

**DECLARAÇÃO DE PRÁTICAS  
DE CERTIFICAÇÃO  
DA AUTORIDADE CERTIFICADORA BRY  
MÚTIPLA**

**“DPC DA AC BRY MÚTIPLA”**

Versão 1.1

**Junho, 2009**

---

## Sumário

<b>LISTA DE ACRÔNIMOS.....</b>	<b>4</b>
<b>1 INTRODUÇÃO.....</b>	<b>6</b>
<b>1.1 VISÃO GERAL .....</b>	<b>6</b>
<b>1.2 IDENTIFICAÇÃO.....</b>	<b>6</b>
<b>1.3 COMUNIDADE E APLICABILIDADE .....</b>	<b>6</b>
<b>1.4 DADOS DE CONTATO.....</b>	<b>7</b>
<b>2 DISPOSIÇÕES GERAIS .....</b>	<b>8</b>
<b>2.1 OBRIGAÇÕES E DIREITOS .....</b>	<b>8</b>
<b>2.2 RESPONSABILIDADES .....</b>	<b>11</b>
<b>2.3 RESPONSABILIDADE FINANCEIRA .....</b>	<b>11</b>
<b>2.4 INTERPRETAÇÃO E EXECUÇÃO .....</b>	<b>11</b>
<b>2.5 TARIFAS DE SERVIÇO .....</b>	<b>12</b>
<b>2.6 PUBLICAÇÃO E REPOSITÓRIO.....</b>	<b>13</b>
<b>2.7 FISCALIZAÇÃO E AUDITORIA DE CONFORMIDADE.....</b>	<b>13</b>
<b>2.8 SIGILO .....</b>	<b>15</b>
<b>3 IDENTIFICAÇÃO E AUTENTICAÇÃO .....</b>	<b>17</b>
<b>3.1 REGISTRO INICIAL .....</b>	<b>17</b>
<b>3.2 GERAÇÃO DE NOVO PAR DE CHAVES ANTES DA EXPIRAÇÃO DO ATUAL .....</b>	<b>20</b>
<b>3.3 GERAÇÃO DE NOVO PAR DE CHAVES APÓS REVOGAÇÃO .....</b>	<b>20</b>
<b>3.4 SOLICITAÇÃO DE REVOGAÇÃO .....</b>	<b>20</b>
<b>4 REQUISITOS OPERACIONAIS.....</b>	<b>21</b>
<b>4.1 SOLICITAÇÃO DE CERTIFICADO .....</b>	<b>21</b>
<b>4.2 EMISSÃO DE CERTIFICADO .....</b>	<b>21</b>
<b>4.3 ACEITAÇÃO DE CERTIFICADO .....</b>	<b>21</b>
<b>4.4 SUSPENSÃO E REVOGAÇÃO DE CERTIFICADO .....</b>	<b>22</b>
<b>4.5 PROCEDIMENTOS DE AUDITORIA DE SEGURANÇA .....</b>	<b>24</b>
<b>4.6 ARQUIVAMENTO DE REGISTROS.....</b>	<b>26</b>

<b>4.7</b>	<b>TROCA DE CHAVE .....</b>	<b>28</b>
<b>4.8</b>	<b>COMPROMETIMENTO E RECUPERAÇÃO DE DESASTRE.....</b>	<b>28</b>
<b>4.9</b>	<b>EXTINÇÃO DOS SERVIÇOS .....</b>	<b>29</b>
<b>5</b>	<b>CONTROLES DE SEGURANÇA FÍSICA, PROCEDIMENTAL E DE PESSOAL .....</b>	<b>30</b>
<b>5.1</b>	<b>CONTROLES FÍSICOS .....</b>	<b>30</b>
<b>5.2</b>	<b>CONTROLES PROCEDIMENTAIS .....</b>	<b>31</b>
<b>5.3</b>	<b>CONTROLES DE PESSOAL.....</b>	<b>32</b>
<b>6</b>	<b>CONTROLES TÉCNICOS DE SEGURANÇA .....</b>	<b>34</b>
<b>6.1</b>	<b>GERAÇÃO E INSTALAÇÃO DO PAR DE CHAVES.....</b>	<b>34</b>
<b>6.2</b>	<b>PROTEÇÃO DA CHAVE PRIVADA .....</b>	<b>36</b>
<b>6.3</b>	<b>OUTROS ASPECTOS DO GERENCIAMENTO DO PAR DE CHAVES .....</b>	<b>37</b>
<b>6.4</b>	<b>DADOS DE ATIVAÇÃO .....</b>	<b>38</b>
<b>6.5</b>	<b>CONTROLES DE SEGURANÇA COMPUTACIONAL .....</b>	<b>39</b>
<b>6.6</b>	<b>CONTROLES TÉCNICOS DO CICLO DE VIDA .....</b>	<b>40</b>
<b>6.7</b>	<b>CONTROLES DE SEGURANÇA DE REDE .....</b>	<b>40</b>
<b>6.8</b>	<b>CONTROLES DE ENGENHARIA DO MÓDULO CRIPTOGRÁFICO .....</b>	<b>40</b>
<b>7</b>	<b>PERFIS DE CERTIFICADO E LCR .....</b>	<b>41</b>
<b>7.1</b>	<b>DIRETRIZES GERAIS .....</b>	<b>41</b>
<b>7.2</b>	<b>PERFIL DO CERTIFICADO .....</b>	<b>41</b>
<b>7.3</b>	<b>PERFIL DE LCR.....</b>	<b>42</b>
<b>8</b>	<b>ADMINISTRAÇÃO DE ESPECIFICAÇÃO .....</b>	<b>42</b>
<b>8.1</b>	<b>PROCEDIMENTOS DE MUDANÇA DE ESPECIFICAÇÃO.....</b>	<b>42</b>
<b>8.2</b>	<b>POLÍTICAS DE PUBLICAÇÃO E NOTIFICAÇÃO .....</b>	<b>42</b>
<b>8.3</b>	<b>PROCEDIMENTOS DE APROVAÇÃO .....</b>	<b>42</b>

## LISTA DE ACRÔNIMOS

- AC** - Autoridade Certificadora
- AC BRy Múltipla** - Autoridade Certificadora Raiz da BRy
- AC BRy Múltipla** - Autoridade Certificadora Múltipla da BRy Tecnologia
- CEI** - Cadastro Específico do INSS
- CG** - Comitê Gestor
- CMVP** - Cryptographic Module Validation Program
- CN** - Common Name
- CNPJ** - Cadastro Nacional de Pessoas Jurídicas
- CPF** - Cadastro de Pessoas Físicas
- CSP** - Cryptographic Service Provider
- DMZ** - Zona Desmilitarizada
- DN** - Distinguished Name
- DPC** - Declaração de Práticas de Certificação
- HD** - Hard disk
- ICP-Brasil** - Infra Estrutura de Chaves Públicas Brasileira
- ICP-BRy** - Infra Estrutura de Chaves Públicas da BRy Tecnologia SA
- IDS** - Sistemas de Detecção de Intrusão
- IEC** - International Electrotechnical Commission
- ISO** - International Organization for Standardization
- ITU** - International Telecommunications Union
- LCR** - Lista de Certificados Revogados
- NBR** - Norma Brasileira
- NIS** - Número de Identificação Social
- NIST** - National Institute of Standards and Technology
- OCSP** - On-line Certificate Status Protocol
- OID** - Object Identifier
- OU** - Organization Unit
- PASEP** - Programa de Formação do Patrimônio do Servidor Público
- PC** - Política de Certificados
- PKCS#1** - Public Key Cryptography Standard - #1 = RSA Cryptography Standard
- PKCS#7** - Public Key Cryptography Standard - #7 = Cryptographic Message Syntax Standard
- PKCS#10** - Public Key Cryptography Standard - #10 = Certification Request Standard
- PIS** - Programa de Integração Social
- PS** - Política de Segurança
- PSS** - Prestadores de Serviço de Suporte
- RFC** - Request For Comments
- RFC 2313**: Internet X.509 Public Key Infrastructure - RSA Encryption
- RFC 2527**: Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework

**RFC4325:** Internet X.509 Public Key Infrastructure - Authority Information Access Certificate Revocation List (CRL) Extension

**RG** - Registro Geral

**SNMP** - Simple Network Management Protocol

**SSL** - Secure Socket Layer

**UF** - Unidade de Federação

**URL** - Uniform Resource Location

**UTC** - Coordinated Universal Time

# 1 INTRODUÇÃO

## 1.1 Visão Geral

Esta Declaração de Práticas de Certificação (DPC) descreve as práticas e os procedimentos empregados pela Autoridade Certificadora Múltipla da BRy Tecnologia S.A (AC BRy Múltipla) pertencente à Infra-estrutura de Chaves Públicas da BRy Tecnologia S.A. (ICP-BRy), na execução dos seus serviços.

A AC BRy Múltipla está certificada em nível imediatamente subsequente ao da AC Raiz BRy. O certificado da AC BRy Múltipla contém a chave pública correspondente à sua chave privada, utilizada para assinar os certificados de assinatura A1, A3 e para assinar a sua Lista de Certificados Revogados (LCR).

Para regulamentar as exigências relacionadas aos tipos de certificados emitidos, a ICP-BRy publica Políticas de Certificados (PC), sujeitas a esta DPC, que especificam como o certificado é gerado, administrado, e utilizado.

## 1.2 Identificação

Esta DPC é chamada Declaração de Práticas de Certificação da Autoridade Certificadora BRy Múltipla e referida como "DPC da AC BRy Múltipla ", cujo OID (object identifier) é 1.3.6.1.4.1.14975.1.1.2.

## 1.3 Comunidade e Aplicabilidade

### 1.3.1 Autoridades Certificadoras

Esta DPC refere-se à AC BRy Múltipla no âmbito da ICP-BRy.

### 1.3.2 Autoridades de Registro

1.3.2.1 Os dados a seguir, referentes às Autoridades de Registro – AR utilizadas pela AC BRy Múltipla para os processos de recebimento, validação e encaminhamento de solicitações de emissão ou de revogação de certificados digitais e de identificação de seus solicitantes, são publicados em serviço de diretório e/ou em página web da AC BRy Múltipla (<http://icp.bry.com.br/repositorio>).

### 1.3.3 Titulares de Certificado

Pessoas físicas ou jurídicas de direito público ou privado, nacionais ou estrangeiras, podem ser titulares de Certificado.

#### 1.3.4 Aplicabilidade

A AC BRy Múltipla implementa as seguintes Políticas de Certificado Digital:

Para Certificados de Assinatura Digital:

Política de Certificado de Assinatura Digital Tipo A1 da Autoridade Certificadora BRy Múltipla, PC A1 da AC BRy Múltipla, OID 1.3.6.1.4.1.14975.1.3.1.1.

Política de Certificado de Assinatura Digital Tipo A3 da Autoridade Certificadora BRy Múltipla, PC A3 da AC BRy Múltipla, OID 1.3.6.1.4.1.14975.1.3.3.1.

### 1.4 Dados de Contato

Nome: Bry Tecnologia S.A.

Endereço: Rua Lauro Linhares 2123 – Torre B – Sala 306 , Trindade – Florianópolis/SC - CEP: 88036-002

Telefone/FAX: (48) 3234-6696

Nome: Marcelo Luiz Brocardo

E-mail: ac@bry.com.br

## 2 DISPOSIÇÕES GERAIS

### 2.1 Obrigações e Direitos

Nos itens a seguir estão descritas as obrigações gerais das entidades envolvidas. Os requisitos específicos associados a essas obrigações estão detalhados nas PC implementadas pela AC BRy Múltipla.

#### 2.1.1 Obrigações da AC BRy Múltipla

operar de acordo com esta DPC e com as PC que implementa;

gerar e gerenciar seus pares de chaves criptográficas;

assegurar a proteção de suas chaves privadas;

notificar a AC Raiz BRy, emitente do seu certificado, quando ocorrer comprometimento de sua chave privada e solicitar a imediata revogação desse certificado.

notificar os usuários quando ocorrer suspeita de comprometimento da chave privada da AC BRy Múltipla, emissão de novo par de chaves e correspondente certificado ou o encerramento de suas atividades;

distribuir seu próprio certificado;

emitir, expedir e distribuir os certificados de AR vinculadas e de usuários finais;

informar a emissão do certificado ao respectivo solicitante;

revogar os certificados emitidos;

emitir, gerenciar e publicar sua LCR;

publicar em sua página web esta DPC da AC BRy Múltipla e as PC que implementa;

publicar em sua página web as informações descritas no item 2.6.1.2 desta DPC;

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

identificar e registrar todas as ações executadas, conforme as normas, práticas e regras estabelecidas pela ICP-BRy;

adotar as medidas de segurança e controle previstas nesta DPC da AC BRy Múltipla, nas PC e Política de Segurança da AC BRy Múltipla que implementar , envolvendo seus processos, procedimentos e atividades, observadas as normas, critérios, práticas e procedimentos da ICP-BRy;

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

manter e testar regularmente seu Plano de Continuidade do Negócio;

manter contrato de seguro de cobertura de responsabilidade civil decorrente das atividades de certificação digital e de registro, com cobertura suficiente e compatível com o risco dessas atividades;

informar à terceira parte e titulares de certificado acerca das garantias, coberturas, condicionantes e limitações estipuladas pela apólice de seguro de responsabilidade civil contratada pela AC BRy Múltipla;  
não emitir certificado com prazo de validade que se estenda além do prazo de validade de seu próprio certificado;  
fiscalizar e auditar as AR vinculadas em conformidade com as políticas, normas e procedimentos; e  
tomar as medidas cabíveis para assegurar que usuários e demais entidades envolvidas tenham conhecimento de seus respectivos direitos e obrigações.

### 2.1.2 Obrigações das AR

receber solicitações de emissão ou de revogação de certificados;  
confirmar a identidade do solicitante e a validade da solicitação;  
encaminhar as solicitações de emissão ou de revogação de certificados à AC BRy Múltipla utilizando protocolo de comunicação seguro;  
informar os titulares de certificado a emissão ou a revogação de seus certificados;  
disponibilizar os certificados emitidos pela AC BRy Múltipla aos seus respectivos solicitantes;  
identificar e registrar todas as ações executadas, conforme as normas, práticas e regras estabelecidas pela ICP BRy;  
manter e garantir a segurança da informação por elas tratada, de acordo com o estabelecido nas normas, critérios, práticas e procedimentos da ICP-BRy;  
manter e testar anualmente seu Plano de Continuidade do Negócio – PCN;  
garantir que todas as aprovações de solicitação de certificados sejam realizadas em instalações técnicas autorizadas a funcionar como AR vinculadas credenciadas; e  
obedecer estritamente a esta DPC da AC BRy Múltipla e às PC aplicáveis, bem como respeitar a legislação aplicável, incluindo as regras definidas pela ICP-BRy.

### 2.1.3 Obrigações dos Titulares do Certificado

fornecer, de modo completo e preciso, todas as informações necessárias para sua identificação;  
garantir a proteção e o sigilo de suas chaves privadas, senhas e dispositivos criptográficos;  
utilizar os seus certificados e chaves privadas de modo apropriado, conforme o previsto na PC correspondente;  
conhecer os seus direitos e obrigações contemplados por esta DPC, pela PC correspondente;

informar à AC BRy Múltipla o comprometimento ou suspeita de comprometimento de sua chave privada e solicitar a imediata revogação do certificado correspondente;  
fornecer cópias autênticas dos documentos que forem exigidos para emissão do certificado;

verificar, no momento da aceitação do certificado, a veracidade e exatidão das informações contidas no seu certificado e notificar a AC BRy Múltipla, solicitando a imediata revogação do certificado que contiver inexatidões ou erros; e  
obedecer estritamente a esta DPC da AC BRy Múltipla e às PC aplicáveis, bem como respeitar a legislação aplicável, incluindo as regras definidas pela ICP-BRy e as obrigações contratuais assumidas perante à AC BRy Múltipla e AR.

Em caso de certificados emitidos para pessoas jurídicas, equipamento ou aplicação, estas obrigações se aplicam ao responsável pelo uso do certificado.

#### 2.1.4 Direitos da Terceira Parte (*Relying Party*)

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

2.1.4.2 Constitui direito da terceira parte:

recusar a utilização do certificado para fins diversos dos previstos na PC correspondente;

verificar, a qualquer tempo, a validade do certificado.

Um certificado emitido pela AC BRy Múltipla é considerado válido quando:

#### 2.1.5 Obrigações do Repositório

disponibilizar, logo após a sua emissão, os certificados emitidos pela AC BRy Múltipla e sua LCR;

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

implementar os recursos necessários para a segurança dos dados nele armazenados.

## **2.2 Responsabilidades**

### 2.2.1 Responsabilidades da AC BRy Múltipla

2.2.1.1 A AC BRy Múltipla responde pelos danos a que der causa.

2.2.1.2 A AC BRy Múltipla responde solidariamente pelos atos das entidades de sua cadeia de certificação: AR.

### 2.2.2 Responsabilidades das AR

A AR é responsável pelos danos a que der causa.

## **2.3 Responsabilidade Financeira**

### 2.3.1 Indenizações devidas pela terceira parte (*Relying Party*)

A terceira parte responde perante a AC BRy Múltipla e ARs vinculadas apenas pelos prejuízos a que der causa com a prática de ato ilícito, nos termos da legislação vigente.

### 2.3.2 Relações Fiduciárias

A AC BRy Múltipla ou sua AR vinculada indeniza os prejuízos que, comprovadamente, limitar-se-á ao valor do certificado

### 2.3.3 Processos Administrativos

Não se aplica.

## **2.4 Interpretação e Execução**

### 2.4.1 Legislação

Esta DPC é baseada na legislação em vigor no Brasil.

## 2.4.2 Forma de Interpretação e Notificação

2.4.2.1 No caso de uma ou mais das disposições desta DPC ser, por qualquer razão, considerada inválida, ilegal, ou não aplicável, somente essa disposição será afetada, todas as demais permanecem válidas dentro do escopo de abrangência deste documento.

2.4.2.2 As notificações ou qualquer outra comunicação necessária, relativa às práticas descritas nesta DPC, são feitas através de mensagem eletrônica assinada digitalmente, com chave pública certificada pela ICP-BRy, ou por escrito, entregues à AC BRy Múltipla.

## 2.4.3 Procedimentos de Solução de Disputa

No caso de um conflito entre esta DPC e outras resoluções do CG da ICP-BRy, prevalecerá sempre a última editada.

## 2.5 Tarifas de Serviço

### 2.5.1 Tarifas de Emissão e Renovação de Certificados

Variável conforme definição interna da BRy.

### 2.5.2 Tarifas de Acesso ao Certificado

Não são cobradas tarifas de acesso ao certificado digital emitido.

### 2.5.3 Tarifas de Revogação ou de Acesso à Informação de Status

Variável conforme definição interna da BRy.

### 2.5.4 Tarifas para Outros Serviços

Variável conforme definição interna da BRy.

### 2.5.5 Política de Reembolso

Variável conforme definição interna da BRy.

## 2.6 Publicação e Repositório

### 2.6.1 Publicação de Informação

2.6.1.1 As informações descritas abaixo são publicadas em serviço de diretório e/ou em página web da AC BRy Múltipla (<http://icp.bry.com.br/repositorio>), obedecendo as regras e os critérios estabelecidos nesta DPC. A disponibilidade das informações publicadas pela AC BRy Múltipla em serviço de diretório e/ou página web é de 99,0% (noventa e nove virgulo cinco por cento) do mês, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.

2.6.1.2 As seguintes informações são publicadas em serviço de diretório e/ou em página web da AC BRy Múltipla:

- a) seu próprio certificado;
- b) suas LCR;
- c) esta DPC;
- d) as PC que implementa;

### 2.6.2 Frequência de Publicação

Os certificados são publicados após sua emissão. A publicação da LCR se dá conforme o item 4.4.9.

### 2.6.3 Controles de Acesso

Não há qualquer restrição ao acesso para consulta a esta DPC, a PC implementada, aos certificados emitidos, e à LCR da AC BRy Múltipla.

São utilizados controles de acesso físico e lógico para restringir a possibilidade de escrita ou modificação dessas informações por pessoal não-autorizado.

### 2.6.4 Repositórios

A AC BRy Múltipla adota como repositório a página web da ICP-BRy: <http://icp.bry.com.br/repositorio>. Este repositório fica disponível para consulta durante 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.

As publicações da AC BRy Múltipla podem ser consultadas através do protocolo http. Somente a AC BRy Múltipla, por seus funcionários qualificados e designados especialmente para esse fim, pode efetuar as atualizações nas informações por ela publicadas no seu repositório.

## 2.7 Fiscalização e Auditoria de Conformidade

A AC Raiz BRy é a responsável pela auditoria de conformidade da AC BRy Múltipla e das AR vinculadas. A auditoria dessas entidades verifica se todos os processos, procedimentos e atividades estão em conformidade com a DPC, a PC, a Política de Segurança e as demais normas e procedimentos estabelecidos pela ICP-BRy.

### 2.7.1 Freqüência de auditoria de conformidade

A AC BRy Múltipla conduz anualmente auditorias de conformidade em todas as entidades à ela vinculadas, podendo também executar, a qualquer momento, auditorias intempestivas.

### 2.7.2 Identidade e Qualificações do Auditor

A auditoria poderá ser realizada por corpo próprio devidamente qualificado e vinculado à AC BRy Múltipla ou contratada.

### 2.7.3 Tópicos Cobertos pela Auditoria

As auditorias de conformidade verificam todos os aspectos relacionados com a emissão e o gerenciamento de certificados digitais, incluindo o controle dos processos de solicitação, identificação, autenticação, geração, publicação, distribuição, renovação e revogação de certificados.

Todos os eventos significativos ocorridos na AC BRy Múltipla ou nas AR devem ser armazenados em trilhas seguras de auditoria, onde cada entrada possua o registro de data, hora e tipo de evento, com assinatura, para garantir que as entradas não possam ser falsificadas.

Os tópicos cobertos pela auditoria de conformidade incluem, dentre outros:

política de segurança;

segurança física;

avaliação de tecnologia;

administração dos Serviços;

investigação pessoal;

PC e DPC implementadas;

contratos;

Termos de Titularidade e Responsabilidade;

considerações de sigilo.

#### 2.7.4 Medidas Adotadas em Caso de Não-Conformidade

- 2.7.4.1 Os relatórios de auditoria são submetidas à AC Raiz BRy e disponibilizados para AC BRy Múltipla. Quando encontradas irregularidades, a AC BRy Múltipla ou AR vinculada, prontamente implementa as correções apropriadas acompanhando suas implementações.
- 2.7.4.2 Cabe à entidade auditada cumprir, no prazo estipulado pela AC Raiz BRy, as recomendações dos auditores para corrigir os casos de não conformidade com a legislação ou com as políticas, normas, práticas e regras estabelecidas.
- 2.7.4.3 Cabe à AC BRy Múltipla tomar todas as medidas cabíveis a fim de garantir a segurança e a confiabilidade da ICP-BRy, podendo cancelar imediatamente o credenciamento da AR auditada, mediante decisão motivada.

#### 2.7.5 Comunicação de Resultados

Os auditores somente informam os resultados da auditoria à entidade auditada e à AC BRy Múltipla.

## 2.8 Sigilo

A chave privada de assinatura digital da AC BRy Múltipla é gerada e mantida pela própria AC BRy Múltipla, que é responsável pelo seu sigilo. A divulgação ou utilização indevida da chave privada de assinatura será de sua inteira responsabilidade.

#### 2.8.1 Tipos de Informações Sigilosas

Como princípio geral, todo documento, informação ou registro fornecido à AC BRy Múltipla é sigiloso.

#### 2.8.2 Tipos de Informações Não-Sigilosas

As informações consideradas não-sigilosas compreendem:

- solicitação de emissão do certificado;
- os certificados e a LCR emitido pela AC BRy Múltipla;
- informações corporativas que façam parte de certificados ou de diretórios públicos;
- a PC implementada;
- esta DPC;
- versões públicas de Políticas de Segurança;
- resultados finais de auditorias.

### 2.8.3 Divulgação de Informação de Revogação ou Suspensão de Certificado

2.8.3.1 As informações sobre a revogação de certificados emitidos pela AC BRy Múltipla são fornecidas em suas LCR. As razões para a revogação do certificado sempre serão informadas para o seu titular, e serão tornadas públicas desde que haja autorização expressa deste.

2.8.3.2 A suspensão de certificados não é admitida na ICP-BRy Múltipla.

#### 2.8.4 Quebra de Sigilo por Motivos Legais

Mediante ordem judicial, serão fornecidos quaisquer documentos, informações ou registros sob a guarda da AC BRy Múltipla.

#### 2.8.5 Informações a Terceiros

Nenhum documento, informação ou registro sob a guarda da AC BRy Múltipla será fornecido a qualquer pessoa, exceto quando o requisitante, através de instrumento devidamente constituído, estiver corretamente identificado e autorizado para fazê-lo.

#### 2.8.6 Divulgação por Solicitação do Titular do Certificado

2.8.6.1 O titular do certificado, ou seu representante legal devidamente identificado, qualificado e autorizado, sempre terão acesso às informações que lhe dizem respeito, e poderão autorizar a divulgação de seus registros a outras pessoas.

2.8.6.2 Essa autorização pode ser feita no ato da solicitação do certificado, no próprio formulário de solicitação, ou posteriormente, por e-mail assinado digitalmente ou outro documento legalmente aceito.

#### 2.8.7 Outras Circunstâncias de Divulgação de Informação

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

#### 2.8.8 Direitos de Propriedade Intelectual

A Bry Tecnologia S.A detém todos os direitos de propriedade intelectual sobre as idéias, conceitos, técnicas e invenções, processos e/ou obras, incluídas ou utilizadas nos produtos e serviços fornecidos pela AC BRy Múltipla nos termos desta DPC. Os direitos de propriedade terão proteção conforme a legislação aplicável.

## 3 IDENTIFICAÇÃO E AUTENTICAÇÃO

### 3.1 Registro Inicial

#### 3.1.1 Disposições gerais

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

Validação da solicitação de certificado – compreende as etapas abaixo, com base nos documentos de identificação citados nos itens 3.1.9, 3.1.10 e nos procedimentos descritos abaixo:

confirmação da identidade de um indivíduo: comprovação de que a pessoa que se apresenta como titular ou responsável pelo certificado ou como representante legal de uma pessoa jurídica é realmente aquela cujos dados constam na documentação apresentada;

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

emissão do certificado: conferência dos dados da solicitação de certificado com os constantes dos documentos apresentados e liberação da emissão do certificado no sistema da AC;

as etapas descritas acima podem ser realizadas por um ou mais agentes de validação.

Verificação da solicitação de certificado confirmação da validação realizada, observando que deve ser executada, obrigatoriamente:

por agente de registro distinto do que executou a etapa de validação.

3.1.1.3. Todas as etapas dos processos de validação e verificação da solicitação de certificado são registradas e assinadas digitalmente pelos agentes AR, na solução de certificação disponibilizada pela AC BRy Múltipla.

### 3.1.2 Tipos de Nomes

3.1.2.1 O tipo de nome admitido para os titulares de certificados emitidos, segundo esta DPC, é o “distinguished name” do padrão ITU X.500, endereços de correio eletrônico, endereço de página Web (URL), ou outras informações que permitam a identificação unívoca do titular. O certificado emitido para pessoa jurídica inclui o nome da pessoa física responsável. Para todos os efeitos legais, os certificados e as respectivas chaves de assinatura são de titularidade do responsável constante do certificado.

### 3.1.3 Necessidade de Nomes Significativos

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

### 3.1.4 Regras para Interpretação de Vários Tipos de Nomes

Não se aplica.

### 3.1.5 Unicidade de Nomes

Os identificadores do tipo *Distinguished Name* (DN) são únicos para cada titular de certificado emitido pela AC BRy Múltipla. Números ou letras adicionais podem ser incluídos ao nome para assegurar a unicidade do campo, conforme o padrão ITU X.509.

### 3.1.6 Procedimento para Resolver Disputa de Nomes

A AC BRy Múltipla se reserva o direito de tomar todas as decisões na hipótese de haver disputa decorrente da igualdade de nomes entre solicitantes de certificados. Durante o processo de confirmação de identidade, caberá ao solicitante do certificado provar o seu direito de uso de um nome específico.

### 3.1.7 Reconhecimento, Autenticação e Papel de Marcas Registradas

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

### 3.1.8 Método para Comprovar a Posse de Chave Privada

A AR verifica se a entidade que solicita o certificado possui a chave privada correspondente à chave pública para a qual está sendo solicitado o certificado digital, através da requisição no formato PKCS#10.

### 3.1.9 Autenticação da Identidade do Indivíduo

A confirmação da identidade de um indivíduo é realizada mediante a presença física do interessado ou através de documentação autenticada em cartório, com base em documentos pessoais de identificação legalmente aceitos.

### 3.1.9.1 Documentos para efeitos de identificação de um indivíduo

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

Cédula de Identidade ou Passaporte, se brasileiro;

Carteira Nacional de Estrangeiro – CNE, se estrangeiro domiciliado no Brasil;

Passaporte, se estrangeiro não domiciliado no Brasil;

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

### 3.1.9.2 Informações contidas no certificado emitido para um indivíduo estão especificadas em cada PC.

#### 3.1.10 Autenticação da identidade de uma organização

##### **3.1.10.1.1 Disposições Gerais**

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

Em sendo o titular do certificado a pessoa jurídica, é designada pessoa física como responsável pelo certificado, que será a detentora da chave privada. Preferencialmente, será designado como responsável pelo certificado o representante legal da pessoa jurídica ou um de seus representantes legais.

É feita a confirmação da identidade da organização e das pessoas físicas, nos seguintes termos:

apresentação do rol de documentos elencados no item 3.1.10.2;

apresentação do rol de documentos elencados no item 3.1.9.1 do(s) representante(s) legal(is) da pessoa jurídica e do responsável pelo uso do certificado;

presença física do responsável pelo uso do certificado e assinatura do termo de responsabilidade de que trata o item 4.1.1; e

assinatura do termo de titularidade de que trata o item 4.1.1.

Documentos para efeitos de identificação de uma organização

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

Relativos a sua habilitação jurídica:

ato constitutivo, devidamente registrado no órgão competente; e

documentos da eleição de seus administradores, quando aplicável;

Relativos a sua habilitação fiscal:

prova de inscrição no Cadastro Nacional de Pessoas Jurídicas – CNPJ; ou

prova de inscrição no Cadastro Específico do INSS – CEI.

Informações contidas no certificado emitido para uma organização. É obrigatório o preenchimento dos seguintes campos do certificado de uma pessoa jurídica, com as informações constantes nos documentos apresentados:

nome empresarial constante do CNPJ (Cadastro Nacional de Pessoa Jurídica), sem abreviações;

Cadastro Nacional de Pessoa Jurídica (CNPJ);

nome completo do responsável pelo certificado, sem abreviações;

data de nascimento do responsável pelo certificado.

Cada PC pode definir como obrigatório o preenchimento de outros campos ou o responsável pelo certificado, a seu critério e mediante declaração expressa no termo de responsabilidade, poderá solicitar o preenchimento de campos do certificado suas informações pessoais.

### **3.2 Geração de Novo Par de Chaves antes da Expiração do Atual**

Antes da expiração do certificado, o titular pode solicitar um novo certificado por meio eletrônico, assinando digitalmente uma solicitação com o uso de certificado vigente de mesmo nível ou superior, limitada a 3 (três) ocorrências sucessivas. Em outros casos são adotados os mesmos requisitos e procedimentos exigidos para solicitação inicial do certificado.

### **3.3 Geração de Novo Par de Chaves após Revogação**

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

### **3.4 Solicitação de Revogação**

A solicitação de revogação de certificado é realizada através de formulário específico, permitindo a identificação inequívoca do solicitante.

A confirmação da identidade do solicitante é feita com base na confrontação de dados fornecidos na solicitação de revogação e os dados previamente cadastrados na AR. As solicitações de revogação de certificado são registradas. O procedimento para solicitação de revogação de certificado emitido pela AC BRy Múltipla está descrito no item 4.4.3 desta DPC.

## 4 REQUISITOS OPERACIONAIS

### 4.1 Solicitação de Certificado

4.1.1 Para atender à solicitação de emissão de certificados a AC BRy Múltipla exige que a AR tenha provido:

a comprovação de atributos de identificação constantes do certificado e o recebimento dos documentos obrigatórios exigidos para identificação dos titulares e responsáveis, conforme item 3.1;

a autenticação do agente de registro responsável pelas solicitações de emissão e de revogação de certificados mediante o uso de certificado digital;

assinatura de um “Termo de Titularidade e Responsabilidade” assinado pelo responsável pelo uso do certificado estabelecendo termos e condições aplicados ao uso do certificado.

### 4.2 Emissão de Certificado

4.2.1 A emissão de certificado depende do correto preenchimento de formulário de solicitação, do recebimento do “Termo de Titularidade e Responsabilidade”. Após o processo de validação das informações fornecidas pelo solicitante, o certificado é emitido e o Titular é notificado, por e-mail da emissão e do método para a retirada do certificado.

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

### 4.3 Aceitação de Certificado

4.3.1 O titular do certificado ou pessoa física responsável verifica as informações contidas no certificado e o aceita caso as informações sejam íntegras, corretas e verdadeiras. Caso contrário, o titular do certificado não pode utilizar o certificado e deve solicitar imediatamente a revogação do mesmo. Ao aceitar o certificado, o titular do certificado:

concorda com as responsabilidades, obrigações e deveres nesta DPC e na PC correspondente;

garante que, com seu conhecimento, nenhuma pessoa sem autorização teve acesso à chave privada associada ao certificado;

afirma que todas as informações contidas no certificado, fornecidas na solicitação, são verdadeiras e estão reproduzidas no certificado de forma correta e completa.

O titular do certificado é informado, quando da emissão do mesmo, do disposto no item 4.3.

- 4.3.2 A aceitação do certificado e do seu conteúdo é declarada, pelo titular do certificado, na primeira utilização da chave privada correspondente. O prazo para aceitação do certificado está definido no item 4.4.4 de cada PC implementada pela AC BRy Múltipla.

## **4.4 Suspensão e Revogação de Certificado**

### **4.4.1 Circunstâncias para Revogação**

O titular do certificado e o responsável pelo certificado podem solicitar a revogação de seu certificado a qualquer tempo, independente de qualquer circunstância.

O certificado é obrigatoriamente revogado:

quando constatada emissão imprópria ou defeituosa do mesmo;

quando for necessária a alteração de qualquer informação constante no mesmo;

no caso de extinção, dissolução ou transformação da AC BRy Múltipla;

no caso de perda, roubo, acesso indevido, comprometimento ou suspeita de comprometimento da chave privada correspondente à pública contida no certificado ou da sua mídia armazenadora;

no caso de falecimento do titular - pessoas físicas;

no caso de mudança na razão ou denominação social do titular - equipamentos, aplicações e pessoas jurídicas;

no caso de extinção, dissolução ou transformação do titular do certificado - equipamentos, aplicações e pessoas jurídicas; ou

no caso de falecimento ou demissão do responsável - equipamentos, aplicações e pessoas jurídicas.

A AC BRy Múltipla revoga, no prazo definido no item 4.4.3, o certificado do titular que deixar de cumprir as políticas, normas e regras estabelecidas.

### **4.4.2 Quem pode Solicitar Revogação**

A revogação de um certificado somente poderá ser feita:

por solicitação do titular do certificado;

por solicitação do responsável pelo certificado, no caso de certificado de equipamentos, aplicações e pessoas jurídicas;

por solicitação da empresa ou órgão, no caso de certificado fornecido por essa empresa ou órgão para seus empregados, funcionários, servidores, parceiros ou fornecedores;

pela AC BRy Múltipla;

pela AR que tiver recebido a solicitação.

#### 4.4.3 Procedimento para Solicitação de Revogação

A solicitação de revogação do certificado da AC BRy Múltipla deve ser efetivada pelo preenchimento de formulário próprio que deverá ser assinado por seu representante legal, contendo o motivo da solicitação de revogação, o fornecimento de dados e da frase de identificação indicada na solicitação de emissão do certificado. Quando utilizada a versão eletrônica do formulário, deve-se informar a frase senha. O formulário pode também ser preenchido em papel, entregue pessoalmente pelo representante à AC BRy Múltipla e assinado no ato da entrega.

O processo de revogação de um certificado terminará com a geração e a publicação de uma LCR que contenha o certificado revogado.

O prazo para a revogação de certificado de AC BRy Múltipla é 1 (dia) útil.

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

#### 4.4.4 Prazo para Solicitação de Revogação

A solicitação de revogação tem que ser imediata quando configuradas as circunstâncias definidas no item 4.4.1.

#### 4.4.5 Circunstâncias para Suspensão

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

#### 4.4.6 Quem pode Solicitar Suspensão

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

#### 4.4.7 Procedimento para Solicitação de Suspensão

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

#### 4.4.8 Limites no Período de Suspensão

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

#### 4.4.9 Freqüência de Emissão de LCR

A freqüência para emissão da LCR da AC BRy Múltipla é de 24 (vinte e quatro) horas.

#### 4.4.10 Requisitos para Verificação de LCR

4.4.10.1 A verificação da validade do certificado na respectiva LCR é obrigatória, antes do mesmo ser utilizado.

4.4.10.2 Também é obrigatória a verificação da autenticidade da LCR, por meio das verificações da assinatura da AC BRy Múltipla e do período de validade da LCR.

#### 4.4.11 Disponibilidade para Revogação ou Verificação de Status *on-line*

A AC BRy Múltipla não suporta o processo de verificação da situação de estado de certificados de forma *on-line* (OCSP).

#### 4.4.12 Requisitos para Verificação de Revogação *on-line*

Não se aplica.

#### 4.4.13 Outras Formas Disponíveis para Divulgação de Revogação

Não se aplica

#### 4.4.14 Requisitos para Verificação de Outras Formas de Divulgação de Revogação

Não se aplica.

#### 4.4.15 Requisitos Especiais para o Caso de Comprometimento de Chave

4.4.15.1 O titular de certificado deve notificar imediatamente, através de solicitação *on-line* de revogação de certificado, à AR responsável caso ocorra perda, roubo, modificação, acesso indevido, comprometimento ou suspeita de comprometimento de sua chave privada. Nessa solicitação são registradas as circunstâncias de comprometimento, observando o previsto no item 4.4.3.

4.4.15.2 O titular do certificado pode ainda comunicar a perda, roubo, modificação, acesso indevido, comprometimento ou suspeita de comprometimento de sua chave privada diretamente na AR Responsável, assinando formulário de solicitação de revogação, observado o item 4.4.3 da PC correspondente.

Todos os documentos e relatórios relativos são arquivados após a conclusão deste processo.

## 4.5 Procedimentos de Auditoria de Segurança

Nos itens seguintes são descritos aspectos dos sistemas de auditoria e de registro de eventos implementados pela AC BRy Múltipla com o objetivo de manter um ambiente seguro.

#### 4.5.1 Tipos de Eventos Registrados

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

A AC BRy Múltipla registra 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:

iniciação e desligamento do sistema de certificação;

tentativas de criar, remover, definir senhas ou mudar os privilégios de sistema dos operadores da AC BRy Múltipla;

mudanças na configuração da AC BRy Múltipla e/ou nas suas chaves;

mudanças nas políticas de criação de certificados;

tentativas de acesso (*login*) e de saída do sistema (*logoff*);

tentativas não-autorizadas de acesso aos arquivos de sistema;

geração de chaves próprias da AC BRy Múltipla;

emissão e revogação de certificados;

geração de LCR;

tentativas de iniciar, remover, habilitar e desabilitar usuários, e de atualizar e recuperar suas chaves;

operações falhas de escrita e leitura no diretório de certificados e da LCR, quando aplicável;

operações de escrita no repositório, quando aplicável.

Todos os registros de auditoria, eletrônicos ou manuais, devem conter a data e a hora do evento e a identidade do usuário que o causou.

Para facilitar os processos de auditoria, toda a documentação relacionada aos serviços da AC BRy Múltipla deverá ser armazenada, eletrônica ou manualmente, em local único, conforme a Política de Segurança da ICP-BRy.

#### 4.5.2 Freqüência de Auditoria de Registros (*log*)

A AC BRy Múltipla garante que seus registros de auditoria serão analisados cada vez que é ligada, sempre que houver utilização de seu sistema de certificação (equipamento *off-line*, que permanece desligado grande parte do tempo) ou em caso de suspeita de comprometimento da segurança. Todos os eventos significativos são explicados em relatório de auditoria de registros. Tal análise envolve uma inspeção breve de todos os registros, verificando que não foram alterados, seguida de uma investigação mais detalhada de quaisquer alertas ou irregularidades nos mesmos.

Todas as ações tomadas em decorrência dessa análise são documentadas.

#### 4.5.3 Período de Retenção para Registros (*log*) de Auditoria

A AC BRy Múltipla mantém em suas próprias instalações os seus registros de auditoria por pelo menos 12 (doze) meses e, subseqüentemente, os armazena da maneira descrita no item 4.6.

#### 4.5.4 Proteção de Registro (*log*) de Auditoria

O sistema de registro de eventos de auditoria inclui mecanismos para proteger os arquivos de auditoria contra leitura não autorizada, modificação e remoção. Informações manuais de auditoria também são protegidas contra a leitura não autorizada, modificação e remoção.

#### 4.5.5 Procedimentos para Cópia de Segurança (*backup*) de Registro (*log*) de Auditoria

Os registros de eventos e sumários de auditoria do equipamento *off-line* utilizado pela AC BRy Múltipla têm cópias de segurança mensais ou sempre que houver alguma utilização desse equipamento.

#### 4.5.6 Sistema de Coleta de Dados de Auditoria

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

#### 4.5.7 Notificação de Agentes Causadores de Eventos

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

#### 4.5.8 Avaliações de Vulnerabilidade

Os eventos que representem possível vulnerabilidade, detectados na análise mensal dos registros de auditoria, são analisados detalhadamente e, dependendo de sua gravidade, são registrados em separado.

Como decorrência, ações corretivas são implementadas e registradas para fins de auditoria.

## 4.6 Arquivamento de Registros

#### 4.6.1 Tipos de Registros Arquivados

As seguintes informações são registradas e arquivadas pela AC BRy Múltipla:

emissão de certificados;

solicitações de revogação de certificados;

emissões de LCR;

trocas de chaves criptográficas da AC BRy Múltipla;

informações de auditoria previstas no item 4.5.1;  
correspondências formais.

#### 4.6.2 Período de Retenção para Arquivo

Os períodos de retenção para cada registro arquivado são os seguintes:  
as LCR referentes a certificados de assinatura digital são retidas por período igual ao do arquivamento dos respectivos certificados;  
as demais informações são retidas por, no mínimo, 6 (seis) anos.

#### 4.6.3 Proteção de Arquivo

Todos os arquivos e registros são classificados e armazenados com requisitos de segurança compatíveis com essa classificação, conforme a Política de Segurança da ICP-BRy.

#### 4.6.4 Procedimentos para Cópia de Segurança (*backup*) de Arquivo

Uma segunda cópia de todo o material arquivado é armazenada em ambiente interno à AC BRy Múltipla.

É feita a verificação da integridade dessas cópias de segurança, no mínimo, a cada 6 (seis) meses.

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

#### 4.6.5 Requisitos para Datação (*time-stamping*) de Registros

Os servidores da AC BRy Múltipla estão sincronizados com a hora UTC (*Coordinated Universal Time*). Todas as informações geradas que possuam alguma identificação de horário recebem o horário em UTC, inclusive os certificados emitidos por esses equipamentos.

#### 4.6.6 Sistema de Coleta de Dados de Arquivo

Todos os sistemas de coleta de dados de arquivo utilizados pela AC BRy Múltipla em seus procedimentos operacionais são internos.

#### 4.6.7 Procedimentos para Obter e Verificar Informação de Arquivo

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

## 4.7 Troca de Chave

A AC BRy Múltipla deverá iniciar, até 3 (três) meses antes da data de expiração do seu certificado, o processo de geração de novo par de chaves e de emissão de novo certificado. Quando o certificado for expirar, será removido imediatamente da página *web*, mantendo-o armazenado por, no mínimo, 30 (trinta) anos para efeito de consulta histórica.

## 4.8 Comprometimento e Recuperação de Desastre

### 4.8.1 Recursos Computacionais, *Software* e Dados Corrompidos

Em caso de suspeita de corrupção de dados, softwares e/ou recursos computacionais, o fato é comunicado ao Gerente de Segurança da AC BRy Múltipla, que decreta o início da fase de resposta. Nessa fase, uma rigorosa inspeção é realizada para verificar a veracidade do fato e as conseqüências que o mesmo pode gerar. Esse procedimento é realizado por um grupo pré-determinado de funcionários devidamente treinados para essa situação. Caso haja necessidade, o Gerente de Segurança decretará a contingência.

### 4.8.2 Certificado de entidade é revogado

Em caso de revogação do certificado da AC BRy Múltipla o Gerente de Segurança, juntamente com o Gerente de Criptografia da AC BRy Múltipla, revogará todos os certificados subseqüentes. Os titulares dos certificados revogados serão informados. A AC BRy Múltipla emitirá certificados em substituição aos revogados com data de expiração coincidente com a do certificado revogado.

### 4.8.3 Chave da entidade é comprometida

Em caso de suspeita de comprometimento de chave da AC BRy Múltipla, o fato é imediatamente comunicado ao Gerente de Segurança que, juntamente com o Gerente de Criptografia da AC BRy Múltipla, decretam o início da fase resposta e seguirão um plano de ação para analisar a veracidade e a dimensão do fato. Caso haja necessidade, será declarada a contingência e então as seguintes providências serão tomadas:

- a) Todos os certificados afetados serão revogados e as partes serão notificadas.
- b) Cerimônias específicas serão realizadas para geração de novos pares de chaves. Isso não acontecerá se a AC BRy Múltipla estiver encerrando suas atividades – DPC Item 4.9.

### 4.8.4 Segurança dos recursos após desastre natural ou de outra natureza

Em caso de desastre natural ou de outra natureza, como por exemplo, incêndio ou inundação ou em caso de impossibilidade de acesso ao site, o Departamento de

Infra-estrutura, responsável pela contingência, notifica o Gerente de Segurança e segue um procedimento que descreve detalhadamente os passos a serem seguidos para:

- a) garantir a integridade física das pessoas que se encontram nas instalações da AC BRy Múltipla;
- b) monitorar e controlar o foco da contingência;
- c) minimizar os danos aos ativos de processamento da companhia, de forma a evitar a descontinuidade dos serviços.

#### 4.8.5 Atividades das Autoridades de Registro

As AR vinculadas à AC BRy Múltipla possuem um Plano de Continuidade de Negócios testado anualmente para garantir a recuperação, total ou parcial das atividades das AR, contendo, no mínimo as seguintes informações:

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

## 4.9 Extinção dos Serviços

No caso de extinção da AC BRy Múltipla, devem ser tomadas, no mínimo, as seguintes providências:

- notificação de todas as entidades integrantes da ICP-BRy;
- manutenção da operação da AC BRy Múltipla pelo período mínimo de 1 (um) ano após a notificação de sua extinção, salvo em casos de sucessão;
- armazenamento dos dados da AC BRy Múltipla pelo período previsto na legislação.

## 5 CONTROLES DE SEGURANÇA FÍSICA, PROCEDIMENTAL E DE PESSOAL

### 5.1 Controles Físicos

#### 5.1.1 Construção e Localização das Instalações

A localização e o sistema de certificação utilizado para a operação da AC BRy Múltipla não são publicamente identificados. Não há identificação pública externa das instalações. A operação da AC BRy Múltipla é realizada num ambiente fechado e protegido.

#### 5.1.2 Acesso Físico

A AC BRy possui sistema de controle de acesso físico que garante a segurança de suas instalações conforme a política de segurança da ICP-BRy.

#### 5.1.3 Exposição à Água

A estrutura do ambiente provê proteção física contra exposição à água, infiltrações e inundações, provenientes de qualquer fonte externa.

#### 5.1.4 Prevenção e Proteção contra Incêndio

Não se aplica.

#### 5.1.5 Armazenamento de Mídia

Atende a norma brasileira NBR.

#### 5.1.6 Destruição de Lixo

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

5.1.6.2 Todos os dispositivos magnéticos não mais utilizáveis e que tenham sido anteriormente utilizados para o armazenamento de informações sensíveis são desmagnetizados com ferramentas específicas, e são fisicamente destruídos.

#### 5.1.7 Instalações de Segurança (*backup*) Externas (*off-site*)

Definido no plano de continuidade.

## 5.2 Controles Procedimentais

### 5.2.1 Perfis Qualificados

A separação das tarefas para funções críticas é uma prática adotada, com o intuito de evitar que um funcionário utilize indevidamente o sistema de certificação sem ser detectado. Isto é realizado criando perfis separados e contas na estação de trabalho de serviço. Cada perfil possui uma quantia limitada de capacidade operacional. Este método permite um sistema de “verificações e equilíbrio” a ocorrer entre os vários perfis.

Os seguintes perfis foram estabelecidos pela AC BRy Múltipla:

Gerente de Configurações (GC):

- configuração e manutenção do *hardware* e do *software* da AC BRy Múltipla;
- início e término dos serviços da AC BRy Múltipla.

Administrador do Sistema (AS):

- gerenciamento dos processos de iniciação dos usuários internos à AC BRy Múltipla;
- emissão, expedição, distribuição, revogação e gerenciamento de certificados;
- distribuição de cartões (*tokens*), quando for o caso.

Gerente de Segurança (GS):

- Este não tem acesso ao *software* e ao *hardware* do sistema de certificação da AC. Comporta-se como um auditor interno que tem pleno conhecimento da DPC e verifica se esta está sendo cumprida.
- gerenciamento dos operadores da AC BRy Múltipla;
- implementação das políticas de segurança da AC BRy Múltipla;
- verificação dos registros de auditoria;
- verificação do cumprimento desta DPC.

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

A AC BRy Múltipla possui rotinas de atualização das permissões de acesso e procedimentos específicos para situações de demissão ou mudança de função dos empregados. Existe uma lista de revogação com todos os recursos, antes disponibilizados, que o empregado devolve à AC BRy Múltipla no ato de seu desligamento.

#### 5.2.2 Número de Pessoas Necessário por Tarefa

O controle multiusuário é requerido para a geração e a utilização da chave privada da AC BRy Múltipla, conforme o descrito em 6.2.2.

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

#### 5.2.3 Identificação e Autenticação para Cada Perfil

Todo empregado da AC BRy Múltipla tem sua identidade e perfil verificados antes de:

- ser incluído em uma lista de acesso às instalações da AC BRy Múltipla;
- ser incluído em uma lista para acesso físico ao sistema de certificação da AC BRy Múltipla;
- receber um certificado digital para executar suas atividades operacionais na AC BRy Múltipla;
- receber uma conta no sistema de certificação da AC BRy Múltipla.

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

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

A AC BRy Múltipla implementa um padrão de utilização de "senhas fortes", definido pela Política de Segurança da ICP-BRy, juntamente com procedimentos de validação dessas senhas.

### 5.3 Controles de Pessoal

Na AC BRy Múltipla, todos os funcionários encarregados de tarefas operacionais têm registrado em contrato:

- os termos e as condições do perfil que ocuparão na AC BRy Múltipla;
- o compromisso de observar as normas, políticas e regras aplicáveis da AC BRy Múltipla;
- o compromisso de não divulgar informações sigilosas a que tenham acesso.

#### 5.3.1 Antecedentes, Qualificação, Experiência e Requisitos de Idoneidade

A seleção de pessoal que operam sob a hierarquia da AC BRy Múltipla, leva em conta os antecedentes, qualificações, experiência anterior e exigências de liberação de cada posição que é comparada contra os perfis de candidatos potenciais.

### 5.3.2 Procedimentos de Verificação de Antecedentes

Todo o pessoal da AC BRy Múltipla em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados é submetido a:

- verificação de antecedentes criminais;
- verificação de situação de crédito;
- verificação de histórico de empregos anteriores;
- comprovação de escolaridade e de residência.

### 5.3.3 Requisitos de Treinamento

Todo o pessoal da AC BRy Múltipla envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados recebem treinamento documentado, suficiente para o domínio dos seguintes temas:

- princípios e mecanismos de segurança da AC BRy Múltipla;
- sistema de certificação em uso na AC BRy Múltipla;
- procedimentos de recuperação de desastres e de continuidade do negócio;
- outros assuntos relativos a atividades sob sua responsabilidade.

### 5.3.4 Frequência e Requisitos para Reciclagem Técnica

Todo o pessoal da AC BRy Múltipla envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados são mantidos atualizados sobre eventuais mudanças tecnológicas nos sistemas utilizados pela AC BRy Múltipla.

### 5.3.5 Frequência e Seqüência de Rodízio de Cargos

Não se aplica.

### 5.3.6 Sanções para Ações Não Autorizadas

Na eventualidade de uma ação não autorizada, real ou suspeita, ser realizada por pessoa encarregada de processo operacional da AC BRy Múltipla, o acesso dessa pessoa ao sistema de certificação é suspenso e são tomadas as medidas administrativas e legais cabíveis.

### 5.3.7 Requisitos para Contratação de Pessoal

Os candidatos ao exercício de funções na AC BRy Múltipla são selecionados a partir do seu quadro de empregados ou empresa contratada, de acordo com suas qualificações técnicas, profissionais e pessoais e conforme o preconizado na Política de Segurança.

### 5.3.8 Documentação Fornecida ao Pessoal

A AC BRy Múltipla disponibiliza para todo o seu pessoal:

- a DPC;
- a PC correspondente;
- a Política de Segurança;
- documentação operacional relativa a suas atividades;
- contratos, normas e políticas relevantes para suas atividades.

A documentação fornecida é mantida atualizada.

## 6 CONTROLES TÉCNICOS DE SEGURANÇA

Neste item são descritos: as medidas de segurança necessárias para proteger as chaves criptográficas dos titulares de certificados emitidos e outros controles técnicos de segurança utilizados pela AC BRy Múltipla na execução de suas funções operacionais.

### 6.1 Geração e Instalação do Par de Chaves

#### 6.1.1 Geração do Par de Chaves

6.1.1.1 O par de chaves criptográficas da AC BRy Múltipla é gerado pela própria AC BRy Múltipla, após ter sido autorizada a funcionar;

6.1.1.2 A geração do par de chaves de AC BRy Múltipla é realizada em processo verificável, obrigatoriamente na presença de múltiplos funcionários de confiança da AC BRy Múltipla, treinados para a função.

A geração destas chaves obedece a procedimento formalizado, controlado e passível de auditoria.

O par de chaves da AC BRy Múltipla é gerado em módulos criptográficos de hardware com padrão de segurança FIPS 140-1 nível 2, utilizando o algoritmo RSA.

Somente os titulares dos certificados emitidos pela AC BRy Múltipla geram os seus respectivos pares de chaves. Os procedimentos específicos estão descritos em cada PC implementada pela AC BRy Múltipla.

#### 6.1.2 Entrega da chave privada à entidade titular

A geração e a guarda de uma chave privada são responsabilidades exclusivas do titular do certificado correspondente.

### 6.1.3 Entrega da chave pública para emissor de certificado

6.1.3.1 A AC BRy Múltipla entrega cópia de sua chave pública para a AC BRy em formato PKCS #10. Essa entrega é feita por representante legal constituído da AC BRy Múltipla, em cerimônia específica, em data e hora previamente estabelecida.

6.1.3.2 Os usuários finais enviam suas chaves públicas a AC BRy Múltipla por meio eletrônico em formato PKCS#10, através de uma sessão segura fixada pelo Secure Socket Layer (SSL).

Os procedimentos específicos aplicáveis estão detalhados nas PC implementadas.

### 6.1.4 Disponibilização de chave pública da AC para usuários

A AC BRy Múltipla disponibiliza o seu certificado e todos os certificados da cadeia de certificação para os usuários, através endereço Web: <http://icp.bry.com.br/repositorio/certificados>.

### 6.1.5 Tamanhos de Chave

6.1.5.1 Cada uma das PC implementadas pela AC BRy Múltipla define o tamanho das chaves criptográficas associadas aos certificados emitidos.

6.1.5.2 O tamanho das chaves criptográficas associadas ao certificado da AC BRy Múltipla é de 2048 bits.

### 6.1.6 Geração de Parâmetros de Chaves Assimétricas

Os parâmetros de geração de chaves assimétricas da AC BRy Múltipla seguem o padrão FIPS (*Federal Information Processing Standards*) 140-2, nível 2.

### 6.1.7 Verificação da Qualidade dos Parâmetros

Os parâmetros são verificados de acordo com as normas estabelecidas pelo CMVP (*Cryptographic Module Validation Program*) do NIST (*National Institute of Standards and Technology*).

### 6.1.8 Geração de Chave por *Hardware* ou *Software*

6.1.8.1 As chaves da AC BRy Múltipla são geradas, armazenadas e utilizadas dentro de hardware específico.

6.1.8.2 Cada PC implementada pela AC BRy Múltipla caracteriza o processo utilizado para a geração de chaves criptográficas privativa dos titulares dos certificados.

### 6.1.9 Propósitos de Uso de Chave (conforme o campo “*key usage*” na X.509 v3)

6.1.9.1 Os propósitos para os quais podem ser utilizadas as chaves criptográficas dos titulares de certificados emitidos pela AC BRy Múltipla, bem como as possíveis restrições cabíveis, em

conformidade com as aplicações definidas para os certificados correspondentes estão especificados em cada PC que implementa.

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

## 6.2 Proteção da Chave Privada

A AC BRy Múltipla implementa uma combinação de controles físicos lógicos e procedimentais de forma a garantir a segurança de suas chaves privadas. Controles Lógico e Procedimental estão descritos no item 5.2. Controle de acesso físico está descrito no item 5.1.2.

A chave privada da AC BRy Múltipla é armazenada de forma cifrada no mesmo componente seguro de hardware utilizado para sua geração. O acesso a esse componente é controlado por meio de chave criptográfica de ativação.

Os titulares de certificados emitidos pela AC BRy Múltipla, são responsáveis pela guarda da chave privada e adotam as medidas de prevenção de perda, divulgação, modificação ou uso desautorizado da suas chaves privadas..

### 6.2.1 Padrões para Módulo Criptográfico

O módulo criptográfico de geração de chaves assimétricas da AC BRy Múltipla adota o padrão FIPS (*Federal Information Processing Standards*) 140-2 nível 3.

### 6.2.2 Controle “n de m” para Chave Privada

- 6.2.2.1 A AC BRy Múltipla exige controle múltiplo para utilização da sua chave privada.

- 6.2.2.2 É necessária a presença de pelo menos 2 (dois) de um grupo de 5 (cinco) funcionários de confiança, com perfis qualificados para o backup e restauração do backup da chave privada da AC BRy Múltipla. Para a utilização do sistema há a necessidade de 1 (um) de um grupo de 3 (três) funcionários de confiança.

### 6.2.3 Custódia (*escrow*) de Chave Privada

Não é permitida, no âmbito da ICP-BRy, a recuperação (*escrow*) de chaves privadas de assinatura, isto é, não se permite que terceiros possam obter uma chave privada de assinatura.

### 6.2.4 Cópia de Segurança (*backup*) de Chave Privada

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

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

#### 6.2.5 Arquivamento de Chave Privada

Não se aplica.

#### 6.2.6 Inserção de Chave Privada em Módulo Criptográfico

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

#### 6.2.7 Método de Ativação de Chave Privada

A ativação da chave privada da AC BRy Múltipla é implementada por meio de cartões criptográficos, protegidos com senha, após a identificação de “2” de “5” dos detentores da chave de ativação da chave criptográfica.

Cada PC implementada descreve os requisitos e os procedimentos necessários para a ativação da chave privada de entidade titular de certificado.

#### 6.2.8 Método de Desativação de Chave Privada

Quando a chave privada da AC BRy Múltipla for desativada, em decorrência de expiração ou revogação, esta deve ser eliminada da memória do módulo criptográfico. Qualquer espaço em disco, onde a chave eventualmente estivesse armazenada, deve ser sobrescrito.

Cada PC implementada descreve os requisitos e os procedimentos necessários para a desativação da chave privada de entidade titular de certificado.

#### 6.2.9 Método de Destruição de Chave Privada

Além do estabelecido no item 6.2.8, todas as cópias de segurança da chave privada da AC BRy Múltipla devem ser destruídas.

Cada PC implementada descreve os requisitos e os procedimentos necessários para a destruição da chave privada de entidade titular de certificado.

### **6.3 Outros Aspectos do Gerenciamento do Par de Chaves**

#### 6.3.1 Arquivamento de Chave Pública

As chaves públicas da AC BRy Múltipla permanecem armazenadas após a expiração dos certificados correspondentes, por no mínimo 30 (trinta) anos, na forma da legislação em vigor, para verificação de assinaturas geradas durante seu período de validade.

### 6.3.2 Períodos de Uso para as Chaves Pública e Privada

A chave privada da AC BRy Múltipla é utilizada apenas durante o período de validade do certificado correspondente e 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.

O período máximo de validade admitido para certificados da AC BRy Múltipla é de 8 (oito) anos.

## 6.4 Dados de Ativação

Os dados de ativação, distintos das chaves criptográficas, são aqueles requeridos para a operação de alguns módulos criptográficos. Cada PC implementada descreve os requisitos específicos aplicáveis.

### 6.4.1 Geração e Instalação dos Dados de Ativação

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

6.4.1.2 Cada PC implementada garante que os dados de ativação da chave privada da entidade titular do certificado, se utilizados, são únicos e aleatórios.

### 6.4.2 Proteção dos Dados de Ativação

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

6.4.2.2 Cada PC implementada garante que os dados de ativação da chave privada da entidade titular do certificado, se utilizados, são protegidos contra o uso não autorizado.

### 6.4.3 Outros Aspectos dos Dados de Ativação

Não se aplica.

## 6.5 Controles de Segurança Computacional

### 6.5.1 Requisitos Técnicos Específicos de Segurança Computacional

- 6.5.1.1 A geração do par de chaves da AC BRy Múltipla é realizada internamente ao módulo criptográfico (HSM).
- 6.5.1.2 Os requisitos de segurança computacional do equipamento onde são gerados os pares de chaves criptográficas dos titulares de certificados emitidos pela AC BRy Múltipla são descritos em cada PC implementada.
- 6.5.1.3 O ambiente computacional da AC BRy Múltipla relacionado diretamente com os processos de emissão, expedição, distribuição, revogação ou gerenciamento de certificados, implementa, entre outras, as seguintes funções:
- a) controle de acesso aos serviços e perfis da AC BRy Múltipla;
  - b) separação das tarefas e atribuições relacionadas a cada perfil qualificado da AC BRy Múltipla;
  - c) uso de criptografia para segurança de base de dados, quando exigido pela classificação de suas informações;
  - d) geração e armazenamento de registros de auditoria da AC BRy Múltipla;
  - e) mecanismos internos de segurança para garantia da integridade de dados e processos críticos; e
  - f) mecanismos para cópias de segurança (backup).
- 6.5.1.4 Essas características são implementadas pelo sistema operacional ou por meio da combinação deste com o sistema de certificação e mecanismos de segurança física.
- 6.5.1.5 As informações sensíveis contidas nos equipamentos são retiradas dos equipamentos para manutenção.

Os números de série dos equipamentos e as datas de envio e de recebimento da manutenção são controladas. Ao retornar às instalações da AC BRy Múltipla, o equipamento que passou por manutenção é inspecionado. As informações sensíveis armazenadas, relativas à atividade da AC BRy Múltipla, são destruídas de maneira definitiva nos equipamentos que deixam de ser utilizados em caráter permanente. Todos esses eventos são registrados para fins de auditoria.

- 6.5.1.6 Equipamentos utilizados pela AC BRy Múltipla são preparados e configurados como previsto na Política de Segurança da AC BRy Múltipla implementada ou em outro documento aplicável, para apresentar o nível de segurança necessário à sua finalidade.

### 6.5.2 Classificação da Segurança Computacional

Não se aplica.

## 6.6 Controles Técnicos do Ciclo de Vida

### 6.6.1 Controles de Desenvolvimento de Sistema

A AC BRy Múltipla utiliza um *software* projetado e desenvolvido por meio de uma metodologia formal rigorosa, específica para ambientes de segurança crítica.

### 6.6.2 Controles de Gerenciamento de Segurança

Uma metodologia formal de gerenciamento de configuração é usada para instalação e contínua manutenção do sistema de certificação da AC BRy Múltipla. O *software* de certificação da AC BRy Múltipla é instalado pelo próprio fabricante. Novas versões desse *software* somente serão instaladas após comunicação do fabricante e testes em ambiente de homologação da AC BRy Múltipla.

### 6.6.3 Classificações de Segurança de Ciclo de Vida

Não se aplica.

## 6.7 Controles de Segurança de Rede

### 6.7.1 Diretrizes Gerais

- 6.7.1.1 Nos servidores do sistema de certificação da AC BRy Múltipla, somente os serviços estritamente necessários para o funcionamento da aplicação são habilitados.
- 6.7.1.2 As versões mais recentes dos sistemas operacionais e dos aplicativos servidores, bem como as eventuais correções (patches), disponibilizadas pelos respectivos fabricantes são implantadas imediatamente após testes em ambiente de desenvolvimento ou homologação.
- 6.7.1.3 O acesso lógico aos elementos de infra-estrutura e proteção de rede é restrito, por meio de sistema de autenticação e autorização de acesso. Os roteadores conectados a redes externas implementam filtros de pacotes de dados, que permitem somente as conexões aos serviços e servidores previamente definidos como passíveis de acesso externo.

## 6.8 Controles de Engenharia do Módulo Criptográfico

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

## 7 PERFIS DE CERTIFICADO E LCR

### 7.1 Diretrizes Gerais

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

7.1.2 As seguintes PCs:

PC A1 da AC BRy Múltipla, OID 1.3.6.1.4.1.14975.1.3.1.1

PC A3 da AC BRy Múltipla, OID 1.3.6.1.4.1.14975.1.3.3.1

Implementadas pela AC BRy Múltipla especificam o formato dos certificados gerados e das correspondentes LCR. Nessas PCs são incluídas informações sobre os padrões adotados, seus perfis, versões e extensões.

### 7.2 Perfil do Certificado

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

7.2.1 Número de Versão

Todos os certificados emitidos pela AC BRy Múltipla implementam a versão 3 de certificado do padrão ITU X.509.

7.2.2 Extensões de Certificado

Não se aplica.

7.2.3 Identificadores de Algoritmo

Não se aplica.

7.2.4 Formatos de Nome

Não se aplica.

7.2.5 Restrições de Nome

Não se aplica.

7.2.6 OID (*Object Identifier*) da Política de Certificado

O OID desta DPC é 1.3.6.1.4.1.14975.1.1.2

7.2.7 Uso da Extensão Policy Constraints

Não se aplica.

#### 7.2.8 Sintaxe e Semântica dos Qualificadores de Política

Não se aplica.

#### 7.2.9 Semântica de Processamento para Extensões Críticas

Não se aplica.

### 7.3 Perfil de LCR

#### 7.3.1 Número(s) de Versão

As LCR emitidas pela AC BRy Múltipla implementam a versão 2 do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 3280.

#### 7.3.2 Extensões de LCR e de suas Entradas

As LCR emitidas pela AC BRy Múltipla adotam as seguintes extensões:

- **AuthorityKeyIdentifier**: contém o resumo SHA-1 da chave pública da AC BRy Múltipla.
- **cRLNumber**: contém um número seqüencial para cada LCR emitida.

## 8 ADMINISTRAÇÃO DE ESPECIFICAÇÃO

### 8.1 Procedimentos de Mudança de Especificação

Qualquer alteração nesta DPC deverá ser submetida para aprovação do CG da ICP-BRy.

### 8.2 Políticas de Publicação e Notificação

A AC BRy Múltipla mantém página específica com a versão corrente desta DPC para consulta pública, a qual está disponibilizada no endereço Web: <http://icp.bry.com.br/repositorio/dpc>.

### 8.3 Procedimentos de Aprovação

Os procedimentos de aprovação deste documento são estabelecidos à critério do CG da ICP-BRy.