RNP
ORGANIZAÇÃO SOCIAL DO MCTI

Educação, Pesquisa
e Inovação em Rede

ICPEdu
CERTIFICADO
PESSOAL

Declaração de práticas de certificação da AC pessoa 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

Declaração de práticas de certificação da AC pessoa 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)

D295	Declaração de práticas de certificação da AC pessoa ICPedu / Rede nacional de Ensino e Pesquisa. – Brasília, DF: Ibict, 2022. 58 p. ISBN 978-65-89167-51-8 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

Neste documento são descritas as práticas e os procedimentos empregados pelo Grupo de Operações da ICPEdu (GO-ICPEdu) na operação e suporte da Autoridade Certificadora de Certificado Pessoal da instituição. A estrutura desta Declaração de Práticas de Certificação está baseada na RFC 3647.

Código de barras: 978-65-89167-51-8
ISBN:

Apoio:



Realização:



Sumário

1 INTRODUÇÃO 11

1.1 VISÃO GERAL 11

1.1.1 Este documento descreve as práticas e os procedimentos empregados pelo Grupo de Operações da ICPEdu (GO-ICPEdu) na operação e suporte da Autoridade Certificadora de Certificado Pessoal do ICPEdu. Este grupo é composto por membros da RNP, Pontos de Presença (PoPs) e consultores indicados pela Diretoria Adjunta de Gestão de Serviços da RNP (DAGSer). 11

1.1.2 Para fins de estar aderente às boas práticas, esta DPC é baseada e adota a mesma estrutura empregada em documentos de Autoridades Certificadoras de referência no mercado. 11

1.1.3 A estrutura desta DPC está aseada na RFC 3647. 11

1.1.4 A GO-ICPEdu é responsável por manter todas as informações desta DPC sempre atualizadas. 11

1.1.5 Apesar deste documento não compor o conjunto normativo da ICP-Brasil, determinados regulamentos das demais normas da ITI podem ser referenciados se verificada a aplicabilidade. 12

1.2 NOME DO DOCUMENTO E IDENTIFICAÇÃO 12

1.2.1 Esta Declaração de Práticas de Certificação é referida a seguir simplesmente como “DPC ICPEdu AC PESSOA”. 12

1.2.2 A ICPEdu AC PESSOA é exclusiva e separada de acordo com os propósitos de uso de chaves de assinatura de documento, autenticação e proteção de e-mail (S/MIME). 12

1.3 PARTICIPANTES DA ICPEDU 12

1.3.1 Autoridades certificadoras 12

1.3.2 Autoridades de Registro 12

1.3.3 Titulares dos certificados 12

1.3.4 Partes confiáveis 12

1.4 USO DO CERTIFICADO 13

1.4.1 Uso proibido do certificado 13

1.5 DADOS DE CONTATO 13

1.5.1 Organização administrativa do documento 13

1.5.2 Contatos 13

1.5.3 Responsável pela adequabilidade da DPC com a PC 13

1.5.4 Procedimento de aprovação da DPC 13

1.6 DEFINIÇÕES E ACRÔNIMOS 13

2 RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO 16

2.1 REPOSITÓRIOS 16

2.1.1 A ICPEdu mantém disponível repositório atendendo os seguintes requisitos: 16

2.1.2 O repositório da AC PESSOA atende aos requisitos: 16

2.1.3 O repositório da AC PESSOA está disponível para consulta de acordo com o definido no item 2.1.1. 16

2.2 PUBLICAÇÃO DE INFORMAÇÕES 16

2.2.1 A AC PESSOA publica e disponibiliza as LCRs na página de repositório, descrito no item. 16

2.2.2 Estão publicados no repositório da AC PESSOA: 16

2.3 FREQUÊNCIA DAS PUBLICAÇÕES 16

2.3.1 O repositório é atualizado no prazo máximo de 1 (um) dia útil, sempre que houver mudança nas informações listadas na Seção 2.2. 16

2.4 CONTROLES DE ACESSO AOS REPOSITÓRIOS 17

2.4.1 Todas as informações citadas na Seção 2.2 podem ser publicamente acessadas para leitura. ... 17

2.4.2 São utilizados controles de acesso apropriados para restringir e controlar a escrita nos locais de armazenamento e publicação, o que é permitido apenas à equipe responsável designada para esse fim. Os controles de acesso incluem identificação pessoal para acesso aos equipamentos, utilização de credenciais de acesso e de protocolos seguros de comunicação de dados. ... 17

3 IDENTIFICAÇÃO E AUTENTICAÇÃO E REPOSITÓRIO ... 18

3.1 ESTRUTURA DE NOMES ... 18

3.1.1 Tipos de nomes ... 18

3.1.2 Necessidade de que nomes sejam significativos ... 18

3.1.3 Anonimato dos titulares de certificado ... 18

3.1.4 Regras para interpretação de diversos formatos de nomes ... 18

3.1.5 Unicidade de nomes ... 18

3.1.6 Procedimento para resolver disputa de nomes ... 18

3.2 VALIDAÇÃO DA IDENTIDADE INICIAL ... 18

3.2.1 Método para comprovar o controle da chave privada ... 18

3.2.2 Autenticação da Identidade Organizacional ... 18

3.2.3 Autenticação da identidade individual ... 19

3.2.4 Informações não verificadas do titular do certificado ... 19

3.2.5 Validação da autoridade certificadora ... 19

3.3 IDENTIFICAÇÃO E AUTENTICAÇÃO PARA PEDIDOS DE NOVAS CHAVES ... 20

3.4 IDENTIFICAÇÃO E AUTENTICAÇÃO PARA SOLICITAÇÃO DE REVOGAÇÃO ... 20

4 REQUISITOS OPERACIONAIS DO CICLO DE VIDA DO CERTIFICADO . 21

4.1 SOLICITAÇÃO DO CERTIFICADO ... 21

4.1.1 Quem pode submeter uma solicitação de certificado ... 21

4.1.2 Processo de registro e responsabilidades ... 21

4.2 EMISSÃO DO CERTIFICADO ... 22

4.2.1 Ações da AC durante a emissão de certificado ... 22

4.2.2 Notificação para o titular na emissão do certificado ... 22

4.3 ACEITAÇÃO DO CERTIFICADO ... 22

4.3.1 Conduta sobre a aceitação do certificado ... 22

4.3.2 Publicação do certificado pela AC ... 22

4.4 USABILIDADE DO PAR DE CHAVES E DO CERTIFICADO ... 22

4.4.1 Usabilidade da chave privada e do certificado do titular ... 22

4.4.2 Usabilidade da chave pública e do certificado das partes confiáveis ... 23

4.5 REEMISSÃO DE CERTIFICADOS POR TROCA DO PRAZO DE VALIDADE ... 23

4.6 NOVA CHAVE DE CERTIFICADO (RE-KEY) ... 23

4.7 MODIFICAÇÃO DE CERTIFICADO POR TROCA DE DADOS ... 23

4.8 SUSPENSÃO E REVOGAÇÃO DE CERTIFICADO ... 23

4.8.1 Circunstâncias para revogação ... 23

4.8.2 Quem pode solicitar a revogação ... 24

4.8.3 Procedimento para solicitação de revogação ... 24

4.8.4 Prazo para solicitação de revogação ... 24

4.8.5 Tempo em que a AC deve processar o pedido de revogação ... 24

4.8.6 Requisitos de verificação de revogação para as partes confiáveis ... 24

4.8.7 Frequência de emissão de LCR 25
4.8.8 Latência máxima para a LCR 25
4.8.9 Procedimentos adicionais no caso de comprometimento da chave privada 25
4.9 SERVIÇO DE STATUS DE CERTIFICADO 25
4.9.1 Características operacionais 25
4.9.2 A AC PESSOA ICPEdu não disponibiliza outros serviços de status de certificados além da publicação de LCRs no repositório, como definido na Seção 2.1. 25
4.10 ENCERRAMENTO DE ATIVIDADES 25
4.10.1 O vínculo com a AC PESSOA ICPEdu é encerrado pela expiração de um certificado ou por solicitação de revogação, conforme definido na Seção 4.9.3. 25
4.11 CUSTÓDIA E RECUPERAÇÃO DE CHAVE 25
5 CONTROLES OPERACIONAIS, GERENCIAMENTO E DE INSTALAÇÕES 26
5.1 CONTROLES FÍSICOS 26
5.1.1 Construções e localização das instalações da AC 26
5.1.2 Acesso físico 26
5.1.3 Energia e ar-condicionado 28
5.1.4 Exposição a água 29
5.1.5 Prevenção e proteção contra incêndio 29
5.1.6 Armazenamento de mídia 29
5.1.7 Descarte de lixo 29
5.1.8 Instalações de segurança (backup) externas (off-site) para AC 29
5.2 CONTROLES PROCEDIMENTAIS 29
5.2.1 Perfis qualificados 29
5.2.2 Número de pessoas necessárias por tarefa 31
5.2.3 Identificação e autenticação para cada papel 31
5.2.4 Funções que requerem separação de deveres 31
5.3 CONTROLES DE PESSOAL 31
5.3.1 Antecedentes, qualificação, experiência e requisitos de idoneidade 31
5.3.2 Procedimentos de verificação de antecedentes 32
5.3.3 Requisitos de treinamento 32
5.3.4 Frequência e requisitos para reciclagem técnica 32
5.3.5 Sanções para ações não autorizadas 32
5.3.6 Requisitos para prestadores de serviço independentes 32
5.3.7 Documentação fornecida aos funcionários 32
5.4 PROCEDIMENTOS DE LOG DE AUDITORIA 33
5.4.1 Tipos de eventos registrados 33
5.4.2 Frequência de auditoria de registros 34
5.4.3 Período de retenção para registros de auditoria 34
5.4.4 Proteção de registros de auditoria 34
5.4.5 Procedimentos para cópia de segurança de registros de auditoria 34
5.4.6 Sistema de coleta de dados de auditoria (interno ou externo) 35
5.4.7 Avaliações de vulnerabilidades 35
5.5 ARQUIVAMENTO DE REGISTROS 35
5.5.1 Tipos de registros arquivados 35
5.5.2 Período de retenção para arquivo 35
5.5.3 Proteção dos registros 35
5.5.4 Procedimentos de cópias de arquivo 36
5.5.5 Requisitos para datação dos registros 36
5.5.6 Sistema de recolhimento de registros (interno ou externo) 36
5.5.7 Procedimentos para obtenção e verificação dos registros armazenados 36
5.6 TROCA DE CHAVE 36
5.6.1 Prazos específicos 36

5.7 COMPROMETIMENTO E RECUPERAÇÃO DE DESASTRE 36

5.7.1 Procedimentos gerenciamento de incidentes e comprometimento 36

5.7.2 Recursos computacionais, *software*, e/ou dados corrompidos 36

5.7.3 Procedimentos para comprometimento de chave privada de entidade 37

5.7.4 Capacidade para continuidade de negócios após desastre 37

5.8 EXTINÇÃO DA AC 37

5.8.1 São adotadas as seguintes providências mínimas em caso de extinção da AC pessoa ICPEDU: 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 Divulgação da chave pública da AC às partes confiantes 38

6.1.3 Tamanhos de chaves 39

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

6.1.5 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 (*escrow*) de chave privada 39

6.2.4 Cópia de segurança de chave privada 39

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 41

6.3.1 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 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 gerenciamento de segurança 42

6.7 CONTROLES DE SEGURANÇA DE REDE 42

6.7.1 Diretrizes gerais 42

6.7.2 Firewall 42

6.7.3 Sistema de Detecção de Intrusão (IDS) 42

6.7.4 Registro de acessos não autorizados à rede 43

6.7.5 Carimbo de tempo 43

6.7.6 Data e hora 43

6.7.7 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 PERFIL DE LCR 44

7.2.1 Número(s) da versão 44

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

8.3 RELAÇÃO DO AVALIADOR COM A ENTIDADE AVALIADA 46

8.4 TÓPICOS COBERTOS PELA AVALIAÇÃO 46

8.4.1 Objetivos 46

8.5 AÇÕES TOMADAS COM RESULTADO DE UMA INEFICIÊNCIA 46

8.5.1 Notificações à DAGSER 46

8.6 COMUNICAÇÃO DOS RESULTADOS 46

9 OUTROS NEGÓCIOS E ASSUNTOS JURÍDICOS 47

9.1 TARIFAS 47

9.1.1 Tarifas de emissão e renovação de certificados 47

9.2 RESPONSABILIDADE FINANCEIRA 47

9.3 CONFIDENCIALIDADE DA INFORMAÇÃO DO NEGÓCIO 47

9.3.1 Escopo de informações confidenciais: 47

9.3.2 Informações fora do escopo de informações confidenciais 47

9.3.3 Responsabilidade em proteger a informação confidencial 47

9.4 PRIVACIDADE DA INFORMAÇÃO PESSOAL 48

9.4.1 Plano de privacidade 48

9.4.2 Informação tratada como privada 48

9.4.3 Informação não considerada privada 48

9.4.4 Responsabilidade de proteção de informação considerada privada 48

9.4.5 Aviso e consentimento para uso de informação privada 48

9.4.6 Divulgação em processos judiciais e administrativos 48

9.5 PRAZO E RESCISÃO 48

9.5.1 Prazo 48

9.5.2 Término 48

9.5.3 Efeito da rescisão e sobrevivência 49

9.6 AVISOS INDIVIDUAIS E COMUNICAÇÕES COM OS PARTICIPANTES 49

9.6.1 Meio de comunicação 49

9.7 ALTERAÇÕES 49

9.7.1 Procedimentos para emendas 49

9.7.2 Mecanismo de notificação e períodos 49

9.7.3 Circunstâncias na qual o OID deve ser alterado 49

9.8 SOLUÇÃO DE CONFLITOS 49

9.8.1 Instâncias 49

9.9 LEI APLICÁVEL 49

9.9.1 Legislação 49

9.10 CONFORMIDADE COM A LEI APLICÁVEL 49

9.11 DISPOSIÇÕES DIVERSAS 50

9.11.1 Acordo completo 50

REFERÊNCIAS BIBLIOGRÁFICAS 51

APÊNDICE A 53

1 INTRODUÇÃO

Este documento constitui a Declaração de Práticas de Certificação (DPC) da ICPEdu AC PESSOA, Autoridade Certificadora de Certificado Pessoal da Infraestrutura de Chaves Públicas para Pesquisa e Ensino.

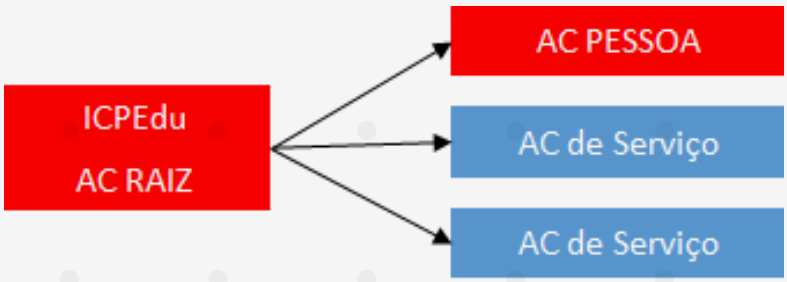
Este é um serviço provido pela RNP – Rede Nacional de Ensino e Pesquisa, que emite certificados digitais para pessoas através de autenticação federada, com fins de cifragem de documentos, autenticação em sistemas eletrônicos, assinaturas eletrônicas e validação de variados procedimentos digitais, em um escopo específico no âmbito das organizações de ensino e pesquisa no Brasil. Por não ser uma autoridade certificadora credenciada na ICPBrasil, a ICPEdu AC PESSOA não garante presunção de validade jurídica aos demais atos e negócios eletrônicos de ordem geral assinados e cifrados com certificados digitais e chaves emitidos.

1.1 VISÃO GERAL

1.1.1 Este documento descreve as práticas e os procedimentos empregados pelo Grupo de Operações da ICPEdu (GO-ICPEdu) na operação e suporte da Autoridade Certificadora de Certificado Pessoal do ICPEdu. Este grupo é composto por membros da RNP, Pontos de Presença (PoPs) e consultores indicados pela Diretoria Adjunta de Gestão de Serviços da RNP (DAGSer).

Por estar inserida na infraestrutura da ICPEdu, a AC PESSOA ICPEdu é considerada uma AC Intermediária de serviço, conforme demonstrado na Figura 1.1.

Figura 1.1 – Topologia do Serviço ICPEdu AC PESSOA ICPEdu.



1.1.2 Para fins de estar aderente às boas práticas, esta DPC é baseada e adota a mesma estrutura empregada em documentos de Autoridades Certificadoras de referência no mercado.

1.1.3 A estrutura desta DPC está baseada na RFC 3647.

1.1.4 A GO-ICPEdu é responsável por manter todas as informações desta DPC sempre atualizadas.

Versão: 2.0

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

1.1.5 Apesar deste documento não compor o conjunto normativo da ICP-Brasil, determinados regulamentos das demais normas da ITI podem ser referenciados se verificada a aplicabilidade.

1.2 NOME DO DOCUMENTO E IDENTIFICAÇÃO

1.2.1 Esta Declaração de Práticas de Certificação é referida a seguir simplesmente como "DPC ICPEdu AC PESSOA".

O *Object Identifier* desta DPC é 1.3.6.1.4.1.15996.1.1.5, onde:

- 1.3.6.1.4.1 - Prefixo para *private enterprises* (IANA);
- 15996 - Prefixo RNP;
- 1 - ICPEdu;
- 1 - PC/DPC;
- 5 - Versão do documento.

1.2.2 A ICPEdu AC PESSOA é exclusiva e separada de acordo com os propósitos de uso de chaves de assinatura de documento, autenticação e proteção de e-mail (S/MIME).

1.3 PARTICIPANTES DA ICPEDU

1.3.1 Autoridades certificadoras

Esta PC/DPC é chamada "Política de Certificado e Declaração de Práticas de Certificação da Autoridade Certificadora Raiz da ICPEdu" e comumente referida como "PC/DPC da AC PESSOA ICPEdu".

O *Object Identifier* - OID desta PC/DPC é 1.3.6.1.4.1.15996.1.1.1.2.

1.3.2 Autoridades de Registro

Não há Autoridades de Registro atreladas à AC PESSOA. As funções de registro e identificação das pessoas é feita pela Instituição de Ensino e Pesquisa que adere ao serviço.

Para a emissão de certificados, a verificação da identidade do solicitante do certificado é descrita na Seção 3.2.3.

1.3.3 Titulares dos certificados

São habilitados a emitir certificados digitais ICPEdu os usuários devidamente cadastrados em instituições que aderem ao serviço, através da Comunidade Acadêmica Federada (CAFe).

1.3.4 Partes confiáveis

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

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

1.4 USO DO CERTIFICADO

1.4.1 Uso apropriado do certificado

Os certificados digitais emitidos pela AC PESSOA podem ser utilizados apenas para:

i. Assinatura;
ii. Cifragem;
iii. Autenticação.

As aplicações são definidas segundo as extensões keyUsage e extkeyUsage mencionadas na Tabela A.8, localizado no Anexo A.

1.4.1 Uso proibido do certificado

Todas não citadas no item 1.4.1.

1.5 DADOS DE CONTATO

1.5.1 Organização administrativa do documento

Esta PC/DPC da AC PESSOA ICPEdu é produzida pela DAGSer/RNP.

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 Comitê Assessor de Gestão de Identidade (CA-GId).

1.6 DEFINIÇÕES E ACRÔNIMOS

Sigla	Descrição
AC	Autoridade Certificadora
AC PESSOA ICPEdu	Autoridade Certificadora Raiz da ICPEdu
Administrador do SGCI	Grupo responsável pela administração do SGCI
AES	*Advanced Encryption Algorithm* (Algoritmo de Cifragem Avançada)

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

Sigla	Descrição
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
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

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

Sigla	Descrição
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)
SSL	*Secure Sockets Layer* (Camada de Soquete Seguro)
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 RESPONSABILIDADES DE PUBLICAÇÃO E REPOSITÓRIO

2.1 REPOSITÓRIOS

2.1.1 A ICPEdu mantém disponível repositório atendendo os seguintes requisitos:

a) Disponibilizar a lista de certificados revogados;
b) Estar disponível para consulta em tempo integral;
c) Implementar todos os recursos necessários para a segurança dos dados armazenados.

2.1.2 O repositório da AC PESSOA atende aos requisitos:

a) Endereço: https://repositorio.icpedu.rnp.br
b) Disponibilidade: definida no item 2.1.1.
c) Protocolo de acesso: HTTPS.
d) Os controles de segurança são definidos no item 5 desta DPC.

2.1.3 O repositório da AC PESSOA está disponível para consulta de acordo com o definido no item 2.1.1.

2.2 PUBLICAÇÃO DE INFORMAÇÕES

2.2.1 A AC PESSOA publica e disponibiliza as LCRs na página de repositório, descrito no item.

2.2.2 Estão publicados no repositório da AC PESSOA:

a) Certificado da AC PESSOA ICPEdu;
b) Lista de Certificados Revogados (LCR);
c) A DC/DPC da AC PESSOA;
d) Dados para contato.

2.3 FREQUÊNCIA DAS PUBLICAÇÕES

2.3.1 O repositório é atualizado no prazo máximo de 1 (um) dia útil, sempre que houver mudança nas informações listadas na Seção 2.2.

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

2.4 CONTROLES DE ACESSO AOS REPOSITÓRIOS

2.4.1 Todas as informações citadas na Seção 2.2 podem ser publicamente acessadas para leitura.

2.4.2 São utilizados controles de acesso apropriados para restringir e controlar a escrita nos locais de armazenamento e publicação, o que é permitido apenas à equipe responsável designada para esse fim. Os controles de acesso incluem identificação pessoal para acesso aos equipamentos, utilização de credenciais de acesso e de protocolos seguros de comunicação de dados.

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

3 IDENTIFICAÇÃO E AUTENTICAÇÃO E REPOSITÓRIO

3.1 ESTRUTURA DE NOMES

3.1.1 Tipos de nomes

Os tipos de nomes seguem o padrão X.500.

3.1.2 Necessidade de que nomes sejam significativos

Os certificados emitidos pela AC PESSOA ICPEdu exigem o uso de nomes significativos que possibilitem determinar de forma unívoca a identidade do seu titular, conforme definido na Seção A.1.

3.1.3 Anonimato dos titulares de certificado

A AC PESSOA ICPEdu não dá suporte ao anonimato dos titulares de certificados.

3.1.4 Regras para interpretação de diversos formatos de nomes

Os nomes devem ser interpretados conforme estabelecido nas Seções 3.1.1 e 3.1.2.

3.1.5 Unicidade de nomes

Os nomes de um certificado são únicos no conjunto de certificados vigentes emitidos pela AC PESSOA ICPEdu. Para assegurar a unicidade do campo "*Distinguished Name*" (DN) é incluído o número do CPF após o nome do titular do certificado, conforme definido na Seção A.1.

3.1.6 Procedimento para resolver disputa de nomes

Não há disputa decorrente da igualdade de nomes entre os solicitantes de certificados no âmbito da AC PESSOA ICPEdu, pois a definição da Seção 3.1.5 garante a unicidade do nome do titular do certificado.

3.2 VALIDAÇÃO DA IDENTIDADE INICIAL

A AC PESSOA ICPEdu delega à Instituição cliente do serviço a realização da identificação dos solicitantes e validação dos seus respectivos documentos de identificação, de acordo com seus procedimentos internos.

3.2.1 Método para comprovar o controle da chave privada

É garantida a posse da chave privada ao se verificar a assinatura do arquivo de requisição nos formatos PKCS#10.

3.2.2 Autenticação da Identidade Organizacional

A identidade organizacional é feita através de um ticket Shibboleth emitidos e assinados pelo IdP de origem devidamente autorizado pela Comunidade Acadêmica Federada - CAFe.

Versão: 2.0

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

3.2.3 Autenticação da identidade individual

3.2.3.1 O processo a seguir, exemplificado na Figura 3.1, é definido para validar a identidade individual do solicitante do certificado:

3.2.3.1.1 Solicitante navega até o sítio https://pessoal.icpedu.rnp.br;

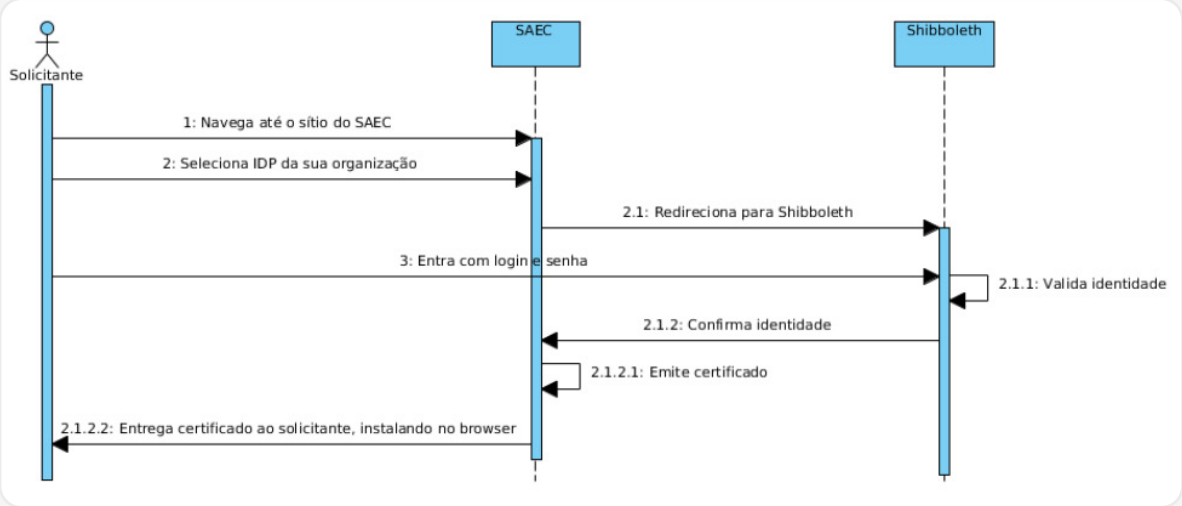
3.2.3.1.2 Seleciona a opção “Emitir Certificado Pessoal”;

3.2.3.1.3 Seleciona o IdP da Instituição a qual está vinculado;

3.2.3.1.4 Entra com as credenciais de acesso (usuário e senha) no IdP.

3.2.3.2 Caso a identidade do usuário seja confirmada junto ao IdP, o usuário estará autenticado pela CAFe e terá sua identidade validada.

Figura 3.1 – Processo de validação de identidade individual.



3.2.3.3 As seguintes informações estão contidas no certificado emitido para um titular:

a) Identificação do IdP (Organização);
b) Nome Completo;
c) E-mail;
d) Cadastro de Pessoa Física (CPF);
e) Data de nascimento;
f) eduPersonPrincipalName (eppn).

3.2.4 Informações não verificadas do titular do certificado

Todas as informações descritas no item 3.2.4.

3.2.5 Validação da autoridade certificadora

A autoridade do solicitante é validada no momento em que o processo de autenticação definido na Seção 3.2.3 é realizado com êxito.

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

3.3 IDENTIFICAÇÃO E AUTENTICAÇÃO PARA PEDIDOS DE NOVAS CHAVES

A substituição de uma chave antes da sua expiração ou após a sua revogação é tratada como uma solicitação de um novo certificado. O solicitante deve seguir os procedimentos definidos na Seção 3.2.

3.4 IDENTIFICAÇÃO E AUTENTICAÇÃO PARA SOLICITAÇÃO DE REVOGAÇÃO

O solicitante da revogação do certificado deve ser identificado e as solicitações de revogação devem ser registradas. A confirmação do titular é feita através do protocolo de desafio-resposta, descrito no item 3.2.3.

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

4
REQUISITOS OPERACIONAIS DO CICLO DE VIDA DO CERTIFICADO

4.1 SOLICITAÇÃO DO CERTIFICADO

4.1.1 Quem pode submeter uma solicitação de certificado

Podem solicitar certificado os usuários que possuem conta de acesso no IdP das respectivas Instituições clientes do Sistema RNP que realizaram a adesão ao serviço "ICPEdu – Certificado Pessoal".

4.1.2 Processo de registro e responsabilidades

Ao efetuar o último passo do processo definido na Seção 3.2.3, o solicitante é encaminhado à interface da plataforma web da AC PESSOA ICPEdu, onde é feita a submissão de requisição de certificado.

Neste passo, o navegador processa a criação do par de chaves e faz a submissão da requisição de certificado em formato PKCS#10 à AC PESSOA ICPEdu.

4.1.2.1 Responsabilidades da AC

4.1.2.1.1 A AC PESSOA ICPEdu é responsável pelos danos a que der causa.

4.1.2.2 Obrigações da AC

4.1.2.2.1 As obrigações da AC PESSOA ICPEdu são as abaixo relacionadas:

a) Operar de acordo com esta PC/DPC;
b) A geração e o gerenciamento dos seus pares de chaves criptográficas;
c) Assegurar a proteção de suas chaves privadas;
d) Revogar imediatamente o certificado da AC PESSOA ICPEdu quando houver suspeita ou comprovação de comprometimento de sua chave privada;
e) Notificar as partes interessadas quando ocorrer a suspeita ou comprovação de comprometimento de sua chave, emissão de novo par de chaves e correspondente certificado ou o encerramento de suas atividades;
f) Distribuir o seu próprio certificado;
g) Informar a emissão do certificado ao respectivo solicitante;
h) Revogar os certificados por ela emitidos;
i) Emitir, gerenciar e publicar suas Listas de Certificados Revogados (LCRs) e disponibilizar consulta on-line de situação de certificado (OCSP – *Online Certificate Status Protocol*);
j) Publicar, no repositório em sua página web, a DPC e PCs aprovadas que implementa;
k) Publicar, no repositório em sua página web, as informações definidas na Seção 2.2.2 deste documento;

Versão: 2.0

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

l) Utilizar protocolo de comunicação seguro ao disponibilizar serviços para os solicitantes ou usuários de certificados digitais via web;

m) Adotar medidas de segurança e controle previstas na DPC e Política de Segurança que implementar, envolvendo seus processos, procedimentos e atividades, baseando-se nas normas, critérios e procedimentos definidos pela ICP-Brasil;

n) Manter a conformidade dos seus processos, procedimentos e atividades com a legislação vigente e baseando-se nas normas, práticas, e regras da ICP-Brasil;

o) Manter e garantir a integridade, sigilo e a segurança da informação por ela tratada;

p) Manter e testar regularmente seu Plano de Continuidade do Negócio;

q) Informar aos titulares de certificado acerca das garantias, coberturas condicionantes e limitações determinadas pela legislação vigente, quando aplicável;

r) Manter o registro da quantidade de certificados digitais emitidos mensalmente;

s) Não emitir certificados com validade que se estenda além da validade de seu próprio certificado;

t) Realizar auditorias pré-operacionais e, anualmente, auditorias operacionais do serviço.

4.2 EMISSÃO DO CERTIFICADO

4.2.1 Ações da AC durante a emissão de certificado

4.2.1.1 A AC PESSOA ICPEdu processa as solicitações de certificados no momento da sua requisição.

4.2.1.1.1 Caso exista um certificado previamente emitido e válido relacionado à requisição, ele é revogado antes da emissão de um novo certificado.

4.2.1.1.2 A verificação é feita utilizando o e-mail como base.

4.2.2 Notificação para o titular na emissão do certificado

4.2.2.1 A notificação da emissão é feita pela interface com o titular, no sítio da plataforma web da AC PESSOA ICPEdu, no ato da emissão. Nenhum outro tipo de notificação é feito.

4.3 ACEITAÇÃO DO CERTIFICADO

4.3.1 Conduta sobre a aceitação do certificado

4.3.1.1 Considera-se que todo certificado digital emitido pela AC PESSOA ICPEdu através da plataforma web é aceito pelo titular do certificado.

4.3.1.2 Caso o titular, por algum motivo, não aceite o certificado emitido, cabe a este, a qualquer momento, solicitar a revogação diretamente à AC PESSOA ICPEdu, conforme definido na Seção 4.9.3.

4.3.2 Publicação do certificado pela AC

4.3.2.1 Os certificados emitidos pela AC PESSOA ICPEdu não são publicados.

4.4 USABILIDADE DO PAR DE CHAVES E DO CERTIFICADO

4.4.1 Usabilidade da chave privada e do certificado do titular

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

4.4.1.1 É de responsabilidade dos titulares dos certificados:

a) A proteção da chave privada associada ao certificado emitido pela AC PESSOA ICPEdu;
b) Obedecer às restrições de uso da chave privada e do certificado definidos na Seção 1.4.1;
c) Solicitar imediatamente a revogação do certificado caso ocorra comprometimento da chave privada correspondente.

4.4.2 Usabilidade da chave pública e do certificado das partes confiáveis

a) É de responsabilidade das partes confiáveis:
b) Ter ciência das definições desta DPC;
c) Verificar as LCRs antes de aceitar um certificado como sendo válido;
d) Observar as restrições de uso da chave privada e do certificado.

4.5 REEMISSÃO DE CERTIFICADOS POR TROCA DO PRAZO DE VALIDADE

A AC PESSOA ICPEdu não renova certificados. Caso o titular necessite de outro certificado após expirar a validade do atual, ele deve realizar a requisição de um novo certificado, seguindo o procedimento definido na Seção 4.1.2.

4.6 NOVA CHAVE DE CERTIFICADO (RE-KEY)

A AC PESSOA ICPEDu não reemite certificados por motivos de troca de chaves. Caso o titular necessite de outro certificado, ele deve realizar a requisição de um novo certificado, seguindo o procedimento definido na Seção 4.1.2.

4.7 MODIFICAÇÃO DE CERTIFICADO POR TROCA DE DADOS

A AC PESSOA ICPEDu não reemite certificados por motivos de troca de dados. Caso o titular necessite de outro certificado, ele deve realizar a requisição de um novo certificado, seguindo o procedimento definido na Seção 4.1.2.

4.8 SUSPENSÃO E REVOGAÇÃO DE CERTIFICADO

4.8.1 Circunstâncias para revogação

4.8.1.1 Um certificado emitido pela AC PESSOA ICPEdu pode ser revogado a qualquer instante pelo próprio titular.

4.8.1.2 Um certificado deve ser obrigatoriamente revogado:

a) Quando for constatada a emissão imprópria ou defeituosa;
b) Quando for necessária a alteração de qualquer informação constante no certificado;
c) Quando do comprometimento da chave privada da AC PESSOA ICPEdu ou da sua mídia armazenadora;
d) Quando este ainda for válido e for solicitado um novo certificado para a mesma conta.

4.8.1.3 Todo certificado deverá ter sua validade verificada na respectiva LCR ou OCSP antes de ser utilizado.

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

4.8.2 Quem pode solicitar a revogação

4.8.2.1 A revogação de um certificado somente poderá ser feita:

a) Por solicitação do titular do certificado;
b) Por solicitação do gestor de identidade da instituição cliente do serviço ICPEdu;
c) Por solicitação do gestor da RNP responsável pelo serviço ICPEdu;
d) Por solicitação do Grupo de Operação do ICPEdu.

4.8.2.2 Caso a solicitação seja feita pela RNP ou pela GO-ICPEdu, a revogação deve ser procedida imediatamente e comunicada ao gestor e ao titular do certificado.

4.8.3 Procedimento para solicitação de revogação

4.8.3.1 O usuário que desejar revogar seu certificado deve acessar o sítio da plataforma web, através do endereço https://pessoal.icpedu.rnp.br, selecionar a opção de Certificado Pessoal, clicar em "Meu Certificado" e autenticar-se com suas credenciais, caso necessário. Por fim, deve-se escolher a opção de revogação do certificado e confirmar a escolha.

4.8.3.2 A solicitação de revogação que não parte do titular também é feita diretamente no sistema de gerenciamento da AC PESSOA ICPEdu, utilizando um *login* administrativo.

4.8.3.3 Como diretrizes gerais, define-se que:

a) O solicitante da revogação de um certificado é identificado;
b) As solicitações de revogação, bem como as ações delas decorrentes, são registradas e armazenadas;
c) O processo de revogação de um certificado termina com a geração e a publicação de uma LCR que contenha o certificado revogado e, no caso de utilização de consulta OCSP, com a atualização da situação do certificado nas bases de dados da AC PESSOA ICPEdu.

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

4.8.4 Prazo para solicitação de revogação

4.8.4.1 A solicitação de revogação pode ser feita à AC PESSOA ICPEdu a qualquer momento, e deve ser realizada imediatamente quando da ocorrência de quaisquer circunstâncias definidas na Seção 4.9.1.

4.8.5 Tempo em que a AC deve processar o pedido de revogação

4.8.5.1 O processo do pedido de revogação deve ocorrer de maneira automática.

4.8.6 Requisitos de verificação de revogação para as partes confiáveis

4.8.6.1 As partes confiáveis devem utilizar a última LCR como meio de assegurar a validade dos certificados emitidos pela AC PESSOA ICPEdu. Além disso, a validade da LCR é verificada através da verificação do prazo de validade desta, bem como de sua autenticidade, garantida pela assinatura da AC PESSOA ICPEdu.

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

4.8.7 Frequência de emissão de LCR

4.8.7.1 A LCR é emitida automaticamente em períodos de, no máximo, 24 horas.

4.8.7.2 A frequência máxima admitida para a emissão de LCR referente a certificados da AC PESSOA ICPEdu é de 112 (cento e doze) dias.

4.8.8 Latência máxima para a LCR

4.8.8.1 A LCR é publicada imediatamente após a sua emissão.

4.8.9 Procedimentos adicionais no caso de comprometimento da chave privada

4.8.9.1 A AC PESSOA ICPEdu comunica a todos os seus usuários sobre o comprometimento da chave privada, bem como os procedimentos que serão adotados para dar continuidade às suas operações.

4.8.9.2 A comunicação do comprometimento ou suspeita de comprometimento da chave privada é feita por correio eletrônico assinado digitalmente pelo representante da AC PESSOA ICPEdu.

4.8.9.3 Circunstâncias para suspensão

4.8.9.3.1 O serviço de suspensão de certificados não é disponibilizado pela AC PESSOA ICPEdu.

4.9 SERVIÇO DE STATUS DE CERTIFICADO

4.9.1 Características operacionais

4.9.2 A AC PESSOA ICPEdu não disponibiliza outros serviços de status de certificados além da publicação de LCRs no repositório, como definido na Seção 2.1.

4.10 ENCERRAMENTO DE ATIVIDADES

4.10.1 O vínculo com a AC PESSOA ICPEdu é encerrado pela expiração de um certificado ou por solicitação de revogação, conforme definido na Seção 4.9.3.

4.11 CUSTÓDIA E RECUPERAÇÃO DE CHAVE

Cabe exclusivamente ao titular do certificado a responsabilidade de custódia ou de recuperação de suas respectivas chaves.

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

5.1.1 Construções e localização das instalações da AC

5.1.1.1 A AC PESSOA ICPEdu está localizada em ambiente seguro, aprovado pelo CA-GId e homologado por auditoria externa. A localização e o sistema de certificação utilizado para a operação da AC PESSOA ICPEdu não são publicamente identificados. Internamente, não são permitidos ambientes compartilhados que permitam visibilidade nas operações de emissão e revogação de certificados. Essas operações são segregadas em compartimentos fechados e fisicamente protegidos.

5.1.1.2 Nas instalações físicas onde estão ativos utilizados para a operação da AC PESSOA ICPEdu foram implementadas, entre outros, os controles de segurança física a seguir:

a) Instalações de equipamentos de apoio, tais como máquinas de ar-condicionado, grupos geradores, *no-breaks*, baterias, quadros de distribuição de energia e de telefonia, retificadores, estabilizadores e similares;
b) Instalações para sistemas de telecomunicações;
c) Sistemas de aterramento e de proteção contra descargas atmosféricas;
d) Iluminação de emergência.

5.1.2 Acesso físico

O sistema de certificação da AC PESSOA ICPEdu está situado em um ambiente seguro gerenciado e controlado, conforme Política de Segurança do ICPEdu, que prevê:

5.1.2.1 Níveis de acesso

5.1.2.1.1 Devem existir, pelo menos, 4 (quatro) níveis de acesso físico e 2 (dois) níveis relativos à proteção da chave privada da AC PESSOA ICPEdu.

5.1.2.1.2 O primeiro nível é situado após a primeira barreira de acesso às instalações da AC PESSOA ICPEdu. Para entrar em uma área de nível 1, cada pessoa é devidamente identificada e registrada. A partir desse nível, pessoas estranhas à operação da AC PESSOA ICPEdu só são autorizadas a transitar com identificação e acompanhadas por um colaborador responsável. Nenhum tipo de processo operacional ou administrativo da AC é executado neste nível.

5.1.2.1.3 A partir do nível 1, equipamentos de gravação, fotografia, vídeo, som ou similares, assim como computadores portáteis, tem entrada controlada e somente podem ser utilizadas mediante autorização formal e supervisão.

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

5.1.2.1.4 O nível 2 é interno ao primeiro e requer identificação individual das pessoas que transitarem nele.

5.1.2.1.5 O nível 3 é interno ao segundo e abriga material e atividades críticos da operação da AC PESSOA ICPEdu. Quaisquer atividades relativas ao ciclo de vida dos certificados digitais emitidos pela AC estão localizadas a partir desse nível. Pessoas que não estejam envolvidas com essas atividades não têm permissão para acesso e não podem permanecer ou transitar sem acompanhamento por um colaborador responsável.

5.1.2.1.6 No nível 3, as entradas e saídas das pessoas responsáveis autorizadas são controladas e registradas. São requeridas formas de identificação individual por meios eletrônicos, como cartões ou biometria.

5.1.2.1.7 No nível 3, não é permitida a entrada de dispositivos móveis ou equipamentos portáteis de comunicação, excetuados aqueles necessários para a operação da AC PESSOA ICPEdu.

5.1.2.1.8 O nível 4 é interno ao terceiro e é onde são executadas as atividades especialmente sensíveis para a operação da AC PESSOA ICPEdu, tais como emissão e revogação de certificados, e a emissão de LCR. Todos os sistemas e equipamentos necessários a estas atividades estão localizados a partir desse nível. O nível 4 possui os mesmos controles de acesso do nível anterior e, além destes, há a obrigatoriedade da identificação de, no mínimo, 2 (dois) colaboradores autorizados. Neste nível, é exigida a presença destes profissionais sempre que houver trânsito de pessoas no ambiente.

5.1.2.1.9 No nível 4, todas as paredes, pisos e tetos possuem reforço em sua estrutura contra ameaças de acesso indevido, água, vapor, gases e fogo. Dutos de refrigeração, de energia e de comunicação são controlados para evitar invasão física. Adicionalmente, são implementados controles contra interferência eletromagnética externa.

5.1.2.1.10 As instalações do ambiente físico devem seguir as normas brasileiras aplicáveis. Eventuais omissões devem ser sanadas por normas internacionais pertinentes.

5.1.2.1.11 Existem, na AC, ambientes de nível 4 segregados, correspondentes a:

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

5.1.2.1.12 O nível 5 é interior aos ambientes de nível 4, e compreende um local de armazenamento reforçado que contém materiais criptográficos, tais como chaves, dados de ativação, suas cópias e equipamentos criptográficos.

5.1.2.1.13 Para garantir a segurança do material armazenado, o local de armazenamento deve ser feito de material de alta resistência e possuir tranca com chave.

5.1.2.2 Sistemas físicos de detecção

5.1.2.2.1 Todas as passagens entre os níveis de acesso, bem com as salas de operação, são monitoradas por câmeras de vídeo ligadas a um circuito de gravação 24x7. As câmeras são posicionadas de modo a não registrar ou recuperar senhas digitadas nos controles de acesso.

5.1.2.2.2 As passagens acima dos níveis de acesso 3 e 4 do ambiente são monitoradas por sistema de alarmes, ligados ininterruptamente.

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

5.1.2.2.3 Nos ambientes de nível 4, os sensores de presença são ativados sempre que o critério mínimo de acesso deixar de ser satisfeito.

5.1.2.2.4 O sistema de monitoramento de vídeo e o sistema de notificação de alarmes são permanentemente monitorados, de modo a permitir o acompanhamento das ações.

5.1.2.3 Sistema de controle de acesso

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

5.1.2.4 Mecanismos de emergência

5.1.2.4.1 São implementados mecanismos para garantir a segurança de pessoal e dos equipamentos da AC PESSOA ICPEdu em situações de emergência.

5.1.2.5 Todos os procedimentos referentes aos mecanismos de emergência estão documentados.

5.1.3 Energia e ar-condicionado

5.1.3.1 A AC PESSOA ICPEdu, os repositórios e a AR estão localizados em ambiente seguro que, além de conectados à rede elétrica, dispõe dos seguintes recursos: 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.

5.1.3.3 Todo cabeamento é estruturado em 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.

5.1.3.4 Toda a rede é identificada e vistoriada na busca de evidências de violação ou de outras anormalidades.

5.1.3.5 A topologia da rede é documentada, observados os requisitos de sigilo estabelecidos pela Política de Segurança da Informação da ICPEdu.

5.1.3.6 Não são permitidas instalações provisórias, fiações expostas ou diretamente conectadas às tomadas sem a utilização de conectores adequados

5.1.3.7 O sistema de climatização atende aos requisitos de temperatura e umidade exigidos pelos equipamentos utilizados no ambiente e dispõe de filtros de poeira. Nos ambientes de nível 4, o sistema de climatização é independente e tolerante a falhas.

5.1.3.8 A temperatura dos ambientes atendidos pelo sistema de climatização é permanentemente monitorada por sistemas de notificação.

5.1.3.9 O sistema de ar condicionando dos ambientes de nível 4 é interno, com troca de ar realizada de forma controlada.

5.1.3.10 A capacidade de redundância de toda a estrutura de energia e ar-condicionado da AC é garantida por meio de geradores de porte compatível, geradores de reserva, sistemas de *nobreaks* redundantes e sistemas redundantes de ar-condicionado.

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

5.1.4 Exposição a água

5.1.4.1 A AC PESSOA ICPEdu está localizada em uma estrutura inteiriça de um ambiente de nível quatro. Essa estrutura deve ser 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 monitoração 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, possuem 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 Não é permitido fumar ou portar objetos que produzam fogo ou faísca nas instalações da AC PESSOA ICPEdu.

5.1.5.3 A sala-cofre de nível 4 possui sistema para detecção precoce de fumaça e sistema de extinção de incêndio por gás. As portas de acesso à sala-cofre só se abrem quando a anterior estiver fechada.

5.1.5.4 Em caso de incêndio nas instalações da AC, o aumento da temperatura interna da sala-cofre de nível 4 está projetada para não exceder os 50 graus Celsius, suportando esta condição por, no mínimo, 1 (uma) hora.

5.1.6 Armazenamento de mídia

5.1.6.1 A AC PESSOA 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 devidamente destruídos antes de ir para o lixo.

5.1.7.2 Todos os dispositivos eletrônicos anteriormente utilizados para o armazenamento de informações sensíveis são fisicamente destruídos.

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

5.1.8.1 A AC PESSOA 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

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

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

5.2.1.2 A AC PESSOA 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 AC PESSOA ICPEdu define a divisão de responsabilidades entre os perfis:

5.2.1.2.1.1 Gerente

a) definir e alterar os grupos de administradores, auditores e operadores;
b) aprovar os relatórios da AC PESSOA ICPEdu;
c) encaminhar os relatórios da AC PESSOA ICPEdu ao CA.

5.2.1.2.1.2 Administrador:

a) instalar, configurar e atualizar os equipamentos e software de gestão do ciclo de vida do Certificado digital;
b) criar uma AC;
c) configurar os templates de certificados de acordo com esta DPC;
d) associar a AC a uma política e atribuir ou trocar os grupos de operadores e auditores da AC;
e) gerenciar os operadores da AC PESSOA ICPEdu;
f) realizar o backup e recuperação de backup de dados e software de acordo com a política estabelecida;
g) iniciar e encerrar os serviços da AC PESSOA ICPEdu;
h) definir e alterar os grupos de auditores e operadores.

5.2.1.2.1.3 Auditor:

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

5.2.1.2.1.4 Operador:

a) utilizar a chave privada de uma AC para a emissão de certificados digitais e LCR;
b) emitir, expedir, distribuir, revogar e gerenciar certificados;
c) distribuir 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.

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

5.2.1.4 No desligamento de um profissional da AC PESSOA ICPEdu, suas permissões de acesso são imediatamente revogadas. Quando há mudança na posição ou função do profissional, as permissões de acesso são revistas. É garantida a devolução e a devida sanitização de todos os recursos disponibilizados quando do desligamento de um profissional.

5.2.2 Número de pessoas necessárias por tarefa

5.2.2.1 O controle multiusuário via uso de segredo compartilhado é requerido para a geração e a utilização da chave privada da AC PESSOA ICPEdu.

5.2.2.2 Todas as tarefas executadas no ambiente onde está localizado o equipamento de certificação da AC PESSOA ICPEdu necessitam da presença do gerente do serviço. Além disso, para a ativação da chave privada da AC PESSOA ICPEdu, são seguidas as definições dispostas na Seção 6.2.2.

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

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

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

5.2.3.3 A AC PESSOA ICPEdu deverá implementar um padrão de utilização de “senhas fortes”, definido em sua Política de Segurança, com procedimentos de validação dessas senhas.

5.2.4 Funções que requerem separação de deveres

5.2.4.1 A AC PESSOA ICPEdu realiza segregação de atividades, ou seja, as pessoas que exercem papel de auditor da AC PESSOA ICPEdu não podem exercer os papéis de administrador nem de operador da AC e do HSM.

5.3 CONTROLES DE PESSOAL

A DPC garante que todos os profissionais da AC PESSOA ICPEdu encarregados de tarefas operacionais tem registrado em contrato ou termo de responsabilidade:

a) o compromisso de observar as normas, políticas e regras aplicáveis da ICPEdu; e
b) o compromisso de não divulgar informações sigilosas a que tenham acesso.

5.3.1 Antecedentes, qualificação, experiência e requisitos de idoneidade

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

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

5.3.2 Procedimentos de verificação de antecedentes

5.3.2.1 O responsável pela AC PESSOA ICPEdu deverá ter seu nome submetido à aprovação da gestão da DAGSer.

5.3.3 Requisitos de treinamento

5.3.3.1 Todo o pessoal da AC PESSOA ICPEdu e das ACs vinculadas envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados deverá receber treinamento documentado, suficiente para o domínio dos seguintes temas:

a) princípios e mecanismos de segurança da AC PESSOA ICPEdu;
b) plataforma computacional e softwares utilizados para gerenciamento da AC PESSOA ICPEdu;
c) atividades sob sua responsabilidade;
d) procedimentos de recuperação de desastres e de continuidade do negócio.

5.3.4 Frequência e requisitos para reciclagem técnica

5.3.4.1 Sempre que novas pessoas são admitidas na equipe ou que há quaisquer alterações em procedimentos ou modificações na plataforma computacional, novos treinamentos e capacitações são realizadas com a equipe.

5.3.5 Sanções para ações não autorizadas

5.3.5.1 Na eventualidade de uma ação não autorizada, real ou suspeita, se realizada por pessoa encarregada de processo operacional da AC PESSOA ICPEdu ou de uma AC vinculada, a AC PESSOA ICPEdu suspende, de imediato, o acesso dessa pessoa ao seu sistema de certificação, instaura processo administrativo para apurar os fatos e, se for o caso, adota as medidas legais cabíveis.

5.3.5.2 O processo administrativo é realizado pela Gerência de Recursos Humanos, que aplicará as devidas providências definidas em normativo interno.

5.3.6 Requisitos para prestadores de serviço independentes

5.3.6.1 Todos os profissionais da AC PESSOA ICPEdu envolvidos em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados são contratados conforme o estabelecido na Política de Segurança da Informação da ICPEdu.

5.3.7 Documentação fornecida aos funcionários

5.3.7.1 A AC PESSOA ICPEdu disponibiliza para todo o seu pessoal:

a) sua DPC;
b) a Política de Segurança da ICPEdu;
c) documentação operacional relativa a 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 PESSOA ICPEdu registra em arquivos de auditoria todos os eventos relacionados à segurança do seu sistema de certificação. Os seguintes eventos estão incluídos em arquivos de auditoria:

a) Iniciação e desligamento do sistema de certificação;
b) Tentativas de criar, remover, definir senhas ou mudar privilégios de sistema dos operadores da AC;
c) Mudanças na configuração da AC 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 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 aplicação;
l) Operações de escrita nesse repositório, quando aplicável; e
m) Realização de *backup* e restauração.

5.4.1.2 A AC PESSOA ICPEdu 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 informações pessoais de usuários.

5.4.1.4 Todos os registros de auditoria contêm a data e hora do evento e a identificação do usuário.

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

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 certificados ou informação pessoal de usuário.

5.4.1.6 Toda a documentação relacionada aos serviços da AC PESSOA ICPEdu é armazenada em local único e protegido, conforme a Política de Segurança da Informação da ICPEdu.

5.4.1.7 A AC PESSOA ICPEdu registra eletronicamente em arquivos de auditoria todos os eventos relacionados à validação e à aprovação da solicitação, bem como a revogação de certificados. Os seguintes eventos são obrigatoriamente em arquivos de auditoria:

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

5.4.2 Frequência de auditoria de registros

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

a) Mensalmente;
b) Quando houver a emissão ou revogação de um Certificado digital;
c) Na ocorrência de uma anormalidade, como em caso de suspeita de comprometimento da segurança.

5.4.3 Período de retenção para registros de auditoria

5.4.3.1 A documentação dos eventos é arquivada pelo seguinte período:

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

5.4.4 Proteção de registros de auditoria

5.4.4.1 O acesso ao arquivo é exclusivo dos administradores e auditores. O arquivo é armazenado pelo gerente da DAGSer e sua integridade é garantida através da validação do resumo criptográfico (*hash*) ou em mídia não volátil, a qual é trocada a cada 5 (cinco) anos.

5.4.5 Procedimentos para cópia de segurança de registros de auditoria

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

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 PESSOA 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 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 PESSOA ICPEdu verifica a integridade das cópias de segurança a cada 6 (seis) meses.

5.4.6 Sistema de coleta de dados de auditoria (interno ou externo)

5.4.6.1 Todos os sistemas de eventos para auditoria utilizados pela AC PESSOA ICPEdu em seus procedimentos operacionais são internos.

5.4.6.2 O sistema de coleta de eventos para auditoria utilizados pela AC PESSOA 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 em seu desligamento, garantindo a integridade e a disponibilidade dos dados coletados.

5.4.7 Avaliações de vulnerabilidades

5.4.7.1 Todos os registros são analisados sob a ótica de possíveis vulnerabilidades na plataforma computacional que hospeda o sistema de gerenciamento de certificados digitais e as chaves criptográficas da AC PESSOA ICPEdu. Também são analisados os registros do ambiente seguro.

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;

b) Certificados emitidos.

5.5.2 Período de retenção para arquivo

5.5.2.1 O período de arquivamento dos registros de auditoria segue a definição descrita no item 5.4.3. Os demais registros são arquivados pelo período de 1 (um) ano após a expiração do certificado.

5.5.2.2 O período de arquivamento dos registros de auditoria segue o que foi definido na Política de Segurança.

5.5.3 Proteção dos registros

5.5.3.1 O procedimento de proteção dos registros de auditoria segue a definição descrita no item 5.4.4.

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

5.5.3.2 A documentação é arquivada em formato digital.

5.5.4 Procedimentos de cópias de arquivo

5.5.4.1 Caso haja outras informações não relacionadas à seção 5.4.4, a cópia de segurança do arquivo é realizada seguindo os mesmos procedimentos da seção 5.4.5.

5.5.4.2 A cópia de segurança das informações do ambiente off-line é realizada no final de qualquer cerimônia e armazenada em um local fora do ambiente, seguindo os mesmos critérios de segurança.

5.5.5 Requisitos para datação dos registros

5.5.5.1 Todos os registros devem conter informações de data e hora.

5.5.5.2 Informações de data e hora dos registros baseiam-se na hora oficial internacional, *Coordinated Universal Time* – UTC, e obedecem ao formato YYYYMMDDHHMMSSZ, incluindo segundos, mesmo que o número de segundos seja zero.

5.5.6 Sistema de recolhimento de registros (interno ou externo)

5.5.6.1 O sistema de coleta de toda informação para arquivamento é feito internamente, isto é, feito pela própria AC PESSOA ICPEdu.

5.5.7 Procedimentos para obtenção e verificação dos registros armazenados

5.5.7.1 Informações do arquivo são somente obtidas mediante aprovação do gerente da AC PESSOA 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 Quando necessário, um novo par de chaves para a AC PESSOA ICPEdu é gerado três meses antes do ponto de atualização de seu certificado.

5.7 COMPROMETIMENTO E RECUPERAÇÃO DE DESASTRE

A ICPEdu mantém procedimentos de recuperação do ambiente em casos de comprometimento da infraestrutura ou desastre.

5.7.1 Procedimentos gerenciamento de incidentes e comprometimento

5.7.1.1 Caso ocorra um comprometimento ou um desastre que comprometa o site principal e o site *backup*, o certificado da AC PESSOA ICPEdu é revogado e um novo certificado é emitido. Este fato é comunicado no site da ICPEDU.

5.7.2 Recursos computacionais, *software*, e/ou dados corrompidos

5.7.2.1 Procedimentos de recuperação utilizados pela AC PESSOA ICPEdu quando recursos computacionais, software ou dados estiverem corrompidos ou houver suspeita de corrupção.

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

5.7.3 Procedimentos para comprometimento de chave privada de entidade

5.7.3.1 Procedimentos de recuperação utilizados na circunstância de revogação do certificado da AC PESSOA ICPEdu.

5.7.4 Capacidade para continuidade de negócios após desastre

5.7.4.1 Procedimentos de recuperação utilizados pela AC PESSOA ICPEdu após a ocorrência de um desastre natural ou de outra natureza, antes do restabelecimento de um ambiente seguro.

5.8 EXTINÇÃO DA AC

5.8.1 São adotadas as seguintes providências mínimas em caso de extinção da AC pessoa ICPEDU:

5.8.1.1 Notificar publicamente todas as partes interessadas;

5.8.1.2 Notificar titulares de certificados;

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 PESSOA 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 PESSOA 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 Política de Segurança da Informação da ICPEdu.

6.1.1.2 A geração do par de chaves da AC PESSOA ICPEdu 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.

6.1.1.3 O par de chaves da AC PESSOA ICPEdu da ICPEdu é gerado em módulo criptográfico de *hardware* compatível com padrão FIPS 140-2 e certificação INMETRO NSH-3/NSC3.

6.1.1.4 Somente os titulares dos certificados emitidos pela ICPEdu podem gerar seus respectivos pares de chaves.

6.1.1.5 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.

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

6.1.2 Divulgação da chave pública da AC às partes confiantes

6.1.2.1 A divulgação do Certificado da AC PESSOA ICPEdu para os usuários da ICPEdu é realizada:

a) no repositório da AC PESSOA ICPEdu;
b) no sítio da AC PESSOA ICPEdu ou das ACs integrantes da ICPEdu;
c) em outros meios seguros definidos pelo CA da ICPEdu.

6.1.2.2 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.

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

6.1.3 Tamanhos de chaves

6.1.3.1 O tamanho das chaves criptográficas assimétricas da AC PESSOA ICPEdu e das ACs de nível imediatamente subsequente devem utilizar chaves preferencialmente de 4096 bits RSA.

6.1.3.2 O tamanho mínimo das chaves criptográficas do item anterior deve ser de 2048 bits RSA.

6.1.4 Geração dos parâmetros de chave pública e verificação de qualidade

6.1.4.1 Os parâmetros de geração de chaves assimétricas da AC PESSOA ICPEdu seguem as recomendações internacionais de qualidade de chaves assimétricas, compatíveis com o padrão FIPS 140-2.

6.1.4.2 Os parâmetros deverão ser verificados de acordo com as normas estabelecidas pelo padrão definido em regulamento editado por instrução normativa da AC PESSOA ICPEdu que defina os padrões e algoritmos criptográficos.

6.1.5 Propósitos de uso de chaves

6.1.5.1 A chave privada da AC PESSOA ICPEdu será usada para os propósitos definidos na extensão *keyUsage* apresentados na seção A.2.

6.1.5.2 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

6.2.1 Padrões e controle para módulo criptográfico

6.2.1.1 O módulo criptográfico de geração de chaves assimétricas da AC PESSOA ICPEdu adota o padrão descrito no item 6.1.

6.2.2 Controle “n de m” para chave privada

6.2.2.1 A chave de ativação do módulo de processamento criptográfico que armazena a chave privada da AC PESSOA ICPEdu é dividida em 6 (seis) partes e guardadas nos cofres de cada ambiente seguro para utilização pelo GO-ICPedu. É necessária a presença de apenas 1 (uma) dessas 6 (seis) partes para a ativação do módulo e a consequente liberação da chave para uso por tempo indeterminado.

6.2.3 Custódia (*escrow*) de chave privada

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

6.2.4 Cópia de segurança de chave privada

6.2.4.1 A AC PESSOA ICPEdu utiliza dois ambientes seguros: em Florianópolis e em Brasília. Em Florianópolis, há 2 (dois) HSMs, ambos em modo operacional, na sala cofre da UFSC e mais 2 (dois) HSMs, ambos em modo *backup*, no Ponto de Presença da RNP. Já em Brasília, no *Internet Data Center* (IDC), há 4 (quatro) HSMs, 2 (dois) em modo operacional e outros 2 (dois) em modo *backup*. O HSM em modo *backup* não contém a chave privada.

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

6.2.4.2 A chave privada do HSM operacional é cifrada utilizando-se a chave pública do HSM *backup* e armazenada em mídia digital. Para restaurar a chave privada da AC PESSOA ICPEdu, o arquivo cifrado contendo a chave privada deve ser copiado para o HSM *backup* e sua recuperação autorizada pelo grupo de administradores.

6.2.4.3 A cópia de segurança é armazenada e cifrada por algoritmo simétrico e protegida com um nível de segurança não inferior àquele definido para a chave original.

6.2.5 Arquivamento de chave privada

6.2.5.1 A chave privada da AC PESSOA 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 exportação e importação da chave privada da AC PESSOA ICPEdu é realizada através de uma cópia de segurança cifrada e que fica sob a responsabilidade 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 PESSOA ICPEdu é ativada pelo grupo de operadores do HSM responsáveis pela chave. Esta identificação é realizada por meio de senha e de dispositivos de controle de acesso em *hardware*, *token* ou Smartcard.

6.2.8.2 O grupo de operadores do HSM da AC PESSOA ICPEdu libera a chave por tempo indeterminado e sem limite de uso.

6.2.8.3 A chave privada é utilizada pelo operador da AC PESSOA ICPEdu no SGCI para assinar LCRs e certificados digitais.

6.2.9 Método de desativação de chave primária

6.2.9.1 Para desativar a chave privada da AC PESSOA ICPEdu, o grupo de operadores do HSM da AC PESSOA ICPEdu executa 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 PESSOA ICPEdu será 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 *smartcards* dos perfis de operador, auditor e administrador do HSM são inabilitados e, quando possível, fisicamente destruídos.

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

6.3 OUTROS ASPECTOS DO GERENCIAMENTO DO PAR DE CHAVES

6.3.10.1 Arquivamento de chave pública

6.3.10.2 A chave pública da AC PESSOA ICPEdu é permanentemente armazenada no formato PEM em mídia digital.

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

6.3.1.1 A chave privada da AC PESSOA ICPEdu é utilizada apenas durante o período de validade do certificado correspondente. A chave pública pode ser utilizada, por tempo indeterminado, para verificação de assinaturas geradas durante o período de validade do certificado correspondente.

6.4 DADOS DE ATIVAÇÃO

6.4.1 Proteção de dados de ativação

6.4.1.1 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 PESSOA ICPEdu é realizada off-line, de forma a impedir o acesso remoto não autorizado.

6.5.1.2 O computador que hospeda a AC PESSOA ICPEdu é dedicado e não roda em servidores que não são relacionados à AC. São implementados os seguintes controles operacionais:

a) Controle de acesso aos serviços através de perfis de administradores da AC PESSOA ICPEdu;
b) Clara separação das tarefas e atribuições relacionadas a cada perfil;
c) Sistema operacional mantido atualizado em relação aos patches de segurança publicados;
d) Controle de acesso físico aos computadores restritos aos administradores da AC;
e) Uso de criptografia para segurança de base de dados, quando exigido pela classificação de suas informações;
f) Geração e armazenamento de registros de auditoria da AC;
g) Mecanismos para cópias de segurança (backup).

6.5.1.3 Essas características são implementadas pela combinação de mecanismos de segurança do sistema operacional dos computadores com mecanismos de segurança física.

6.5.1.4 Ao ser enviado para manutenção, qualquer equipamento ou parte dele é sanitizado de forma a ter apagadas as informações sensíveis nele contidas e controlados seu número de série e as datas de envio e de recebimento. Ao retornar às instalações da AC PESSOA ICPEdu, o equipamento é inspecionado. Todos os eventos são registrados para fins de auditoria.

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

6.5.1.5 Qualquer equipamento incorporado à AC PESSOA ICPEdu é preparado e configurado de forma a apresentar o nível de segurança necessário à sua finalidade.

6.6 CONTROLES TÉCNICOS DO CICLO DE VIDA

6.6.1.1 Controles de desenvolvimento de sistemas

6.6.1.2 A AC PESSOA ICPEdu utiliza um sistema de gerenciamento de certificados digitais e um módulo criptográfico elaborados sob uma metodologia de desenvolvimento seguro.

6.6.1.3 Os processos de projeto e desenvolvimento conduzidos pela AC PESSOA ICPEdu possuem documentação suficiente para suportar avaliações externas de segurança dos componentes da AC.

6.6.1 Controles de gerenciamento de segurança

6.6.1.1 A DAGSer verifica se os requisitos apresentados na Seção 6.5.1 e 6.6.1 são atendidos.

6.7 CONTROLES DE SEGURANÇA DE REDE

6.7.1 Diretrizes gerais

6.7.1.1 O computador que hospeda o SGCI da AC PESSOA ICPEdu opera off-line, fisicamente desconectado de qualquer rede.

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

6.7.1.3 As versões mais recentes dos sistemas operacionais e dos aplicativos, bem como as eventuais correções (patches) disponibilizadas pelos respectivos fabricantes são aplicadas 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 Um *firewall* provê o isolamento dos equipamentos servidores com acesso externo através de DMZ em relação aos equipamentos com acesso exclusivamente interno à AC PESSOA ICPEdu.

6.7.2.2 O *firewall* armazena os devidos 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.

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

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 em norma interna da RNP sobre Tratamento de Incidentes de Segurança da Informação.

6.7.5 Carimbo de tempo

6.7.6 Data e hora

6.7.6.1 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.

6.7.7 Atualização off-line

6.7.7.1 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 PESSOA ICPEdu está em conformidade com a RFC 5280, pelo padrão ITU X.509 ou ISO/IEC 9594-8.

7.1.1 Número de versão

Todos os certificados emitidos pela AC PESSOA ICPEdu usam 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.

7.1.3 Identificadores de algoritmo

As informações referentes aos identificadores de objeto dos algoritmos podem ser encontradas na Seção A.2.

7.1.4 Formatos de nome

Os valores e regras para o nome distinto da AC PESSOA ICPEdu seguem o padrão X.500 e podem ser encontrados na Seção A.1.

7.1.5 Restrições de nome

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

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 PESSOA ICPEdu é 1.3.6.1.4.1.15996.1.1.4.

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.

7.2 PERFIL DE LCR

7.2.1 Número(s) da versão

Versão: 2.0

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

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

7.2.2 Extensões de LCR e de suas entradas

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

7.3 PERFIL DE OCSP

A AC PESSOA ICPEdu não provê 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 e procedimentos estão em conformidade com a DPC, Política de Segurança da Informação da ICPEdu e demais normas e procedimentos estabelecidos pela DAGSer e Comitê Assessor de Gestão de Identidade (CA-GID).

8.1 FREQUÊNCIA E CIRCUNSTÂNCIAS DAS AVALIAÇÕES

8.1.1 Frequência

8.1.1.1 A AC PESSOA ICPEdu é auditada anualmente.

8.2 IDENTIFICAÇÃO/QUALIFICAÇÃO DO AVALIADOR

8.2.1 Identificação dos avaliadores

8.2.1.1 A DAGSer indicará os auditores (internos e externos) da AC PESSOA ICPEdu, respeitando critérios de qualificação, tais como proficiência em infraestruturas de chaves públicas, segurança de sistemas e da informação e experiência em processos de auditoria.

8.3 RELAÇÃO DO AVALIADOR COM A ENTIDADE AVALIADA

8.3.1.1 Avaliação da AC Pessoa ICPEDU

8.3.1.2 Os avaliadores da AC PESSOA ICPEdu devem ser externos à estrutura administrativa e operacional da ICPEdu.

8.4 TÓPICOS COBERTOS PELA AVALIAÇÃO

8.4.1 Objetivos

8.4.1.1 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 são avaliados com critérios específicos.

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, a qual, por sua vez, tomará as devidas providências junto às equipes responsáveis pelas ações corretivas.

8.6 COMUNICAÇÃO DOS RESULTADOS

8.6.1.1 Encaminhamento

8.6.1.2 Os relatórios resultantes das avaliações devem ser encaminhados para a DAGSer.

Versão: 2.0

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.

9.2 RESPONSABILIDADE FINANCEIRA

A AC PESSOA ICPEdu da ICPEdu não terá qualquer responsabilidade financeira.

9.3 CONFIDENCIALIDADE DA INFORMAÇÃO DO NEGÓCIO

9.3.1 Escopo de informações confidenciais:

9.3.1.1 Informações relativas a solicitações de certificados;

9.3.1.2 Registros de trilhas de auditoria;

9.3.1.3 Relatórios de auditorias;

9.3.1.4 Planos de contingência e planos de recuperação de desastres;

9.3.1.5 Medidas de segurança relativas:

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

9.3.2 Informações fora do escopo de informações confidenciais

9.3.2.1 São consideradas informações públicas:

a) Certificados da AC PESSOA ICPEdu;
b) Lista de certificados revogados;
c) Versões publicadas de PCs, DPCs e Política de Segurança.

9.3.3 Responsabilidade em proteger a informação confidencial

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

Versão: 2.0

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

9.4 PRIVACIDADE DA INFORMAÇÃO PESSOAL

9.4.1 Plano de privacidade

9.4.1.1 As informações relacionadas aos usuários de certificados emitidos pela AC PESSOA ICPEdu são confidenciais.

9.4.2 Informação tratada como privada

9.4.2.1 Todas as informações pessoais que não constam no certificado emitido.

9.4.3 Informação não considerada privada

9.4.3.1 Informações pessoais que constam no certificado emitido.

9.4.4 Responsabilidade de proteção de informação considerada privada

9.4.4.1 A AC PESSOA ICPEdu mantém a confidencialidade das informações classificadas como privadas.

9.4.5 Aviso e consentimento para uso de informação privada

9.4.5.1 Não há previsão de uso das informações privadas obtidas pela AC PESSOA ICPEdu para finalidades diversas.

9.4.5.2 O titular de certificado e seu representante legal terão amplo acesso a quaisquer dos seus próprios dados e identificações, conforme Lei n. 13.709/18 e demais legislações aplicáveis.

9.4.6 Divulgação em processos judiciais e administrativos

9.4.6.1 Nenhum documento, informação ou registro são fornecidos a terceiros, salvo o titular ou o seu representante legal, devidamente constituído por instrumento público ou particular, com poderes específicos, vedado substabelecimento.

9.4.6.2 As informações privadas ou confidenciais somente têm previsão de uso na hipótese de instrução de processo administrativo ou judicial, ou por ordem judicial ou da autoridade administrativa competente, observada a legislação aplicável.

9.5 PRAZO E RESCISÃO

9.5.1 Prazo

9.5.1.1 Esta DPC entra em vigor a partir da publicação que a aprovar e permanece válida e eficaz até que venha a ser revogada ou substituída.

9.5.2 Término

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

9.5.2.2 Os certificados emitidos no período de validade de uma DPC permanecem sujeitos às suas determinações até o final do período de validade do certificado.

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

9.5.3 Efeito da rescisão e sobrevivência

9.5.3.1 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.

9.6 AVISOS INDIVIDUAIS E COMUNICAÇÕES COM OS PARTICIPANTES

9.6.1 Meio de comunicação

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

9.7 ALTERAÇÕES

9.7.1 Procedimentos para emendas

9.7.1.1 Compete à DAGSer a proposição de alterações à DPC.

9.7.1.2 Novas versões resultantes de alterações são encaminhadas ao CA-GID para aprovação. O nome do arquivo da nova versão da DPC no repositório da AC PESSOA ICPEdu deve seguir a convenção de nomenclatura definida na extensão CertificatePolicies, descrita no Anexo A.2.

9.7.2 Mecanismo de notificação e períodos

9.7.2.1 O surgimento de novas versões e subversões da DPC é noticiado no site da AC PESSOA ICPEdu.

9.7.3 Circunstâncias na qual o OID deve ser alterado

9.7.3.1 O ODI é alterado sempre que surgem novas versões.

9.8 SOLUÇÃO DE CONFLITOS

9.8.1 Instâncias

9.8.1.1 Quando for o caso, a disputa deve ser resolvida pela DAGSer. Caso não seja aplicável ou mesmo não se chegue ao consenso, a disputa deve ser resolvida pelo CA-GID.

9.9 LEI APLICÁVEL

9.9.1 Legislação

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

9.10 CONFORMIDADE COM A LEI APLICÁVEL

9.10.1.1 Instâncias e cumprimento

9.10.1.2 A AC PESSOA ICPEdu 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

9.11 DISPOSIÇÕES DIVERSAS

9.11.1 Acordo completo

9.11.1.1 Esta DPC representa as obrigações e deveres aplicáveis à AC PESSOA ICPEdu.

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 24, de 29 de agosto de 2003**. Aprova a versão revisada e consolidada do documento critérios e procedimentos para realização de Auditorias nas Entidades da ICP-Brasil – DOC-ICP-08.

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.

HOUSLEY, R. *et al*. **RFC 328**: Internet X.509 public key infrastructure certificate and certificate revocation list (CRL) profile. Internet Engineering Task Force, apr. 2002. Wilmington: IETF, 2002. Disponível em: https://datatracker.ietf.org/doc/html/rfc3280 Acesso em: 7 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.

KILLE, S. *et al*. **RFC 2247**: Using domains in LDAP/X.500 distinguished names, January 1998. Disponível em: https://www.ietf.org/rfc/rfc2247.txt Acesso em: 7 jun. 2022.

NIST. National Institute of Standards and Technology. **FIPS 140-2**: security requirements for cryptographic modules. Disponível em: https://csrc.nist.gov/publications/detail/fips/140/2/final Acesso em: 7 jun. 2022.

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

NYSTROM, M.; KALISKI, B. **RFC 2986**: PKCS #10: Certification Request Syntax Specification Version 1.7, November 2000. Disponível em: https://datatracker.ietf.org/doc/html/rfc2986 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 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 PESSOA ICPEdu.

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

Tabela A.3. – Campos de nome dos certificados dos Usuários Finais.

Campo	Conteúdo	Mandatório
C	BR	Sim
O	ICPEdu	Sim
OU	Cliente do serviço ICPEdu	Sim
L	Localidade	Não
S	Unidade da Federação	Não
CN	Nome do requerente	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.4. – Tamanhos de chave da AC PESSOA ICPEdu.

Algoritmo	Tamanho
RSA	4096

Tabela A.5. – Tamanhos de chave dos usuários da AC PESSOA ICPEdu.

Algoritmo	Tamanho
RSA	2048
RSA	4096

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

Tabela A.6. – Campos do certificado AC PESSOA 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 ICPEdu são definidos no documento "**Padrões e Algoritmos Criptográficos da ICPEdu**". [2]
Extensões	Os certificados contêm extensões apresentadas na Seção A.2.2.

Tabela A.7. – Campos do certificado de usuários.

Campo	Conteúdo
Versão (*Version*)	3
Emissor (*Issuer*)	DN conforme tabela A.2
Titular (*Subject*)	DN conforme tabela A.3
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 ICPEdu são definidos no documento "**Padrões e Algoritmos Criptográficos da ICPEdu**". [2]
Extensões	Os certificados contêm extensões apresentadas na Seção A.2.2.

Tabela A.8. – 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.

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

Tabela A.9. – Extensões do certificado da AC PESSOA ICPEdu.

Extensão	Descrição	Crítica
SubjectKeyIdentifier	*Hash* da chave pública da AC PESSOA 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.	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. 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.	Não

Tabela A.10. – Extensões do certificado emitido pela AC PESSOA ICPEdu.

Extensão	Descrição	Crítica
SubjectKeyIdentifier	*Hash* da chave pública do titular do certificado	Não
CRLDistributionPoints	Contém o endereço na web onde se obtém a LCR emitida pela AC PESSOA ICPEdu (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
CertificatePolicies	Especifica o ObjectIdentifier (OID) da PC/DPC da AC PESSOA ICPEdu 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 ICPEdu.	Não

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

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.11. – Campos da LCR da AC PESSOA 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.12. – Extensões da LCR.

Extensão	Descrição	Crítica
AuthorityKeyIdentifier	Contém o mesmo valor do campo *Subject Key Identifier* do certificado da AC PESSOA ICPEdu.	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