

AC CNDL RFB Declaração de Práticas de Certificação

Autor: CONFEDERAÇÃO NACIONAL DE DIRIGENTES E LOGISTAS – SPC BRASIL
Edição: 20/10/2014
Versão: 1.0

1. INTRODUÇÃO

1.1 Visão Geral

1.1.1. As informações contidas neste documento estabelecem os requisitos mínimos, obrigatoriamente observados pela Autoridade Certificadora CNDL, AC integrante da Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil na elaboração de suas Declarações de Práticas de Certificação - DPC. A DPC é o documento que descreve as práticas e os procedimentos empregados pela AC na execução de seus serviços.

1.1.2. A elaboração desta DPC foi disciplinada no DOC-ICP-05 do Comitê Gestor da ICP-Brasil que obrigatoriamente adota a mesma estrutura empregada no documento REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DE CERTIFICAÇÃO DAS AUTORIDADES CERTIFICADORAS DA ICP-BRASIL [10].

1.1.3. A AC CNDL para a Secretaria da Receita Federal do Brasil está no nível imediatamente subsequente ao da Autoridade Certificadora da Secretaria da Receita Federal do Brasil (AC-RFB).

1.1.4. Com relação aos tipos específicos de certificado emitidos pela AC CNDL para a Secretaria da Receita Federal do Brasil, referida a seguir como "AC CNDL RFB", devem ser consultadas as Políticas de Certificado da CNDL (<https://www.spcbrasil.org.br/produtos/produto/40-certificacaodigital>), que explicam como um tipo específico de certificado é gerado e administrado pela AC CNDL RFB e utilizado pela comunidade.

1.2 Identificação

Esta DECLARAÇÃO DE PRÁTICAS DE CERTIFICAÇÃO DA AUTORIDADE CERTIFICADORA CNDL referida a seguir simplesmente como "DPC-AC CNDL RFB" descreve as práticas e os procedimentos adotados pela AC CNDL RFB no âmbito da ICP-Brasil.

O OID da DPC-AC CNDL RFB é 2.16.76.1.1.65

1.3 Comunidade e Aplicabilidade

1.3.1 Autoridade Certificadora (AC)

1.3.1.1. Dados da Autoridade Certificadora

Esta DPC-AC CNDL RFB se refere à AC CNDL RFB (CNDL com sede na Rua. Leôncio de Carvalho nº 234, 5º Andar CEP: 04003-010 São Paulo – SP CNPJ 34.173.682/0003-18).

1.3.2 Autoridade de Registro (AR)

1.3.2.1. Dados da Autoridade 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 das Autoridades de Registro. As Autoridades de Registro vinculadas à AC CNDL RFB (AR Vinculadas) estão relacionados na página <https://www.spcbrasil.org.br/produtos/produto/40-certificacaodigital>.

A página <https://www.spcbrasil.org.br/produtos/produto/40-certificacaodigital> contém:

- relação de todas as AR credenciadas, com informações sobre as PCs que implementam;
- para cada AR credenciada, os endereços de todas as instalações técnicas, autorizadas pela AC Raiz a funcionar;
- para cada AR credenciada, relação de eventuais postos provisórios autorizados pela AC Raiz a funcionar, com data de criação e encerramento de atividades;
- relação de AR que tenham se descredenciado da cadeia da AC, com as respectivas datas do descredenciamento;
- relação de instalações técnicas de AR credenciadas que tenham deixado de operar, com as respectivas datas de encerramento das atividades;
- acordos operacionais celebrados pelas AR vinculadas com outras AR da ICP-Brasil se for o caso.

1.3.2.2. Atualização de Dados

A AC CNDL RFB mantém as informações acima sempre atualizadas.

AC CNDL RFB
Declaração de Práticas de Certificação

1.3.3 Prestador de Serviços de Suporte

1.3.3.1.Dados das PSS

Os Prestadores de Serviços de Suporte vinculados à AC CNDL RFB estão relacionados na página <https://www.spcbrasil.org.br/produtos/produto/40-certificacaodigital..>

1.3.3.2.PSS

PSS são entidades utilizadas pela AC CNDL RFB ou pelas AR para desempenhar atividades descritas nesta DPC ou na PC e se classificam em três categorias, conforme o tipo de atividade prestada:

- a) disponibilização de infraestrutura física e lógica;
- b) disponibilização de recursos humanos especializados; ou
- c) disponibilização de infraestrutura física e lógica e de recursos humanos especializados.

1.3.3.3. Atualização de Dados

A AC CNDL RFB mantém as informações acima sempre atualizadas.

1.3.4 Titulares de Certificado

Pessoa físicas ou jurídicas de direito público ou privado, nacionais ou internacionais, que atendam aos requisitos desta DPC-AC CNDL RFB e das Políticas de Certificado aplicáveis, podem ser Titulares de Certificado, para uso por pessoas físicas, pessoas jurídicas, em equipamentos ou aplicações.

NOTA 1: Sendo o titular do certificado pessoa jurídica, o representante legal da pessoa jurídica é designado como responsável pelo certificado e detentor da chave privada.

NOTA 2: Se tratando de certificado emitido para equipamento ou aplicação, o titular é a pessoa física ou jurídica solicitante do certificado, que deverá indicar o responsável pela chave privada.

1.3.5 Aplicabilidade

A AC CNDL RFB decide seguir as seguintes Políticas de Certificado Digital:

Política de Certificado	Nome conhecido	OID
Política de Certificado de Assinatura Digital tipo A1 da AC CNDL RFB	PC AC CNDL RFB A1	2.16.76.1.2.1.52
Política de Certificado de Assinatura Digital tipo A3 da AC CNDL RFB	PC AC CNDL RFB A3	2.16.76.1.2.3.49

Nas PCs correspondentes estão relacionadas as aplicações para as quais são adequados os certificados emitidos pela AC CNDL RFB e, quando cabíveis, as aplicações para as quais existam restrições ou proibições para o uso desses certificados.

1.4 Dados de Contato

Dúvidas decorrentes da leitura desta DPC-AC CNDL RFB e que não sejam respondidas mediante a leitura da página <https://www.spcbrasil.org.br/produtos/produto/40-certificacaodigital> podem ser esclarecidas contactando:

AR CNDL RFB
Rua Leôncio de Carvalho, Nº234 - 5º andar - Paraíso
CEP: 04003-010
São Paulo - SP
Telefones: (55 11) 3549- 6800
Pessoa para contato: Marta Santos
E-mail: compliance.cert@spcbrasil.org.br

2. DISPOSIÇÕES GERAIS

2.1 Obrigações

Nos itens a seguir estão descritas as obrigações gerais das entidades envolvidas.

2.1.1 Obrigações da AC CNDL

As obrigações da AC CNDL RFB são as abaixo relacionadas:

- a) operar de acordo com esta DPC-AC CNDL RFB e com as PCs implementadas;
- b) gerar e gerenciar o seu par de chaves criptográficas;
- c) assegurar a proteção de suas chaves privadas;
- d) notificar a AC RFB e a AC RAIZ quando ocorrer comprometimento de sua chave privada e solicitar a imediata revogação desse certificado;
- e) notificar os seus usuários quando ocorrer: suspeita de comprometimento de sua chave, emissão de novo par de chaves e correspondente certificado, ou encerramento de suas atividades;
- f) distribuir o seu próprio certificado;
- g) emitir, expedir e distribuir os certificados de usuários finais;

AC CNDL RFB
Declaração de Práticas de Certificação

- h) informar a emissão do certificado ao respectivo solicitante;
- i) revogar os certificados por ela emitidos;
- j) emitir, gerenciar e publicar suas Listas de Certificados Revogados (LCR) e, quando aplicável, disponibilizar consulta *on-line* de situação do certificado (OCSP - *On-line Certificate Status Protocol*);
- k) publicar em sua página web, sua DPC-AC CNDL RFB e as PCs aprovadas que implementadas;
- l) publicar, em sua página web, as informações definidas no item 2.6.1.2 deste documento;
- m) publicar, em página web, informações sobre o descredenciamento de AR bem como sobre extinção de instalação técnica;
- n) utilizar protocolo de comunicação seguro ao disponibilizar serviços para os solicitantes ou usuários de certificados digitais via web;
- o) identificar e registrar todas as ações executadas, conforme as normas, práticas e regras estabelecidas pelo CG da ICP-Brasil;
- p) atender à Instrução Normativa no. 222, de 11 de outubro de 2002, nos seus artigos 10 e 11;
- q) adotar as medidas de segurança e controle previstas na DPC-AC CNDL RFB, nas PCs implementadas e Política de Segurança implementada, envolvendo seus processos, procedimentos e atividades, observadas as normas, critérios, práticas e procedimentos da ICP-Brasil e da Secretaria da Receita Federal do Brasil;
- r) manter a conformidade dos seus processos, procedimentos e atividades com as normas, práticas e regras da ICP-Brasil e da Secretaria da Receita Federal do Brasil com a legislação vigente;
- s) manter e garantir a integridade, o sigilo e a segurança da informação por ela tratada;
- t) manter e testar regularmente seu Plano de Continuidade do Negócio;
- u) manter contrato de seguro de cobertura de responsabilidade civil decorrente das atividades de certificação digital e de registro, com cobertura suficiente e compatível com o risco dessas atividades, e exigir sua manutenção pelas AC de nível subsequente ao seu, quando estas estiverem obrigadas a contratá-lo, de acordo com as normas do Comitê Gestor da ICP-Brasil;
- v) informar às terceiras partes e titulares de certificado acerca das garantias, coberturas, condicionantes e limitações estipuladas pela apólice de seguro de responsabilidade civil contratada pela AC CNDL RFB;
- w) informar à AC Raiz, mensalmente, a quantidade de certificados digitais emitidos; e
- x) não emitir certificado com prazo de validade que se estenda além do prazo de validade de seu próprio certificado.

2.1.2 Obrigações das Autoridades de Registro

As obrigações das AR Vinculadas são as abaixo relacionadas:

- a) receber solicitações de emissão ou de revogação de certificados;
- b) confirmar a identidade do solicitante e a validade da solicitação;
- c) encaminhar a solicitação de emissão ou de revogação de certificado à AC CNDL RFB utilizando protocolo de comunicação seguro, conforme padrão definido no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP-BRASIL [1];
- d) informar aos respectivos titulares a emissão ou a revogação de seus certificados;
- e) disponibilizar os certificados emitidos pela AC CNDL RFB aos seus respectivos solicitantes;
- f) identificar e registrar todas as ações executadas, conforme as normas, práticas e regras estabelecidas pelo CG da ICP-Brasil;
- g) manter a conformidade dos seus processos, procedimentos e atividades com as normas, critérios, práticas e regras estabelecidas pela AC CNDL RFB e pela ICP-Brasil, em especial com o contido no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP-BRASIL [1];
- h) manter e garantir a segurança da informação por elas tratada, de acordo com o estabelecido nas normas, critérios, práticas e procedimentos da ICP-Brasil;
- i) manter e testar anualmente seu Plano de Continuidade do Negócio - PCN;
- j) proceder com o reconhecimento das assinaturas e da validade dos documentos apresentados na forma dos itens 3.1.9, 3.1.10 e 3.1.11;
- k) garantir que todas as aprovações de solicitação de certificados sejam realizadas em instalações técnicas autorizadas a funcionar como AR vinculadas credenciadas.

2.1.3 Obrigações do Titular do Certificado

Constituem-se obrigações do titular de certificado emitido pela AC CNDL RFB:

- a) fornecer, de forma completa e precisa, todas as informações necessárias para sua identificação;
- b) garantir a proteção e o sigilo de suas chaves privadas, senhas e dispositivos criptográficos;
- c) utilizar os seus certificados e chaves privadas de forma apropriada, conforme o previsto na PC correspondente;
- d) conhecer os seus direitos e obrigações, contemplados pela DPC-AC CNDL RFB, pela PC correspondente e por outros documentos aplicáveis da ICP-Brasil;
- e) informar à AC CNDL RFB qualquer comprometimento de sua chave privada e solicitar a imediata revogação do certificado correspondente.
- f) assumir a responsabilidade pelo custo do processo de emissão do certificado.
- g) responsabilizar-se por todos os atos praticados perante a RFB utilizando o referido certificado e sua correspondente chave privada.
- h) utilizar obrigatoriamente senha para proteção da chave privativa do certificado e-CPF e e-CNPJ.
- i) obedecer estritamente a esta DPC-AC CNDL RFB e às PC aplicáveis, bem como respeitar a legislação aplicável, incluindo as regras definidas pelo CG da ICP-Brasil e as obrigações contratuais assumidas perante a AC CNDL RFB e à AR vinculada.

AC CNDL RFB
Declaração de Práticas de Certificação

NOTA: Em se tratando 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)

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

2.1.4.2. Constituem direitos da terceira parte:

- a) recusar a utilização do certificado para fins diversos dos previstos na PC correspondente;
- b) verificar, a qualquer tempo, a validade do certificado. Um certificado emitido por AC integrante da ICP-Brasil é considerado válido quando:
 - i. não constar da LCR da AC emitente;
 - ii. não estiver expirado; e
 - iii. puder ser verificado com o uso de certificado válido da AC emitente.

2.1.4.3. O não exercício desses direitos não afasta a responsabilidade da AC CNDL RFB e do titular do certificado.

2.1.5 Obrigações do Repositório da AC CNDL RFB

- a) disponibilizar, logo após a sua emissão, os certificados emitidos pela AC CNDL RFB e a sua LCR;
- b) estar disponível para consulta durante 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana; e
- c) implementar os recursos necessários para a garantia da segurança dos dados nele armazenados.

2.2 Responsabilidades

2.2.1 Responsabilidades da AC CNDL RFB

2.2.1.1. A AC CNDL RFB responde pelos danos a que der causa.

2.2.1.2. A AC CNDL RFB responde solidariamente pelos atos das entidades de sua cadeia de certificação: AR e PSS.

2.2.2 Responsabilidades da AR Vinculadas

As AR Vinculadas serão responsáveis pelos danos a que derem causa.

2.3 Responsabilidade Financeira

2.3.1 Indenizações devidas pela terceira parte (Relying Parties)

A terceira parte (Relying Party) não é responsável perante a AC CNDL RFB e AR a ela vinculada, exceto na hipótese de prática de ato ilícito. Essa terceira parte deverá indenizar a AC CNDL RFB e/ou os titulares de seus certificados pelos danos a que der causa em decorrência de omissão ou ação não conforme com a legislação aplicável.

2.3.2 Relações Fiduciárias

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

2.3.3 Processos Administrativos

O titular do certificado que sofrer perdas e danos decorrentes do uso do certificado digital terá o direito de comunicar à AC CNDL RFB que deseja a indenização prevista no documento Política de Garantia (<https://www.spcbrasil.org.br/produtos/produto/40-certificacaodigital>) para tais casos, observadas as seguintes condições:

- a) nos casos de perdas e danos decorrentes de comprometimento da chave privada da AC CNDL RFB, tal comprometimento deverá ter sido comprovado por perícia realizada por perito especializado e independente;
- b) nos casos de erro na identificação, o titular do certificado não poderá requerer qualquer indenização quando os dados constantes no certificado corresponderem aos dados fornecidos por esse titular à AC CNDL RFB ou à AR vinculada;
- c) nos casos de erro na transcrição, o titular do certificado não poderá requerer qualquer indenização quando houver aceito o certificado.

2.4 Interpretação e Execução

2.4.1 Legislação

Esta DPC-AC CNDL RFB 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, a Portaria SRF/Cotec no. 64, de 11 de outubro de 2002, ao anexo I da Portaria RFB/Cotec no. 061, de 04 de setembro de 2008, bem como as Resoluções do CG da ICP-Brasil e da Secretaria da Receita Federal do Brasil.

AC CNDL RFB Declaração de Práticas de Certificação

2.4.2 Forma de interpretação e notificação

2.4.2.1. Na eventual hipótese desta DPC-AC CNDL RFB ou alguma de suas disposições venha a ser considerada ou declarada inválida, ilegal ou não aplicável por lei, a AC CNDL RFB tomará de imediato as medidas necessárias para adequar esta DPC-AC CNDL RFB ou a disposição em questão às exigências legais, sem prejuízo para o titular do certificado.

2.4.2.2. As notificações, solicitações ou quaisquer outras comunicações necessárias, sujeitas às práticas descritas nesta DPC-AC CNDL RFB, serão realizadas pela AC CNDL RFB e pelas AR vinculadas por e-mail a ser enviado ao endereço eletrônico fornecido pelo solicitante no formulário de solicitação. O e-mail será considerado como recebido quando enviado a esse endereço. compliance.cert@spcbrasil.org.br.

2.4.3 Procedimentos de solução de disputa

2.4.3.1. Em caso de conflito entre esta DPC-AC CNDL RFB e outras declarações, políticas, planos, acordos, contratos ou documentos, esta DPC-AC CNDL RFB prevalecerá.

2.4.3.2. Esta DPC-AC CNDL RFB não prevalecerá sobre as normas, critérios, práticas e procedimentos da ICP-Brasil e da Secretaria da Receita Federal do Brasil.

2.4.3.3. Os casos omissos deverão ser encaminhados para apreciação da AC Raiz.

2.5 Tarifas de Serviço

Pelo certificado emitido será cobrado o valor estabelecido contratualmente.

2.5.1 Tarifas de emissão e renovação de certificados

Pela emissão e renovação do certificado será cobrado o valor estabelecido contratualmente.

2.5.2 Tarifas de acesso ao certificado

Pelo acesso ao certificado será cobrado o valor estabelecido contratualmente.

2.5.3 Tarifas de revogação ou de acesso a informação de status

Pela revogação ou acesso a informação de status será cobrado o valor estabelecido contratualmente.

2.5.4 Tarifas para outros serviços

Pelos demais serviços serão cobrados o valor estabelecido contratualmente.

2.5.5 Política de reembolso

Caso haja a necessidade do certificado ser revogado por motivo de comprometimento da chave privada da AC CNDL RFB ou da mídia armazenadora da chave privada da AC CNDL RFB, ou ainda quando constatada a emissão imprópria ou defeituosa, imputável à AC CNDL RFB, será reembolsado ao solicitante o preço pago pelo certificado, exceto em caso de emissão de outro certificado em substituição, sem cobrar pelo mesmo.

2.6 Publicação e Repositório

2.6.1 Publicação de informação da AC CNDL RFB

2.6.1.1. A AC CNDL RFB publica e mantém disponível em seu site (<https://www.spcbrasil.org.br/produtos/produto/40-certificacaodigital>), informações com disponibilidade mínima de 99,5% (noventa e nove vírgula cinco por cento) do mês, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.

2.6.1.2. As seguintes informações são publicadas pela AC CNDL RFB em página web:

- Seu próprio certificado;
- Suas LCR;
- Sua DPC-AC CNDL RFB;
- As PCs que implementadas;
- O certificado da AC RFB, também está disponível no site da AC-RFB (<http://hom.receita.fazenda.gov.br/acsr/dpcacsr/pdf>);
- Uma relação, regularmente atualizada, contendo as ARs vinculadas e seus respectivos endereços de instalações técnicas em funcionamento;
- Uma relação, regularmente atualizada, das ARs vinculadas que tenham celebrado acordos operacionais com outras ARs da ICP-Brasil, contendo informações sobre os pontos do acordo que sejam de interesse dos titulares e solicitantes de certificado; e
- Uma relação, regularmente atualizada, dos PSSs vinculados.

2.6.2 Frequência de publicação

A AC CNDL RFB atualiza as informações acima tão logo sejam geradas, de modo a assegurar a disponibilização sempre atualizada de seus conteúdos.

AC CNDL RFB Declaração de Práticas de Certificação

2.6.3 Controles de acesso

Somente a AC CNDL RFB, por seus funcionários competentes e designados especialmente para esse fim, pode alterar as informações constantes nesta DPC-AC CNDL RFB e nas PCs que implementa, após haver obtido a competente autorização do CG da ICP-Brasil.

Somente a AC CNDL RFB, por seus funcionários competentes e designados especialmente para esse fim, pode efetuar as necessárias atualizações de suas LCRs.

O certificado da AC CNDL RFB e os certificados emitidos pela AC CNDL RFB não podem ser modificados. Caso se faça necessário modificar os dados contidos nos mesmos, será necessária a revogação dos certificados.

Não há restrições para o acesso da leitura desta DPC-AC CNDL RFB, das PCs e das LCRs.

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

2.6.4 Repositórios

Os repositórios da AC CNDL RFB são acessados, utilizando o protocolo de acesso http, através da página <https://www.spcbrasil.org.br/produtos/produto/40-certificacaodigital>.

Os repositórios estão disponíveis em no mínimo 99,5% (noventa e nove vírgula cinco por cento) do mês, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.

Os repositórios obedecem aos requisitos de segurança estabelecidos no item 5 desta DPC.

2.7 Fiscalização e Auditoria de Conformidade

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

2.7.2. As fiscalizações das entidades integrantes da ICP-Brasil são realizadas pela AC Raiz, por meio de servidores de seu quadro próprio, a qualquer tempo, sem aviso prévio, observado o disposto no documento CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [2].

2.7.3. Com exceção da auditoria da própria AC Raiz, que é de responsabilidade do CG da ICP-Brasil, as auditorias das entidades integrantes da ICP-Brasil são realizadas pela AC Raiz, por meio de servidores de seu quadro próprio, ou por terceiros por ela autorizado, observado o disposto no documento CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL [3].

2.7.4. A AC CNDL RFB recebeu auditoria prévia da AC Raiz para fins de credenciamento na ICP-Brasil e é auditada anualmente, para fins de manutenção do credenciamento, com base no disposto no documento CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL [3]. Esse documento trata do objetivo, frequência e abrangência das auditorias, da identidade e qualificação do auditor e demais temas correlacionados.

2.7.5.A AC CNDL RFB e as entidades da ICP-Brasil a ela diretamente vinculadas –AR Vinculadas e PSS, receberam auditoria prévia, para fins de credenciamento, sendo a AC CNDL RFB responsável pela realização de auditorias anuais nessas entidades, para fins de manutenção de credenciamento, conforme disposto no documento citado no parágrafo anterior.

2.8 Sigilo

2.8.1 Disposições Gerais

2.8.1.1.A chave privada de assinatura digital da AC CNDL RFB foi gerada e é mantida pela própria AC CNDL RFB, que assegura o seu sigilo. A divulgação ou utilização indevida da chave privada de assinatura pela AC CNDL RFB é de sua inteira responsabilidade.

2.8.1.2 Os titulares de certificados emitidos pela AC CNDL RFB têm as atribuições de geração, manutenção e sigilo de suas respectivas chaves privadas. Além, disso, responsabilizam-se pela divulgação ou utilização indevidas dessas mesmas chaves.

2.8.1.3.No caso de certificados de sigilo emitidos pela AC CNDL RFB, as responsabilidades de manutenção e de garantia do sigilo das respectivas chaves privadas cabe aos titulares de certificados ou os responsáveis pelo uso de certificados emitidos para pessoas jurídicas, equipamentos ou aplicações.

2.8.2 Tipos de informações sigilosas

2.8.2.1. Toda e qualquer informação coletada, gerada, transmitida e mantida pela AC CNDL RFB são informações consideradas sigilosas, e de acordo com as normas, critérios, práticas e procedimentos da ICP-Brasil.

AC CNDL RFB Declaração de Práticas de Certificação

2.8.2.2. Como princípio geral, nenhum documento, informação ou registro fornecido à AC CNDL RFB ou à AR Vinculada deve ser divulgado.

2.8.3 Tipos de informações não sigilosas

Não são considerados como informações sigilosas pela AC CNDL RFB e pela AR Vinculada:

- a) os certificados e as LCRs emitidos pela AC CNDL RFB,
- b) as informações corporativas ou pessoais que façam parte de certificados ou de diretórios públicos;
- c) as PCs implementadas pela AC CNDL RFB;
- d) esta DPC-AC CNDL RFB;
- e) as versões públicas de Políticas de Segurança;
- f) a conclusão dos relatórios de auditoria.

A AC CNDL RFB e a AR Vinculada tratam como confidenciais os dados fornecidos pelo solicitante que não constem no certificado. Contudo, tais dados não são considerados confidenciais quando:

- a) estejam na posse legítima da AC CNDL RFB ou da AR Vinculada antes de seu fornecimento pelo solicitante ou o solicitante autorize formalmente a sua divulgação;
- b) posteriormente ao seu fornecimento pelo solicitante, sejam obtidos ou possam ter sido obtidos legalmente de terceiro (s) com direitos legítimos para divulgação sua sem quaisquer restrições para tal;
- c) sejam requisitados por determinação judicial ou governamental, desde que a AC CNDL RFB ou a AR Vinculada comunique previamente, se possível e de imediato ao solicitante, a existência de tal determinação;

Os motivos que justificaram a não emissão de um certificado são mantidos confidenciais pela AC CNDL RFB e pela AR Vinculada, exceto na hipótese da alínea "c" acima, ou quando o solicitante requerer ou autorizar expressamente a sua divulgação a terceiros.

2.8.4 Divulgação de informação de revogação ou suspensão de certificado

2.8.4.1. A AC CNDL RFB disponibiliza permanentemente em seu site <https://www.spcbrasil.org.br/produtos/produto/40-certificacaodigital>, com atualização definida nas correspondentes PC, relação de certificados por ela emitidos que foram revogados.

2.8.4.2. Os motivos que justificaram a revogação são sempre informados ao titular ou responsável pelo certificado e mantidos confidenciais pela AC CNDL RFB e pela AR Vinculada, exceto quando o titular do certificado revogado solicitar ou autorizar expressamente a sua divulgação a terceiros, ou quando tais motivos sejam requisitados por determinação judicial ou governamental, caso em que a AC CNDL RFB ou a AR Vinculada, se estiver obrigada a divulgá-los, comunicará previamente ao titular do certificado a existência de tal determinação.

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

2.8.5 Quebra de sigilo por motivos legais

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

2.8.6 Informações a terceiros

A AC CNDL RFB não fornece nem fornecerá a terceiros nenhum documento, informação ou registro sob sua guarda, exceto nas hipóteses mencionadas nesta DPC-AC CNDL RFB.

2.8.7 Divulgação por solicitação do titular

2.8.7.1. 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 CNDL RFB e da AR Vinculada em razão da solicitação e da emissão do certificado digital. O titular do certificado pode autorizar a AC CNDL RFB ou a AR Vinculada a divulgar tais informações a terceiros ou unicamente às pessoas que indique nessa autorização.

2.8.7.2. Qualquer liberação de informação pela a AC CNDL RFB ou a AR Vinculada somente será permitida mediante autorização formal do titular do certificado. Essa autorização pode ser feita no ato da solicitação do certificado, no próprio formulário de solicitação, ou posteriormente, por e-mail ou outro documento legalmente aceito.

2.8.8 Outras circunstâncias de divulgação de informação

A AC CNDL RFB e a AR Vinculada podem divulgar informações que não sejam consideradas sigilosas pelo fato de:

- a) estarem na posse legítima da AC CNDL RFB ou da AR Vinculada antes de seu fornecimento pelo solicitante ou titular do certificado ou o solicitante ou titular do certificado haver 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;
- c) terem sido requisitadas por determinação judicial ou governamental, obrigando-se a AC CNDL RFB, 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 a 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 CNDL RFB ou de AR vinculadas para o solicitante.

3. IDENTIFICAÇÃO E AUTENTICAÇÃO

3.1 Registro Inicial

3.1.1 Disposições Gerais

3.1.1.1. As ARs vinculadas à AC CNDL RFB utilizam os seguintes requisitos e procedimentos para realização dos seguintes processos:

a) Validação da solicitação de certificado – compreende as etapas abaixo, realizadas mediante a presença física do interessado, com base nos documentos de identificação citados nos itens 3.1.9, 3.1.10 e 3.1.11:

- i. confirmação da identidade de um indivíduo: comprovação de que a pessoa que se apresenta como titular do certificado de pessoa física é realmente aquela cujos dados constam na documentação apresentada, vedada qualquer espécie de procuração para tal fim. No caso de pessoa jurídica, comprovar que a pessoa física que se apresenta como responsável pelo uso do certificado ou como representante legal é realmente aquela cujos dados constam na documentação apresentada, admitida a procuração apenas se o ato constitutivo prever expressamente tal possibilidade, devendo-se, para tanto, revestir-se da forma pública com poderes específicos para atuar perante a ICP-Brasil;
- ii. confirmação da identidade de uma organização: comprovação de que os documentos apresentados referem-se efetivamente à pessoa jurídica titular do certificado e de que a pessoa que se apresenta como representante legal da pessoa jurídica realmente possui tal atribuição;
- iii. emissão do certificado: conferência dos dados da solicitação de certificado com os constantes dos documentos apresentados e liberação da emissão do certificado no sistema da AC.

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

- i. por agente de registro distinto do que executou a etapa de validação;
- ii. em uma das instalações técnicas da AR devidamente autorizadas a funcionar pela AC Raiz;
- iii. somente após o recebimento, na instalação técnica da AR, de cópia dos da documentação apresentada na etapa de validação;
- iv. antes do início da validade do certificado, devendo esse ser revogado automaticamente caso a verificação não tenha ocorrido até o início de sua validade.

3.1.1.2. O processo de validação ao ser realizado pelo agente de registro fora do ambiente físico da AR, deverá utilizar ambiente computacional auditável e devidamente registrado no inventário de hardware e softwares da AR.

3.1.1.3. Todas as etapas dos processos de validação e verificação da solicitação de certificado devem ser registradas e assinadas digitalmente pelos executantes, na solução de certificação disponibilizada pela AC CNDL RFB, com a utilização de certificado digital ICP-Brasil no mínimo do tipo A3. Tais registros devem ser feitos de forma a permitir a reconstituição completa dos processos executados, para fins de auditoria.

3.1.1.4. Deve ser mantido arquivo com as cópias de todos os documentos utilizados para confirmação da identidade de uma organização e/ou de um indivíduo. Tais cópias poderão ser mantidas em papel ou em forma digitalizada, observadas as condições definidas no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP-BRASIL [1].

3.1.1.5. Nos casos de certificado digital emitido para Servidores do Serviço Exterior Brasileiro, em missão permanente no exterior, assim caracterizados conforme a Lei nº 11.440, de 29 de dezembro de 2006, se houver impedimentos para a identificação conforme o disposto no subitem 3.1.1.1 deste anexo, é facultada a remessa da documentação pela mala diplomática e a realização da identificação por outros meios seguros, a serem definidos e aprovados pela AC-Raiz da ICP-Brasil.

3.1.2 Tipos de nomes

3.1.2.1. A AC CNDL RFB emite certificados com nomes que permitam a identificação unívoca. Para isso utiliza o "distinguished name" do padrão ITU X.500, endereços de correio eletrônico ou endereços de página Web (URL). O certificado emitido para pessoa jurídica inclui o nome da pessoa física responsável. Para todos os efeitos legais, os certificados e as respectivas chaves de assinatura são de titularidade do responsável constante do certificado.

3.1.2.2. Item não aplicável.

3.1.3 Necessidade de nomes significativos

A AC CNDL RFB faz uso de nomes significativos que possibilitam determinar a identidade da pessoa ou organização a que se referem para a identificação dos titulares dos certificados emitidos pela AC CNDL RFB.

Para certificados de pessoa física (e-CPF), o campo Common Name é composto do nome do Titular do Certificado, conforme consta no Cadastro de Pessoa Física.

Para os certificados de pessoa jurídica (e-CNPJ), o campo Common Name é composto do nome empresarial da pessoa jurídica, conforme consta no Cadastro Nacional de Pessoa Jurídica.

3.1.4 Regras para interpretação de vários tipos de nomes

Item não aplicável.

3.1.5 Unicidade de nomes

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

Para assegurar a unicidade do campo, no certificado de pessoa física (e-CPF) é incluído o número do CPF após o nome do titular do certificado e, no certificado de pessoa jurídica (e-CNPJ) é incluído o número do CNPJ.

3.1.6 Procedimento para resolver disputa de nomes

No âmbito da AC CNDL RFB não há disputa decorrente de igualdade de nomes entre solicitantes de certificados pois o nome do Titular do Certificado será formado a partir do nome constante dos cadastros da RFB, CPF ou CNPJ para certificados de pessoa física ou jurídica respectivamente, acrescido do número de inscrição nestes cadastros. Este procedimento garante a unicidade de todos os nomes no âmbito da AC CNDL RFB.

3.1.7 Reconhecimento, autenticação e papel de marcas registradas

Tais procedimentos são analisados com base na legislação em vigor.

3.1.8 Método para comprovar a posse de chave privada

A confirmação de 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, relativos a POP (*Proof of Possession*).

3.1.9 Autenticação da identidade de um indivíduo

A confirmação da identidade é realizada mediante a presença física do interessado, com base em documentos de identificação legalmente aceitos.

3.1.9.1. Documentos para efeitos de identificação de um indivíduo

Durante a solicitação do certificado modelo e-CPF é realizada consulta da situação cadastral do solicitante perante o CPF, conforme art. 6º da Instrução Normativa SRF Nº 222. Se o CPF informado for inexistente ou se a pessoa física apresentar a condição de cancelada ou nula, a solicitação não será enviada à AC CNDL RFB.

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

- Cédula de Identidade ou Passaporte, se brasileiro;
- Carteira Nacional de Estrangeiro – CNE, se estrangeiro domiciliado no Brasil;
- Passaporte, se estrangeiro não domiciliado no Brasil;
- caso os documentos acima tenham sido expedidos há mais de 5 (cinco) anos ou não possuam fotografia, uma foto colorida recente ou documento de identidade com foto colorida, emitido há no máximo 5 (cinco) anos da data da validação presencial;
- comprovante de residência ou domicílio, emitido há no máximo 3 (três) meses da data da validação presencial.

NOTA 1: Entende-se como cédula de identidade os documentos emitidos pelas Secretarias de Segurança Pública bem como os que, por força de lei, equivalem a documento de identidade em todo o território nacional, desde que contenham fotografia.

NOTA 2: Entende-se como comprovante de residência ou de domicílio contas de concessionárias de serviços públicos, extratos bancários ou contrato de aluguel onde conste o nome do titular; na falta desses, declaração emitida pelo titular ou seu empregador.

AC CNDL RFB
Declaração de Práticas de Certificação

NOTA 3: A emissão de certificados em nome dos absolutamente incapazes e dos relativamente incapazes observará o disposto na lei vigente.

NOTA 4: Para a identificação de indivíduo na emissão de certificado que integra o Documento RIC, deverá ser observado o disposto no item 3.1.1.6.

NOTA 5: Caso não haja suficiente clareza no documento apresentado, a AR deve solicitar outro documento, preferencialmente a CNH - Carteira Nacional de Habilitação ou o Passaporte Brasileiro.

NOTA 6: Deverão ser consultadas as bases de dados dos órgãos emissores da Carteira Nacional de Habilitação, e outras verificações documentais expressas no item 7 do documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICPBRASIL [1].

NOTA 7: Caso haja divergência dos dados constantes do documento de identidade, a emissão do certificado digital deverá ser suspensa e o solicitante orientado a regularizar sua situação junto ao órgão responsável.

NOTA 8: É obrigatória a realização da consulta do CPF do Titular do Certificado Digital e demais sócios (em caso de emissão para organização) no site da Receita Federal, por meio do link: <http://www.receita.fazenda.gov.br/aplicacoes/atcta/cpf/consultapublica.asp>.

3.1.9.2. Informações contidas no certificado emitido para um indivíduo

3.1.9.2.1. É obrigatório o preenchimento dos seguintes campos do certificado de uma pessoa física com as informações constantes nos documentos apresentados:

- a) Cadastro de Pessoa Física (CPF);
- b) nome completo, sem abreviações;
- c) data de nascimento.

3.1.9.2.2. Cada PC pode definir como obrigatório o preenchimento de outros campos ou o titular do certificado, a seu critério e mediante declaração expressa no termo de titularidade, poderá solicitar o preenchimento de campos do certificado com as informações constantes nos seguintes documentos:

- a) Cadastro de Pessoa Física (CPF)
- b) número de Identificação Social - NIS (PIS, PASEP ou CI);
- c) número do Registro Geral - RG do titular e órgão expedidor;
- d) número do Cadastro Específico do INSS (CEI);
- e) número do Título de Eleitor; Zona Eleitoral; Seção; Município e UF do Título de Eleitor;
- f) número de habilitação ou identificação profissional emitido por conselho de classe ou órgão competente.

3.1.9.2.3. Para tanto, o titular deverá apresentar a documentação respectiva, caso a caso, em sua versão original. Deve ser mantido arquivo com as cópias de todos os documentos utilizados.

NOTA 1: É permitida a substituição dos documentos elencados acima por documento único, desde que este seja oficial e contenha as informações constantes daqueles.

NOTA 2: O cartão CPF poderá ser substituído por consulta à página da Receita Federal do Brasil, devendo a cópia da mesma ser arquivada junto à documentação, para fins de auditoria.

3.1.10 Autenticação da identidade de uma organização

3.1.10.1. Disposições Gerais

3.1.10.1.1. Os métodos empregados para confirmação da identidade de pessoa jurídica é feita mediante consulta as bases de dados da RFB.

3.1.10.1.2. Quando se tratar de titular do certificado pessoa jurídica, será designado o representante legal da pessoa jurídica como responsável pelo certificado, que será o detentor da chave privada.

3.1.10.1.3. A confirmação da identidade da organização e das pessoas físicas deverá ser feita nos seguintes termos:

- a) Apresentação do rol de documentos elencados no item 3.1.10.2;
- b) Apresentação do rol de documentos elencados no item 3.1.9.1 do(s) representante(s) legal (is) da pessoa jurídica e do responsável pelo uso do certificado; e
- c) Presença física dos representantes legais e do responsável pelo uso do certificado, e assinatura do termo de titularidade de que trata o item 4.1.1.

AC CNDL RFB
Declaração de Práticas de Certificação

3.1.10.2. Documentos para efeitos de identificação de uma organização

Durante a solicitação de certificado e-CNPJ é realizada consulta à situação cadastral do CNPJ junto ao cadastro da RFB. Se o CNPJ estiver INAPTO, CANCELADO, BAIXADO, NULO ou SUSPENSO – situações que impedem o fornecimento do certificado - a solicitação não é enviada para a AC-CNDL RFB.

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

- a) Relativos a sua habilitação jurídica:
 - i. se pessoa jurídica criada ou autorizada a sua criação por lei, cópia do ato constitutivo e CNPJ;
 - ii. se entidade privada:
 - 1. ato constitutivo, devidamente registrado no órgão competente; e
 - 2. documentos da eleição de seus administradores, quando aplicável;
- b) Relativos a sua habilitação fiscal:
 - i. prova de inscrição no Cadastro Nacional de Pessoas Jurídicas – CNPJ; ou
 - ii. prova de inscrição no Cadastro Específico do INSS – CEI.

3.1.10.3. Informações contidas no certificado emitido para uma organização

3.1.10.3.1. O preenchimento dos seguintes campos do certificado de uma pessoa jurídica, são obrigatórios, com as informações constantes nos documentos apresentados:

- a) nome empresarial constante do CNPJ (Cadastro Nacional de Pessoa Jurídica), sem abreviações;
- b) Cadastro Nacional de Pessoa Jurídica (CNPJ);
- c) nome completo do responsável pelo certificado, sem abreviações;
- d) data de nascimento do responsável pelo certificado.

3.1.10.3.2. Toda PC pode definir a obrigatoriedade do preenchimento de outros campos ou o responsável pelo certificado, a seu critério e mediante declaração expressa no termo de titularidade, poderá também solicitar o preenchimento de campos do certificado suas informações pessoais, conforme item 3.1.9.2.

3.1.11. Autenticação da identidade de equipamento, aplicação ou código

3.1.11.1. Disposições Gerais

3.1.11.1.1. Item não aplicável.

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

3.2.1. os métodos de identificação do solicitante utilizados pela AC CNDL RFB para a geração de novo par de chaves, e de seu correspondente certificado, antes da expiração de um certificado vigente.

3.2.2. Tal processo será conduzido segundo uma das seguintes possibilidades:

- a) adoção dos mesmos requisitos e procedimentos exigidos para a solicitação do certificado;
- b) solicitação por meio eletrônico, assinada digitalmente com o uso de certificado vigente que seja pelo menos do mesmo nível de segurança, limitada a 1 (uma) ocorrência sucessiva;
- c) Em caso de pessoa jurídica, qualquer alteração em sua constituição e funcionamento deverá constar do processo de renovação.

3.2.3. Item não aplicável.

3.3 Geração de novo par de chaves após revogação ou expiração

3.3.1. Após a revogação ou expiração do certificado, o solicitante pode requerer um novo certificado, enviando à AC CNDL, ou AR Vinculada uma solicitação, na forma, condições e prazo estabelecidos como a solicitação inicial de um certificado.

3.3.2. Item não aplicável.

3.4 Solicitação de Revogação

A solicitação de revogação de certificado é feita através de formulário específico, permitindo a identificação inequívoca do solicitante. A confirmação da identidade do solicitante é feita com base na confrontação de dados entre a solicitação de revogação e a solicitação de emissão.

4. REQUISITOS OPERACIONAIS

4.1 Solicitação de Certificado

4.1.1. A solicitação de emissão de um Certificado Digital CNDL é feita mediante o preenchimento de formulário colocado à disposição do solicitante pela AR Vinculada. Toda referência a formulário deverá ser entendida também como referência a outras formas que a AR Vinculada possa vir a adotar.

Dentre os requisitos e procedimentos operacionais estabelecidos pela AC CNDL RFB para as solicitações de emissão de certificado, estão:

- a) a comprovação de atributos de identificação constantes do certificado, conforme item 3.1;
- b) 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, equivalentes a de um certificado de tipo A3; e
- c) um termo de titularidade assinado pelo titular do certificado e um termo de responsabilidade assinado pelo responsável pelo uso do certificado, elaborados conforme o documento MODELO DE TERMO DE TITULARIDADE [4].

4.1.2. Item não aplicável.

4.1.3. Item não aplicável.

4.1.4. Item não aplicável.

4.2 Emissão de Certificado

4.2.1. Após a validação da solicitação do certificado, de que trata o item 3.1.1.1, a AC CNDL RFB procede à emissão do certificado.

O certificado emitido é inserido na relação de certificados emitidos pela AC CNDL RFB.

A notificação de emissão é feita por diferentes meios (e-mail contendo o certificado ou e-mail solicitando download em url específico ou em mídia).

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

4.3 Aceitação de Certificado

4.3.1. O certificado é considerado aceite assim que for utilizado. A aceitação implica que a pessoa física responsável pelo certificado reconhece a veracidade dos dados contidos nele.

4.3.2. A aceitação de todo certificado emitido é declarada implicitamente pelo respectivo titular assim que for utilizado. Para certificados emitidos para pessoas jurídicas, a declaração deverá ser feita pela pessoa física responsável por esses certificados.

4.3.3. Item não aplicável.

4.4 Suspensão e Revogação de Certificado

4.4.1 Circunstâncias para revogação

4.4.1.1. A AC CNDL, nesta DPC evidencia as circunstâncias nas quais um certificado poderá ser revogado.

4.4.1.2. Um certificado é obrigatoriamente revogado nas seguintes circunstâncias:

- a) caso haja constatação de emissão imprópria ou defeituosa do mesmo;
- b) mediante a necessidade de alteração de qualquer informação constante no mesmo; ou
- c) em caso de perda, roubo, modificação, acesso indevido ou comprometimento da chave privada correspondente ou da sua mídia armazenadora.

4.4.1.3. Deve-se observar ainda que:

- a) a AC CNDL RFB revogará, no 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;
- b) o CG da ICP-Brasil 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.
- c) a AC RFB determinará a revogação do certificado da AC CNDL RFB caso esta deixe de cumprir as normas, práticas e regras estabelecidas pela RFB.

4.4.2 Quem pode solicitar revogação

A revogação de um certificado somente pode ser solicitada:

- a) pelo titular do certificado;
- b) pelo responsável pelo certificado de pessoas jurídicas;
- c) por empresa ou órgão, quando o titular do certificado fornecido por essa empresa ou órgão for seu empregado, funcionário ou servidor;
- d) pela AC CNDL RFB;
- e) pela AC RFB;
- f) pela AR Vinculada; ou
- g) por determinação do CG da ICP-Brasil ou da AC Raiz.

4.4.3 Procedimento para solicitação de revogação

4.4.3.1. Para requerer a revogação é necessário o envio à AC CNDL RFB ou à AR vinculada de um formulário disponibilizado pela AC CNDL RFB (<https://www.spcbrasil.org.br/produtos/produto/40-certificacaodigital>), preenchido com os dados do solicitante, o número de série do certificado e a indicação do motivo da solicitação.

A AC CNDL RFB garante que todos agentes habilitados, conforme o item 4.4.2., possam, facilmente e a qualquer tempo, solicitar a revogação de seus respectivos certificados.

4.4.3.2. Como diretrizes gerais:

- a) o solicitante da revogação de um certificado é identificado;
- b) as solicitações de revogação, bem como as ações delas decorrentes são registradas e armazenadas;
- c) as justificativas para a revogação de um certificado são documentadas;
- d) o processo de revogação de um certificado termina com a geração e a publicação de uma LCR que contém o certificado revogado e com a atualização da situação do certificado nas bases de dados da AC CNDL RFB de consulta OCSP.

4.4.3.3. O prazo máximo admitido para a conclusão do processo de revogação de certificado, após o recebimento da respectiva solicitação, para todos os tipos de certificado previstos pela ICP-Brasil é de 12 (doze) horas.

4.4.3.4. O prazo máximo admitido para a conclusão do processo de revogação de certificado de AC, após o recebimento da respectiva solicitação, é de 12 (doze) horas.

4.4.3.5. A AC CNDL RFB 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.

4.4.3.6. Item não aplicável.

4.4.4 Prazo para solicitação de revogação

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

4.4.4.2. O prazo máximo para a aceitação do certificado por seu titular, dentro do qual a revogação desse certificado pode ser solicitada sem cobrança de tarifa pela AC CNDL RFB é de 3 (três) dias.

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 Frequência de emissão de LCR

4.4.9.1. Neste item a AC CNDL define a frequência de emissão da LCR referente a certificados de usuários finais.

4.4.9.2. A frequência máxima admitida para a emissão de LCR para os certificados de usuários finais é de 6 horas.

4.4.9.3. Item não aplicável.

4.4.9.4. Item não aplicável.

4.4.10 Requisitos para verificação de LCR

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

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

4.4.11 Disponibilidade para revogação/verificação de status on-line

A AC CNDL RFB dispõe de recursos para verificação on-line de status de certificados. A verificação da situação de um certificado poderá ser feita diretamente na AC CNDL RFB, por meio do protocolo OCSP (On-line Certificate Status Protocol).

4.4.12 Requisitos para verificação de revogação on-line

Não há requisitos específicos para a verificação on-line de informações de revogação de certificados por parte das terceiras partes (relying parties).

4.4.13 Outras formas disponíveis para divulgação de revogação

Item não aplicável.

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

4.4.15.1. Caso ocorra perda, roubo, modificação, acesso indevido ou comprometimento de chave privada ou de sua mídia armazenadora, o titular deve notificar imediatamente a AC CNDL RFB, solicitando a revogação de seu certificado, através do formulário específico para tal fim.

4.4.15.2. O comprometimento ou suspeita de comprometimento de chave deve ser comunicado pelo titular do certificado de maneira imediata à AC CNDL RFB. Tal comunicação deverá ser formalizada através do formulário específico para tal fim.

4.5 Procedimentos de Auditoria de Segurança

4.5.1 Tipos de evento registrados

4.5.1.1 Eventos relacionados ao sistema de certificação

A AC CNDL RFB registra em arquivos de auditoria os eventos relacionados à segurança do seu sistema de certificação. Os seguintes eventos são incluídos em arquivos de auditoria:

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

4.5.1.2 Eventos não diretamente relacionados ao sistema de certificação

A AC CNDL RFB registra, eletrônica ou manualmente, as seguintes informações de segurança não geradas diretamente pelo seu sistema de certificação, tais como:

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

4.5.1.3. A AC CNDL RFB não registra outras informações.

4.5.1.4. Os registros de auditoria, eletrônicos ou manuais, contém a data e a hora do evento registrado e a identidade do agente que o causou.

4.5.1.5. No intuito de facilitar os processos de auditoria, toda a documentação relacionada aos serviços da AC CNDL RFB é armazenada, eletrônica ou manualmente, em local único, conforme a POLÍTICA DE SEGURANÇA DA ICP-BRASIL[8].

4.5.1.6. A AR vinculada registra eletronicamente em arquivos de auditoria todos os eventos relacionados à validação e aprovação da solicitação, bem como, à revogação de certificados. Os seguintes eventos estão obrigatoriamente incluídos em arquivos de auditoria:

AC CNDL RFB Declaração de Práticas de Certificação

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

4.5.1.7. A AC CNDL RFB define, em documento disponível nas auditorias de conformidade, o local de arquivamento das cópias dos documentos para identificação apresentadas no momento da solicitação e revogação de certificados e do termo de titularidade.

4.5.2 Frequência de auditoria de registros (logs)

A análise dos registros correspondentes à auditoria da AC CNDL é feita periodicamente, não sendo superior a uma semana. Todo e qualquer evento estranho é destacado no relatório de auditoria e analisado em profundidade, gerando relatório de ação para eventual correção. Essa análise envolve também uma inspeção breve de todos os registros, com a verificação de que não foram alterados, e é seguida de 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 CNDL RFB mantém localmente seus registros de auditoria por pelo menos 2 (dois) meses e, subsequentemente, armazena os seus registros de auditoria da maneira descrita no item 4.6.

4.5.4 Proteção de registro (log) de auditoria

4.5.4.1. O sistema de registro de eventos de auditoria inclui mecanismos para proteger os arquivos de auditoria contra leitura não autorizada, modificação e remoção, através das funcionalidades nativas dos sistemas operacionais.

4.5.4.2. Mecanismos de proteção utilizados:

- a) Os acessos lógicos são liberados através da ferramenta nativa do sistema operacional de modo a assegurar o uso apenas a usuários ou processos autorizados;
- b) Os acessos lógicos aos registros de eventos de auditoria são registrados em logs do próprio sistema operacional;
- c) Informações manuais de auditoria também são protegidas contra a leitura não autorizada, modificação e remoção.

4.5.4.3. Os mecanismos de proteção descritos neste item obedecem à Política de Segurança implementada, de conformidade com a POLÍTICA DE SEGURANÇA DA ICP-BRASIL[8].

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

É gerado pela AC CNDL RFB semanalmente cópia de backup de seus registros de auditoria, através de procedimentos utilizando conexão segura.

4.5.6 Sistema de coleta de dados de auditoria

O sistema de coleta de dados de auditoria é interno à AC CNDL RFB e utiliza processos automatizados e manuais.

4.5.7 Notificação de agentes causadores de eventos

No momento em que um evento é registrado pelo conjunto de sistemas de auditoria da AC CNDL RFB, nenhuma notificação é enviada à pessoa ou organização que causou o evento.

4.5.8 Avaliações de vulnerabilidade

Os possíveis eventos de vulnerabilidade detectados na análise periódica dos registros de auditoria da AC CNDL RFB, são analisados detalhadamente e, dependendo de sua gravidade, registrados em separado. Ações corretivas decorrentes são tomadas pela AC CNDL RFB e registradas para fins de auditoria.

4.6 Arquivamento de Registros

4.6.1 Tipos de eventos registrados

Os tipos de eventos arquivados pela AC CNDL RFB, são:

- a) solicitações de certificados;
- b) solicitações de revogação de certificados;
- c) notificações de comprometimento de chaves privadas;
- d) emissões e revogações de certificados;
- e) emissões de LCR;
- f) trocas de chaves criptográficas da AC CNDL RFB;
- g) informações de auditoria previstas no item 4.5.1.

AC CNDL RFB Declaração de Práticas de Certificação

4.6.2 Período de retenção para arquivo

Os períodos de retenção para cada evento arquivado, são:

- a) as LCR e os certificados de assinatura digital são retidos permanentemente, para fins de consulta histórica;
- b) as cópias dos documentos para identificação apresentadas no momento da solicitação e da revogação de certificados, e os termos de titularidade e responsabilidade devem ser retidos, no mínimo, por 10 (dez) anos, a contar da data de expiração ou revogação do certificado.
- c) as demais informações, inclusive arquivos de auditoria, são retidas por, no mínimo, 6 (seis) anos.

4.6.3 Proteção de arquivo

Os registros arquivados da AC CNDL RFB são classificados e armazenados com requisitos de segurança compatíveis com essa classificação e com a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8].

4.6.4 Procedimentos para cópia de segurança (backup) de arquivo

4.6.4.1. A cópia de todo o material arquivado será armazenada em local físico externo à AC responsável, recebendo o mesmo tipo de proteção utilizada por ela no arquivo principal.

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

4.6.4.3. A AC CNDL RFB verifica a integridade dessas cópias de segurança, no mínimo, a cada 6 (seis) meses.

4.6.5 Requisitos para datação (time-stamping) de registros

Os servidores estão sincronizados com a hora GMT. 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 e formulários de requisição de certificados, estes contêm a Hora Oficial do Brasil.

4.6.6 Sistema de coleta de dados de arquivo

Todos os sistemas de coleta de dados de arquivo utilizados pela AC CNDL RFB em seus procedimentos operacionais são automatizados e manuais e internos.

4.6.7 Procedimentos para obter e verificar informação de arquivo

A verificação de informação de arquivo deve ser solicitada formalmente à AC CNDL RFB ou à AR Vinculada, identificando de forma precisa o tipo e o período da informação a ser verificada. O solicitante da verificação de informação deve ser devidamente identificado.

4.7 Troca de chave

4.7.1. Trinta dias antes da data de expiração do certificado digital, a AR Vinculada comunica ao seu titular, através do e-mail cadastrado no formulário de solicitação de certificado, a data de expiração do mesmo, junto com link <https://www.spcbrasil.org.br/produtos/produto/40-certificacaodigital> para a solicitação de novo certificado.

4.7.2. Item não aplicável.

4.8 Comprometimento e Recuperação de Desastre

A AC CNDL RFB possui um Plano de Continuidade de Negócio, estabelecido conforme a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8] e testado pelo menos uma vez por ano, para garantir a continuidade dos seus serviços críticos.

Esse Plano administra as situações de crise mediante: identificação do motivo da crise, acionamento dos principais responsáveis pelo processo de certificação digital, acionamento das equipes envolvidas na solução do incidente, ação para impedir a continuidade do problema, avaliação da extensão da crise, acionamento da situação de recuperação, ações de recuperação propriamente ditas, notificações à AC Raiz da evolução corretiva e solução, registro da crise e análise para melhoria.

4.8.1 Recursos computacionais, software e dados corrompidos

Procedimentos descritos no Plano de Continuidade do Negócio da AC CNDL RFB, que incluem a identificação da crise, acionamento dos principais gestores, acionamento das equipes, contenção da crise, avaliação da extensão da crise, declaração do início das atividades de acionamento da situação de recuperação, notificação da crise, registro da crise, análise para melhoria.

Nas situações de crise relacionadas aos recursos computacionais, software e dados corrompidos ou quando houver suspeita de corrupção dos mesmos, após a identificação da crise ou confirmação da suspeita de corrupção, são notificados os gestores do processo de certificação digital, que acionam as equipes envolvidas, de forma a identificar o grau de corrupção.

AC CNDL RFB Declaração de Práticas de Certificação

Os procedimentos de recuperação dos recursos computacionais, softwares e dados corrompidos envolvem identificação da necessidade de recurso computacional alternativo e, em caso de necessidade, disponibilização de outro recurso computacional equivalente, instalação dos softwares necessários e recuperação dos dados através do arquivo de back-up.

4.8.2 Certificado de entidade é revogado

Procedimentos descritos no Plano de Continuidade do Negócio da AC CNDL RFB, que incluem a identificação da crise, acionamento dos principais gestores, acionamento das equipes, contenção da crise, avaliação da extensão da crise, declaração do início das atividades de acionamento da situação de recuperação, notificação da crise, registro da crise, análise para melhoria.

Em caso de revogação do certificado da AC CNDL RFB, 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 dos usuários finais, é gerado um novo par de chaves da AC CNDL RFB, emitido certificado associado ao novo par de chaves gerado e emitidos novos certificados digitais para os usuários finais.

4.8.3 Chave de entidade é comprometida

Procedimentos descritos no Plano e Continuidade do Negócio da AC CNDL RFB, que incluem a identificação da crise, acionamento dos principais gestores, acionamento das equipes, contenção da crise, avaliação da extensão da crise, declaração do início das atividades de acionamento da situação de recuperação, notificação da crise, registro da crise, análise para melhoria.

Em caso de comprometimento da chave da AC CNDL RFB, 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 CNDL RFB e dos usuários finais, é gerado um novo par de chaves, emitido certificado associado ao novo par de chaves gerado e emitidos novos certificados digitais para os usuários finais.

4.8.4 Segurança dos recursos após desastre natural ou de outra natureza

Procedimentos descritos no Plano de Continuidade do Negócio da AC CNDL RFB, que incluem a identificação da crise, acionamento dos principais gestores, acionamento das equipes, contenção da crise, avaliação da extensão da crise, declaração do início das atividades de acionamento da situação de recuperação, notificação da crise, registro da crise, análise para melhoria.

Em caso de desastre natural ou de outra natureza, após a identificação da crise são notificados os gestores do processo de certificação digital, que acionam as equipes envolvidas, de forma a identificar o grau de exposição e comprometimento do ambiente. Na confirmação do desastre e constatado impossibilidade de operação no site, as atividades são transferidas para o site de recuperação de desastre.

4.8.5. Atividades das Autoridades de Registro

Procedimentos descritos no Plano de Continuidade do Negócio da AR Vinculada contemplam a recuperação, total ou parcial das atividades das AR, contendo, no mínimo as seguintes informações:

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

4.9 Extinção dos serviços de AC, AR ou PSS

4.9.1. Em caso de extinção da AC CNDL RFB, AR Vinculada ou PSS serão tomadas as providências preconizadas no documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6].

4.9.2. Os procedimentos incluem: a divulgação da decisão do encerramento de atividades, prazos para essa divulgação, atividades relacionadas à geração de novos certificados, revogação de certificados, aplicativos dedicados à certificação digital, guarda de bases de dados e registro observará os mesmos requisitos de segurança exigidos pela AC CNDL RFB.

5. CONTROLES DE SEGURANÇA FÍSICA, PROCEDIMENTAL E DE PESSOAL

São implementados pela AC CNDL RFB os controles descritos a seguir para executar de modo seguro suas funções de geração de chaves, identificação, certificação, auditoria e arquivamento de registros.

5.1 Controles Físicos

Os controles físicos referentes às instalações que abrigam os sistemas da AC CNDL RFB, estão descritos nos itens a seguir.

5.1.1 Construção e localização das instalações de AC

5.1.1.1. A localização e o sistema de certificação da AC CNDL RFB não são publicamente identificados. Não há identificação pública externa das instalações e, internamente, não são admitidos ambientes compartilhados que permitam visibilidade das operações de emissão e revogação de certificados. Essas operações são segregadas em compartimentos fechados e fisicamente protegidos.

5.1.1.2. Na construção das instalações da AC CNDL RFB foram considerados, entre outros, os seguintes aspectos relevantes para os controles de segurança física:

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

5.1.2 Acesso físico

A AC CNDL RFB implantou um sistema de controle de acesso físico que garante a segurança de suas instalações, conforme a Política de Segurança implementada e os requisitos que seguem.

5.1.2.1 Níveis de acesso

5.1.2.1.1. A AC CNDL RFB definiu 4 (quatro) níveis de acesso físico aos diversos ambientes, e 2 (dois) níveis relativos à proteção da chave privada da AC CNDL RFB.

5.1.2.1.2. O primeiro nível - ou nível 1 - situa-se após a primeira barreira de acesso às instalações da AC CNDL RFB. Para entrar em uma área de nível 1, cada indivíduo deve ser identificado e registrado por segurança armado. A partir desse nível, pessoas estranhas à operação da AC CNDL RFB devem transitar devidamente identificadas e acompanhadas. Nenhum tipo de processo operacional ou administrativo da AC CNDL RFB é executado nesse nível.

5.1.2.1.3. Excetuados os casos previstos em lei, o porte de armas não é admitido nas instalações da AC CNDL RFB, a partir do nível 1. A partir desse nível, equipamentos de gravação, fotografia, vídeo, som ou similares, bem como computadores portáteis, têm sua entrada controlada e somente podem ser utilizados mediante autorização formal e supervisão.

5.1.2.1.4. O segundo nível - ou nível 2 - é interno ao primeiro e requer, da mesma forma que o primeiro, a identificação individual das pessoas que nele entram. A passagem do primeiro para o segundo nível exige identificação 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 CNDL RFB.

5.1.2.1.5. O terceiro nível - ou nível 3 - situa-se dentro do segundo e é o primeiro nível a abrigar material e atividades sensíveis da operação da AC CNDL RFB. As atividades relativas ao ciclo de vida dos certificados digitais estão localizadas 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 podem permanecer nesse nível se não estiverem acompanhadas por alguém que tenha essa permissão.

5.1.2.1.6. 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: cartão eletrônico individual e identificação biométrica.

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

5.1.2.1.8. No quarto nível (nível 4), interior ao terceiro, é onde ocorrem atividades especialmente sensíveis da operação da AC CNDL RFB 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 no mínimo de duas pessoas autorizadas é exigida enquanto o ambiente estiver ocupado.

5.1.2.1.9. No quarto nível todas as paredes, piso e teto são revestidos de aço e concreto ou de outro material de resistência equivalente. As paredes, piso e o teto são inteiriços, constituindo uma célula estanque contra ameaças de acesso indevido, água, vapor, gases e fogo.

No quarto nível, 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 possuem proteção contra interferência eletromagnética externa.

5.1.2.1.10. As salas-cofre foram construídas segundo as normas brasileiras aplicáveis. Eventuais omissões dessas normas deverão ser sanadas por normas internacionais pertinentes.

5.1.2.1.11. Na AC CNDL RFB há 1 (um) ambiente de quarto nível para abrigar e segregar, respectivamente:

- Equipamentos de produção on-line;
- Equipamentos de produção off-line e cofre de armazenamento.

5.1.2.1.12. O quinto nível (nível 5), interior aos ambientes de nível 4, compreende um gabinete reforçado trancado. Materiais criptográficos tais como chaves, dados de ativação, suas cópias e equipamentos criptográficos estão armazenados em ambiente de nível 5 ou superior.

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

- É feito em aço ou material de resistência equivalente;
- Possui tranca com chave.

5.1.2.1.14. O sexto nível (nível 6) consiste de pequenos depósitos localizados no interior do cofre de quinto nível. Cada um desses depósitos dispõe de duas fechaduras, sendo uma comum a todos os depósitos e uma individual. Os dados de ativação da chave privada da AC CNDL RFB são armazenados nesses depósitos.

5.1.2.2 Sistemas físicos de detecção

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

5.1.2.2.2. As fitas de vídeo resultantes da gravação 24 x 7 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.

5.1.2.2.3. Todas as portas de passagem entre os níveis de acesso 3 e 4 do ambiente são monitoradas por sistema de notificação de alarmes. Onde há, a partir do nível 2, vidros separando níveis de acesso, foi implantado um mecanismo de alarme de quebra de vidros, que permanece ligado ininterruptamente.

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

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

5.1.2.2.6. O sistema de monitoramento das câmeras 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 câmeras 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

5.1.2.4.1. Mecanismos específicos foram implantados pela AC CNDL RFB para garantir a segurança de seu pessoal e de seus equipamentos 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.

5.1.2.4.2. Todos os procedimentos referentes aos mecanismos de emergência são 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 nas instalações de AC

5.1.3.1. A infraestrutura do ambiente de certificação da AC CNDL RFB foi dimensionada com sistemas e dispositivos que garantem o fornecimento ininterrupto de energia elétrica às instalações. As condições de fornecimento de energia são mantidas de forma a atender os requisitos de disponibilidade dos sistemas da AC CNDL RFB e seus respectivos serviços. Um sistema de aterramento foi implantado.

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

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

5.1.3.4. 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.

5.1.3.5. 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[8]. Qualquer modificação nessa rede é previamente documentada.

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

5.1.3.7. O sistema de climatização atende os 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 tolerante a falhas.

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

5.1.3.9. O sistema de ar condicionado do nível 4 é interno, com troca de ar realizada apenas por abertura da porta.

5.1.3.10. A capacidade de redundância de toda a estrutura de energia e ar condicionado da AC CNDL RFB é garantida, por meio de:

- Geradores de porte compatível;
- Geradores de reserva;
- Sistemas de no-breaks redundantes;
- Sistemas redundantes de ar condicionado.

5.1.4 Exposição à água nas instalações de AC

O ambiente de nível 4 encontra-se fisicamente protegido contra exposição à água, infiltrações e inundações, provenientes de qualquer fonte externa.

5.1.5 Prevenção e proteção contra incêndio nas instalações de AC

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

5.1.5.2 Nas instalações da AC CNDL RFB não é permitido fumar ou portar objetos que produzam fogo ou faísca.

5.1.5.3. O ambiente de nível 4 possui sistema para detecção precoce de fumaça e sistema de extinção de incêndio por gás. As portas de acesso ao ambiente de nível 4 constituem eclusas, onde uma porta só se abre quando a anterior estiver fechada.

5.1.5.4. Em caso de incêndio nas instalações da AC CNDL RFB, o aumento da temperatura interna da sala-cofre de nível 4 não excede 50 graus Celsius, e a sala suporta esta condição por, no mínimo, 1 (uma) hora.

5.1.6 Armazenamento de mídia nas instalações de AC

São observados os critérios estabelecidos na norma brasileira NBR 11.515/NB 1334 ("Critérios de Segurança Física Relativos ao Armazenamento de Dados").

5.1.7 Destruição de lixo nas instalações de AC

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

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

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

As instalações de backup atendem os requisitos mínimos estabelecidos por este documento. Sua localização é tal que, em caso de sinistro que torne inoperantes as instalações principais, as instalações de backup não serão atingidas e tornem - se totalmente operacionais em, no máximo, 48 (quarenta e oito) horas.

5.1.9. Instalações técnicas de AR

As instalações técnicas da AR Vinculada atendem aos requisitos estabelecidos no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP-BRASIL [1].

5.2. Controles Procedimentais

5.2.1. Perfis qualificados

5.2.1.1. A AC CNDL RFB efetua separação das tarefas para funções críticas, com o intuito de evitar que um empregado utilize o seu sistema de certificação sem ser detectado. As ações de cada empregado estão limitadas de acordo com seu perfil.

5.2.1.2. A AC CNDL RFB estabelece perfis distintos para sua operação, distinguindo as operações do dia-a-dia do sistema, o gerenciamento e a auditoria dessas operações, bem como o gerenciamento de mudanças substanciais no sistema.

O detalhamento dos perfis encontra-se em documento interno normativo.

5.2.1.3. Todos os operadores do sistema de certificação da AC CNDL RFB 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.

5.2.1.4. Quando um empregado se desligar da AC CNDL RFB, suas permissões de acesso são revogadas imediatamente. Quando houver mudança na posição ou função que o empregado ocupa dentro da AC CNDL RFB, suas permissões de acesso são revistas. Há uma lista de revogação, com todos os recursos, antes disponibilizados, que o empregado deve devolver à AC no ato de seu desligamento.

5.2.2. Número de pessoas necessário por tarefa

5.2.2.1. A AC CNDL RFB utiliza o requisito de controle multiusuário para a geração e a utilização da sua chave privada, na forma definida no item 6.2.2.

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

5.2.3. Identificação e autenticação para cada perfil

5.2.3.1. Todo empregado da AC CNDL RFB tem sua identidade e perfil verificados antes de:

- Ser incluído em uma lista de acesso às instalações da AC CNDL RFB;
- Ser incluído em uma lista para acesso físico ao sistema de certificação da AC CNDL RFB;
- Receber um certificado para executar suas atividades operacionais na AC CNDL RFB;
- Receber uma conta no sistema de certificação da AC CNDL RFB.

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

- São diretamente atribuídos a um único empregado;
- Não são compartilhados;
- São restritos às ações associadas ao perfil para o qual foram criados.

5.2.3.3. A AC CNDL RFB implementa um padrão de utilização de "senhas fortes", definido na Política de Segurança implementada e em conformidade com a POLÍTICA DE SEGURANÇA DA ICP-BRASIL[8], juntamente com procedimentos de validação dessas senhas.

5.3. Controles de Pessoal

Todos os empregados da AC CNDL RFB e da AR Vinculada encarregados de tarefas operacionais têm registrado em contrato ou termo de responsabilidade:

- Os termos e as condições do perfil que ocuparão;
- O compromisso de observar as normas, políticas e regras aplicáveis da ICP-Brasil;
- 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 CNDL RFB e da AR Vinculada 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 ICP-BRASIL[8] e na Política de Segurança implementada.

5.3.2. Procedimentos de verificação de antecedentes

5.3.2.1. Com o propósito de resguardar a segurança e a credibilidade das entidades, todo o pessoal da AC CNDL RFB e da AR Vinculada envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados é submetido a:

- a) Verificação de antecedentes criminais;
- b) Verificação de situação de crédito;
- c) Verificação de histórico de empregos anteriores;
- d) Comprovação de escolaridade e de residência.

5.3.2.2. A AC CNDL RFB não define requisitos adicionais para a verificação de antecedentes.

5.3.3. Requisitos de treinamento

Todo o pessoal da AC CNDL RFB e da AR Vinculada 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:

- a) princípios e mecanismos de segurança da AC CNDL RFB e das AR vinculadas;
- b) sistema de certificação em uso na AC CNDL RFB;
- c) procedimentos de recuperação de desastres e de continuidade do negócio;
- d) reconhecimento de assinaturas e validade dos documentos apresentados, na forma do item 3.1.9 e 3.1.10 e 3.1.11; e
- e) outros assuntos relativos a atividades sob sua responsabilidade.

5.3.4. Frequência e requisitos para reciclagem técnica

Todo o pessoal da AC CNDL RFB e da AR Vinculada envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados é mantido atualizado sobre eventuais mudanças tecnológicas nos sistemas da AC CNDL RFB e da AR Vinculada.

5.3.5. Frequência e sequência de rodízio de cargos

A AC CNDL RFB e a AR Vinculadas possuem pessoal e efetivo de contingência devidamente treinado, não fazendo uso de rodízio de pessoal.

5.3.6. Sanções para ações não autorizadas

5.3.6.1. Na eventualidade de uma ação não autorizada, real ou suspeita, ser realizada por pessoa encarregada de processo operacional da AC CNDL RFB e da AR Vinculada, a AC CNDL RFB ou a AR Vinculada suspenderá o acesso dessa pessoa ao seu sistema de certificação e tomará as medidas administrativas e legais cabíveis.

5.3.6.2. O processo administrativo referido acima contém os seguintes itens:

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

5.3.6.3. Concluído o processo administrativo, a AC CNDL RFB encaminha suas conclusões à AC Raiz.

5.3.6.4. As punições passíveis de aplicação, em decorrência de processo administrativo, são:

- a) advertência;
- b) suspensão por prazo determinado; ou
- c) impedimento definitivo de exercer funções no âmbito da ICP-Brasil.

5.3.7. Requisitos para contratação de pessoal

Todo o pessoal da AC CNDL RFB e da AR Vinculada envolvido em 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 ICP-BRASIL[8] e na Política de Segurança implementada.

5.3.8. Documentação fornecida ao pessoal

5.3.8.1. A AC CNDL RFB torna disponível para todo o seu pessoal e para o pessoal da AR vinculada:

- a) Sua DPC-AC CNDL RFB;
- b) As PC que implementa;
- c) A POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8] e a sua Política de Segurança;
- d) Documentação operacional relativa a suas atividades;
- e) Contratos, normas e políticas relevantes para suas atividades.

5.3.8.2. Toda a documentação fornecida ao pessoal é classificada segundo a política de classificação de informação definida pela AC CNDL RFB e é mantida atualizada.

6. CONTROLES TÉCNICOS DE SEGURANÇA

6.1. Geração e Instalação do Par de Chaves

6.1.1. Geração do par de chaves

6.1.1.1. O par de chaves criptográficos da AC CNDL RFB é gerado pela própria AC CNDL RFB, após o deferimento do seu pedido de credenciamento e a consequente autorização de funcionamento no âmbito da ICP-Brasil.

6.1.1.2. Pares de chaves são gerados somente pelo titular do certificado correspondente.

6.1.1.3. Cada PC implementada pela AC CNDL RFB define o meio utilizado para armazenamento da chave privada, com base nos requisitos aplicáveis estabelecidos nos REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [7].

6.1.2. Entrega da chave privada à entidade titular

A geração e a guarda de uma chave privada são de responsabilidade exclusiva do titular do certificado correspondente.

6.1.3. Entrega da chave pública para emissor de certificado

6.1.3.1. Para a entrega de sua chave pública à CNDL Autoridade Certificadora Principal, encarregada da emissão de seu certificado, a AC CNDL RFB fará uso do padrão PKCS#10.

6.1.3.2. Os procedimentos para a entrega da chave pública de um solicitante de certificado à AC CNDL RFB estão detalhados em cada PC implementada.

6.1.4. Disponibilização de chave pública da AC CNDL RFB para usuários

As formas para a disponibilização do certificado da AC CNDL RFB, e de todos os certificados da cadeia de certificação, para os usuários da ICP-Brasil, compreendem, entre outras:

- a) formato PKCS#7 (RFC 2315), que inclui toda a cadeia de certificação, no momento da disponibilização de um certificado para seu titular;
- b) diretório;
- c) página Web da AC CNDL RFB (<https://www.spcbrasil.org.br/produtos/produto/40-certificacaodigital>);
- d) outros meios seguros a serem aprovados pelo CG da ICP-Brasil.

6.1.5. Tamanhos de chave

6.1.5.1. Cada PC implementada pela AC CNDL RFB define o tamanho das chaves criptográficas associadas aos certificados emitidos, com base nos requisitos aplicáveis estabelecidos nos REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [7].

6.1.5.2. Não se aplica.

6.1.6. Geração de parâmetros de chaves assimétricas

A AC CNDL RFB adota o padrão FIPS (Federal Information Processing Standards) 140-2, level 3 para a geração de suas chaves assimétricas, observado o disposto no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

6.1.7. Verificação da qualidade dos parâmetros

Os parâmetros são verificados de acordo com as normas estabelecidas pelo padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

6.1.8. Geração de chave por hardware ou software

6.1.8.1 O processo de geração do par de chaves da AC CNDL RFB é feito por hardware padrão FIPS (Federal Information Processing Standards) 140-2, level 3, observado o disposto no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

6.1.8.2. Cada PC implementada pela AC CNDL RFB caracteriza o processo utilizado para a geração de chaves criptográficas dos titulares de certificados, com base nos requisitos aplicáveis estabelecidos nos REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [7].

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

6.1.9.1 Os propósitos para os quais podem ser utilizadas as chaves criptográficas dos titulares de certificados emitidos pela AC CNDL RFB, bem como as possíveis restrições cabíveis, em conformidade com as aplicações definidas para os certificados correspondentes estão especificados em cada PC implementada.

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

6.2. Proteção da Chave Privada

As chaves privadas da AC CNDL RFB trafegam cifradas entre o módulo gerador e a mídia utilizada para o seu armazenamento.

Cada PC implementada especifica os requisitos específicos aplicáveis para a proteção das chaves privadas das entidades titulares de certificados.

6.2.1. Padrões para módulo criptográfico

6.2.1.1. O módulo criptográfico de geração de chaves assimétricas da AC CNDL RFB adota o padrão FIPS (Federal Information Processing Standards) 140-2, level 3, padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

6.2.1.2. Cada PC implementada especifica os requisitos específicos aplicáveis para a geração de chaves criptográficas dos titulares de certificado.

6.2.2. Controle "n de m" para chave privada

6.2.2.1. Item não aplicável

6.2.2.2. Item não aplicável

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

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

6.2.4.2. A AC CNDL RFB mantém cópia de segurança de sua própria chave privada.

6.2.4.3. A AC CNDL RFB não mantém cópia de segurança de chave privada de titular de certificados e-CPF e e-CNPJ por ela emitido. Por solicitação do respectivo titular, ou de empresa ou órgão, quando o titular do certificado for seu empregado ou cliente, a AC CNDL RFB manterá cópia de segurança de chave privada correspondente a certificado de sigilo por ela emitido. Cada PC implementada define os requisitos específicos aplicáveis.

6.2.4.4. Em qualquer caso, a cópia de segurança é armazenada, cifrada, por algoritmo simétrico definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9], e protegida com um nível de segurança não inferior àquele definido para a chave original.

6.2.5. Arquivamento de chave privada

6.2.5.1. A AC CNDL RFB não emite certificados de sigilo. Não são arquivadas chaves privadas de assinatura digital.

6.2.5.2. 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

Cada PC implementada define, quando aplicável, os requisitos para inserção da chave privada dos titulares de certificado em módulo criptográfico.

6.2.7. Método de ativação de chave privada

Para a ativação das chaves privadas exige-se o número mínimo de 2 ("n") (duas) pessoas de um grupo de 5 ("m") (cinco). A confirmação da identidade desses agentes é feita através de senhas, só lhes sendo permitido o acesso ao ambiente em duplas devidamente autorizadas.

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

6.2.8. Método de desativação de chave privada

Para a desativação das chaves privadas exige-se o número mínimo de 2 ("n") (duas) pessoas de um grupo de 5 ("m") (cinco). A confirmação da identidade desses agentes é feita através de senhas, só lhes sendo permitido o acesso ao ambiente em duplas devidamente autorizadas.

AC CNDL RFB Declaração de Práticas de Certificação

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

6.2.9. Método de destruição de chave privada

Para a destruição das chaves privadas exige-se o número mínimo de 2 ("n") (duas) pessoas de um grupo de 5 ("m") (cinco). A confirmação da identidade desses agentes é feita através de senhas, só lhes sendo permitido o acesso ao ambiente em duplas devidamente autorizadas.

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

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

6.3. Outros Aspectos do Gerenciamento do Par de Chaves

6.3.1. Arquivamento de chave pública

As chaves públicas da AC CNDL RFB e dos titulares de certificados de assinatura digital por ela emitidos permanecem armazenadas permanentemente, para verificação de assinaturas geradas durante seu período de validade.

6.3.2. Períodos de uso para as chaves pública e privada

6.3.2.1. As chaves privadas da AC CNDL RFB e dos titulares de certificados de assinatura digital por ela emitidos são utilizadas apenas durante o período de validade dos certificados correspondentes. As correspondentes chaves públicas são utilizadas durante todo o período de tempo determinado pela legislação aplicável, para verificação de assinaturas geradas durante o prazo de validade dos respectivos certificados.

6.3.2.2. Não se aplica.

6.3.2.3. Cada PC implementada pela AC CNDL RFB define o período máximo de validade do certificado, com base nos requisitos aplicáveis estabelecidos nos REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [7].

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

6.4. Dados de Ativação

6.4.1. Geração e instalação dos dados de ativação

6.4.1.1. Os dados de ativação da chave privada da AC CNDL RFB são únicos e aleatórios.

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

6.4.2. Proteção dos dados de ativação

6.4.2.1. Os dados de ativação da chave privada da AC CNDL RFB são protegidos contra uso não autorizado, por meio de mecanismos de criptografia e de controle de acesso físico.

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

6.4.3. Outros aspectos dos dados de ativação

Não se aplica.

6.5. Controles de Segurança Computacional

6.5.1. Requisitos Técnicos Específicos de Segurança Computacional

6.5.1.1. A geração do par de chaves da AC CNDL RFB é realizada off-line, para impedir o acesso remoto não autorizado.

6.5.1.2. Os requisitos específicos aplicáveis são descritos em cada PC implementada.

6.5.1.3. Cada computador servidor da AC CNDL RFB, relacionado diretamente com os processos de emissão, expedição, distribuição, revogação ou gerenciamento de certificados, implementam, entre outras, as seguintes características:

- a) controle de acesso aos serviços e perfis da AC CNDL RFB;
- b) clara separação das tarefas e atribuições relacionadas a cada perfil qualificado da AC CNDL RFB;
- c) uso de criptografia para segurança de base de dados, quando exigido pela classificação de suas informações;
- d) geração e armazenamento de registros de auditoria da AC CNDL RFB;
- e) mecanismos internos de segurança para garantia da integridade de dados e processos críticos; e

AC CNDL RFB Declaração de Práticas de Certificação

f) mecanismos para cópias de segurança (backup).

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

6.5.1.5. Qualquer equipamento, ou parte deste, ao ser enviado para manutenção tem apagadas as informações sensíveis nele contidas e controlados seu número de série e as datas de envio e de recebimento. Ao retornar às instalações da AC CNDL RFB, o equipamento que passou por manutenção é inspecionado. Em todo equipamento que deixa de ser utilizado em caráter permanente, serão destruídas de maneira definitiva todas as informações sensíveis armazenadas, relativas à atividade da AC CNDL RFB. Todos esses eventos são registrados para fins de auditoria.

6.5.1.6. Qualquer equipamento incorporado à AC CNDL RFB 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

A segurança computacional da AC CNDL RFB segue as recomendações do Trusted System Evaluation Criteria (TCSEC).

6.5.3. Controles de Segurança para as Autoridades de Registro

6.5.3.1. A AC CNDL RFB implementa requisitos de segurança computacional das estações de trabalho e dos computadores portáteis utilizados pela AR Vinculada para os processos de validação e aprovação de certificados.

6.5.3.2. São incluídos, no mínimo, os requisitos especificados no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP-BRASIL [1].

6.6. Controles Técnicos do Ciclo de Vida

6.6.1. Controles de desenvolvimento de sistema

6.6.1.1. A AC CNDL RFB adota tecnologias de certificação digital e efetua as devidas customizações para adequar as necessidades do ambiente da AC, os quais são desenvolvidos por Analistas de Suporte, todos empregados de confiança de seu PSS. Estas customizações são realizadas inicialmente em um ambiente de desenvolvimento e depois de concluído, é colocado em um ambiente de homologação. Finalizado o processo de homologação é encaminhado um pedido para a "Gerência de Mudança" que é coordenada pelo Gestor do Processo de Certificação Digital e é composto de outras áreas do PSS da AC CNDL RFB, como por exemplo, Segurança de Sistemas de Informação, Produção, etc., que avaliam e decidem quanto a sua implementação.

6.6.1.2. Os processos de projeto e desenvolvimento conduzidos pela AC CNDL RFB provêm documentação suficiente para suportar avaliações externas de segurança dos componentes da AC CNDL RFB.

6.6.2. Controles de gerenciamento de segurança

6.6.2.1. A AC CNDL RFB e AR vinculada utilizam ferramentas e os procedimentos formais para garantir que os seus sistemas e redes operacionais implementem os níveis configurados de segurança.

6.6.2.2. A AC CNDL RFB utiliza metodologia formal de gerenciamento de configuração para a instalação e a contínua manutenção do sistema de certificação da AC CNDL RFB.

6.6.3. Classificações de segurança de ciclo de vida

Não se aplica.

6.6.4. Controles na Geração de LCR

Antes de publicadas, todas as LCR geradas pela AC são checadas quanto à consistência de seu conteúdo, comparando-o com o conteúdo esperado em relação a número da LCR, data/hora de emissão e outras informações relevantes.

6.7. Controles de Segurança de Rede

6.7.1. Diretrizes Gerais

6.7.1.1. Neste item são descritos os controles relativos à segurança da rede da AC CNDL RFB, incluindo firewalls e recursos similares.

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

6.7.1.3. Todos os servidores e elementos de infraestrutura e proteção de rede, tais como roteadores, hubs, switches, firewalls e sistemas de detecção de intrusão (IDS), localizados no segmento de rede que hospeda o sistema de certificação da AC CNDL RFB, estão localizados e operam em ambiente de nível 4.

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

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

6.7.2. Firewall

6.7.2.1. Mecanismos de firewall são implementados em equipamentos de utilização específica, configurados exclusivamente para tal função. Firewalls promovem o isolamento, em sub-redes específicas, dos equipamentos servidores com acesso externo - a conhecida "zona desmilitarizada" (DMZ) - em relação aos equipamentos com acesso exclusivamente interno à AC CNDL RFB.

6.7.2.2. O software de firewall, entre outras características, implementa registros de auditoria.

6.7.3. Sistema de detecção de intrusão (IDS)

6.7.3.1. O sistema de detecção de intrusão tem 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 aos firewalls ou ao terminal de gerenciamento, promover a desconexão automática de conexões suspeitas, ou ainda a reconfiguração dos firewalls.

6.7.3.2. O sistema de detecção de intrusão tem capacidade de reconhecer diferentes padrões de ataques, inclusive contra o próprio sistema, apresentando a possibilidade de atualização da sua base de reconhecimento.

6.7.3.3. O sistema de detecção de intrusão provê o registro dos eventos em logs, recuperáveis em arquivos do tipo texto, além de implementar uma gerência de configuração.

6.7.4. Registro de acessos não autorizados à rede

As tentativas de acesso não autorizado - em roteadores, firewalls ou IDS - são registradas em arquivos para posterior análise. A frequência de exame dos arquivos de registro é, no mínimo, diária e todas as ações tomadas em decorrência desse exame são documentadas.

6.8. Controles de Engenharia do Módulo Criptográfico

O módulo criptográfico de geração de chaves assimétricas da AC CNDL RFB adota o padrão FIPS (Federal Information Processing Standards) 140-2, level 3.

7. PERFIS DE CERTIFICADO E LCR

7.1. Diretrizes Gerais

7.1.1. Nos itens seguintes, são descritos os aspectos dos certificados e LCR emitidos pela AC CNDL RFB.

7.1.2. As PC's abaixo, implementadas pela AC CNDL RFB, especificam os formatos dos certificados gerados e das correspondentes LCR. Nessas PC's são incluídas informações sobre os padrões adotados, seus perfis, versões e extensões.

Política de Certificado	Nome conhecido	OID
Política de Certificado de Assinatura Digital tipo A1 da AC CNDL RFB	PC AC CNDL RFB A1	2.16.76.1.2.1.52
Política de Certificado de Assinatura Digital tipo A3 da AC CNDL RFB	PC AC CNDL RFB A3	2.16.76.1.2.3.49

7.1.3. Item não aplicável.

7.2. Perfil do Certificado

Todos os certificados emitidos pela AC CNDL RFB estão em conformidade com o formato definido pelo padrão ITU X.509 ou ISO/IEC 9594-8.

7.2.1. Número(s) de versão

Todos os certificados emitidos pela AC CNDL RFB implementam a versão 3 do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 5280.

7.2.2. Extensões de certificado

Item não aplicável.

7.2.3. Identificadores de algoritmo

Item não aplicável.

AC CNDL RFB
Declaração de Práticas de Certificação

7.2.4. Formatos de nome

Item não aplicável.

7.2.5. Restrições de nome

Item não aplicável.

7.2.6. OID (Object Identifier) de DPC

O OID desta DPC-AC CNDL RFB é 2.16.72.1.1.65.

7.2.7. Uso da extensão "Policy Constraints"

Item não aplicável.

7.2.8. Sintaxe e semântica dos qualificadores de política

Item não aplicável.

7.2.9. Semântica de processamento para extensões críticas

Item não aplicável.

7.3. Perfil de LCR

7.3.1. Número(s) de versão

As LCR geradas pela AC CNDL RFB implementam a versão 2 do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 5280.

7.3.2. Extensões de LCR e de suas entradas

7.3.2.1. Neste item são descritas todas as extensões de LCR utilizadas pela AC CNDL RFB e sua criticalidade.

7.3.2.2. As LCRs da AC CNDL RFB e SRF obedecem a ICP - Brasil que define como obrigatórias as seguintes extensões:

7.3.2.2.1. Para LCRs emitidos pela AC CNDL RFB v2:

- a) "Authority Key Identifier": contém o hash SHA-1 da chave pública da AC que assina a LCR;
- b) "CRL Number", não crítica: contém um número sequencial para cada LCR emitida pela AC CNDL RFB;
- c) "Authority Information Access", não crítica, contendo endereço na Web onde se obtêm o arquivo p7b com os certificados da cadeia: <https://www.spcbrasil.org.br/produtos/produto/40-certificacaodigital>.

8. ADMINISTRAÇÃO DE ESPECIFICAÇÃO

8.1. Procedimentos de mudança de especificação

Qualquer alteração nesta DPC-AC CNDL RFB é submetida à aprovação do CG da ICP-Brasil. Esta DPC-AC CNDL RFB é atualizada sempre que uma nova PC implementada pela AC CNDL RFB o exigir.

8.2. Políticas de publicação e notificação

Esta DPC-AC CNDL RFB está disponível para a comunidade no endereço web <https://www.spcbrasil.org.br/produtos/produto/40-certificacaodigital>.

8.3. Procedimentos de aprovação

Esta DPC-AC CNDL RFB foi submetida à aprovação, durante o processo de credenciamento da AC CNDL RFB, conforme o determinado pelo documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6].

9. DOCUMENTOS REFERENCIADOS

9.1 Resoluções do Comitê-Gestor da ICP-Brasil

Os documentos abaixo são aprovados por Resoluções do Comitê-Gestor da ICP-Brasil, podendo ser alterados, quando necessário, pelo mesmo tipo de dispositivo legal. O sítio <http://www.iti.gov.br> publica a versão mais atualizada desses documentos e as Resoluções que os aprovaram.

Ref.	Nome do documento	Código
[2]	CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-09
[3]	CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-08

AC CNDL RFB
Declaração de Práticas de Certificação

[6]	CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-03
[7]	REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL	DOC-ICP-04
[8]	POLÍTICA DE SEGURANÇA DA ICP-BRASIL	DOC-ICP-02
[10]	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DE CERTIFICAÇÃO DAS AUTORIDADES CERTIFICADORAS DA ICP-BRASIL	DOC-ICP-05

9.2 Instruções Normativas da AC Raiz

Os documentos abaixo são aprovados por Instrução Normativa da AC Raiz, podendo ser alterados, quando necessário, pelo mesmo tipo de dispositivo legal. O sítio <http://www.iti.gov.br> publica a versão mais atualizada desses documentos e as Instruções Normativas que os aprovaram.

Ref.	Nome do documento	Código
[1]	CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP-BRASIL	DOC-ICP-03.01
[9]	PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL	DOC-ICP-01.01

9.3 Documentos da AC Raiz

Os documentos abaixo são aprovados pela AC Raiz, podendo ser alterados, quando necessário, mediante publicação de uma nova versão no sítio <http://www.iti.gov.br>.

Ref.	Nome do documento	Código
[4]	MODELO DE TERMO DE TITULARIDADE	ADE-ICP-05.A

10. LISTA DE ACRÔNIMOS

AC - Autoridade Certificadora
 AC Raiz - Autoridade Certificadora Raiz da ICP-Brasil
 AR - Autoridades de Registro
 ARV- Autoridades de Registro Vinculadas
 CEI - Cadastro Específico do INSS
 CG - Comitê Gestor
 CMM-SEI - Capability Maturity Model do Software Engineering Institute
 CMVP - Cryptographic Module Validation Program
 CN - Common Name
 CNE - Carteira Nacional de Estrangeiro
 CNPJ - Cadastro Nacional de Pessoas Jurídicas
 COBIT - Control Objectives for Information and related Technology
 COSO - Comitee of Sponsoring Organizations
 CPF - Cadastro de Pessoas Físicas
 DMZ - Zona Desmilitarizada
 DN - Distinguished Name
 DPC - Declaração de Práticas de Certificação
 ICP-Brasil - Infraestrutura de Chaves Públicas Brasileira
 IDS - Sistemas de Detecção de Intrusão
 IEC - International Electrotechnical Commission
 ISO - International Organization for Standardization
 ITSEC - European Information Technology Security Evaluation Criteria
 ITU - International Telecommunications Union
 LCR - Lista de Certificados Revogados
 NBR - Norma Brasileira
 NIS - Número de Identificação Social
 NIST - National Institute of Standards and Technology
 OCSP - On-line Certificate Status Protocol
 OID - Object Identifier
 OU - Organization Unit
 PASEP - Programa de Formação do Patrimônio do Servidor Público
 PC - Políticas de Certificado
 PCN - Plano de Continuidade de Negócio
 PIS - Programa de Integração Social
 POP - Proof of Possession
 PS - Política de Segurança
 PSS - Prestadores de Serviço de Suporte
 RFC - Request For Comments
 RG - Registro Geral
 SNMP - Simple Network Management Protocol
 TCSEC - Trusted System Evaluation Criteria
 TSDM - Trusted Software Development Methodology
 UF - Unidade de Federação
 URL - Uniform Resource Location