Declaração de Práticas de Negócios
da
Autoridade Registradora
do
SERPRO

(DPN AR SERPRO)

Versão 1.1 de Outubro de 2023

SUMÁRIO

CONTROLE DE ALTERAÇÕES

Versão	Data	Responsável	Motivo	Descrição
1.0	Março/2021	Lucia Castelli	Versão Inicial	Versão inicial compatível com a versão 1.1 do *WebTrust Principles and Criteria for Registration Authorities* – www.webtrust.org
1.0	Março/2021	Alice Vasconcellos	Aprovação	
1.0	Março/2022	Lucia Castelli	Atualização	Sem atualização necessária. Permanece compatível com a versão 1.1 do *WebTrust Principles and Criteria for Registration Authorities* – www.webtrust.org
1.0	Março/2022	Alice Vasconcellos	Aprovação	
1.1	Outubro/2023	Lucia Castelli	Atualização	Atualizado lista de Acs cadastradas na AR SERPRO(item 1.7).
1.1	Outubro/2023	Alice Vasconcellos	Aprovação	

1. Práticas de negócios da AR

1.1. Está Declaração de Práticas de Negócio da Autoridade de Registro do SERPRO (DPN AR SERPRO) se refere unicamente a Autoridade de Registro do SERPRO e que é utilizada pelas Autoridades Certificadoras (Quadro 1) vinculada à AR.

Os procedimentos, utilizados pela AR SERPRO, vinculada às ACs (Quadro 1), para a realização dos procedimentos gerais da AR para validação da solicitação de certificado, que compreende as seguintes etapas realizadas mediante a presença de forma física ou videoconferência do interessado, com base em documentos oficiais legalmente aceitos e pelo processo de identificação biométrica ICP-Brasil.

1.2. O endereço da página *web* (URL) da AR SERPRO é https://certificados.serpro.gov.br/arserpro/

1.3. Neste link estão publicados informações, referente a Autoridade de Registro do SERPRO, responsável pelo processo de recebimento, validação e encaminhamento de solicitação de emissão ou de revogação de certificados digitais, e de identificação de seus solicitantes.

1.4. Os critérios e procedimentos para credenciamento de uma AR estão definidos no documento DOC-ICP-03 [3].

1.5. Esta DPN AR SERPRO é administrada pelo SERPRO.

1.6. Contatos:

Administrativo:

Nome: Pedro Moacir Rigo Motta

Endereço: SGAN 601, Módulo V, Asa Norte, Brasília, Distrito Federal, CEP 70.836-900.

E-mail: certificados@serpro.gov.br

Telefone: (61) 2021-7957

Suporte:

Nome: Central de Serviços SERPRO

Página Web: http://www.serpro.gov.br/menu/suporte/css

E-mail: css.serpro@serpro.gov.br

Telefone: 0800 7282323

1.7. Autoridades Certificadoras que utilizam os serviços da AR SERPRO:

Autoridade Certificadora	Site	Tipo de Certificado
AC SERPRO	https://ccd.serpro.gov.br/acserpro	A1
AC SEFAZ CE	https://certificados.serpro.gov.br/csefazce/	A CF e-SAT
AC SERPRO SSL	https://certificados.serpro.gov.br/serprossl/	A1
AC SERPRO ACF	https://certificados.serpro.gov.br/serproacf/	A1 e A3

AC SERPRO ACF TS	https://certificados.serpro.gov.br/serproacfts/	T3
AC SERPRO RFB	https://certificados.serpro.gov.br/acserprorfb/	A1 e A3
AC SERPRO JUS	https://certificados.serpro.gov.br/acserprojus/	A3

Quadro 1: Autoridades Certificadoras que utilizam os serviços da AR SERPRO.

2. Gestão de Práticas Comerciais

A AR SERPRO segue os itens relevantes da Declaração de Práticas de Certificação (DPC) de cada AC em que está vinculada.

2.1. Gerenciando a Declaração de Práticas de Certificação da AC (DPC)

2.1. A AR SERPRO segue os itens relevantes da Declaração de Práticas de Certificação (DPC) atual das ACs(Quadro 1) em que está vinculada.

2.1.1. As responsabilidades pela contratação pela AC e a identificação das seções relevantes da DPC da AC são de conhecimento da AR SERPRO.

2.1.2. As alterações na DPC e PC de cada AC é informado à AR SERPRO.

2.2. Prestação de Serviços Adicionais

2.2. A AR não realiza serviços adicionais.

3. Controles Ambientais da Autoridade de Registro

3.1 Gerenciamento de Segurança

Os seguintes procedimentos são previstos para a segurança da AR:

- Os riscos de segurança são identificados e gerenciados;
- A segurança das instalações, sistemas e ativos de informação de AR acessados por terceiros é mantida.

3.1.1. A AR SERPRO utiliza a política de segurança da informação das ACs, que inclui controles físicos, pessoais, procedimentais e técnicos, e é aprovado pela ICP-Brasil e que é de conhecimento de todos os empregados da AR e das AC.

A Política de Segurança está disponível no site de cada AC, conforme Quadro 1.

3.1.2. A Política de Segurança:

A PS utilizada é da Autoridade Certificadora(Quadro 1) e tem por finalidade estabelecer as diretrizes de segurança que são adotadas.

A Política de Segurança das ACs tem os seguintes objetivos específicos:

a) Definir o escopo da segurança da AC;

b) Orientar, por meio de suas diretrizes, todas as ações de segurança, para reduzir riscos e garantir a integridade, sigilo e disponibilidade das informações dos sistemas de informação e recursos;

c) Permitir a adoção de soluções de segurança integradas; e

d) Servir de referência para auditoria, apuração e avaliação de responsabilidades.

3.1.3. A Política de Segurança abrange os seguintes aspectos:

a) Requisitos de Segurança Humana;

b) Requisitos de Segurança Física;

c) Requisitos de Segurança Lógica;

d) Requisitos de Segurança dos Recursos Criptográficos.

3.1.4. A PS das ACs se aplicam a todos os seus recursos humanos, administrativos e tecnológicos. A abrangência dos recursos citados refere-se tanto àqueles ligados a ela como em caráter permanente, quanto temporário.

3.1.5. Esta política é comunicada para todo o pessoal envolvido e largamente divulgada da AC, garantindo que todos tenham consciência da mesma e a pratiquem na organização.

3.1.6. Todo o pessoal recebe as informações necessárias para cumprir adequadamente o que está determinado nesta política de segurança.

3.1.7. Um programa de conscientização sobre segurança da informação está implementado para assegurar que todo o pessoal seja informado sobre os potenciais riscos de segurança e exposição a que estão submetidos os sistemas e operações da AC.

Especialmente, o pessoal envolvido ou que se relaciona com os usuários e são treinados sobre ataques típicos de engenharia social e como se proteger deles.

3.1.8. Os procedimentos são documentados e implementados para garantir que quando o pessoal contratado ou prestadores de serviços sejam transferidos, remanejados, promovidos ou demitidos, todos os privilégios de acesso aos sistemas, informações e recursos sejam devidamente revistos, modificados ou revogados.

3.1.9. Previsão de mecanismo e repositório centralizado para ativação e manutenção de trilhas, logs e demais notificações de incidentes. Este mecanismo é incluído nas medidas tomadas por um grupo encarregado de responder a este tipo de ataque, para promover uma defesa ativa e corretiva contra os mesmos.

3.1.10. Os processos de aquisição de bens e serviços, especialmente de Tecnologia da Informação – TI, estão em conformidade com a PS.

3.1.11. No que se refere a segurança da informação, considera-se proibido tudo aquilo que não esteja previamente autorizado pelo responsável da área de segurança da AC;

3.1.12. O processo de gerenciamento de riscos é revisto, no máximo anualmente, pela AC, para prevenção contra riscos, inclusive aqueles advindos de novas tecnologias, visando a elaboração de planos de ação apropriados para proteção aos componentes ameaçados

3.2. Classificação e gerenciamento de ativos

Os ativos da AR e as informações dos assinantes e usuários, recebem um nível apropriado de proteção com base nos riscos relevantes que foram identificados pela AR e pelas ACs e, de acordo com as práticas de negócios divulgadas pela AR e ACs em suas respectivas DPCs.

3.2.1. Todos os ativos da AR SERPRO são inventariados, classificados, permanentemente atualizados, e possuem gestor responsável formalmente designado

3.2.3. A AR SERPRO implementa a classificação de informações e controles de proteção associados para informações, com base nas necessidades de negócios e nos impactos de negócios associados a essas necessidades (com base nas expectativas das ACs para os quais os serviços estão sendo executados).

3.2.4. A classificação e o manuseio das informações são realizados de acordo com o esquema de classificação de informações e procedimentos documentados da AR.

3.3. Segurança Pessoal

Existem um conjunto de medidas e procedimentos de segurança, que são observados pelos prestadores de serviço e todos os empregados, necessário à proteção dos ativos da AC.

3.3.1. Disposições Gerais

3.3.1.1 Os normativos que tratam da segurança de pessoas estão descritos no DOC-ICP-02 [1] e no DOC-ICP-05 [4].

3.3.1.2 Não são admitidos estagiários nem funcionários terceirizados no exercício das atividades de Agente de Registro. Os Agentes de Registro são funcionários ou servidores da própria organização credenciada como AR junto à ICP-Brasil.

3.3.1.3 A AR envia à AC a relação atualizada dos Agentes de Registro em atividade, seus perfis qualificados e suas necessidades de acesso a informações do gerenciamento de ciclo de vida dos certificados. A AC deve mantém essa informação atualizada, organizada e consolidada, inclusive com o histórico das alterações realizadas, à disposição do ITI para os procedimentos de auditoria e fiscalização.

3.3.2. Documentação do Agente de Registro

3.3.2.1 Cada Agente de Registro que esteja atuando ou que já tenha atuado na AR deve possuir um dossiê, contendo:

a) contrato de trabalho ou cópia das páginas da carteira de trabalho onde consta o registro da contratação, termo de posse de servidor ou comprovante de situação funcional;

b) comprovante da verificação de antecedentes criminais;

c) comprovante da verificação de situação de crédito;

d) comprovante da verificação de histórico de empregos anteriores;

e) comprovação de escolaridade e de residência;

f) comprovante dos treinamentos realizados;

g) resultado da entrevista inicial, com a assinatura do entrevistador;

h) declaração em que afirma conhecer as suas atribuições e em que assume o dever de cumprir a Política de Segurança - PS da AC, as políticas e regras aplicáveis da ICPBrasil. Nessa declaração assume também o dever de manter a confidencialidade e exclusividade

de propriedade das informações disponibilizadas pela AC à AR e de manter sigilo, mesmo quando desligado da AR, sobre todas as informações e os processos executados na AR;

i) resultado da avaliação periódica, prevista no DOC-ICP-02 [1];

j) confirmação da AC quanto à inclusão do Agente em seu sistema de certificação.

3.3.2.2 Caso o Agente de Registro tenha sido desligado de suas atividades na AR, seu dossiê deve conter, também:

a) confirmação da AC quanto à desabilitação do Agente de Registro no sistema de certificação e no Cadastro de Agentes de Registros - CAR mantido no site do ITI;

b) declaração assinada pelo Agente de Registro de que não possui pendências, conforme previsto no item referente ao processo de liberação do DOC-ICP-02 [1];

c) resultado da entrevista de desligamento, com a assinatura do entrevistador.

3.3.2.3 Os documentos do item 3.3.2.1, que compõem o dossiê, devem ser examinados por uma das seguintes pessoas, que declarará, sob as penas da lei, a existência de tais documentos e que eles comprovam efetivamente que o Agente de Registro atende a todos os requisitos da ICPBrasil pertinentes:

a) Auditor interno da AR, cadastrado junto à ICP-Brasil conforme DOC-ICP-08 [6];

b) Auditor ou funcionário designado da Autoridade Certificadora à qual a AR se vincula; e

c) Representante Legal da própria AR, caso a AR não possua agente de registro como sócio.

3.3.2.4 Somente após o recebimento da solicitação de habilitação do Agente de Registro e da declaração prevista no item anterior, a AC pode incluí-lo nas bases de dados e conceder as permissões de acesso no sistema de certificação, sendo necessária para isso prévia autorização documentada do Gerente da AC ou do responsável por ele designado.

3.3.2.5 Os dossiês de todos os Agentes de Registro da AR ficam em um mesmo ponto de centralização da AC.

3.3.3. Treinamento

3.3.3.1 Todo Agente de Registro, na ocasião de sua admissão, deve receber treinamento documentado, com carga horária mínima de 16 (dezesseis) horas, sobre os seguintes temas:

a) princípios e mecanismos de segurança da AR;

b) sistema de certificação em uso na AC;

c) procedimentos de recuperação de desastres e de continuidade do negócio;

d) reconhecimento de assinaturas e validade dos documentos apresentados; e

e) outros assuntos relativos a atividades sob sua responsabilidade.

3.3.3.2 No treinamento sobre princípios e mecanismos de segurança são apresentados a Política de Segurança da AC[1], suas normas e procedimentos relativos ao trato de informações e/ou

dados sigilosos, com o propósito de desenvolver e manter uma efetiva conscientização de segurança, assim como instruir o seu fiel cumprimento.

3.3.3.3 O treinamento em reconhecimento de assinaturas e validade dos documentos apresentados é ministrado (ou preparado, quando se tratar de treinamentos tipo elearning) por empresa ou profissional especializado em grafotecnia.

3.3.4. Acompanhamento periódico

3.3.4.1 A AR acompanha o desempenho das funções de seus Agentes de Registro e realiza os avalia anualmente com o propósito de detectar a necessidade de atualização técnica e de segurança. Esse processo é documentado.

3.3.4.2 A AR renova bianualmente, para todos os seus Agentes de Registro, as verificações de antecedentes criminais e situação creditícia.

3.3.4.3 Para os casos em que o acompanhamento anual apontar a necessidade de suspensão ou desligamento do Agente de Registro, essa é solicitada de imediato à AC.

3.3.4.4 A AC arquiva os comprovantes relativos aos procedimentos acima no dossiê dos Agentes de Registro em seu poder.

3.3.5. Suspensão e Desligamento

3.3.5.1 Quando o Agente de Registro é suspenso ou desligado de suas atividades, a AR imediatamente providencia a revogação de suas permissões de acesso ao sistema de certificação da AC e permissões de acesso físico e lógico aos equipamentos e mecanismos inerentes à atividade de Agente de Registro. Esses processos são documentados e esses documentos são arquivados no dossiê do Agente, os quais deverão ser mantidos em poder da AC.

3.4. Segurança Física

Com base nos requisitos de risco da AC e nos requisitos estabelecidos em cada DPC pertinente da AC, a AR garante que:

3.4.1. O acesso físico às instalações e equipamentos da AR está limitado a indivíduos autorizados, protegido por perímetros de segurança restritos e operado sob controle de múltiplas pessoas;

3.4.2. Recepção: equipe para controlar o acesso físico restringindo o acesso ao local que abriga as operações da AR, apenas para o pessoal autorizado.

3.4.3. Existem portas corta-fogo nos perímetros de segurança em torno das instalações operacionais da AR como também alarmes e estão em conformidade com os regulamentos locais contra incêndio.

3.4.4. Sistemas de detecção de intrusos são instalados e testados regularmente para cobrir todas as portas externas do prédio que abriga as instalações operacionais da AR.

3.4.5. As instalações operacionais da AR são fisicamente bloqueadas e alarmadas quando desocupadas.

3.4.6. Todo o pessoal utiliza uma identificação visível.

3.4.7. O acesso às instalações operacionais da AR é controlado e restrito a pessoas autorizadas por meio do uso de controles de autenticação multifator.

3.4.8. Todo o pessoal que entra e sai das instalações operacionais da AR é registrado (ou seja, uma trilha de auditoria de todo o acesso é mantida com segurança). O uso de um sistema de crachá é suficiente para o pessoal permanente.

3.4.9. A entrada e a saída das instalações da AR são monitoradas por câmeras.

3.4.10. Os visitantes das instalações da AR são supervisionados e sua data e hora de entrada e saída são registradas.

3.4.11. O pessoal de serviços de suporte terceirizado tem acesso restrito às instalações operacionais seguras da AR e apenas quando necessário e esse acesso é autorizado e acompanhado.

3.4.12. Os direitos de acesso às instalações da AR são regularmente revisados e atualizados.

3.4.13. As estações de trabalho é localizado ou protegido de forma a reduzir os riscos de ameaças e perigos ambientais e as oportunidades de acesso não autorizado.

3.4.14. As estações de trabalho está protegido contra falhas de energia e outras anomalias elétricas.

3.4.15. Energia e telecomunicações, dentro das instalações que abrigam a operação da AR, o cabeamento que transporta dados ou os serviços da AR de suporte estão protegidos contra interceptação ou danos.

3.4.16. As estações de trabalho são mantidas de acordo com as instruções do fabricante e / ou outros procedimentos documentados.

3.4.17. Todos os itens das estações de trabalho que contêm mídia de armazenamento (discos fixos e removíveis) são verificados para garantir que não contenham dados confidenciais antes de serem descartados. A mídia de armazenamento que contém dados confidenciais é fisicamente destruída ou substituída com segurança antes do descarte ou reutilização.

3.4.18. Informações confidenciais ou críticas de negócios são bloqueadas quando não são necessárias e quando as instalações da AR estão desocupadas.

3.4.19. Os procedimentos exigem que os computadores pessoais e as estações de trabalho sejam desconectados ou protegidos por travas de chave, senhas ou outros controles quando não estiverem em uso.

3.4.20. A movimentação de materiais de / para as instalações da AR requer autorização prévia.

3.5 Gerência de Operações

A AR assegura:

- Operação correta e segura dos recursos de processamento de informações;
- O risco de falha dos sistemas de AR é minimizado;
- A integridade dos sistemas e informações de AR é protegida contra vírus e softwares mal-intencionados;

- Danos causados por incidentes de segurança e mau funcionamento são minimizados através do uso de relatórios de incidentes e procedimentos de resposta; e
- As mídias são manuseadas com segurança para protegê-las contra danos, roubo e acesso não autorizado.

3.6. Gerenciamento de acesso ao sistema

O acesso ao sistema da AR está limitado a indivíduos autorizados da seguinte maneira:

3.6.1. O sistema operacional e o acesso ao banco de dados são limitados a indivíduos autorizados com privilégios de tarefa predeterminados;

3.6.2. O acesso a segmentos de rede que abrigam o sistema da AR está limitado a indivíduos, aplicações e serviços autorizados; e

3.6.3. O uso do aplicativo da AR está limitado a indivíduos autorizados.

3.6.4. A atribuição e o uso de privilégios são restritos e controlados.

3.6.5. A atribuição de privilégios e senhas é controlada por meio de um processo de gerenciamento formal.

3.6.6. Os usuários são obrigados a seguir as políticas e procedimentos definidos na seleção e uso de senhas.

3.6.7. Os usuários são obrigados a garantir que o equipamento não supervisionado seja protegido.

3.6.8. O pessoal empregado pela AR tem acesso direto apenas aos serviços para os quais foi especificamente autorizado a usar. O caminho do terminal do usuário para os serviços de computador é controlado.

3.6.10. As conexões feitas por funcionários da AR ou sistemas da AR a sistemas de computador remotos são autenticadas.

3.6.11. Os sistemas operacionais e bancos de dados são configurados de acordo com os padrões de configuração do sistema do RA e periodicamente revisados e atualizados.

3.6.12. Os patches e atualizações do sistema operacional e do banco de dados são aplicados em tempo hábil, quando considerados necessários, com base em uma avaliação de risco.

3.6.13. O acesso ao sistema da AR tem um processo de logon seguro.

3.6.14. Todos os AGRs possuem um identificador único (ID do usuário) para seu uso pessoal e exclusivo para que as atividades possam ser rastreadas.

3.7. Desenvolvimento e Manutenção de Sistemas

As atividades de desenvolvimento e manutenção de sistemas da AR estão documentadas, testadas, autorizadas e implementadas adequadamente para manter a integridade do sistema da AR.

3.8. Gestão de Continuidade de Negócios

A AR garante que interrupções para os usuários do certificado digital são minimizados como resultado da cessação ou degradação dos serviços da AR.

A AR opera com a gestão de continuidade das operações no caso de um desastre, tais como:

- Desenvolvimento e teste de um plano de continuidade de negócios da AR;
- Processo de recuperação de desastres para componentes críticos do sistema da AR com base, no mínimo, nos requisitos das ACs, aos quais os serviços estão sendo prestados;
- Existe um site de contingência com a finalidade de armazenamento de backups de sistemas, dados e informações de configuração.

3.9. Monitoramento e Conformidade

Quanto ao monitoramento e conformidade, a AR SERPRO garante;

3.9.1. A AR está em conformidade com os requisitos legais, regulamentares e contratuais relevantes, com as ACs;

3.9.2. A conformidade com as políticas e procedimentos de segurança da AR é assegurada;

3.9.3. A eficácia do processo de auditoria do sistema é maximizada e a interferência de e para o processo de auditoria do sistema é minimizada; e

3.9.4. Uso não autorizado do sistema da AR é monitorado e detectado.

3.10. Registro de Auditoria

Quanto ao registros de auditoria, a AR SERPRO garante;

3.10.1. Eventos significativos (conforme definido pela AC) são registrados de forma precisa e apropriada;

3.10.2. A confidencialidade e integridade dos logs de auditoria atuais e arquivados;

3.10.3. Os registros de auditoria são arquivados completa e confidencialmente de acordo com as práticas comerciais divulgadas; e

3.10.4. Os registros de auditoria são revisados periodicamente por pessoal autorizado.

4. CONTROLES DE GERENCIAMENTO DE CICLO DE VIDA DO CERTIFICADO

A Autoridade de Registro do SERPRO gerencia o ciclo de vida do certificado através de controles.

4.1. Identificação do Titular

A confirmação da identidade de um indivíduo é realizada pela AR SERPRO, vinculada às ACs do quadro 1, mediante a presença de forma física ou videoconferência do interessado, com base em documentos oficiais legalmente aceitos e pelo processo de identificação biométrica ICP-Brasil.

Esta AR verifica a autenticidade da identidade de pessoas físicas e jurídicas titulares de certificados.

Para efeito de identificação de um indivíduo serão aceitos os documentos pessoais listados abaixo, em sua versão original oficial, podendo ser físico ou digital, com vistas a identificação de um indivíduo solicitante de certificado:

- Registro de identidade ou passaporte se brasileiro;
- Título de eleitor, com foto;
- Carteira Nacional de Estrangeiro – CNE, se estrangeiro domiciliado no Brasil;
- Passaporte, se estrangeiro não domiciliado no Brasil;

Na hipótese das biometrias do titular já estarem cadastradas na base da ICP-Brasil, e houver parecer positivo ao realizar a identificação biométrica, fica dispensada a apresentação dos documentos acima e o certificado poderá ser liberado para emissão.

Se faz também é necessário apresentar os seguintes documentos:

- Documento oficial com fotografia, no caso de certificados de tipos A4.
- Fotografia da face do requerente de um certificado digital ICP-Brasil, conforme disposto no DOC-ICP-05.03[5];
- Impressões digitais do requerente de um certificado digital ICP-Brasil, conforme disposto no DOC-ICP-05.03[5].

NOTA 1: Entende-se como cédula de identidade os documentos oficiais, físicos ou digitais, conforme admitidos pela legislação específica, 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: Os documentos digitais deverão ser verificados por meio de barramentos ou aplicações oficiais dos entes federativos

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

NOTA 4: 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 5: 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.

4.2. Identificação de uma organização

A confirmação da identidade de uma pessoa jurídica é feita com a presença do representante legal portando os documentos da organização legalmente aceitos.

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

Os documentos aceitos para confirmar a identidade da pessoa jurídica são:

Ato constitutivo, devidamente registrado em órgão competente;

Documentos de eleição dos administradores, quando aplicável;

Lei de criação ou documento oficial de constituição no caso de pessoa jurídica criada ou autorizada por lei.

Comprovante de Inscrição e de Situação Cadastral do CNPJ.

4.3. Verificação do dossiê do certificado

Os documentos em papel, os quais não existam formas de verificação por meio de barramentos ou aplicações oficiais, deverão ser verificados seguindo os requisitos abaixo.

- Por Agente de Registro distinto do que realizou a etapa de identificação;
- Pela AR ou ainda AR própria do PSS da AC;
- Antes do início da validade do certificado, devendo este ser revogado automaticamente caso a verificação não tenha ocorrido até o início de sua validade.

4.4. Identificação e autenticação para pedidos de novas chaves antes da expiração

Um novo certificado poderá ser requerido pelo solicitante antes da expiração de seu certificado vigente, no qual deverá enviar à AC uma solicitação, por meio eletrônico, assinada digitalmente com o uso de um certificado de assinatura digital de mesmo nível de segurança do certificado a ser renovado.

O processo de identificação e autenticação para rotinas de novas chaves antes da expiração poderá ser conduzido segundo uma das seguintes possibilidades:

- Adoção dos mesmos requisitos e procedimentos exigidos para a solicitação do certificado;
- A 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, permitida tal hipótese apenas para os certificados digitais de pessoa física;

5. SOLICITAÇÃO DO CERTIFICADO

Os requisitos e procedimentos para solicitação de emissão do certificado por esta AR são:

- Confirmação da identidade da pessoa física ou jurídica titular do certificado.
- Assinatura do Termo de Titularidade e Responsabilidade pelo titular ou responsável pelo uso do certificado;
- Autenticação biométrica do Agente de Registro responsável pela identificação e verificação do certificado.

6. RENOVAÇÃO ONLINE

Para que o cliente esteja apto para a Emissão Certificado Digital Online é necessário que alguns critérios sejam obedecidos, tais como:

- Possuir Certificado PF A3 válido do representante legal da organização Para que seja possíveis emissões de Certificados Digitais de PJ, a partir de um Certificado Digital PF, podendo ter sido emitido por qualquer AC;
- Possuir Certificado PJ A3 válido da organização para emissões de certificados PJ a partir de um PJ, podendo ter sido emitido por qualquer AC;
- Para ambos os casos (citados no item 1 e 2) deverão possuir atos constitutivos que sejam possíveis ser validados/consultados na íntegra seja em sites da Junta Comercial, ou em aplicações oficiais do orgão de registro;
- No caso de emissão de um Certificado Digital de um PJ a partir de um PF A3 válido deverá ser confirmado se o titular do certificado pessoa física é o representante legal da organização;
- Ter as biometrias do representante legal cadastradas no PSBIO.

7. ATENDIMENTO POR VIDEOCONFERÊNCIA

A emissão de Certificados Digitais por meio de videoconferência é uma opção do solicitante, e não um requisito obrigatório para emissões genéricas.

Ainda, para que haja a realização da emissão dos Certificados Digitais por videoconferência, é necessário cumprir os requisitos:

- Cliente precisa realizar o agendamento no link correspondente à sua AR
- Todos os documentos enviados à AR, devem ser digitalizados de forma colorida. Fotografias também são aceitas, desde que sejam nítidas.
- Para Certificados Digitais PJ, o contrato/ato constitutivo deve permitir a validação eletronicamente nos sites e aplicações oficiais dos órgãos de registro, nos casos de documentos eletrônicos Já os atos físicos que são registrados nas Juntas Comerciais precisam permitir a consulta do registro do Ato.
- Para Certificados Digitais PJ, a Certidão Simplificada, se válida, substuiu o Ato Constitutivo.

Os equipamentos necessários para a emisão por videoconferência são: Computadores, desde que tenham webcam, microfone e acesso à internet Smartphones, com câmera frontal e acesso à internet.

8. GERAÇÃO E INSTALAÇÃO DO PAR DE CHAVES

Quando o titular de certificado for uma pessoa física, esta será a responsável pela geração dos pares de chaves criptográficas. Quando o titular for uma pessoa jurídica, este indicará por seu

representante legal no momento da emissão, a pessoa responsável pela geração e uso do certificado.

O armazenamento do certificado deverá obedecer à Política de Certificado correspondente, sendo:

Tipo do Certificado	Mídia Armazenadora
A1	Repositório protegido por senha e/ou identificação biométrica, cifrado por software na forma definida acima
A3	Hardware criptográfico, homologado junto à ICP-Brasil ou com certificação INMETRO.
A4	Hardware criptográfico, homologado junto à ICP-Brasil ou com certificação INMETRO.
T3	Hardware criptográfico, homologado junto à ICP-Brasil ou com certificação INMETRO.
A CF-e-SAT	Hardware criptográfico

9. Revogação de Certificados

As solicitações de revogação de certificados validados são processadas dentro do prazo, de acordo com as práticas comerciais relevantes da AC.
O certificado digital poderá ser revogado antes da expiração do prazo de validade.

9.1 Circunstância para revogação

A revogação poderá ser feita pelos seguintes motivos:

- Quando constatada emissão imprópria ou defeituosa;
- Quando for necessária a alteração de qualquer informação constante no certificado;
- No caso de comprometimento da chave privada correspondente ou da mídia armazenadora;
- Por determinação judicial;
- Quando o responsável pelo uso se destituir da função;
- Por razões comerciais;
- Risco de fraude.

9.2. Quem pode solicitar revogação

A solicitação de revogação de um certificado somente poderá ser feita:

- Por solicitação do titular do certificado;
- Por solicitação do responsável pelo certificado, no caso de certificado de pessoas jurídicas;

- Por solicitação de empresa ou órgão, quando o titular do certificado fornecido por essa empresa ou órgão for seu empregado, funcionário ou servidor;
- Por determinação da AC;
- Por determinação da AR;
- Por determinação do Comitê Gestor da ICP-Brasil ou da AC Raiz.

9.3. Procedimentos para solicitação de revogação

- O solicitante da revogação de um certificado deve ser identificado;
- A solicitação de revogação é feita através de um formulário específico, permitindo a identificação inequívoca do solicitante;
- O procedimento para revogação do certificado pode ser realizado por todos os Agentes de Registros habilitados na AR;
- As solicitações de revogação, bem como as ações delas decorrentes deverão ser registradas e armazenadas;
- As justificativas para a revogação de um certificado são documentadas;
- O processo de revogação de um certificado terminará com a geração e a publicação de uma LCR que contenha o certificado revogado.

10. OBRIGAÇÕES DA AR:

- Confirmar a identidade do solicitante do certificado;
- Encaminhar a AC solicitação de emissão ou revogação do certificado;
- Manter a conformidade dos seus processos, procedimentos e atividades com as normas, critérios, práticas e regras estabelecidas pela AC vinculada e pela ICP-Brasil.

11. OBRIGAÇÕES DO TITULAR DO CERTIFICADO

- Fornecer, de modo completo e preciso, todas as informações necessárias para sua identificação;
- Garantir a proteção e o sigilo de suas chaves privadas, senhas e dispositivos criptográficos;
- Utilizar seus certificados de modo apropriado;
- Informar à AC emitente qualquer comprometimento de sua chave privada e solicitar a imediata revogação do certificado correspondente.

12. Referências Bibliográficas

Ref.	Nome do Documento	DOC
[1]	POLÍTICA DE SEGURANÇA DA ICP-BRASIL	**DOC-ICP-02**
[3]	CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	**DOC-ICP-03**

[4]	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DE CERTIFICAÇÃO DAS AUTORIDADES CERTIFICADORAS DA ICP-BRASIL	**DOC-ICP-05**
[5]	PROCEDIMENTOS PARA IDENTIFICAÇÃO BIOMÉTRICA NA ICP-BRASIL	**DOC-ICP-05.03**
[6]	CRITÉRIOS E PROCEDIMENTOS PARA AUDITORIA DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	**DOC-ICP-08**

8.2. Os documentos referenciados abaixo são de responsabilidade da *WebTrust*, e se encontram no link: www.webtrust.org