	*Distinguished Name*
DPC	Declaração de Práticas de Certificação
EAL	*Evaluation Assurance Level (Nível de Avaliação de Garantia)*
GNA	Gerador de Números Aleatórios
Grupo de Administradores do HSM	Grupo responsável pela administração do HSM

CORPORATIVO: Documento para uso interno. A impressão deste documento torna a cópia não controlada

Sigla	Descrição
Grupo de Auditores do HSM	Grupo responsável pela auditoria do HSM
Grupo de Operadores do HSM	Grupo responsável pela operação do HSM
ICP	Infraestrutura de Chaves Públicas
ICPEdu	Infraestrutura de Chaves Públicas para Pesquisa e Ensino
IEC	*International Electrotechnical Commission*
ISO	*International Standards Organization* (Organização Internacional de Padrões)
ITU	*International Telecommunications Union*
LCR	Lista de certificados Revogados
NIST	*National Institute of Standards* (Instituto Nacional de Padrões dos EUA)
OID	*Object Identifier*
Operador do SGCI	Grupo responsável pela operação do SGCI
OSCP	*Online Certificate Status Protocol*
Parte Confiante	Entidade que age confiando no teor e validade de certificados de terceiros
PC	Política de certificados
PCN	Plano de Continuidade de Negócio
PP	*Protection Profile* (Perfil de Proteção)
OS	Política de Segurança
PSC	Provedor de Serviços Criptográficos
RCD	Repositório de certificados Digitais
RFC	*Request For Comments*
RNP	Rede Nacional de Ensino e Pesquisa
RSA	Algoritmo RSA de chave pública
SHA	*Secure Hash Algorithm* (Algoritmo Seguro de Resumo Criptográfico)
SEG.P.005	Política de Segurança da Informação do ICPEdu
Status do certificado	Estado de validade do certificado, que pode ser vigente, expirado ou revogado
UTC	*Coordinated Universal Time*

CORPORATIVO:
Documento para uso interno. A impressão deste documento torna a cópia não controlada

2 REPOSITÓRIOS

2.1 RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO

2.1.1 O repositório da AC Raiz da ICPEdu é acessível através do endereço https://repositorio.icpedu.rnp.br.

2.2 PUBLICAÇÕES DE INFORMAÇÕES

2.2.1 A ICPEdu mantém disponível repositório atendendo os seguintes requisitos:

a) Disponibilizar, logo após a sua emissão, os certificados emitidos pela AC e sua LCR/OCSP;

b) Estar disponível para consulta 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana;

c) Definir os protocolos de acesso; e

d) Implementar todos os recursos necessários para a segurança dos dados armazenados.

2.2.2 No repositório, são publicadas as versões atuais e todas as anteriores de LCRs, DPCs, PCs, certificados de ACs e ARs credenciadas e dados para contato.

2.3 FREQUÊNCIA DE PUBLICAÇÕES

2.3.1 O repositório é atualizado no prazo máximo de até 8 horas sempre que houver mudança nas informações listadas na Seção 2.2.

2.4 CONTROLES DE ACESSO AOS REPOSITÓRIOS

2.4.1 Todas as informações do repositório são públicas e podem ser acessadas para consulta em modo somente leitura e de forma anônima.

2.4.2 São utilizados controles de acesso físico e lógico para restringir a possibilidade de escrita ou modificação dos documentos publicados no repositório por pessoas não autorizadas. O servidor que armazena as informações acima se encontra em nível adequado de segurança física e requer credenciais de acesso.

CORPORATIVO: Documento para uso interno. A impressão deste documento torna a cópia não controlada

3 IDENTIFICAÇÃO E AUTENTICAÇÃO

Esta seção apresenta as formas de identificação e de autenticação das instituições participantes ICPEdu.

3.1 ATRIBUIÇÃO DE NOMES

Esta seção apresenta a estrutura de nomes adotados pela AC Raiz da ICPEdu.

3.1.1 Tipos de nomes

O tipo de nome admitido para os titulares dos certificados emitidos é o "*Distinguished Name*" (DN), respeitando as regras do X.500 [1].

3.1.2 Necessidade dos nomes serem significativos

O Anexo A apresenta o conteúdo do nome distinto (DN) dos certificados emitidos para ACs pela AC Raiz da ICPEdu. Não são admitidos caracteres especiais ou de acentuação nos campos do DN. Os valores para o nome distinto da AC Raiz da ICPEdu, ACs Credenciadas, ACs de serviço e ARs Credenciadas podem ser encontrados na seção A.1 do Anexo A.

3.1.3 Anonimato dos titulares de certificado

A AC Raiz da ICPEdu não emite certificados com suporte ao anonimato.

3.1.4 Regras para interpretação dos diversos formatos de nomes

Os nomes são interpretados conforme estabelecido nas Seções 3.1.1 e 3.1.2.

3.1.5 Unicidade dos nomes

Os nomes de um certificado são únicos no conjunto de certificados emitidos pela AC Raiz da ICPEdu.

3.2 VALIDAÇÃO INICIAL DE IDENTIDADE

Este item apresenta o processo de validação inicial da identidade da organização interessada em possuir uma AC e de seu representante. Além de terem seus dados validados, essas organizações também terão suas PC/DPC's (Política de certificados e Declaração de Práticas de Certificação) avaliadas pela DAGSer.

Versão: 2.0

CORPORATIVO: Documento para uso interno. A impressão deste documento torna a cópia não controlada

3.2.1 Método para prova da posse de chave privada

O requerente deverá apresentar à AC Raiz da ICPEdu um arquivo de requisição de certificado assinado usando a chave privada que faz par à chave pública da AC. Esta assinatura consiste na prova de posse da chave privada.

3.2.2 Autenticação da identificação da organização

3.2.2.1 A identificação da organização é feita de forma automática quando esta se torna qualificada a utilizar os serviços da RNP, não sendo realizada autenticação específica.

3.2.3 Validação de autoridade

É reconhecido como responsável pela AC da organização a pessoa nomeada pelo dirigente máximo da organização solicitante, por meio de publicação em Diário Oficial ou equivalente.

3.2.4 Autenticação da identidade de equipamento ou aplicação

A AC Raiz da ICPEdu não emite certificado para equipamentos ou aplicações.

3.2.5 Procedimentos complementares

3.2.5.1 A AC mantém políticas e procedimentos internos que são revisados regularmente a fim de cumprir os requisitos dos vários programas de raiz dos quais a AC é membro.

3.2.5.2 Cópias de todos os documentos utilizados para confirmação da identidade de uma organização e/ou de um indivíduo são arquivadas, observadas as condições definidas na SEG.P.005.

3.2.5.3 A AC Raiz da ICPEdu emite instrução normativa que define os procedimentos para identificação do requerente e comunicação de irregularidades no processo de emissão de um certificado digital.

3.3 IDENTIFICAÇÃO E AUTENTICAÇÃO PARA PEDIDOS DE NOVAS CHAVES

Esse item descreve o procedimento para a validação da identidade do requerente de novas chaves.

3.3.1 Estabelecer processos

Os processos de identificação e confirmação do cadastro do solicitante e utilizados para a geração de novo par de chaves e novo certificado correspondente são previstos e elaborados pela AC Raiz da ICPEdu.

3.3.1.1 Possibilidades de condução

Esse processo é conduzido segundo uma das seguintes possibilidades:

a) por meio de videoconferência, conforme procedimentos e requisitos técnicos definidos em Instrução Normativa da AC Raiz da ICPEdu, os quais devem assegurar nível de segurança equivalente à forma presencial, garantindo a validação das mesmas informações de identificação e biométricas, mediante o emprego de tecnologias eletrônicas seguras de comunicação, interação, documentação e tratamento biométrico; ou

b) por meio de mecanismo automatizado de gerenciamento de certificado do tipo SSL/TLS.

CORPORATIVO: Documento para uso interno. A impressão deste documento torna a cópia não controlada

3.3.2 Procedimentos específicos

Caso sejam requeridos procedimentos específicos para as PC implementadas, eles são descritos nessas PC, no item correspondente.

3.3.3 Procedimentos específicos de expiração ou revogação

Para os casos específicos de expiração ou revogação de um certificado de AC de nível imediatamente subsequente ao da AC Raiz da ICPEdu, esta deve executar os processos regulares de geração de seu novo par de chaves após a expiração ou revogação de seu certificado.

CORPORATIVO:
Documento para uso interno. A impressão deste documento torna a cópia não controlada

4
REQUISITOS OPERACIONAIS DO CICLO DE VIDA DO CERTIFICADO

Este capítulo especifica os requisitos impostos aos certificados emitidos pela AC Raiz da ICPEdu para AC credenciada e listas de certificados revogados.

4.1 PROCEDIMENTOS DO REQUERENTE PARA SOLICITAR O CERTIFICADO

Este item descreve o processo de solicitação do certificado por uma organização aprovada a possuir uma Autoridade certificadora.

4.1.1 Quem pode submeter uma solicitação de certificado

Organizações credenciadas pela DAGSer, que tiverem sua PC/DPC aprovadas.

4.1.2 Processo de registro e responsabilidades

Após a validação da PC/DPC pela DAGSer, esta inicia o processo de auditoria do ambiente onde estará instalada a Autoridade certificadora. Após o parecer favorável da auditoria, a DAGSer informa à instituição sobre o parecer favorável, que, por sua vez, solicitará a emissão do certificado. A requisição, em formato PKCS#10, deve ser enviada para a DAGSer pelo gerente da AC requisitante, que, após conferir as informações contidas no arquivo, realiza a validação da origem do pedido e do gerente da AC e encaminha a requisição para a DAGSer para que a emissão do certificado seja feita.

4.1.2.1 Responsabilidades da AC:

4.1.2.1.1 Da AC Raiz da ICPEdu

a) gerenciamento de seu par de chaves criptográficas;
b) emissão e distribuição do seu certificado digital;
c) emissão e distribuição dos certificados de AC de nível imediatamente abaixo do seu;
d) publicação dos certificados emitidos por ela;
e) revogação dos certificados emitidos por ela;
f) gerenciamento da Lista de certificados Revogados (LCR);
g) garantia da segurança da operação, conforme estabelecido nesta DPC e na Política de Segurança.
h) aplicação e manutenção do PCN – Plano de Continuidade de Negócios.

CORPORATIVO:
Documento para uso interno. A impressão deste documento torna a cópia não controlada

4.2 PROCESSAMENTO DE SOLICITAÇÃO DE CERTIFICADO

Esta seção descreve os procedimentos para a solicitação de emissão de certificados pela AC Raiz da ICPEdu.

4.2.1 Execução das funções de identificação e autenticação

A autenticação da solicitação é realizada por meio da prova de posse da chave e da validação da Identificação do requerente.

4.2.2 Aprovação ou rejeição das solicitações de certificado

As requisições de certificados válidas são aprovadas mediante a homologação do ambiente onde a AC será instalada. Não conformidades encontradas são documentadas em um relatório, com prazo definido para providências e apresentação de nova solicitação.

4.2.3 Tempo para processamento das solicitações

O prazo máximo para a validação da requisição de emissão de certificados é de 07 (sete) dias úteis, devendo o relatório da auditoria do ambiente ser entregue em, no máximo, 07 (sete) dias úteis para a realização desta.

4.3 PROCESSAMENTO DE EMISSÃO DE CERTIFICADO

Esta seção descreve como é realizada a emissão de um certificado digital pela AC Raiz da ICPEdu.

4.3.1 Ações da AC durante a emissão de certificado

Esta seção descreve os procedimentos gerais para a emissão de certificados pela AC Raiz da ICPEdu.

4.3.1.1 A solicitação de certificado para uma AC de nível imediatamente subsequente ao da AC Raiz da ICPEdu só é possível após o deferimento de seu pedido de credenciamento e a consequente autorização de funcionamento da AC em questão por parte da DAGSer da RNP;

4.3.1.2 A AC deve encaminhar a solicitação de seu certificado à DAGSer por meio de seus representantes legais;

4.3.1.3 A emissão de um certificado pela DAGSer é feita em cerimônia específica na qual são registrados todos os procedimentos executados;

4.3.1.4 A DAGSer garante que a cerimônia de emissão de um certificado para AC de nível imediatamente subsequente ao seu ocorre, caso haja demanda, na primeira semana a cada bimestre;

4.3.1.5 O certificado é considerado válido a partir do momento em que é emitido e publicado no repositório da AC Raiz da ICPEdu;

4.3.1.6 A DAGSer entrega o certificado emitido para o representante legal da AC credenciada;

CORPORATIVO: Documento para uso interno. A impressão deste documento torna a cópia não controlada

4.3.1.7 A emissão dos certificados da AC Raiz da ICPEdu, da AR Raiz, e das ACs e ARs de nível imediatamente subsequente é feita em equipamentos da DAGSer que operam off-line.

4.3.2 Notificação do solicitante pela AC sobre a emissão de certificado

A organização solicitante é notificada da emissão do certificado por comunicação oficial da RNP, acompanhada do Termo de Recebimento e Aceitação.

4.4 ACEITAÇÃO DO CERTIFICADO

4.4.1 Conduta que constitui a aceitação de certificado

4.4.1.1 A DAGSer garante que as informações do certificado foram verificadas de acordo com esta PC/DPC quando da emissão para uma AC Intermediária. O certificado é, então, publicado pela DAGSer, que envia o certificado para o responsável pela organização junto à ICPEdu, juntamente com um documento denominado Termo de Recebimento e Aceitação, que deverá ser assinado e enviado de volta ao DAGSer no prazo de até 05 (cinco) dias úteis. Se, ao término deste prazo, a organização não enviar o Termo de Recebimento e Aceitação, o certificado será revogado e, neste caso, a AC deverá realizar uma nova solicitação à DAGSer.

4.4.1.2 No momento da entrega do certificado, o requerente atesta o seu recebimento por meio de assinatura de Termo de Recebimento e Aceitação por seu representante legal.
A aceitação do certificado se dá no momento em que seus dados constantes são verificados pela AC solicitante.

4.4.1.3 A verificação dos dados do certificado e o envio do Termo de Recebimento e Aceitação devem ser realizados pela AC titular no prazo de 5 (cinco) dias úteis, contados a partir do seu recebimento.

4.4.1.4 Ao aceitar o certificado, a AC:

a) concorda com as responsabilidades, obrigações e deveres a ela impostas pelo Termo de Recebimento e Aceitação e sua DPC aprovada;
b) afirma que todas as informações de certificado fornecidas durante o processo de credenciamento são verdadeiras e estão reproduzidas no certificado de forma correta e completa.

4.4.2 Publicação do certificado pela AC

O certificado emitido é publicado no repositório da AC Raiz da ICPEdu, conforme Seção 2.1, 2.2 e 2.3.

4.4.3 Notificação da emissão de certificado pela AC para outras entidades

A AC Raiz da ICPEdu não notifica outras entidades, além do próprio titular, quando emitir certificados.

4.5 USABILIDADE DO PAR DE CHAVES E DO CERTIFICADO

4.5.1 Responsabilidade pela utilização das chaves privadas e dos certificados por parte dos titulares

Os titulares dos certificados das ACs são responsáveis pela proteção da chave privada. Estas devem ser geradas e armazenadas em módulos de *hardware* seguros (HSM). O uso da chave

CORPORATIVO:
Documento para uso interno. A impressão deste documento torna a cópia não controlada

privada deve respeitar todas as políticas impostas pela AC Raiz da ICPEdu, seja indiretamente através da sua DPC, PS ou de extensões contendo políticas registradas em seu certificado. Havendo ocorrência de qualquer anormalidade ou suspeita de comprometimento da chave privada da AC, a DAGGer deve ser imediatamente informada.

4.5.2 Responsabilidade pela utilização das chaves públicas e dos certificados das partes confiáveis

4.5.2.1 As entidades devem:

a) estar cientes das informações presentes nesta PC/DPC;

b) verificar a mais recente LCR emitida pela AC Raiz da ICPEdu antes de aceitar o certificado da AC como válido;

c) observar restrições de uso da chave privada e do certificado.

d) verificar as datas de validade do certificado.

4.6 RENOVAÇÃO DE CERTIFICADOS

A AC Raiz da ICPEdu não renova certificados. O titular da AC pode solicitar um novo certificado de acordo com os procedimentos descritos na seção 4.1.

4.7 REEMISSÃO DE CERTIFICADOS POR TROCA DE CHAVES

A AC Raiz da ICPEdu não realiza reemissão de um certificado de uma AC pela simples troca do par de chaves criptográficas. O titular da AC pode solicitar um novo certificado, de acordo com os procedimentos descritos na seção 4.1.

4.8 REEMISSÃO DE CERTIFICADOS POR TROCA DE DADOS

Se for necessária a modificação dos dados de um certificado, esta deverá ser feita a partir da emissão de um novo certificado, de acordo com os procedimentos descritos na seção 4.1.

4.9 SUSPENSÃO E REVOGAÇÃO DE CERTIFICADO

Informações sobre revogação de certificados de ACs de nível imediatamente subsequente ao da AC Raiz da ICPEdu são fornecidas na LCR da AC Raiz da ICPEdu. As razões para a revogação de certificado são públicas. A suspensão de certificados não é realizada no âmbito da ICPEdu.

4.9.1 Circunstâncias para revogação

4.9.1.1 Um certificado de AC de nível imediatamente subsequente ao da AC Raiz da ICPEdu pode ser revogado a qualquer instante, resguardados os princípios do contraditório e da ampla defesa.

4.9.1.2 Um certificado deve obrigatoriamente ser revogado:

a) quando for constatada a emissão imprópria ou defeituosa;

b) quando for necessária a alteração de qualquer informação que consta nele;

c) na dissolução da AC titular do certificado;

d) no comprometimento da chave privada da AC ou da sua mídia armazenadora.

CORPORATIVO: Documento para uso interno. A impressão deste documento torna a cópia não controlada

4.9.1.3 A DAGSer pode revogar o certificado da AC que deixar de cumprir a legislação vigente ou as políticas, normas, práticas e regras estabelecidas para a ICPEdu;

4.9.1.4 As chaves públicas dos certificados emitidos por uma AC dissolvida serão armazenadas por outra AC, após aprovação da DAGSer (RNP);

4.9.1.5 Quando houver mais de uma AC interessada, assume a responsabilidade do armazenamento das chaves públicas aquela indicada pela AC que encerrou as suas atividades;

4.9.1.6 A AC que encerrou as suas atividades deve transferir, se for o caso, a documentação dos certificados digitais emitidos à AC que tenha assumido a guarda das respectivas chaves públicas;

4.9.1.7 Caso as chaves públicas não tenham sido assumidas por outra AC, os documentos referentes aos certificados digitais e as respectivas chaves públicas são repassados à DAGSer.

4.9.2 Quem pode solicitar revogação

A revogação de um certificado somente pode ser feita:

a) por solicitação justificada dos seguintes grupos integrantes da ICPEdu: CA-GId e DAGSer.

b) por solicitação justificada da AC titular do certificado;

c) por determinação judicial.

4.9.3 Procedimento para solicitação de revogação

4.9.3.1 A solicitação de revogação do certificado à AC Raiz da ICPEdu deve ser encaminhada à DAGSer pelo representante legal da AC titular do certificado.

4.9.3.2 O processo de revogação de um certificado de AC é precedido, quando for o caso, do recebimento, pela DAGSer, da solicitação de revogação e termina quando uma nova LCR, contendo o certificado revogado, é emitida e publicada.

4.9.3.3 O prazo para a revogação de certificado de AC de nível imediatamente subsequente ao da AC Raiz da ICPEdu é de no máximo 48 (quarenta e oito) horas úteis, contados a partir do recebimento da solicitação de revogação ou da determinação de revogação emitido pela DAGSer.

4.9.3.4 Um certificado de AC revogado somente pode ser usado para a verificação de assinaturas geradas durante o período em que o referido certificado esteve válido.

4.9.4 Prazo para a solicitação de revogação

4.9.4.1 A solicitação de revogação deve ser imediata quando ocorre uma das circunstâncias definidas na seção 4.9.1 desta PC/DPC.

4.9.5 Prazo para a AC processar a solicitação de revogação

4.9.5.1 A DAGSer publica em até 24 (vinte e quatro) horas úteis o certificado revogado na LCR.

CORPORATIVO:
Documento para uso interno. A impressão deste documento torna a cópia não controlada

4.9.6 Requisitos para verificação de revogação para as partes confiáveis

4.9.6.1 Todos os certificados das AC de nível imediatamente subsequente ao da AC Raiz da ICPEdu têm a validade verificada de cada certificado na cadeia de certificação de acordo com os padrões IETF PKIX, incluindo a verificação da validade do certificado, encadeamento do nome do emissor e titular, restrições de uso de chaves e de políticas de certificação e o status de revogação por meio de LCRs ou respostas OCSP identificados em cada certificado na cadeia de certificação.

4.9.7 Frequência de emissão de LCRs

4.9.7.1 A frequência máxima admitida para a emissão de LCR referente a certificados de AC é de 112 (cento e doze) dias. Em caso de revogação de certificado de AC de nível imediatamente subsequente ao seu, a AC Raiz da ICPEdu emite nova LCR no prazo previsto no item 4.9.5 e notifica todas as ACs de nível imediatamente subsequente ao seu.

4.9.7.2 Caso sejam utilizadas frequências de emissão de LCR específicas para as PCs implementadas, estas devem ser descritas nessas PCs, no item correspondente.

4.9.7.3 A LCR é emitida com validade de 113 (cento e treze) dias.

4.9.8 Latência máxima para LCRs

4.9.8.1 A LCR é divulgada no repositório em, no máximo, 24 (vinte e quatro) horas após sua geração.

4.9.9 Procedimentos adicionais no caso de comprometimento da chave privada

4.9.9.1 A AC Raiz da ICPEdu é obrigada a avisar as ACs subsequentes do comprometimento de sua chave privada e dos procedimentos que irá adotar para dar continuidade às suas operações.

4.9.9.2 Uma AC subsequente deve garantir que a sua DPC contenha determinações que definam os meios que serão utilizados para notificar o comprometimento ou suspeita de comprometimento de sua chave privada.

4.9.10 Circunstâncias para suspensão

4.9.10.1 A AC Raiz da ICPEdu não realiza a suspensão de certificados, salvo em casos específicos e determinados pelo DAGSer.

4.10 SERVIÇOS DE STATUS DE CERTIFICADO

4.10.1 Características operacionais

4.10.1.1 A AC Raiz da ICPEdu não disponibiliza outros serviços de status de certificados além da publicação de LCRs.

CORPORATIVO:
Documento para uso interno. A impressão deste documento torna a cópia não controlada

4.11 ENCERRAMENTO DO VÍNCULO COM A AC

4.11.1 Prazo de solicitação

4.11.1.1 A AC subsequente deve solicitar à DAGSer, com pelo menos 30 dias de antecedência, o encerramento do seu vínculo com a AC Raiz da ICPEdu. O vínculo é considerado encerrado quando ocorrer expiração ou revogação do certificado.

4.12 CUSTÓDIA E RECUPERAÇÃO DE CHAVES

A AC Raiz da ICPEdu não oferece serviços de custódia e recuperação de chaves para as ACs subsequentes.

CORPORATIVO:
Documento para uso interno. A impressão deste documento torna a cópia não controlada

5
CONTROLES OPERACIONAIS, GERENCIAMENTO E DE INSTALAÇÕES

5.1 CONTROLES FÍSICOS

O gerenciamento de certificados da AC Raiz da ICPEdu possui os seguintes controles:

a) segurança física e controles ambientais;

b) controles de integridade de sistemas, incluindo gerenciamento de configuração, manutenção de integridade de código confiável e detecção e prevenção de incidentes;

c) segurança de rede e gerenciamento de *firewalls*, incluindo restrições de porta e filtragem de endereços de IP;

d) gerenciamento de usuários, segregação de funções, capacitação e treinamento;

e) controles de acesso lógico com registro de atividades a fim de fornecer responsabilidades individuais.

Esses controles são implementados com o objetivo de evitar perda, danos ou comprometimento de ativos, interrupção das atividades do negócio relacionadas aos processos de gerenciamento de certificados, roubo de informações e comprometimento das instalações de processamento de informações.

5.1.1 Construção e localização das instalações da AC

Para a execução das atividades relacionadas aos processos de gerenciamento de certificados, a AC Raiz da ICPEdu utiliza instalações aprovadas pela DAGSer (RNP). Essas instalações estão de acordo com as normas de classificação e práticas para segurança física relativa ao armazenamento de dados.

5.1.2 Acesso físico

5.1.2.1 O acesso físico às dependências da AC Raiz da ICPEdu onde são realizadas as atividades relacionadas aos processos de gerenciamento de certificados da AC Raiz da ICPEdu é gerenciado e controlado internamente de acordo com os requisitos definidos na SEG.P.005.

5.1.2.2 O controle de acesso é realizado por meio de chaves, senhas, cartões criptográficos, identificações biométricas e outros dispositivos de forma que apenas pessoas autorizadas participem das atividades pertinentes.

5.1.2.3 O acesso físico é monitorado por meio de circuito fechado de TV (CFTV) com gravação digital 24x7.

5.1.2.4 O sistema de certificação da AC Raiz da ICPEdu está situado em ambientes seguros redundantes, tipo sala cofre, localizados em instalações geograficamente segregadas.

CORPORATIVO: Documento para uso interno. A impressão deste documento torna a cópia não controlada

5.1.2.5 Segurança física e controles de acesso através de identificação biométrica restringem o acesso aos equipamentos e sistemas relativos aos processos de gerenciamento de certificados.

5.1.2.6 São definidos 4 (quatro) níveis de acesso físico aos diversos ambientes da AC Raiz da ICPEdu:

a) Primeiro nível: a primeira barreira de acesso às instalações da AC Raiz da ICPEdu. Neste nível 1, cada indivíduo é identificado e registrado em algum sistema de gerenciamento de tarefas e pessoas no interior da área guarnecida por algum profissional qualificado. A partir desse nível, pessoas estranhas à operação da AC transitam devidamente identificadas e acompanhadas. Nenhum tipo de processo operacional ou administrativo relacionado ao gerenciamento de certificados da AC é executado neste nível. A partir deste nível, equipamentos de gravação, fotografia, vídeo, som ou similares, bem como computadores portáteis, tem entrada controlada e somente podem ser utilizados mediante autorização formal e com supervisão;

b) Segundo nível: Interno ao primeiro nível e requer identificação individual das pessoas que nele entram. Esse é o nível mínimo de segurança exigido para a execução de qualquer processo operacional ou administrativo da AC Raiz da ICPEdu. A passagem do primeiro para o segundo nível exige identificação por meio eletrônico e uso de crachá;

c) Terceiro nível: nível a partir do qual são abrigados materiais e atividades sensíveis relacionadas aos processos de gerenciamento de certificados da AC Raiz da ICPEdu. Pessoas que não estejam envolvidas com essas atividades não têm permissão de acesso a este nível, não podendo permanecer nele se não estiverem acompanhadas por alguém que tenha permissão. São controladas tanto as entradas quanto as saídas de cada pessoa autorizada. Dois mecanismos de controle de identificação são requeridos para permitir a entrada: individual e biométrica. Dispositivos móveis e portáteis de comunicação e armazenamento de dados, exceto aqueles necessários para a operação da AC Raiz da ICPEdu, não são permitidos;

d) Quarto nível: onde ocorrem as atividades especialmente sensíveis da operação da AC Raiz da ICPEdu, tais como emissão e revogação de certificados e a emissão de LCR. Todos os sistemas e equipamentos necessários a essas atividades estão localizados a partir desse nível. O nível 4 possui os mesmos níveis de controles de acesso do nível 3 e, adicionalmente, exige em cada acesso ao seu ambiente a identificação de, no mínimo, 2 pessoas autorizadas;

e) Quinto nível: compreende em um cofre ou um gabinete reforçado trancado. Materiais criptográficos, como chaves, dados de ativação, senhas, cartões eletrônicos e equipamentos criptográficos são armazenados neste ambiente.

5.1.2.7 As salas-cofre são construídas segundo as normas brasileiras aplicáveis e eventuais omissões dessas normas são sanadas por normas internacionais pertinentes.

5.1.2.8 São permitidos vários ambientes de quarto nível para abrigar e segregar, quando for o caso: equipamentos de produção on-line e cofre de armazenamento, equipamentos de produção off-line e cofre de armazenamento, equipamentos de rede e infraestrutura (*firewall*, roteadores, *switches* e servidores);

CORPORATIVO:
Documento para uso interno. A impressão deste documento torna a cópia não controlada

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

a) ser feito em aço ou material de resistência equivalente;

b) possuir tranca com chave.

5.1.2.10 Mecanismos de emergência

a) Mecanismos específicos são implantados pela AC Raiz da ICPEdu para garantir a segurança dos equipamentos e das pessoas que operam em emergências. 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.

b) A AC Raiz da ICPEdu poderá especificar e implantar outros mecanismos de emergência específicos para cada tipo de instalação. Todos os procedimentos referentes aos mecanismos de emergência são documentados.

5.1.3 Energia e ar-condicionado

5.1.3.1 A AC Raiz da ICPEdu e os repositórios estão localizados em ambiente seguro que, além de conectados à rede elétrica, dispõe de gerador principal, sistema de *nobreaks*, sistema de aterramento e proteção a descargas atmosféricas;

5.1.3.2 Todos os cabos elétricos estão protegidos por tubulações ou dutos apropriados.

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

5.1.3.3 Os registros sobre a topologia da rede são mantidos atualizados, observados os requisitos de sigilo estabelecidos pela SEG.P.005.

5.1.3.4 Não são admitidas instalações provisórias, fiações expostas ou diretamente conectadas às tomadas sem a utilização de conectores adequados.

5.1.3.5 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 (quatro), o sistema de climatização é independente e tolerante a falhas.

5.1.3.6 A temperatura dos ambientes atendidos pelo sistema de climatização é permanentemente monitorada pelo sistema de notificação de alarmes.

5.1.3.7 O sistema de ar condicionando dos ambientes de nível 4 (quatro) é interno, com troca de ar realizada apenas por abertura da porta.

5.1.3.8 A capacidade de redundância de toda a estrutura de energia e ar-condicionado da AC é garantida, por meio de:

a) Geradores de porte compatível;

b) Geradores de reserva;

c) Sistemas de *nobreaks* redundantes; e

d) Sistemas redundantes de ar-condicionado.

CORPORATIVO: Documento para uso interno. A impressão deste documento torna a cópia não controlada

5.1.4 Exposição à água

5.1.4.1 A AC Raiz da ICPEdu está localizada em uma estrutura inteiriça de um ambiente de nível quatro, construída na forma de uma célula estanque a fim de prover a proteção física contra infiltrações e inundações provenientes de qualquer fonte externa. Além disso, existe um sistema de alarme de detecção de umidade e uma equipe de monitoramento pronta para responder a qualquer exposição à água.

5.1.5 Prevenção e proteção contra incêndio

5.1.5.1 Os sistemas de prevenção contra incêndios, internos aos ambientes, possibilitam alarmes preventivos antes de fumaça visível, disparados somente com a presença de partículas que caracterizam o sobreaquecimento de materiais elétricos e outros materiais combustíveis presentes nas instalações.

5.1.5.2 Nas instalações da AC Raiz da ICPEdu, não é permitido fumar ou portar quaisquer objetos que possam produzir fogo ou faísca.

5.1.5.3 A sala de nível 4 (quatro) possui sistema para detecção precoce de fumaça e sistema de extinção de incêndio por gás, além de portas corta-fogo.

5.1.5.4 Em caso de incêndio nas instalações da AC Raiz da ICPEdu, a sala de nível 4 (quatro) está preparada para não exceder a temperatura interna de 50 graus Celsius por, no mínimo, 1 (uma) hora.

5.1.6 Armazenamento de mídia

5.1.6.1 A AC Raiz da ICPEdu atende a norma brasileira NBR 11.515/NB 1334 (“Critérios de Segurança Física Relativos ao Armazenamento de Dados”).

5.1.7 Descarte de lixo

5.1.7.1 Todos os documentos em papel que contenham informações classificadas como sensíveis são adequadamente destruídos no procedimento de descarte.

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

5.1.8 Instalações de segurança (*backup*) externas (off-site) para AC

5.1.8.1 A AC Raiz da ICPEdu mantém cópias de segurança em uma instalação de *backup* que atende aos mesmos requisitos de segurança de sua instalação principal.

5.1.8.2 Em caso de sinistro que torne inoperante a instalação principal, a instalação de *backup* não é atingida e se torna totalmente operacional em condições idênticas em, no máximo, 48 (quarenta e oito) horas.

5.2 CONTROLES PROCEDIMENTAIS

5.2.1 Perfis qualificados

5.2.1.1 A AC Raiz da ICPEdu garante a separação das tarefas para funções críticas com o intuito de evitar que um empregado utilize indevidamente o sistema de certificação sem ser detectado. As ações de cada empregado estão limitadas de acordo com o respectivo perfil.

CORPORATIVO:
Documento para uso interno. A impressão deste documento torna a cópia não controlada

5.2.1.2 A AC Raiz da ICPEdu estabelece um mínimo de 4 (quatro) perfis distintos para sua operação, distinguindo as operações do dia a dia do sistema, o gerenciamento e auditoria dessas operações, bem como o gerenciamento de mudanças substanciais no sistema.

5.2.1.2.1 A divisão de responsabilidades entre os perfis é:

5.2.1.2.1.1 Gerente:

a) define e altera os grupos de administradores, auditores e operadores;
b) aprova os relatórios da AC Raiz da ICPEdu;
c) Encaminha relatórios da AC Raiz da ICPEdu ao CA-GID;

5.2.1.2.1.2 Administrador:

a) instala, configura e atualiza os equipamentos e softwares de gestão do ciclo de vida do certificado digital;
b) cria uma AC;
c) configura os templates de certificados de acordo com esta DPC;
d) associa a AC a uma política e atribui ou troca os grupos de operadores e auditores da AC;
e) gerencia os operadores da AC Raiz da ICPEdu;
f) realiza o backup e recuperação de backup de dados e software de acordo com a política estabelecida;
g) inicia e encerra os serviços da AC Raiz da ICPEdu;
h) define e altera os grupos de auditores e operadores.

5.2.1.2.1.3 Auditor:

a) audita as operações da AC Raiz da ICPEdu;
b) audita o ciclo de vida do certificado digital, das chaves criptográficas e de todas as operações do GOPAC realizadas para a operação da AC;
c) verifica os registros de auditoria;
d) verifica o cumprimento desta DPC.

5.2.1.2.1.4 Operador:

a) utiliza a chave privada de uma AC para a emissão de certificados digitais e LCR;
b) emite, expede, distribui, revoga e gerencia certificados;
c) distribui cartões (*tokens*), quando for o caso.

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

5.2.1.4 Quando um empregado se desliga da AC Raiz da ICPEdu, suas permissões de acesso são revogadas imediatamente. Quando há mudança na posição ou função que o empregado ocupa dentro da AC, as permissões de acesso são revistas. Em ambos os casos, todos os recursos disponibilizados ao empregado são devolvidos à AC Raiz após o seu desligamento.

CORPORATIVO:
Documento para uso interno. A impressão deste documento torna a cópia não controlada

5.2.2 Número de pessoas necessárias por tarefa

5.2.2.1 O controle multiusuário via o uso de segredo compartilhado é requerido para a geração e a utilização da chave privada da AC Raiz da ICPEdu, conforme o descrito na Seção 6.2.2.

5.2.2.2 Todas as tarefas executadas no ambiente onde está localizado o equipamento de certificação da AC Raiz da ICPEdu são realizadas na presença de, no mínimo, 2 (dois) funcionários da DAGSer, sendo facultada a presença de um auditor durante a execução do procedimento. As demais tarefas da AC Raiz da ICPEdu podem ser executadas por um único funcionário.

5.2.3 Identificação e autenticação para cada papel

5.2.3.1 Todo funcionário da DAGSer tem sua identidade e perfil verificados antes de:

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

5.2.3.2 Os certificados, contas e senhas utilizadas para identificação e autenticação dos funcionários:

a) são diretamente atribuídos a um único empregado;
b) não permitem compartilhamento;
c) são restritos às ações associadas ao perfil para o qual foram criados.

5.2.3.3 A AC Raiz da ICPEdu implementa o padrão de senhas conforme definido na norma SEG.N.002, com procedimentos de validação dessas senhas.

5.2.4 Funções que requerem separação de deveres

A AC Raiz da ICPEdu não permite que o auditor exerça os papéis de administrador e operador, segregando as atividades para o pessoal especificamente atribuído às funções definidas no item.

5.3 CONTROLES DE PESSOAL

Esta DPC garante que todos os empregados da AC Raiz da ICPEdu e das ACs vinculadas, encarregados de tarefas operacionais, tenham registrado em contrato ou termo de responsabilidade:

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

5.3.1 Antecedentes, qualificação, experiência e requisitos de idoneidade

Todo o pessoal da AC Raiz da ICPEdu em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados é admitido conforme o estabelecido na SEG.P.005.

CORPORATIVO: Documento para uso interno. A impressão deste documento torna a cópia não controlada

5.3.2 Procedimentos de verificação de antecedentes

5.3.2.1 Com o propósito de resguardar a segurança e a credibilidade da AC Raiz da ICPEdu, todo o pessoal envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados são submetidos aos critérios de validação de idoneidade profissional definidos na SEG.P.005

5.3.2.2 O responsável pela AC Raiz da ICPEdu é aprovado formalmente pela DAGSer.

5.3.3 Requisitos de treinamento

5.3.3.1 Todo o pessoal da AC Raiz da ICPEdu e das ACs vinculadas envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados recebem a devida capacitação profissional suficiente para o domínio dos seguintes temas:

a) princípios e mecanismos de segurança da informação;
b) atividades sob sua responsabilidade;
c) procedimentos de recuperação de desastres e de continuidade do negócio.

5.3.4 Sanções para ações não autorizadas

5.3.4.1 Na eventualidade de uma ação não autorizada, real ou suspeita, ser realizada por pessoa encarregada de processo operacional da AC Raiz da ICPEdu ou vinculada, a AC Raiz da ICPEdu, de imediato, tem como procedimento padrão suspender o acesso dessa pessoa ao seu sistema de certificação, instaurar processo administrativo para apurar os fatos e, se for o caso, adotar as medidas legais cabíveis.

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

a) relato da ocorrência;
b) identificação dos envolvidos;
c) eventuais prejuízos causados;
d) punições aplicadas, se for o caso; e
e) conclusões.

5.3.4.3 As punições passíveis de aplicação, em decorrência de processo administrativo, são determinadas pela Gerência de Recursos Humanos da RNP.

5.3.5 Requisitos para prestadores de serviço independentes

Todo o pessoal da AC Raiz da ICPEdu envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados segue as diretrizes de contratação estabelecidas na SEG.P.005. A AC Raiz da ICPEdu poderá definir requisitos adicionais para a contratação.

5.3.6 Documentação fornecida aos funcionários

5.3.6.1 A AC Raiz da ICPEdu disponibiliza para todo o seu pessoal:

a) sua DPC;
b) a SEG.P.005;
c) documentação operacional relativa às suas atividades;
d) contratos, normas e políticas relevantes para suas atividades.

CORPORATIVO: Documento para uso interno. A impressão deste documento torna a cópia não controlada

5.4 PROCEDIMENTOS DE LOG DE AUDITORIA

5.4.1 Tipos de eventos registrados

5.4.1.1 A AC Raiz da ICPEdu registra em arquivos de auditoria todos os eventos relacionados à segurança do seu sistema de certificação. Entre outros, os arquivos incluem os seguintes eventos:

a) inicialização e desligamento do sistema de certificação;
b) tentativas de criar, remover, definir senhas ou mudar privilégios de sistema dos operadores da AC Raiz;
c) mudanças na configuração da AC Raiz ou nas suas chaves;
d) tentativas de acesso (*login*) e de saída do sistema (*logoff*);
e) tentativas não autorizadas de acesso aos arquivos de sistema;
f) geração de chaves próprias da AC Raiz ou de chaves de seus usuários finais;
g) emissão e revogação de certificados;
h) geração de LCR;
i) tentativas de iniciar, remover, habilitar e desabilitar usuários de sistemas e recuperar suas chaves;
j) mudanças nas políticas de criação de certificados;
k) operações falhas de escrita ou leitura no repositório de certificados e da aplicável;
l) operações de escrita nesse repositório, quando aplicável; e
m) realização de *backup* e procedimentos de recuperação.

5.4.1.2 A AC Raiz da ICPEdu pela DPC também registra informações de segurança não geradas diretamente pelo seu sistema de certificação, tais como:

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

5.4.1.3 A DAGSer coleta e consolida, eletrônica ou manualmente, informações de segurança não geradas diretamente pelo sistema de certificação, tais como:

a) registros de acessos físicos;
b) manutenção e mudanças na configuração dos seus sistemas;
c) mudanças de pessoal;
d) relatórios de discrepância e comprometimento;
e) registros de destruição de mídia contendo chaves criptográficas, dados de ativação de certificados ou informação pessoal de usuário.

5.4.1.3.1 Para facilitar o processo de auditoria, toda a documentação relacionada aos serviços do GOPAC da DAGSer é coletada e consolidada, eletrônica ou manualmente, em um local único, conforme a SEG.P.005.

CORPORATIVO: Documento para uso interno. A impressão deste documento torna a cópia não controlada

5.4.1.4 Todos os registros de auditoria, eletrônicos ou manuais, contêm data e hora do evento, bem como a identidade do usuário que o causou.

5.4.1.5 A DAGSer também coleta e consolida, eletrônica ou manualmente, informações de segurança não geradas diretamente pelo sistema de certificação, tais como:

a) registros de acessos físicos;
b) manutenção e mudanças na configuração dos seus sistemas;
c) mudanças de pessoal;
d) relatórios de discrepância e comprometimento;
e) registros de destruição de mídia contendo chaves criptográficas, dados de ativação de.

5.4.2 Frequência de auditoria de registros

Os eventos registrados são analisados, dependendo da sua criticidade, das seguintes formas:

a) mensalmente;
b) quando há a emissão ou revogação de um certificado digital;
c) quando há a ocorrência de uma anormalidade, como em caso de suspeita de comprometimento da segurança.

5.4.3 Período de retenção para registros de auditoria

A documentação dos eventos relacionados no item anterior é arquivada pelo seguinte período:

a) certificados digitais e respectivas LCR são armazenados permanentemente, para fins de consulta histórica;
b) demais informações, inclusive arquivos de auditoria, são retidas por, no mínimo, 5 (cinco) anos.

5.4.4 Proteção de registros de auditoria

Os arquivos que contêm os registros de auditoria têm integridade garantida através da validação da função criptográfica hash, e com acesso restrito e exclusivo aos administradores e auditores.

5.4.5 Procedimentos para cópia de segurança (backup) de registros de auditoria

5.4.5.1 Os registros de eventos e sumários de auditoria do sistema de gerenciamento de certificados, plataformas criptográficas e demais componentes da infraestrutura, utilizados pela AC Raiz da ICPEdu, possuem cópias de segurança mensais ou sempre que houver alguma utilização desses equipamentos quando em ambiente off-line.

5.4.5.2 Os registros de auditoria são armazenados em um local seguro (sala-cofre ou cofre de segurança) à prova de incêndio, sob o controle de pessoas autorizadas em função de confiança, e em local diferente dos componentes que os originaram. As cópias de segurança dos registros de auditoria são protegidas no mesmo grau dos originais.

5.4.5.3 A AC Raiz da ICPEdu verifica a integridade das cópias de segurança a cada 6 (seis) meses.

CORPORATIVO: Documento para uso interno. A impressão deste documento torna a cópia não controlada

5.4.6 Sistema de coleta de dados de auditoría

5.4.6.1 Todos os sistemas de eventos para auditoria utilizados pela AC Raiz da ICPEdu em seus procedimentos operacionais operam internamente.

5.4.6.2 O sistema de coleta de eventos para auditoria utilizados pela AC Raiz da ICPEdu é executado por seu pessoal operacional ou por seus sistemas.

5.4.6.3 Os eventos para auditoria começam na inicialização dos sistemas e *hardwares* e terminam apenas em seu desligamento, sendo garantidas a integridade e a disponibilidade dos dados coletados.

5.4.7 Notificação de agentes causadores de eventos

5.4.7.1 A notificação de agentes causadores de eventos segue os procedimentos contidos na norma SEG.N.010 (Norma de Gestão de Incidentes de Segurança).

5.4.8 Avaliações de vulnerabilidades

5.4.8.1 Todos os registros são analisados visando encontrar possíveis vulnerabilidades na plataforma computacional que hospeda o sistema de gerenciamento de certificados digitais e as chaves criptográficas da AC Raiz da ICPEdu.

5.5 ARQUIVAMENTO DE REGISTROS

5.5.1 Tipos de registros arquivados

Além dos registros de eventos para auditoria mencionados na seção 5.4.1, também são arquivados:

a) lista de certificados revogados; e

b) certificados emitidos.

5.5.2 Período de retenção para arquivo

5.5.2.1 As cópias de segurança dos arquivos de registros de auditoria são armazenadas pelo gerente do grupo e sua integridade deve ser garantida através da validação da função criptográfica hash, em mídia não volátil, trocada a cada 5 (cinco) anos.

5.5.2.2 O armazenamento das mídias está situado fisicamente distante do local original do arquivo.

5.5.3 Requisitos para datação dos registros

5.5.3.1 Todos os registros contêm informações de data e hora, baseados na hora oficial internacional (UTC – ***Universal Time Coordinated***) e obedecem ao formato YYYYMMDDHHMMSSZ, incluindo segundos.

5.5.4 Sistema de recolhimento de registros (interno ou externo)

5.5.4.1 O sistema de coleta de toda informação para arquivamento é feito pela própria AC Raiz da ICPEdu.

CORPORATIVO: Documento para uso interno. A impressão deste documento torna a cópia não controlada

5.5.5 Procedimentos para obtenção e verificação dos registros armazenados

5.5.5.1 Informações do arquivo só podem ser obtidas mediante aprovação do gerente da AC Raiz da ICPEdu. A integridade das informações extraídas do arquivo pode ser verificada por meio da comparação com resumo criptográfico do arquivo publicado a cada modificação deste.

5.6 TROCA DE CHAVE

5.6.1 Prazos específicos

5.6.1.1 Um novo par de chaves para a AC Raiz da ICPEdu deve ser gerado, no mínimo, três meses antes do ponto de atualização de seu certificado.

5.7 COMPROMETIMENTO E RECUPERAÇÃO DE DESASTRE

A ICPEdu disponibiliza um Plano de Tratamento de Incidentes e Continuidade do Negócio (PCN) que descreve os procedimentos para recuperação em caso de comprometimento ou desastre a fim de garantir a continuidade dos seus serviços críticos.

5.8 EXTINÇÃO DA AC OU AR

5.8.1 Providências mínimas a serem tomadas em caso de extinção

5.8.1.1 Notificar a todas as entidades integrantes da ICPEdu;

5.8.1.2 Notificar titulares de certificados e entidades;

5.8.1.3 Notificar contatos de segurança relevantes;

5.8.1.4 Revogar todos os certificados emitidos;

5.8.1.5 Emitir e publicar pelo menos um LCR final válida e disponível até a data de expiração original do certificado da AC;

5.8.1.6 Destruir qualquer cópia das chaves privadas;

5.8.1.7 Arquivar os registros de forma segura, indicando o responsável pela sua custódia;

5.8.1.8 Manutenção da operação da AC Raiz da ICPEdu pelo período mínimo de 1 (um) ano após a notificação de sua extinção, salvo em casos de sucessão. Após este período, seu certificado deve ser revogado;

5.8.1.9 Armazenamento dos dados da AC Raiz da ICPEdu pelo período previsto nesta DPC.

CORPORATIVO: Documento para uso interno. A impressão deste documento torna a cópia não controlada

6 CONTROLES TÉCNICOS DE SEGURANÇA

6.1 GERAÇÃO E INSTALAÇÃO DE PARES DE CHAVES

6.1.1 Geração de pares de chaves

6.1.1.1 O par de chaves da ICPEdu é gerado pela própria AC da ICPEdu, em módulo criptográfico de *hardware* com padrão de segurança definido na SEG.P.005.

6.1.1.2 A geração do par de chaves da AC Raiz da ICPEdu é feita em processo verificável, obedecendo a procedimento formalizado, controlado e passível de auditoria, feito obrigatoriamente na presença de colaboradores de confiança designados pela DAGSer e treinados para a função.

6.1.1.3 O par de chaves da AC Raiz da ICPEdu é gerado em módulo criptográfico de ***hardware*** no padrão compatível com FIPS 140-2 Nível 3 e certificação INMETRO NSH-3/NSC3.

6.1.1.4 Os requisitos aplicáveis ao módulo criptográfico utilizado para armazenamento da chave privada da AC ICPEdu são baseados nos padrões mais atuais em vigência usados pelas Autoridades Certificadoras Raiz em operação no mercado.

6.1.1.5 O par de chaves criptográficas de uma AC de nível imediatamente subsequente ao da AC Raiz da ICPEdu é gerado pela própria AC.

6.1.1.6 As Políticas de Certificação implementadas pela AC Raiz da ICPEdu definem o meio utilizado para armazenamento da chave privada, baseada nos padrões mais atuais em vigência usados pelas Autoridades Certificadoras Raiz em operação no mercado.

6.1.2 Entrega pública para emissor de certificado

6.1.2.1 A AC de nível imediatamente subsequente ao da AC Raiz da ICPEdu entrega à DAGSer sua chave pública no arquivo de requisição em formato PKCS#10.

6.1.2.2 A DAGSer assina a requisição após verificar seu conteúdo e a encaminha de volta à AC requisitante.

6.1.3 Divulgação da chave pública da AC

CORPORATIVO: Documento para uso interno. A impressão deste documento torna a cópia não controlada

6.1.3.1 A divulgação do certificado da AC Raiz da ICPEdu para os usuários da ICPEdu é realizada:

a) no repositório da AC Raiz da ICPEdu;

b) no sítio da AC Raiz da ICPEdu ou das ACs integrantes da ICPEdu;

c) em outros meios seguros definidos pelo CA da ICPEdu.

6.1.3.2 A verificação de sua autenticidade pode ser feita por comparação do resumo criptográfico (***hash***) do certificado obtido acima com o hash publicado em documento oficial da RNP.

6.1.4 Tamanhos de chaves

6.1.4.1 As chaves criptográficas assimétricas da AC Raiz da ICPEdu e das ACs de nível imediatamente subsequente utilizam tamanho mínimo de 2048 bits RSA e, preferencialmente de 4096 bits RSA.

6.1.5 Geração dos parâmetros de chave pública e verificação de qualidade

6.1.5.1 Os parâmetros de geração de chaves assimétricas da AC Raiz da ICPEdu seguem as recomendações internacionais de qualidade de chaves assimétricas, baseados no padrão FIPS 140-2.

6.1.6 Propósitos de uso de chaves

6.1.6.1 É utilizada apenas para a assinatura do seu próprio certificado, dos certificados das ACs imediatamente subsequentes e de sua LCR.

6.2 PROTEÇÃO DA CHAVE PRIVADA E CONTROLE DE ENGENHARIA DO MÓDULO CRIPTOGRÁFICO

A AC Raiz utiliza um *hardware* criptográfico para gerar e armazenar seu par de chaves, emitir seu Certificado e os certificados das ACs de nível imediatamente subsequente ao seu e assinar suas LCRs. O *hardware* criptográfico possui um mecanismo de proteção contra violações lógicas e físicas. A chave privada é usada pelo operador de uma AC ou AR no SGCI após ser ativada pelo grupo de operadores do HSM. Ao término do uso, o grupo de operadores do HSM deve proceder a sua desativação. A DAGSer (RNP) é responsável pela decisão de destruição da chave privada da AC Raiz.

6.2.1 Padrões e controle para módulo criptográfico

6.2.1.1 A AC Raiz utiliza um *hardware* criptográfico conforme estabelecido na Seção 6.2.11.

6.2.2 Controle “n de m” para chave privada

6.2.2.1 A chave privada da AC Raiz da ICPEdu é liberada para uso por um número mínimo de 2 (dois) operadores de um total de 4 (quatro).

6.2.3 Custódia (*scrow*) de chave privada

6.2.3.1 A AC Raiz da ICPEdu não permite a custódia de sua chave privada.

CORPORATIVO:
Documento para uso interno. A impressão deste documento torna a cópia não controlada

6.2.4 Cópia de segurança de chave privada

6.2.4.1 A AC Raiz da ICPEdu mantém cópia de segurança de sua própria chave privada.

6.2.4.2 A cópia da chave privada é armazenada cifrada e com um nível de proteção não inferior àquele definido na cópia original da chave e mantido pelo menos pelo prazo de validade do certificado correspondente.

6.2.5 Arquivamento de chave privada

6.2.5.1 A chave privada da AC Raiz da ICPEdu é arquivada apenas internamente ao HSM e na forma de cópia de segurança.

6.2.6 Inserção de chave privada em módulo criptográfico

6.2.6.1 A única forma de exportação e importação da chave privada da AC Raiz da ICPEdu é através de uma cópia de segurança cifrada e que fica sob a responsabilidade do grupo de administradores da DAGSer.

6.2.6.2 A chave privada é mantida cifrada quando fora do módulo criptográfico.

6.2.7 Armazenamento de chave privada em módulo criptográfico

6.2.7.1 A chave privada é armazenada na forma cifrada na memória permanente do módulo criptográfico.

6.2.8 Método de ativação de chave primária

6.2.8.1 A chave privada da AC Raiz é ativada pelo grupo de operadores responsáveis pela chave. Esta identificação será sempre realizada por meio de senha e de dispositivos de controle de acesso em *hardware* (***token*** ou ***smartcard***).

6.2.9 Método de desativação de chave primária

6.2.9.1 Em casos de necessidade de desativação da chave privada da AC Raiz da ICPEdu, o grupo de operadores do HSM da AC Raiz da ICPEdu deve executar o comando de descarregar a chave por meio do sistema de gerenciamento do HSM.

6.2.9.2 A chave privada é automaticamente desativada quando o HSM é desligado.

6.2.10 Método de destruição da chave privada

6.2.10.1 A destruição da chave privada da AC Raiz da ICPEdu é realizada pela DAGSer, sobrescrevendo todo o conteúdo do HSM onde a chave privada está armazenada, disponível através do sistema de gerenciamento do HSM.

6.2.10.2 Todos os *tokens* dos perfis de operador, auditor e administrador do HSM devem ser fisicamente destruídos.

6.3 OUTROS ASPECTOS DO GERENCIAMENTO DO PAR DE CHAVES

6.3.1 Arquivamento de chave pública

CORPORATIVO: Documento para uso interno. A impressão deste documento torna a cópia não controlada

6.3.1.1 As chaves públicas da AC Raiz e das ACs de nível imediatamente subsequente ao seu são permanentemente armazenadas no formato PEM em mídia digital.

6.3.2 Períodos de operação do certificado e períodos de uso para as chaves pública e privada

6.3.2.1 As chaves privadas da AC Raiz da ICPEdu pela DPC e dos titulares de certificados de assinatura digital por ela emitidos são utilizadas apenas durante o período de validade dos certificados correspondentes. As correspondentes chaves públicas podem ser utilizadas durante todo o período de tempo determinado pela DAGSer para verificação de assinaturas geradas durante o prazo de validade dos respectivos certificados.

6.3.2.2 A chave privada da AC Raiz da ICPEdu é utilizada apenas durante o período de validade do certificado correspondente. As chaves públicas tanto da AC Raiz da ICPEdu quanto das ACs imediatamente subordinadas podem ser utilizadas por 15 (quinze) anos para verificação de assinaturas geradas durante o período de validade do certificado correspondente.

6.3.2.3 Cada PC/PDC implementada pela AC Raiz da ICPEdu define o período máximo de validade do certificado, baseada nos padrões mais atuais em vigência usados pelas Autoridades Certificadoras Raiz em operação no mercado.

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

6.4 DADOS DE ATIVAÇÃO

6.4.1 Geração e instalação dos dados de ativação

6.4.1.1 Os dados de ativação são gerados aleatoriamente e instalados em dispositivos de controle criptográficos, como *smartcards* ou *tokens*.

6.4.2 Proteção de dados de ativação

6.4.2.1 Os dados de ativação são protegidos contra o uso não autorizado por meio do uso de criptografia ou de controles de acesso físico.

6.5 CONTROLES DE SEGURANÇA COMPUTACIONAL

6.5.1 Requisitos técnicos

6.5.1.1 A geração do par de chaves da AC Raiz da ICPEdu é realizada off-line, de modo a impedir o acesso remoto não autorizado.

6.5.1.2 Cada computador servidor da AC Raiz da ICPEdu, relacionado diretamente com os processos de emissão, expedição, distribuição, revogação ou gerenciamento de certificados, implementa as seguintes características:

a) controle de acesso aos serviços e perfis da AC;
b) clara separação das tarefas e atribuições relacionadas a cada perfil qualificado da AC;
c) uso de criptografia para segurança de base de dados, quando exigido pela classificação de suas informações;

CORPORATIVO: Documento para uso interno. A impressão deste documento torna a cópia não controlada

d) geração e armazenamento de registros de auditoria da AC;
e) mecanismos internos de segurança para garantia da integridade de dados e processos críticos; e
f) mecanismos para cópias de segurança (backup).

6.5.1.3 Essas características são implementadas pela combinação de recursos do sistema operacional e do sistema de certificação com mecanismos de segurança física.

6.5.1.4 Os equipamentos enviados para manutenção passam por processo de sanitização das informações sensíveis nele contidas, controlados seu número de série e as datas de envio e de recebimento. Ao retornar às instalações da AC Raiz da ICPEdu, são realizados procedimentos de inspeção do equipamento que passou por manutenção. Em todo equipamento que deixar de ser utilizado em caráter permanente, são executados procedimentos de sanitização de todas as informações sensíveis relativas à atividade da AC de maneira definitiva. Todos esses eventos são registrados para fins de auditoria.

6.5.1.5 Qualquer equipamento incorporado à AC é preparado e configurado como previsto na SEG.P.005 ou em outro documento aplicável, de forma a apresentar o nível de segurança necessário à sua finalidade.

6.6 CONTROLES TÉCNICOS DO CICLO DE VIDA

6.6.1 Controles de desenvolvimento de sistemas

6.6.1.1 A AC Raiz da ICPEdu utiliza um sistema de gerenciamento de certificados digitais e um módulo criptográfico elaborados sob uma metodologia de desenvolvimento segura, fazendo uso de sistemas de controle de versões, notificação de erros e melhorias, definição de planos de requisitos, projeto, qualidade, configuração e testes.

6.6.1.2 Os processos de projeto e desenvolvimento conduzidos pela AC Raiz possuem documentação disponível para serem usados em avaliações externas de segurança dos componentes da AC.

6.6.2 Controles de gerenciamento de segurança

6.6.2.1 A DAGSer verifica se os requisitos apresentados na Seção 6.6.1 são atendidos.

6.6.2.2 A DAGser realiza o devido gerenciamento de configuração para a instalação e a contínua manutenção do sistema de certificação da AC.

6.7 CONTROLES DE SEGURANÇA DE REDE

6.7.1 Diretrizes gerais

6.7.1.1 A máquina hospedeira do SGCI da AC Raiz da ICPEdu opera off-line, fisicamente desconectada de qualquer rede.

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

CORPORATIVO: Documento para uso interno. A impressão deste documento torna a cópia não controlada

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

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

6.7.2 *Firewall*

6.7.2.1 O isolamento da rede na qual operam os ativos da AC Raiz é realizado por um *firewall*, segregando, em sub-redes específicas, os equipamentos servidores com acesso externo (DMZ), em relação aos equipamentos com acesso exclusivamente interno à AC.

6.7.2.2 O *firewall* realiza registros de auditoria.

6.7.3 Sistema de detecção de intrusão (IDS)

6.7.3.1 O sistema de detecção de intrusão tem a capacidade de reconhecer ataques em tempo real e notificá-los automaticamente.

6.7.3.2 O sistema de detecção de intrusão tem a 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.

6.7.4 Registro de acessos não autorizados à rede

6.7.4.1 As tentativas de acesso não autorizado são registradas em arquivos para posterior análise. As notificações seguem as diretrizes dispostas no SEG.N.010.

6.8 CARIMBO DE TEMPO

6.8.1 Data e hora

6.8.1.1 A data e a hora dos eventos e dados dos sistemas computacionais on-line que precisam ser datados são obtidas a partir de um relógio sincronizado pelo protocolo NTP a uma fonte de tempo confiável.

6.8.2 Atualização off-line

6.8.2.1 Os relógios dos sistemas computacionais off-line e do módulo criptográfico são atualizados manualmente sempre que inicializados.

CORPORATIVO:
Documento para uso interno. A impressão deste documento torna a cópia não controlada

7
PERFIS DE CERTIFICADO, LCR E OCSP

7.1 PERFIL DO CERTIFICADO

O formato de todos os certificados emitidos pela AC Raiz está em conformidade com a RFC 5280. O Certificado da AC Raiz é o único Certificado autoassinado da ICPEdu. As informações referentes ao Perfil dos Certificados podem ser encontradas no Apêndice A. Os certificados das ACs imediatamente subsequentes ao da AC Raiz são assinados pela AC Raiz e possuem validade limitada à validade do certificado da AC Raiz.

7.1.1 Número de versão

Todos os certificados emitidos pela AC deverão implementar a versão 3 (três) de certificado definida no padrão X.509, de acordo com o perfil estabelecido na RFC5280.

7.1.2 Extensões de certificado

As extensões são definidas na Seção A.2.2.

7.1.3 Identificadores de algoritmo

As informações referentes aos identificadores de objeto dos algoritmos podem ser encontradas na Tabela A.6 da Seção A.2.1

7.1.4 Formatos de nome

Os valores para o nome distinto da AC Raiz da ICPEdu podem ser encontrados na Tabela A.1 definida na Seção A.1. As regras de nome distinto da AC Raiz da ICPEdu podem ser encontradas na Tabela A.2 definida na Seção A.1.

7.1.5 Restrições de nome

A AC Raiz da ICPEdu estabelece as seguintes restrições para os nomes, aplicáveis a todos os certificados: não deverão ser utilizados sinais de acentuação, tremas ou cedilhas; e, além dos caracteres alfanuméricos, poderão ser utilizados somente os símbolos especiais listados na Tabela A.1.

7.1.6 OID (Object Identifier) da DPC

7.1.6.1 O OID da Política de certificado/Declaração de Práticas de Certificação (PC/DPC) da AC Raiz da ICPEdu é 1.3.6.1.4.1.15996.1.1.1.2.

7.1.7 Sintaxe e semântica dos qualificadores de política

7.1.7.1 O ponteiro para a DPC contém uma URL para um documento em formato PDF disponível via protocolo HTTP.

7.1.7.2 O qualificador “User Notice” contém o texto descrito na Seção A.2.2.

Versão: 2.0

CORPORATIVO: Documento para uso interno. A impressão deste documento torna a cópia não controlada

7.2 7.2 PERFIL DE LCR

O formato da LCR emitida pela AC Raiz está em conformidade com a RFC 5280, conforme é descrito na Tabela A.11 contida na Seção A.3.

7.2.1 Número(s) da versão

7.2.1.1 As LCRs geradas pela AC Raiz da ICPEdu deverão implementar a versão 2 do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 5280.

7.2.1.2 A LCR deve conter os seguintes campos:

a) Version: v2;
b) *Signature Algorithm*: Conforme definido em Tabela A.8 da Seção A.3;
c) *Issuer*: DN da AC;
d) *thisUpdate*: Data de emissão da LCR;
e) *nextUpdate*: Data da emissão da próxima LCR;
f) *revokedCertificates*: Número de série e data de revogação de todos os certificados revogados que ainda não expiraram.

7.2.2 Extensões de LCR e de suas entradas

7.2.2.1 As extensões para a LCR da AC Raiz da ICPEdu podem ser encontradas na Seção A.3.

7.3 PERFIL DE OCSP

A AC Raiz da ICPEdu não irá prover o serviço OCSP.

CORPORATIVO:
Documento para uso interno. A impressão deste documento torna a cópia não controlada

8
AUDITORIA DE CONFORMIDADE E OUTROS PADRÕES

As avaliações e auditorias realizadas no âmbito da ICPEdu têm por objetivo verificar se os processos, procedimentos e atividades das entidades integrantes da ICPEdu estão em conformidade com suas respectivas DPC, PC, PS e demais normas e procedimentos estabelecidos pela ICPEdu.

8.1 FREQUÊNCIA E CIRCUNSTÂNCIAS DAS AVALIAÇÕES

8.1.1 Frequência

8.1.1.1 A ICPEdu não realiza auditoria prévia nas entidades integrantes.

8.2 IDENTIFICAÇÃO/QUALIFICAÇÃO DO AVALIADOR

8.2.1 Identificação dos avaliadores

8.2.1.1 A DAGSer indica os auditores, internos e externos, respeitando critérios de qualificação, tais como proficiência em infraestruturas de chaves públicas, segurança de sistemas e da informação e experiência em processos de auditoria observado o disposto no documento “Critérios e Procedimentos para Realização de Auditorias nas Entidades Integrantes da ICPEdu”.

8.2.2 Avaliações

8.2.2.1 Com exceção da auditoria da própria AC Raiz da ICPEdu, que é de responsabilidade da DAGSer, as auditorias das entidades integrantes da ICPEdu são realizadas pela AC Raiz da ICPEdu, por meio de servidores de seu quadro próprio, ou por terceiros por ela autorizados, observado o disposto no documento “Critérios e Procedimentos para Realização de Auditorias nas Entidades Integrantes da ICPEdu”.

8.3 RELAÇÃO DO AVALIADOR COM A ENTIDADE AVALIADA

8.3.1 Avaliação da AC Raiz da ICPEdu

8.3.1.1 As auditorias da ICPEdu serão realizadas por avaliadores por meio de colaboradores do quadro da DAGSer ou por terceiros por ela autorizados.

8.3.2 Avaliação das ACs vinculadas

8.3.2.1 As auditorias da ICPEdu serão realizadas por avaliadores do seu quadro próprio ou por terceiros por ela autorizados.

Versão: 2.0

CORPORATIVO: Documento para uso interno. A impressão deste documento torna a cópia não controlada

8.4 TÓPICOS COBERTOS PELA AVALIAÇÃO

8.4.1 Verificação da conformidade da AC Raiz com esta PC/DPC e com as políticas e regras estabelecidas no contexto da ICPEdu. Aspectos como gerência das chaves e gerência do ciclo de vida do Certificado devem ser avaliados com especial cuidado.

8.4.2 Declaração de auditoria da AC-Raiz

8.4.2.1 A AC Raiz da ICPEdu documenta o escopo e frequência das auditorias realizadas conforme disposto no documento “Critérios e Procedimentos para Realização de Auditorias nas Entidades Integrantes da ICPEdu”.

8.4.3 Declaração de auditoria de AC vinculada

8.4.3.1 A AC subsequente da ICPEdu, para fins de credenciamento, documenta o escopo e frequência das auditorias realizadas conforme disposto no documento “Critérios e Procedimentos para Realização de Auditorias nas Entidades Integrantes da ICPEdu”.

8.5 AÇÕES TOMADAS COM RESULTADO DE UMA INEFICIÊNCIA

8.5.1 Notificações à DAGSer

8.5.1.1 Na ocorrência de qualquer deficiência, a DAGSer é notificada e analisa as devidas providências a serem tomadas junto às equipes responsáveis pelas ações corretivas.

8.6 COMUNICAÇÃO DOS RESULTADOS

8.6.1 Encaminhamento

8.6.1.1 Os relatórios resultantes das avaliações são encaminhados para a DAGSer.

CORPORATIVO:
Documento para uso interno. A impressão deste documento torna a cópia não controlada

9
OUTROS NEGÓCIOS E ASSUNTOS JURÍDICOS

9.1 TARIFAS

9.1.1 Tarifas de emissão e renovação de certificados

9.1.1.1 Não serão cobradas tarifas de emissão e renovação de certificados.

9.1.2 Tarifas de acesso ao certificado

9.1.3 Tarifas de revogação ou de acesso à informação de status

9.1.3.1 Não há tarifa de revogação ou de status de certificado.

9.1.4 Tarifas de outros serviços

9.1.4.1 Não há tarifas de outros serviços

9.2 RESPONSABILIDADE FINANCEIRA

A AC Raiz da ICPEdu não tem qualquer responsabilidade financeira.

9.3 CONFIDENCIALIDADE DA INFORMAÇÃO DO NEGÓCIO

9.3.1 Escopo de informações confidenciais:

9.3.1.1 Informações sobre solicitações de credenciamento de ACs aprovadas ou não;

9.3.1.2 Informações relativas a solicitações de certificados;

9.3.1.3 Registros de trilhas de auditoria;

9.3.1.4 Relatórios de auditorias;

9.3.1.5 Planos de contingência e planos de recuperação de desastres;

9.3.1.6 Medidas de segurança relativas:

a) à operação de *hardware* e software da ICPEdu; e
b) aos serviços de certificação.

Versão: 2.0

CORPORATIVO: Documento para uso interno. A impressão deste documento torna a cópia não controlada

9.3.2 Informações fora do escopo de informações confidenciais

9.3.2.1 São consideradas informações públicas:

a) certificados das ACs Raiz e vinculadas;
b) Listas de certificados revogados;
c) Versões publicadas de PCs, DPCs e Política de Segurança (PS);
d) A conclusão dos relatórios de auditoria;
e) Informações corporativas ou pessoais que fazem parte de certificados ou diretórios públicos.

9.3.3 Responsabilidade em proteger a informação confidencial

9.3.3.1 A AC Raiz se compromete a manter a confidencialidade das informações classificadas como confidenciais.

9.4 PRIVACIDADE DA INFORMAÇÃO PESSOAL

A AC Raiz não emite certificados para pessoas e, portanto, não se aplicam considerações sobre a privacidade de informações pessoais.

9.5 DIREITOS DE PROPRIEDADE INTELECTUAL

9.5.1 Critério de proteção

9.5.1.1 De acordo com a legislação vigente.

9.6 LIMITAÇÕES DE RESPONSABILIDADES

9.6.1 Danos

9.6.1.1 A AC Raiz não responde pelos danos que não lhe sejam imputáveis ou a que não tenha dado causa, na forma da legislação vigente.

9.7 INDENIZAÇÕES

9.7.1 Responsabilização

9.7.1.1 A AC responde pelos danos que der causa, e lhe sejam imputáveis, na forma da legislação vigente, assegurado o direito de regresso contra o agente ou entidade responsável.

9.8 PRAZO E RESCISÃO

9.8.1 Prazo

9.8.1.1 Esta DPC entra em vigor a partir da publicação que a aprovar, e permanecerá válida e eficaz até que venha a ser revogada ou substituída, expressa ou tacitamente.

9.8.2 Término

9.8.2.1 Esta DPC vigorará por prazo indeterminado, permanecendo válida e eficaz até que venha a ser revogada ou substituída, expressa ou tacitamente.

CORPORATIVO: Documento para uso interno. A impressão deste documento torna a cópia não controlada

9.8.3 Efeito da rescisão e sobrevivência

9.8.3.1 Os atos praticados na vigência desta DPC são válidos e eficazes para todos os fins de direito, produzindo efeitos mesmo após a sua revogação ou substituição.

9.9 AVISOS INDIVIDUAIS E COMUNICAÇÕES COM OS PARTICIPANTES

9.9.1 Meio de comunicação

9.9.1.1 As notificações, intimações, solicitações ou qualquer outra comunicação necessária sujeita às práticas descritas nesta DPC serão feitas, preferencialmente, por e-mail assinado digitalmente.

9.10 ALTERAÇÕES

9.10.1 Procedimentos para emendas

9.10.1.1 Qualquer alteração ou proposta de alteração nesta DPC deverá ser submetida para AC Raiz da ICPEdu.

9.11 SOLUÇÃO DE CONFLITOS

9.11.1 Instâncias

9.11.1.1 Casos omissos ou conflitantes são intermediados pela DAGSer.

9.12 LEI APLICÁVEL

9.12.1 Legislação

9.12.1.1 Esta DPC é regida pela Lei 14.063/2020, e a legislação que a substituir ou alterar, bem como pelas demais leis e normas aplicáveis em vigor no Brasil.

9.13 COM A LEI APLICÁVEL

9.13.1 Instâncias e cumprimento

9.13.1.1 A AC está sujeita à legislação que lhe é aplicável, comprometendo-se a cumprir e a observar as obrigações e direitos previstos em lei.

CORPORATIVO:
Documento para uso interno. A impressão deste documento torna a cópia não controlada

REFERÊNCIAS BIBLIOGRÁFICAS

ABNT. Associação Brasileira de Normas Técnicas. **NBR 11.515**: Critérios de segurança física relativos ao armazenamento de dados. Rio de Janeiro: ABNT, 2007.

ADAMS, C. et al. **RFC 4210**: Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP), september 2005. Disponível em: https://datatracker.ietf.org/doc/html/rfc4210 Acesso em: 08 jun. 2022.

BRASIL. **Resolução nº 07, de 12 de dezembro de 2001**. Aprova os requisitos mínimos para políticas de certificado na ICP-Brasil. Disponível em: https://www.gov.br/iti/pt-br/central-de-conteudo/doc-icp-04-versao-1-0-pdf#:~:text=RESOLU%C3%87%C3%83O%20N%C2%BA%207%2C%20DE%2012%20DE%20DEZEMBRO%20DE,DO%20COMIT%C3%8A%20GESTOR%20DA%20INFRA-ESTRUTURA%20DE%20CHAVES%20P%C3%9ABLICAS Acesso em: 11 jun. 2022.

BRASIL. **Resolução nº 177, de 20 de outubro de 2020**. Aprova a versão revisada e consolidada do documento Requisitos Mínimos para as Declarações de Práticas de Certificação das Autoridades Certificadoras da ICP-Brasil – DOC-ICP-05. Disponível em: https://www.gov.br/iti/ptbr/assuntos/legislacao/instrucoesnormativas/Resolucao177_DOCICP05_compilada.pdf Acesso em: 07 jun. 2022.

CHOKHANI, S. et al. **RFC 3647**: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, november 2003. Disponível em: https://datatracker.ietf.org/doc/html/rfc3647 Acesso em: 08 jun. 2022.

COMITÊ TÉCNICO DE POLÍTICAS DA ICPEDU. **Padrões e algoritmos criptográficos da ICPEDU**: relatório técnico. Rio de Janeiro: ICPEDU, 2006.

COOPER, D. et al. **RFC 5280**: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, may 2008. Disponível em: https://datatracker.ietf.org/doc/html/rfc5280 Acesso em: 08 jun. 2022.

DEACON, A.; HURST, R. **RFC 5019**: The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments, september 2007. Disponível em: https://datatracker.ietf.org/doc/html/rfc5019 Acesso em: 07 jun. 2022.

KAUSE, T.; PEYLO, M. **RFC 6712**: Internet X.509 Public Key Infrastructure - HTTP Transfer for the Certificate Management Protocol (CMP), september 2012. Disponível em: https://datatracker.ietf.org/doc/html/rfc6712 Acesso em: 08 jun. 2022.

SANTESSON, S. et al. **RFC 6960**: X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, june 2003.Disponível em: https://datatracker.ietf.org/doc/html/rfc6960 Acesso em: 08 jun. 2022.

CORPORATIVO:
Documento para uso interno. A impressão deste documento torna a cópia não controlada

APÊNDICE A

FORMATO DE DADOS

A.1 FORMATO DO DISTINGUISHED NAME

Não devem ser utilizados sinais de acentuação, tremas ou cedilhas; e, além dos caracteres alfanuméricos, poderão ser utilizados somente símbolos especiais listados na Tabela A.1.

Tabela A.1. – Símbolos admitidos em nomes.

Símbolo	Descrição	Código NBR9611 (hexadecimal)
	Espaço em branco	20
!	Ponto de exclamação	21
“	aspas	22
#	Cerquilha	23
$	Cifrão	24
%	Percentual	25
&	E comercial	26
‘	Apóstrofo	27
(	Abre parênteses	28
)	Fecha parênteses	29
*	Asterisco	2A
+	Mais	2B
,	Vírgula	2C
-	Menos	2D
.	Ponto	2E
/	Barra	2F
:	Dois pontos	3A
;	Ponto e vírgula	3B
=	Igual	3D
?	Ponto de interrogação	3F
@	Arroba	40
\	Barra invertida	5C

As tabelas A.2 e A.3 apresentam, respectivamente, o conteúdo dos campos dos certificados da AC Raiz da ICPEdu e dos usuários. Vale lembrar que não é admitida acentuação no campo *Distinguished Name*.

Versão: 2.0

CORPORATIVO: Documento para uso interno. A impressão deste documento torna a cópia não controlada

Tabela A.2. – Campos de nome dos certificados da AC Raiz da ICPEdu.

Campo	Conteúdo	Mandatório
C	BR	Sim
O	RNP	Sim
OU	ICPEdu	Sim
L	Florianópolis	Não
ST	SC	Não
CN	AC Pessoa	Sim

A.2 FORMATO DO CERTIFICADO

Não devem ser utilizados sinais de acentuação, tremas ou cedilhas; e, além dos caracteres alfanuméricos, poderão ser utilizados somente símbolos especiais listados na Tabela A.1.

A.2.1 Atributos básicos

Os atributos básicos dos certificados estão descritos nas Tabelas A.4 e A.5 e os Identificadores de objeto dos algoritmos na Tabela A.6.

Tabela A.3. – Tamanhos de chave da AC Raiz da ICPEdu.

Algoritmo	Tamanho
RSA	4096

Tabela A.4. – Campos do certificado AC Raiz da ICPEdu.

Campo	Conteúdo
Versão *(Version)*	3
Emissor *(Issuer)*	Conforme tabela A.2
Titular *(Subject)*	DN conforme tabela A.2
Período de Validade *(Validity)*	A data de validade é a data de emissão do certificado. A data final é 1 ano após a data inicial.
Chave pública *(Public Key)*	O algoritmo criptográfico e o tamanho da chave da AC Pessoa são definidos no documento "**Padrões e Algoritmos Criptográficos da ICPEdu**". [2]
Extensões	Os certificados contêm extensões apresentadas na Seção A.2.2.

CORPORATIVO: Documento para uso interno. A impressão deste documento torna a cópia não controlada

Tabela A.5. – Identificadores de objetos dos algoritmos utilizados para emitir certificados digitais.

Função	Nome	OID
Função hash	id-sha1	1.3.14.3.2.26
Ciframento	rsaEncryption	1.2.840.113549.1.1.1
Assinatura	Sha512WithRSAEncryption	2.16.840.1.101.3.4.2.3

A.2.2 Extensões

Os certificados contêm as extensões apresentadas nas tabelas A.9 e A.10.

Tabela A.6. – Extensões do certificado da AC Raiz da ICPEdu.

Extensão	Descrição	Crítica
SubjectKeyIdentifier	Hash da chave pública da AC Pessoa conforme definido no documento "**Padrões e Algoritmos Criptográficos da ICPEdu**".	Não
basicConstraints	Contém o campo CA=True e pathLenConstraint=0	Sim
CRLDistributionPoints	Contém o endereço na web onde se obtém a LCR emitida pela AC Raiz da ICPEdu.	Não
keyUsage	Contém apenas os bits keyCertSign(5) e CRLSign(6) ligados. Os demais bits estão desligados.	Sim
CertificatePolicies	Especifica o ObjectIdentifier (OID) da PC/DPC da AC Raiz da ICPEdu. O atributo id-qt-cps especifica a URL da PC/DPC e é representado no formato "https://repositorio.icpedu.rnp.br/acpessoa/pc-dpc-ac-raiz-AAAAMMDD.pdf", onde AAAAMMDD designa a data de emissão da PC/DPC vigente no dia da emissão do certificado. O atributo id-qt-unotice contém o texto: "Os certificados da ICPEdu são para uso exclusivo por instituições brasileiras de ensino e pesquisa e não têm eficácia jurídica."	Não
AuthorityKeyIdentifier	Contém o *hash* da chave pública da AC Raiz da ICPEdu.	Não

Tabela A.7. – Extensões do certificado emitido pela AC Raiz da ICPEdu.

Extensão	Descrição	Crítica
SubjectKeyIdentifier	*Hash* da chave pública do usuário final conforme definido no documento "**Padrões e Algoritmos Criptográficos da ICPEdu**".	Não
CRLDistributionPoints	Contém o endereço na web onde se obtém a LCR emitida pela AC Pessoa (https://repositorio.rnp.br/acpessoa/lcr/FILENAME.crl).	Não
keyUsage	Contém apenas os bits digitalSignature(0), nonRepudiation(1), dataEncipherment(3) ligados.	Sim
extkeyUsage	Contém o OID 1.3.6.1.5.5.7.3.2 (id-kp-clientAuth)	Sim

CORPORATIVO: Documento para uso interno. A impressão deste documento torna a cópia não controlada

Extensão	Descrição	Crítica
CertificatePolicies	Especifica o ObjectIdentifier (OID) da PC/DPC da AC Pessoa conforme especificado na Seção 1.2. O atributo id-qt-cps especifica a URL da PC/DPC e é representado no formato https://repositorio.icpedu.rnp.br/acpessoa/pc-dpc-acpessoa-AAAAMMDD.pdf, onde AAAAMMDD designa a data de emissão da PC/DPC vigente no dia da emissão do certificado. O atributo id-qt-unotice contém o texto: "Os certificados da ICPEdu são para uso exclusivo por instituições brasileiras de ensino e pesquisa e não têm eficácia jurídica."	Não
SubjectAltName	Permite que vários valores sejam associados com um certificado X.509. Estes valores são chamados *Subject Alternative Names*, estes incluem e-mail, endereço IP, *URI*, e outros, como, por exemplo, *General Name*.	Não
AuthorityKeyIdentifier	Contém o *hash* da chave pública da AC Pessoa.	Não

A.3 FORMATO DA LISTA DE CERTIFICADOS REVOGADOS

A LCR está de acordo com o padrão RFC 3280 [3] e possui os campos e as extensões definidos nas Tabelas A.11 e A.12.

Tabela A.8. – Campos da LCR da AC Raiz da ICPEdu.

Campo	Conteúdo
Versão (*Version*)	2
Emissor (*Issuer*)	DN conforme a Tabela A.2.
Atualização atual (*thisUpdate*)	Data da emissão da LCR.
Próxima atualização (*nextUpdate*)	Data da emissão da próxima LCR.
certificados revogados (*revokedCertificates*)	Número de série e data de revogação de todos os certificados revogados que ainda não expiraram.
Extensões	A LCR contém as extensões apresentadas na tabela A.12.

Tabela A.9. – Extensões da LCR.

Extensão	Descrição	Crítica
AuthorityKeyIdentifier	Contém o mesmo valor do campo *Subject Key Identifier* do certificado da AC Pessoa.	Sim
CRLNumber	Contém um número sequencial para cada LCR emitida.	Não

CORPORATIVO: Documento para uso interno. A impressão deste documento torna a cópia não controlada

RNP

ORGANIZACÃO SOCIAL DO MCTI

Educação, Pesquisa
e Inovação em Rede