

MINISTÉRIO DA ECONOMIA

Secretaria Especial de Desburocratização, Gestão e Governo Digital

PRÁTICAS E PROCEDIMENTOS PARA VALIDADORES DE ACESSO DIGITAL

1 INTRODUÇÃO

1.1 Visão Geral

1.1.1 O credenciamento de validadores de acesso digital será precedido de análise e verificação de conformidade com os critérios estabelecidos em Portaria Nº 2.154 da SEDGGME e Portaria Conjunta ITI/CC/PR SGD/SEDGG/ME Nº 1, de 8 de setembro 2021. As diretrizes destas portarias têm em vista viabilizar ao cidadão meios seguros de validação de identidade biométrica, biográfica e documental em processos de identificação digital utilizados na plataforma de serviços digitais gov.br e padrões de referência para as assinaturas eletrônicas avançadas.

1.2 Objetivo

1.2.1 Este documento tem como objetivo somente orientar o proponente em relação a comprovação das práticas e dos procedimentos requeridos e recomendados para o perfeito desempenho das funções de validador de acesso digital. Quaisquer comentários ou dúvidas envie um e-mail para int-assinatura-govbr@economia.gov.br

2 VALIDAÇÃO DE IDENTIDADE

Os procedimentos de validação de identidade do cidadão serão definidos pelo próprio proponente com base no que é solicitado nas portarias para a prestação do serviço. Estes procedimentos podem ser documentados e protocolados junto à Secretaria de Governança Digital (SGD) do Ministério da Economia (ME). Desde já é importante destacarmos o estabelecido na portaria em relação aos seguintes pontos:

- a) as formas de validação concedidas de acordo com a natureza jurídica do proponente;
- b) o proponente integrado a Plataforma de Autenticação Digital do Cidadão - Login Único é previamente considerado validador de acesso digital, caso atenda requisitos do Decreto nº 10.543/2020;
- c) o proponente aprovado no processo de credenciamento de Autoridade Certificadora junto ao Instituto Nacional de Tecnologia da Informação é dispensado da comprovação de alguns requisitos da portaria.

2.1. Validação biográfica e documental

2.1.1. Com o propósito de atestar atendimento aos critérios para validação biográfica e documental do cidadão, recomendamos ao proponente documentar seus processos e procedimentos empregados para validação de acordo com o tipo de documento de identificação apresentado pelo requerente. Responder as seguintes perguntas pode ajudá-lo a definir seu processo de validação:

- Quais procedimentos são empregados para garantia de autenticidade deste documento?
- Quais procedimentos são empregados para verificação das informações junto a entidade que realiza a emissão deste documento?

- Quais os procedimentos empregados para verificar que a identidade pertence à pessoa que a está reivindicando?

Sabemos que existem casos em que podem ser utilizados mais de um procedimento para coletar as evidências necessárias para a validação. Consideramos adequado registrar todos eles na documentação.

2.1.2. Para validação biográfica realizada remotamente é aconselhável especificar os procedimentos, as principais funcionalidades e interfaces envolvidas, empregados mediante a utilização de tecnologias, que possibilitam esta modalidade de validação.

2.1.3. Para efeito de identificação da pessoa, o documento de registro de identidade deve ser apresentado, em sua versão oficial original, podendo ser física ou digital, por meio de aplicação oficial do ente federativo. Entende-se como registro de identidade os documentos oficiais, físicos ou digitais, 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. Na lista abaixo relacionamos todos os documentos válidos como registro de identidade com a sua legislação específica:

- Carteira de identidade (LEI Nº 7.116, DE 29 DE AGOSTO DE 1983.)
- Carteira profissional (LEI Nº 6.206, DE 7 DE MAIO DE 1975.)
- Passaporte (DECRETO Nº 5.978 DE 4 DE DEZEMBRO DE 2006.)
- Carteira de identificação funcional (DECRETO Nº 10.266, DE 5 DE MARÇO DE 2020)
- DNI (LEI Nº 13.444, DE 11 DE MAIO DE 2017.)
- CNH e CNH Digital (LEI Nº 9.503, DE 23 DE SETEMBRO DE 1997)
- RIC (DECRETO Nº 7.166, DE 5 DE MAIO DE 2010.)

2.2 Validação biométrica

2.2.1. Para atestar atendimento aos critérios para validação biométrica, recomendamos documentar os procedimentos, as principais funcionalidades e interfaces envolvidas na identificação biométrica do requerente. Podem ser mencionados quais os dados biométricos são coletados, os equipamentos utilizados para a coleta desses dados e também as especificações técnicas dos sistemas próprios ou de fornecedores contratados para atender a esta necessidade. Novamente aqui sugerimos ao proponente responder as seguintes perguntas para ajudá-lo a definir o seu processo de validação:

- O sistema utilizado associa a pessoa às informações biométricas que pertencem à identidade do requerente (isso é conhecido como verificação 1:1)?
- O sistema é capaz de confirmar que a pessoa é real (realiza prova de vida)?
- É utilizada alguma base biométrica de governo para realizar a validação biométrica? Se sim, qual?

2.2.2. Também recomendamos ao proponente apresentar os aspectos técnicos e operacionais destinados a assegurar a confiabilidade dos sistemas que operam na identificação biométrica, bem como os aspectos relacionados à interface de comunicação com base de dados governamentais admitidas para fins de batimento biométrico.

3.CONTROLES OPERACIONAIS, INSTALAÇÃO E APARELHOS

O validador de acesso digital credenciado é autorizado a fornecer meios de validação de identidade para o cidadão. Deste modo, ainda que não seja reconhecido como um agente público, acreditamos que é prudente ao validador considerar os princípios que devem orientar o atendimento ao usuário dos serviços públicos da administração pública, prescritos na Lei nº 13.460/2017 (Código de Defesa do Usuário de Serviços Públicos).

3.1. Atendimento ao público

3.1.1. Para o registro da documentação que ateste o efetivo atendimento ao público recomendamos ao proponente apresentar as suas formas de atendimento, suas orientações e práticas em relação à conduta de atendimento que estão em uso em sua organização.

3.1.2. Os atendimentos realizados de forma remota, por meio de soluções tecnológicas, podem ter documentados as suas informações relativas ao serviço, seu funcionamento, bem como se o serviço foi construído atendendo aos padrões de usabilidade e acessibilidade.

3.2. Instalação física e aparelhamento

3.2.1. Sobre o atendimento a este critério o proponente pode documentar, por meio de fotografias ou vídeos, os locais onde são realizados os procedimentos de validação da identidade. No caso de pontos de atendimento presenciais: os acessos, as estações de trabalho dos atendentes e os locais de espera do cidadão.

3.2.2. É recomendável apresentar os controles de ativo imobilizado utilizados, que devem ser adequados à realização de suas atividades. Além disso, recomendamos que os controles de ativos contenham inventários patrimoniais com pelo menos as seguintes informações: descrição, marca, modelo e nota fiscal do equipamento, se houver.

3.3. Pessoal Qualificado

3.3.1 Para assegurar que os funcionários entendam suas responsabilidades e sejam adequados aos papéis para os quais são considerados, é recomendável a realização de processo de seleção para o recrutamento e a assinatura de termo e condições de emprego.

3.3.2. É recomendável realizar treinamentos constantes dos colaboradores sobre os seguintes assuntos:

- a) conduta e procedimentos para atendimento ao público;
- b) normas e procedimentos para validação de identidade;

4 SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE DOS DADOS NO PROCESSO DE VALIDAÇÃO

4.1. Privacidade dos dados

Os agentes de tratamento são os responsáveis pelo tratamento dos dados pessoais sujeitos às regras da LGPD e à fiscalização da ANPD. O controlador é quem toma as decisões referentes ao tratamento de dados pessoais e o operador é aquele que realiza o tratamento de dados pessoais em nome do controlador.

4.1.1. O validador de acesso digital credenciado é agente de tratamento de dados pessoais. Deste modo, deve realizar a prestação do serviço nos termos da Lei nº 13.709, de 14 de agosto de 2018 Lei Geral de Proteção de Dados Pessoais (LGPD), considerando seus princípios e requisitos.

4.2. Declarações de Práticas de Certificação (DPC) e requisitos de segurança da informação

4.2.1. O validador de acesso deve dispor em suas DPC e Políticas de Certificados (PC) a conformidade aos parâmetros estabelecidos, os controles técnicos e operacionais de segurança envolvidos nos processos de validação da identidade do cidadão e os padrões criptográficos empregados para as assinaturas eletrônicas avançadas, definidos na PORTARIA CONJUNTA ITI/CC/PR SGD/SEDGG/ME Nº 1, DE 8 DE SETEMBRO DE 2021. Ademais, devem ser descritos na DPC, os procedimentos adotados com base nos requisitos relacionados na Parte Técnica do Anexo I da portaria SEDGGME Nº 2.154.

4.2.2. Acerca da Política de Segurança da Informação, ela deve ser elaborada sob a coordenação do Gestor de Segurança da Informação do proponente, que deve promover a divulgação dela a todos os funcionários, aos usuários e aos prestadores de serviço. É recomendável que a Política esteja adequada a medidas que objetivem a proteção dos dados pessoais.

5 ABRANGENCIA DE ATENDIMENTO

5.1.1. O proponente interessado deverá indicar a sua abrangência de atendimento. A abrangência pode ser nacional ou estadual e para este último caso deve ser observada a obrigatoriedade da portaria: Atender pelo menos 1 (um) Estado de cada região geográfica (Sul, Sudeste, Centro-Oeste, Nordeste, Norte). Ao indicar a sua abrangência, o proponente deve delimitar as localidades que tem interesse em realizar a prestação do serviço.

5.1.2. Para comprovar a sua abrangência de atendimento, o proponente pode se dispor da apresentação de seus relatórios internos ou outro documento de sua escolha que evidencie o atendimento de pelo menos 1% da população economicamente ativa da localidade onde o seu serviço é prestado. A documentação apresentada deve ser assinada pelo representante legal do proponente.

6 INDICADORES

Indicadores dos números de certificados e assinaturas avançadas são necessários para acompanhamento do projeto e monitorar os indicadores da SGD sobre uso da Assinatura Avançada no governo.

6.1. Indicadores de certificados avançados

6.1.1 Número de certificados avançados emitidos por meio da solução disponibilizada e certificados revogados.

6.2. Indicadores de assinatura avançadas

6.2.1 Número de assinaturas avançadas realizadas por sistemas/serviços.

6.3. Formato e disponibilização dos dados

6.3.1 Os dados podem ser disponibilizados em D-1, em uma visão por dia, mês e ano, em formato aberto, como CSV.

7 DOCUMENTAÇÃO

Encaminhar a Secretaria de Governo Digital, por meio do serviço de **Protocolo Digital - Cidadão**, os seguintes documentos:

- Formulário SOLICITAÇÃO DE CREDENCIAMENTO DE VALIDADOR DE ACESSO DIGITAL, presente no Anexo I deste documento, devidamente preenchido e assinado pelos representantes legais do proponente a validador de acesso digital;
- Inscrição CNPJ (A)
- Inscrição estadual e municipal, relativo ao domicílio sede da candidata (B)
- Certidões negativas de débito junto à Fazenda Federal, Estadual e Municipal; inclusive Seguridade Social e ao Fundo de Garantia do Tempo de Serviço (C)
 - Certidão Negativa Fazenda Federal [Emissão de Certidão Negativa \(fazenda.gov.br\)](http://fazenda.gov.br)
 - Certidão Negativa Fazenda Estadual [SINTEGRA](#)
 - Certidão Negativa Fazenda Municipal
 - Certidão Negativa de débitos do FGTS [Consulta Regularidade do Empregador \(caixa.gov.br\)](#)
- Declaração de que não foi declarada inidônea nas esferas de Governo Federal, Estadual e Municipal (D)
 - Certidão Negativa de Inidôneo [Sistema de consulta de Inabilitados e Inidôneos TCU](#)

NOTA: As empresas cadastradas no Sistema Unificado de Cadastramento de Fornecedores – SICAF, registro cadastral oficial do Poder Executivo Federal, poderão, para fins de comprovação do disposto nos itens A, B, C e D, apresentar seu extrato.

ANEXO I - Formulário de Solicitação de Cadastro de Validador de Acesso Digital

Dados da empresa		
Nome (Razão Social):		
CNPJ:		
Endereço:		
Nº:	Complemento:	CEP:
UF:	Cidade:	Bairro:
Identificação do responsável pelo credenciamento		
Nome do responsável:		
CPF do responsável:		
Telefone do responsável:		
Endereço eletrônico (e-mail) do responsável:		
Identificação do Gestor de Segurança da Informação		
Nome do Gestor:		
CPF do Gestor:		
Telefone do Gestor:		
Endereço eletrônico (e-mail) do Gestor:		

Declaro que todos os dados informados neste documento são verdadeiros e que a entidade apresentada para credenciamento para desenvolver as atividades de Validador de Acesso Digital atende às exigências estabelecidas na PORTARIA SEDGGME Nº 2.154, DE 23 DE FEVEREIRO DE 2021.

Local e Data:

NOME e CPF do responsável legal da empresa