Política de Certificado e Declaração de Práticas de Certificação
AC CBPF

Versão 0.6 – 20/07/2011

Sumário

1. Introdução

1.1 Visão Geral

Este documento constitui a Política de Certificado (PC) e a Declaração de Práticas de Certificação (DPC) da Autoridade Certificadora do Centro Brasileiro de Pesquisas Físicas (AC CBPF) na Infra-estrutura de Chaves Públicas para Pesquisa e Ensino (ICPEDU) da Rede Nacional de Pesquisa e Ensino (RNP). A RNP foi criada em 1989 pelo Ministério da Ciência e Tecnologia (MCT) com o objetivo de construir uma infra-estrutura de rede Internet nacional para a comunidade acadêmica. Uma das iniciativas atuais é a implantação de um serviço nacional de chaves publicas para seus usuários, a ICPEDU.

O funcionamento da ICPEDU é determinado pelo Comitê Gestor (CG). A âncora de confiança da ICPEDU é a AC Raiz operada pelo Grupo de Operação da Autoridade Certificadora (GOPAC), que fica sob a responsabilidade da RNP. Subordinados à AC Raiz podem operar duas classes de autoridades certificadoras intermediárias: ACs Institucionais e ACs de Serviços. As autoridades certificadoras internas são aquelas criadas e operadas pelo GOPAC. As autoridades certificadoras externas são aquelas de responsabilidade das organizações parceiras, podendo ou não ser operadas pelo GOPAC.

Neste documento, são descritas as polìticas para emissão de certificados assim como as práticas e controles operacionais empregadas pela AC CBPF na execução dos seus serviços. A AC CBPF é a autoridade certificadora de nìvel mais alto no âmbito do Centro Brasileiro de Pesquisas Físicas e tem seu certificado digital assinado pela Autoridade Certificadora Raiz da ICPEDU. A AC CBPF emite certificados digitais para pessoas fìsicas e serviços vinculados ao CBPF. Esta PC/DPC estabelece os requisitos para a emissão e gerenciamento de certificados digitais que podem ser utilizados para autenticação nos serviços computacionais oferecidos no âmbito do CBPF.
Esta DPC foi elaborada seguindo a RFC 3647 [1].

1.2 Nome do Documento e Identificação

Titulo: Política de Certificação e Declaração de Práticas de Certificação do Centro Brasileiro de Pesquisas Físicas
Versão: [0.6].
Data: 20/07/2011
Aprovação: Este documento foi aprovado pelo CG da ICPEDU em [Insira aqui a data de aprovação do documento]
ANSI.1 OID: 1.3.6.1.4.1.34897.1.1.1.1.1.0.6

1.3.6.1.4.1	Prefixo para IANA private enterprises iso(1).org(3).dod(6).internet(1).private(4).enterprise(1)
34897	Identificador registrado do CBPF
1	Identificador interno na hierarquia CBPF
1	Identificador interno na hierarquia (Dir)
1	AC CBPF no ICP-EDU
1	Identificador para uso futuro

1	Tipo de identificação – PC/DPC
0.6	Número de versão do PC/DPC

1.3 Participantes da ICP

1.3.1 Autoridades Certificadoras

A AC CBPF emite certificados digitais para pessoas que trabalham na instituição e para serviços computacionais.

1.3.2 Autoridades de Registro

A atividade de identificação e cadastramento dos titulares de certificados digitais da AC CBPF será realizada pela AR da AC CBPF.

1.3.3 Titulares dos Certificados

Os titulares dos certificados são funcionários, alunos ou terceirizados, vinculados ao CBPF., alem de serviços da infraestrutura de rede do CBPF.

1.3.4 Entidades Confiantes

As partes confiantes são pessoas físicas ou sistemas vinculados aos sistemas administrativos, acadêmico e de pesquisa brasileiros.

1.3.5 Outros Participantes

Não estipulado.

1.4 Uso do Certificado

1.4.1 Aplicações apropriadas para os certificados

O certificado da AC CBPF deve ser usado somente para emitir outros certificados, assinar a LCR da AC CBPF e para checar certificados que reivindicam ser emitidos pela AC CBPF.
Os certificados emitidos pela AC CBPF podem ser usados para:

- autenticação de usuários e serviços;
- autenticação de emails assinados;

O certificado da AR CBPF deve ser utilizado somente por seus administradores e operadores para atividades relacionadas à AR CBPF.

1.4.2 Aplicações proibidas para os certificados

Certificados emitidos pela AC CBPF são válidos apenas no contexto de pesquisa e atividades educacionais. Qualquer outro uso é estritamente proibido.

1.5 Dados para Contato

1.5.1 Entidade responsável por este documento

Coordenação de Atividades Técnicas do Centro Brasileiro de Pesquisas Físicas – CAT/CBPF.

O endereço postal para contato da AC CBPF é:

Centro Brasileiro de Pesquisas Físicas,
Rua Dr. Xavier Sigaud, 150 – URCA
22090-180 Rio de janeiro , RJ

E-mail: accbpf@cbpf.br
Website: http://ac.cat.cbpf.br

1.5.2 Ponto de Contato

A pessoa de contato para questões relacionadas a este documento é Marita Campos Maestrelli e seus dados para contato são:

Gerente da AC CBPF
Coordenação de Atividades Técnicas - CAT
Rua Dr. Xavier Sigaud, 150 – URCA
22090-180 Rio de janeiro , RJ
E-mail: ger-accbpf@cbpf.br
Telefone: (21)2141-7124

1.5.3 Responsável por determinar a adequabilidade da DPC à política

Esta DPC é elaborada pela equipe de segurança da CAT com supervisão do gerente da AC CBPF.

1.5.4 Procedimentos de aprovação da DPC

A PC/DPC é submetida á Autoridade de Gerência de Políticas da ICPEDU para

análise. Em seguida, ela é encaminhada para o Comitê Gestor para aprovação.

1.6 Definições e Acrônimos

AC Autoridade Certificadora.
AC Raiz Autoridade Certificadora Raiz da ICPEDU.
AGP Autoridade de Gerência de Polìticas.
AR Autoridade de Registro.
CAT Coordenação de Atividades Técnicas
CBPF Centro Brasileiro de Pesquisas Físicas
CEO Coordenação de Engenharai e Operações da REDERIO
CN *Common Name*.
CPD Centro de Processamento de Dados.
CSR Requisição de certificado (*Certificate Signing Request*).
DN *Distinguished Name*.
DPC Declaração de Práticas de Certificação.
FQDN Nome de domínio completo (*Fully Qualified Domain Nome*).
HSM Módulo de segurancca em hardware.
ICPEDU Infra-estrutura de Chaves Públicas para Ensino e Pesquisa.
IDC Internet Data Center
ISO International Standards Organization
ITU International Telecommunications Union
LCR Lista de Certificados Revogados.
OID Object Identifier
PC Política de Certificação.
POP-RJ Ponto de Presença da RNP do Rio de Janeiro.
PKCS *Public-Key Cryptography Standards*.
PS Polìtica de Segurança.
REDERIO backbone acadêmico e governamental do estado do RJ
RNP Rede Nacional de Ensino e Pesquisa.
SGCI Sistema de Gestão de Certificados da ICPEDU.
SSL Secure Sockets Layer
URL Uniform Resource Locator
UTC Hora Universal Coordenada (*Coordinated Universal Time*).

2. Responsabilidades referentes a publicações e repositórios

2.1 Repositórios

A AC CBPF mantem seu repositório na seguinte URL: https://ac.cat.cbpf.br/repositorio

2.2 Publicação de informações

O repositório contém as seguintes informações:

- certificado da AC CBPF;
- LCR da AC CBPF(versão atual);
- certificados emitidos pela AC CBPF;
- PC/DPC da AC CBPF atual e anteriores;

2.3 Freqüência de publicação

Os certificados são publicados imediatamente após sua emissão. A publicação da LCR será feita imediatamente após sua alteração. As mudanças nas PCs e DPCs da AC CBPF serão publicadas no prazo máximo de 2 (dois) dias úteis após sua aprovação pelo ICP EDU.

2.4 Controles de acesso aos repositórios

Todas as informações do repositório são públicas e podem ser acessadas de forma anônima apenas para consulta.O acesso ao repositório é monitorado pela equipe responsável da AC CBPF.

3. Identificação e Autenticação

3.1 Estrutura de Nomes

3.1.1 Tipos de nomes

Os titulares serão nomeados respeitando as regras do X.500[4].Os tipos de nomes estão listados no apêndice A.

3.1.2 Necessidade de que nomes sejam significativos

O CN dos certificados de usuários contém o nome completo dos mesmos. No caso de certificados emitidos para serviços o CN é composto do FQDN do servidor em questão opcionalmente com o prefixo (Nome do Serviço). Não são admitidos caracteres especiais ou de acentuação nos campos do DN. Os valores para o nome distinto da AC CBPF podem ser encontrados na tabela definida na seção A.1.

3.1.3 Anonimato dos titulares de certificado

A AC CBPF não emitirá certificados com suporte ao anonimato.

3.1.4 Regras para interpretação dos diversos formatos de nomes

Os nomes são interpretados conforme nas seções 3.1.1 e 3.1.2..

3.1.5 Unicidade dos nomes

O Distinguished Name (DN) em cada certificado emitido pela AC CBPF DEVE ser único. Nesta política da PC/DPC, dois nomes são considerados idênticos se eles diferem exclusivamente em letras maiúsculas e minúsculas, pontuação ou espaços em branco; Portanto, estes não DEVEM ser usados para diferenciar nomes. Em casos onde o nome pessoal não é suficiente para diferenciar dois certificados, números serão adicionados ao final do Common Name (CN)". Todos os titulares serão identificados de forma única durante todo o ciclo de vida da AC CBPF, e não apenas pelo período de validade do certificado.

3.1.6 Reconhecimento, autenticação e papel de marcas registradas

A AC CBPF respeitará as marcas registradas e os direitos autorais vigentes.

3.2 Validação da Identidade Inicial

3.2.1 Método para prova de posse da chave privada

O requerente deverá apresentar à AC CBPF um arquivo de requisição de certificado assinado com a chave privada que faz par a chave pública contida na requisição.

3.2.2 Autenticação da identidade organizacional

O relacionamento entre o titular e a coordenação da instituição mencionada no nome deve ser provada através de um cartão de identificação da unidade, um documento legalmente aceito ou um documento oficial institucional em papel timbrado e assinado por um representante oficial da organização. Opcionalmente, a requisição pode ser autorizada eletronicamente através da assinatura digital de um representante oficial da iunidade de posse de um certificado válido emitido pela AC CBPF.

3.2.3 Autenticação da identidade individual

O requerente deverá apresentar pessoalmente sua identidade funcional do CBPF ou outro documento de identidade oficial, como RG ou CNH, email institucional e comprovação de vínculo com a institutição, na AR
As cópias de todos os documentos necessários no processo de autenticação serão arquivadas pela AR.

3.2.4 Dados dos titulares de certificado que não são verificados

Apenas o nome do requerente, e-mail e o vínculo institucional **são verificados**. Os demais dados recebidos não são verificados.

3.2.5 Validação de autoridade

Uma declaração assinada por um representante legal da instituição reconhecido pela AC ou AR, ou equivalente, é suficiente para validação da autoridade.

3.2.6 Critérios para interoperabilidade

Não estipulado.

3.3 Identificação e Autenticação para Requisição de Substituição de Chaves

3.3.1 Identificação e autenticação para troca de chaves de rotina

Toda requisição de certificado é tratada como uma nova requisição. Desta forma não é permitida a simples substituição da chave.

3.3.2 Identificação e autenticação para troca de chaves após revogação

A requisição recebida após a revogação será tratada como uma nova requisição.

3.4 Identificação e Autenticação para Requisição de Revogação

A solicitação de revogação do certificado de uma AC ou AR deve ser feito por meio de ofício assinado pelo representante legítimo (diretor/coordenador) da Unidade organizacional à qual a AC ou AR está vinculada.

4. Requisitos Operacionais do Ciclo de Vida do Certificado

4.1 Procedimentos do requerente para solicitar o certificado

4.1.1 Quem pode submeter uma solicitação de certificado

Qualquer pesquisador, tecnologista, técnico ou funcionário administrativo do CBPF devidamente autorizado pelo representante legal da unidade organizacional a qual está vinculado, pode solicitar certificado pessoal.
Os administradores da rede computacional do CBPF podem solicitar certificados para determinados serviços de Rede.

4.1.2 Processo de solicitação e responsabilidades

O requerente deverá se dirigir pessoalmente as instalações da AR-CBPF, munido do documento de identificação (carteira de identidade), o arquivo contendo a requisição de certificado e um endereço e-mail válido do CBPF, que deve ser aderente às normas estabelecidas na PC/DPC da AC CBPF .

4.2 Processamento da solicitação pela AR

4.2.1 Realização das funções de identificação e autenticação

A identificação e autenticação do requerente será realizada pessoalmente nas instalações da AC CBPF.

4.2.2 Aprovação ou rejeição das solicitações

Para aprovação da solicitação, a AC solicitante deve estar em conformidade com a Política de Segurança e com as diretrizes expressas no Documento de Requisitos Mínimos da ICPEDU. As políticas adotadas para o estabelecimento desta conformidade devem estar descritas na sua PC.
Se a autenticação da informação se mostrar inexata, ou a parte requisitante não for capaz de atender os requisitos dentro de 5 (cinco) dias úteis após o recebimento da solicitação pela AR, o pedido deve ser recusado
Todas as requisições aprovadas e rejeitadas serão registradas na AC CBPF.

4.2.3 Tempo para processamento das solicitações

O tempo esperado para o processamento de uma solicitação é de até 5(cinco) dias úteis.

4.3 Processamento da solicitação pela AC

4.3.1 Ações da AC durante a emissão de certificado

Apenas solicitações assinadas pela AR CBPF são processadas pela AC CBPF.

4.3.2 Notificação da emissão do certificado pela AC para o solicitante

A emissão do certificado é notificada ao solicitante através de correio eletrônico.

4.4 Aceitação do certificado

4.4.1 Conduta que constitui a aceitação do certificado

A aceitação por parte do Titular do certificado se dará pela assinatura do termo de Titularidade na presença dos validadores presenciais da AR, no ato do seu recebimento.

4.4.2 Publicação do certificado pela AC

Os certificados emitidos serão publicados imediatamente após a sua emissão.

4.4.3 Notificação da emissão do certificado pela AC para outras entidades

Nenhuma outra entidade é notificada após a emissão de um certificado.

4.5 Utilização de pares de chaves e de certificados

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

É responsabilidade unicamente do usuário a manutenção da sua chave privada, que só deve ser utilizada para os fins descritos nesta PC/DPC.A ocorrência de qualquer anormalidade ou suspeita de comprometimento da chave privada, deve ser imediatamente comunicada a AC CBPF.

4.5.2 Responsabilidade pela utilização das chaves públicas e dos certificados por parte das entidades confiantes

As entidades confiantes devem:

- Estar cientes das informações presentes neste documento.
- Verificar a última versão da LCR antes de aceitar um certificado como sendo válido.
- Observar as políticas estabelecidas para o certificado.

4.6 Reemissão de certificados por troca do prazo de validade

4.6.1 Circunstância para renovação de certificados

A AC CBPF não renova certificados de usuários e serviços. O titular pode solicitar um novo certificado de acordo com os procedimentos descritos nesta polìtica.

4.6.2 Quem pode solicitar renovação

Não se aplica.

4.6.3 Processamento de solicitações de renovação

Não se aplica.

4.6.4 Notificação de nova emissão de certificado para o titular

Não se aplica.

4.6.5 Conduta que constitui aceitação de um certificado renovado

Não se aplica.

4.6.6 Publicação do certificado renovado pela AC

Não se aplica.

4.6.7 Notificação pela AC da emissão de um certificado para outras entidades

Não se aplica.

4.7 Reemissão de certificados por troca de chaves

4.7.1 Circunstâncias para substituição das chaves criptográficas

A AC CBPF não realiza a troca de chaves de certificados. O titular pode solicitar um novo certificado de acordo com os procedimentos descritos nesta polìtica.

4.7.2 Quem pode solicitar a certificação de uma nova chave pública

Não se aplica.

4.7.3 Processamento de solicitações de substituição de certificados

Não se aplica.

4.7.4 Notificação de nova emissão de certificado para o titular

Não se aplica.

4.7.5 Conduta para a aceitação de um novo certificado

Não se aplica.

4.7.6 Publicação do novo certificado

Não se aplica.

4.7.7 Notificação pela AC da emissão de um certificado para outras entidades

Não se aplica.

4.8 Reemissão de certificados por troca de dados

4.8.1 Circunstâncias para modificação de certificados

A AC CBPF não realiza a modificação de certificados. O titular pode solicitar um novo certificado de acordo com os procedimentos descritos nesta polìtica.

4.8.2 Quem pode solicitar a modificação de um certificado

Não se aplica.

4.8.3 Processamento de solicitações de modificação de certificados

Não se aplica.

4.8.4 Notificação de nova emissão de certificado para o titular

Não se aplica.

4.8.5 Conduta para a aceitação de um novo certificado modificado

Não se aplica.

4.8.6 Publicação do certificado pela AC

Não se aplica.

4.8.7 Notificação pela AC da emissão de um certificado para outras entidades

Não se aplica.

4.9 Revogação e Suspensão

4.9.1 Circunstâncias para revogação de certificados

Um certificado digital emitido pela AC CBPF é revogado nas seguintes circunstâncias:

- houver comprometimento da chave privada ou da sua mídia armazenadora;
- for constatado o não cumprimento da DPC
- for constatada a emissão imprópria ou defeituosa
- houver dissolução da AC emissora do certificado
- quando qualquer informação contida no certificado não for mais válida;
- se houver informações incorretas no certificado
- por medida de segurança, deliberado pelo gerente da AC;

- por solicitação do titular ou do responsável pela Unidade do CBPF, que não deseja manter vínculo com a AC

4.9.2 Quem pode solicitar revogação

[A revogação de um certificado digital emitido pela AC CBPF pode ser solicitada:

- . determinação do Comitê Gestor do ICPEDU
- pelo seu titular ou responsável;
- pelos administradores da AC CBPF, quando julgarem necessário;
- pela representante legal do CBPF;
- pela AR CBPF;
- por uma entidade confiante;
- por determinação judicial;

4.9.3 Processamento de solicitações de revogação

O pedido de revogação, eletrônico ou papel, deve ser assinado pelo responsável ou representante legal a qual está vinculada a AC. Todas as solicitações serão registradas.

4.9.4 Prazo para solicitação de revogação

A solicitação de revogação deve ser feita à AC CBPF no prazo máximo de dois dias úteis quando houver constatação de um evento que motive a revogação.

4.9.5 Prazo para a AC processar a solicitação de revogação

O processamento das solicitações de revogação de certificados são processadas em até um dia útil.

4.9.6 Requisitos para verificação de revogação por entidades confiantes

A parte confiante deve sempre utilizar a LCR mais recente da AC responsável pela emissão do certificado para verificar a validade do mesmo. A autenticidade e validade da LCR deve ser verificada pela assinatura da AC e pelo seu período de validade.

4.9.7 Freqüência de emissão de LCRs

A LCR é emitida sempre que um conjunto de certificados (um ou mais certificados) é revogado em um curto espaço de tempo. Adicionalmente é emitida uma LCR a cada 30 (trinta) dias.

4.9.8 Latência máxima para LCRs

As LCRs são publicadas no repositório em no máximo 30 minutos após a sua emissão.

4.9.9 Mecanismos para verificação on-line do status de certificados

A AC CBPF não disponibiliza serviços de verificação de status em tempo real.

4.9.10 Obrigações da entidade confiante de verificar on-line o status

Não se aplica.

4.9.11 Outras formas de comunicação de revogação

Não existem outras formas.

4.9.12 Procedimentos adicionais no caso de comprometimento da chave privada

Não estipulado.

4.9.13 Circunstâncias para suspensão de certificados

Não de aplica.

4.9.14 Quem pode solicitar suspensão

Não de aplica.

4.9.15 Processamento de solicitações de suspensão

Não de aplica.

4.9.16 Limites para o período de suspensão

Não de aplica.

4.10 Serviços de status de certificado

4.10.1 Características operacionais

A AC CBPF utiliza LCRs como único mecanismo de verificação do estado dos certificados emitidos.

4.10.2 Disponibilidade do serviço

A LCR estará disponível no repositório da AC que oferece o serviço continuamente mesmo durante manutenções programadas, exceto por falhas fora do controle da AC.

4.10.3 Características operacionais

Não estipulado.

4.11 Encerramento do vínculo com a AC

O vínculo é encerrado quando ocorre expiração ou revogação de um certificado.

4.12 Custódia e recuperação de chaves

4.12.1 Políticas e práticas para custódia e recuperação de chaves

A AC CBPF não oferece os serviços de custódia e recuperação de chaves.

4.12.2 Políticas e práticas para custódia e recuperação de chaves de sessão

Não se aplica.

5. Controles operacionais, gerenciais e de instalações físicas

5.1 Controles de Segurança Física

5.1.1 Localização e construção das instalações físicas

A AC CBPF está localizada em uma sala de servidores da Coordenação de Atividades Técnicas(CAT) com acesso restrito aos membros dessa coordenação.

5.1.2 Acesso físico

O acesso físico as depêndencias da AC CBPF obedece a política de segurança dos servidores da CAT que permite a entrada somente a seus técnicos.

5.1.3 Energia e refrigeração

A AC CBPF, os repositórios e a AR estão localizados em ambiente seguro que, além de conectados à rede elétrica, dispõe dos seguintes recursos:
a) gerador principal;
b) sistema de no-breaks;
c) sistema de aterramento e proteção a descargas atmosféricas;
d) iluminação de emergência.

O sistema de ar condicionado é tolerante a falhas com controle de calor e umidade, independente do sistema de ar condicionado da construçãoao onde está localizado.
Adicionalmente, as facilidades listadas seguem as especificações de disponibilidade definidas no documento de Políticas de Segurança.

5.1.4 Exposição à água

A sala da AC CBPF possui piso elevado para evitar exposição à água.

5.1.5 Prevenção e proteção contra incêndio

A sala da AC CBPF, assim como toda CAT possui sensores que detectam a presença de fumaça. Na ocorrência da mesma, alarmes são disparados.

5.1.6 Armazenamento de mídia

A CAT possui um cofre para o armazenamento e proteção de mídias eletrônicas removíveis.

5.1.7 Descarte de lixo

Material contendo informação potencialmente confidencial e dados que devem ser protegidos (dados relevantes como chaves privadas ou passphrases, ou dados pessoais) são descartados de forma a garantir que a informação não seja obtida ou reutilizada.

5.1.8 Cópias de segurança em outras instalações

As cópias de segurança das informações e software serão feitas e testadas regularmente e serão mantidas em um ambiente distinto da sala de certificação, onde se encontram o módulo de segurança criptográfico (HSM) e sistema de gerenciamento de certificados (SGCI)..

5.2 Procedimentos de Controle

5.2.1 Papéis de Confiança

A AC CBPF 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. A divisão de responsabilidades entre os quatro perfis é a seguinte:

Gerente:
Servidor técnico administrativo designado pelo Diretor do CBPF para ser o responsável pela AC CBPF, que formará os grupos de administradores, operadores e auditores. Ele também é responsável pela aprovação dos relatórios da AC CBPF. Adicionalmente, depois de ter recebido os relatórios de auditorias, ele é responsável por encaminhar estes relatórios ao CG da ICPEDU.

Administrador:
O administrador é responsável pela instalação, configuração, backup e manuteção dos equipamentos e software de gestão do ciclo de vida do certificado digital. Também define as políticas e cria ACs, além de definir ou trocar os grupo de operadores e auditores. Adicionalmente, é responsável pelos relatórios de operação da AC CBPF.

Auditor:
O auditor é responsável pela auditoria do ciclo de vida do certificado digital, das chaves criptográficas e de todas as operações AC CBPF.

Operador:
Os operadores são os responsáveis pelo uso da chave privada da AC CBPF para a emissão de LCRs e de certificados digitais.

5.2.2 Número de pessoas necessárias por tarefa

Para as tarefas de geração e utilização de chaves privadas da AC CBPF , o controle multiusuário, atraves do uso de segredo compartilhado, será utilizado pela Coordenação de Atividades Técnicas – CAT. As demais tarefas da AC CBPF podem ser executadas por um único funcionário.

5.2.3 Identificação e autenticação para cada papel

Cada membro de um grupo deve ter um smartcard para se autenticar perante o módulo de segurança criptográfica. Quanto ao sistema de

gerenciamento de certificados digitais, cada administrador possuirá uma senha secreta.

5.2.4 Papéis que requerem separação de responsabilidade

As pessoas que exercem papéis de administrador, gerente ou operador, não exercem papel de auditor.

5.3 Controle de Pessoal

5.3.1 Requisitos de qualificação, experiência e conformidade com obrigações governamentais

O pessoal envolvido na operação da AC CBPF é pertencente ao quadro de funcionários do CBPF. Desta forma os requisitos de qualificação, experiência e conformidade com obrigações governamentais foram verificados na sua admissão.

5.3.2 Procedimentos de verificação de antecedentes

O pessoal envolvido na operação da AC-CBPF é pertencente ao quadro de funcionários do CBPF. Desta forma a verificação de antecedentes foi realizada na sua admissão.

5.3.3 Requisitos de treinamento

Todo o pessoal envolvido na operação da AC-CBPF recebe um treinamento referente à operação do sistema de certificação digital empregado.

5.3.4 Requisitos de freqüência de treinamento

Sempre que houver alterações em procedimentos ou quaisquer modificações na plataforma computacional, um novo treinamento será realizado.

5.3.5 Freqüência e seqüência para revezamento de trabalho

Não estipulado.

5.3.6 Sanções para ações não autorizadas

O acesso de um indivíduo envolvido na operação da AC CBPF será imediatamente cancelado quando verificado a ocorrência de uma ação não

autorizada. As medidas administrativas cabíveis são tomadas pela administração do CBPF.

5.3.7 Requisitos para prestadores de serviços independentes

Os prestadores de serviços devem proceder de acordo com as normas da política de segurança da CAT, emitndor relatórios das suas operações e todas as visitas serão registradas e monitoradas pela equipe da CAT..

5.3.8 Documentação fornecida aos funcionários

A AC CBPF disponibilizará para todo o seu pessoal:

1. sua DPC/PC;
2. PS da ICPEDU;
3. documentação operacional relativa a suas atividades;
4. contratos, normas e políticas relevantes para suas atividades.

5.4 Sistemas de auditoria e procedimentos para registro de eventos

5.4.1 Tipos de eventos registrados

a. Todas as ações executadas pelo pessoal da AC CBPF no desempenho de suas atribuições são registradas de modo que cada ação esteja associada à pessoa que a realizou;

b. A AC CBPF registrará, em arquivos de auditoria, todos os eventos relacionados à segurança do sistema de certificação. Dentre outros, os seguintes eventos devem obrigatoriamente estar incluídos no arquivo de auditoria:

i. Erro: Quando ocorre um erro na execução de um comando;
ii. Verbose: Mensagens durante a execução de todas as operações no HSM;
iii. Warning: Mensagens de aviso enviadas aos clientes conectados;
iv. Connection: Quando as conexões são iniciadas e finalizas;
v. Commands: Todos os comandos que são enviados ao HSM;
vi. Answer: Todas as mensagens de resposta (finalização da execução de um comando) a um comando;
vii. Logs Gerais: Por exemplo: opções selecionadas na configuração inicial do sistema;
viii. Iniciação e desligamento do sistema de certificação;
ix. Tentativas de criar, remover, definir senhas ou mudar os privilégios de sistema dos administradores, operadores e auditores;

x. Mudanças na configuração da AC ou da chave privada de assinatura;
xi. Mudanças nas políticas de criação de certificados;
xii. Geração de chaves;
xiii. Emissão e revogação de certificados;
xiv. Geração de LCR.

c) Registros de destruição de mídia;
d) Ativação ou desativação dos registros automáticos de auditoria.

5.4.2 Freqüência de análise dos registros de auditoria

Os registros de eventos devem ser analisados mensalmente.

5.4.3 Período de arquivamento de registros de auditoria

Os registros de eventos devem ser retidos por cinco anos.

5.4.4 Proteção de registros de eventos

Os registros de eventos são armazenados nos discos dos servidores que hospedam o sistema de certificação digital que tem acesso restrito e registrado em livro ao grupo de funcionários da AC CBPF.

5.4.5 Procedimentos para cópias de segurança de registros de eventos

As cópias de segurança dos registros de eventos são armazenados de forma cifrada em mídias eletrônicas. A integridade das cópias de segurança é verificada mensalmente.Os procedimentos de cópia são documentados, para facilitar o processo de auditoria e implantação..

5.4.6 Sistema de recolhimento de registros de eventos (interno ou externo)

O sistema de recolhimento de registros de eventos é interno, ou seja, feito pela própria AC CBPF.

5.4.7 Notificação do sujeito causador do evento

Não estipulado.

5.4.8 Avaliação de vulnerabilidades

Todos os registros serão 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 CBPF, além da plataforma hospedeira do seu repositório. Também serão analisados os registros do ambiente seguro.

5.5 Arquivamento de Registros

5.5.1 Tipos de registros armazenados

Além dos registros de eventos para auditoria mencionados na seção 5.4.1 também são arquivados:
• documentação de credenciamento dos titulares;
• documentação relacionada a solicitação de certificados;
• solicitações de revogação;
• listas de certificados revogados;
• certificados emitidos;
• changelogs das PC/DPCś;

5.5.2 Período de retenção dos registros arquivados

Os registros devem ser retidos por cinco anos.

5.5.3 Proteção dos registros armazenados

Os registros devem ser guardados em local seguro na CAT . Os registros são acessíveis somente pelo grupo de auditores e administradores.

5.5.4 Procedimentos para cópias dos registros armazenados

As cópias de segurança dos registros de eventos são armazenados de forma criptografada em mídias óticas. A integridade das cópias de segurança é verificada anualmente. É feita uma cópia de segurança completa mensalmente.

5.5.5 Requisitos para datação dos registros armazenados

Os registros devem ser datados pela hora oficial internacional (UTC).

5.5.6 Sistema de recolhimento de registros arquivados (interno ou externo)

O sistema de coleta de informações para arquivamento é interno, ou seja, deverá ser realizado pela própria AC CBPF.

5.5.7 Procedimentos para obtenção e verificação dos registros armazenados

Os registros poderão ser obtidos pelo pessoal envolvido na operação da AC CBPF. O procedimento de verificação consiste de verificar a integridade das cópias de segurança com auxílio de funções de resumo criptográfico (*hash functions*).

5.6 Nova Chave Pública para a AC

Um novo par de chaves para a AC CBPF deve ser gerado seis meses antes do ponto de atualização de seu certificado.

5.7 Comprometimento e Recuperação de Desastre

5.7.1 Procedimentos para tratamento de incidentes e comprometimentos

Na ocorrência de incidentes e comprometimentos, esses eventos devem ser imediatamente notificados à gerência da AC CBPF e à Chefia da Coordenação de Atividades Técnicas - CAT do CBPF, além da gerência de Incidentes de Segurança da REDERIO - CEO. Caso o incidente seja relacionado a segurança de rede e seja causado por um ataque externo, o evento também deve ser notificado ao Centro de Atendimento a Incidentes de Segurança (CAIS) da RNP. Em caso de comprometimento das instalações da AC CBPF, a equipe responsável pela mesma deverá iniciar o processo de recuperação a partir das cópias de segurança.

5.7.2 Procedimentos para o caso de comprometimento de recursos computacionais, software e/ou dados

Seguir as Normas de Segurança da CEO/REDERIO.

5.7.3 Procedimentos para o comprometimento de chave privada de entidade

Em caso de comprometimento da chave privada da AC CBPF, o seu certificado é revogado imediatamente. Neste caso, o CG da ICPEDU, as entidades confiantes e os titulares são notificados imediatamente.

5.7.4 Procedimentos para continuidade de negócio após desastre

Seguir as Normas de Segurança da CEO/REDERIO.

5.8 Finalização da AC ou AR

Ao encerrar suas operações a AC CBPF deve realizar as seguintes atividades:

1. notificar o CG da ICPEDU;
2. Notificar as Ars credenciadas;
3. notificar titulares de certificados e entidades confiantes;
4. notificar a Chefia da Coordenação de Atividades Técnicas - CAT do CBPF;
5. revogar todos os certificados emitidos;
6. emitir e publicar a sua LCR;
7. destruir qualquer cópia da sua chave privada;
8. arquivar os registros de forma segura.

6. Controles Técnicos de Segurança

6.1 Geração e Instalação do Par de Chaves

6.1.1 Geração do par de chaves

Os pares de chaves criptográficas da AC CBPF e de suas ARs subordinadas devem ser gerados em hardware criptográfico desenvolvido no contexto do grupo de trabalho ICPEDU. A AC CBPF seguirá o procedimento padrão para geração de pares de chaves por este equipamento. Os pares de chaves de certificados de usuários e de serviços são gerados pelos próprios titulares. O algoritmo a ser utilizado para as chaves criptográficas está definido em [2].

6.1.2 Fornecimento de chave privada ao titular

Não se aplica, uma vez que as chaves criptográficas são geradas pelo próprio titular.

6.1.3 Entrega da chave pública à Autoridade Certificadora

As chaves públicas são entregues à AC CBPF utilizando o formato PKCS#10[4].

6.1.4 Divulgação da chave pública da AC às partes confiantes

A chave pública da AC-CBPF é publicadas no repositório da AC-CBPF cujo URL é definido em Seção 2.1.

6.1.5 Tamanho das chaves

O tamanho da chave pública da AC CBPF é de 2048 bits.

6.1.6 Geração dos parâmetros de chave pública e verificação de qualidade

As chaves são geradas de acordo com os padrões definidos no documento Padrões e Algoritmos Criptográficos da ICPEDU [2].

6.1.7 Propósito de uso de chaves

A chave privada da AC CBPF só pode ser utilizada para assinar certificados e LCRs. As chaves devem ser utilizadas conforme o conteúdo do campo "key usage"(ver A2) e devem ser documentados.

6.2 Proteção de Chaves Privadas e Controles Tecnológicos de módulos Criptográficos

6.2.1 Padrões e controles de módulos criptográficos

A AC CBPF utiliza um hardware criptográfico conforme estabelecido na Seção 6.2.11.

6.2.2 Número de operadores para o Controle da Chave Privada

A chave privada da AC CBPF é liberada para uso por um número mínimo de 2 operadores simultâneos de um total de 6.

6.2.3 Custódia de chaves privadas

A AC CBPF não realiza a custódia de chaves privadas.

6.2.4 Cópias de segurança de chaves privadas

O módulo de segurança criptográfica (HSM) permite que se faça, através do uso de um segundo HSM (HSM backup), várias cópias cifradas de toda a base de dados interna do HSM (HSM operacional). Estas cópias podem ser utilizadas para, em caso de falha no HSM original, poder-se colocar o segundo HSM a operar com a mesma chave privada.

A chave privada do HSM operacional é cifrada utilizando-se a chave pública do HSM backup e armazenada em mídia digital e sua recuperação deve ser autorizada formalmente pelo gerente da AC CBPF.

6.2.5 Arquivamento de chaves privadas

A chave privada da AC CBPF é armazenada somente no HSM principal e na HSM backup.

6.2.6 Transferência de chaves privadas de/para módulos criptográficos

A única forma de exportação e importação da chave privada da AC CBPF é através de uma cópia de segurança sob a responsabilidade do grupo de administradores, conforme descrito na Seção 6.2.4. A chave privada será mantida cifrada quando fora do módulo criptográfico.

6.2.7 Armazenamento de chaves privadas em módulos criptográficos

A chave privada da AC CBPF deverá ser armazenada na forma cifrada na memória permanente do módulo criptográfico.

6.2.8 Método para ativação de chaves privadas

A chave privada da AC CBPF é ativada pelo grupo de operadores do HSM, conforme a Seção 6.2.2. Cada membro do grupo possui um smartcard e respectivo PIN que são utilizados em conjunto para liberar o uso da chave privada.

6.2.9 Método para desativação de chaves privadas

Para desativar a chave privada da AC CBPF, o operador do SGCI deve executar o comando de descarregar a chave por meio do sistema de gerenciamento remoto do HSM (OpenHSMd Client).
Além disso, a chave privada é automaticamente desativada quando o HSM é desligado ou o número de usos é alcançado.

6.2.10 Método para destruição de chaves privadas

A chave privada da AC CBPF é destruída através da reinicialização (sendo consequentemente apagadas) do HSM que a armazena.

6.2.11 Avaliação requerida de módulos criptográficos

A AC CBPF utiliza hardware criptográfico construído de acordo com as recomendações do FIPS 140-2, nível 3[5] ou compatível.

6.3 Outros Aspectos do Gerenciamento de Chaves

6.3.1 Armazenamento de chaves públicas

As chaves públicas da AC CBPF são armazenadas permanentemente, após a expiração dos certificados correspondentes, para verificação de assinaturas geradas durante seu prazo de validade.

6.3.2 Períodos operacionais de certificados e períodos de utilização de pares de chaves

A chave privada da AC CBPF deve ser utilizada apenas durante o período de validade do certificado correspondente. A chave pública da AC CBPF pode ser utilizada durante todo o período de tempo determinado pela legislação aplicável, para verificação de assinaturas geradas durante o prazo de validade do certificado correspondente. Os certificados emitidos pela AC CBPF terão um prazo de validade máximo de 2 anos.

6.4 Dados de Ativação

6.4.1 Geração e instalação dos dados de ativação

Os PINs e senhas são definidos no documento de cerimônia de criação da chave priivada da AC.

6.4.2 Proteção dos dados de ativação

Os dados de ativação são protegidos contra cópia e perda indevidas. O acesso aos dados de ativação são feitos da mesma forma que os utilizados para acesso ao HSM.

6.4.3 Outros aspectos de dados de ativação

Não estipulado.

6.5 Controles de Segurança computacional

6.5.1 Requisitos técnicos específicos de segurança computacional

O computador que hospeda o sistema de gerenciamento de certificados digitais (SGCI) é de uso exclusivo da AC CBPF. Este computador não é conectado em rede e não é modificado durante a sua vida útil. A substituição do computador, por outro deve ser feita a partir de um cerimônia especialmente concebida para este fim.

6.5.2 Classificação de segurança computacional

O computador contendo a AC CBPF, antes de ser utilizado para gerar o certificado da AC, é verificado e corrigido quanto a todas as falhas conhecidas de segurança.

6.6 Controles técnicos de ciclo de vida

6.6.1 Controles de desenvolvimento de sistemas

A AC CBPF utilizará o SGCI como sistema de gerenciamento de certificados digitais, e um módulo criptográfico desenvolvido no contexto do grupo de trabalho ICPEDU.

6.6.2 Controles do gerenciamento de segurança

Os controles de segurança da CAT, onde está instalada a AC CBPF, serão renovados conforme as políticas de segurança estabelecidas

6.6.3 Controles de segurança de ciclo de vida

Não estipulado.

6.7 Controles para a Segurança da Rede de Comunicações

A rede do CBPF deve ser protegida por um filtro de pacotes e possuirá um sistema de detecção de intrusões (IDS). Periodicamente é realizada uma varredura (*scan*) em busca de vulnerabilidades conhecidas.

6.8 Carimbo do Tempo

A data e hora dos eventos e dados dos sistemas computacionais online devem ser obtidas através de um relógio sincronizado pelo protocolo NTP a uma fonte

de tempo confiável. Os relógios dos sistemas computacionais off-line e do módulo criptográfico serão atualizados sempre que iniciados.

7. Perfis dos Certificados, LCR e OCSP

7.1 Perfil dos Certificados

7.1.1 Versão

A AC CBPF emitirá certificados digitais X.509 versão 3.

7.1.2 Extensões

As extensões são definidas na seção A.2.2

7.1.3 Identificadores de objeto dos algoritmos

O certificado da AC CBPF é assinado com o uso do algoritmo definido no documento Padrões e Algoritmos Criptográficos da ICPEDU [2].

Função	**Nome**	**OID**
Função Hash	Id-SHA1	1.3.14.3.2.26
	Id-sha256	2.16.840.1.101.3.4.2.1
	Id-sha512	2.16.840.1.101.3.4.2.3
Criptografia	rsaEncryption	1.2.840.113549.1.1.1
Assinatura	sha1WithRSAEncryption	1.2.840.113549.1.1.5
	sha2WithRSAEncryption	1.2.840.113549.1.1.13

Tabela 7.1.3.1 OID dos algoritmos utilizados

7.1.4 Formato dos nomes

O formato dos dados estão definidos no Apêndice A1.

7.1.5 Restrições para nomes

Não devem ser utilizados sinais de acentuação, tremas ou cedilhas. Além dos caracteres alfanuméricos e espaço em branco, poderão ser utilizados somente os símbolos:

Símbolo	**Descrição**	**Código NBR9611 (hexadecimal)**
	Espaço em branco	20

!	Ponto de exclamação	21
“	Aspas	22
#	Cerquila	23
$	Dólar	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

Tabela 7.1.5.1 Outros símbolos permitidos

7.1.6 Identificador de objeto da PC

Veja Item 1.2.

7.1.7 Uso da extensão *Policy Constraints*

Não se aplica.

7.1.8 Sintaxe e semântica dos qualificadores de política

Não se aplica.

7.1.9 Semântica de Processamento para a extensão crítica Certificate Policies

Não se aplica.

7.2 Perfil da LCR

O formato da LCR emitida pela AC CBPF está em conformidade com a RFC 5280[3].

7.2.1 Versão

Versão 2.

7.2.2 Extensões da LCR e de entradas da LCR

As extensões para a LCR da AC CBPF podem ser encontradas na tabela A.4 da seção A.3

7.3 Perfil da OCSP

7.3.1 Versão

Não se aplica.

7.3.2 Extensões OCSP

Não se aplica.

8. Auditoria de conformidade e outras avaliações

8.1 Freqüência ou circunstâncias das avaliações

A AC CBPF é auditada anualmente.

8.2 Identidade e qualificações do avaliador

As avaliações são realizadas por grupo de avaliadores, especialmente treinados para este fim.

8.3 Relação entre o avaliador e a entidade avaliada

O avaliador não deve ser responsável pela operação da AC CBPF, porem ambos são da CAT..

8.4 Tópicos cobertos na avaliação

Verificação da conformidade da AC CBPF com esta DPC e com as políticas e regras estabelecidas no contexto da ICPEDU. Aspectos como gerência das chaves e gerência do ciclo de vida do certificado devem ser avaliados com especial cuidado.

8.5 Ações tomadas resultantes de deficiências

Na ocorrência de qualquer deficiência, notifica-se o responsável pela AC CBPF para tomar as ações cabíveis.

8.6 Comunicação dos resultados

Os resultados da avaliação devem ser entregues ao gerente da AC CBPF e ao Comitê Gestor da ICPEDU.

9. Aspectos Legais e Assuntos Gerais

9.1 Taxas

9.1.1 Taxas de emissão e renovação de certificados

Não serão cobradas.

9.1.2 Taxas para acesso aos certificados

Não se aplica.

9.1.3 Taxas revogação ou informações de estado

Não se aplica.

9.1.4 Outras taxas

Não se aplica.

9.1.5 Política de reembolso

Não se aplica.

9.2 Responsabilidade Financeira

9.2.1 Cobertura de Seguro

Não se aplica.

9.2.2 Outros ativos

Não se aplica.

9.2.3 Cobertura de Seguro ou garantia para entidades finais

Não se aplica.

9.3 Informações confidenciais

9.3.1 Escopo de informações confidenciais

Fazem parte do escopo de informações confidenciais:

- informações relativas a solicitações de certificados;
- registros de trilhas de auditoria;
- relatórios de auditorias;
- planos de contingência e planos de recuperação de desastre;
- medidas de segurança relativas:
  à operação de hardware e software da AC CBPF;
  aos serviços de certificação.

9.3.2 Informações fora do escopo de informações confidenciais

São consideradas informações não confidenciais:

- certificados emitidos;
- listas de certificados revogados;
- versões publicadas da PC/DPC.

9.3.3 Responsabilidade de proteção de informações confidenciais

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

9.4 Privacidade das Informações Pessoais

9.4.1 Plano de Privacidade

O titular de certificado e seu representante legítimo terão amplo acesso a quaisquer dos seus próprios dados e identificações, e poderão autorizar a divulgação de seus registros a outras pessoas.
Autorizações formais podem ser apresentadas de três formas:
a) por meio eletrônico, contendo assinatura válida garantida por certificado reconhecido pela ICPEDU;
b) por meio de pedido escrito com firma reconhecida;
c) através de formulário eletrônico seguro, desde que comprovada autenticidade do autorizador.
Nenhuma liberação de informação é permitida sem autorização formal.

9.4.2 Informação tratada como privada

Com exceção da informação presente no certificado, que é pública, toda informação provida pelo titular do certificado não liberada formalmente é tratada como privada, devendo ser mantida no mesmo nível de qualquer informação confidencial.

9.4.3 Informação não considerada privada

É toda aquela que seu titular de certificado ou representante legítimo liberar formalmente como descrito na seção 9.4.1.

9.4.4 Responsabilidade de proteção de informação privada

A AC CBPF é responsável pela proteção de qualquer informação considerada privada.

9.4.5 Aviso e consentimento para o uso de informação privada

Ver Seção 9.4.1.

9.4.6 Circunstâncias para revelação de informações confidenciais em processos judiciais e administrativos

Não estipulado.

9.4.7 Outras Circunstâncias para revelação de informações

Não estipulado.

9.5 Direitos de Propriedade Intelectual

Em conformidade com as regras estabelecidas pelo CBPF.

9.6 Representações e Garantias

9.6.1 Garantias de AC

Não estipulado.

9.6.2 Garantias de AR

Não estipulado.

9.6.3 Garantias de titulares de certificado

Não estipulado.

9.6.4 Garantias de entidades confiantes

Não estipulado.

9.6.5 Garantias de outros participantes

Não estipulado.

9.7 Renúncia das Garantias

Não estipulado.

9.8 Limitações das Responsabilidades

Não estipulado.

9.9 Indenização

Não estipulado.

9.10 Finalização

9.10.1 Prazo de validade

Esta PC/DPC entra em vigor no momento da sua publicação e é válida até que uma nova PC/DPC seja publicada ou seja revogada por determinação explícita do Comitê Gestor.

9.10.2 Finalização

Os certificados emitidos no período de validade de uma DPC permanecem sujeitos às suas determinações até o final do período de validade do certificado.
As provisões de PCs e DPCs são válidas até que uma nova versão seja publicada ou que sejam revogadas por determinação explícita da AC imediatamente superior ou do Comitê Gestor da ICPEDU.

9.10.3 Efeitos de finalização e provisões remanescentes

Não estipulado.

9.11 Notificações Individuais e Comunicações com Participantes

As notificações serão feitas por e-mail.

9.12 Emendas

9.12.1 Procedimento para emendas

Compete a AC CBPF propor alterações à DPC.
A nova versão resultante das alterações deve ser encaminhada ao CG da ICPEDU para aprovação.
Alterações menores, como correções meramente ortográficas, não são consideradas emendas.

9.12.2 Período e mecanismo de notificação

Novas versões da PC/DPC são informadas no repositório da AC CBPF.

9.12.3 Circunstâncias nas quais o identificador de objeto deve ser modificado

Sempre que surgirem novas versões o identificador de objeto deverá ser modificado.

9.13 Procedimentos para Resolução de Disputas

Nãoestipulado.

9.14 Leis Governamentais

A AC CBPF respeita a legislação vigente no país.

9.15 Conformidade com as leis aplicáveis

Não estipulado.

9.16 Provisões Diversas

9.16.1 Concordância completa

Não estipulado.

9.16.2 Delegação de direitos e obrigações

Não estipulado.

9.16.3 Acordo entre as partes em caso de revogação de cláusula pela justiça

Não estipulado.

9.16.4 Responsabilidades relacionadas a encargos jurídicos

Não estipulado.

9.16.5 Força maior

Não estipulado.

9.15 Outras Provisões

Não estipulado.

10. Controle de Mudanças

Seção	**Mudança**	**Autor**	**Data**
[Insira a seção alterada aqui]	[Insira a mudança aqui]	[Autor]	01/01/01
[Insira a seção alterada aqui]	[Insira a mudança aqui]	[Autor]	01/01/01
[Insira a seção alterada aqui]	[Insira a mudança aqui]	[Autor]	01/01/01

Referências

[ICPEDU08] Autoridade de Gerência de Políticas da ICPEDU*, Requisitos Mínimos para Políticas de Certificado e Melhores Práticas de Certificação*, Versão 1.0 RC1, 20 de Agosto de 2008.

[1] S. Chokani, W. Ford, R. Sabett, C. Merrill, and S. Wu. Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework. RFC 3647, Internet Engineering Task Force, 2003.

[2] Comitê Técnico de Políticas da ICPEDU. Padrões e algoritmos criptográficos da ICPEDU. Relatório técnico, ICPEDU, RNP, Rio de Janeiro, 2006.

[3] R. Housley, W. Polk, W. Ford, and D. Solo. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. RFC 3280, Internet Engineering Task Force, 2002.

[4] M. Nystrom and B. Kaliski. PKCS #10: Certification Request Syntax Specification. RFC 2986, Internet Engineering Task Force, 2000.

Apêndice A

Formatos de dados

A.1 Formato do Distinguished Name

A Tabela A.1 apresenta o nome distinto (DN) dos certificados. Para garantir a interoperabilidade dos certificados digitais com as mais diversas aplicações, fica proibido o uso de caracteres de acentuação no *Distinguished Name* dos certificados.

Tabela A.1: Distinguished Name

CAMPO	Usuários	Serviços	AC
C	BR	BR	BR
O	ICPEDU	ICPEDU	ICPEDU
O	CBPF	CBPF	CBPF
OU	Login do usuario CBPF	Nome do serviço	Unidade do CBPF
L	Rio de Janeiro	Rio de Janeiro	Rio de Janeiro
ST	RJ	RJ	RJ
CN	(nome do usuario)	(FQDN)	AC CBPF

A.2 Formato do certificado

A.2.1 Atributos básicos

Os atributos básicos dos certificados estão descritos na Tabela A.2.

A.2.2 Extensões

Os certificados para usuarios e serviços terão as extensões apresentadas na Tabela A.3. O texto a ser colocado na extensão de políticas de certificado é o seguinte: Este certificado é para uso exclusivo dos usuários e aplicações internas do CBPF. Utilize certificados ICP-Brasil caso seja necessário assinar documentos eletrônicos com eficácia jurídica.

Tabela A.2: Atributos básicos dos certificados

	Nome atributo	Descrição atributo	valor
conteúdo	version	versão do padrão X.509	v3
	serialNumber	número serial do certificado	diferente para cada certificado
	signature	algoritmo de assinatura	Sha1WithRSAEncryption
	issuer	emissor, sempre uma AC	DN da AC CBPF
	validity	intervalo de validade	validade 10 anos
	subject	titular do certificado	DN do titular.
	subjectPublicKeyInfo	chave pública	diferente para cada certificado.
	issuerUniqueID	não é usado	
	subjectUniqueID	não é usado	
	extensions	extensões, discutidos na Tab. A3	
envelope	signatureAlgorithm	algoritmo de assinatura	Sha1WithRSAEncryption.
	signatureValue	valor da assinatura	diferente para cada certificado.

Tabela A.3: Extensões dos certificados para usuarios e serviços

Extensão	Crítica	Conteúdo
crlDistributionPoints	sim	http://ac.cat.cbpf.br/repositorio/ac-cbpf.crl
certificatePolicies	sim	especifica o OID da PC da AC CBPF. O atributo id-qtcps especifica a url da DPC e é apresentado no formato: http://ac.cat.cbpf.br/repositorio/dpc-ac-cbpf-AAAAMMDD.pdf, onde AAAAMMDD designa a data de emissão da 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 instituicoes brasileiras de ensino e pesquisa, e não tem eficacia juridica.”
subjectKeyIdentifier	não	hash da chave pública do próprio certificado
authorityKeyIdentifier	não	contém o hash da chave pública da AC CBPF
keyUsage	sim	Critical certificateSigning e crlSigning
basicContraints	sim	Critical CA:false

A.3 Formato da Lista de Certificados Revogados

A Tabela A.4 apresenta as extensões e respectivas entradas da LCRs emitidas.

Tabela A.4: Extensões da LCR

Extensão	Crítica	Conteúdo
authorityKeyIdentifier	Sim	hash da chave pública da AC CBPF
crlNumber	sim	contém um número sequencial para cada LCR emitida