Declaração de Práticas de Negócios
da
Autoridade Registradora
MPDG

(DPN AR MPDG)

Versão 1.0 de Janeiro de 2026

SUMÁRIO

CONTROLE DE ALTERAÇÕES

Versão	Data	Responsável	Motivo	Descrição
1.0	Fevereiro/2026	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	Fevereiro/2026	Alice Vasconcellos	Aprovação	

1. Práticas de negócios da AR

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

Os procedimentos, utilizados pela AR MPDG, vinculada às ACs (Quadro 1), para a realização dos procedimentos gerais da AR para validação da solicitação de certificado, que compreende as etapas listados nos itens 4 e 5.

1.2. No link https://www.serpro.gov.br/links-fixos-superiores/pss-serpro , está publicado essa DPN AR MPDG.

1.3. Esta DPN AR MPDG é administrada pelo SERPRO

1.5. 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.MPDG@MPDG.gov.br

Telefone: 0800 7282323

1.6. Autoridades Certificadoras que utilizam os serviços da AR MPDG:

Autoridade Certificadora	Site	Tipo de Certificado
AC SERPRO RFB	https://certificados.serpro.gov.br/acserprorfb/	**SerproID**: Certificado em nuvem, utilizando telefone móvel; **A3-Token**: Certificado Digital com fornecimento do TOKEN; **A3** – Certificado Digital sem fornecimento do TOKEN, para servidores que já possuem certificados com token com um certificado anterior.
AC SERPRO ACF	https://certificados.serpro.gov.br/acserproacf/	

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

2. Gestão de Práticas Comerciais

A AR MPDG opera por meio de módulo eletrônico, utilizando o sistema de certificação digital integrado à plataforma SouGov.br (https://www.gov.br/servidor/pt-br/assuntos/sou-gov),via web ou aplicativo, para emissão de certificados digitais, pode ser realizada por qualquer funcionário público, desde que o Órgão de lotação do funcionário já tenha contratado essa modalidade junto ao SERPRO, exclusivamente, ou seja, não existe venda dos certificados pela AR MPDG.

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

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

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:

3.1.1. A AR MPDG 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.

As políticas de segurança das informações aplicáveis ao funcionamento do Módulo Eletrônico da AR MPDG, com base nos requisitos estabelecidos na Declaração de Práticas de Certificação (DPC) da AC SERPRO RFB e AC SERPRO ACF, nas Políticas de Certificado vigentes e nas boas práticas da ICP-Brasil.

Os controles de segurança da informação estão implementados de forma satisfatória e em conformidade com os padrões estabelecidos pela ICP-Brasil e pela AC vinculada.

3.1.2. A Política de Segurança:

Existência de Política de Segurança (PS) da entidade, com diretrizes atualizadas;

• Controles de acesso lógico ao sistema de emissão de certificados;

• Mecanismos de autenticação forte para aprovadores e usuários do sistema;

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;

3.1.13 Os riscos de segurança são identificados e gerenciados pela AR MPDG com apoio do SERPRO.

3.2. Classificação e gerenciamento de ativos

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. A AR é um sistema eletrônico e portanto não possuem ativos diretos.

3.2.3. A AR MPDG implementa a classificação de informações publicado pelo SERPRO.

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

3.3. Segurança Pessoal

Considerando que o Módulo Eletrônico da AR MPDG opera exclusivamente por meio digital, os procedimentos relacionados à Segurança de Pessoal, descritos nos itens 2.2.1 e 2.2.2 do DOC-ICP-03.01, não se aplicam da mesma forma que em Autoridades de Registro convencionais.

Neste modelo, não há atuação de Agentes de Registro em processos de atendimento presencial, sendo as validações realizadas por um Aprovador, de forma automatizada, com base em sistemas integrados à base biométrica oficial, conforme previsto no DOC-ICP-05.

A autorização da emissão dos certificados digitais fica sob responsabilidade dos Aprovadores Internos da entidade, que realizam a liberação das solicitações diretamente no ambiente digital da AR.

3.3.1. Disposições Gerais

3.3.1.1 Os normativos que tratam da segurança de pessoas da AC, estão descritos no DOC-ICP-02 [1] e no DOC-ICP-05 [2

].

3.3.1.2 Os Agentes de Registro são servidores da própria organização credenciada como AR e são denominados como Autorizadores.

3.3.1.3 Não se aplica.

3.3.2. Documentação do Agente de Registro

Nessa AR MPDG estamos tratando de um sistema eletrônico e, portanto, os Agentes de Registros, são denominados Aprovadores que, quando necessário, exercem o papel de um AGR mas que são do próprio orgão, respeitando o grau de hierarquia com relação ao solicitante do certificado. Seu dossiê faz parte da autarquia em que o mesmo está vinculado.

3.3.3. Treinamento

O treinamento é online no próprio site do Sougov.br - Certificado Digital — Portal do Servidor.

3.3.4. Acompanhamento periódico

Não se aplica.

3.3.5. Suspensão e Desligamento

Para o solicitante a posse do certificado deve ser tratada pelo órgão. Para o autorizador, no caso de aprovação por chefia direta, ao logar, valida a condição da pessoa se ainda estar como chefe, disponibiliza para aprovação, apenas se ainda atender a esta condição.

Para o autorizador, no caso de grupo de aprovadores, deve ser comunicado a gestão do SERPRO para que o funcionário seja desabilitado como aprovador.

3.4. Segurança Física

Não se aplica, uma vez que estamos tratando de um sistema eletrônico, operado, diretamente pelos servidores ligados a um órgão, ou, quando necessário, operado por um Aprovador, também ligado diretamente a esse órgão.

3.5 Gerência de Operações

A AR assegura:

- O risco de falha dos sistemas de AR é minimizado através de um PCN testado;
- 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

3.6. Gerenciamento de acesso ao sistema

Detalhado no item 5.0

3.7. Desenvolvimento e Manutenção de Sistemas

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

3.8. Gestão de Continuidade de Negócios

A AR MPDG possui um PCN testado anualmente e que tem como áreas responsáveis:

SERPRO → responsável por coordenar e fornecer informações referentes ao serviço da Autoridade de Registro e das Autoridades Certificadoras(envolvidas);

Os cenários previstos no PCN são: Indisponibilidade do SouGov.br;

- Impossibilidade da aprovação eletrônica do certificado;
- Indisponibilidade do módulo de aprovação da AR eletrônica no SCDS(Sistema de Certificação Digital do SERPRO);
- Falha nos servidores ou infraestrutura do SCDS ou do SERPRO;
- Outras causas que comprometam o uso do equipamento.

3.9. Monitoramento e Conformidade

Quanto ao monitoramento e conformidade, a AR MPDG 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.

3.10. Registro de Auditoria

Quanto ao registros de auditoria, a AR MPDG 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 estão arquivados;

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

3.10.4. Os registros transacionais apresentam consistência, completude e rastreabilidade, estando em conformidade com os padrões técnicos e normativos exigidos pela ICP-Brasil para ambientes de operação exclusivamente eletrônicos

4. CONTROLES DE GERENCIAMENTO DE CICLO DE VIDA DO CERTIFICADO

A Autoridade de Registro MPDG 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 MPDG, 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.

4.1.1 Identificação Biométrica

Conforme previsto na normativa, o processo de validação da identidade do titular é realizado de forma automatizada e obrigatoriamente integrado a bases biométricas oficiais, garantindo a autenticidade da identificação.

O procedimento ocorre no momento da solicitação do certificado, por meio da captura e comparação de imagens faciais do requerente, com as bases do Governo Federais habilitadas para esse fim.

O sistema valida a qualidade da imagem coletada e em caso de atendimento aos critérios mínimos - similaridade facial superior a 85%, a solicitação é formalizada e ficará disponível para apreciação por parte do Aprovador.

5. SOLICITAÇÃO DO CERTIFICADO

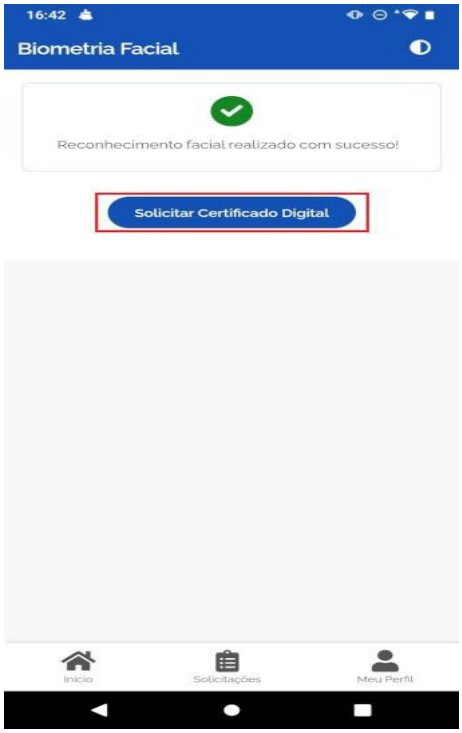
O processo de emissão de certificados digitais no módulo eletrônico da AR MPDG segue um fluxo estruturado, priorizando a segurança, a autenticidade e a integridade das informações, por meio de webservice seguro, utilizando RESTful sobre HTTPS e com autenticação via OAuth 2.0.

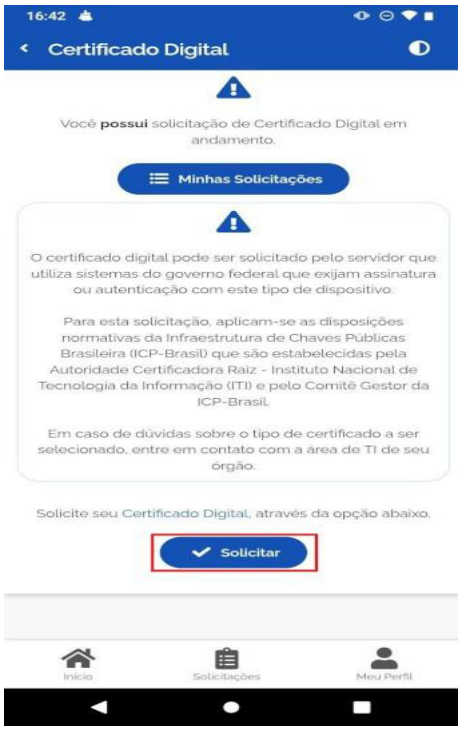
Após o recebimento, o sistema da AC envia um e-mail ao solicitante com instruções para a continuidade do processo.

A solicitação se inicia pelo aplicativo SOUgovbr, conforme as figuras abaixo:

O processo contempla as etapas de requisição, validação, aprovação e emissão, sendo executado de forma digital, com autenticação por login único e validação biométrica facial, garantindo a autenticidade do titular no momento da emissão do certificado.

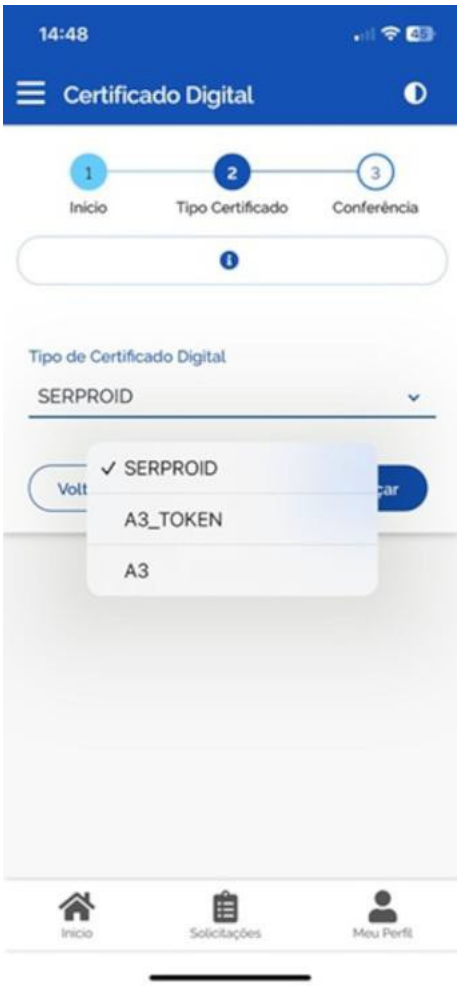
O solicitante realiza um auto coleta facial através da câmera do dispositivo, sendo orientado pelo sistema. A imagem é validada conforme os critérios mínimos da solução PSBio. Em caso de qualidade adequada, a solicitação é formalizada e disponibilizada ao Aprovador.

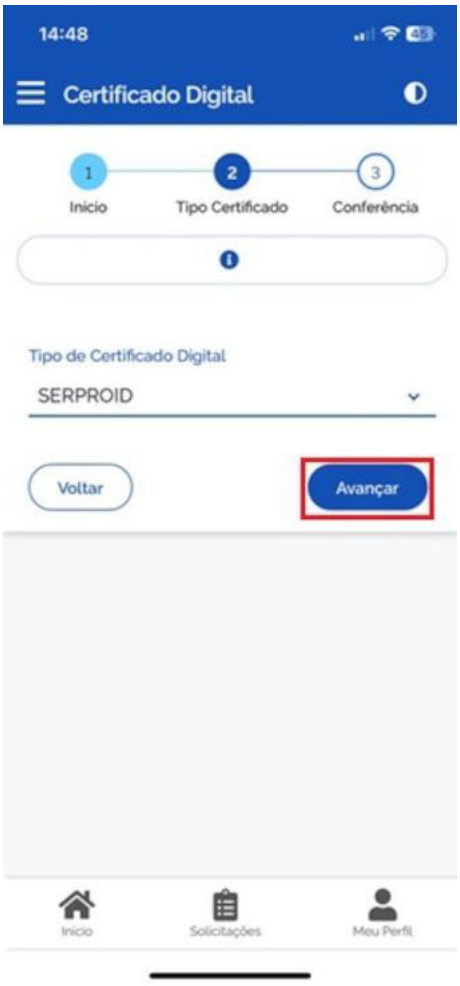




O fluxo é automatizado, com registro eletrônico de logs, conferência documental digital e assinatura do termo de titularidade pelo requerente e pelo aprovador.

Nas evidências acima, o requisitante do certificado deverá conferir se o nome dos superiores hierárquicos (chefia imediata e superior) estão corretos, pois eles são os Aprovadores validados para autorizar a emissão do certificado.





Para casos em que o requisitante tenha dúvidas sobre qual tipo de certificado escolher, deverá entrar em contato com a área de TI de seu respectivo órgão, para verificar qual o tipo de certificado a ser emitido, entre:

•SerproID – certificado SerproID em nuvem com utilização no telefone celular;

•A3_TOKEN – certificado digital com fornecimento do Token (pendrive) pelo SERPRO;

•A3 – Certificado digital sem fornecimento do Token, para os casos em que o servidor já possui Token com um certificado anterior.


Certificado Digital
1 Início
2 Tipo Certificado
3 Conferência
Tipo de Certificado
Certificado
Superiores Hierárquicos
Chefe Imediato
Nome
Função SUPERINTENDENTE
Unidade
Chefe Superior
Nome
Função DIRETOR DE DEPARTAMENTO
Unidade
Início
Solicitações
Ajuda
Meu Perfil

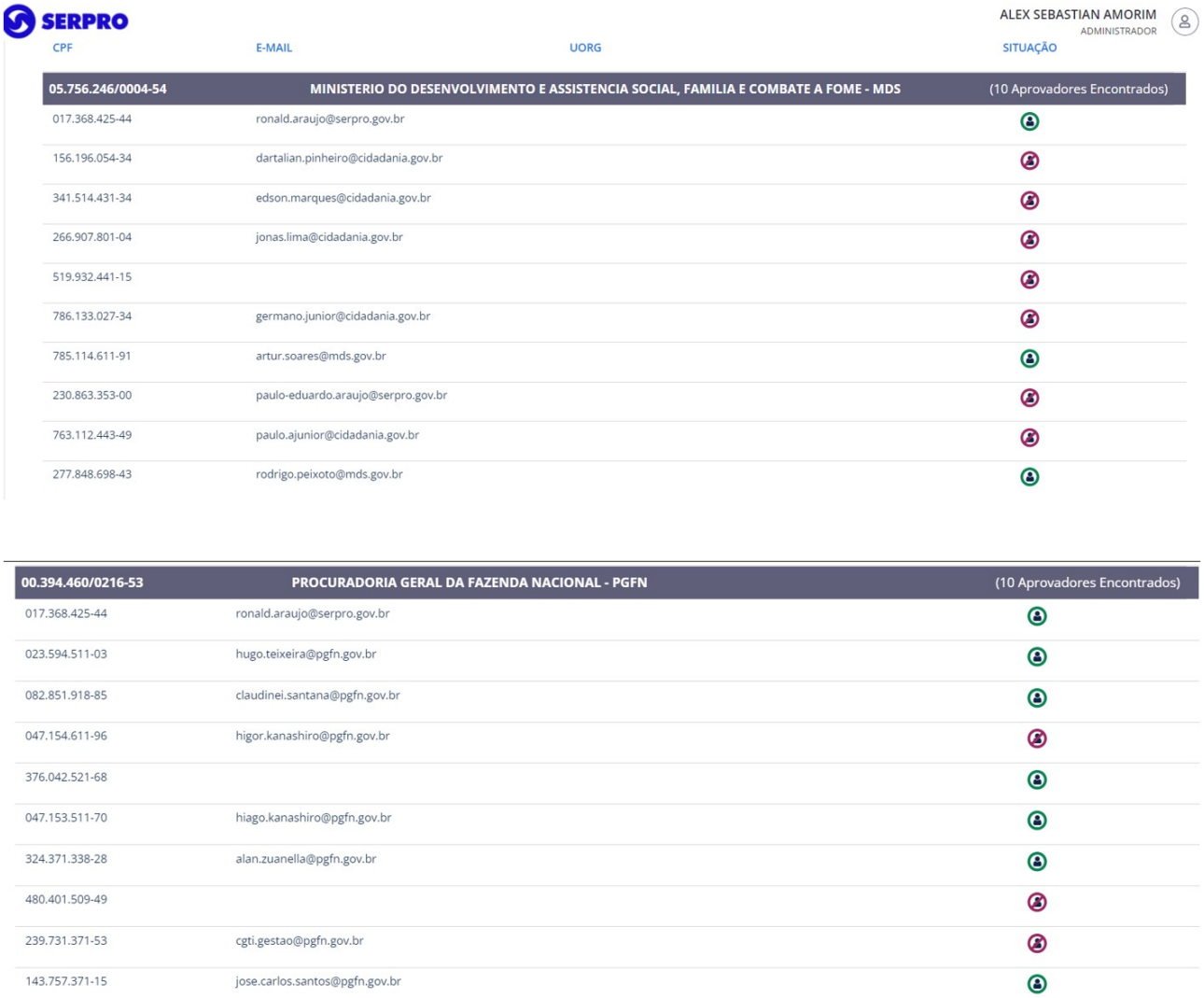

Certificado Digital
Função SUPERINTENDENTE
Unidade
Chefe Superior
Nome
Função DIRETOR DE DEPARTAMENTO
Unidade
Chefe Superior
Nome
Função SECRETARIO
Unidade
Voltar
Solicitar
Início
Solicitações
Ajuda
Meu Perfil


Solicitação enviada com sucesso.
Função SUPERINTENDENTE
Unidade
Chefe Superior
Nome
Função DIRETOR DE DEPARTAMENTO
Solicitação enviada para análise
Pronto, agora você pode aguardar a aprovação do seu certificado. Você receberá um e-mail com a senha para acesso ao certificado após a aprovação do mesmo.
Início
Minhas Solicitações
Unidade
Voltar
Solicitar
Início
Solicitações
Ajuda
Meu Perfil

Com os passos acima, o requisitante finaliza o processo de solicitação do certificado digital, que será avaliada pelo respectivo Aprovador.

5.1. Fluxo de Aprovação e Emissão de Certificados

Finalizado o processo de solicitação do certificado, o Aprovador, por sua vez, acessa o módulo eletrônico da AR com autenticação por certificado digital ICP-Brasil tipo A3, visualiza as solicitações pendentes e realiza a análise biométrica.



O sistema verifica automaticamente se há correspondência biométrica com as bases oficiais - PSBio. Caso a similaridade facial seja inferior a 85%, a aprovação só poderá ocorrer mediante justificativa por escrito.

Se a solicitação for aprovada, o Aprovador é direcionado à tela de conferência e assinatura do Termo de Titularidade, que formaliza a aprovação da emissão. Após essa etapa, o solicitante recebe um novo e-mail com as instruções para instalação do certificado, seja ele armazenado em token/cartão ou em nuvem.

Por fim, o solicitante também assina o Termo de Titularidade, agora já assinado previamente pelo Aprovador. O termo, com ambas as assinaturas digitais, é anexado ao dossiê do certificado, concluindo o processo de emissão.

6. RENOVAÇÃO ONLINE

Não está previsto para a AR MPDG.

7. ATENDIMENTO POR VIDEOCONFERÊNCIA

O atendimento por video não é uma opção do solicitante no caso da ARMPDG ele acontece quando não tem um aprovador ou quando o sistema não consegue identificar a identidade do solicitante.

8. GERAÇÃO E INSTALAÇÃO DO PAR DE CHAVES

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

Tipo do Certificado	Mídia Armazenadora
A3 - Nuvem	Repositório protegido(HSM) por senha e/ou identificação biométrica, cifrado por software.
A3	Hardware criptográfico, homologado junto à ICP-Brasil ou com certificação INMETRO.

9. Revogação de Certificados

9.1 Circunstância para revogação

A revogação poderá ser feita pelos seguintes motivos:

Quando constatada emissão imprópria ou defeituosa ou com alguma informação constante no certificado que precisa ser alterado;

No caso de comprometimento da chave privada correspondente ou da mídia armazenadora;

Por determinação judicial;

Quando o responsável pelo uso se destituir da função;

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 órgão em que o solicitante é 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

As solicitações de revogação de certificados pode ser realizada pelo próprio solicitante pela página https://certificadodigital.serpro.gov.br/revogacao ou por um Agente de Registro / Supervisor da AR SERPRO via SCDS-AR.

10. OBRIGAÇÕES DA AR:

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 ao órgão 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**
[2]	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DE CERTIFICAÇÃO DAS AUTORIDADES CERTIFICADORAS DA ICP-BRASIL	**DOC-ICP-05**

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