PROTOCOLO COTEC
2006/00920.2

MINISTÉRIO DA FAZENDA
Secretaria da Receita Federal
Coordenação-Geral de Tecnologia e Segurança da informação

Portaria SRF/Cotec nº 06 , de 08 de fevereiro de 2006.

Aprova documentação técnica dos certificados e-CPF e e-CNPJ.

O COORDENADOR-GERAL SUBSTITUTO DE TECNOLOGIA E SEGURANÇA DA INFORMAÇÃO, no uso da atribuição que lhe confere o inciso III do art. 239 do Regimento Interno da Secretaria da Receita Federal - SRF, aprovado pela Portaria MF nº 030, de 25 de fevereiro de 2005 e alterado pela Portaria MF nº 275, de 15 de agosto de 2005, e tendo em vista o disposto no art. 15 da IN SRF nº 580, de 12 de dezembro de 2005, resolve:

Art. 1º Ficam aprovados os documentos constantes dos Anexos I, II e III desta Portaria, em substituição às suas versões anteriores:

I - Declaração de Práticas de Certificação da Autoridade Certificadora da SRF - Versão 1.0 (Anexo I);
II - Política de Certificados da Autoridade Certificadora da SRF - Versão 1.0 (Anexo II);
III - Política de Segurança da Autoridade Certificadora da SRF - Versão 1.0 (Anexo III);

Art. 2º Esta Portaria entra em vigor na data de sua publicação.

DONIZETTI VICTOR RODRIGUES

PUBLICADO NO
BP Nº 06
Responsável pela
Publicação
Em 10/02/2006

Receita Federal

Declaração de Práticas de Certificação da Autoridade Certificadora da SRF

DPC AC-SRF

SECRETARIA DA RECEITA FEDERAL

Versão 1.0

SUMÁRIO

1. INTRODUÇÃO 4

1.1 VISÃO GERAL 4
1.2 IDENTIFICAÇÃO 4
1.3 COMUNIDADE E APLICABILIDADE 4
1.4 DADOS DE CONTATO 5

2. DISPOSIÇÕES GERAIS 6

2.1 OBRIGAÇÕES 6
2.2 RESPONSABILIDADES 9
2.3 RESPONSABILIDADE FINANCEIRA 9
2.4 INTERPRETAÇÃO E EXECUÇÃO 10
2.5 TARIFAS DE SERVIÇO 10
2.6 PUBLICAÇÃO E REPOSITÓRIO 11
2.7 AUDITORIA DE CONFORMIDADE 12
2.8 SIGILO 15
2.9 DIREITOS DE PROPRIEDADE INTELECTUAL 16

3. IDENTIFICAÇÃO E AUTENTICAÇÃO 17

3.1 REGISTRO INICIAL 17
3.2 GERAÇÃO DE NOVO PAR DE CHAVES ANTES DA EXPIRAÇÃO DO ATUAL 19
3.3 CRIAÇÃO DE NOVO PAR DE CHAVES APÓS REVOGAÇÃO 19
3.4 SOLICITAÇÃO DE REVOGAÇÃO 20

4. REQUISITOS OPERACIONAIS 20

4.1 SOLICITAÇÃO DE CERTIFICADO 20
4.2 EMISSÃO DE CERTIFICADO 21
4.3 ACEITAÇÃO DE CERTIFICADO 21
4.4 SUSPENSÃO E REVOGAÇÃO DE CERTIFICADO 21
4.5 PROCEDIMENTOS DE AUDITORIA DE SEGURANÇA 24
4.6 ARQUIVAMENTO DE REGISTROS 28
4.7 TROCA DE CHAVE 30
4.8 COMPROMETIMENTO E RECUPERAÇÃO DE DESASTRE 30
4.9 EXTINÇÃO DA AC-SRF OU AR-SRF 32

5. CONTROLES DE SEGURANÇA FÍSICA, PROCEDIMENTAL E DE PESSOAS 33

5.1 CONTROLE FÍSICO 33
5.2 CONTROLES PROCEDIMENTAIS 39
5.3 CONTROLES DE PESSOAL 41

6. CONTROLES TÉCNICOS DE SEGURANÇA 43

6.1 GERAÇÃO E INSTALAÇÃO DO PAR DE CHAVES 43
6.2 PROTEÇÃO DA CHAVE PRIVADA 45
6.3 OUTROS ASPECTOS DO GERENCIAMENTO DO PAR DE CHAVES 47
6.4 DADOS DE ATIVAÇÃO 47
6.5 CONTROLES DE SEGURANÇA DOS COMPUTADORES 48
6.6 CONTROLES TÉCNICOS DO CICLO DE VIDA 49
6.7 CONTROLES DE SEGURANÇA DE REDE 49
6.8 CONTROLES DE ENGENHARIA DO MÓDULO CRIPTOGRÁFICO 51

7. PERFIS DE CERTIFICADO E LCR 52

7.1 PERFIL DO CERTIFICADO 52
7.2 PERFIL DE LCR 55

8. ADMINISTRAÇÃO DE ESPECIFICAÇÃO 55

8.1 PROCEDIMENTOS DE MUDANÇA DE ESPECIFICAÇÃO 55
8.2 POLÍTICAS DE PUBLICAÇÃO E DE NOTIFICAÇÃO 55
8.3 PROCEDIMENTOS DE APROVAÇÃO 55

1. 1. INTRODUÇÃO

1.1 VISÃO GERAL

Esta Declaração de Práticas de Certificação (DPC) descreve as práticas e os procedimentos empregados pela Autoridade Certificadora da Secretaria da Receita Federal (AC-SRF) integrante da Infra-estrutura de Chaves Públicas Brasileira (ICP-Brasil) na execução dos seus serviços.

A AC-SRF possui certificado de nível intermediário na ICP-Brasil, assinado pela AC Raiz da ICP-Brasil.

A SRF utilizará o ambiente e os serviços do Centro de Certificação Digital do Serviço Federal de Processamento de Dados (CCD-Serpro) para hospedar, operar e dar manutenção a AC-SRF.

A estrutura desta DPC AC-SRF está baseada nas resoluções do Comitê Gestor da ICP-Brasil (CG ICP-Brasil).

1.2 IDENTIFICAÇÃO

Esta DPC é chamada "Declaração de Práticas de Certificação da Autoridade Certificadora da SRF, integrante da ICP-Brasil", e comumente referida como "DPC AC-SRF". O Identificador de Objeto (OID) desta DPC, atribuído pela AC Raiz, após conclusão do processo de seu credenciamento, é 2.16.76.1.1.8.

1.3 COMUNIDADE E APLICABILIDADE

1.3.1 Autoridades Certificadoras

Esta DPC refere-se, unicamente, à Autoridade Certificadora da SRF (AC-SRF) e encontra-se publicada na página http://www.receita.fazenda.gov.br/acsrf/dpcacsrf.pdf.

1.3.2 Autoridades de Registro

Os processos de recebimento, validação e encaminhamento de solicitações de emissão ou de revogação de certificados digitais e de identificação de seus solicitantes, são de competência da AC-SRF através de sua Autoridade de Registro, doravante chamada de AR-SRF.

A PC operada pela AC-SRF no âmbito da ICP-Brasil possui sua própria Autoridade de Registro identificada neste mesmo item.

1.3.3 Titulares de Certificado

Os titulares dos certificados são as entidades pessoas jurídicas, autorizadas pela AR-SRF a receberem certificados digitais emitidos pela AC-SRF, cujos nomes aparecem no certificado digital, no campo "*Distinguished Name (DN)*".

Será 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.

1.3.4 Aplicabilidade

Os certificados definidos por esta DPC AC-SRF têm sua utilização exclusiva para a assinatura de certificados digitais e de Lista de Certificados Revogados (LCR).

1.4 Dados de Contato

1.4.1 Organização da Administração da PC AC-SRF

Esta DPC é administrada pela Coordenação-Geral de Tecnologia e Segurança da Informação (COTEC) da Secretaria da Receita Federal.

Nome: Secretaria da Receita Federal.

- ✓ Endereço: Ministério da Fazenda, Anexo A, Sala 301.
- ✓ Telefone: (550xx61) 412 3708, 412 3710, 412 3713.
- ✓ Fax: (550xx61) 412 1533.
- ✓ Página *Web*: http://www.receita.fazenda.gov.br.
- ✓ *E-mail*: ac-srf@receita.fazenda.gov.br.

1.4.2 Pessoas de Contato

Nome: Ariosto Rodrigues de Souza Junior.

- ✓ Endereço: SRF - Ministério da Fazenda, Anexo A, Sala 339.
- ✓ Telefone: (550xx61) 412 3741, 412 3743.
- ✓ Fax: (550xx61) 412 1547.
- ✓ *E-mail*: ariosto.souza@receita.fazenda.gov.br.

Nome: Sergio Roberto Fuchs da Silva.

- ✓ Endereço: SRF - Ministério da Fazenda, Anexo A, Sala 339.
- ✓ Telefone: (550xx61) 412 3776, 412 3743.
- ✓ Fax: (550xx61) 412 1547.
- ✓ *E-mail*: sergio.fuchs@receita.fazenda.gov.br.

2. 2. DISPOSIÇÕES GERAIS

2.1 OBRIGAÇÕES

2.1.1 Obrigações da AC-SRF

As obrigações da AC-SRF são as abaixo relacionadas:

1. Operar de acordo com esta DPC e com a PC implementada.
2. Gerar e gerenciar o seu par de chaves criptográficas.
3. Assegurar a proteção de sua chave privada.
4. Notificar a AC Raiz da ICP-Brasil, emitente do seu certificado, quando ocorrer comprometimento de sua chave privada e solicitar a imediata revogação desse certificado.
5. Notificar as AC de nível imediatamente subseqüente ao seu quando ocorrer: suspeita de comprometimento de sua chave, emissão de novo par de chaves e correspondente certificado ou o encerramento de suas atividades.
6. Distribuir o seu próprio certificado.
7. Emitir, expedir e distribuir os certificados das AC de nível imediatamente subseqüente ao seu ou os certificados de AR vinculados.
8. Informar a emissão do certificado ao respectivo solicitante.
9. Revogar os certificados por ela emitidos.
10. Emitir, gerenciar e publicar sua Lista de Certificados Revogados (LCR).
11. Identificar e registrar todas as ações executadas, conforme as normas, práticas e regras estabelecidas pelo Comitê Gestor da ICP-Brasil (CG ICP-Brasil).
12. Publicar em sua página *web* (http://www.receita.fazenda.gov.br/acsrf) a DPC AC-SRF e a PC AC-SRF aprovadas e implementadas.

13. Adotar as medidas de segurança e controle previstas nas PC, DPC e Política de Segurança que implementar, envolvendo seus processos, procedimentos e atividades, observadas as normas, critérios, práticas e procedimentos da ICP-Brasil.

14. Manter a conformidade dos seus processos, procedimentos e atividades com as normas, práticas e regras da ICP-Brasil e com a legislação vigente.

15. Manter e garantir a integridade, o sigilo e a segurança da informação por ela tratada.

16. Manter e testar regularmente seu Plano de Continuidade do Negócio.

17. Não emitir certificado com prazo de validade que se estenda além do prazo de validade de seu próprio certificado.

2.1.2 Obrigações da AR-SRF

As obrigações da AR-SRF são as abaixo relacionadas:

1. Receber solicitações de emissão e revogação de certificados e respectivos documentos de identificação armazenado-os conforme critérios estabelecidos pelo CG da ICP-Brasil.

2. Confirmar a identidade do solicitante e a validade da solicitação, de acordo com os requisitos estabelecidos pelos itens 3 e 4 desta DPC AC-SRF.

3. Encaminhar a solicitação de emissão e de revogação de certificado à AC-SRF, utilizando VPN (virtual private network - rede privativa virtual), SSL (secure socket layer - protocolo de comunicação seguro) ou outra tecnologia de igual ou superior nível de segurança e privacidade.

4. Utilizar VPN (virtual private network - rede privativa virtual), SSL (secure socket layer - protocolo de comunicação seguro) ou outra tecnologia de igual ou superior nível de segurança e privacidade, ao disponibilizar serviços para os solicitantes ou usuários de certificados digitais via web.

5. Informar aos respectivos titulares a emissão ou a revogação de seus certificados.

6. Disponibilizar os certificados emitidos pela AC-SRF aos seus respectivos solicitantes.

7. Identificar e registrar todas as ações executadas, conforme as normas, práticas e regras estabelecidas pelo CG da ICP-Brasil.

8. Manter a conformidade dos seus processos, procedimentos e atividades com as normas, critérios, práticas e regras estabelecidas pela AC vinculada.

9. Manter e garantir a segurança da informação por ela tratada, de acordo com o estabelecido nas normas, critérios, práticas e procedimentos da ICP –Brasil.

10. Oferecer treinamento aos seus agentes de registro, especialmente quanto ao reconhecimento de assinaturas e validade dos documentos apresentados na forma dos itens 3.1.8 e 3.1.9.

2.1.3 Obrigações do Titular do Certificado

As obrigações dos titulares de certificados emitidos de acordo com esta DPC AC-SRF são as abaixo relacionadas:

1. Fornecer, de modo completo e preciso, todas as informações necessárias para sua identificação.
2. Garantir a proteção e o sigilo de suas chaves privadas, senhas e dispositivos criptográficos.
3. Utilizar os seus certificados e suas respectivas chaves privadas de modo apropriado, conforme o previsto na PC AC-SRF.
4. Conhecer os seus direitos e obrigações, contemplados na PC da AC-SRF, nesta DPC e em outros documentos aplicáveis da ICP-Brasil.
5. Informar à AC-SRF qualquer comprometimento de sua chave privada e solicitar a imediata revogação do certificado correspondente.

Por se tratar de certificado emitido para pessoa jurídica, estas obrigações se aplicam ao responsável pelo uso do certificado.

2.1.4 Direitos da Terceira Parte (Relying Party)

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

- utilizar o certificado para os propósitos previstos nesta DPC, bem como outros fins lícitos;

- verificar a qualquer tempo a validade do certificado, sendo este considerado válido quando:

  - puder ser verificado com o uso de certificado válido da AC-SRF;

  - não constar da LCR da AC-SRF; e

  - não estiver expirado.

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

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

2.1.5 Obrigações do Repositório

Em caso de uso de repositório, são as seguintes as obrigações do mesmo:

- disponibilizar, logo após a sua emissão, os certificados emitidos pela AC-SRF e a sua LCR;

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

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

2.2 RESPONSABILIDADES

2.2.1 Responsabilidades da AC-SRF

A Autoridade de Certificadora da SRF responde pelos danos a que der causa. A AC-SRF responde solidariamente pelos atos das AC da cadeia a ela subordinada.

2.2.2 Responsabilidades da AR

A AR-SRF será responsável pelos danos a que der causa. A AC-SRF responde solidariamente pelos atos da AR-SRF.

2.3 RESPONSABILIDADE FINANCEIRA

2.3.1 Indenizações devidas pela terceira parte (Relying Party)

Não existe situação específica de utilização do certificado da AC-SRF que requeira prática de indenização pelos Usuários de Certificados, exceto na prática de ato ilícito.

2.3.2 Relações Fiduciárias

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

2.3.3 Processos Administrativos

Será seguida a legislação específica, uma vez que a AC-SRF e a AR-SRF são administradas pela Secretaria da Receita Federal, órgão da Administração Pública Federal.

2.4 Interpretação e Execução

2.4.1 Legislação

Atos e regulamentos federais que regulam os assuntos do governo também regulam esta DPC no que diz respeito a sua aplicação, construção, interpretação e validade. Isto inclui leis e regulamentos que governam os seguintes relacionamentos:

1) Governo Federal e seus funcionários, incluindo empregados contratados por tempo indeterminado ou temporários e consultores sobre contrato.

2) Governo Federal e organizações do setor privado com relações de negócio estabelecidas.

3) Funcionários do Governo Federal com outros funcionários do Governo Federal.

A DPC AC-SRF obedece às leis da República Federativa do Brasil e atende aos requisitos da legislação em vigor, incluindo a Medida Provisória nº 2200-2, de 24 de agosto de 2001, bem como as Resoluções do CG da ICP-Brasil.

2.4.2 Forma de interpretação e notificação

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.

As práticas descritas nesta DPC não prevalecerão sobre as normas, critérios, práticas e procedimentos da ICP-Brasil.

2.4.3 Procedimentos de solução de disputa

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

2.5 Tarifas de Serviço

Não há tarifas previstas pela AC-SRF para os serviços prestados às AC de nível imediatamente subseqüente ao seu.

2.5.1 Tarifas de emissão e renovação de certificados

Não há tarifas previstas pela AC-SRF para os serviços prestados às AC de nível imediatamente subseqüente ao seu.

2.5.2 Tarifas de acesso ao certificado

Não há tarifas previstas pela AC-SRF para os serviços prestados às AC de nível imediatamente subseqüente ao seu.

2.5.3 Tarifas de revogação ou de acesso à informação de status

Não há tarifas previstas pela AC-SRF para os serviços prestados às AC de nível imediatamente subseqüente ao seu.

2.5.4 Tarifas para outros serviços, tais como informação de política

Não há tarifas previstas pela AC-SRF para os serviços prestados às AC de nível imediatamente subseqüente ao seu.

2.5.5 Política de reembolso

Não há política de reembolso prevista pela AC-SRF para os serviços prestados às AC de nível imediatamente subseqüente ao seu.

2.6 Publicação e Repositório

2.6.1 Publicação de informação da AC-SRF

A AC-SRF publica em sua página *web*, (*http://www.receita.fazenda.gov.br/acsrf*), as seguintes informações:

- seu próprio certificado;
- sua LCR;
- sua PC AC-SRF;
- esta DPC AC-SRF;
- legislação especifica da SRF;
- o endereço da instalação técnica da AR-SRF;
- leiaute do certificado e-CPF e e-CNPJ; e
- lista de certificados emitidos

A DISPONIBILIDADE DA PÁGINA WEB É DE, NO MÍNIMO, 99,0% (NOVENTA E NOVE VÍRGULA ZERO POR CENTO) DO MÊS, 24 (VINTE E QUATRO) HORAS POR DIA, 7(SETE) DIAS POR SEMANA.

2.6.2 Freqüência de publicação

Os certificados e a LCR são publicados imediatamente após sua emissão pela AC-SRF. Esta DPC AC-SRF e a PC AC-SRF são publicadas, sempre que sofrerem atualizações, após aprovação pela AC Raiz da ICP-Brasil e publicação de normativa de aprovação.

2.6.3 Controles de acesso

Não há qualquer restrição ao acesso para consulta a esta DPC, à sua PC, aos certificados emitidos e à LCR da AC-SRF.

São utilizados controles de acesso apropriados para restringir a possibilidade de escrita ou modificação dessas informações a pessoal autorizado.

2.6.4 Repositórios

O repositório da AC-SRF está disponível para consulta durante 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana e atende aos seguintes requisitos:

- localização: http://www.receita.fazenda.gov.br/acsrf;
- disponibilidade: aquela definida no item 2.6.1 desta DPC AC-SRF;
- protocolos de acesso: HTTP e HTTPS;
- requisitos de segurança: obedece aos requisitos definidos no item 5 desta DPC AC-SRF.

2.7 AUDITORIA DE CONFORMIDADE

A AC Raiz da ICP-Brasil é a responsável pela auditoria dos processos, procedimentos e atividades de todas as AC integrantes da ICP-Brasil e das AR e prestadores de serviço de suporte a elas vinculadas. A AC Raiz audita a AC-SRF no âmbito da ICP-Brasil. A auditoria dessas entidades é realizada com o objetivo de verificar a conformidade com suas respectivas DPC, PC, PS e demais normas e procedimentos estabelecidos pela ICP-Brasil.

As AC subordinadas, após o seu credenciamento, disponibilizarão à AC-SRF, anualmente, para repasse a AC Raiz, relatórios de auditoria executados por empresas de auditoria independentes, contratadas pela mesma e autorizadas pela AC Raiz.

A AC-SRF pode auditar as AC subordinadas, as AR e os prestadores de serviço vinculados as AC de conformidade com seus procedimentos específicos, estando estes de acordo com os procedimentos estabelecidos pela ICP-Brasil.

2.7.1 Freqüência de auditoria de conformidade de entidade

As AC credenciadas pelo CG da ICP-Brasil subordinadas à AC-SRF, suas AR e seus prestadores de serviço sofrem auditoria:

- previamente ao seu credenciamento pela AC-Raiz e à sua habilitação pela AC-SRF; e

- a qualquer tempo, sem aviso prévio, pela AC Raiz ou pela AC-SRF.

Adicionalmente, as AC de nível imediatamente subseqüente ao da AC-SRF, para fins de continuidade do credenciamento, apresentarão anualmente relatório de auditoria fornecido por empresa de auditoria especializada e independente, contratada pela AC credenciada e autorizada pela AC Raiz.

2.7.2 Identidade/Qualificações do Auditor

Os relatórios de auditoria das AC de nível imediatamente subseqüente à AC-SRF são fornecidos por empresa de auditoria especializada e independente, contratada pela AC a ser auditada e autorizada pela AC Raiz.

Os relatórios de auditoria das AR e dos prestadores de serviço de suporte não precisam ser fornecidos por empresa de auditoria especializada e independente, podendo ser elaborados pela AC-SRF.

2.7.3 Relação entre auditor e parte auditada

No caso de contratação de auditoria independente, o auditor deve ser totalmente independente da AC auditada. Ao auditor, sem prejuízo do disposto nesta PC, aplicam-se, no que couber, as regras de suspeição e impedimento estabelecidas nos arts. 134 e 135 do Código de Processo Civil.

O auditor, no caso de contratação de auditoria independente, será declarado impedido de realizar auditoria, quando:

- houver motivo íntimo declarado;

- for amigo íntimo ou inimigo capital de membros da AC auditada;

- for credor ou devedor da AC auditada ou de um de seus membros;

- tiver recebido, nos últimos 5 anos, da AC auditada, pagamentos referentes à prestação de serviços de outra natureza;

- tiver interesse no resultado da auditoria da AC auditada; e

- houver relacionamento, de fato ou de direito, como cônjuge, parente, consangüíneo ou afim, com algum dos membros da AC auditada, em linha reta ou na colateral até o terceiro grau.

O auditor firmará declaração, sob as penas da lei, de que não se enquadra em qualquer das causas de impedimento.

2.7.4 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 em um sistema de AC ou de AR serão 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 por uma auditoria de conformidade incluem, dentre outros:

- Política de Segurança;

- Segurança física;

- Avaliação de tecnologia;

- Administração dos serviços;

- Investigação de pessoal;

- PC e DPC utilizadas;

- Contratos; e

- Considerações de sigilo.

2.7.5 Medidas a serem adotadas em caso de não conformidade

Cabe à entidade auditada cumprir, no menor dos prazos estipulados, as recomendações dos auditores para corrigir os casos de não conformidade com a legislação ou com as políticas, normas, práticas e regras estabelecidas. O não cumprimento das recomendações, no prazo estipulado, acarretará a revogação do seu certificado pela AC-SRF.

A AC-SRF, em casos de iminente dano irreparável ou de difícil reparação a terceiros, poderá suspender cautelarmente, no todo ou em parte, a emissão de certificados pela AC de nível imediatamente subseqüente ao seu.

2.7.6 Comunicação de resultados

Os auditores somente informam os resultados da auditoria à entidade auditada, à AC-SRF e à AC Raiz da ICP-Brasil.

2.8 SIGILO

A chave privada de assinatura digital da AC-SRF foi gerada e é mantida pela própria AC-SRF, que é responsável pelo seu sigilo.

A divulgação ou utilização indevida da chave privada de assinatura pela AC-SRF é de sua inteira responsabilidade.

Os titulares de certificados emitidos pela AC-SRF, ou os responsáveis pelo seu uso, terão as atribuições de geração, manutenção e sigilo de suas respectivas chaves privadas. Além, disso, são responsáveis pela divulgação ou utilização indevidas dessas mesmas chaves.

2.8.1 Tipos de informações sigilosas

Todas as informações coletadas, geradas, transmitidas e mantidas pela AC-SRF são consideradas sigilosas, exceto os certificados de chaves públicas e LCR, os quais são considerados não sigilosas, assim como a versão desta DPC AC-SRF e da PC por ela implementada.

Essas informações serão arquivadas de acordo com sua classificação que estão especificadas no Manual de Segurança.

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

2.8.2 Tipos de informações não sigilosas

Certificados, LCR e informações corporativas ou pessoais que necessariamente façam parte deles ou de diretórios públicos são consideradas informações não sigilosas.

Os seguintes documentos da AC-SRF são considerados documentos não sigilosos:

- qualquer PC aplicável;

- qualquer DPC;

- versões públicas de Políticas de Segurança; e

- resultados finais de auditoria.

2.8.3 Divulgação de informação de revogação/suspensão de certificado

A AC-SRF disponibiliza permanentemente em sua página (http://www.receita.fazenda.gov.br/acsrf/acsrf.crl), relação de certificados por ela emitidos e posteriormente revogados através de consulta à LCR.

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

Os motivos que justificaram a revogação são mantidos confidenciais pela AC-SRF e pela AR-SRF, exceto quando o titular do certificado revogado autorizar expressamente

a sua divulgação a terceiros ou quando esses motivos tenham sido ou venham a ser publicados, ou sejam ou venham a se tornar de domínio público, desde que tal publicação ou publicidade não tenha sido, de qualquer forma, ocasionada por culpa ou interferência indevida da AC-SRF ou da AR-SRF, ou ainda quando tais motivos sejam requisitados por determinação judicial ou governamental, caso em que a AC-SRF ou a AR-SRF, se estiver obrigada a divulgá-los, comunicará previamente ao titular do certificado a existência de tal determinação.

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

2.8.4 Quebra de sigilo por motivos legais

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

2.8.5 Informações a terceiros

Como diretriz geral, nenhum documento, informação ou registro, sob a guarda da AC-SRF, será fornecido, exceto quando o requerente o faça através de instrumento devidamente constituído, seja autorizado para fazê-lo e esteja corretamente identificado.

2.8.6 Divulgação por solicitação do titular

O titular de certificado e seu representante legal 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 duas formas:

- por meio eletrônico, contendo assinatura válida garantida por certificado reconhecido pela AC-SRF; ou

- por meio de pedido escrito com firma reconhecida.

Nenhuma liberação de informação é permitida sem autorização formal do titular do certificado.

2.8.7 Outras circunstâncias de divulgação de informação

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

2.9 Direitos de Propriedade Intelectual

Todos os direitos de propriedade intelectual inclusive todos os direitos autorais em todos os certificados e todos os documentos gerados para a AC-SRF (eletrônicos ou não) pertencem e continuarão sendo propriedade da SRF.

O Titular do Certificado concede à AC-SRF, o direito de publicar e divulgar em página *web* a chave pública que corresponde à chave privada que está sob posse do Titular do Certificado. Esta publicação ocorrerá pela incorporação da chave pública em certificado emitido pela AC-SRF.

3. 3. IDENTIFICAÇÃO E AUTENTICAÇÃO

3.1 REGISTRO INICIAL

Neste item e nos seguintes a DPC descreve os requisitos e os procedimentos gerais utilizados pela AR-SRF vinculada à AC-SRF responsável no processo inicial de identificação dos solicitantes de certificado.

A AR-SRF realiza a autenticação da identidade de uma organização (item 3.1.8) e a autenticação da identidade de um indivíduo (item 3.1.9) por meio de, no mínimo, dois agentes de registro responsáveis pelo recolhimento e verificação da validade dos documentos apresentados.

3.1.1 Tipos de nomes

As AC de nível imediatamente subseqüente ao da AC-SRF, titulares de certificados de AC habilitada, terão um nome que as identifiquem univocamente no âmbito da AC-SRF, no padrão ITU X.500, não incluindo no certificado o nome da pessoa física responsável pelo mesmo.

A AC-SRF segue as regras de identificação de nomes da AC Raiz da ICP-Brasil.

3.1.2 Necessidade de nomes significativos

Para identificação dos titulares dos certificados emitidos, a AC-SRF faz uso de nomes significativos que possibilitam determinar a identidade da organização a que se refere.

3.1.3 Regras para interpretação de vários tipos de nomes

Item não aplicável.

3.1.4 Unicidade de nomes

Os identificadores "*Distinguished Name*" (DN) são únicos para cada AC de nível imediatamente subseqüente ao da AC-SRF. Para cada AC, números ou letras adicionais podem ser incluídos ao nome para assegurar a unicidade do campo, conforme o padrão ITU X.509. A extensão "*Unique Identifiers*" não será admitida para diferenciar as AC com nomes idênticos.

3.1.5 Procedimento para resolver disputa de nomes

A AC-SRF reserva-se o direito de tomar todas as decisões referentes a disputas de nomes das AC de nível imediatamente subseqüente ao seu. Durante o processo de confirmação de identidade, a AC que solicita o certificado deve provar o seu direito de uso de um nome específico (DN) em seu certificado.

3.1.6 Reconhecimento, autenticação e papel de marcas registradas

De acordo com a legislação em vigor.

3.1.7 Método para comprovar a posse de chave privada

A confirmação que a entidade solicitante possui a chave privada correspondente à chave pública para a qual está sendo solicitado o certificado digital é realizada seguindo o padrão RFC 2510, item 2.3.

3.1.8 Autenticação da Identidade de uma organização

A confirmação da identidade de pessoa jurídica responsável pela solicitação de certificado da AC subseqüente é realizada mediante a apresentação dos seguintes documentos:

- ✓ Registro comercial, no caso de empresa individual;
- ✓ Ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado, em se tratando de sociedades comerciais ou civis, e, no caso de sociedade por ações, acompanhado de documentos de eleição de seus administradores;
- ✓ Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas (CNPJ);
- ✓ Prova de inscrição no Cadastro Específico do INSS (CEI), se aplicável.

A pessoa física responsável pela AC subordinada será identificada na forma descrita no item seguinte.

3.1.9 Autenticação da identidade de um indivíduo

A confirmação da identidade da pessoa física responsável pela AC subordinada é realizada mediante a presença física do interessado, com base em documentos legalmente aceitos.

A PC AC-SRF definirá os documentos exigidos com base nos requisitos aplicáveis estabelecidos pelo documento "Requisitos Mínimos para Certificados da ICP-Brasil.

As solicitações de certificados, para a AC subordinada, devem ser realizadas por pessoa física legalmente responsável.

Cabe a AR-SRF verificar a autorização atribuída ao solicitante, bem assim a presença dos documentos exigidos. Os procedimentos utilizados pela AR-SRF para

identificação e verificação da autorização do solicitante estão descritos na PC AC-SRF.

Todos os documentos de identificação exigidos serão arquivados pela AR-SRF conforme definido na PC AC-SRF.

O representante legal da AC subordinada assina o termo de titularidade denominado "Termo de Titularidade" e é, para todos os efeitos legais Titular do Certificado emitido.

A pessoa física indicada como responsável pelo certificado assina o termo de responsabilidade denominado "Termo de Acordo".

Os Termos de Titularidade e de Acordo serão mantidos junto à documentação exigida neste item.

Tanto a pessoa jurídica titular do certificado, como a pessoa física designada como responsável pelo certificado, serão responsáveis, pela correta utilização deste conforme as normas da ICP-Brasil, assim como pelos danos a que derem causa pelo uso indevido do certificado.

É mantido arquivo contendo o tipo e os detalhes do procedimento de identificação utilizado pela AR-SRF.

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

Antes de sua expiração pode ser solicitado um novo certificado, enviando-se à AR-SRF uma solicitação, por meio eletrônico, assinada digitalmente com o uso de certificado vigente, que seja pelo menos do mesmo nível de segurança, limitada a 3 (três) ocorrências sucessivas.

Nos demais casos ou quando o solicitante não utilizar o meio eletrônico, seu titular poderá solicitar um novo certificado, preenchendo "Formulário de Solicitação de Renovação de Certificado para Desenvolver Atividades de Autoridade Certificadora Habilitada", disponibilizado na página da AC-SRF (www.receita.fazenda.gov.br/acsrf), e enviando à AR-SRF. A emissão de um novo certificado obedece ao estabelecido na PC AC-SRF.

3.3 Criação de novo par de chaves após revogação

Após a revogação de seu certificado, uma AC deve executar os processos regulares de geração de novo par de chaves.

3.4 SOLICITAÇÃO DE REVOGAÇÃO

O solicitante da revogação de certificado deverá ser identificado. Somente os agentes descritos no item 4.4.2 podem solicitar a revogação do certificado de uma AC de nível imediatamente subseqüente ao da AC-SRF. O procedimento para solicitação de revogação de certificado pela AC-SRF está descrito no item 4.4.3. As solicitações de revogação de certificados são documentadas.

4. 4. REQUISITOS OPERACIONAIS

4.1 SOLICITAÇÃO DE CERTIFICADO

A solicitação de emissão de um Certificado Digital para Autoridade Certificadora Habilitada será feita mediante o formulário colocado à disposição do solicitante na página (*http://www.receita.fazenda.gov.br/acsrf*). Toda referência a formulário será entendida também como referência a outras formas que a AC-SRF possa vir a adotar.

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

1) A comprovação de atributos de identificação constantes do certificado.

2) Para o certificado emitido em 14/10/2002 a autenticação do agente de registro responsável pelas solicitações de emissão e de revogação de certificados mediante o uso de certificado digital que tenha requisitos de segurança, no mínimo, equivalente a de um certificado de nível A3, a partir 22/11/2004, a solicitação de emissão de certificados passou a ser realizada em ambiente offline, sendo a chave privada da AC-SRF ativada com a presença de 3 dos 9 dos detentores de participação de chave de ativação.

3) Assinatura do Termo de Titularidade (item 3.1.9.1) e do Termo de Acordo (item 3.1.9.1).

A solicitação de certificado para AC de nível imediatamente subseqüente ao da AC-SRF somente é possível após o deferimento do pedido de credenciamento e a respectiva autorização de funcionamento da AC em questão por parte do CG da ICP-Brasil.

Nesse caso, aquela AC deve encaminhar a solicitação de seu certificado à AC-SRF por meio de seus representantes legais, utilizando o padrão de solicitação de certificado PKCS#10 (Public Key Cryptographic Standards).

4.2 Emissão de Certificado

A emissão de um certificado pela AC-SRF é feita em cerimônia especifica, com a presença dos representantes da AC-SRF, da AC subseqüente, e convidados, na qual são registrados todos os procedimentos executados.

A AC-SRF garante que a cerimônia de emissão de um certificado para AC de nível imediatamente subsequente ao seu ocorre em, no máximo, 10 (dez) dias úteis após a autorização de funcionamento da AC em questão.

A AC-SRF entrega o certificado emitido, em formato padrão PKCS#7, para os representantes legais da AC credenciada.

O certificado é considerado valido a partir da assinatura do "Termo de Acordo".

A emissão da AC-SRF é feita em equipamentos que operam off-line.

4.3 Aceitação de Certificado

A AC de nível imediatamente subseqüente irá declarar, mediante assinatura do "Termo de Acordo", que aceita o certificado emitido.

Ao aceitar o certificado, a AC titular:

- concorda com as responsabilidades, obrigações e deveres estipulados pelo Termo de Acordo, nesta DPC e na PC implementada;

- garante que nenhuma pessoa sem autorização teve acesso a chave privada associada ao certificado; e

- afirma que todas as informações de certificado fornecidas durante o processo de credenciamento são verdadeiras e estão reproduzidas no certificado de forma correta e completa.

4.4 Suspensão e Revogação de Certificado

4.4.1 Circunstâncias para revogação

Um certificado de AC de nível imediatamente subseqüente ao da AC-SRF pode ser revogado a qualquer instante, por solicitação da AC titular do certificado ou por decisão da AC-SRF.

Um certificado é obrigatoriamente revogado nas seguintes circunstâncias:

• quando constatada emissão imprópria ou defeituosa do mesmo;

• quando for necessária a alteração de qualquer informação constante no mesmo;
• no caso de dissolução de AC titular do certificado; ou

• no caso de perda, roubo, modificação, acesso indevido ou comprometimento da chave privada correspondente ou da sua mídia armazenadora.

Em relação à revogação, deve ainda ser observado que:

1) A AC-SRF revogará, no prazo definido no item 4.4.3, o certificado da entidade que deixar de cumprir as políticas, normas e regras estabelecidas pela ICP-Brasil.

2) O CG da ICP-Brasil ou a AC Raiz determinará a revogação do certificado da AC que deixar de cumprir a legislação vigente ou as políticas, normas, práticas e regras estabelecidas para a ICP-Brasil.

4.4.2 Quem pode solicitar revogação

A revogação do certificado de uma AC de nível imediatamente subseqüente ao da AC-SRF somente pode ser feita:

- Por determinação da AC-SRF;
- Por solicitação de um AR vinculada;
- Por solicitação da AC Titular do Certificado;
- Por determinação da CG da ICP-Brasil ou da AC Raiz.

4.4.3 Procedimento para solicitação de revogação

A solicitação de revogação de certificado é feita através de formulário específico, permitindo a identificação inequívoca do solicitante. Os agentes habilitados, conforme o item 4.4.2, podem a qualquer tempo solicitar a revogação de seus respectivos certificados. Os procedimentos detalhados de solicitação de revogação estão descritos na correspondente PC.

Como diretrizes gerais, fica estabelecido que:

1) O solicitante da revogação de um certificado é identificado.

2) As solicitações de revogação, bem como as ações delas decorrentes serão registradas e armazenadas.

3) As justificativas para a revogação de um certificado são documentadas.

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

O prazo limite para a conclusão do processo de revogação de certificado, após o recebimento da respectiva solicitação é de 24 (vinte e quatro) horas.

4.4.4 Prazo para solicitação de revogação

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

A PC implementada pela AC-SRF estabelece os prazos para a aceitação do certificado solicitado pela AC Titular do Certificado, dentro dos quais a revogação do certificado poderá ser solicitada, sem ônus.

4.4.5 Circunstâncias para suspensão

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

4.4.6 Quem pode solicitar suspensão

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

4.4.7 Procedimento para solicitação de suspensão

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

4.4.8 Limites no período de suspensão

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

4.4.9 Freqüência de emissão de LCR

O prazo máximo admitido para a emissão de LCR referente a certificados de AC subordinadas é de 15 (quinze) dias.

Na revogação de certificado de AC de nível imediatamente subseqüente ao seu, a AC-SRF deverá emitir nova LCR no prazo máximo de 24 (vinte e quatro) horas e notificar todas as AC de nível imediatamente subseqüente ao seu.

São emitidas LCR na freqüência determinada na PC, mesmo quando não houver nenhuma mudança ou atualização, para assegurar a periodicidade da informação.

4.4.10 Requisitos para verificação de LCR

Todo certificado deve ter a sua validade verificada, na respectiva LCR, antes de ser utilizado.

Os números de série de certificados de qualquer entidade final que estejam revogados aparecem na LCR emitida pela AC-SRF. Estes números permanecem nas LCR emitidas até a data de expiração dos certificados ser atingida, sendo removidos na primeira LCR emitida após data de suas expirações.

A autenticidade da LCR deve também ser confirmada por meio das verificações da assinatura da AC-SRF e do período de validade da LCR.

4.4.11 Disponibilidade para revogação/verificação de status on-line

Item não aplicável.

4.4.12 Requisitos para verificação de revogação on-line

Item não aplicável.

4.4.13 Outras formas disponíveis para divulgação de revogação

Informações de revogação de certificado de AC de nível imediatamente subseqüente ao da AC-SRF serão divulgadas por meio de sua publicação no Diário Oficial da União e na página WEB, (http://www.receita.fazenda.gov.br/acsrf), da SRF.

4.4.14 Requisitos para verificação de outras formas de divulgação de revogação

Item não aplicável.

4.4.15 Requisitos especiais para o caso de comprometimento de chave

No caso do comprometimento da chave privada de uma AC de nível imediatamente subseqüente ao da AC-SRF, a mesma deve notificar imediatamente à AC-SRF, solicitando a revogação de seu certificado, por meio de formulário específico disponibilizado pela AC-SRF em sua página WEB, http://www.receita.fazenda.gov.br/acsrf.

4.5 Procedimentos de Auditoria de Segurança

4.5.1 Tipos de Evento Registrados

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

A AC-SRF registra em arquivos para fins de auditoria todos os eventos relacionados à segurança do seu sistema de certificação, quais sejam:

1) Iniciação e desligamento do sistema de certificação.

2) Tentativas de criar, remover, definir senhas ou mudar privilégios de sistema dos operadores da AC-SRF.

3) Mudanças na configuração da AC-SRF ou nas suas chaves.

4) Mudanças nas políticas de criação de certificados.

5) Tentativas de acesso (*login*) e de saída do sistema (*logoff*).

6) Tentativas não autorizadas de acesso aos arquivos de sistema.

7) Geração de chaves próprias da AC-SRF ou de chaves de Titulares de Certificados.

8) Emissão e revogação de certificados.

9) Geração de LCR.

10) Tentativas de iniciar, remover, habilitar e desabilitar usuários de sistemas, e de atualizar e recuperar suas chaves.

11) Operações falhas de escrita ou leitura no repositório de certificados e da LCR, quando aplicável.

12) Operações de escrita nesse repositório, quando aplicável.

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

1) Registros de acessos físicos.

2) Manutenção e mudanças na configuração de seus sistemas.

3) Mudanças de pessoal e de perfis qualificados.

4) Relatórios de discrepância e comprometimento.

5) Registros de destruição de meios de armazenamento contendo chaves criptográficas, dados de ativação de certificados ou informação pessoal de usuários.

Os registros de auditoria mínimos a serem mantidos pela AC-SRF incluem além dos acima:

1) Registros de solicitação, inclusive registros relativos a solicitações rejeitadas.

2) Pedidos de geração de certificado, mesmo que a geração não tenha êxito.

3) Registros de solicitação de emissão de LCR.

Todos os registros de auditoria, eletrônico ou manual, contém a data e a hora do evento registrado e a identidade do agente que o causou.

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

4.5.2 Freqüência de auditoria de registros (logs)

Para o certificado emitido em 14/10/2002 a periodicidade de auditoria de registros não será superior a uma semana, ou sempre que houver utilização do seu sistema de certificação.

Para o certificado emitido a partir de 22/11/2004 a auditoria de registro será realizada sempre que houver utilização do sistema de certificação.

Os registros de auditoria são analisados pelo pessoal operacional da AC-SRF. Todos os eventos significativos são explicados em relatório de auditoria de registros. Tal análise envolve uma inspeção breve de todos os registros verificando-se que não foram alterados, em seguida procede-se a uma investigação mais detalhada de quaisquer alertas ou irregularidades nesses registros. Todas as ações tomadas em decorrência dessa análise são documentadas.

4.5.3 Período de Retenção para registros (logs) de Auditoria

A AC-SRF mantém localmente, nas instalações do Centro de Certificação Digital do SERPRO/RJ (CCD) os seus registros de auditoria por pelo menos 2 (dois) meses e, subseqüentemente, faz o armazenamento da maneira descrita no item 4.6.

4.5.4 Proteção de registro (log) de Auditoria

Os equipamentos da AC-SRF, onde são gerados os diversos registros de sistemas pelo sistema operacional, banco de dados e do aplicativo de AC, encontram-se fisicamente em um ambiente classificado como nível 4 de segurança.

A inspeção contínua dos diversos registros dos sistemas é feita por meio das ferramentas nativas do sistema operacional, banco de dados e do aplicativo de AC, e estão disponíveis somente para leitura. Pode ser feita também por relatórios emitidos a partir destas ferramentas. Estes dados de auditoria são coletados e armazenados periodicamente em uma sala de arquivos, de nível de segurança 3.

Os registros de auditoria gerados eletrônica ou manualmente são obrigatoriamente protegidos contra leitura não autorizada, modificação e remoção. Estes registros são classificados e mantidos conforme sua classificação, segundo os requisitos da Política de Segurança da ICP-Brasil.

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

Para o certificado emitido em 14/10/2002 a AC-SRF executa procedimentos de *backup* de todo o sistema de certificação (SISTEMA OPERACIONAL + APLICAÇÃO DE AC + BANCO DE DADOS) de duas formas:

- ✓ Semanalmente: cópia de segurança; e
- ✓ Sempre que houver utilização do sistema de certificação da AC-SRF: cópia armazenada para processos de auditoria.

Para o certificado emitido a partir de 22/11/2004 a AC-SRF executa procedimentos de backup de todo o sistema de certificação, sempre que houver utilização do mesmo.

4.5.6 Sistema de coleta de dados de auditoria

O sistema de coleta de dados de auditoria da AC-SRF é uma combinação de processos automatizados e manuais executados pelo sistema operacional, pelos sistemas de certificação de AC-SRF, pelo sistema de controle de acesso e pelo pessoal operacional.

Tipo de evento	Sistema de coleção	Registrado por
Sucesso e Fracasso de tentativas a mudanças sistema operacional segurança parâmetros.	Automático	Sistema operacional
Inicio e Parada de aplicação.	Automático	Sistema operacional
Sucesso e Fracasso de tentativas de *log-in* e *log-out*.	Automático	Sistema operacional
Sucesso e Fracasso de tentativas para criar, modificar, ou apagar contas de sistema.	Automático	Sistema operacional
Sucesso e Fracasso de tentativas para criar, modificar ou apagar usuários de sistemas autorizados.	Automático	Sistema operacional
Sucesso e Fracasso de tentativas para pedir, gerar, assinar, emitir ou revogar chaves e certificados.	Automático	AC ou Software de AR
Sucesso e Fracasso de tentativas para criar, modificar ou apagar informação de Titular de Certificado.	Automático	Software de AR
Logs de *Backup* e restauração.	Automático e manual	Sistema operacional e pessoal de operações
Mudanças de configuração de sistema.	Manual	Pessoal de operações
Atualizações de *software* e *hardware*.	Manual	Pessoal de operações
Manutenção de sistema.	Manual	Pessoal de operações
Mudanças de pessoal	Manual	Pessoal de operações
Registros de acessos físicos	Automático e manual	*Software* de controle de acesso e

		Pessoal de operações

4.5.7 Notificação de agentes causadores de eventos

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

4.5.8 Avaliações de vulnerabilidade

Uma Avaliação de Riscos de Segurança foi realizada para a AC-SRF. Esta avaliação cobre a incidência de riscos e ameaças que podem impactar na operação dos serviços de certificação.

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

4.6 Arquivamento de Registros

4.6.1 Tipos de registros arquivados

As seguintes informações são registradas e arquivadas pela AC-SRF:

1) solicitações de certificados.
2) solicitações de revogação de certificados.
3) notificações de comprometimento de chaves privadas.
4) emissões e revogações de certificados.
5) emissões de LCR.
6) trocas de chaves criptográficas da AC-SRF.
7) informações de auditoria previstas no item 4.5.1.
8) correspondências formais.
9) Processos de credenciamento de AC de nível imediatamente subseqüente ao da AC-SRF.

4.6.2 Período de retenção para arquivo

Os períodos de retenção para cada registro arquivado são os seguintes:

1) as LCR referentes a certificados de assinatura digital são retidas por, no mínimo, período igual ao do arquivamento dos respectivos certificados.

2) as demais informações são retidas por, no mínimo, 6 (seis) anos.

4.6.3 Proteção de arquivos

Mídias de arquivos são guardadas em local seguro, sendo que a proteção criptográfica das mídias é adotada quando a classificação da informação assim o exigir. Também são protegidas de fatores ambientais como temperatura, umidade, e magnetismo.

Todos os registros arquivados são classificados e armazenados com requisitos de segurança compatíveis com sua classificação, conforme a Política de Segurança da ICP-Brasil.

4.6.4 Procedimentos para cópia de segurança (backup) de arquivos

Uma segunda cópia de todo o material arquivado é armazenada em ambiente externo ao sistema de certificação da AC-SRF, protegido com nível 3 de segurança.

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

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

4.6.5 Requisitos para datação (time-stamping) de registros

Os servidores da AC-SRF estão sincronizados com a hora GMT fornecida pelo Observatório Nacional. Todas as informações geradas que possuam alguma identificação de horário recebem o horário em GMT, inclusive os certificados emitidos por esses equipamentos.

No caso dos registros feitos manualmente, estes contêm a Hora Oficial do Brasil.

4.6.6 Sistema de coleta de dados de arquivo

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

Tipo de evento	Sistema de coleção	Registrado por
Solicitações de certificados	Automático e manual	*Software* de AC/AR e pessoal de operações
Solicitações de revogação de certificados	Automático e	*Software* de

	manual	AC/AR e pessoal de operações
Notificações de comprometimento de chaves privadas	Manual	Pessoal de operações
Emissões e revogações de certificados;	Automático	*Software* de AC/AR
Emissões de LCR	Automático	*Software* de AC/AR
Correspondências formais	Manual	Pessoal de operações

4.6.7 Procedimentos para obter e verificar informação de arquivo

A integridade dos arquivos da AC-SRF e da AR-SRF é verificada:

1) Na ocasião em que o arquivo é preparado.

2) Semestralmente no momento de uma auditoria de segurança programada.

3) Em qualquer outro momento quando uma auditoria de segurança completa é requerida.

Somente podem ter acesso às informações de arquivo da AR-SRF:

1) Pessoas devidamente autorizadas por meio de instrumento devidamente constituído e corretamente identificadas, conforme definido no item 2.8.5.

2) Titulares de Certificados, ou seus representantes legais, mediante solicitação formal, conforme definido no item 2.8.6.

4.7 Troca de chave

A AC-SRF comunica através de oficio, com 90 dias de antecedência, à AC subseqüente o vencimento do seu certificado, junto com as informações necessárias para a solicitação de uma nova chave.

4.8 Comprometimento e Recuperação de Desastre

A AC-SRF:

1) Estabelece e mantém documentação detalhada composta por:

- Plano de Contingência, incluindo o comprometimento de chaves, *hardware*, *software,* falhas de comunicações, e desastres naturais como fogo e inundação;
- Padrões de configuração, incluindo sistema operacional, *software* de anti-vírus e programas aplicativos específicos;
- Procedimentos de *backup*, arquivamento e armazenamento externo de segurança.

2) Provê a documentação a pedido:
   - do CG da ICP-Brasil, quando da auditoria de práticas de DPC;
   - de pessoas que administram a segurança ou auditoria de conformidade.
3) Provê treinamento apropriado a todo pessoal pertinente em contingência e procedimentos de recuperação de desastre.

4.8.1 Recursos computacionais, software, e/ou dados são corrompidos

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

1) É feita a identificação de todos os elementos corrompidos.
2) O instante do comprometimento é determinado e é crítico para invalidar as transações executadas após aquele instante.
3) É feita uma análise do nível do comprometimento para a determinação das ações a serem executadas, que podem variar de uma simples restauração de um *backup* de segurança até a revogação do certificado da AC-SRF.

4.8.2 Certificado de entidade é revogado

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

- Em caso de revogação do certificado da AC-SRF, após a identificação do incidente, são notificados os gestores do processo de certificação digital, que acionam as equipes envolvidas, de forma a indisponibilizar temporariamente os serviços de autoridade certificadora. Na confirmação do incidente, são revogados os certificados das AC de nível imediatamente subseqüente, é gerado o novo par de chaves da AC-SRF, sendo emitido, pela AC Raiz, certificado associado ao novo par de chaves gerado e emitidos, pela AC-SRF, novos certificados digitais para as AC de nível imediatamente subseqüente.

4.8.3 Chave de entidade é comprometida

A AC-SRF possui um Plano de Continuidade de Negócio que especifica as ações a serem tomadas no caso em que a chave privada de uma entidade é comprometida, e que podem ser resumidas nas ações listadas a seguir:

- Em caso de comprometimento da chave da AC-SRF, após a identificação da crise, são notificados os gestores do processo de certificação digital, que acionam as equipes envolvidas, de forma a indisponibilizar temporariamente os serviços de autoridade certificadora. Na confirmação do incidente, são revogados os certificados da AC-SRF e das AC de nível imediatamente subseqüente. É gerado, então, um novo par de chaves e emitido, pela AC Raiz, certificado associado ao novo par de chaves gerado e emitidos, pela AC-SRF, novos certificados digitais para as AC de nível imediatamente subseqüente.

4.8.4 Segurança dos recursos após desastre natural ou de outra natureza

A AC-SRF possui um Plano de Continuidade de Negócio que especifica as ações a serem tomadas no caso desastre natural ou de outra natureza. O propósito deste plano é restabelecer as principais operações da AC-SRF quando a operação de sistemas é significativamente e adversamente abalada por fogo, greves, etc.

O plano garante que qualquer impacto em operações de sistema não causará um impacto operacional direto e imediato dentro da ICP-Brasil da qual a AC-SRF faz parte. Isto significa que o plano deve ter como meta primária, restabelecer a AC-SRF para tornar acessível os registros lógicos mantidos dentro do *software*. Serão tomadas as ações de recuperação aprovadas dentro do plano segundo uma ordem de prioridade.

4.9 Extinção da AC-SRF ou AR-SRF

Quando for necessário encerrar as atividades da AC-SRF ou da AR-SRF, o impacto deste término deve ser minimizado da melhor forma possível tendo em vista as circunstâncias prevalecentes. Isto inclui:

1) Prover com maior antecedência possível notificação para:
   - a AC Raiz da ICP-Brasil;
   - todas as entidades subordinadas.
2) A transferência progressiva do serviço e dos registros operacionais, para um sucessor, que deverá observar os mesmos requisitos de segurança exigidos para a AC-SRF ou para a AR-SRF extinta.
3) Preservar qualquer registro não transferido a um sucessor.

As chaves públicas dos certificados emitidos pela AC-SRF, dissolvida, serão armazenadas por outra AC, após aprovação da AC Raiz.

Quando houver mais de uma AC interessada, assumirá a responsabilidade do armazenamento das chaves públicas, aquela indicada pela AC-SRF.

A AC-SRF, ao encerrar as suas atividades transferirá, se for o caso, a documentação dos certificados digitais emitidos à AC que tenha assumido a guarda das respectivas chaves públicas.

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

5. 5. Controles de Segurança Física, Procedimental e de Pessoas

5.1 Controle Físico

5.1.1 Construção e localização das instalações

A operação da AC-SRF é executada dentro de um ambiente físico seguro em área de instalação altamente protegida.

Os componentes do sistema de certificação utilizados para a operação da AC-SRF estão situados nas instalações do SERPRO Rio de Janeiro, Horto.

A localização e o sistema de certificação utilizado para a operação da AC-SRF não são publicamente identificados. Internamente, não são admitidos ambientes compartilhados que permitam visibilidade nas operações de emissão e revogação de certificados. Essas operações são segregadas em compartimentos fechados e fisicamente protegidos. Nenhuma das linhas telefônicas dentro do CCD oferece suporte a modems.

Alguns aspectos de construção das instalações da AC-SRF relevantes para os controles de segurança física são descritos abaixo. Outros detalhes estão descritos no restante do item 5.1.

- Todas as instalações de equipamentos de apoio, tais como: máquinas de ar condicionado, grupos geradores, *no-breaks*, baterias, quadros de distribuição de energia e de telefonia, instalações para sistemas de telecomunicações e sistema de aterramento e de proteção contra descargas atmosféricas, foram executadas por técnicos especializados para garantir a proteção física da AC-SRF.

5.1.2 Acesso físico

O acesso físico às dependências da AC-SRF é gerenciado e controlado internamente conforme o previsto na Política de Segurança da AC-SRF. Chaves, senhas, cartões, identificações biométricas ou outros dispositivos são utilizados para controle de acesso.

O acesso físico é monitorado e o seu controle assegura que apenas pessoas autorizadas participem das atividades pertinentes.

O sistema de certificação da AC-SRF está situado em uma sala-cofre. Segurança patrimonial e controles de segurança biométricos restringem o acesso aos equipamentos da sala-cofre.

5.1.2.1 Níveis de Acesso

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

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

Excetuados os casos previstos em lei, o porte de armas não é admitido nas instalações do ambiente onde estão instalados os equipamentos utilizados na operação da AC-SRF, esse procedimento ocorre a partir do nível 1. A partir desse nível, equipamentos de gravação, fotografia, telefones celulares, *pagers*, vídeo, som ou similares, bem como computadores portáteis, tem sua entrada controlada e somente podem ser utilizados mediante autorização formal e supervisão.

O segundo nível – ou nível 2 – o acesso é interno ao primeiro nível. A passagem do primeiro para o segundo nível exige identificação das pessoas autorizadas por meio eletrônico, e o uso de crachá. Esse é o nível mínimo de segurança requerido para a execução de qualquer processo operacional ou administrativo da AC-SRF.

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

No terceiro nível são controladas tanto as entradas quanto as saídas de cada pessoa autorizada. Dois tipos de mecanismos de controle são requeridos para a entrada nesse nível: a identificação individual, como cartão eletrônico, e a identificação biométrica.

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

O quarto nível - ou nível 4 – o acesso é interno ao terceiro nível, é onde ocorrem atividades especialmente sensíveis de operação da AC-SRF, tais como: emissão e revogação de certificados e emissão de LCR. Todos os sistemas e equipamentos necessários a estas atividades estão localizados a partir desse nível. O nível 4 possui os mesmos controles de acesso do nível 3 e, adicionalmente, exige em cada acesso ao seu ambiente, a identificação de, no mínimo, 2 (duas) pessoas autorizadas. Nesse nível, a permanência dessas pessoas é exigida enquanto o ambiente estiver ocupado.

No quarto nível, todas as paredes, piso e teto são revestidos de aço e concreto. As paredes, piso e o teto são inteiriços, constituindo uma célula estanque contra ameaças de acesso indevido, água, vapor, gases e fogo. Os dutos de refrigeração e de energia, bem como os dutos de comunicação, não permitem a invasão física das áreas de quarto nível. Adicionalmente, esses ambientes de nível 4 – que constituem a chamada sala cofre - possuem proteção contra interferência eletromagnética externa.

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

São dois os ambientes de quarto nível abrigados pela sala cofre:

1) Sala de equipamentos da AC-SRF de produção *on-line* e cofre de armazenamento.

2) Sala de equipamentos de rede e infra-estrutura (*firewall*, roteadores, *switches* e servidores).

No quarto nível são controladas tanto as entradas quanto as saídas de cada pessoa autorizada. Dois tipos de mecanismos de controle são requeridos para a entrada nesse nível: algum tipo de identificação individual, como cartão eletrônico, e identificação biométrica.

O quinto nível – ou nível 5 – é interno aos ambientes de nível 4, e compreende cofres e gabinetes trancados. Materiais criptográficos tais como chaves, dados de ativação, suas cópias e equipamentos criptográficos são armazenados em nível 5 ou superior.

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

1) Ser feito em aço ou material de resistência equivalente.

2) Possuir tranca com chave.

O sexto nível – ou nível 6 - consiste de pequenos depósitos localizados no interior do cofre ou gabinete de quinto nível, ou hardware criptográfico. Cada um desses depósitos dispõe de fechadura individual. A chave privada da AC-SRF esta armazenada em um desses depósitos quando não estiver em operação. Quando em operação, a chave privada da AC-SRF é armazenada em cartão criptográfico, em gabinete de nível 5.

5.1.2.2 Sistema físico de detecção

Todas as passagens entre os níveis de acesso, bem como as salas de operação de nível 4, são monitoradas por câmaras de vídeo ligadas a um sistema de gravação 24x7. O posicionamento e a capacidade dessas câmaras não permitem a recuperação de senhas digitadas nos controles de acesso.

As fitas de vídeo resultantes da gravação 24x7 são armazenadas por, no mínimo, um ano. Elas são testadas (verificação de trechos aleatórios no início, meio e final da fita) pelo menos a cada 3 (três) meses, com a escolha de, no mínimo, uma fita referente a cada semana. Essas fitas são armazenadas em ambiente de terceiro nível.

Todas as portas de passagem entre os níveis de acesso 3 e 4 do ambiente são monitoradas por sistema de notificação de alarmes. O sistema de notificação de alarmes utiliza 2 (dois) meios de notificação: sonoro e visual.

Em todos os ambientes de quarto nível, um alarme de detecção de movimentos permanece ativo enquanto não for satisfeito o critério de acesso ao ambiente. Assim que, devido à saída de um ou mais funcionários de confiança, o critério mínimo de ocupação deixar de ser satisfeito, ocorre a reativação automática dos sensores de presença.

O sistema de notificação de alarmes utiliza 2 (dois) meios de notificação: sonoro e visual.

O sistema de monitoramento das câmaras de vídeo, bem como o sistema de notificação de alarmes, são permanentemente monitorados por guarda armado e estão localizados em ambiente de nível 3. As instalações do sistema de monitoramento, por sua vez, são monitoradas por câmaras de vídeo cujo posicionamento permite o acompanhamento das ações do guarda.

5.1.2.3 Sistema de Controle de Acesso

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

5.1.2.4 Mecanismos de emergência

Mecanismos específicos foram implantados para garantir a segurança do pessoal e dos equipamentos da AC-SRF em situações de emergência. Esses mecanismos permitem o destravamento de portas por meio de acionamento mecânico, para a saída de emergência de todos os ambientes com controle de acesso. A saída efetuada por meio desses mecanismos aciona imediatamente os alarmes de abertura de portas.

Todos os procedimentos referentes aos mecanismos de emergência estão documentados. Os mecanismos e procedimentos de emergência são verificados semestralmente, por meio de simulação de situações de emergência.

5.1.3 Energia e ar condicionado

A AC-SRF possui sistema de fornecimento de energia sobressalente. Em caso de falta de energia, a AC-SRF funciona temporariamente utilizando no-breaks com autonomia

suficiente para casos onde é necessário o acionamento do gerador de apoio, que funciona durante o tempo da falta de energia.

A área de operações segura da AC-SRF é conectada a uma fonte de energia padrão. Todos os componentes críticos são conectados a provisão de energia ininterrupta (UPS), prevenindo paradas anormais no caso de uma deficiência de força, de forma a atender os requisitos de disponibilidade dos sistemas da AC-SRF e seus respectivos serviços. Um sistema de aterramento está implantado.

A área tem um sistema de ar condicionado para controlar o calor e umidade que é independente do sistema de ar condicionado de edifício.

Todos os cabos elétricos são protegidos por tubulações ou dutos apropriados. São utilizadas tubulações, dutos, calhas, quadros e caixas de passagem, de distribuição e de terminação, projetados e construídos de forma a facilitar vistorias e a detecção de tentativas de violação. São utilizados dutos separados para os cabos de energia, de telefonia e de dados.

Todos os cabos são catalogados, identificados e periodicamente vistoriados, no mínimo a cada 6 meses, na busca de evidências de violação ou de outras anormalidades.

São mantidos atualizados os registros sobre a topologia da rede de cabos, observados os requisitos de sigilo estabelecidos pela Política de Segurança da ICP-Brasil. Qualquer modificação nessa rede é previamente documentada.

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

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

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

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

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

1) Geradores de porte compatível.
2) Geradores de reserva.
3) Sistemas de *nobreaks* redundantes.
4) Sistemas redundantes de ar condicionado.

5.1.4 Exposição à água

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

5.1.5 Prevenção e proteção contra incêndio

Todas as instalações da AC-SRF possuem sistemas de prevenção contra incêndio.

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

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

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

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

5.1.6 Armazenamento de mídia

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

5.1.7 Destruição de lixo

Documentos em papel e em mídia magnética que contenham elementos confidenciais da AC-SRF, informações comercialmente sensíveis ou confidenciais são eliminadas seguramente:

1) No caso de mídias magnéticas:
   - dano físico, ou destruição completa do recurso;
   - uso de uma utilidade aprovada para esfregar ou sobrescrever mídias magnéticas;
2) No caso de material impresso, rasgando, ou destruindo através de meios aprovados.
3) No caso de documentos em papel que contenham informações classificadas como sensíveis serão trituradas antes de ir para o lixo.

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

A AC-SRF mantém instalações de contingência que atendem os requisitos mínimos estabelecidos pelo CG da ICP-Brasil. Em caso de sinistro que torne inoperantes as instalações principal, as instalações de contingência não serão atingidas e tornar-se-ão totalmente operacionais em, no máximo, 48 (quarenta e oito) horas depois de decretado o estado de contingência.

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. Um exemplo desta prática é que as pessoas que executam atividades de examinar registros de sistema, ou examinar *logs* de auditoria não são as mesmas pessoas envolvidas na atividade que gerou estes registros e *logs*, assegurando que as pessoas que executam estão agindo dentro das responsabilidades e dentro da política de segurança declarada.

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-SRF:

1) Gerente do CCD.

2) Administrador de Segurança.

3) Administrador de Banco de Dados.

4) Administrador do Sistema de Gerenciamento de Certificados.

5) Administrador do Servidor WEB.

6) Administrador do Sistema Unix.

7) Administrador do Security Sever.

8) Administrador de AC.

9) Operador.

10) Segurança patrimonial.

11) Apoio administrativo.

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.

Quando um empregado se desliga da AC-SRF, suas permissões de acesso são revogadas imediatamente. Quando há mudança na posição ou função que o empregado ocupa com relação à AC-SRF, são revistas suas permissões de acesso. Os termos de responsabilidade assinados pelo funcionário contém a descrição de todos os recursos, antes disponibilizados, que o empregado deverá devolver à AC-SRF no ato de seu desligamento.

5.2.2 Número de pessoas necessário por tarefa

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

Todas as tarefas executadas no ambiente onde está localizado o equipamento de certificação da AC-SRF necessitam da presença de no mínimo 2 (dois) empregados da AC-SRF. As demais tarefas da AC-SRF podem ser executadas por um único empregado.

5.2.3 Identificação e autenticação para cada perfil

Pessoas que ocupam os perfis designados pela AC-SRF passam por um processo rigoroso de seleção.

Todo funcionário da AC-SRF tem sua identidade e perfil verificados antes de:

1) Ser incluído em uma lista de acesso às instalações da AC-SRF.

2) Ser incluído em uma lista para acesso físico ao sistema de certificação da AC-SRF.

3) Receber um certificado para executar suas atividades operacionais na AC-SRF.

4) Receber uma conta no sistema de certificação da AC-SRF.

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

1) São diretamente atribuídos a um único empregado.

2) Não são compartilhados.

3) São restritos às ações associadas ao perfil para o qual foram criados.

A AC-SRF implementa um padrão de utilização de "senhas fortes", definido em seu Manual de Segurança e em conformidade com a Política de Segurança da ICP-Brasil, juntamente com procedimentos de validação dessas senhas.

5.3 CONTROLES DE PESSOAL

Todos os funcionários da AC-SRF e da AR-SRF, encarregados de tarefas operacionais, tem registrado em contrato ou termo de responsabilidade:

1) Os termos e as condições do perfil que ocupam.

2) O compromisso de observar as normas, políticas e regras aplicáveis da AC-SRF.

3) O compromisso de observar as normas, políticas e regras aplicáveis da ICP-Brasil.

4) O compromisso de não divulgar informações sigilosas a que tenham acesso.

5.3.1 Antecedentes, qualificação, experiência e requisitos de idoneidade

Todo o pessoal da AC-SRF envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados é admitido conforme o estabelecido na Política de Segurança da AC-SRF e na Política de Segurança da ICP-Brasil.

5.3.2 Procedimentos de Verificação de Antecedentes

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

1) Verificação de antecedentes criminais.

2) Verificação de situação de crédito.

3) Verificação de histórico de empregos anteriores.

4) Comprovação de escolaridade e de residência.

5.3.3 Requisitos de treinamento

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

1) Princípios e mecanismos de segurança da AC-SRF e das AR vinculadas.

2) Sistema de certificação em uso na AC-SRF.

3) Procedimentos de recuperação de desastres e de continuidade do negócio.

4) Outros assuntos relativos a atividades sob sua responsabilidade.

5.3.4 Freqüência e requisitos para reciclagem técnica

Todo o pessoal da AC-SRF envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados é mantido atualizado sobre eventuais mudanças tecnológicas no sistema de certificação da AC-SRF. Treinamentos de reciclagem são realizados pela AC-SRF sempre que necessário.

5.3.5 Freqüência e seqüência de rodízios de cargos

A AC-SRF não implementa rodízio de cargos.

5.3.6 Sanções para ações não autorizadas

Na eventualidade de uma ação não autorizada, real ou suspeita, realizada por pessoa responsável por processo de emissão, expedição, distribuição, revogação ou gerenciamento de certificados, a AC-SRF suspende o seu acesso ao sistema de certificação e toma as medidas administrativas e legais cabíveis.

5.3.7 Requisitos para contratação de pessoal

O pessoal da AC-SRF no exercício de atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados é contratado conforme o estabelecido na Política de Segurança da AC-SRF.

5.3.8 Documentação disponibilizada ao pessoal

A AC-SRF disponibiliza para todo o seu pessoal e para o da AR-SRF:

1) Esta DPC-SRF.

2) A PC que implementa.

3) A Política de Segurança da ICP-Brasil.

4) A Política de Segurança da AC-SRF.

5) Documentação de hardware e software relativa à função desempenhada.

6) Documentação operacional relativa às suas atividades.

7) Contratos, normas e políticas relevantes para suas atividades.

Toda a documentação fornecida ao pessoal da AC-SRF e da AR-SRF é classificada segundo a política de classificação de informação definida e é mantida atualizada.

6. 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-SRF e das AC subordinadas são gerados pelas mesmas, após seu credenciamento pela ICP-Brasil. As AC subordinadas indicarão, por intermédio de seus representantes legais, a pessoa responsável pela geração dos pares de chaves criptográficas e pelo uso do certificado.

Ao ser gerada, a chave privada da entidade titular é gravada cifrada, por algoritmo simétrico como 3-DES, IDEA, SAFER+ ou outros aprovados pelo CG da ICP-Brasil, em hardware criptográfico aprovado pelo CG da ICP - Brasil.

A chave privada trafega cifrada, empregando os mesmos algoritmos citados no parágrafo anterior, entre o dispositivo gerador e a mídia utilizada para o seu armazenamento.

O meio de armazenamento da chave privada assegura, por meios técnicos e procedimentais adequados, no mínimo, que:

• a chave privada é única e seu sigilo é suficientemente assegurado;

• a chave privada não pode, com uma segurança razoável, ser deduzida;

• a chave privada está protegida contra falsificações realizadas através das tecnologias atualmente disponíveis; e

• a chave privada pode ser eficazmente protegida pelo legítimo titular contra a utilização por terceiros.

Esse meio de armazenamento não modifica os dados a serem assinados, nem impede que esses dados sejam apresentados ao signatário antes do processo de assinatura.

Os pares de chaves da AC-SRF e das AC subordinadas são gerados em módulo criptográfico de hardware com no mínimo padrão de segurança FIPS 140-1 nível 2, utilizando algoritmo RSA para geração do par de chaves.

Os pares de chaves da AC-SRF e das AC subordinadas são gerados somente pelo Titular do Certificado correspondente.

6.1.2 Entrega da chave privada à entidade titular

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

6.1.3 Entrega da chave pública para emissor de certificado

Para a entrega de sua chave pública à AC-SRF, encarregada da emissão de seu certificado, a AC solicitante faz uso do padrão PKCS#10. Essa entrega é feita por representante legalmente constituído da AC subordinada, em data e hora previamente estabelecida pela AC-SRF.

6.1.4 Disponibilização de chave pública da AC-SRF para usuários

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

1) Formato PKCS#7 (RFC 2315), que inclui toda a cadeia de certificação, no momento da disponibilização de um certificado para seu titular.

2) Diretório.

3) Página *Web* da AC–SRF (http://www.receita.fazenda.gov.br/acsrf).

4) Outros meios seguros aprovados pelo CG da ICP-Brasil.

6.1.5 Tamanhos de chave

O tamanho das chaves criptográficas associadas a certificados emitidos pela AC-SRF será de 2048 (dois mil e quarenta e oito) bits, tamanho mínimo admitido pela ICP-Brasil para chaves criptográficas associadas a certificados de AC.

6.1.6 Geração de parâmetros de chaves assimétricas

Os parâmetros de geração de chaves assimétricas da AC-SRF seguem o padrão FIPS (*Federal Information Processing Standards*) 140-1[1] *level* 2, uma vez que utilizam *hardware* criptográfico com esta certificação.

6.1.7 Verificação da qualidade dos parâmetros

A verificação dos parâmetros de geração de chave é feita de acordo com as normas estabelecidas pelo CMVP (*Cryptographic Module Validation Program*) do NIST (*National Institute of Standards and Technology*), uma vez que o *hardware* utilizado é certificado pelo NIST como FIPS 140-1 *level* 2.

6.1.8 Geração de chave por hardware ou software

A AC-SRF utiliza componente seguro de hardware para a geração de seu par de chaves, de seu certificado, dos certificados das AC subsequente ao seu e para a geração e assinatura de sua LCR. O componente seguro de hardware utiliza um mecanismo de detecção de violação.

[1] FIPS 140-1 – *Federal Information Processing Standards* 140-1. Esse padrão será substituído pelo FIPS 140-2, hoje em fase de implantação por parte do National Institute of Standards and Technology.

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

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

As chaves privadas dos titulares de certificados emitidos pela AC-SRF são utilizadas apenas para a assinatura dos certificados por ela emitidos e de suas LCR.

6.2 Proteção da Chave Privada

A chave privada da AC-SRF é gerada, armazenada e utilizada apenas em *hardware* criptográfico específico, classificado como FIPS 140-1 *level* 2, não havendo portanto tráfego da mesma em nenhum momento.

A PC implementada pela AC-SRF define os requisitos específicos aplicáveis à proteção das chaves das AC de nível imediatamente subseqüentes ao da AC-SRF, seguindo sempre o definido pelo CG da ICP-Brasil.

6.2.1 Padrões para módulo criptográfico

Toda a geração e armazenamento da chave da AC-SRF, e também operações de assinatura de certificados pela AC-SRF, são realizadas em um módulo de *hardware* criptográfico classificado como FIPS 140-1 Nível 2.

O padrão requerido para os módulos de geração de chaves criptográficas das AC de nível imediatamente subseqüente ao da AC-SRF é o FIPS 140-1 Nível 2.

6.2.2 Controle "n de m' para chave privada

A AC-SRF implementa o controle múltiplo para a ativação e desativação da sua chave privada através de controles de acesso físico que exigem a presença de pelo menos 3 (três) de 9 (nove) custodiantes.

6.2.3 Recuperação (escrow) de chave privada

Não é permitida, no âmbito da ICP-Brasil, a recuperação (*escrow*) de chaves privadas, das AC de nível imediatamente subseqüente.

6.2.4 Cópia de segurança (backup) de chave privada

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

A AC-SRF não mantém cópia de segurança das chaves privadas das AC de nível imediatamente subseqüentes ao seu.

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

A cópia de segurança deve ser armazenada, cifrada, por algoritmo simétrico como 3-DES, IDEA, SAFER+, ou outros aprovados pelo CG da ICP-Brasil, e protegida com um nível de segurança não inferior àquele definido para a chave original.

6.2.5 Arquivamento de chave privada

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

Define-se arquivamento como o armazenamento da chave privada para seu uso futuro, após o período de validade do certificado correspondente

6.2.6 Inserção de chave privada em módulo criptográfico

A chave privada da AC-SRF é inserida no módulo criptográfico de acordo com o estabelecido na RFC 2510.

6.2.7 Método de ativação de chave privada

Para o certificado emitido em 14/10/2002 a chave privada da AC-SRF é ativada mediante a aplicação de uma senha exigida pelo *software* de certificação, pelos Administradores do Sistema de Certificação da AC-SRF. Esta senha obedece à política de senhas estabelecida pela AC-SRF.

A ativação da chave privada é realizada pelos detentores da senha de ativação da chave, devidamente autorizados, e a confirmação da identidade é feita através de senhas, só lhes sendo permitido o acesso ao ambiente em duplas devidamente autorizadas.

Para o certificado emitido a partir de 29/11/2004 a chave privada da AC-SRF é implementada por meio de cartões criptográficos, protegidos com senha, após a identificação dos detentores da chave de ativação da chave criptográfica.

6.2.8 Método de desativação de chave privada

Quando a chave privada da AC-SRF 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.

6.2.9 Método de destruição de chave privada

Além do estabelecido no item 6.2.8 desta DPC, todas as cópias de segurança da chave privada da AC –SRF serão destruídas.

As mídias de armazenamento das chaves privadas serão reinicializadas de forma a não restarem nelas informações sensíveis.

6.3 Outros Aspectos do Gerenciamento do Par de Chaves

6.3.1 Arquivamento de chave pública

A chave pública da AC-SRF e dos certificados por ela emitidos, é armazenada 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-SRF é utilizada apenas durante o período de validade do certificado correspondente. A chave pública da AC-SRF 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 de validade do certificado emitido em 14/10/2002 é de 5 anos e o certificado emitido a partir de 22/11/2004 é de 8 anos.

6.4 Dados de Ativação

6.4.1 Geração e instalação dos dados de ativação

Nenhum dado de ativação é necessário para operar os módulos criptográficos utilizados pela AC-SRF. O método de ativação das chaves privadas está descrito no item 6.2.7.

6.4.2 Proteção dos dados de ativação.

Nenhum dado de ativação é necessário para operar os módulos criptográficos utilizados pela AC-SRF. O método de ativação das chaves privadas está descrito no item 6.2.7.

6.4.3 Outros aspectos dos dados de ativação

Item não aplicável.

6.5 CONTROLES DE SEGURANÇA DOS COMPUTADORES

6.5.1 Requisitos técnicos específicos de segurança computacional

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

Os computadores servidores utilizados pela AC-SRF e pelas AC subordinadas, relacionado diretamente com os processos de emissão, expedição, distribuição, revogação ou gerenciamento de certificados, implementam, entre outras, as seguintes características:

1) Controle de acesso aos serviços e perfis da AC-SRF.

2) Separação das tarefas e atribuições relacionadas a cada perfil qualificado da AC-SRF.

3) Acesso restrito aos bancos de dados da AC-SRF.

4) Geração e armazenamento de registros de auditoria da AC-SRF.

5) Mecanismos internos de segurança para garantia da integridade de dados e processos críticos.

6) Mecanismos para cópias de segurança (*backup*).

Essas características são implementadas pelo sistema operacional ou por meio da combinação deste com o sistema de certificação e com mecanismos de segurança física.

Qualquer equipamento, ou parte deste, ao ser enviado para manutenção tem as informações sensíveis nele contidas apagadas e é efetuado controle de entrada e saída, registrando número de série e as datas de envio e de recebimento. Ao retornar às instalações onde residem os equipamentos utilizados para operação da AC-SRF ou da AC subordinada, o equipamento que passou por manutenção é inspecionado. Em todo equipamento que deixar de ser utilizado em caráter permanente, são destruídas de maneira definitiva todas as informações sensíveis armazenadas, relativas à atividade da AC-SRF ou AC subordinada. Todos esses eventos são registrados para fins de auditoria.

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

6.5.2 Classificação da segurança computacional

A AC-SRF aplica configurações de segurança conforme recomendações do SANS INSTITUTE. Também são seguidas as recomendações de segurança do ITSEC que avaliou a plataforma da solução Autoridade Certificadora CMS da Baltimore/Cybertrust.

6.6 Controles Técnicos do Ciclo de Vida

6.6.1 Controles de desenvolvimento de sistemas

A AC-SRF adota como solução no certificado emitido em 14/10/2002 o sistema CMS Baltimore/Cybertrust versão 4.0, não havendo desenvolvimento por parte da AC-SRF.

Para o certificado emitido a partir de 22/11/2004, à AC-SRF adota sistema de certificação próprio desenvolvido em código aberto.

6.6.2 Controle de gerenciamento de segurança

A administração de segurança de sistema é controlada pelos privilégios nomeados a contas de sistema operacional, e pelos papéis confiados descritos no item 5.2.1.

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

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

.6.6.3 Classificação de segurança de ciclo de vida

Item não aplicável.

6.7 Controles de Segurança de Rede

Para o certificado emitido a partir de 22/11/2004 o computador servidor que hospeda o sistema de certificação opera off-line, fisicamente desconectando de qualquer rede.

Para o certificado da AC-SRF emitido em 14/10/2002 os controles implementados para garantir a confidencialidade, integridade e disponibilidade dos serviços da AC-SRF são os seguintes:

1) Os servidores e elementos de infra-estrutura e proteção de rede, tais como roteadores, *hubs*, *switches*, *firewalls* localizados no segmento de rede que hospeda o sistema de certificação da AC-SRF, estão localizados e operam em ambiente de nível 4.

2) Os servidores e elementos de infra-estrutura e proteção de rede, tais como roteadores, *hubs*, *switches*, *firewalls* e sistemas de detecção de intrusão (IDS), que atendem o segmento de rede dos servidores web do sistema de certificação da AC-SRF, estão localizados e operam em ambiente protegido por três perímetros de segurança: os dois primeiros controlados por vigilantes e o terceiro constituído por controle de acesso biométrico.

3) 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.

4) Acesso lógico aos elementos de infra-estrutura e proteção de rede é restrito, por meio de sistema de autenticação e autorização de acesso. Os roteadores conectados a redes externas implementam filtros de pacotes de dados, que permitam somente as conexões aos serviços e servidores previamente definidos como passíveis de acesso externo.

5) Infra-estrutura de conectividade, incluindo:

- alojamento seguro de equipamento de comunicação;
- *firewall* seguro e serviços de roteador;
- serviço de LAN seguro;
- serviço *back office* seguro; e
- serviço de internet seguro e redundante.

6) Prevenção incidente e avaliação, incluindo:

- descoberta de intrusão;
- análise de vulnerabilidade;
- configuração segura de servidor; e
- auditorias técnicas.

7) administração de Infra-estrutura, incluindo:

- monitoramento de servidor;
- monitoramento de rede;
- monitoramento de URL; e
- relatórios de largura da banda.

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

6.7.1 Firewall

Para o certificado da AC-SRF emitido em 14/10/2002 mecanismos de *firewall* estão implementados em equipamentos de utilização específica, configurados exclusivamente para tal função. O *firewall* promove o isolamento, em sub-redes específicas, dos equipamentos servidores com acesso externo – a conhecida "zona desmilitarizada" (ZDM) – em relação aos equipamentos com acesso exclusivamente interno à AC-SRF. O *software* de *firewall*, entre outras características, implementa registros de auditoria.

6.7.2 Sistema de detecção de intrusão (IDS)

Para o certificado da AC-SRF emitido em 14/10/2002 são as seguintes características do IDS:

1) Capacidade de ser configurado para reconhecer ataques em tempo real e responde-los automaticamente, com medidas tais como: enviar *traps SNMP*, executar programas definidos pela administração da rede, enviar e-mail aos administradores, enviar mensagens de alerta ao *firewall* ou ao terminal de gerenciamento, promover a desconexão automática de conexões suspeitas, ou ainda a reconfiguração do *firewall*.

2) Capacidade de reconhecer diferentes padrões de ataques, inclusive contra o próprio sistema, apresentando a possibilidade de atualização da sua base de reconhecimento.

3) Prover o registro dos eventos em *logs*, recuperáveis em arquivos do tipo texto, além de implementar uma gerência de configuração.

6.7.3 Registro de acessos não autorizados à rede

Para o certificado da AC-SRF emitido em 14/10/2002 as tentativas de acesso não autorizado – em roteadores, *firewalls* ou IDS – são registradas em arquivos para análise, que é automatizada. A freqüência de exame dos arquivos de registro é diária e todas as ações tomadas em decorrência desse exame são documentadas.

6.8 Controles de Engenharia do Módulo Criptográfico

Para o certificado da AC-SRF emitido em 14/10/2002 o módulo criptográfico utilizado pela AC-SRF para o armazenamento de sua chave privada é certificado como FIPS (*Federal Information Processing Standards*) 140-1, *level* 2 e para o certificado da AC-SRF emitido em 29/11/2004 o modulo criptográfico utilizado pela AC-SRF é certificado como FIPS (*Federal Information Processing Standards*) 140-1, *level* 3.

Ao ser gerada, a chave privada da entidade titular é gravada cifrada, por algoritmo simétrico como 3-DES, IDEA, SAFER+ ou outros aprovados pelo CG da ICP-Brasil, em hardware criptográfico aprovado pelo CG da ICP - Brasil.

O meio de armazenamento da chave privada assegura, por meios técnicos e procedimentais adequados, no mínimo, que:

• a chave privada utilizada na geração de uma assinatura é única e seu sigilo é suficientemente assegurado;

• a chave privada utilizada na geração de uma assinatura não pode, com uma segurança razoável, ser deduzida e que está protegida contra falsificações realizadas através das tecnologias atualmente disponíveis; e

• a chave privada utilizada na geração de uma assinatura pode ser eficazmente protegida pelo legítimo titular contra a utilização por terceiros.

Esse meio de armazenamento não modifica os dados a serem assinados, nem impede que esses dados sejam apresentados ao signatário antes do processo de assinatura.

7. 7. Perfis de Certificado e LCR

7.1 Perfil do Certificado

Todos os certificados emitidos pela AC-SRF estão em conformidade com o formato definido pelo padrão ITU X.509.

7.1.1 Número de versão

Todos os certificados emitidos pela AC-SRF implementam a versão 3 do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 2459.

7.1.2 Extensões de certificados

Os certificados emitidos pela AC-SRF, sob esta DPC da AC-SRF, obedecem às resoluções da ICP-Brasil, que define como obrigatórias as seguintes extensões para certificados de AC:

1) "*Authority Key Identifier*", não crítica: o campo keyIdentifier contém o resumo SHA-1 da chave pública da AC-SRF.

2) "*Subject Key Identifier*", não crítica: contém o *hash* SHA-1 da chave pública da AC titular do certificado.

3) "*Key Usage*", crítica: somente os bits e keyCertSign e cRLSign são ativados.

4) "*Certificate Policies*", não crítica:

- o campo policyIdentifier contém o OID das PC que a AC titular do certificado implementa;
- o campo policyQualifiers contém o endereço *URL* da página *Web, http://www.receita.fazenda.gov.br/acsrf/dpcacsrf.pdf,* onde se obtém a DPC da AC-SRF.

5) O "Basic Constraints", crítica: contém o campo CA=TRUE.

6) "*CRL Distribution Points*", não crítica: contém o endereço *URL* da página *Web*:

- Para certificados emitidos em 14/10/2002 (http://www.receita.fazenda.gov.br/acsrf/acsrf.crl),
- Para certificados emitidos em 22/11/2004 (http://www.receita.fazenda.gov.br/acsrf/acsrfv1.crl).

7.1.3 Identificadores de algoritmos

Os certificados emitidos pela AC-SRF são assinado com o uso do algoritmo RSA com SHA-1 como função *hash* (OID = 1.2.840.113549.1.1.5), conforme o padrão PKCS#1 (RFC 2313).

7.1.4 Formatos de nome

Para os certificados emitidos sob a PC AC-SRF, o nome da AC titular do certificado, constante do campo "*Subject*", adota o "*Distinguished Name*" (DN) do padrão ITU X.500/ISO 9594, da seguinte forma:

C= BR;

O= ICP-Brasil;

OU= Secretaria da Receita Federal – SRF;

CN= nome da AC.

7.1.5 Restrições de nome

As restrições aplicáveis para os nomes dos titulares de certificados emitidos pela AC-SRF são as seguintes:

• não serão utilizados sinais de acentuação, tremas ou cedilhas;

• além dos caracteres alfanuméricos, podem ser utilizados somente os seguintes caracteres especiais:

Caractere	Código NBR9611 (hexadecimal)
Branco	20
!	21
"	22
#	23
$	24
%	25

&	26
'	27
(	28
)	29
*	2A
+	2B
,	2C
-	2D
.	2E
/	2F
:	3A
;	3B
=	3D
?	3F
@	40
\	5C

7.1.6 OID (Object Identifier) de DPC

O Identificador de Objeto (OID) desta DPC, atribuído pela ICP-Brasil para a AC-SRF após conclusão do processo de seu credenciamento, é 2.16.76.1.1.8.

7.1.7 Uso da extensão "Policy Constraints"

Não se aplica.

7.1.8 Sintaxe e semântica dos qualificadores de política

O campo policy Qualifiers da extensão "Certificate Policies" contém o endereço Web da DPC da AC-SRF, http://www.receita.fazenda.gov.br/acsrf/dpcacsrf.pdf.

7.1.9 Semântica de processamento para extensões criticas

Extensões críticas são interpretadas, no âmbito da AC-SRF, conforme a RFC 2459.

7.2 PERFIL DE LCR

7.2.1 Número (s) de versão

As LCR geradas pela AC-SRF implementam a versão 2 do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 2459.

7.2.2 Extensões de LCR e de suas entradas

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

1) "*Authority Key Identifier*": contém o resumo SHA-1 da chave pública da AC-SRF.

2) "*CRL Number*", não crítica: contém número seqüencial para cada LCR emitida.

8. 8. Administração de Especificação

8.1 PROCEDIMENTOS DE MUDANÇA DE ESPECIFICAÇÃO

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

8.2 POLÍTICAS DE PUBLICAÇÃO E DE NOTIFICAÇÃO

A AC-SRF publica essa DPC em sua página *Web* (http://www.receita.fazenda.gov.br/acsrf/dpcacsrf.pdf). Sempre que essa DPC for atualizada será alterado o arquivo disponibilizado na *Web*.

8.3 PROCEDIMENTOS DE APROVAÇÃO

Essa DPC foi submetida à aprovação do CG da ICP-Brasil, durante o processo de credenciamento da AC-SRF, conforme o determinado pelo documento "Critérios e Procedimentos para Credenciamento das Entidades Integrantes da ICP-Brasil".

Receita Federal

Política de Certificados da Autoridade Certificadora da SRF

PC AC-SRF

SECRETARIA DA RECEITA FEDERAL

Versão 1.0

SUMÁRIO

1.1 VISÃO GERAL 4
1.2 IDENTIFICAÇÃO 4
1.3 COMUNIDADE E APLICABILIDADE 4
1.4 DADOS DE CONTATO 5

2. DISPOSIÇÕES GERAIS 6

2.1 OBRIGAÇÕES E DIREITOS 6
2.2 RESPONSABILIDADES 9
2.3 RESPONSABILIDADE FINANCEIRA 9
2.4 INTERPRETAÇÃO E EXECUÇÃO 9
2.5 TARIFAS DE SERVIÇO 10
2.6 PUBLICAÇÃO E REPOSITÓRIO 11
2.7 AUDITORIA DE CONFORMIDADE 12
2.8 SIGILO 15
2.9 DIREITOS DE PROPRIEDADE INTELECTUAL 17

3. IDENTIFICAÇÃO E AUTENTICAÇÃO 17

3.1 REGISTRO INICIAL 17
3.2 GERAÇÃO DE NOVO PAR DE CHAVES ANTES DA EXPIRAÇÃO DO ATUAL 20
3.3 GERAÇÃO DE NOVO PAR DE CHAVES APÓS REVOGAÇÃO 20
3.4 SOLICITAÇÃO DE REVOGAÇÃO 20

4. REQUISITOS OPERACIONAIS 21

4.1 SOLICITAÇÃO DE CERTIFICADO 21
4.2 EMISSÃO DE CERTIFICADO 21
4.3 ACEITAÇÃO DE CERTIFICADO 22
4.4 SUSPENSÃO E REVOGAÇÃO DE CERTIFICADO 22
4.5 PROCEDIMENTOS DE AUDITORIA DE SEGURANÇA 25
4.6 ARQUIVAMENTO DE REGISTROS 29
4.7 TROCA DE CHAVE 31
4.8 COMPROMETIMENTO E RECUPERAÇÃO DE DESASTRE 31

4.9 EXTINÇÃO DA AC-SRF OU AR-SRF 32

5. CONTROLES DE SEGURANÇA FÍSICA, PROCEDIMENTAL E DE PESSOAL 33

5.1 CONTROLES FÍSICOS 33
5.2. CONTROLES PROCEDIMENTAIS 39
5.3 CONTROLES DE PESSOAL 41

6. CONTROLES TÉCNICOS DE SEGURANÇA 43

6.1. GERAÇÃO E INSTALAÇÃO DO PAR DE CHAVES 43
6.3. OUTROS ASPECTOS DO GERENCIAMENTO DO PAR DE CHAVES 47
6.4. DADOS DE ATIVAÇÃO 48
6.5. CONTROLES DE SEGURANÇA COMPUTACIONAL 48
6.6. CONTROLES TÉCNICOS DO CICLO DE VIDA 49
6.7. CONTROLES DE SEGURANÇA DE REDE 50
6.8. CONTROLES DE ENGENHARIA DE MÓDULO CRIPTOGRÁFICO 50

7. PERFIS DE CERTIFICADO E LCR 51

7.1. PERFIL DO CERTIFICADO 51
7.2. PERFIL DE LCR 53

8. ADMINISTRAÇÃO DE ESPECIFICAÇÃO 54

8.1. PROCEDIMENTOS DE MUDANÇA DE ESPECIFICAÇÃO 54
8.2. POLÍTICAS DE PUBLICAÇÃO E NOTIFICAÇÃO 54
8.3. PROCEDIMENTOS DE APROVAÇÃO 54

1. INTRODUÇÃO

1.1 VISÃO GERAL

Este documento descreve a Política de Certificados da Autoridade Certificadora da SRF (AC-SRF), doravante denominada PC AC-SRF, implementada sob a Declaração de Práticas de Certificação da Autoridade Certificadora da SRF (DPC AC-SRF).

Ela é dirigida a todos aqueles que necessitam verificar a confiabilidade da AC-SRF e verificar a adequabilidade de seus certificados às exigências de segurança da AC-SRF.

1.2 IDENTIFICAÇÃO

Esta PC AC-SRF segue as recomendações da ICP-Brasil para emissão de certificados digitais para autoridades certificadoras de nível imediatamente subseqüente ao da AC-SRF.

O OID desta PC AC-SRF é: 2.16.76.1.1.8.

1.3 COMUNIDADE E APLICABILIDADE

1.3.1 Autoridades Certificadoras

Esta PC AC-SRF é implementada pela AC-SRF, cuja DPC AC-SRF encontra-se publicada na página (http://www.receita.fazenda.gov.br/acsrf/dpcacsrf.pdf).

1.3.2 Autoridade de Registro (AR)

A responsável pelo processo de recebimento, validação e encaminhamento de solicitações de emissão e revogação de certificados digitais para AC de nível imediatamente subseqüente ao da AC-SRF, e pela confirmação da identidade de seus solicitantes, é a Autoridade de Registro da Secretaria da Receita Federal (AR-SRF), cujos procedimentos estão em conformidade com esta Política de Certificado.

1.3.3 Titulares de Certificado

Os titulares dos certificados são as entidades pessoas jurídicas, autorizadas pela AR-SRF a receberem certificados digitais emitidos pela AC-SRF, cujos nomes aparecem no certificado digital, no campo "*Distinguished Name (DN)*".

Será 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.

1.3.4 Aplicabilidade

Os certificados definidos por esta PC AC-SRF têm sua utilização exclusiva para a assinatura de certificados digitais e de Lista de Certificados Revogados (LCR).

1.4 DADOS DE CONTATO

1.4.1 Organização da Administração da PC AC-SRF

Esta PC é administrada pela Coordenação-Geral de Tecnologia e Segurança da Informação (COTEC) da Secretaria da Receita Federal.

Nome: Secretaria da Receita Federal

- ✓ Endereço: Ministério da Fazenda, Anexo A, Sala 301.
- ✓ Telefone: (550xx61) 412 3708, 412 3710, 412 3713.
- ✓ Fax: (550xx61) 412 1533.
- ✓ Página *Web*: http://www.receita.fazenda.gov.br.
- ✓ *E-mail*: ac-srf@receita.fazenda.gov.br.

1.4.2 Pessoas de Contato

Nome: Ariosto Rodrigues de Souza Junior.

- ✓ Endereço: SRF - Ministério da Fazenda, Anexo A, Sala 339.
- ✓ Telefone: (550xx61) 412 3741, 412 3743.
- ✓ Fax: (550xx61) 412 1547.
- ✓ *E-mail*: ariosto.souza@receita.fazenda.gov.br.

Nome: Sergio Roberto Fuchs da Silva.

- ✓ Endereço: SRF - Ministério da Fazenda, Anexo A, Sala 339.
- ✓ Telefone: (550xx61) 412 3776, 412 3743.

- ✓ Fax: (550xx61) 412 1547.
- ✓ *E-mail*: sergio.fuchs@receita.fazenda.gov.br.

1. 2. DISPOSIÇÕES GERAIS

2.1 OBRIGAÇÕES E DIREITOS

2.1.1 Obrigações da Autoridade Certificadora

As obrigações da AC-SRF são as abaixo relacionadas:

1. Operar de acordo com a DPC AC-SRF e com esta PC AC-SRF.
2. Adotar as medidas cabíveis para assegurar que usuários e demais entidades envolvidas tenham conhecimento de seus respectivos direitos e obrigações.
3. Gerar e gerenciar o seu par de chaves criptográficas.
4. Assegurar a proteção de sua chave privada.
5. Notificar as AC de nível imediatamente subseqüente ao seu quando ocorrer: suspeita de comprometimento de sua chave, emissão de novo par de chaves e correspondente certificado ou o encerramento de suas atividades.
6. Distribuir o seu próprio certificado.
7. Emitir, expedir e distribuir os certificados das AC de nível imediatamente subseqüente ao seu;
8. Informar a emissão do certificado ao respectivo solicitante.
9. Revogar os certificados por ela emitidos.
10. Emitir, gerenciar e publicar sua Lista de Certificados Revogados (LCR).
11. Identificar e registrar todas as ações executadas, conforme as normas, práticas e regras estabelecidas pelo Comitê Gestor da ICP-Brasil (CG ICP-Brasil).
12. Publicar em sua página *web* (http://www.receita.fazenda.gov.br/acsrf) a DPC AC-SRF e a PC AC-SRF aprovadas.
13. Adotar as medidas de segurança e controle previstas na PC, DPC e Política de Segurança que implementar, envolvendo seus processos, procedimentos e atividades, observadas as normas, critérios, práticas e procedimentos da ICP-Brasil.

14. Manter a conformidade dos seus processos, procedimentos e atividades com as normas, práticas e regras da ICP-Brasil e com a legislação vigente.

15. Manter e garantir a integridade, o sigilo e a segurança da informação por ela tratada.

16. Manter e testar regularmente seu Plano de Continuidade do Negócio.

17. Não emitir certificado com prazo de validade que se estenda além do prazo de validade de seu próprio certificado.

2.1.2 Obrigações da AR-SRF

As obrigações da AR-SRF são as abaixo relacionadas:

1. Receber solicitações de emissão e revogação de certificados e respectivos documentos de identificação armazenado-os conforme critérios estabelecidos pelo CG da ICP-Brasil.

2. Confirmar a identidade do solicitante e a validade da solicitação, de acordo com os requisitos estabelecidos pelos itens 3 e 4 desta PC AC-SRF.

3. Encaminhar a solicitação de emissão e de revogação de certificado à AC-SRF utilizando VPN (virtual private network - rede privativa virtual), SSL (secure socket layer - protocolo de comunicação seguro) ou outra tecnologia de igual ou superior nível de segurança e privacidade.

4. Utilizar VPN (virtual private network - rede privativa virtual), SSL (secure socket layer - protocolo de comunicação seguro) ou outra tecnologia de igual ou superior nível de segurança e privacidade, ao disponibilizar serviços para os solicitantes ou usuários de certificados digitais via web.

5. Informar aos respectivos titulares a emissão ou a revogação de seus certificados.

6. Disponibilizar os certificados emitidos pela AC-SRF aos seus respectivos solicitantes.

7. Identificar e registrar todas as ações executadas, conforme as normas, práticas e regras estabelecidas pelo CG da ICP-Brasil.

8. Manter a conformidade dos seus processos, procedimentos e atividades com as normas, critérios, práticas e regras estabelecidas pela AC a qual está vinculada.

9. Manter e garantir a segurança da informação por ela tratada, de acordo com o estabelecido nas normas, critérios, práticas e procedimentos da ICP – Brasil.

10. Oferecer treinamento aos seus agentes de registro, especialmente quanto ao reconhecimento de assinaturas e validade dos documentos apresentados na forma dos itens 3.1.8 e 3.1.9.

2.1.3 Obrigações do Titular do Certificado

As obrigações dos titulares de certificados emitidos de acordo com esta PC AC-SRF são as abaixo relacionadas:

1. Fornecer, de modo completo e preciso, todas as informações necessárias para sua identificação.
2. Garantir a proteção e o sigilo de suas chaves privadas, senhas e dispositivos criptográficos.
3. Utilizar os seus certificados e suas respectivas chaves privadas de modo apropriado, conforme o previsto nesta PC AC-SRF.
4. Conhecer os seus direitos e obrigações, contemplados nesta PC AC-SRF, na DPC da AC-SRF e em outros documentos aplicáveis da ICP-Brasil.
5. Informar à AC-SRF qualquer comprometimento de sua chave privada e solicitar a imediata revogação do certificado correspondente.

Por se tratar de certificado emitido para pessoa jurídica, estas obrigações se aplicam ao responsável pelo uso do certificado.

2.1.4 Direitos da terceira parte (Relying Party)

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

Constituem direitos da terceira parte:

1. Recusar a utilização do certificado para fins diversos dos previstos nesta PC AC-SRF.
2. Verificar, a qualquer tempo, a validade do certificado. Um certificado emitido pela AC-SRF é valido quando:
   a) não constar da LCR da AC SRF;
   b) não estiver expirado; e
   c) puder ser verificado com o uso de certificado válido da AC SRF.

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

2.1.5 Obrigações do Repositório

O repositório da AC-SRF está disponível para consulta durante 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, possuindo os recursos necessários para a segurança dos dados nele armazenados. Disponibiliza, ainda, logo após a sua emissão, os certificados emitidos pela AC-SRF e sua LCR.

2.2 RESPONSABILIDADES

2.2.1 Responsabilidades da AC-SRF

A Autoridade de Certificadora da SRF responde pelos danos a que der causa. A AC-SRF responde solidariamente pelos atos das AC da cadeia a ela subordinadas.

2.2.2 Responsabilidades da AR-SRF

A AR-SRF será responsável pelos danos a que der causa.

2.3 RESPONSABILIDADE FINANCEIRA

2.3.1. Indenizações devidas pela terceira parte (Relying Party)

Não existe situação específica de utilização do certificado da AC-SRF que requeira prática de indenização pelos Usuários de Certificados, exceto na prática de ato ilícito.

2.3.2. Relações Fiduciárias

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

2.3.3. Processos Administrativos

Será seguida a legislação específica uma vez que a AC-SRF e a AR-SRF são administradas pela Secretaria da Receita Federal, órgão da Administração Pública Federal.

2.4 INTERPRETAÇÃO E EXECUÇÃO

2.4.1 Legislação

Atos e regulamentos federais que regulam os assuntos do governo também regulam esta PC no que diz respeito a sua aplicação, construção, interpretação e validade. Isto inclui leis e regulamentos que governam os seguintes relacionamentos:

1)Governo Federal e seus funcionários, incluindo empregados contratados por tempo indeterminado ou temporários e consultores sobre contrato.

2)Governo Federal e organizações do setor privado com relações de negócio estabelecidas.

3)Funcionários do Governo Federal com outros funcionários do Governo Federal.

A PC ACSRF obedece às leis da República Federativa do Brasil e atende aos requisitos da legislação em vigor, incluindo a Medida Provisória nº 2200-2, de 24 de agosto de 2001, bem como as Resoluções do CG da ICP-Brasil.

2.4.2 Forma de interpretação e notificação

No caso de uma ou mais das disposições desta PC 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.

As práticas descritas nesta PC não prevalecerão sobre as normas, critérios, práticas e procedimentos da ICP-Brasil.

Todas solicitações, notificações ou quaisquer outras comunicações necessárias sujeitas às práticas descritas na PC serão realizadas por iniciativa da AC-SRF por intermédio de seus responsáveis.

2.4.3 Procedimentos de solução de disputa

Esta PC AC-SRF não prevalece sobre as normas, critérios, práticas e procedimentos da ICP-Brasil, sendo a norma, critério ou prática divergentes, alterada nesta PC AC-SRF de forma a torná-la compatível.

2.5 TARIFAS DE SERVIÇO

Não há tarifas previstas pela AC-SRF para os serviços prestados às AC de nível imediatamente subseqüente ao seu.

2.5.1 Tarifas de emissão e renovação de certificados

Não há tarifas previstas pela AC-SRF para os serviços prestados às AC de nível imediatamente subseqüente ao seu.

2.5.2 Tarifas de acesso ao certificado

Não há tarifas previstas pela AC-SRF para os serviços prestados às AC de nível imediatamente subseqüente ao seu.

2.5.3 Tarifas de revogação ou de acesso a informação de status

Não há tarifas previstas pela AC-SRF para os serviços prestados às AC de nível imediatamente subseqüente ao seu.

2.5.4 Tarifas para outros serviços

Não há tarifas previstas pela AC-SRF para os serviços prestados às AC de nível imediatamente subseqüente ao seu.

2.5.5 Política de reembolso

Não há política de reembolso prevista pela AC-SRF, pelos serviços prestados às AC de nível imediatamente subseqüente ao seu.

2.6 PUBLICAÇÃO E REPOSITÓRIO

2.6.1 Publicação de informação da AC-SRF

A AC-SRF publica em sua página *web*, (http://www.receita.fazenda.gov.br/acsrf), as seguintes informações:

- seu próprio certificado;
- sua LCR;
- sua DPC AC-SRF;
- esta PC AC-SRF;
- legislação especifica da SRF;
- o endereço da instalação técnica da AR-SRF;
- leiaute do certificado e-CPF e e-CNPJ; e
- lista de certificados emitidos

A disponibilidade da página web é de, no mínimo, 99,0% (noventa e nove vírgula zero por cento) do mês, 24 (vinte e quatro) horas por dia, 7(sete) dias por semana.

2.6.2 Freqüência de publicação

As informações de que trata o item anterior serão publicadas tão logo sejam atualizadas e, no caso da LCR, a mesma será publicada imediatamente após sua emissão.

2.6.3 Controles de acesso

Somente a AC-SRF, por seus funcionários competentes e designados especialmente para esse fim, pode alterar as informações constantes nesta PC AC-SRF, após haver obtido a competente autorização do CG da ICP-Brasil.

Somente a AC-SRF, por seus funcionários competentes e designados especialmente para esse fim, pode efetuar as necessárias atualizações em sua LCR.

O certificado da AC-SRF e os certificados emitidos pela AC-SRF não podem ser modificados. Caso se faça necessário modificar os dados contidos nos mesmos, estes serão revogados.

Não há restrições de acesso para leitura desta PC AC-SRF, da DPC AC-SRF e da LCR.

Todas as informações disponibilizadas pela AC-SRF, conforme o item 2.6.1 desta PC AC-SRF, estão disponíveis para leitura sem restrições.

2.6.4 Repositório

O repositório da AC-SRF pode ser acessado através da página (http://www.receita.fazenda.gov.br/acsrf), utilizando os protocolos de acesso https e http.

Os repositórios estão disponíveis em no mínimo 99,0% (noventa e nove vírgula zero por cento), 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.

Somente a AC-SRF, por seus funcionários competentes e designados especialmente para esse fim, pode alterar as informações constantes nos repositórios. Os requisitos do item 5 desta PC AC-SRF serão observados para os repositórios.

2.7 AUDITORIA DE CONFORMIDADE

A AC Raiz será responsável pela auditoria dos processos, procedimentos e atividades de todas as AC integrantes da ICP-Brasil e das AR a elas vinculadas. A auditoria dessas entidades é realizada com o objetivo de verificar a conformidade com suas respectivas DPC, PC, Política de Segurança e demais normas e procedimentos estabelecidos pela ICP - Brasil.

A AC-SRF disponibiliza à AC Raiz relatórios anuais de auditoria das entidades da ICP-Brasil a ela subordinadas diretamente.

2.7.1 Freqüência de auditoria de conformidade

As AC credenciadas pelo CG da ICP-Brasil subordinadas à AC-SRF, suas AR e seus prestadores de serviço sofrem auditoria:

- previamente ao seu credenciamento pela AC Raiz e à sua habilitação pela AC-SRF; e

- a qualquer tempo, sem aviso prévio, pela AC Raiz ou pela AC-SRF.

Adicionalmente, as AC de nível imediatamente subseqüente ao da AC-SRF, para fins de continuidade do credenciamento, apresentarão anualmente relatório de auditoria fornecido por empresa de auditoria especializada e independente, contratada pela AC credenciada e autorizada pela AC Raiz.

2.7.2 Identidade/Qualificações do Auditor

Os relatórios de auditoria das AC de nível imediatamente subseqüente à AC-SRF são fornecidos por empresa de auditoria especializada e independente, contratada pela AC a ser auditada e autorizada pela AC Raiz.

Os relatórios de auditoria das AR e dos prestadores de serviço de suporte não precisam ser fornecidos por empresa de auditoria especializada e independente, podendo ser elaborados pela AC-SRF.

2.7.3 Relação entre auditor e parte auditada

No caso de contratação de auditoria independente, o auditor deve ser totalmente independente da AC auditada. Ao auditor, sem prejuízo do disposto nesta PC, aplicam-se, no que couber, as regras de suspeição e impedimento estabelecidas nos arts. 134 e 135 do Código de Processo Civil.

O auditor, no caso de contratação de auditoria independente, será declarado impedido de realizar auditoria, quando:

1) houver motivo íntimo declarado.

2) for amigo íntimo ou inimigo capital de membros da AC auditada.

3) for credor ou devedor da AC auditada ou de um de seus membros.

4) tiver recebido, nos últimos 5 anos, da AC auditada, pagamentos referentes à prestação de serviços de outra natureza.

5) tiver interesse no resultado da auditoria da AC auditada.

6) houver relacionamento, de fato ou de direito, como cônjuge, parente, consangüíneo ou afim, com algum dos membros da AC auditada, em linha reta ou na colateral até o terceiro grau.

O auditor firmará declaração, sob as penas da lei, de que não se enquadra em qualquer das causas de impedimento.

2.7.4 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 em um sistema de AC ou de AR serão 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 por uma auditoria de conformidade incluem, dentre outros:

1) Política de Segurança.
2) Segurança física.
3) Avaliação de tecnologia.
4) Administração dos serviços.
5) Investigação de pessoal.
6) PC e DPC utilizadas.
7) Contratos.
8) Considerações de sigilo.

2.7.5 Medidas adotadas em caso de não conformidade

Cabe à entidade auditada cumprir, no menor dos prazos estipulados, as recomendações dos auditores para corrigir os casos de não conformidade com a legislação ou com as políticas, normas, práticas e regras estabelecidas. O não cumprimento das recomendações, no prazo estipulado, acarretará a revogação do seu certificado pela AC-SRF.

A AC-SRF, em casos de iminente dano irreparável ou de difícil reparação a terceiros, poderá suspender cautelarmente, no todo ou em parte, a emissão de certificados pela AC de nível imediatamente subseqüente ao seu.

2.7.6 Comunicação de resultados

Os auditores somente informam os resultados da auditoria à entidade auditada, à AC-SRF e à AC Raiz da ICP-Brasil.

2.8 SIGILO

A chave privada de assinatura digital da AC-SRF foi gerada e é mantida pela própria AC-SRF, que é responsável pelo seu sigilo.

A divulgação ou utilização indevida da chave privada de assinatura pela AC-SRF é de sua inteira responsabilidade.

Os titulares de certificados emitidos pela AC-SRF, ou os responsáveis pelo seu uso, terão as atribuições de geração, manutenção e sigilo de suas respectivas chaves privadas. Além, disso, são responsáveis pela divulgação ou utilização indevidas dessas mesmas chaves.

2.8.1 Tipos de informações sigilosas

Como princípio geral, todo documento, informação ou registro fornecido à AC-SRF ou à AR-SRF é sigiloso.

2.8.2 Tipos de informações não sigilosas

Não são considerados como informações sigilosas pela AC-SRF e pela AR-SRF:

- os certificados e a LCR emitidos pela AC-SRF,
- as informações de identificação que façam parte de certificados ou de diretórios públicos;
- a DPC AC-SRF;
- esta PC AC-SRF;
- as versões públicas da PS AC-SRF;
- os resultados finais de auditorias.

2.8.3 Divulgação de informação de revogação e de suspensão de certificado

A AC-SRF disponibiliza permanentemente em sua página (http://www.receita.fazenda.gov.br/acsrf), relação de certificados por ela emitidos e posteriormente revogados através de consulta à LCR.

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

Os motivos que justificaram a revogação são mantidos confidenciais pela AC-SRF e pela AR-SRF, exceto quando o titular do certificado revogado autorizar expressamente a sua divulgação a terceiros ou quando esses motivos tenham sido ou venham a ser publicados, ou sejam ou venham a se tornar de domínio público, desde que tal publicação ou publicidade não tenha sido, de qualquer forma, ocasionada por culpa ou interferência indevida da AC-SRF ou da AR-SRF, ou ainda quando tais motivos sejam

requisitados por determinação judicial ou governamental, caso em que a AC-SRF ou a AR-SRF, se estiver obrigada a divulgá-los, comunicará previamente ao titular do certificado a existência de tal determinação.

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

2.8.4 Quebra de sigilo por motivos legais

As informações fornecidas pelo solicitante ou titular do certificado, bem assim os documentos e registros relativos ao solicitante, ao titular do certificado, à solicitação ou ao certificado emitido não são mantidos sob sigilo pela AC-SRF ou pela AR-SRF quando a lei prevê a sua publicidade ou divulgação ou por ordem judicial.

2.8.5 Informações a terceiros

A AC-SRF não fornece nem fornecerá a terceiros nenhum documento, informação ou registro sob sua guarda, exceto nas hipóteses mencionadas nos itens 2.8.4, 2.8.6 e 2.8.7 desta PC AC-SRF.

2.8.6 Divulgação por solicitação do titular

O titular do certificado, ou seu representante legal devidamente identificado, qualificado e autorizado, tem e terá sempre acesso às informações que lhe dizem respeito, que estejam sob a guarda da AC-SRF ou da AR-SRF, em razão da solicitação e da emissão do certificado digital. O titular do certificado pode autorizar a AC-SRF ou a AR-SRF a divulgar tais informações a terceiros ou unicamente às pessoas que indique nessa autorização. Para tanto a solicitação de liberação de informações será acompanhada de autorização formal do titular do certificado.

2.8.7 Outras circunstâncias de divulgação de informação

A AC-SRF e a AR-SRF podem divulgar informações que não sejam consideradas sigilosas pelo fato de:

a) estarem na posse legítima da AC-SRF ou da AR-SRF antes de seu fornecimento pelo solicitante ou titular do certificado ou o solicitante ou titular do certificado houver autorizado a sua divulgação;

b) posteriormente ao seu fornecimento pelo solicitante ou titular do certificado, terem sido obtidas ou puderem ter sido obtidas legalmente de um terceiro com direitos legítimos para sua divulgação sem quaisquer restrições; e

c) terem sido requisitadas por determinação judicial ou governamental, obrigando-se a AC-SRF, nesse caso, a comunicar previamente, se possível, e de imediato o solicitante ou titular do certificado a existência de tal determinação.

2.9 DIREITOS DE PROPRIEDADE INTELECTUAL

A emissão do certificado não implica na transferência, cessão ou licença de direitos de propriedade intelectual de softwares, certificados, políticas, especificações de práticas e procedimentos, nomes, chaves criptográficas e outros da AC-SRF ou da AR-SRF para o solicitante.

2. 3. IDENTIFICAÇÃO E AUTENTICAÇÃO

3.1 REGISTRO INICIAL

A AR-SRF efetua a identificação e autenticação da AC subordinada, com base nos dados fornecidos no formulário de solicitação e nos documentos exigidos nesta PC AC-SRF.

A AR-SRF realiza a autenticação da identidade de uma organização (item 3.1.8) e a autenticação da identidade de um indivíduo (item 3.1.9) por meio de, no mínimo, dois agentes de registro responsáveis pelo recolhimento e verificação da validade dos documentos apresentados.

3.1.1 Tipos de nomes

A AC-SRF emite certificados com nomes que permitem a identificação unívoca. Para isso utiliza o "distinguished name" do padrão ITU X.500.

O certificado emitido para AC subordinadas não incluirão o nome da pessoa física responsável.

3.1.2 Necessidade de nomes significativos

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

3.1.3 Regras para interpretação de vários tipos de nomes

Não se aplica.

3.1.4 Unicidade de nomes

Os identificadores do tipo "Distinguished Name" (DN) são únicos para cada entidade titular de certificado, no âmbito da AC-SRF. Números ou letras adicionais podem ser incluídos ao nome de cada entidade para assegurar a unicidade do campo.

3.1.5 Procedimento para resolver disputa de nomes

A AC-SRF se reserva o direito de tomar todas as decisões referentes a disputas de nomes das entidades solicitantes de certificados. Durante o processo de confirmação de identidade, cabe à entidade solicitante do certificado provar o seu direito de uso de um nome específico.

3.1.6 Reconhecimento, autenticação e papel de marcas registradas

De acordo com a legislação em vigor.

3.1.7 Método para comprovar a posse de chave privada

A confirmação que a entidade solicitante possui a chave privada correspondente à chave pública para a qual está sendo solicitado o certificado digital é realizada seguindo o padrão RFC 2510, item 2.3.

3.1.8 Autenticação da identidade de uma organização

A confirmação da identidade de pessoa jurídica responsável pela solicitação de certificado da AC subseqüente é realizada mediante a apresentação dos seguintes documentos:

- ✓ Registro comercial, no caso de empresa individual;
- ✓ Ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado, em se tratando de sociedades comerciais ou civis, e, no caso de sociedade por ações, acompanhado de documentos de eleição de seus administradores;
- ✓ Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas (CNPJ);
- ✓ Prova de inscrição no Cadastro Especifico do INSS (CEI), se aplicável.

A pessoa física responsável pela AC subordinada será identificada na forma descrita no item seguinte.

3.1.9 Autenticação da identidade de um indivíduo

A confirmação da identidade da pessoa física responsável pela AC subordinada a AC SRF será realizada mediante a presença física do interessado, com base em documentos legalmente aceitos.

É mantido arquivo contendo o tipo e os detalhes do procedimento de identificação utilizado pela AR-SRF.

3.1.9.1 Documentos para identificação

Devem ser apresentados, acompanhados de cópia, no mínimo os seguintes documentos:

- Uma foto recente;
- Cédula de Identidade ou Passaporte, se estrangeiro;
- Cadastro de Pessoa Física (CPF);
- Comprovante de Residência;
- Número de identificação Social-NIS (Cadastro do Programa de Integração Social-PIS, Cadastro do Programa de Formação do Patrimônio do Servidor Público-PASEP ou Cadastro de Contribuintes Individuais do INSS-CI), se aplicável;
- Cadastro Especifico do INSS-CEI, se aplicável;
- Titulo de eleitor, se aplicável;
- Os documentos acima relacionados do responsável, caso o solicitante seja incapaz.

Entende-se por cédula de identidade as carteiras instituídas por lei, desde que contenham foto e às mesmas seja atribuída fé pública em todo o território nacional, tais como: Carteira de Identidade emitida pela Secretaria de Segurança Pública, Carteira Nacional de Habilitação, Carteira de Identidade Funcional, Carteira de Identidade Profissional.

O representante legal da AC subordinada assina o termo de titularidade denominado "Termo de Titularidade" e é, para todos os efeitos legais Titular do Certificado emitido.

A pessoa física indicada como responsável pelo certificado assina o termo de responsabilidade denominado "Termo de Acordo".

Os Termos de Titularidade e de Acordo serão mantidos junto à documentação exigida neste item.

Tanto a pessoa jurídica titular do certificado, como a pessoa física designada como responsável pelo certificado, serão responsáveis, pela correta utilização deste conforme as normas da ICP-Brasil, assim como pelos danos a que derem causa pelo uso indevido do certificado.

3.1.9.2 Certificado Emitido para Pessoa Física

Não se aplica aos certificados emitidos sob esta política.

3.1.9.3 Certificado Emitido para Pessoa Jurídica.

Não se aplica aos certificados emitidos sob esta política.

3.1.9.4 Certificado Emitido para Equipamentos ou Aplicação

Não se aplica aos certificados emitidos sob esta política.

3.2 GERAÇÃO DE NOVO PAR DE CHAVES ANTES DA EXPIRAÇÃO DO ATUAL

Antes de sua expiração pode ser solicitado um novo certificado, enviando-se à AR-SRF uma solicitação, por meio eletrônico, assinada digitalmente com o uso de certificado vigente, que seja pelo menos do mesmo nível de segurança, limitada a 3 (três) ocorrências sucessivas.

Nos demais casos ou quando o solicitante não utilizar o meio eletrônico, seu titular poderá solicitar um novo certificado, preenchendo "Formulário de Solicitação de Renovação de Certificado para Desenvolver Atividades de Autoridade Certificadora Habilitada", disponibilizado na página da AC-SRF (www.receita.fazenda.gov.br/acsrf), e entregá-lo à AR-SRF. A emissão de um novo certificado obedece ao estabelecido nesta PC AC-SRF.

3.3 GERAÇÃO DE NOVO PAR DE CHAVES APÓS REVOGAÇÃO

Após a revogação do certificado de AC de nível imediatamente subseqüente ao da AC-SRF, a AC subordinada executará os processos regulares de geração de seu novo par de chaves.

3.4 SOLICITAÇÃO DE REVOGAÇÃO

A solicitação de revogação de certificado será feita por meio de formulário específico disponível na página (http://www.receita.fazenda.gov.br/acsrf). Este formulário será preenchido e assinado pelo responsável pela AC subordinada ou pela AR-SRF, permitindo a identificação inequívoca do solicitante.

3. 4. REQUISITOS OPERACIONAIS

4.1 SOLICITAÇÃO DE CERTIFICADO

A solicitação de emissão de um Certificado Digital para Autoridade Certificadora habilitada será feita mediante o formulário colocado à disposição do solicitante na página (*http://www.receita.fazenda.gov.br/acsrf*). Toda referência a formulário será entendida também como referência a outras formas que a AC-SRF possa vir a adotar.

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

1) A comprovação de atributos de identificação constantes do certificado.

2) Para o certificado emitido em 14/10/2002 a autenticação do agente de registro responsável pelas solicitações de emissão e de revogação de certificados mediante o uso de certificado digital que tenha requisitos de segurança, no mínimo, equivalente a de um certificado de nível A3, para os certificados a partir 21/11/2004, a solicitação de emissão de certificados passou a ser realizada em ambiente off-line, sendo a chave privada da AC-SRF ativada com a presença de de "3" dos "9" dos detentores de partição de chave de ativação.

a a chave é ativada com a presença dos detentores da chave de ativação.

3) Assinatura do Termo de Titularidade e do Termo de Acordo.

A solicitação de certificado para AC de nível imediatamente subseqüente ao da AC-SRF somente é possível após o deferimento do pedido de credenciamento e a respectiva autorização de funcionamento da AC em questão por parte do CG da ICP-Brasil.

Nesse caso, aquela AC deve encaminhar a solicitação de seu certificado à AC-SRF por meio de seus representantes legais, utilizando o padrão de solicitação de certificado PKCS#10 (Public Key Cryptographic Standards).

4.2 EMISSÃO DE CERTIFICADO

Somente após a validação conclusiva dos dados fornecidos pelo solicitante no formulário de solicitação de Certificado Digital para Autoridade Certificadora subordinada, a AC-SRF procederá à emissão e assinatura do certificado.

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

O processo de emissão é inicializado com a verificação da CSR (Certificate Signing Request) e submissão da requisição no padrão PKCS # 10 ao software da AC-SRF.

Em seguida o certificado emitido é inserido na relação de certificados emitidos pela AC-SRF.

A notificação de emissão é feita através da entrega do certificado emitido, em uma mídia magnética, ao responsável legal da AC titular do certificado.

4.3 ACEITAÇÃO DE CERTIFICADO

A AC de nível imediatamente subseqüente irá declarar, mediante assinatura do "Termo de Acordo", que aceita o certificado emitido.

4.4 SUSPENSÃO E REVOGAÇÃO DE CERTIFICADO

4.4.1 Circunstâncias para revogação

Um certificado é obrigatoriamente revogado nas seguintes circunstâncias:

1) quando constatada emissão imprópria ou defeituosa do mesmo.

2) quando for necessária a alteração de qualquer informação constante no mesmo.

3) no caso de dissolução da AC titular do certificado.

4) no caso de perda, roubo, modificação, acesso indevido, comprometimento ou suspeita de comprometimento da chave privada correspondente ou da sua mídia armazenadora.

A AC-SRF pode a seu critério revogar, conforme prazo definido no item 4.4.3, o certificado da entidade que deixar de cumprir as políticas, normas e regras estabelecidas para a ICP-Brasil e pela AC-SRF.

O CG da ICP-Brasil pode, a seu critério, determinar a revogação do certificado da AC que deixar de cumprir a legislação vigente ou as políticas, normas, práticas e regras estabelecidas para a ICP-Brasil.

4.4.2 Quem pode solicitar revogação

A revogação de um certificado somente pode ser solicitada:

1) pelo titular do certificado.

2) pelo responsável pela utilização do certificado.

3) pela AC-SRF.

4) pela AR-SRF.

5) por determinação do CG da ICP-Brasil ou da AC Raiz.

4.4.3 Procedimento para solicitação de revogação

A solicitação de revogação de certificado será feita através de formulário específico, permitindo a identificação inequívoca do solicitante. Os procedimentos detalhados de solicitação de revogação e da revogação estão descritos na página (http://www.receita.fazenda.gov.br/acsrf).

Como diretrizes gerais:

1) o solicitante da revogação de um certificado é identificado.

2) as solicitações de revogação, bem como as ações delas decorrentes são registradas e armazenadas.

3) as justificativas para a revogação de um certificado são documentadas.

4) o processo de revogação de um certificado termina com a geração e a publicação de uma LCR que contenha o certificado revogado.

O prazo máximo admitido para a conclusão do processo de revogação de certificado após o recebimento da respectiva solicitação é de 24 horas.

A revogação será solicitada mediante o preenchimento de formulário específico, identificando o certificado cuja revogação é solicitada, a entidade titular e a pessoa do solicitante. O formulário será assinado pelo Responsável Legal da AC solicitante e encaminhado à AC-SRF, que confirma as informações e procede a revogação.

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

4.4.4 Prazo para solicitação de revogação

A solicitação de revogação será imediata quando configuradas as circunstâncias definidas no seu item 4.4.1.

A AC titular do certificado pode solicitar a sua revogação no prazo de (5) cinco dias úteis, após o recebimento do mesmo, sem quaisquer ônus.

4.4.5 Circunstâncias para suspensão

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

4.4.6 Quem pode solicitar suspensão

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

4.4.7 Procedimento para solicitação de suspensão

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

4.4.8 Limites no período de suspensão

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

4.4.9 Freqüência de emissão de LCR

A Lista de Certificados Revogados (LCR) da AC-SRF é atualizada a cada 14 dias. São emitidas LCR na freqüência determinada nesta PC-SRF, mesmo quando não houver nenhuma mudança ou atualização, para assegurar a periodicidade da informação.

Na revogação de certificado de AC de nível imediatamente subseqüente ao seu, a AC-SRF deverá emitir nova LCR no prazo máximo de 24 (vinte e quatro) horas e notificar todas as AC de nível imediatamente subseqüente ao seu.

4.4.10 Requisitos para verificação de LCR

Todo certificado terá a sua validade verificada, na respectiva LCR, antes de ser utilizado.

A autenticidade da LCR também será confirmada, por meio das verificações da assinatura da AC-SRF e do período de validade da LCR.

4.4.11 Disponibilidade para revogação/verificação de status on-line

Não se aplica.

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

Caso ocorra perda, roubo, modificação, acesso indevido, comprometimento ou suspeita de comprometimento da chave privada correspondente ou da sua mídia

armazenadora, o titular notificará imediatamente a AC-SRF, solicitando a revogação de seu certificado, através do formulário específico para tal fim.

4.5 PROCEDIMENTOS DE AUDITORIA DE SEGURANÇA

Os itens a seguir estão definidos na DPC da AC-SRF sob a mesma numeração. O leitor obterá a cópia atualizada da DPC e referir-se ao item de mesmo número para informações sobre o processo de recuperação de desastre da AC-SRF.

4.5.1 Tipos de evento registrados

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

A AC-SRF registra em arquivos para fins de auditoria todos os eventos relacionados à segurança do seu sistema de certificação, quais sejam:

1) Iniciação e desligamento do sistema de certificação.

2) Tentativas de criar, remover, definir senhas ou mudar privilégios de sistema dos operadores da AC-SRF.

3) Mudanças na configuração da AC-SRF ou nas suas chaves.

4) Mudanças nas políticas de criação de certificados.

5) Tentativas de acesso (*login*) e de saída do sistema (*logoff*).

6) Tentativas não autorizadas de acesso aos arquivos de sistema.

7) Geração de chaves próprias da AC-SRF ou de chaves de Titulares de Certificados.

8) Emissão e revogação de certificados.

9) Geração de LCR.

10) Tentativas de iniciar, remover, habilitar e desabilitar usuários de sistemas, e de atualizar e recuperar suas chaves.

11) Operações falhas de escrita ou leitura no repositório de certificados e da LCR, quando aplicável.

12) Operações de escrita nesse repositório, quando aplicável.

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

1) Registros de acessos físicos.

2) Manutenção e mudanças na configuração de seus sistemas.

3) Mudanças de pessoal e de perfis qualificados.

4) Relatórios de discrepância e comprometimento.

5) Registros de destruição de meios de armazenamento contendo chaves criptográficas, dados de ativação de certificados ou informação pessoal de usuários.

Os registros de auditoria mínimos a serem mantidos pela AC-SRF incluem além dos acima:

1) Registros de solicitação, inclusive registros relativos a solicitações rejeitadas.

2) Pedidos de geração de certificado, mesmo que a geração não tenha êxito.

3) Registros de solicitação de emissão de LCR.

Todos os registros de auditoria, eletrônico ou manual, contém a data e a hora do evento registrado e a identidade do agente que o causou.

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

4.5.2 Freqüência de auditoria de registros (logs)

Para o certificado emitido em 14/10/2002 a periodicidade de auditoria de registros não será superior a uma semana, ou sempre que houver utilização do seu sistema de certificação.

Para o certificado emitido a partir de 22/11/2004 a auditoria de registro será realizada sempre que houver utilização do sistema de certificação.

Os registros de auditoria são analisados pelo pessoal operacional da AC-SRF. Todos os eventos significativos são explicados em relatório de auditoria de registros. Tal análise envolve uma inspeção breve de todos os registros verificando-se que não foram alterados, em seguida procede-se a uma investigação mais detalhada de quaisquer alertas ou irregularidades nesses registros. Todas as ações tomadas em decorrência dessa análise são documentadas.

4.5.3 Período de retenção para registros (logs) de auditoria

A AC-SRF mantém localmente, nas instalações do Centro de Certificação Digital do SERPRO/RJ (CCD) os seus registros de auditoria por pelo menos 2 (dois) meses e, subseqüentemente, faz o armazenamento da maneira descrita no item 4.6.

4.5.4 Proteção de registro (log) de auditoria

Os equipamentos da AC-SRF, onde são gerados os diversos registros de sistemas pelo sistema operacional, banco de dados e do aplicativo de AC, encontram-se fisicamente em um ambiente classificado como nível 4 de segurança.

A inspeção contínua dos diversos registros dos sistemas é feita por meio das ferramentas nativas do sistema operacional, banco de dados e do aplicativo de AC, e estão disponíveis somente para leitura. Pode ser feita também por relatórios emitidos a partir destas ferramentas. Estes dados de auditoria são coletados e armazenados periodicamente em uma sala de arquivos, de nível de segurança 3.

Os registros de auditoria gerados eletrônica ou manualmente são obrigatoriamente protegidos contra leitura não autorizada, modificação e remoção. Estes registros são classificados e mantidos conforme sua classificação, segundo os requisitos da Política de Segurança da ICP-Brasil.

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

Para o certificado emitido em 14/10/2002 a AC-SRF executa procedimentos de *backup* de todo o sistema de certificação (SISTEMA OPERACIONAL + APLICAÇÃO DE AC + BANCO DE DADOS) de duas formas:

- ✓ Semanalmente: cópia de segurança; e
- ✓ Sempre que houver utilização do sistema de certificação da AC-SRF: cópia armazenada para processos de auditoria.

Para o certificado emitido a partir de 22/11/2004 a AC-SRF executa procedimentos de backup de todo o sistema de certificação, sempre que houver utilização do mesmo.

4.5.6 Sistema de coleta de dados de auditoria

O sistema de coleta de dados de auditoria da AC-SRF é uma combinação de processos automatizados e manuais executados pelo sistema operacional, pelos sistemas de certificação de AC-SRF, pelo sistema de controle de acesso e pelo pessoal operacional.

Tipo de evento	Sistema de coleção	Registrado por
Sucesso e Fracasso de tentativas a mudanças sistema operacional segurança parâmetros.	Automático	Sistema operacional
Inicio e Parada de aplicação.	Automático	Sistema operacional
Sucesso e Fracasso de tentativas de *log-in* e *log-out*.	Automático	Sistema operacional

Sucesso e Fracasso de tentativas para criar, modificar, ou apagar contas de sistema.	Automático	Sistema operacional
Sucesso e Fracasso de tentativas para criar, modificar ou apagar usuários de sistemas autorizados.	Automático	Sistema operacional
Sucesso e Fracasso de tentativas para pedir, gerar, assinar, emitir ou revogar chaves e certificados.	Automático	AC ou Software de AR
Sucesso e Fracasso de tentativas para criar, modificar ou apagar informação de Titular de Certificado.	Automático	Software de AR
Logs de *Backup* e restauração.	Automático e manual	Sistema operacional e pessoal de operações
Mudanças de configuração de sistema.	Manual	Pessoal de operações
Atualizações de *software* e *hardware*.	Manual	Pessoal de operações
Manutenção de sistema.	Manual	Pessoal de operações
Mudanças de pessoal	Manual	Pessoal de operações
Registros de acessos físicos	Automático e manual	*Software* de controle de acesso e Pessoal de operações

4.5.7 Notificação de agentes causadores de eventos

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

4.5.8 Avaliações de vulnerabilidade

Uma Avaliação de Riscos de Segurança foi realizada para a AC-SRF. Esta avaliação cobre a incidência de riscos e ameaças que podem impactar na operação dos serviços de certificação.

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

4.6 ARQUIVAMENTO DE REGISTROS

Os itens a seguir estão definidos na DPC da AC-SRF sob a mesma numeração. O leitor obterá a cópia atualizada da DPC e referir-se ao item de mesmo número para informações sobre o processo de recuperação de desastre da AC-SRF.

4.6.1 Tipos de eventos registrados

As seguintes informações são registradas e arquivadas pela AC-SRF:

1) solicitações de certificados.
2) solicitações de revogação de certificados.
3) notificações de comprometimento de chaves privadas.
4) emissões e revogações de certificados.
5) emissões de LCR.
6) trocas de chaves criptográficas da AC-SRF.
7) informações de auditoria previstas no item 4.5.1.
8) correspondências formais.
9) Processos de credenciamento de AC de nível imediatamente subseqüente ao da AC-SRF.

4.6.2 Período de retenção para arquivo

Os períodos de retenção para cada registro arquivado são os seguintes:

1) as LCR referentes a certificados de assinatura digital são retidas por, no mínimo, período igual ao do arquivamento dos respectivos certificados.
2) as demais informações são retidas por, no mínimo, 6 (seis) anos.

4.6.3 Proteção de arquivo

Mídias de arquivos são guardadas em local seguro, sendo que a proteção criptográfica das mídias, é adotada quando a classificação assim o exigir. Também são protegidas de fatores ambientais como temperatura, umidade, e magnetismo.

Todos os registros arquivados são classificados e armazenados com requisitos de segurança compatíveis com sua classificação, conforme a Política de Segurança da ICP-Brasil.

4.6.4 Procedimentos para cópia de segurança (backup) de arquivo

Uma segunda cópia de todo o material arquivado é armazenada em ambiente externo ao sistema de certificação da AC-SRF, protegido com nível 3 de segurança.

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

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

4.6.5 Requisitos para datação (time-stamping) de registros

Os servidores da AC-SRF estão sincronizados com a hora GMT fornecida pelo Observatório Nacional. Todas as informações geradas que possuam alguma identificação de horário recebem o horário em GMT, inclusive os certificados emitidos por esses equipamentos.

No caso dos registros feitos manualmente, estes contêm a Hora Oficial do Brasil.

4.6.6 Sistema de coleta de dados de arquivo

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

Tipo de evento	Sistema de coleção	Registrado por
Solicitações de certificados	Automático e manual	*Software* de AC/AR e pessoal de operações
Solicitações de revogação de certificados	Automático e manual	*Software* de AC/AR e pessoal de operações
Notificações de comprometimento de chaves privadas	Manual	Pessoal de operações
Emissões e revogações de certificados;	Automático	*Software* de AC/AR
Emissões de LCR	Automático	*Software* de AC/AR
Correspondências formais	Manual	Pessoal de operações

4.6.7 Procedimentos para obter e verificar informação de arquivo

A integridade dos arquivos da AC-SRF e da AR-SRF é verificada:

1) Na ocasião em que o arquivo é preparado.

2) Semestralmente no momento de uma auditoria de segurança programada.

3) Em qualquer outro momento quando uma auditoria de segurança completa é requerida.

Somente podem ter acesso às informações de arquivo da AR-SRF:

1) Pessoas devidamente autorizadas por meio de instrumento devidamente constituído e corretamente identificadas, conforme definido no item 2.8.5.

2) Titulares de Certificados, ou seus representantes legais, mediante solicitação formal, conforme definido no item 2.8.6.

4.7 TROCA DE CHAVE

A AC-SRF comunica através de oficio, com 90 dias de antecedência, à AC subseqüente o vencimento do seu certificado, junto com as informações necessárias para a solicitação de uma nova chave.

4.8 COMPROMETIMENTO E RECUPERAÇÃO DE DESASTRE

A AC-SRF possui um Plano de Continuidade do Negócio, testado pelo menos uma vez por ano, para garantir a continuidade dos seus serviços críticos.

4.8.1 Recursos computacionais, software, e dados corrompidos

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

1) É feita a identificação de todos os elementos corrompidos.

2) O instante do comprometimento é determinado e é crítico para invalidar as transações executadas após aquele instante.

3) É feita uma análise do nível do comprometimento para a determinação das ações a serem executadas, que podem variar de uma simples restauração de um *backup* de segurança até a revogação do certificado da AC-SRF.

4.8.2 Certificado de entidade é revogado

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

- Em caso de revogação do certificado da AC-SRF, após a identificação do incidente, são notificados os gestores do processo de certificação digital, que acionam as equipes envolvidas, de forma a indisponibilizar temporariamente os serviços de autoridade certificadora. Na confirmação do incidente, são revogados os certificados das AC de nível imediatamente subseqüente, é gerado o novo par de chaves da AC-SRF, sendo emitido, pela AC Raiz, certificado associado ao novo par de chaves gerado e emitidos, pela AC-SRF, novos certificados digitais para as AC de nível imediatamente subseqüente.

4.8.3 Chave de entidade é comprometida

A AC-SRF possui um Plano de Continuidade de Negócio que especifica as ações a serem tomadas no caso em que a chave privada de uma entidade é comprometida, e que podem ser resumidas nas ações listadas a seguir.

- Em caso de comprometimento da chave da AC-SRF, após a identificação da crise, são notificados os gestores do processo de certificação digital, que acionam as equipes envolvidas, de forma a indisponibilizar temporariamente os serviços de autoridade certificadora. Na confirmação do incidente, são revogados os certificados da AC-SRF e das AC de nível imediatamente subseqüente. É gerado, então, um novo par de chaves e emitido, pela AC Raiz, certificado associado ao novo par de chaves gerado e emitidos, pela AC-SRF, novos certificados digitais para as AC de nível imediatamente subseqüente.

4.8.4 Segurança dos recursos após desastre natural ou de outra natureza

A AC-SRF possui um Plano de Continuidade de Negócio que especifica as ações a serem tomadas no caso desastre natural ou de outra natureza. O propósito deste plano é restabelecer as principais operações da AC-SRF quando a operação de sistemas é significativamente e adversamente abalada por fogo, greves, etc.

O plano garante que qualquer impacto em operações de sistema não causará um impacto operacional direto e imediato dentro da ICP-Brasil da qual a AC-SRF faz parte. Isto significa que o plano deve ter como meta primária, restabelecer a AC-SRF para tornar acessível os registros lógicos mantidos dentro do *software*. Serão tomadas as ações de recuperação aprovadas dentro do plano segundo uma ordem de prioridade.

4.9 EXTINÇÃO DA AC-SRF OU AR-SRF

Quando for necessário encerrar as atividades da AC-SRF ou da AR-SRF, o impacto deste término deve ser minimizado da melhor forma possível tendo em vista as circunstâncias prevalecentes. Isto inclui:

1) Prover com maior antecedência possível notificação para:
   - a AC Raiz da ICP-Brasil;
   - todas as entidades subordinadas.
2) A transferência progressiva do serviço e dos registros operacionais, para um sucessor, que deverá observar os mesmos requisitos de segurança exigidos para a AC-SRF ou para a AR-SRF extinta.
3) Preservar qualquer registro não transferido a um sucessor.

As chaves públicas dos certificados emitidos pela AC-SRF, dissolvida, serão armazenadas por outra AC, após aprovação da AC Raiz.

Quando houver mais de uma AC interessada, assumirá a responsabilidade do armazenamento das chaves públicas, aquela indicada pela AC-SRF.

A AC-SRF, ao encerrar as suas atividades transferirá, se for o caso, a documentação dos certificados digitais emitidos à AC que tenha assumido a guarda das respectivas chaves públicas.

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

4. 5. CONTROLES DE SEGURANÇA FÍSICA, PROCEDIMENTAL E DE PESSOAL

Os itens a seguir estão definidos na DPC da AC-SRF sob a mesma numeração. O leitor obterá a cópia atualizada da DPC e referir-se ao item de mesmo número para informações sobre o processo de recuperação de desastre da AC-SRF.

5.1 CONTROLES FÍSICOS

5.1.1 Construção e localização das instalações

A operação da AC-SRF é executada dentro de um ambiente físico seguro em área de instalação altamente protegida.

Os componentes do sistema de certificação utilizados para a operação da AC-SRF estão situados nas instalações do Centro de Certificação Digital do SERPRO no Rio de Janeiro, Horto.

A localização e o sistema de certificação utilizado para a operação da AC-SRF não são publicamente identificados. Internamente, não são admitidos ambientes

compartilhados que permitam visibilidade nas operações de emissão e revogação de certificados. Essas operações são segregadas em compartimentos fechados e fisicamente protegidos. Nenhuma das linhas telefônicas dentro do CCD oferece suporte a modems.

Alguns aspectos de construção das instalações da AC-SRF relevantes para os controles de segurança física são descritos abaixo. Outros detalhes estão descritos no restante do item 5.1.

- Todas as instalações de equipamentos de apoio, tais como: máquinas de ar condicionado, grupos geradores, *no-breaks*, baterias, quadros de distribuição de energia e de telefonia, instalações para sistemas de telecomunicações e sistema de aterramento e de proteção contra descargas atmosféricas, foram executadas por técnicos especializados para garantir a proteção física da AC-SRF.

5.1.2 Acesso físico

O acesso físico às dependências da AC-SRF é gerenciado e controlado internamente conforme o previsto na Política de Segurança da AC-SRF. Chaves, senhas, cartões, identificações biométricas ou outros dispositivos são utilizados para controle de acesso.

O acesso físico é monitorado e o seu controle assegura que apenas pessoas autorizadas participem das atividades pertinentes.

O sistema de certificação da AC-SRF está situado em uma sala-cofre. Segurança patrimonial e controles de segurança biométricos restringem o acesso aos equipamentos da sala-cofre.

5.1.2.1 Níveis de Acesso

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

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

Excetuados os casos previstos em lei, o porte de armas não é admitido nas instalações do ambiente onde estão instalados os equipamentos utilizados na operação da AC-SRF, esse procedimento ocorre a partir do nível 1. A partir desse nível, equipamentos de gravação, fotografia, telefones celulares, *pagers*, vídeo, som ou similares, bem como computadores portáteis, tem sua entrada controlada e somente podem ser utilizados mediante autorização formal e supervisão.

O segundo nível – ou nível 2 – o acesso é interno ao primeiro nível. A passagem do primeiro para o segundo nível exige identificação das pessoas autorizadas por meio eletrônico, e o uso de crachá. Esse é o nível mínimo de segurança requerido para a execução de qualquer processo operacional ou administrativo da AC-SRF.

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

No terceiro nível são controladas tanto as entradas quanto as saídas de cada pessoa autorizada. Dois tipos de mecanismos de controle são requeridos para a entrada nesse nível: a identificação individual, como cartão eletrônico, e a identificação biométrica.

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

O quarto nível - ou nível 4 – o acesso é interno ao terceiro nível, é onde ocorrem atividades especialmente sensíveis de operação da AC-SRF, tais como: emissão e revogação de certificados e emissão de LCR. Todos os sistemas e equipamentos necessários a estas atividades estão localizados a partir desse nível. O nível 4 possui os mesmos controles de acesso do nível 3 e, adicionalmente, exige em cada acesso ao seu ambiente, a identificação de, no mínimo, 2 (duas) pessoas autorizadas. Nesse nível, a permanência dessas pessoas é exigida enquanto o ambiente estiver ocupado.

No quarto nível, todas as paredes, piso e teto são revestidos de aço e concreto. As paredes, piso e o teto são inteiriços, constituindo uma célula estanque contra ameaças de acesso indevido, água, vapor, gases e fogo. Os dutos de refrigeração e de energia, bem como os dutos de comunicação, não permitem a invasão física das áreas de quarto nível. Adicionalmente, esses ambientes de nível 4 – que constituem a chamada sala cofre - possuem proteção contra interferência eletromagnética externa.

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

São dois os ambientes de quarto nível abrigados pela sala cofre:

1) Sala de equipamentos da AC-SRF de produção *on-line* e cofre de armazenamento.

2) Sala de equipamentos de rede e infra-estrutura (*firewall*, roteadores, *switches* e servidores).

No quarto nível são controladas tanto as entradas quanto as saídas de cada pessoa autorizada. Dois tipos de mecanismos de controle são requeridos para a entrada nesse nível: algum tipo de identificação individual, como cartão eletrônico, e identificação biométrica.

O quinto nível – ou nível 5 – é interno aos ambientes de nível 4, e compreende cofres e gabinetes trancados. Materiais criptográficos tais como chaves, dados de ativação, suas cópias e equipamentos criptográficos são armazenados em nível 5 ou superior.

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

1) Ser feito em aço ou material de resistência equivalente.

2) Possuir tranca com chave.

O sexto nível – ou nível 6 - consiste de pequenos depósitos localizados no interior do cofre ou gabinete de quinto nível, ou hardware criptográfico. Cada um desses depósitos dispõe de fechadura individual. A chave privada da AC-SRF esta armazenada em um desses depósitos quando não estiver em operação. Quando em operação, a chave privada da AC-SRF é armazenada em cartões criptográfico, em gabinete de nível 5.

5.2.2.2 Sistema físico de detecção

Todas as passagens entre os níveis de acesso, bem como as salas de operação de nível 4, são monitoradas por câmaras de vídeo ligadas a um sistema de gravação 24x7. O posicionamento e a capacidade dessas câmaras não permitem a recuperação de senhas digitadas nos controles de acesso.

As fitas de vídeo resultantes da gravação 24x7 são armazenadas por, no mínimo, um ano. Elas são testadas (verificação de trechos aleatórios no início, meio e final da fita) pelo menos a cada 3 (três) meses, com a escolha de, no mínimo, uma fita referente a cada semana. Essas fitas são armazenadas em ambiente de terceiro nível.

Todas as portas de passagem entre os níveis de acesso 3 e 4 do ambiente são monitoradas por sistema de notificação de alarmes. O sistema de notificação de alarmes utiliza 2 (dois) meios de notificação: sonoro e visual.

Em todos os ambientes de quarto nível, um alarme de detecção de movimentos permanece ativo enquanto não for satisfeito o critério de acesso ao ambiente. Assim que, devido à saída de um ou mais funcionários de confiança, o critério mínimo de ocupação deixar de ser satisfeito, ocorre a reativação automática dos sensores de presença.

O sistema de notificação de alarmes utiliza 2 (dois) meios de notificação: sonoro e visual.

O sistema de monitoramento das câmaras de vídeo, bem como o sistema de notificação de alarmes, são permanentemente monitorados por guarda armado e estão localizados em ambiente de nível 3. As instalações do sistema de monitoramento, por sua vez, são monitoradas por câmaras de vídeo cujo posicionamento permite o acompanhamento das ações do guarda.

5.1.2.3 Sistema de Controle de Acesso

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

5.1.2.4 Mecanismos de emergência

Mecanismos específicos foram implantados para garantir a segurança do pessoal e dos equipamentos da AC-SRF em situações de emergência. Esses mecanismos permitem o destravamento de portas por meio de acionamento mecânico, para a saída de emergência de todos os ambientes com controle de acesso. A saída efetuada por meio desses mecanismos aciona imediatamente os alarmes de abertura de portas.

Todos os procedimentos referentes aos mecanismos de emergência estão documentados. Os mecanismos e procedimentos de emergência são verificados semestralmente, por meio de simulação de situações de emergência.

5.1.3 Energia e ar condicionado

A AC-SRF possui sistema de fornecimento de energia sobressalente. Em caso de falta de energia, a AC-SRF funciona temporariamente utilizando no-breaks com autonomia suficiente para casos onde é necessário o acionamento do gerador de apoio, que funciona durante o tempo da falta de energia.

A área de operações segura da AC-SRF é conectada a uma fonte de energia padrão. Todos os componentes críticos são conectados a provisão de energia ininterrupta (UPS), prevenindo paradas anormais no caso de uma deficiência de força, de forma a atender os requisitos de disponibilidade dos sistemas da AC-SRF e seus respectivos serviços. Um sistema de aterramento está implantado.

A área tem um sistema de ar condicionado para controlar o calor e umidade que é independente do sistema de ar condicionado de edifício.

Todos os cabos elétricos são protegidos por tubulações ou dutos apropriados. São utilizadas tubulações, dutos, calhas, quadros e caixas de passagem, de distribuição e de terminação, projetados e construídos de forma a facilitar vistorias e a detecção de tentativas de violação. São utilizados dutos separados para os cabos de energia, de telefonia e de dados.

Todos os cabos são catalogados, identificados e periodicamente vistoriados, no mínimo a cada 6 meses, na busca de evidências de violação ou de outras anormalidades.

São mantidos atualizados os registros sobre a topologia da rede de cabos, observados os requisitos de sigilo estabelecidos pela Política de Segurança da ICP-Brasil. Qualquer modificação nessa rede é previamente documentada.

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

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

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

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

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

1) Geradores de porte compatíve.
2) Geradores de reserva.
3) Sistemas de *no-breaks* redundantes.
4) Sistemas redundantes de ar condicionado.

5.1.4 Exposição à água

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

5.1.5 Prevenção e proteção contra incêndio

Todas as instalações da AC-SRF possuem sistemas de prevenção contra incêndio.

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

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

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

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

5.1.6 Armazenamento de mídia

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

5.1.7 Destruição de lixo

Documentos em papel e em mídia magnética que contêm elementos confidenciais da AC-SRF, informações comercialmente sensíveis ou confidenciais são eliminadas seguramente:

1) No caso de mídias magnéticas:
   - dano físico, ou destruição completa do recurso;
   - uso de uma utilidade aprovada para esfregar ou sobrescrever mídias magnéticas.
2) No caso de material impresso, rasgando, ou destruindo através de meios aprovados.
3) No caso de documentos em papel que contenham informações classificadas como sensíveis serão trituradas antes de ir para o lixo.

5.1.8. Instalações de segurança (backup) externas (off-site)

A AC-SRF mantém instalações de contingência que atendem os requisitos mínimos estabelecidos pelo CG da ICP-Brasil. Em caso de sinistro que torne inoperantes as instalações principal, as instalações de contingência não serão atingidas e tornar-se-ão totalmente operacionais em, no máximo, 48 (quarenta e oito) horas depois de decretado o estado de contingência.

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. Um exemplo desta prática é que as pessoas que executam atividades de examinar registros de sistema, ou examinar *logs* de auditoria não são as mesmas pessoas envolvidas na atividade que gerou estes registros e *logs*, assegurando que as pessoas que executam estão agindo dentro das responsabilidades e dentro da política de segurança declarada.

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-SRF:

1) Gerente do CCD.
2) Administrador de Segurança.
3) Administrador de Banco de Dados.
4) Administrador do Sistema de Gerenciamento de Certificados.
5) Administrador do Servidor WEB.
6) Administrador do Sistema Unix.
7) Administrador do Security Server.
8) Administrador de AC.
9) Operador.
10) Segurança patrimonial.
11) Apoio administrativo.

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.

Quando um empregado se desliga da AC-SRF, suas permissões de acesso são revogadas imediatamente. Quando há mudança na posição ou função que o empregado ocupa com relação à AC-SRF, são revistas suas permissões de acesso. Os termos de responsabilidade assinados pelo funcionário contém a descrição de todos os recursos, antes disponibilizados, que o empregado deverá devolver à AC-SRF no ato de seu desligamento.

5.2.2. Número de pessoas necessário por tarefa

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

Todas as tarefas executadas no ambiente onde está localizado o equipamento de certificação da AC-SRF necessitam da presença de no mínimo 2 (dois) empregados da AC-SRF. As demais tarefas da AC-SRF podem ser executadas por um único empregado.

5.2.3. Identificação e autenticação para cada perfil

Pessoas que ocupam os perfis designados pela AC-SRF passam por um processo rigoroso de seleção.

Todo funcionário da AC-SRF tem sua identidade e perfil verificados antes de:

1) Ser incluído em uma lista de acesso às instalações da AC-SRF.

2) Ser incluído em uma lista para acesso físico ao sistema de certificação da AC-SRF.

3) Receber um certificado para executar suas atividades operacionais na AC-SRF.

4) Receber uma conta no sistema de certificação da AC-SRF.

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

1) São diretamente atribuídos a um único empregado.

2) Não são compartilhados.

3) São restritos às ações associadas ao perfil para o qual foram criados.

A AC-SRF implementa um padrão de utilização de "senhas fortes", definido em seu Manual de Segurança e em conformidade com a Política de Segurança da ICP-Brasil, juntamente com procedimentos de validação dessas senhas.

5.3 CONTROLES DE PESSOAL

Todos os funcionários da AC-SRF e da AR-SRF, encarregados de tarefas operacionais, tem registrado em contrato ou termo de responsabilidade:

1) Os termos e as condições do perfil que ocupam.

2) O compromisso de observar as normas, políticas e regras aplicáveis da AC-SRF.

3) O compromisso de observar as normas, políticas e regras aplicáveis da ICP-Brasil.

4) O compromisso de não divulgar informações sigilosas a que tenham acesso.

5.3.1. Antecedentes, qualificação , experiência e requisitos de idoneidade

Todo o pessoal da AC-SRF envolvidos em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados é admitido conforme o estabelecido na Política de Segurança da AC-SRF e na Política de Segurança da ICP-Brasil.

5.3.2. Procedimentos de verificação de antecedentes

Com o propósito de resguardar a segurança e a credibilidade da AC-SRF, todo o pessoal envolvido em atividades diretamente relacionadas com os processos de

emissão, expedição, distribuição, revogação e gerenciamento de certificados, é submetido aos seguintes processos, antes do começo das atividades de:

1) Verificação de antecedentes criminais.

2) Verificação de situação de crédito.

3) Verificação de histórico de empregos anteriores.

4) Comprovação de escolaridade e de residência.

5.3.3. Requisitos de treinamento

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

1) Princípios e mecanismos de segurança da AC-SRF e das AR vinculadas.

2) Sistema de certificação em uso na AC-SRF.

3) Procedimentos de recuperação de desastres e de continuidade do negócio.

4) Outros assuntos relativos a atividades sob sua responsabilidade.

5.3.4. Freqüência e requisitos para reciclagem técnica

Todo o pessoal da AC-SRF envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados é mantido atualizado sobre eventuais mudanças tecnológicas no sistema de certificação da AC-SRF. Treinamentos de reciclagem são realizados pela AC-SRF sempre que necessário.

5.3.5. Freqüência e seqüência de rodízio de cargos

A AC-SRF não implementa rodízio de cargos.

5.3.6. Sanções para ações não autorizadas

Na eventualidade de uma ação não autorizada, real ou suspeita, realizada por pessoa responsável por processo de emissão, expedição, distribuição, revogação ou gerenciamento de certificados, a AC-SRF suspende o seu acesso ao sistema de certificação e toma as medidas administrativas e legais cabíveis.

5.3.7. Requisitos para contratação de pessoal

O pessoal da AC-SRF no exercício de atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de

certificados é contratado conforme o estabelecido na Política de Segurança da AC-SRF.

5.3.8. Documentação fornecida ao pessoal

A AC-SRF disponibiliza para todo o seu pessoal e o da AR-SRF:

1) Esta PC-SRF.

2) A DPC que implementa.

3) A Política de Segurança da ICP-Brasil.

4) A Política de Segurança da AC-SRF.

5) Documentação de hardware e software relativas à função desempenhada.

6) Documentação operacional relativa às suas atividades.

7) Contratos, normas e políticas relevantes para suas atividades.

Toda a documentação fornecida ao pessoal da AC-SRF e da AR-SRF é classificada segundo a política de classificação de informação definida e é mantida atualizada.

5. 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-SRF e das AC subordinadas são gerados pelas mesmas, após seu credenciamento pela ICP-Brasil. As AC subordinadas indicarão, por intermédio de seus representantes legais, a pessoa responsável pela geração dos pares de chaves criptográficas e pelo uso do certificado.

Ao ser gerada, a chave privada da entidade titular é gravada cifrada, por algoritmo simétrico como 3-DES, IDEA, SAFER+ ou outros aprovados pelo CG da ICP-Brasil, em hardware criptográfico aprovado pelo CG da ICP - Brasil.

A chave privada trafega cifrada, empregando os mesmos algoritmos citados no parágrafo anterior, entre o dispositivo gerador e a mídia utilizada para o seu armazenamento.

O meio de armazenamento da chave privada assegura, por meios técnicos e procedimentais adequados, no mínimo, que:

• a chave privada é única e seu sigilo é suficientemente assegurado;

• a chave privada não pode, com uma segurança razoável, ser deduzida;

• a chave privada está protegida contra falsificações realizadas através das tecnologias atualmente disponíveis;

• a chave privada pode ser eficazmente protegida pelo legítimo titular contra a utilização por terceiros.

Esse meio de armazenamento não modifica os dados a serem assinados, nem impede que esses dados sejam apresentados ao signatário antes do processo de assinatura.

Os pares de chaves da AC-SRF e das AC subordinadas são gerados em módulo criptográfico de hardware com no mínimo padrão de segurança FIPS 140-1 nível 2, utilizando algoritmo RSA para geração do par de chaves.

Os pares de chaves da AC-SRF e das AC subordinadas são gerados somente pelo Titular do Certificado correspondente.

6.1.2. Entrega da chave privada à entidade titular

A geração e a guarda de uma chave privada é de responsabilidade exclusiva do titular do certificado correspondente.

6.1.3. Entrega da chave pública para emissor de certificado

Para a entrega de sua chave pública à AC-SRF, encarregada da emissão de seu certificado, a AC solicitante faz uso do padrão PKCS#10. Essa entrega é feita por representante legalmente constituído da AC subordinada, em data e hora previamente estabelecida pela AC-SRF.

6.1.4. Disponibilização de chave pública da AC-SRF para usuários

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

• formato PKCS#7 (RFC 2315), que inclui toda a cadeia de certificação, no momento da disponibilização de um certificado para seu titular;

• diretório;

• página Web da AC-SRF (http://www.receita.fazenda.gov.br/acsrf);

• outros meios seguros aprovados pelo CG da ICP-Brasil.

6.1.5. Tamanhos de chave

O tamanho admitido para chaves criptográficas é de 2048 bits.

6.1.6. Geração de parâmetros de chaves assimétricas

As entidades titulares de certificados adotarão, no mínimo o padrão FIPS (Federal Information Processing Standards) 140-1 nível 2, para a geração de chaves assimétricas de sua propriedade.

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

A geração de chaves criptográficas dos certificados das AC Subordinadas à AC-SRF se dará por hardware criptográfico, aprovado pela ICP-Brasil. O componente seguro de hardware utiliza um mecanismo de detecção de violação.

6.1.9. Propósitos de uso de chave (conforme o campo "key usage" na X.509 v3)

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

As chaves privadas dos titulares de certificados emitidos pela AC-SRF são utilizadas apenas para a assinatura dos certificados por ela emitidos e de suas LCR.

6.2. PROTEÇÃO DA CHAVE PRIVADA

6.2.1. Padrões para módulo criptográfico

A chave privada das AC subordinadas à AC-SRF são geradas, armazenadas e utilizadas apenas em hardware criptográfico especifico, classificado como FIPS 140-1 nível 3, não havendo portanto tráfego da chave privada fora do mesmo em nenhum momento.

6.2.2. Controle "n de m" para chave privada

A chave de ativação do componente seguro de hardware que armazena e utilizada apenas em hardware criptográfico especifico, classificado como FIPS 140-1 nível 3, não havendo portanto tráfego fora do mesmo em nenhum momento.

6.2.3. Recuperação (escrow) de chave privada

Não é permitida, no âmbito da ICP-Brasil, a recuperação (escrow) de chaves privadas, isto é, não se permite que terceiros possam legalmente obter uma chave privada sem o consentimento de seu titular.

6.2.4. Cópia de segurança (backup) de chave privada

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

A AC-SRF não mantém cópia de segurança das chaves privadas das AC de nível imediatamente subseqüentes ao seu.

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

A cópia de segurança deve ser armazenada, cifrada, por algoritmo simétrico com 3-DES, IDEA, SAFER+, ou outros aprovados pelo CG da ICP-Brasil, e protegida com um nível de segurança não inferior àquele definido para a chave original.

6.2.5. Arquivamento de chave privada

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

Define-se arquivamento como o armazenamento da chave privada para seu uso futuro, após o período de validade do certificado correspondente.

6.2.6. Inserção de chave privada em módulo criptográfico

Item não se aplica.

6.2.7. Método de ativação de chave privada

Para o certificado emitido em 14/10/2002 a chave privada da AC-SRF é ativada mediante a aplicação de uma senha exigida pelo *software* de certificação, pelos Administradores do Sistema de Certificação da AC-SRF. Esta senha obedece à política de senhas estabelecida pela AC-SRF.

A ativação da chave privada é feita por três pessoas, devidamente autorizadas, e a confirmação da identidade desses agentes é feita através de senhas, só lhes sendo permitido o acesso ao ambiente em duplas devidamente autorizadas.

Para o certificado emitido a partir de 22/11/2004 a chave privada da AC-SRF é implementada por meio de cartões criptográficos, após a identificação dos operadores com senha.

A Ativação da chave privada das AC subordinadas à AC-SRF implementa por meio de cartões criptográficos, protegidos com senha, após a identificação dos custodiantes da chave de ativação da chave criptográfica.

6.2.8. Método de desativação de chave privada

As chave privada das AC-SRF e das AC Subordinadas, armazenadas em módulos criptográficos são desativadas quando não mais necessárias, através de mecanismos disponibilizado pelo software de certificação que permite o apagamento de todas as informações contidas no módulo criptográfico. Este procedimento é implementado por meio de cartões criptográficos, protegidos com senha, após a identificação dos custodiantes da chave de ativação da chave criptográfica.

6.2.9. Método de destruição de chave privada

Além do estabelecido no item 6.2.8 desta PC, todas as cópias de segurança da chave privada da AC –SRF e AC Subordinadas serão destruídas.

As mídias de armazenamento das chaves privadas serão reinicializadas de forma a não restarem nelas informações sensíveis.

6.3. OUTROS ASPECTOS DO GERENCIAMENTO DO PAR DE CHAVES

6.3.1. Arquivamento de chave pública

As chaves públicas, da AC-SRF e dos titulares de certificados de assinatura para Autoridade Certificadora subordinada por ela emitidos, permanecem armazenadas após a expiração dos certificados correspondentes, por no mínimo 30 (trinta) anos, na forma da legislação em vigor, para a 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-SRF e das AC Subordinadas são utilizadas apenas durante o período de validade do certificado correspondente. A chave pública da AC-SRF 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 de validade do certificado emitido em 14/10/2002 é de 5 anos e o certificado emitido a partir de 22/11/2004 é de 8 anos.

6.4. DADOS DE ATIVAÇÃO

6.4.1. Geração e instalação dos dados de ativação

Os dados de ativação da chave privada do titular do certificado, são únicos e aleatórios.

6.4.2. Proteção dos dados de ativação

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

6.4.3. Outros aspectos dos dados de ativação

Não aplicável.

6.5. CONTROLES DE SEGURANÇA COMPUTACIONAL

6.5.1. Requisitos técnicos específicos de segurança computacional

A geração do par de chaves das AC subordinadas é realizada off-line, para impedir o acesso remoto não autorizado.

Cada computador servidor das AC subordinadas relacionado diretamente com os processos de emissão, expedição, distribuição, revogação ou gerenciamento de certificados, implementa, entre outras, as seguintes características:

- controle de acesso aos serviços e perfis da AC;
- clara separação das tarefas e atribuições relacionadas a cada perfil das AC subordinadas;
- uso de criptografia para segurança de base de dados, quando exigido pela classificação de suas informações;
- geração e armazenamento de registros de auditoria das AC subordinadas;
- mecanismos internos de segurança para garantia da integridade de dados e processos críticos; e
- mecanismos para cópias de segurança (backup).

Essas características são implementadas pelo sistema operacional ou por meio da combinação deste com o sistema de certificação e com mecanismos de segurança física.

Qualquer equipamento, ou parte deste, ao ser enviado para manutenção, tem todas as informações sensíveis nele contidas apagadas e seu número de série e as datas de envio e de recebimento controlados. Ao retornar às instalações das AC subordinadas, o equipamento que passa por manutenção é inspecionado. Em todo equipamento que deixe de ser utilizado em caráter permanente, são destruídas de maneira definitiva todas as informações sensíveis armazenadas, relativas à atividade das AC subordinadas. Todos esses eventos são registrados para fins de auditoria.

Qualquer equipamento incorporado às AC subordinadas é preparado e configurado como previsto na Política de Segurança implementada, de forma a apresentar o nível de segurança necessário à sua finalidade.

6.5.2. Classificação da segurança computacional

Item não aplicável.

6.6. CONTROLES TÉCNICOS DO CICLO DE VIDA

6.6.1. Controles de desenvolvimento de sistema

Item não aplicável.

6.6.2. Controles de gerenciamento de segurança

A administração de segurança de sistema é controlada pelos privilégios nomeados a contas de sistema operacional, e pelos papéis confiados descritos no item 5.2.1.

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

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

6.6.3. Classificações de segurança de ciclo de vida

Não aplicável.

6.7. CONTROLES DE SEGURANÇA DE REDE

As redes de operação online usam sistemas com vários níveis de firewall e detecção de invasão. Apenas os serviços essenciais para a operação das Ac subordinadas estão disponíveis para o ambiente externo. Todos eles operam em nível 4 de segurança física.

6.8. CONTROLES DE ENGENHARIA DE MÓDULO CRIPTOGRÁFICO

O módulo criptográfico utilizado pela AC-SRF emitido em 14/10/2004 para o armazenamento de sua chave privada e certificado como FIPS (Federal Information Processing Standards) 140-1 level 2.

O módulo criptográfico utilizado pela AC-SRF emitido em 29/11/2004 para o armazenamento de sua chave privada e certificado como FIPS (Federal Information Processing Standards) 140-1 level 3.

O módulo criptográfico utilizado pelas AC Subordinadas à AC-SRF para o armazenamento de sua chave privada e certificado como FIPS (Federal Information Processing Standards) 140-1 level 3.

Ao ser gerada, a chave privada da entidade titular é gravada cifrada, por algoritmo simétrico como 3-DES, IDEA, SAFER+ ou outros aprovados pelo CG da ICP-Brasil, em hardware criptográfico aprovado pelo CG da ICP - Brasil.

O meio de armazenamento da chave privada assegura, por meios técnicos e procedimentais adequados, no mínimo, que:

• a chave privada utilizada na geração de uma assinatura é única e seu sigilo é suficientemente assegurado;

• a chave privada utilizada na geração de uma assinatura não pode, com uma segurança razoável, ser deduzida e que está protegida contra falsificações realizadas através das tecnologias atualmente disponíveis;

• a chave privada utilizada na geração de uma assinatura pode ser eficazmente protegida pelo legítimo titular contra a utilização por terceiros.

Esse meio de armazenamento não modifica os dados a serem assinados, nem impede que esses dados sejam apresentados ao signatário antes do processo de assinatura.

6. 7. PERFIS DE CERTIFICADO E LCR

7.1. PERFIL DO CERTIFICADO

Os certificados emitidos pela AC-SRF estão em conformidade com o formato definido pelo padrão ITU X.509.

7.1.1. Número de versão

Os certificados emitidos pela AC-SRF implementam a versão 3 do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 2459.

7.1.2. Extensões de certificado

Os certificados emitidos pela AC-SRF, sob esta PC AC-SRF, obedecem as resoluções da ICP-Brasil, que define como obrigatórias as seguintes extensões para certificados de AC:

1) "*Authority Key Identifier*", não crítica: o campo keyIdentifier contém o resumo SHA-1 da chave pública da AC-SRF.
2) "*Subject Key Identifier*", não crítica: contém o *hash* SHA-1 da chave pública da AC titular do certificado.
3) "*Key Usage*", crítica: somente os bits e keyCertSign e cRLSign são ativados.
4) "*Certificate Policies*", não crítica:
    - o campo policyIdentifier contém o OID das PC que a AC titular do certificado implementa;
    - o campo policyQualifiers contém o endereço *URL* da página *Web, http://www.receita.fazenda.gov.br/acsrf/dpcacsrf.pdf,* onde se obtém a DPC da AC-SRF.
5) O "Basic Constraints", crítica: contém o campo CA=TRUE;
6) "*CRL Distribution Points*", não crítica: contém o endereço *URL* da página *Web*:
    - Para certificados emitidos em 14/10/2002 (http://www.receita.fazenda.gov.br/acsrf/acsrf.crl),
    - Para certificados emitidos em 22/11/2004 (http://www.receita.fazenda.gov.br/acsrf/acsrfv1.crl).

7.1.3. Identificadores de algoritmo

Os certificados da AC-SRF e de titulares de certificado são assinados com o uso do algoritmo RSA com SHA-1 como função hash (OID= 1.2.840.113549.1.1.5), conforme o padrão PKCS#1 (RFC 2313).

7.1.4. Formatos de nome

Para os certificados emitidos sob esta PC AC-SRF, o nome da AC titular do certificado, constante do campo "*Subject*", adota o "*Distinguished Name*" (DN) do padrão ITU X.500/ISO 9594, da seguinte forma:

C= BR;

O= ICP-Brasil;

OU= Secretaria da Receita Federal – SRF;

CN= nome da AC (deve corresponder ao nome empresarial constante do CNPJ - Cadastro Nacional de Pessoa Jurídica, e será escrito até o limite do tamanho do campo disponível, vedada a abreviatura.

7.1.5. Restrições de nome

As restrições aplicáveis para os nomes dos titulares de certificados emitidos pela AC-SRF são as seguintes:

• não serão utilizados sinais de acentuação, tremas ou cedilhas;

• além dos caracteres alfanuméricos, podem ser utilizados somente os seguintes caracteres especiais:

Caractere	Código NBR9611 (hexadecimal)
Branco	20
!	21
"	22
#	23
$	24
%	25
&	26
'	27
(	28
)	29
*	2A
+	2B
,	2C

-	2D
.	2E
/	2F
:	3A
;	3B
=	3D
?	3F
@	40
\	5C

7.1.6. OID (Object Identifier) de Política de Certificado

O OID desta PC AC-SRF é 2.16.76.1.1.8.

7.1.7. Uso da extensão "Policy Constraints"

Não aplicável.

7.1.8. Sintaxe e semântica dos qualificadores de política

Nos certificados emitidos segundo esta PC AC-SRF, o campo policyQualifiers da extensão "Certificate Policies" contém o endereço Web da DPC da AC-SRF (http://www.receita.fazenda.gov.br/acsrf/dpcacsrf.pdf).

7.1.9. Semântica de processamento para extensões críticas

Extensões críticas são interpretadas conforme a RFC 2459.

7.2. PERFIL DE LCR

7.2.1. Número de versão

As LCR geradas pela AC-SRF, segundo esta PC AC-SRF, implementam a versão 2 de LCR definida no padrão ITU X.509, de acordo com o perfil estabelecido na RFC 2459.

7.2.2. Extensões de LCR e de suas entradas

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

1) "Authority Key Identifier": conterá o hash SHA-1 da chave pública da AC-SRF.

2) "CRL Number", não crítica: conterá um número seqüencial para cada LCR emitida pela AC-SRF.

7. 8. ADMINISTRAÇÃO DE ESPECIFICAÇÃO

8.1. PROCEDIMENTOS DE MUDANÇA DE ESPECIFICAÇÃO

Qualquer alteração nesta PC AC-SRF é submetida à aprovação do CG da ICP-Brasil. Esta PC AC-SRF é atualizada sempre que a DPC da AC-SRF o exigir.

8.2. POLÍTICAS DE PUBLICAÇÃO E NOTIFICAÇÃO

Esta Política de Certificados, PC AC-SRF, está disponível para a comunidade no endereço web (http://www.receita.fazenda.gov.br/acsrf/pcacsrf.pdf).

8.3. PROCEDIMENTOS DE APROVAÇÃO

Esta PC AC-SRF foi submetida à aprovação do CG da ICP-Brasil, durante o processo de credenciamento da AC-SRF, conforme o determinado pelo documento Critérios e Procedimentos para Credenciamento das Entidades Integrantes da ICP-Brasil.

Receita Federal

Política de Segurança da Autoridade Certificadora da SRF

PS AC-SRF

SECRETARIA DA RECEITA FEDERAL

Versão 1.0

SUMÁRIO

1- INTRODUÇÃO 4
2- OBJETIVOS 4
2.1 - A POLÍTICA DE SEGURANÇA DA AC-SRF TEM OS SEGUINTES OBJETIVOS ESPECÍFICOS: 4
3- ABRANGÊNCIA 4
3.1 - A POLÍTICA DE SEGURANÇA ABRANGE OS SEGUINTES ASPECTOS: 4
4- TERMINOLOGIA 4
5- CONCEITOS E DEFINIÇÕES 5
5.1 - CONCEITOS 5
6- REGRAS GERAIS 6
6.1- GESTÃO DE SEGURANÇA 6
6.2- GERENCIAMENTO DE RISCOS 6
6.3- INVENTÁRIO DE ATIVOS 7
6.4- PLANO DE CONTINUIDADE DO NEGÓCIO 7
7- REQUISITOS DE SEGURANÇA DE PESSOAL 7
7.1 - DEFINIÇÃO 7
7.2 – OBJETIVOS 7
7.3- DIRETRIZES 8
7.3.2- As Atribuições da Função 8
7.3.3- O Levantamento de Dados Pessoais 8
7.3.4- A Entrevista de Admissão 9
7.3.5- Avaliação Psicológica 9
7.3.6- O Desempenho da Função 9
7.3.7- A Credencial de Segurança 9
7.3.8- Treinamento em Segurança da Informação 9
7.3.9- Acompanhamento no Desempenho da Função 9
7.3.10- O Processo de Desligamento 10
7.3.11- O Processo de Liberação 10
7.3.12- A Entrevista de Desligamento 10
7.4- DEVERES 10
7.4.1- Deveres dos Empregados, Servidores e Prestadores de Serviço 10
7.4.2- Responsabilidades das Chefias 11
7.4.3- Responsabilidades Gerais 11
7.4.4- Responsabilidades da Gerência de Segurança 12
7.4.5- Responsabilidades dos Prestadores de Serviço 12
7.5- SANÇÕES 12

8- REQUISITOS DE SEGURANÇA DO AMBIENTE FÍSICO 13

8.1- DEFINIÇÃO 13
8.2- DIRETRIZES GERAIS 13

9- REQUISITOS DE SEGURANÇA DO AMBIENTE LÓGICO 14

9.1- DEFINIÇÃO 14
9.2- DIRETRIZES GERAIS 14
9.3- DIRETRIZES ESPECÍFICAS 15
9.3.1- Sistemas 15
9.3.2- Máquinas Servidoras 15
9.3.3- Redes Utilizadas Pela AC-SRF 16
9.3.4- Controle de Acesso Lógico (Baseado em Senhas) 18
9.3.5- Computação Pessoal 19
9.3.6- Combate a Vírus de Computador 20

10- REQUISITOS DE SEGURANÇA DOS RECURSOS CRIPTOGRÁFICOS 20

10.1- REQUISITOS GERAIS PARA SISTEMA CRIPTOGRÁFICO DA AC-SRF 20
10.2- CHAVES CRIPTOGRÁFICAS 21
10.3- TRANSPORTE DAS INFORMAÇÕES 21

11- AUDITORIA 21

11.1- INTRODUÇÃO 21
11.2- OBJETIVO DA AUDITORIA 22
11.3- ABRANGÊNCIA 22
11.3.1- Ambiente de Operação 22
11.3.2- Ciclo de Vida do Certificado. 22
11.4- DOCUMENTOS DE REFERÊNCIA 22
11.5- IDENTIDADE E QUALIFICAÇÃO DO AUDITOR 22
11.6- O RESULTADO DA AUDITORIA PODE CONTER AS SEGUINTES RECOMENDAÇÕES 23
11.7- FREQÜÊNCIA DAS AUDITORIAS 23

12- GERENCIAMENTO DE RISCOS 23

12.1- DEFINIÇÃO 23
12.2- FASES PRINCIPAIS 24
12.3- RISCOS RELACIONADOS ÀS ENTIDADES INTEGRANTES DA ICP-BRASIL: 24
12.4- CONSIDERAÇÕES GERAIS 25
12.5- IMPLEMENTAÇÃO DO GERENCIAMENTO DE RISCOS 25

13 - PLANO DE CONTINUIDADE DO NEGÓCIO 25

13.1- DEFINIÇÃO 25
13.2- DIRETRIZES GERAIS 25

1- INTRODUÇÃO

Este documento tem por finalidade estabelecer as diretrizes de segurança adotadas pela Autoridade Certificadora da SRF (AC-SRF). Tais diretrizes fundamentam as normas e procedimentos de segurança implementados.

Para o cumprimento da finalidade supramencionada são estabelecidos os objetivos a seguir.

2- OBJETIVOS

2.1 - A Política de Segurança da AC-SRF tem os seguintes objetivos específicos:

2.1 1 - Definir o escopo da segurança da AC-SRF.

2.1.2 - Orientar, por meio de suas diretrizes, todas as ações de segurança, para reduzir riscos e garantir a integridade, sigilo e disponibilidade das informações dos sistemas de informação e recursos.

2.1.3 - Permitir a adoção de soluções de segurança integradas.

2.1.4 - Servir de referência para auditoria, apuração e avaliação de responsabilidades.

3- ABRANGÊNCIA

3.1 - A Política de Segurança abrange os seguintes aspectos:

3.1.1- Requisitos de Segurança Humana.

3.1.2- Requisitos de Segurança Física.

3.1.3- Requisitos de Segurança Lógica.

3.1.4- Requisitos de Segurança dos Recursos Criptográficos.

4- TERMINOLOGIA

As regras e diretrizes de segurança são interpretadas de forma que todas as suas determinações são obrigatórias e cogentes.

5- CONCEITOS E DEFINIÇÕES

5.1 - Conceitos

Aplicam-se os conceitos abaixo no que se refere à Política de Segurança das entidades:

5.1.1 - Ativo de Informação – é o patrimônio, composto por todos os dados e informações geradas e manipuladas durante a execução dos sistemas e processos, da Autoridade Certificadora da Secretaria da Receita Federal (AC-SRF).

5.1.2 - Ativo de Processamento – é o patrimônio composto por todos os elementos de *hardware* e *software* necessários para a execução dos sistemas e processos das entidades, tanto os produzidos internamente quanto os adquiridos.

5.1.3 - Controle de Acesso – são restrições ao acesso às informações de um sistema exercido pela gerência de Segurança da Informação da AC-SRF.

5.1.4- Custódia – consiste na responsabilidade de se guardar um ativo para terceiros. Entretanto, a custódia não permite automaticamente o acesso ao ativo, nem o direito de conceder acesso a outros.

5.1.5- Direito de Acesso – é o privilégio associado a um cargo, pessoa ou processo para ter acesso a um ativo.

5.1.6- Ferramentas – é um conjunto de equipamentos, programas, procedimentos, normas e demais recursos através dos quais se aplica a Política de Segurança da Informação da AC-SRF.

5.1.7- Incidente de Segurança – é qualquer evento ou ocorrência que promova uma ou mais ações que comprometam ou que sejam uma ameaça à integridade, à autenticidade, ou à disponibilidade de qualquer ativo da AC-SRF.

5.1.8- Política de Segurança – é um conjunto de diretrizes destinadas a definir a proteção adequada dos ativos produzidos pelos Sistemas de Informação da AC-SRF.

5.1.9- Proteção dos Ativos – é o processo pelo qual os ativos receberão classificação quanto ao grau de sensibilidade. O meio de registro de um ativo de informação receberá a mesma classificação de proteção dada ao ativo que o contém.

5.1.10- Responsabilidade – é definida como sendo o conjunto das obrigações e dos deveres da pessoa que ocupa determinada função em relação ao acervo de informações.

5.1.11- Senha Fraca ou Óbvia – é aquela onde se utilizam caracteres de fácil associação com o dono da senha, ou que seja muito simples ou pequena; tais como: datas de aniversário, casamento, nascimento, o próprio nome, o nome de familiares, seqüências numéricas simples, palavras com significado, dentre outras.

6- REGRAS GERAIS

6.1- Gestão de Segurança

6.1.1- A Política de Segurança da AC-SRF se aplica a todos os seus recursos humanos, administrativos e tecnológicos. A abrangência dos recursos citados refere-se tanto àqueles ligados a ela em caráter permanente quanto temporário.

6.1.2- Esta política é comunicada para todo o pessoal envolvido e largamente divulgada pela AC-SRF, garantindo que todos tenham consciência da mesma e a pratiquem na organização.

6.1.3- Todo o pessoal recebe as informações necessárias para cumprir adequadamente o que está determinado nesta política de segurança.

6.1.4- Um programa de conscientização sobre segurança da informação está implementado para assegurar que todo o pessoal seja informado sobre os potenciais riscos de segurança e exposição a que estão submetidos os sistemas e operações da AC-SRF. Especificamente, o pessoal envolvido ou que se relaciona com os usuários é informado sobre ataques típicos de engenharia social e como se proteger deles.

6.1.5- Os procedimentos são documentados e implementados para garantir que quando o pessoal contratado ou prestadores de serviços sejam transferidos, remanejados, promovidos ou demitidos, todos os privilégios de acesso aos sistemas, informações e recursos sejam devidamente revistos, modificados ou revogados.

6.1.6- Existe previsão de mecanismo e repositório centralizado para ativação e manutenção de trilhas, *logs* e demais notificações de incidentes. Este mecanismo é incluído nas medidas tomadas por um grupo encarregado de responder a este tipo de ataque, para prover uma defesa ativa e corretiva contra os mesmos.

6.1.7- Os processos de aquisição de bens e serviços, especialmente de Tecnologia da Informação – TI, estão em conformidade com esta Política de Segurança.

6.1.8- Esta Política de Segurança será revisada e atualizada periodicamente no máximo a cada 2 (dois) anos, caso não ocorram eventos ou fatos relevantes que exijam uma revisão imediata.

6.1.9- No que se refere a segurança da informação, é considerado proibido, tudo aquilo que não esteja previamente autorizado pelo responsável da área de segurança da AC-SRF.

6.2- Gerenciamento de Riscos

O processo de gerenciamento de riscos é revisto, no máximo a cada 18 (dezoito) meses, pela AC-SRF, para prevenção contra riscos, inclusive aqueles advindos de

novas tecnologias, visando a elaboração de planos de ação apropriados para proteção dos componentes ameaçados.

6.3- Inventário de Ativos

Todos os ativos da AC-SRF são inventariados, classificados, permanentemente atualizados, e possuem gestor responsável formalmente designado.

6.4- Plano de Continuidade do Negócio

6.4.1- Existe um plano de continuidade do negócio implementado. O qual é testado, pelo menos uma vez por ano, para garantir a continuidade dos serviços críticos.

6.4.2- A AC-SRF apresenta planos de gerenciamento de incidentes e de ação de resposta a incidentes, aprovados pela AC Raiz da ICP-Brasil.

6.4.3- O certificado da AC-SRF será imediatamente revogado se um evento provocar a perda ou comprometimento de sua chave privada ou do seu meio de armazenamento. Nesta situação, seguirá os procedimentos detalhados na sua DPC.

6.4.4- Todos os incidentes são reportados à AC Raiz imediatamente, a partir do momento em que for verificada a ocorrência. Estes incidentes são reportados de modo sigiloso a pessoas especialmente designadas para isso.

7- REQUISITOS DE SEGURANÇA DE PESSOAL

7.1 - Definição

Conjunto de medidas e procedimentos de segurança, a serem observados pelos prestadores de serviço e todos os empregados, necessário à proteção dos ativos da AC-SRF.

7.2 – Objetivos

7.2.1- Reduzir os riscos de erros humanos, furto, roubo, apropriação indébita, fraude ou uso não apropriado dos ativos da AC-SRF.

7.2.2- Prevenir e neutralizar as ações sobre as pessoas que possam comprometer a segurança da AC-SRF.

7.2.3- Orientar e capacitar todo o pessoal envolvido na realização de trabalhos diretamente relacionados à AC-SRF, assim como o pessoal em desempenho de funções de apoio, tais como a manutenção das instalações físicas e a adoção de medidas de proteção compatíveis com a natureza da função que desempenham.

7.2.4- Orientar o processo de avaliação de todo o pessoal que trabalhe na AC-SRF, mesmo em caso de funções desempenhadas por prestadores de serviço.

7.3- Diretrizes

7.3.1- O Processo de Admissão

7.3.1.1- São adotados critérios rígidos para o processo seletivo de candidatos, com o propósito de selecionar, para os quadros da AC-SRF, pessoas reconhecidamente idôneas e sem antecedentes que possam comprometer a segurança ou credibilidade.

7.3.1.2- A AC-SRF não admite estagiários no exercício de atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados.

7.3.1.3- O empregado, servidor ou prestador de serviço assina termo de compromisso assumindo o dever de manter sigilo, mesmo quando desligado, sobre todos os ativos de informações e de processos da AC-SRF.

7.3.2- As Atribuições da Função

7.3.2.1- As atribuições de cada função estão claramente relacionadas, de acordo com a característica das atividades desenvolvidas, a fim de determinar-se o perfil necessário do empregado, servidor ou prestador de serviço, considerando-se os seguintes itens:

7.3.2.1.1- A descrição sumária das tarefas inerentes à função.

7.3.2.1.2- As necessidades de acesso a informações sensíveis.

7.3.2.1.3- O grau de sensibilidade do setor onde a função é exercida;

7.3.2.1.4- As necessidades de contato de serviço interno e/ou externo.

7.3.2.1.5- As características de responsabilidade, decisão e iniciativa inerentes à função.

7.3.2.1.6- A qualificação técnica necessária ao desempenho da função.

7.3.3- O Levantamento de Dados Pessoais

É elaborada pesquisa do histórico da vida pública do candidato, com o propósito de levantamento de seu perfil.

7.3.4- A Entrevista de Admissão

7.3.4.1- É realizada por profissional qualificado, com o propósito de confirmar e/ou identificar dados não detectados ou não confirmados, durante a pesquisa para a sua admissão.

7.3.4.2- Na entrevista inicial são avaliadas as características de interesse e motivação do candidato, sendo que as informações veiculadas na entrevista do candidato serão somente aquelas de caráter público.

7.3.5- Avaliação Psicológica

É realizada por profissional legalmente qualificado, com o propósito de avaliar o candidato e a existência de atributos pessoais exigidos para o cargo e/ou função a ser desempenhado.

7.3.6- O Desempenho da Função

7.3.6.1- Os servidores, empregados e prestadores de serviço terão seu desempenho avaliado e acompanhado periodicamente com o propósito de detectar a necessidade de atualização técnica e de segurança.

7.3.6.2- Os empregados, servidores e prestadores de serviço da AC-SRF têm acesso às informações, mediante o fornecimento de instruções e orientações sobre as medidas e procedimentos de segurança.

7.3.7- A Credencial de Segurança

7.3.7.1- Os empregados, servidores e prestadores de serviço são identificados por meio de uma credencial, a qual os habilita a ter acesso a informações sensíveis, de acordo com a classificação do grau de sigilo da informação e, conseqüentemente, com o grau de sigilo compatível ao cargo e/ou a função a ser desempenhada.

7.3.7.2- A Credencial de Segurança somente é concedida por autoridade competente, ou por ela delegada, e se fundamenta na necessidade de conhecimento técnico dos aspectos inerentes ao exercício funcional e na análise da sensibilidade do cargo e/ou função.

7.3.8- Treinamento em Segurança da Informação

Existe um processo pelo qual é apresentada aos empregados, servidores e prestadores de serviço a Política de Segurança da Informação e suas normas e procedimentos relativos ao trato de informações e/ou dados sigilosos, com o propósito de desenvolver e manter uma efetiva conscientização de segurança, assim como instruir o seu fiel cumprimento.

7.3.9- Acompanhamento no Desempenho da Função

7.3.9.1- É realizado processo de avaliação de desempenho da função que documenta a observação do comportamento pessoal e funcional dos empregados, servidores e prestadores de serviço, realizada pela chefia imediata dos mesmos.

7.3.9.2- É motivo de registro atos, atitudes e comportamentos positivos e negativos relevantes, verificados durante o exercício profissional do empregado.

7.3.9.3- Os comportamentos incompatíveis, ou que possam gerar comprometimentos á segurança, são averiguados e comunicados à chefia imediata.

7.3.9.4- As chefias imediatas asseguram que todos os empregados, servidores e prestadores de serviço tenham conhecimento e compreensão das normas e procedimentos de segurança em vigor.

7.3.10- O Processo de Desligamento

7.3.10.1- O acesso de ex-empregados às instalações, quando necessário, é restrito às áreas de acesso público.

7.3.10.2- Sua credencial, identificação, crachá, uso de equipamentos, mecanismos e acessos físicos e lógicos são revogados.

7.3.11- O Processo de Liberação

O empregado, o servidor ou o prestador de serviço firma, antes do desligamento, declaração de que não possui qualquer tipo de pendência junto às diversas unidades que compõem a AC-SRF.

7.3.12- A Entrevista de Desligamento

É realizada entrevista de desligamento para orientar o empregado, servidor e prestador de serviço sobre sua responsabilidade na manutenção do sigilo de dados e/ou conhecimentos sigilosos de sistemas críticos aos quais teve acesso durante sua permanência na AC-SRF.

7.4- Deveres

7.4.1- Deveres dos Empregados, Servidores e Prestadores de Serviço

7.4.1.1- Preservar a integridade e guardar sigilo das informações de que fazem uso, bem como zelar e proteger os respectivos recursos de processamento de informações.

7.4.1.2- Cumprir está política de segurança, sob pena de incorrer nas sanções disciplinares e legais cabíveis.

7.4.1.3- Utilizar os Sistemas de Informações da AC-SRF e os recursos a ela relacionados somente para os fins previstos pela Gerência de Segurança.

7.4.1.4- Cumprir as regras específicas de proteção estabelecidas aos ativos de informação.

7.4.1.5- Manter o caráter sigiloso da senha de acesso aos recursos e sistemas da AC-SRF.

7.4.1.6- Não compartilhar, sob qualquer forma, informações confidenciais com outros que não tenham a devida autorização de acesso.

7.4.1.7- Responder, por todo e qualquer acesso, aos recursos da AC-SRF bem como pelos efeitos desses acessos efetivados através do seu código de identificação, ou outro atributo para esse fim utilizado.

7.4.1.8- Respeitar a proibição de não usar, inspecionar, copiar ou armazenar programas de computador ou qualquer outro material, em violação da legislação de propriedade intelectual pertinente.

7.4.1.9- Comunicar ao seu superior imediato o conhecimento de qualquer irregularidade ou desvio.

7.4.2- Responsabilidades das Chefias

7.4.2.1- As responsabilidades das chefias compreendem, dentre outras, as seguintes atividades:

7.4.2.1.1- Gerenciar o cumprimento desta política de segurança, por parte de seus empregados, servidores e prestadores de serviço.

7.4.2.1.2- Identificar os desvios praticados e adotar as medidas corretivas apropriadas.

7.4.2.1.3- Impedir o acesso de empregados demitidos ou demissionários aos ativos de informações, utilizando-se dos mecanismos de desligamento contemplados pelo respectivo plano de desligamento do empregado, servidor e prestador de serviço.

7.4.2.1.4- Proteger, em nível físico e lógico, os ativos de informação e de processamento utilizados pela AC-SRF relacionados com sua área de atuação.

7.4.2.1.5- Garantir que o pessoal sob sua supervisão compreenda e desempenhe a obrigação de proteger a Informação da AC-SRF.

7.4.2.1.6- Comunicar formalmente à unidade que efetua a concessão de privilégios a usuários de TI, quais os empregados, servidores e prestadores de serviço, sob sua supervisão, que podem acessar as informações da AC-SRF.

7.4.2.1.7- Comunicar formalmente à unidade que efetua a concessão de privilégios aos usuários de TI, quais os empregados, servidores e prestadores de serviço demitidos ou transferidos, para exclusão no cadastro dos usuários.

7.4.2.1.8- Comunicar formalmente à unidade que efetua a concessão de privilégios a usuários de TI, aqueles que estejam respondendo a processos, sindicâncias ou que estejam licenciados, para inabilitação no cadastro dos usuários.

7.4.3- Responsabilidades Gerais

7.4.3.1- Cada área que detém os ativos de processamento e de informação é responsável por eles, provendo a sua proteção de acordo com a política de classificação da informação da AC-SRF.

7.4.3.2- Todos os ativos de informações têm claramente definidos os responsáveis pelo seu uso.

7.4.3.3- Todos os ativos de processamento da AC-SRF estão relacionados no Plano de Continuidade do Negócio.

7.4.4- Responsabilidades da Gerência de Segurança

7.4.4.1- Estabelecer as regras de proteção dos ativos da AC-SRF.

7.4.4.2 - Decidir quanto às medidas a serem tomadas no caso de violação das regras estabelecidas.

7.4.4.3 - Revisar pelo menos anualmente, as regras de proteção estabelecidas.

7.4.4.4- Restringir e controlar o acesso e os privilégios de usuários remotos e externos.

7.4.4.5- Elaborar e manter atualizado o Plano de Continuidade de Negócio da AC-SRF;

7.4.4.6- Executar as regras de proteção estabelecidas por esta Política de Segurança;

7.4.4.7- Detectar, identificar, registrar e comunicar a AC Raíz as violações ou tentativas de acesso não autorizado.

7.4.4.8- Definir e aplicar, para cada usuário de TI, restrições de acesso à Rede, como horário e dias autorizados, entre outras.

7.4.4.9- Manter registros de atividades de usuários de TI (logs) por um período de tempo superior a 6 (seis) anos. Os registros conterão a hora e a data das atividades, a identificação do usuário de TI, comandos (e seus argumentos) executados, identificação da estação local ou da estação remota que iniciou a conexão, número dos processos e condições de erro observadas (tentativas rejeitadas, erros de consistência etc).

7.4.4.10- Limitar o prazo de validade das contas de prestadores de serviço ao período da contratação.

7.4.4.11- Excluir as contas inativas.

7.4.4.12- Fornecer senhas de contas privilegiadas somente aos empregados que necessitem efetivamente dos privilégios, mantendo-se o devido registro e controle.

7.4.5- Responsabilidades dos Prestadores de Serviço

Estão previstas no contrato, cláusulas que contemplam a responsabilidade dos prestadores de serviço no cumprimento desta Política de Segurança da Informação e suas normas e procedimentos.

7.5- Sanções

Sanções previstas pela legislação vigente.

8- REQUISITOS DE SEGURANÇA DO AMBIENTE FÍSICO

8.1- Definição

Ambiente físico é aquele composto por todo o ativo permanente da AC-SRF.

8.2- Diretrizes Gerais

8.2.1- As responsabilidades pela segurança física dos sistemas da AC-SRF estão definidas e atribuídas a indivíduos claramente identificados.

8.2.2- A localização das instalações e o sistema de certificação da AC-SRF não são publicamente identificados.

8.2.3- Sistemas de segurança para acesso físico estão instalados para controlar e auditar o acesso aos sistemas de certificação.

8.2.4- Controles duplicados sobre o inventário e cartões/chaves de acesso estão estabelecidos. Uma lista atualizada do pessoal que possui cartões/chaves é mantida.

8.2.5- Chaves criptográficas sob custódia do responsável são fisicamente protegidas contra acesso não autorizado, uso ou duplicação.

8.2.6- Perdas de cartões/chaves de acesso são imediatamente comunicadas ao responsável pela gerência de segurança da AC-SRF. Ele tomará as medidas apropriadas para prevenir acessos não autorizados.

8.2.7- Os sistemas da AC-SRF estão localizados em área protegida ou afastada de fontes potentes de magnetismo ou de interferência de rádio freqüência.

8.2.8- Recursos e instalações críticas ou sensíveis são mantidos em áreas seguras, protegidas por um perímetro de segurança definido, com barreiras de segurança e controle de acesso. Elas são fisicamente protegidas de acesso não autorizado, dano ou interferência. A proteção fornecida é proporcional aos riscos identificados.

8.2.9- A entrada e saída, nestas áreas ou partes dedicadas, são automaticamente registradas com data e hora definidas e são revisadas diariamente pelo responsável pela gerência de segurança da informação que atende a AC-SRF e mantidas em local adequado e sob sigilo.

8.2.10- O acesso aos componentes da infra-estrutura, atividade fundamental ao funcionamento dos sistemas de AC-SRF, como painéis de controle de energia, comunicações e cabeamento, é restrito ao pessoal autorizado.

8.2.11- Sistemas de detecção de intrusão são utilizados para monitorar e registrar os acessos físicos aos sistemas de certificação nas horas de utilização.

8.2.12- O inventário de todo o conjunto de ativos de processamento é registrado e mantido atualizado, no mínimo, mensalmente.

8.2.13- Quaisquer equipamentos de gravação, fotografia, vídeo, som ou outro tipo de equipamento similar, só são utilizados a partir de autorização formal e mediante supervisão.

8.2.14- Nas instalações da AC-SRF, todos utilizam alguma forma visível de identificação (por exemplo: crachá), e informam à segurança sobre a presença de qualquer pessoa não identificada ou de qualquer estranho não acompanhado.

8.2.15- Visitantes das áreas de segurança são supervisionados. Suas horas de entrada e saída e o local de destino são registrados. Essas pessoas obtêm acesso apenas às áreas específicas, com propósitos autorizados, e esses acessos seguem instruções baseadas nos requisitos de segurança da área visitada.

8.2.16- Os ambientes onde ocorrem os processos críticos da AC-SRF são monitorados, em tempo real, com as imagens registradas por meio de sistemas de CFTV.

8.2.17- Existem sistemas de detecção de intrusos instalados e testados regularmente de forma a cobrir os ambientes, as portas e janelas acessíveis, nos ambientes onde ocorrem processos críticos. As áreas não ocupadas possuem um sistema de alarme que permanece sempre ativado.

9- REQUISITOS DE SEGURANÇA DO AMBIENTE LÓGICO

9.1- Definição

Ambiente lógico é composto por todo o ativo de informações da AC-SRF.

9.2- Diretrizes Gerais

9.2.1- A informação é protegida de acordo com o seu valor, sensibilidade e criticidade. Para tanto, existe um sistema de classificação da informação.

9.2.2- Os dados, as informações e os sistemas de informação da AC-SRF e sob sua guarda, são protegidos contra ameaças e ações não autorizadas, acidentais ou não, de modo a reduzir riscos e garantir a integridade, sigilo e disponibilidade desses bens.

9.2.3- As violações de segurança são registradas e esses registros analisados periodicamente para o propósito de caráter corretivo, legal e de auditoria. Os registros são protegidos e armazenados de acordo com a sua classificação.

9.2.4- Os sistemas e recursos que suportam funções críticas para operação da AC-SRF, asseguram a capacidade de recuperação nos prazos e condições definidas em situações de contingência.

9.2.5- O inventário sistematizado de toda a estrutura que serve como base para manipulação, armazenamento e transmissão dos ativos de processamento, é registrado e mantido atualizado em intervalos de tempo definidos pela AC-SRF.

9.3- Diretrizes Específicas

9.3.1- Sistemas

9.3.1.1- As necessidades de segurança são identificadas para cada etapa do ciclo de vida dos sistemas disponíveis na AC-SRF. A documentação dos sistemas é mantida atualizada. A cópia de segurança é testada e mantida atualizada.

9.3.1.2- Os sistemas possuem controle de acesso de modo a assegurar o uso apenas a usuários ou processos autorizados. O responsável pela autorização ou confirmação da autorização está claramente definido e registrado.

9.3.1.3- Os arquivos de *logs* estão criteriosamente definidos para permitir recuperação nas situações de falhas, auditoria nas situações de violações de segurança e contabilização do uso de recursos. Os *logs* são periodicamente analisados, conforme definido na DPC AC-SRF, para identificar tendências, falhas ou usos indevidos. Os *logs* são protegidos e armazenados de acordo com sua classificação.

9.3.1.4- Estão estabelecidas e mantidas medidas e controles de segurança para verificação crítica dos dados e configuração de sistemas e dispositivos quanto a sua precisão, consistência e integridade.

9.3.1.5- Os sistemas são avaliados com relação aos aspectos de segurança (testes de vulnerabilidade) antes de serem disponibilizados para a produção. As vulnerabilidades do ambiente são avaliadas periodicamente e as recomendações de segurança são adotadas.

9.3.2- Máquinas Servidoras

9.3.2.1- O acesso lógico, ao ambiente ou serviços disponíveis em servidores, é controlado e protegido. As autorizações são revistas, confirmadas e registradas continuadamente. O responsável pela autorização ou confirmação da autorização está claramente definido e registrado.

9.3.2.2- Os acessos lógicos são registrados em *logs*, que são analisados periodicamente. O tempo de retenção dos arquivos de *logs* e as medidas de proteção associadas estão precisamente definidos.

9.3.2.3- São adotados procedimentos sistematizados para monitorar a segurança do ambiente operacional, principalmente no que diz respeito à integridade dos arquivos de configuração do Sistema Operacional e de outros arquivos críticos. Os eventos são armazenados em relatórios de segurança (*logs*) de modo que sua análise permita a geração de trilhas de auditoria a partir destes registros.

9.3.2.4- As máquinas estão sincronizadas para permitir o rastreamento de eventos.

9.3.2.5- Proteção lógica adicional (criptografia) é adotada para evitar o acesso não-autorizado às informações.

9.3.2.6- A versão do Sistema Operacional, assim como outros *softwares* básicos instalados em máquinas servidoras, são mantidos atualizados, em conformidade com as recomendações dos fabricantes.

9.3.2.7- São utilizados somente *softwares* autorizados pela própria AC-SRF nos seus equipamentos. É realizado o controle da distribuição e instalação dos mesmos.

9.3.2.8- O acesso remoto a máquinas servidoras é realizado adotando os mecanismos de segurança definidos para evitar ameaças à integridade e sigilo do serviço.

9.3.2.9- Os procedimentos de cópia de segurança (*backup*) e de recuperação *(restore)* são documentados, mantidos atualizados e são regularmente testados, de modo a garantir a disponibilidade das informações.

9.3.3- Redes Utilizadas Pela AC-SRF

9.3.3.1- O tráfego das informações no ambiente de rede é protegido contra danos ou perdas, bem como acesso, uso ou exposição indevidas.

9.3.3.2- Componentes críticos da rede local são mantidos em salas protegidas e com acesso físico e lógico controlado, sendo protegidos contra danos, furtos, roubos e intempéries.

9.3.3.3- São adotadas as facilidades de segurança disponíveis de forma inata nos ativos de processamento da rede.

9.3.3.4- A configuração de todos os ativos de processamento é averiguada quando da sua instalação inicial, para que sejam detectadas e corrigidas as vulnerabilidades inerentes à configuração padrão que se encontram nesses ativos em sua primeira ativação.

9.3.3.5- Serviços vulneráveis recebem nível de proteção adicional.

9.3.3.6- O uso de senhas é submetido a uma política específica para sua gerência e utilização.

9.3.3.7- O acesso lógico aos recursos da rede local é realizado por meio de sistema de controle de acesso. O acesso é concedido e mantido pela administração da rede, baseado nas responsabilidades e tarefas de cada usuário.

9.3.3.8- A utilização de qualquer mecanismo capaz de realizar testes de qualquer natureza, como por exemplo, monitoração sobre os dados, os sistemas e dispositivos que compõem a rede, são utilizados à partir de autorização formal e mediante supervisão.

9.3.3.9- A conexão com outros ambientes de rede e alterações internas na sua topologia e configuração são formalmente documentadas e mantidas, de forma a permitir registro histórico, tendo a autorização da administração da rede e da

gerência de segurança. O diagrama topológico, a configuração e o inventário dos recursos são mantidos atualizados.

9.3.3.10- Estão definidos relatórios de segurança (*logs*) de modo a auxiliar no tratamento de desvios, recuperação de falhas, contabilização e auditoria. Os *logs* são analisados periodicamente e o período de análise estabelecido é o menor possível.

9.3.3.11- São adotadas proteções físicas adicionais para os recursos de rede considerados críticos.

9.3.3.12- Proteção lógica adicional é adotada para evitar o acesso não-autorizado às informações.

9.3.3.13- A infra-estrutura de interligação lógica é protegida contra danos mecânicos e conexão não autorizada.

9.3.3.14- A alimentação elétrica para a rede local é separada da rede convencional, sendo observadas as recomendações dos fabricantes dos equipamentos utilizados, assim como as normas ABNT aplicáveis.

9.3.3.15- O tráfego de informações é monitorado, a fim de verificar sua normalidade, assim como detectar situações anômalas do ponto de vista da segurança.

9.3.3.16- São observadas as questões envolvendo propriedade intelectual quando da cópia de software ou arquivos de outras localidades.

9.3.3.17- Informações sigilosas, corporativas ou que possam causar prejuízo à AC-SRF são protegidas e não são enviadas para outras redes, sem proteção adequada.

9.3.3.18- Todo serviço de rede não explicitamente autorizado é bloqueado ou desabilitado.

9.3.3.19- Mecanismos de segurança baseados em sistemas de proteção de acesso (*firewall*) são utilizados para proteger as transações entre redes externas e a rede interna da AC-SRF.

9.3.3.20- Os registros de eventos são analisados periodicamente, no menor prazo possível e em intervalos de tempo adequados.

9.3.3.21- É adotado um padrão de segurança para todos os tipos de equipamentos servidores, considerando aspectos físicos e lógicos.

9.3.3.22- Todos os recursos considerados críticos para o ambiente de rede, e que possuam mecanismos de controle de acesso, utilizam tal controle.

9.3.3.23- A localização dos serviços baseados em sistemas de proteção de acesso (*firewall*) é resultante de uma análise de riscos. No mínimo, os seguintes aspectos são considerados: requisitos de segurança definidos pelo serviço; objetivo do serviço; público alvo; classificação da informação; forma de acesso; freqüência de atualização do conteúdo; forma de administração do serviço; e volume de tráfego.

9.3.3.24- Ambientes de rede considerados críticos são isolados de outros ambientes de rede, de modo a garantir um nível adicional de segurança.

9.3.3.25- Conexões entre as redes da AC-SRF e redes externas estão restritas somente àquelas que visem efetivar os processos.

9.3.3.26- As conexões de rede são ativadas: primeiro, sistemas com função de certificação; segundo, sistemas que executam as funções de registros e repositório. Se isto não for possível, emprega-se controles de compensação, tais como o uso de *proxies* que são implementados para proteger os sistemas que executam a função de certificação contra possíveis ataques.

9.3.3.27- Sistemas que executam a função de certificação estão isolados para minimizar a exposição contra tentativas de comprometer o sigilo, a integridade e a disponibilidade das funções de certificação.

9.3.3.28- A chave de certificação da AC-SRF é protegida de acesso desautorizado, para garantir seu sigilo e integridade.

9.3.3.29- A segurança das comunicações intra-rede e inter-rede, entre os sistemas das entidades da AC-SRF, é garantida pelo uso de mecanismos que assegurem o sigilo e a integridade das informações trafegadas.

9.3.3.30- As ferramentas de detecção de intrusos são implantadas para monitorar as redes críticas, alertando periodicamente os administradores das redes sobre as tentativas de intrusão.

9.3.4- Controle de Acesso Lógico (Baseado em Senhas)

9.3.4.1- Usuários e aplicações que necessitem ter acesso a recursos da AC-SRF são identificados e autenticados.

9.3.4.2- O sistema de controle de acesso mantém as habilitações atualizadas e registros que permitem a contabilização do uso, auditoria e recuperação nas situações de falha.

9.3.4.3- Nenhum usuário é capaz de obter os direitos de acesso de outro usuário.

9.3.4.4- A informação que especifica os direitos de acesso de cada usuário ou aplicação é protegida contra modificações não autorizadas.

9.3.4.5- O arquivo de senhas tem o acesso controlado.

9.3.4.6- As autorizações são definidas de acordo com a necessidade de desempenho das funções (acesso motivado) e considerando o princípio dos privilégios mínimos (ter acesso apenas aos recursos ou sistemas necessários para a execução de tarefas).

9.3.4.7- As senhas são individuais, secretas, intransferíveis e são protegidas com grau de segurança compatível com a informação associada.

9.3.4.8- O sistema de controle de acesso possui mecanismos que impedem a geração de senhas fracas ou óbvias.

9.3.4.9- As seguintes características das senhas são definidas de forma adequada: conjunto de caracteres permitidos; tamanho mínimo e máximo; prazo de validade máximo; forma de troca; e, restrições específicas.

9.3.4.10- A distribuição de senhas aos usuários de TI (inicial ou não) é feita de forma segura. A senha inicial, quando gerada pelo sistema, é trocada, pelo usuário de TI, no primeiro acesso.

9.3.4.11- O sistema de controle de acesso permite ao usuário alterar sua senha sempre que desejar. A troca de uma senha bloqueada só é executada após a identificação positiva do usuário. A senha digitada não é exibida.

9.3.4.12- São adotados critérios para bloquear ou desativar usuários de acordo com o período definido sem acesso ou tentativas de acesso mal sucedidas.

9.3.4.13- O sistema de controle de acesso solicita nova autenticação após certo tempo de inatividade da sessão (*time-out*).

9.3.4.14- O sistema de controle de acesso exibe, na tela inicial, mensagem informando que o serviço só pode ser utilizado por usuários autorizados. No momento de conexão o sistema exibirá para o usuário informações sobre o último acesso.

9.3.4.15- O registro das atividades (*logs*) do sistema de controle de acesso é definido de modo a auxiliar no tratamento das questões de segurança, permitindo a contabilização do uso, auditoria e recuperação nas situações de falhas. Os *logs* são periodicamente analisados.

9.3.4.16- Os usuários e administradores do sistema de controle de acesso são formal e expressamente conscientizados de suas responsabilidades, mediante assinatura de termo de compromisso.

9.3.5- Computação Pessoal

9.3.5.1- As estações de trabalho, incluindo equipamentos portáteis ou *stand alone*, e informações são protegidas contra danos ou perdas, bem como acesso, uso ou exposição indevidos.

9.3.5.2- Equipamentos que executem operações sensíveis recebem proteção adicional, considerando os aspectos lógicos (controle de acesso e criptografia) e físicos (proteção contra furto ou roubo do equipamento ou componentes).

9.3.5.3- São adotadas medidas de segurança lógica referentes a combate a vírus, *backup*, controle de acesso e uso de software não autorizado.

9.3.5.4- As informações armazenadas em meios eletrônicos são protegidas contra danos, furtos ou roubos, sendo adotados procedimentos de *backup*, definidos em documento específico.

9.3.5.5- Informações sigilosas, corporativas ou cuja divulgação possa causar prejuízo à AC-SRF, só são utilizadas em equipamentos da AC-SRF onde foram geradas ou naqueles por elas autorizados, com controles adequados.

9.3.5.6- O acesso às informações atende aos requisitos de segurança, considerando o ambiente e forma de uso do equipamento (uso pessoal ou coletivo).

9.3.5.7- Os usuários de TI utilizam apenas *softwares* licenciados pelo fabricante nos equipamentos da AC-SRF, observadas as normas da ICP-Brasil e legislação de *software*.

9.3.5.8- A AC-SRF estabelece os aspectos de controle, distribuição e instalação de *softwares* utilizados.

9.3.5.9- A impressão de documentos sigilosos é feita sob supervisão do responsável. Os relatórios impressos são protegidos contra perda, reprodução e uso não-autorizado.

9.3.5.10- O inventário dos recursos é mantido atualizado.

9.3.5.11- Os sistemas em uso solicitam nova autenticação após certo tempo de inatividade da sessão (*time-out*).

9.3.5.12- As mídias são eliminadas de forma segura, quando não forem mais necessárias. Procedimentos formais para a eliminação segura das mídias são definidos, para minimizar os riscos.

9.3.6- Combate a Vírus de Computador

Os procedimentos de combate a processos destrutivos (*vírus, cavalo-de-tróia e worms*) estão sistematizados e abrangem máquinas servidoras, estações de trabalho, equipamentos portáteis e microcomputadores *stand alone*.

10- REQUISITOS DE SEGURANÇA DOS RECURSOS CRIPTOGRÁFICOS

10.1- Requisitos Gerais para Sistema Criptográfico da AC-SRF

10.1.1- O sistema criptográfico da AC-SRF é entendido como sendo um sistema composto de documentação normativa específica de criptografia aplicada na ICP-Brasil, conjunto de requisitos de criptografia, projetos, métodos de implementação, módulos implementados de *hardware* e *software*, definições relativas a algoritmos criptográficos e demais algoritmos integrantes de um processo criptográfico, procedimentos adotados para gerência das chaves criptográficas, métodos adotados para testes de robustez das cifras e detecção de violações dessas.

10.1.2- Toda a documentação, referente a definição, descrição e especificação dos componentes dos sistemas criptográficos utilizada na AC-SRF é aprovada pela AC Raiz.

10.1.3- A força do sistema criptográfico é periodicamente testada por entidades competentes na área de criptografia. A periodicidade a que se refere este item não será superior a 2 (dois) anos.

10.1.4- Os testes necessários para satisfazer o item anterior são previamente definidos em documento normativo específico e de caráter oficial aprovado pelo CG ICP-Brasil.

10.1.5- Todo parâmetro crítico cuja exposição indevida comprometa a segurança do sistema criptográfico da AC-SRF é armazenado cifrado.

10.1.6- Os aspectos relevantes relacionados à criptografia no âmbito da AC-SRF são detalhados em documentos específicos, aprovados pela AC Raiz.

10.2- Chaves Criptográficas

10.2.1- A manipulação das chaves criptográficas utilizadas nos sistemas criptográficos da AC-SRF é restrita a um número mínimo e essencial de pessoas, assim como esta submetida a mecanismos de controle considerados adequados pela CG da ICP Brasil.

10.2.2- As pessoas, a que se refere o item anterior, estão formalmente designadas pela chefia competente, conforme as funções desempenhadas e o correspondente grau de privilégios, assim como tem suas responsabilidades explicitamente definidas.

10.2.3- Os algoritmos de criação e de troca das chaves criptográficas utilizados no sistema criptográfico da AC-SRF serão aprovados pelo CG ICP-Brasil.

10.2.4- Os diferentes tipos de chaves criptográficas e suas funções no sistema criptográfico da AC-SRF estão explicitados na Política de Certificados da AC-SRF.

10.3- Transporte das Informações

10.3.1- O processo de transporte de chaves criptográficas e demais parâmetros do sistema de criptografia da AC-SRF tem a integridade e o sigilo assegurados, por meio do emprego de soluções criptográficas específicas.

10.3.2- São adotados recursos de VPN (*Virtual Private Networks* – redes privadas virtuais), baseado em criptografia, para a troca de informações sensíveis por meio de redes públicas, entre as redes das entidades da ICP-Brasil que pertençam a uma mesma organização.

11- AUDITORIA

11.1- Introdução

11.1.1- São realizadas auditorias periódicas na AC-SRF, pela AC Raiz ou por prestadores de serviço por ela contratados.

11.1.2- As atividades da AC-SRF estão associadas ao conceito de confiança. O processo de auditoria periódica representa um dos instrumentos que facilita a percepção e transmissão de confiança à comunidade de usuários.

11.2- Objetivo da Auditoria

Verificar a capacidade da AC-SRF, AR e repositórios em atender os requisitos da ICP-Brasil. O resultado da auditoria é um item fundamental a ser considerado no processo de credenciamento da AC-SRF para a ICP-Brasil, assim como, para a manutenção da condição de credenciada.

11.3- Abrangência

A auditoria aborda os aspectos relativos ao ambiente de operação e ciclo de vida de certificados. Os seguintes tópicos são verificados:

11.3.1- Ambiente de Operação

11.3.1.1- Segurança da operação.

11.3.1.2- Segurança de pessoal.

11.3.1.3- Segurança física.

11.3.1.4- Segurança lógica.

11.3.1.5- Segurança de telecomunicações.

11.3.1.6- Segurança de recursos criptográficos.

11.3.1.7- Plano de contingência.

11.3.2- Ciclo de Vida do Certificado.

11.3.2.1- Solicitação.

11.3.2.2- Validação.

11.3.2.3- Emissão;

11.3.2.4- Uso.

11.3.2.5- Revogação.

11.4- Documentos de Referência

A auditoria é realizada tendo como orientação básica os atos normativos que disciplinam as atividades exercidas no âmbito da ICP-Brasil.

11.5- Identidade e Qualificação do Auditor

A auditoria da AC-SRF atende aos seguintes requisitos mínimos:

11.5.1. - Corpo técnico com comprovada experiência nas áreas de segurança da informação (ambientes físico e lógico), criptografia, infra-estrutura de chaves pública e sistemas críticos.

11.5.2- Experiência em serviços de auditoria dessa mesma natureza e referências de outros serviços de auditoria similares.

11.5.3- Utilização de padrões internacionais (como exemplo: ISO 17799) ou padrão similar como referência de melhores práticas e procedimentos.

11.6- O Resultado da Auditoria Pode Conter as Seguintes Recomendações

11.6.1- Suspender temporariamente os serviços na AC-SRF até correção dos problemas.

11.6.2- Revogar o certificado da AC-SRF.

11.6.3- Substituir e treinar pessoal.

11.7- Freqüência das Auditorias

O processo de auditoria é realizado nas seguintes situações e respectivas freqüências:

11.7.1- Credenciamento inicial – antes do credenciamento e do início de suas atividades no âmbito da ICP-Brasil.

11.7.2- Auditoria periódica anual – para manutenção do credenciamento.

11.7.3- Por determinação do CG ICP-Brasil ou da AC Raiz, a qualquer tempo.

12- GERENCIAMENTO DE RISCOS

12.1- Definição

Processo que visa a proteção dos serviços da AC-SRF, por meio da eliminação, redução ou transferência dos riscos, conforme seja economicamente (e estrategicamente) mais viável. Os seguintes pontos principais são identificados:

12.1.1.1- O que é protegido.

12.1.1.2- Análise de riscos (Contra quem ou contra o quê é protegido).

12.1.1.3- Avaliação de riscos (Análise da relação custo/benefício).

12.2- Fases Principais

O gerenciamento de riscos consiste das seguintes fases principais:

12.2.1 - Identificação dos recursos a serem protegidos – *hardware*, rede, *software*, dados, informações pessoais, documentação, suprimentos.

12.2.2- Identificação dos riscos (ameaças) - que podem ser naturais (tempestades, inundações), causadas por pessoas (ataques, furtos, vandalismos, erros ou negligências) ou de qualquer outro tipo (incêndios).

12.2.3- Análise dos riscos (vulnerabilidades e impactos) - identificar as vulnerabilidades e os impactos associados.

12.2.4- Avaliação dos riscos (probabilidade de ocorrência) - levantamento da probabilidade da ameaça vir a acontecer, estimando o valor do provável prejuízo. Esta avaliação pode ser feita com base em informações históricas ou em tabelas internacionais.

12.2.5- Tratamento dos riscos (medidas a serem adotadas) - maneira como lidar com as ameaças. As principais alternativas são: eliminar o risco, prevenir, limitar ou transferir as perdas ou aceitar o risco.

12.2.6- Monitoração da eficácia dos controles adotados para minimizar os riscos identificados.

12.2.7- Reavaliação periódica dos riscos em intervalos de tempo não superiores a 6 (seis) meses.

12.3- Riscos Relacionados às Entidades Integrantes da ICP-Brasil:

Os riscos avaliados para a AC-SRF compreendem, dentre outros, os seguintes:

Segmento	**Riscos**
Dados e Informação	Indisponibilidade, interrupção (perda), interceptação, modificação, fabricação, destruição
Pessoas	Omissão, erro, negligência, imprudência, imperícia, desídia, sabotagem, perda de conhecimento
Rede	*Hacker*, acesso desautorizado, interceptação, engenharia social, identidade forjada, reenvio de mensagem, violação de integridade, indisponibilidade ou recusa de serviço
Hardware	Indisponibilidade, interceptação (furto ou roubo), falha
Software e sistemas	Interrupção (apagamento), interceptação, modificação, desenvolvimento, falha
Recursos	Ciclo de vida dos certificados, gerenciamento das chaves

criptográficos	criptográficas, *hardware* criptográfico, algoritmos (desenvolvimento e utilização), material criptográfico.

12.4- Considerações Gerais

12.4.1- Os riscos que não puderem ser eliminados tem seus controles documentados e são levados ao conhecimento da AC-Raiz e do CG ICP-Brasil.

12.4.2- Um efetivo gerenciamento dos riscos permite decidir se o custo de prevenir um risco (medida de proteção) é mais alto que o custo das conseqüências do risco (impacto da perda).

12.4.3- Existe a participação e o envolvimento da alta administração da AC-SRF.

12.5- Implementação do Gerenciamento de Riscos

O gerenciamento de riscos, na AC-SRF, é conduzido de acordo com a metodologia proprietária e atendidos todos os tópicos relacionados.

13 - PLANO DE CONTINUIDADE DO NEGÓCIO

13.1- Definição

Plano cujo objetivo é manter em funcionamento os serviços e processos críticos da AC-SRF, na eventualidade da ocorrência de desastres, atentados, falhas e intempéries.

13.2- Diretrizes Gerais

13.2.1- Sistemas e dispositivos redundantes estão disponíveis para garantir a continuidade da operação dos serviços críticos de maneira oportuna;

13.2.2- A AC-SRF possui um Plano de Continuidade do Negócio que estabelece, no mínimo, o tratamento adequado dos seguintes eventos de segurança:

13.2.2.1- Comprometimento da chave privada da AC-SRF.

13.2.2.2- Invasão do sistema e da rede interna da AC-SRF.

13.2.2.3- Incidentes de segurança física e lógica.

13.2.2.4- Indisponibilidade da Infra-estrutura.

13.2.2.5- Fraudes ocorridas no registro do usuário, na emissão, expedição, distribuição, revogação e no gerenciamento de certificados.

13.2.3- Todo pessoal envolvido com o Plano de Continuidade do Negócio recebe um treinamento específico para poder enfrentar estes incidentes.

13.2.4- Um plano de ação de resposta a incidentes está estabelecido para a AC-SRF. Este plano prevê, no mínimo, o tratamento adequado dos seguintes eventos:

13.2.4.1- Comprometimento de controle de segurança em qualquer evento referenciado no Plano de Continuidade do Negócio.

13.2.4.2- Notificação à comunidade de usuários, se for o caso.

13.2.4.3- Revogação dos certificados afetados, se for o caso.

13.2.4.4- Procedimentos para interrupção ou suspensão de serviços e investigação.

13.2.4.5- Análise e monitoramento de trilhas de auditoria.

13.2.4.6- Relacionamento com o público e com meios de comunicação, se for o caso.