

MANUAL OPERACIONAL

1. Visão geral:

O credenciamento de validadores de acesso digital será precedido de análise e verificação de conformidade com os critérios estabelecidos em Portaria SGD/MGI Nº 11.230/2025 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 ou biográfica em processos de identificação digital utilizados na plataforma de serviços digitais gov.br

2. Objetivo:

Este documento tem como objetivo orientar o proponente em relação ao preenchimento do formulário e documentação comprobatória dos requisitos de credenciamento para validador de acesso digital.

3. Vedações:

É vedada a participação no processo de credenciamento de pessoa jurídica que se encontre, ao tempo do requerimento de credenciamento, impossibilitada de licitar e contratar com o Poder Público ou que tenha sido declarada inidônea, pelo tempo em que durar a respectiva sanção.

A vedação aplica-se à entidade de direito privado que tenha como sócio ou administrador pessoa física ou jurídica impossibilitada de licitar e contratar com o Poder Público ou declarada inidônea ou que tenha sido, ao tempo da aplicação da sanção, sócio controlador ou administrador, bem como a sua controladora, controlada ou coligada, quando constatado o intuito de burlar a efetividade da sanção aplicada ou verificada a utilização fraudulenta da personalidade jurídica.

4. Credenciamento do validador de acesso digital:

Órgão ou entidade de direito público:

O órgão ou entidade de direito público deverá:

- a) realizar validação biográfica e documental, presencial ou remota, conferida por agente público; ou
- b) realizar validação biométrica conferida em base de dados governamental;

Pessoa jurídica de direito privado:

- a) comprovar o efetivo exercício de atividades de atendimento ao público, com

instalação, aparelhamento e pessoal qualificado;

b) realizar validação biográfica e documental de forma presencial; ou

c) realizar validação biométrica, de forma presencial ou remota, desde que conferida em base de dados governamental;

d) ter sede administrativa localizada no território nacional; e

e) comprovar a abrangência de atendimento de:

1. pelo menos 1 (um) estado de cada região geográfica brasileira; e

2. prestação de serviço para, no mínimo, um por cento da população economicamente ativa das localidades onde o serviço é prestado.

5. Critérios para comprovação para validação biográfica e documental do cidadão:

Com o propósito de atestar atendimento aos critérios para validação biográfica e documental do cidadão, é necessário apresentar documentação relativa a procedimentos utilizados para:

a) garantir a autenticidade do documento de identificação civil apresentado pelo usuário;

b) verificar as informações junto ao órgão emissor do documento de identificação civil; e

c) verificar que a identidade pertence à pessoa que a está reivindicando.

6. Critérios para comprovação de validação biométrica do cidadão:

Com o propósito de atestar atendimento aos critérios do requisito de validação biométrica, é necessário apresentar documentação relativa aos:

a) procedimentos, principais funcionalidades e interfaces envolvidas no processo de identificação biométrica;

b) dados biométricos coletados e os respectivos equipamentos utilizados para a coleta; e

c) especificações técnicas dos sistemas próprios ou de fornecedores contratados para coleta de dados.

7. 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).

a) Atendimento ao público

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.

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.

b) Instalação física e aparelhamento

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.

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.

c) Pessoal qualificado

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.

É recomendável realizar treinamentos constantes dos colaboradores sobre os seguintes assuntos: i) conduta e procedimentos para atendimento ao público; ii) normas e procedimentos para validação de identidade;

8. Segurança da informação e privacidade de dados no processo de validação

a) 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.

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.

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

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.

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.

9. Julgamento e análise:

A Secretaria de Governo Digital analisará e julgará a documentação apresentada pelo proponente.

O proponente poderá ser notificado, por meio eletrônico, para, no prazo de 30 (trinta) dias corridos, complementar informações acerca dos documentos já apresentados.

Da decisão do Secretário de Governo Digital que indeferir o requerimento de credenciamento ou que descredenciar o órgão ou entidade caberá a interposição

de recurso, no prazo de 10 (dez) dias corridos, contados da data da ciência da decisão, observado o disposto na Lei nº 9.784, de 29 de janeiro de 1999.

10. Monitoramento:

O monitoramento e avaliação dos serviços prestados pelos validadores de acesso digital serão realizados pela Secretaria de Governo Digital, por meio, entre outras, das seguintes atividades:

- a) coleta sistemática de dados relacionados aos serviços prestados;
- b) realização de visitas técnicas remotas ou *in loco*;
- c) análise de indicadores de desempenho; e
- d) análise de documentos e informações que poderão ser solicitados, a qualquer momento, aos validadores de acesso digital.

11. Indicadores de desempenho:

Indicadores de desempenho que serão monitorados:

a) Indicadores de certificados avançados

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

b) Indicadores de assinatura avançadas

Número de assinaturas avançadas realizadas por sistemas/serviços.

c) Formato e disponibilização dos dados

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

12. Encaminhamento da documentação comprobatória:

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

- a) 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;

- b) Inscrição CNPJ (A);
- c) Inscrição estadual e municipal, relativas ao domicílio sede da candidata (B);
- d) 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 \(fazenda.gov.br\)](#);

- Certidão Negativa Fazenda Estadual [SINTEGRA](#)

- Certidão Negativa Fazenda Municipal

- Certidão Negativa de débitos do FGTS [Consulta Regularidade do Empregador \(caixa.gov.br\)](#)

- e) 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 Cadastro 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 do órgão ou empresa		
Nome (razão social):		
CNPJ:		
Endereço:		
Nº:	Complemento:	Cep:
UF:	Cidade:	Bairro:
Responsável pelo credenciamento		
Nome do responsável:		
CPF do responsável:		
Telefone do responsável:		
E-mail do responsável:		
Identificação do gestor de segurança da informação		
Nome do gestor:		
CPF do gestor:		

Telefone do gestor:
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 Nº 11.230/2025.

Local e Data:

NOME e CPF do responsável legal da empresa