MINISTÉRIO DA ECONOMIA

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS

Serviço conta gov.br

Brasília, 27 de dezembro de 2022

MINISTÉRIO DA ECONOMIA

Histórico de Revisões

Data	Versão	Descrição	Autor
10/10/2021	1.0	Conclusão da primeira versão do relatório	SGD/ME
14/04/2022	1.1	Revisão do relatório após análise da equipe	SGD/ME
27/10/2022	2.0	Revisão do relatório após análise da equipe da Encarregada de dados pessoais	SGD/ME
23/11/2022	2.1	Correções de acordo com Revisões do Serpro	SGD/ME
06/12/2022	2.2	Inclusão do Gaap	SGD/ME
13/12/2022	2.3	Inclusão de RIPD da CentralIT	SGD/ME

MINISTÉRIO DA ECONOMIA

Sumário

MINISTÉRIO DA ECONOMIA

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS - RIPD
Serviço conta gov.br

OBJETIVO
O Relatório de Impacto à Proteção de Dados Pessoais visa descrever os processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco. **Referência:** Art. 5º, XVII da Lei 13.709/2018 (LGPD).

1 – IDENTIFICAÇÃO DOS AGENTES DE TRATAMENTO E DO ENCARREGADO

Controlador
Ministério da Economia – Secretaria do Governo Digital (SGD) Esplanada dos Ministério, Bloco K, 6 Andar, Brasília, CEP.: 70048-900
Operadores
Serviço Federal de Processamento de Dados – Serpro SGAN Av. L-2 Norte Quadra 601 Módulo G, Brasília, Distrito Federal, CEP.: 70.836-900 e Rua Olívia Guedes Penteado, 941, Capela do Socorro, São Paulo, CEP: 04766-900 Central IT CentralIT - Setor Hoteleiro Norte – Quadra 2 – Bloco F – Ed. Executive Office Tower – 17º Andar, CEP: 70702-906
Encarregada
Marta Juvina de Medeiros

E-mail Encarregada	**Telefone Encarregada**
marta.medeiros@economia.gov.br	(61) 3412-2498

2 – NECESSIDADE DE ELABORAR O RELATÓRIO

A elaboração do RIPD é indicada por existir a possibilidade de ocorrer impacto na privacidade dos dados pessoais, resultante de:

- Serviço em que dados pessoais e dados pessoais sensíveis são tratados;
- Tratamento de dado pessoal biométrico, quando vinculado a uma pessoa natural" (LGPD, art. 5º, II);
- Processamento de dados pessoais usados para tomar decisões automatizadas que possam ter efeitos legais;
- Tratamento de dados que possa resultar em algum tipo de dano patrimonial,

moral, individual ou coletivo aos titulares de dados, se houver vazamento (LGPD, art. 42).

•Reuso de dados de contato: e-mail, telefone e endereço pelo setor não governamental por meio do projeto piloto do Modelo de Governo como Plataforma(GaaP).

3 – DESCRIÇÃO DO TRATAMENTO

O objetivo principal desta descrição é apresentar o cenário institucional relativo aos processos que envolvem o tratamento dos dados pessoais, fornecendo subsídios para avaliação e tratamento de riscos.

- *Fluxos e Processos do Tratamento*

O serviço conta gov.br é uma solução custeada pelo Ministério da Economia e fornecida gratuitamente ao cidadão e usuário (titular de dados pessoais, ou titular). A conta é utilizada para identificação e autenticação no acesso com segurança aos serviços governamentais e pode ser criada e acessada pela web ou pelo aplicativo. **Saiba mais sobre a conta Gov.br.**

A versão web, ou seja, sites com o prefixo acesso.gov.br, é apresentada ao titular conforme Figura 1.

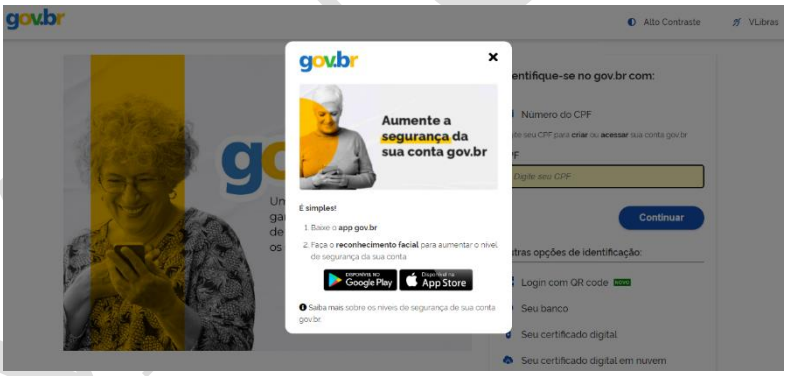


Figura 1- Acesso gov.br

O serviço versão aplicativo é disponibilizado para dispositivos móveis com sistemas Android ou IOS. A tela de acesso ao serviço versão aplicativo é apresentada conforme Figura 2.

Figura 2 – Aplicativo gov.br

Com objetivo de alinhar o conhecimento, ambos são considerados em conjunto e chamados de serviço conta gov.br, porém, caso haja necessidade de especificação, para um melhor esclarecimento, serão referenciados por seus nomes completos: acesso.gov.br e aplicativo gov.br.

No âmbito do Serviço conta gov.br, o Ministério da Economia trata dados pessoais em seis fluxos distintos: **criação de conta, autenticação do titular, aumento do nível de segurança da conta, recuperação da conta, alteração de dados e exclusão da conta.**

Visando segurança da informação e proteção de dados pessoais, o Serviço conta gov.br atribui níveis de confiabilidade que são Ouro, Prata ou Bronze às contas. Para mais detalhamento dos níveis das contas: https://gov.br/conta.

Para atribuição do nível de segurança à conta, o Ministério da Economia faz uso de tratamento automatizado para validações de dados pessoais nas seguintes bases governamentais:

1. Identificação Civil Nacional (**ICN**), sob gestão do TSE, é utilizada para a validação biométrica facial, na comparação da foto-selfie, capturada pelo aplicativo com a foto que consta na base de dados ICN, possibilitando uma identificação mais segura do titular. Para este cadastro, a decisão automatizada atribui o nível de segurança ouro.

2. Registro Nacional de Condutores Habilitados (**Renach**), sob gestão da Senatran, é utilizada para a validação biométrica facial, na comparação da foto-selfie, capturada pelo aplicativo com a foto que consta na base de dados do Renach, possibilitando uma identificação mais segura do titular. Para este cadastro, a decisão automatizada atribui o nível de segurança prata;

3. Sistema de Gestão de Acesso (**Sigac**), sob gestão do Ministério da Economia, é utilizada na validação de dados de servidor público, que passará a ter uma conta nível prata. A validação no Sigac é feita a partir da digitação da senha do Sigac pelo titular;

4. **Base de dados do CPF,** sob gestão da Receita Federal do Brasil (RFB), é utilizada para a validação do número e status do CPF, assim como validação das respostas dadas pelo titular em um carrossel de perguntas. Os dados utilizados no carrossel de perguntas são ano, mês e dia do nascimento e primeiro nome da mãe. Para este cadastro pelo carrossel, a decisão automatizada atribui o nível de segurança bronze (Portaria SEDGG nº 2154 de 23/02/2021).

Os níveis de segurança atribuídos a conta foram estabelecidos a partir das legislações que normatizam o serviço de assinatura digital. O qual requer nível de confiabilidade distintos para a efetuação da assinatura avançada. A legislação relacionada são: Decreto nº 10.543, de 13 de novembro de 2020, Lei nº 14.063, de 23 de setembro de 2020 e Portaria SEDGGME nº 2.154, de 23 de fevereiro de 2021.

Criação da Conta

A criação da conta pode ser realizada por meio de uma das cinco interações disponíveis ao titular: reconhecimento facial, internet banking, certificado digital, carrossel de perguntas, balcão gov.br e o balcão SAT. Para criar uma conta de acesso ao gov.br, o compartilhamento do CPF do titular se faz necessário, pois a partir dele são iniciadas as validações para identificação do titular de dados. Nas contas criadas por meio de interação com **Reconhecimento Facial, KBA e Balcão gov.br**, o próprio titular fornece seu CPF. Na criação por meio de **Bancos Credenciados e Certificado Digital** e **Certificado Digital em Nuvem,** o CPF do titular é compartilhado pelo Banco e Provedor do Serviço de Certificado ao gov.br. Após o compartilhamento do CPF, o titular deve confirmar estar ciente do Termo de Uso e Aviso de Privacidade para seguir com a criação da conta.

O serviço acesso.gov.br então:

- realiza a consulta do CPF (validação biográfica) na base da Receita Federal, e valida a existência e o status do CPF informado;

- realiza uma pesquisa biográfica (sim/não) para identificar se o CPF possui dados biométricos (nas bases da ICN e do Renach). Havendo dados biométricos disponíveis, o Serviço conta gov.br oferece ao titular a opção de criação de conta por meio de **Reconhecimento Facial**. Caso o cidadão não possua biometrias coletadas nas bases de governo mencionadas, o Serviço conta gov.br oferecerá a opção de criação de contas via **Bancos Credenciados** (internet banking). Se o cidadão não possuir biometria coletada, não possuir conta nos Bancos credenciados

ou optar por criar a conta por outro modo, o mesmo será direcionado à criação por meio de carrossel de perguntas (**KBA)**;

- Para criação de conta por meio de reconhecimento facial (validação biométrica), é necessário que o titular realize a captura de uma foto-selfie, com o aplicativo gov.br. Ao compartilhar, a foto-selfie é encaminhada para batimento biométrico em duas bases governamentais: ICN ou Renach. A primeira base a ser requisitada é a da ICN, pois os dados nela contidos são submetidos a um processo de individualização dos dados biométricos, enquanto a do Renach, não. A conta então é criada, e recebe nível de confiabilidade Ouro se validado na ICN e Prata se validado no Renach. (Portaria SEDGG nº 2154 de 23/02/2021).

- Para criação de conta por meio de bancos credenciados, é necessário que o titular se autentique com sua conta bancária, através de Bancos credenciados ao Serviço conta gov.br, neste processo, o Banco compartilha o número do CPF com o Ministério da Economia. É responsabilidade dos Bancos obter autorização do titular para compartilhamento.

- Para criação de conta por KBA, é necessário que o titular responda a perguntas relacionadas a seus dados pessoais, como, por exemplo, nome, nome da mãe e data de nascimento. As respostas são comparadas com a base da RFB (validação biográfica). A conta então é criada, e recebe um nível de segurança classificado como Bronze.

- após escolha do método de criação, o titular deve informar os dados para contato (e-mail ou telefone) e criar uma senha para acesso a sua conta.

O Balcão gov.br e o Balcão SAT, possuem um processo distinto dos demais mencionados acima, pois é um processo iniciado de forma presencial e será tratado de forma singular no final desta sessão.
O Balcão SAT é utilizado apenas por um cliente e está em fase de descontinuação. O encerramento deste serviço está previsto para o final de 2022. O Balcão gov.br substituirá este serviço.

Foram pensadas e implementadas formas distintas para o acesso, criação e recuperação da conta gov.br, de forma a buscar amplo acesso aos cidadãos e mitigar riscos de acessibilidade a ela atribuídos, como por exemplo, falha de validações. Abaixo detalharemos as formas de acesso e os processos e funcionalidades pertencente a conta.

Para mais detalhamento dos processos mencionados a seguir são apresentados os Fluxos:

Macroprocesso de criação de conta
Na Figura 3, estão evidenciadas as atividades comuns dos processos de Criação via Reconhecimento Facial, Bancos Credenciados e Carrossel de perguntas. As atividades que

são singulares de cada processo estão apresentadas via subprocesso. Neste Macroprocesso está o subprocesso de KBA.

Fluxo técnico Login Único - Criação Macroprocesso.png

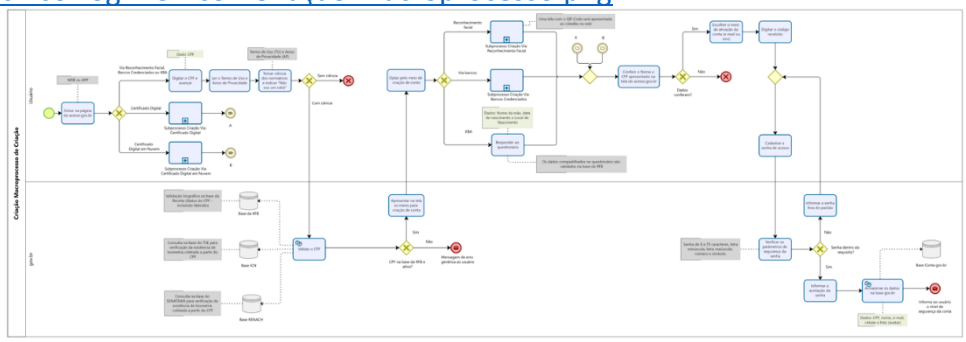


Figura 3

Subprocesso de Criação via Reconhecimento Facial

Fluxo técnico Login Único - Criação Via Reconhecimento Facial.png

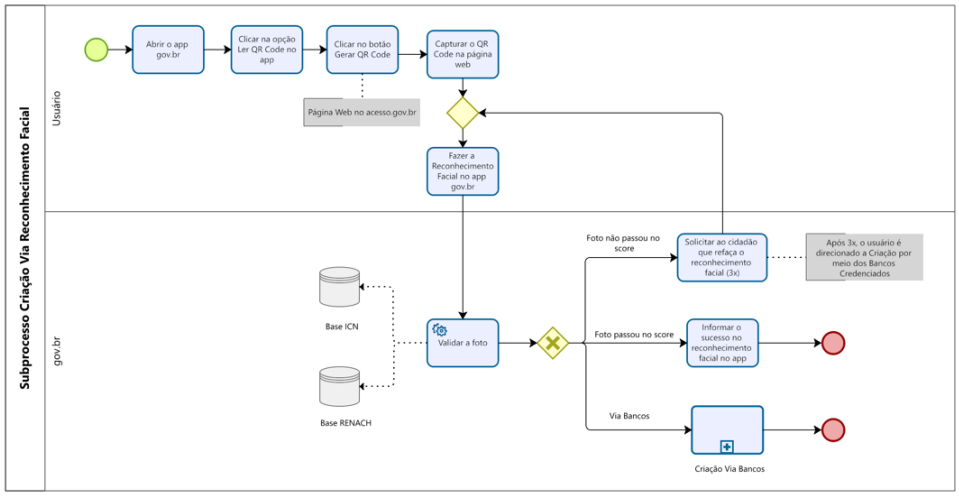


Figura 4

Subprocesso de Criação via Bancos Credenciados

Fluxo técnico Login Único - Criação Via Bancos Credenciados.png

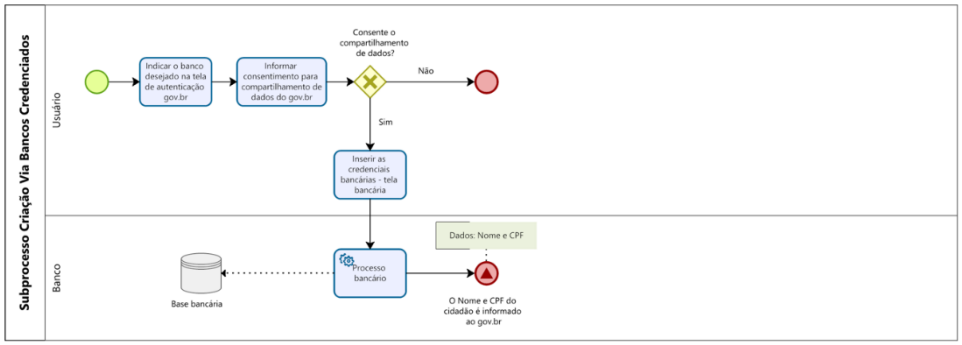


Figura 5

MINISTÉRIO DA ECONOMIA

Certificado Digital

O certificado digital pode ser utilizado em 3 processos distintos na plataforma: na criação de conta, na autenticação do titular e na vinculação de um conjunto de CPFs a um CNPJ para uso do módulo de empresas.

Os provedores de certificado digital compartilham CPF e nome para o serviço conta gov.br. Nos fluxos de interação com Certificado Digital não há validação do CPF na base da RFB, pois, entende-se que a validação de segurança é realizada por parte do Provedor do certificado.

No momento do uso do certificado digital é realizado um redirecionamento pelo Serviço conta gov.br para o provedor que valida os dados do certificado digital, inclusive se não está revogado, e o provedor retorna para o Serviço conta gov.br a autenticação do CPF, liberando assim o acesso via certificado digital.

Para criar uma conta de acesso ao gov.br, por meio de Certificado Digital e Certificado Digital em Nuvem:

- na página do acesso.gov.br o titular indica o seu certificado digital em máquina ou realiza os procedimentos necessários para login no provedor, caso utilize certificado em nuvem;
- os provedores do certificado enviam ao gov.br o CPF do titular;
- o titular confirma estar ciente do Termo de Uso e Aviso de Privacidade;
- o titular responde ao desafio captcha para criação de sua senha.

Para mais detalhamento dos processos mencionados acima, vide os fluxos a seguir:

Subprocesso de Criação via Certificado Digital

Fluxo técnico Login Único - Criação Via Certificado Digital.png

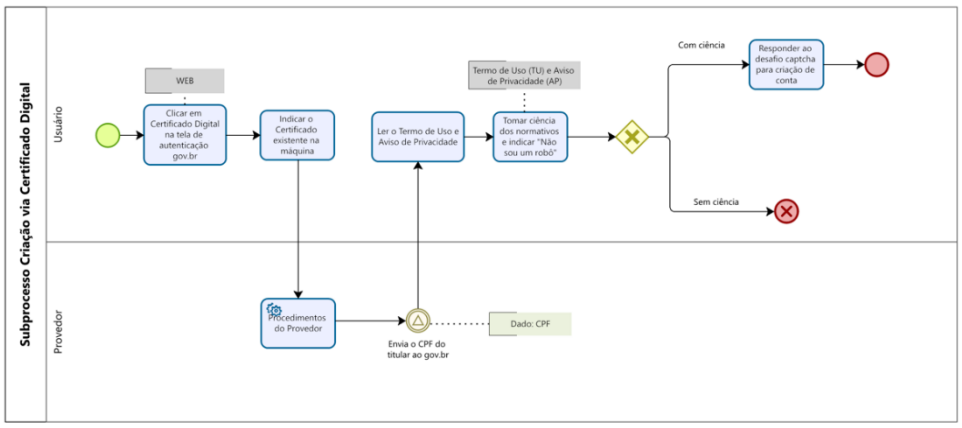


Figura 6

Subprocesso de Criação via Certificado Digital em Nuvem

Fluxo técnico Login Único - Criação Via Certificado Digital em Nuvem.png

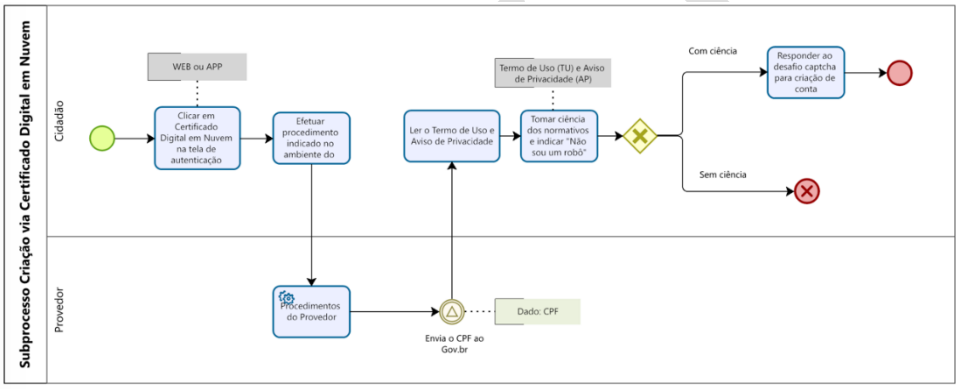


Figura 7

Vinculação do e-CNPJ à conta

Os titulares que optaram pela criação da conta por meio de Certificado Digital, ao realizarem a autenticação pela primeira vez, serão direcionados a área Minha Conta gov.br e precisarão realizar passos adicionais para vinculação da conta ao CNPJ, conforme ilustrado na figura abaixo:

Figura 8

Após as informações do certificado digital serão apresentadas na tela para que o titular possa realizar a validação e finalizar o processo de vinculação.

Figura 9

Cadastro do colaborador do CNPJ

O serviço conta gov.br permite o cadastramento de pessoas que não pertencem diretamente a empresa. Esse cadastro ocorre pela indicação de colaboradores.

Balcão gov.br

O Balcão de Atendimento gov.br é um sistema de criação e recuperação da conta gov.br, desenvolvido pelo Serpro em parceria com o Ministério da Economia. Nele o cidadão que busca atendimento a algum serviço governamental e não possua a conta ou não se recorde do seu e-mail cadastrado, pode realizar o processo de criação ou recuperação da conta por meio de um atendente credenciado, permitindo maior controle do processo, com rastreabilidade de todas as etapas e eventos.

Para realizar os procedimentos no sistema, o atendente precisa seguir os requisitos de segurança:

- Estar cadastrado no sistema com o perfil de atendente ou gestor;
- Possuir conta gov.br com o selo de confiabilidade “prata”;
- Estar com a verificação em duas etapas (segundo fator de autenticação) habilitada. A verificação em duas etapas é aplicada na área de configuração de segurança da conta gov.br na versão web. Abaixo segue duas telas sobre o procedimento:

Habilitação da verificação em duas etapas

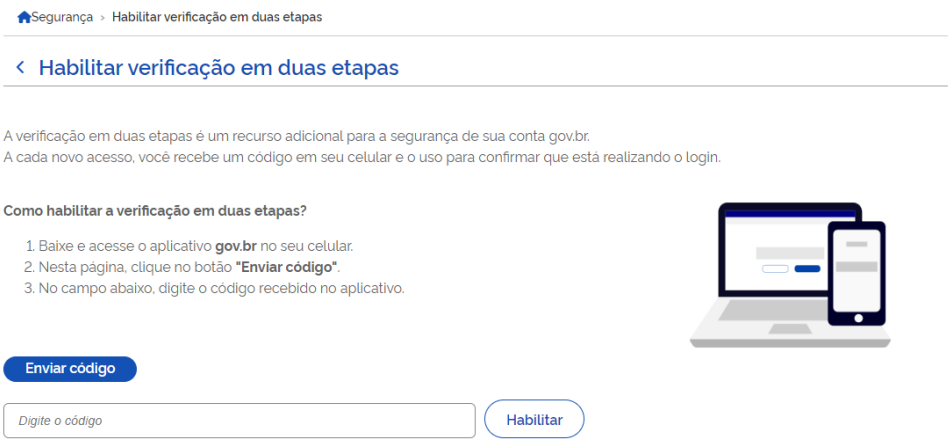


Figura 10

Identificação da verificação em duas etapas habilitada

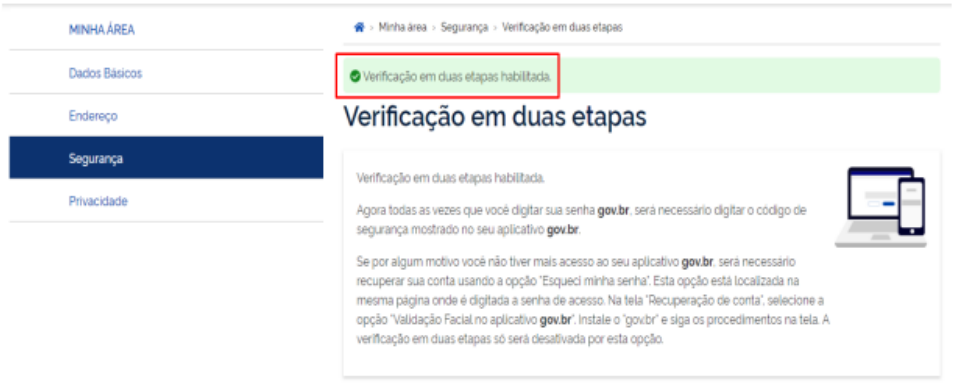


Figura 11

Para iniciar o procedimento, o atendente deve identificar se o solicitante presencial é o titular dos dados ou representante. No procedimento iniciado por representante, se faz necessária a apresentação de uma procuração, a qual será anexada a solicitação no sistema. Diferente dos demais órgãos, o INSS faz solicitação adicional do documento identificação do representante e também o anexa a solicitação.

Ao criar ou recuperar o e-mail cadastrado na conta, o atendente entrega a senha provisória de forma impressa e caso o solicitante tenha informado algum meio de contato, como e-mail ou telefone, a senha é enviada também para estes meios. Os dados de contato coletados neste momento não são armazenados em nenhuma base.

Os órgãos que utilizam este serviço são: o INSS, o Ministério do Trabalho e o governo de Minas Gerais no serviço UAI. O sistema é acessado por meio da URL www.balcao.acesso.gov.br.

Para mais detalhamento dos processos mencionados acima, vide o fluxo a seguir:

Fluxo técnico Login Único - Criação Via Balcão gov.br.png

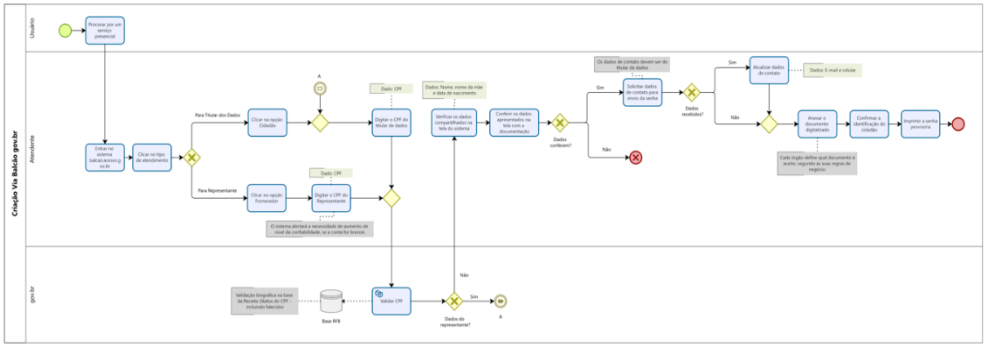


Figura 12

Recuperação da conta

Caso o titular não lembre a sua senha de acesso ao Serviço conta gov.br, para recuperar a conta, há as seguintes possibilidades:

- reconhecimento facial pela ICN (processo similar da criação de conta). Após este processo o nível da conta é mantido, se o nível for ouro. Se o nível da conta for bronze, este é elevado para ouro. Se for prata é modificado para ouro.

- reconhecimento facial pelo Renach (processo similar da criação de conta). Após este processo o nível da conta é mantido, se o nível for prata. Se o nível da conta for bronze, este é elevado para prata.

- bancos credenciados (processo similar da criação de conta). Após este processo o nível da conta é mantido, se o nível for prata. Se o nível da conta for bronze, este é elevado para prata. Se for ouro, é modificado para prata.

- dados de contato (e-mail ou telefone). Após este processo, a conta passa a ter nível bronze, por não ter validação biométrica;

- formulário de atendimento (envio de uma selfie com um documento de identificação dom foto e CPF para uma central de serviços que realiza a atualização do e-mail do titular, possibilitando que ele realize a recuperação da conta a partir do e-mail cadastrado. Após este processo, a conta passa a ter nível bronze, por não ter validação biométrica (Este processo é feito pelo operador CentralIT e mais detalhes estão no RIPD do Formulário de atendimento);

- Também é possível a recuperação de conta comparecendo presencialmente a um balcão de atendimento gov.br em um dos órgãos parceiros (processo similar da criação de conta). Após este processo, a conta passa a ter nível bronze, por não ter validação biométrica.

Para mais detalhamento dos processos mencionados acima, vide os fluxos a seguir:

Macroprocesso de Recuperação de Conta

Neste desenho de fluxo estão evidenciadas as atividades comuns dos processos mencionados acima (Recuperação Via Reconhecimento Facial, Via Bancos Credenciados, Via E-mail, Via SMS e Via Formulário de Atendimento). As atividades que são singulares de cada processo estão apresentadas via subprocesso. Os subprocessos de Recuperação Via Reconhecimento Facial e Via Bancos Credenciados não estão detalhados nos fluxos abaixo, pois são similares ao processo de criação e podem ser verificadas na sessão anterior.

Fluxo técnico Login Único - Macroprocesso Recuperação de Conta.png

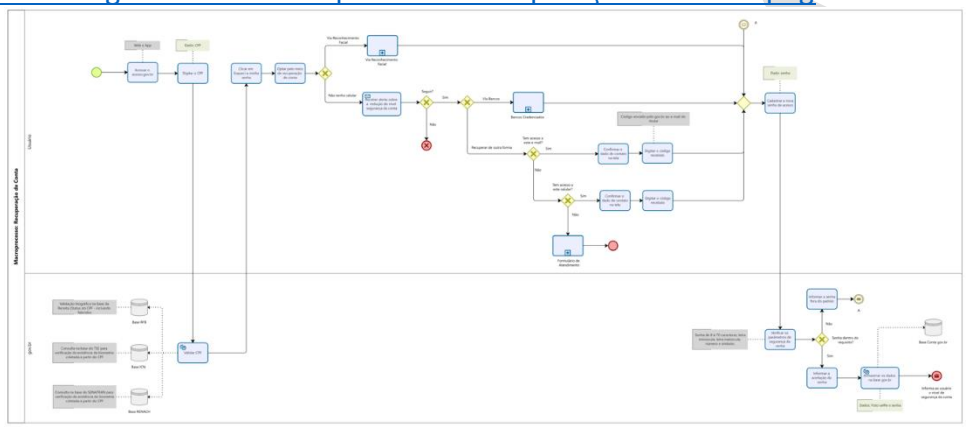


Figura 13

Via Formulário de Atendimento (Central IT)

Fluxo técnico Login Único - Recuperação de Conta - Formulario de Atendimento.png

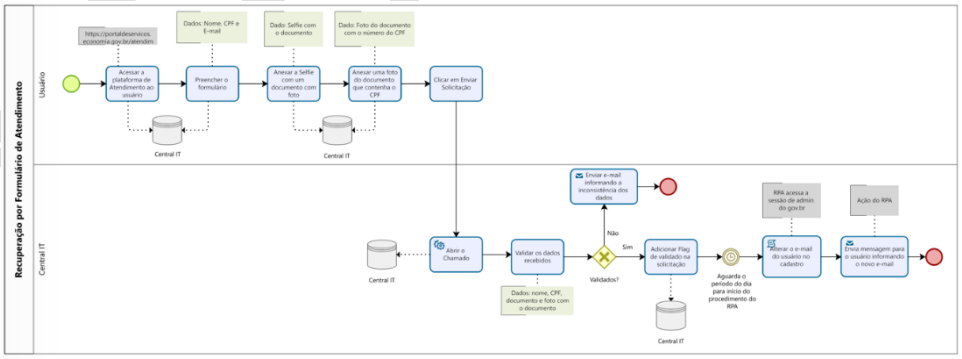


Figura 14

Autenticação da conta

Seguindo a estrutura do serviço, a autenticação pode ser realizada tanto na versão Web quanto no aplicativo gov.br. Além da autenticação por meio do compartilhamento do CPF e senha, é possível autenticar pelas formas de interação Bancos Credenciados, QR-Code e

Certificado Digital (A1 e A3). Há formas de autenticação diferenciadas na versão Web e no aplicativo. Abaixo detalhes das diferenças:

Web:

- Para autenticar por meio de Bancos Credenciados e Certificados Digitais, o titular deverá seguir o mesmo procedimento utilizado para a criação da conta;

- Para autenticação por meio de QR-Code, será necessário o uso do aplicativo gov.br. Ao clicar na opção Login com QR-Code, uma tela com o código será aberta. No aplicativo o titular deverá estar logado e clicar na opção Leitura de QR-Code no aplicativo e realizar o procedimento de leitura. Assim o gov.br realizará a autenticação do titular no serviço.

Aplicativo gov.br:

- é possível autenticar por meio dos Bancos Credenciados, o titular deverá seguir o mesmo procedimento utilizado para a criação da conta;

- no caso de Certificados Digitais, nesta versão do serviço conta gov.br, é possível realizar a autenticação somente por meio dos Certificados A3.

Em ambas as versões a autenticação pode ser feita por meio de CPF e senha.

Aumento do nível de confiabilidade da conta

Para o aumento de nível de confiabilidade, o titular precisa estar logado em sua conta e na sessão Minha área gov.br iniciar o processo. Dependendo do nível de confiabilidade atual da conta, o titular será direcionado para fluxos diferenciados:

- **Web:** após clicar em Aumentar o Nível e finalizada a validação pelo gov.br sobre qual o nível de confiabilidade da conta atual, o titular é direcionado a escolher o modo pelo qual deseja realizar o procedimento. Se a escolha for por meio das bases de dados da ICN ou Renach, a opção de geração do QRCODE é apresentada na tela. A leitura do QRCODE na tela web deve ser feita pelo aplicativo e assim o titular prossegue com os procedimentos de validação biométrica. Caso o titular opte por Certificado Digital, uma tela para leitura do certificado (máquina) será apresentada na tela;

- **Aplicativo gov.br**: após clicar em Aumentar o Nível e finalizada a validação pelo gov.br sobre qual o nível de confiabilidade da conta atual, o titular é direcionado a realização da validação biométrica.

MINISTÉRIO DA ECONOMIA

Alteração de dados

A alteração de dados pode ser realizada diretamente no Serviço conta gov.br. Os dados adicionados diretamente pelo titular são passíveis de alteração: e-mail, telefone, endereço, foto-selfie. Na versão web, também é possível alterar o nome e imagem de perfil. Os demais dados pessoais não são editáveis.
A forma de compartilhamento das fotos difere entre a versão web e aplicativo:

- **Web (imagem de perfil):** o Ministério da Economia permite que o usuário adicione no perfil de sua conta, qualquer imagem do seu desejo, pois esta foto, imagem de perfil, não é submetida a validações. Esta é a que identificamos como Imagem de perfil;

- **Aplicativo (foto-selfie)**: após o procedimento de validação biométrica, seja vindoura do fluxo de criação, recuperação de senha ou aumento de nível, a foto coletada é adicionada automaticamente como foto do perfil. Entretanto, após a validação a foto pode ser alterada sem necessidade validação biométrica. Esta é a que identificamos como Foto-selfie.

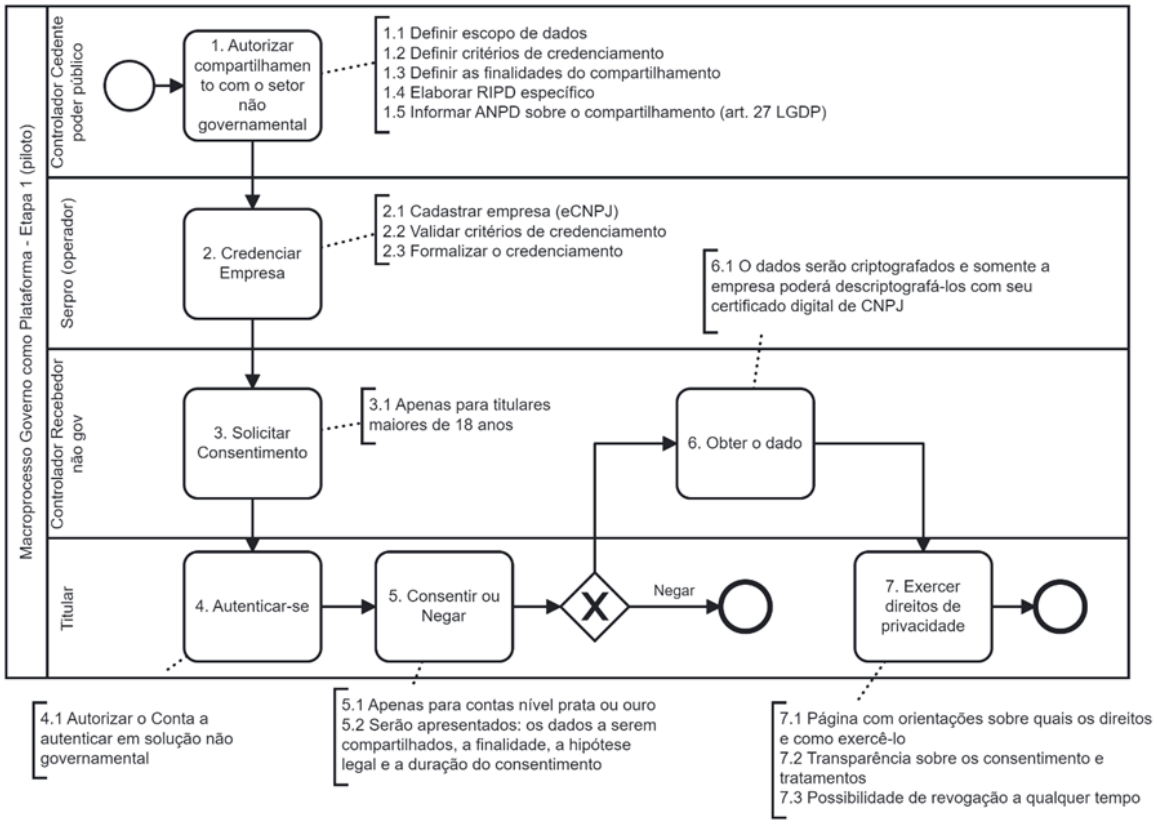
Exclusão da conta

O Ministério da Economia utiliza a plataforma Fala.BR (falabr.cgu.gov.br) como meio de comunicação entre o órgão e o titular. Para registro da solicitação, o titular deve anexar um documento de identificação com foto e escrever sua solicitação. A solicitação é encaminhada a equipe do Serviço conta gov.br, a qual entra em contato com o titular do dado para atendimento a solicitação.

Reuso de dados de contato pelo Setor não Governamental

O modelo Governo como Plataforma (Government as a Platform - GaaP), é um modelo que busca viabilizar a prestação de serviços que conecte **os setores governamental e não governamental por meio do empoderamento do titular no uso de seus dados pessoais para melhorar a experiência no consumo de serviços públicos e privados** de seu interesse, estimulando a inovação e a atividade econômica do país. Este modelo, ainda em fase experimental de projeto piloto, estabelece as regras e condições para o reuso dos dados que estão em posse do Poder Público.

O modelo tende a eliminar o trabalho manual de catalogação e entrega de documentações por parte do cidadão às instituições com as quais se relaciona, bem como a checagem e validação destes documentos por parte da instituição, pois, na medida em que que estas informações estejam disponíveis para uma consulta automatizada nem o cidadão nem a instituição precisarão desperdiçar tempo com estas tarefas manuais, já que os sistemas envolvidos obterão os dados de maneira automatizada e diretamente das bases do poder público.



A figura acima demonstra o fluxo básico do modelo, onde de forma simplificada, temos:

1. Análise de viabilidade e autorização de disponibilidade de dados em posse do governo para o setor não governamental.
2. Habilitação/credenciamento das empresas que poderão ter acesso aos dados disponibilizados. Essa habilitação/credenciamento, é realizada com base em critérios definidos no passo anterior.
3. A empresa credenciada deverá solicitar consentimento ao cidadão titular dos dados pessoais para efetivamente obter acesso aos dados.
4. O titular dos dados pessoais, autoriza o serviço de conta gov.br a autenticar na solução da empresa solicitante dos dados.
5. O titular dos dados pessoais, devidamente autenticado no serviço de conta gov.br, poderá consentir ou não, que seus dados sejam compartilhados com a empresa solicitante.
6. Após o consentimento e enquanto ele for válido, a empresa solicitante poderá obter os dados consentidos diretamente das bases do governo.
7. O titular de dados pessoais poderá a qualquer tempo, exercer seus direitos previstos no art. 18 da LGPD.

A SGD disponibiliza para acesso pelo setor não governamental, através do Modelo de Governo como Plataforma, os dados de contato e-mail, telefone, endereço, do serviço contas gov.br.

O Modelo Governo como Plataforma proporcionará a identificação do cidadão por meio da conta gov.br (utilizando nome, cpf e nível de confiabilidade da conta) e o compartilhamento de dados de contato (e-mail, telefone e endereço), para comunicação entre o AUTORIZADO e o titular dos dados pessoais.

Mais informações sobre os fluxos e detalhamentos do processo de disponibilização de dados para setor não governamental através do Modelo de Governo como Plataforma, estão disponíveis no RIPD do referido modelo.
Ressalta-se que para uma completa avaliação do impacto da disponibilização dos dados de contato do serviço conta gov.br para setor não governamental, é necessária a análise dos dois Relatórios de Impacto de Proteção de Dados, ou seja, este documento que trata dos dados do serviço de conta e o RIPD do modelo Governo como Plataforma que trata as questões específicas do modelo.

3.1 – NATUREZA DO TRATAMENTO

Nesta seção é descrito como a plataforma gov.br trata os dados pessoais, apresentando informações sobre:

- Fonte e utilização;
- Agentes e Tratamentos de Dados pessoais
- Eliminação dos dados
- Compartilhamento
- Tratamento Automatizado
- Controles de segurança e de privacidade adotados

• *Fonte e utilização*

As fontes de dados pessoais do Serviço conta gov.br são o titular de dados pessoais, as bases da RFB, da ICN, do Renach, de Bancos credenciados e de provedores de Certificados digitais. Os dados são utilizados na criação da conta, recuperação da conta, aumento do nível de confiabilidade da conta, na autenticação do titular, na interoperabilidade dos dados entre órgãos públicos, que ocorre por meio da autenticação, na alteração dos dados, na exclusão da conta, na monitoração, detecção e investigação de fraudes.

• *Agentes e Tratamentos de Dados pessoais*

Para o Serviço conta gov.br, as decisões referentes ao tratamento de dados pessoais são de responsabilidade do Ministério da Economia, ou seja, do controlador dos dados pessoais.

Quando o titular prova sua identidade com a conta gov.br, o Serviço conta gov.br consulta e valida os dados em outras bases de dados governamentais, como o cadastro do CPF na RFB, a biometria nas bases de dados do ICN e Renach. Quando houver estas validações de dados, os validadores, RFB, TSE e Senatran, se tornarão os Controladores durante esse processo.

Como alternativas para a autenticação no Serviço conta gov.br, é disponibilizada ao titular a possibilidade de autenticação por provedores de certificado digital ou por Bancos

credenciados. Neste cenário, as autoridades certificadoras e os Bancos também atuam como Controladores.

Para o serviço contas gov.br, o tratamento de dados pessoais, em nome do Ministério da Economia, é realizado pelos operadores:

- Serpro: responsável pelo tratamento (coleta, armazenamento, processamento, compartilhamento, eliminação) dos dados pessoais e pelo envio de e-mails, seguindo todas as determinações do Ministério da Economia.

Os dados pessoais tratados para o Serviço conta gov.br são armazenados nas unidades do Serpro. Em São Paulo fica o ambiente de produção e os backups e em Brasília a redundância da solução. Os dados pessoais apresentados na versão aplicativo são armazenados no dispositivo do titular.

- CentralIT : responsável pelo processo de recuperação de contas através do canal: https://portaldeservicos.economia.gov.br/atendimento/

A CentralIT é responsável pelo tratamento de dados pessoais para a recuperação de contas, que ocorre por meio de formulário de atendimento, quando o titular não se recorda do e-mail cadastrado em sua conta ou quando há erro em seu cadastro. (Mais detalhes estão no RIPD do Formulário de atendimento)

• *Eliminação dos dados*

A exclusão da conta gov.br acontece com pedido expresso do usuário, mas os dados de logs de uso permanecem retidos.

Há um processo para a exclusão de contas que ocorre quando o titular comprova que ele, como titular do CPF, não foi o criador da conta. Esta exclusão é feita apenas por autorizados do Ministério da Economia.

Alguns dados podem ser excluídos e/ou alterados pelo titular. Detalhes sobre retenção e exclusão no Tópico 3.2 deste relatório.

• *Compartilhamento com entes públicos*

O compartilhamento ocorre na autenticação de serviços públicos, com entes do Governo, que são responsáveis por estes serviços e tem respaldo no Decreto nº 10.046, de 9 de outubro de 2019.

Quando o titular acessa serviços, autenticando com sua conta gov.br, ele é perguntado se autoriza o compartilhamento de dados pessoais, da base do Serviço conta gov.br, com o ente que executa o serviço e este ente passa a ser o controlador dos dados, tendo suas próprias regras e aviso de privacidade.

Solicitação dos Entes públicos: Para que o ente público integre o Serviço conta gov.br, como um login único para seus sites, é preciso preencher o documento de solicitação do Plano de Integração.

Este documento tem por objetivo descrever e firmar compromisso em relação a estratégia do ente, para a transformação digital dos serviços públicos, no que se refere à

implementação do Login Único, conforme diretrizes da Plataforma de Cidadania Digital, previstas no Decreto nº 8.936/16.
Os dados pessoais compartilhados com o ente solicitante estão no Escopo de Atributos do Roteiro de Integração. O Ente solicitante escolhe qual escopo de dados será necessário. Os dados compartilhados são para autenticação e preencher formulários de cadastros dos serviços. Além desta solicitação, há um processo interno, em que os entes solicitantes enviam Ofício e Plano de Trabalho, especificando a finalidade de integração. Neste ofício é especificado quais sistemas/serviços serão integrados e é determinado qual nível de confiabilidade mínimo da conta que acessará o serviço, visando a proteção dos dados. Os ofícios estão armazenados no SEI.
O Ministério da Economia não atua como auditor das informações, cuja fidedignidade é de responsabilidades dos entes solicitantes e credita-se como verídicas, baseando-se na fé pública inerente aos servidores e funcionários públicos.
O Ministério da Economia mantém esses documentos com disponibilidade para análise quando solicitado pelos entes ou por pedidos judiciais.
Se o ente definir nível confiabilidade ouro, pois entende que as informações a serem apresentadas são críticas, as contas com os demais níveis de confiabilidade não conseguirão acessar o serviço. É responsabilidade do órgão instruir o titular, que caso deseje acessar o serviço em questão, será necessário passar pelo processo de aumento do nível de confiabilidade.

Autorização dos titulares de dados: Os dados pessoais apenas serão compartilhados com a autorização do titular, que é mantida para garantir a confirmação de sua autorização, de forma livre, informada e inequívoca, e a concordância com o tratamento de seus dados pessoais pelo serviço autenticado com sua conta gov.br.
Esta autorização pode ser verificada a qualquer momento na área de Autorizações da conta. O titular pode desautorizar futuros compartilhamentos, mas os dados compartilhados anteriormente continuarão no cadastro do serviço e sob responsabilidade do ente que disponibiliza o serviço.

• Compartilhamento com o setor não governamental

O Modelo Governo como Plataforma está em fase piloto e permite o compartilhamento de dados pessoais com o setor não governamental. Nesta fase piloto, a primeira base a ser compartilhada, será a do serviço de contas gov.br, minimizado aos dados de contato: e-mail, telefone e endereço, com autorização e consentimento do titular de dados.
Para que a empresa/organização integre o serviço de contas gov.br, com um login único, é preciso um **credenciamento**.

Autorização dos titulares de dados: Os dados pessoais de nome, cpf e método de autenticação (senha ou certificado digital), para autenticação em serviços das empresas/organizações, apenas serão compartilhados com a autorização do titular, que é mantida para garantir a confirmação de sua autorização, de forma livre, informada e inequívoca, e a concordância com o tratamento de seus dados pessoais pelo serviço privado

autenticado com sua conta gov.br.
Esta autorização pode ser verificada a qualquer momento na área de Autorizações da conta. O titular pode desautorizar futuros compartilhamentos, mas os dados compartilhados anteriormente continuarão no cadastro do serviço e sob responsabilidade do ente privado que disponibiliza o serviço.

Consentimento dos titulares de dados: Os dados pessoais de contato, e-mail, telefone e endereço, para preenchimento de cadastro em serviços de empresas/organizações, apenas serão compartilhados com o Consentimento do titular, que é mantido para garantir a confirmação de seu consentimento, de forma livre, informada e inequívoca, e a concordância com o compartilhamento de seus dados pessoais com serviço privado.
Este consentimento pode ser verificado a qualquer momento na área de Consentimentos do aplicativo gov.br. O titular pode desautorizar futuros compartilhamentos, mas os dados compartilhados anteriormente continuarão no cadastro do serviço e sob responsabilidade da empresa/organização, que disponibiliza o serviço.

Para mais detalhes sobre o fluxo do compartilhamento de dados pessoais com o setor não governamental através do Modelo de Governo como Plataforma, vide o RIPD do referido modelo: RIPD GaaP.

• *Tratamento automatizado*

Os dados pessoais estarão sujeitos à tomada de decisão automatizada quando:

- Os dados pessoais são verificados e/ou validados em relação aos dados mantidos nas bases da RFB, ICN e Renach;
- As respostas às perguntas para criação de contas por Carrossel de perguntas são comparadas com os dados mantidos pela RFB;
- A conta é classificada em níveis de segurança, ou seja, confiabilidade bronze, prata e ouro.

• *Controles de segurança e de privacidade adotados.*

Os controles adotados se encontram na seção 7 deste relatório.

3.2 – ESCOPO DO TRATAMENTO

O escopo representa a abrangência do tratamento de dados.

Nesse sentido, destacam-se

- Informações sobre os tipos dos dados pessoais tratados;
- Volume, extensão e frequência em que os dados são tratados;
- Período de retenção, informação sobre quanto tempo os dados pessoais serão mantidos, retidos ou armazenados;
- Número de titulares de dados afetados pelo tratamento e
- Abrangência da área geográfica do tratamento.

Com o levantamento destas informações conclui-se que o tratamento de dados pessoais, no Serviço conta gov.br, é realizado em alta escala.

O serviço conta gov.br possui dois operadores e visto a complexidade, este RIPD se limita ao tratamento de dados pessoais pelo Operador Serpro.
No RIPD do Formulário de Atendimento, há detalhes sobre o Tratamento de dados pela CentralIT.

- *Informações sobre os tipos dos dados pessoais tratados*

O Ministério da Economia trata dados pessoais que identificam ou que podem identificar o titular como um cidadão, para o uso seguro do Serviço conta gov.br. As categorias de dados tratados são:

  - Identificação atribuídas por instituições governamentais/Biográfico: Número do CPF e Dados de vinculação de empresas do gov.br (CNPJ);
  - Identificação pessoal/Biográfico: Nome, E-mail, Telefone, Endereço
  - Segurança: Senha e Nível de Segurança/ Confiabilidade da conta (ouro, prata e bronze);
  - Identificação eletrônica: Endereço IP;
  - Dados de Imagem: Imagem de Perfil;
  - Detalhes pessoais/Biográfico: Data de nascimento, Naturalidade;
  - Dados de membros da família/Biográfico: Nome da mãe;
  - Dado Biométrico/Sensível: Foto-selfie

Essas categorias são do Guia de inventario de dados pessoais.

- *Período de retenção*

Os dados pessoais armazenados nas bases de dados do Serviço conta gov.br, durante o período que o usuário tem conta são: Foto/selfie, CPF, nome, e-mail, telefone, endereço, imagem de perfil, senha e nível de confiabilidade. Além desses, também é armazenado o CNPJ, caso a conta tenha vinculação de empresa.
Os dados pessoais de data de nascimento, naturalidade e nome da mãe são retidos apenas durante o processo de validação dos dados e para a apresentação no Aplicativo.
Os dados apresentados no aplicativo (nome, CPF, data de nascimento, naturalidade, nome da mãe, e-mail, telefone e endereço) ficam em área restrita do dispositivo móvel, com permissão de acesso apenas pelo aplicativo gov.br. Esses dados são consultados na base da RFB e atualizados no aplicativo a cada 7 dias.
A foto-selfie, capturada no aplicativo gov.br, é armazenada na base de dados do Serviço conta gov.br. Futuramente essa mesma foto-selfie será usada pela versão web do Serviço conta gov.br, em substituição a imagem de perfil. Se o titular decidir trocar a foto-selfie, a nova é comparada com a anterior, em vez de realizar nova validação biométrica nas bases da ICN e Renach, pois é um processo caro, custoso e com capacidade limitada de resposta.
É possível alteração direto no Serviço conta gov.br para os dados de nome, e-mail, telefone, endereço e imagem de perfil.
O endereço pode ser excluído.

Os dados de registros (logs), que contemplam CPF, data do evento, endereço IP e eventos realizados, permitindo a rastreabilidade, ficam retidos.

A Tabela 1 apresenta a descrição dos dados pessoais. Na coluna Natureza, verifica-se a categoria de cada dado, se o dado é biográfico, biométrico e sensível ou não. Na coluna Origem/Validação, verifica-se a fonte, se apenas pelo titular ou, se na validação dos dados, pelas bases da RFB, ICN e Renach, ou no recebimento de dados de Bancos ou de Certificados Digitais. Na coluna Finalidades, verificam-se todas as finalidades para qual o dado é tratado. Na coluna Hipóteses estão as hipóteses alinhadas às finalidades e por fim a última coluna apresenta a duração(retenção) do Tratamento. O tempo de retenção apresentado se refere à base de dados do Serviço conta gov.br, ou seja, os dados pessoais são tratados enquanto o titular possuir conta gov.br. No caso dos logs referentes ao uso da conta, estes são tratados durante o tempo que o usuário possuir conta e após a exclusão da conta.

Alguns dos dados, listados na Tabela 1, também são armazenados por cookies estritamente necessários do Serviço conta gov.br. No Anexo A há mais detalhes sobre esses cookies.

Tabela 1 - Descrição dos dados pessoais

Natureza/ Categoria	Dado Pessoal	Origem/ Validação	Finalidade	Hipóteses de Tratamento	Tempo de Retenção
Identificação atribuídas por instituições governamentais Biográfico	**Número do CPF**	Titular/RFB, Bancos e Certificado Digital	Identificar por biografia, Identificar por biometria, Preencher cadastro, Notificar e Monitorar Identificar GaaP	Obrigação Legal e Políticas Públicas Consentimento	Até solicitação expressa do Titular para exclusão da conta. Depois da conta excluída, os dados de logs ficam retidos.
Identificação pessoal Biográfico	**Nome**	Titular/RFB, Bancos e Certificado Digital	Identificar por biografia, Preencher cadastro, Notificar e Monitorar	Obrigação Legal e Políticas Públicas	Até solicitação expressa do Titular para exclusão da conta. Depois da conta excluída, os dados de logs ficam retidos.

			Identificar GaaP	Consentimento	Titular pode alterar direto no serviço conta gov.br.
Identificação pessoal Biográfico	**E-mail**	Titular	Preencher cadastro e Notificar Entrar em contato GaaP	Obrigação Legal e Políticas Públicas Consentimento	Até solicitação expressa do Titular para exclusão da conta. Depois da conta excluída, os dados de logs ficam retidos. Titular pode alterar direto no serviço conta gov.br.
Identificação pessoal Biográfico	**Telefone**	Titular	Preencher cadastro e Notificar Entrar em contato GaaP	Obrigação Legal e Políticas Públicas Consentimento	Até solicitação expressa do Titular para exclusão da conta. Depois da conta excluída, os dados de logs ficam retidos. Titular pode alterar direto no serviço conta gov.br.
Identificação pessoal Biográfico	**Endereço**	Titular	Preencher cadastro	Políticas Públicas	Até solicitação expressa do

			Entrar em contato GaaP	Consentimento	Titular para exclusão da conta. Depois da conta excluída, os dados de logs ficam retidos. Titular pode alterar ou excluir direto no serviço conta gov.br.
Segurança	**Senha**	Titular	Identificar por biografia	Políticas Públicas	Até solicitação expressa do Titular para exclusão da conta. Titular pode alterar direto no serviço conta gov.br.
Identificação eletrônica	**Endereço IP**	Titular	Monitorar	Obrigação Legal	Até solicitação expressa do Titular para exclusão da conta. Depois da conta excluída, os dados de logs ficam retidos.
Dados de Imagem	**Imagem de Perfil**	Titular	Preencher cadastro	Políticas Públicas	Até solicitação expressa do Titular para exclusão da conta. Depois da conta excluída, os dados de

					logs ficam retidos. Titular pode alterar direto no serviço conta gov.br.
Detalhes pessoais Biográfico	**Data de nascimento**	Titular e RFB	Identificar por biografia	Obrigação Legal e Políticas Públicas	Durante o processo de validação. Não há armazenamento do dado na base do serviço conta gov.br
Detalhes pessoais Biográfico	**Naturalidade**	Titular e RFB	Identificar por biografia	Obrigação Legal e Políticas Públicas	Durante o processo de validação. Não há armazenamento do dado na base do serviço conta gov.br
Membros da família Biográfico	**Nome da mãe**	Titular e RFB	Identificar por biografia	Obrigação Legal e Políticas Públicas	Durante o processo de validação. Não há armazenamento do dado na base do serviço conta gov.br
Dado Biométrico/ **Sensível**	**Foto-selfie**	Titular	Identificar por biometria	Dado Sensível (Obrigação legal, Políticas Públicas, identificação e autenticação)	Até solicitação expressa do Titular para exclusão da conta. Depois da conta excluída, os dados de logs ficam retidos. Titular pode alterar no Aplicativo.

MINISTÉRIO DA ECONOMIA

Segurança	**Nível de Confiabilidade da conta (ouro, prata e bronze)**	Serviço conta gov.br	Identificar por biografia, Preencher cadastro Monitorar Identificar GaaP	Obrigação Legal e Políticas Públicas Consentimento	Até solicitação expressa do Titular para exclusão da conta. Depois da conta excluída, os dados de logs ficam retidos. Titular pode alterar direto no serviço conta gov.br.
Identificação atribuídas por instituições governamentais	**Dados de vinculação de empresas do gov.br (CNPJ)**	Certificado Digital de pessoa jurídica	Identificar por biografia, Preencher cadastro Monitorar	Obrigação Legal e Políticas Públicas	Até solicitação expressa do Titular para exclusão da conta. Depois da conta excluída, os dados de logs ficam retidos.

- *Volume, extensão e frequência em que os dados são tratados*

São tratados 15 dados pessoais, sendo 1 dado pessoal sensível. Estima-se uma quantidade de 30GB de retenção dos dados pessoais. A frequência de tratamento dos dados pessoais é 24x7 (vinte e quatro horas por dia nos sete dias da semana).

- *Número de titulares de dados afetados pelo tratamento*

Em outubro de 2022, o número de titulares cadastrados é de mais de 138 milhões de titulares únicos, com expectativa de chegar a 145 milhões até o final de 2022.
Para os compartilhamentos dos dados de contato através do piloto do Modelo de Governo como Plataforma, o volume será de até um 200 mil de tratamentos, distribuídos e limitados a, no máximo, 20 mil consultas com sucesso por empresa/organização participante do projeto.

- *Abrangência da área geográfica do tratamento*

Os dados pessoais associados à conta do gov.br são tratados em território nacional (Brasil).

3.3 – CONTEXTO DO TRATAMENTO

Nesta seção são destacados:

- natureza do relacionamento do Ministério da Economia com o titular de dados;
- nível ou método de controle que o titular de dados exerce sobre seus dados pessoais;
- se o tratamento realizado está de acordo com o que é determinado em leis e regulamentos, e comunicado pela instituição ao titular de dados;
- destaque de avanços relevantes do Ministério da Economia em tecnologia ou segurança que contribuem para a proteção dos dados pessoais.

- *Natureza do relacionamento com os titulares*

O Ministério da Economia, no âmbito de seu relacionamento público, pelo Serviço conta gov.br, é centrado no titular que necessita de uma conta para ter acesso aos serviços digitais. Desta maneira, permite que o titular configure uma conta online, prove quem é e use essa única conta para acessar diferentes serviços públicos digitais.
O compartilhamento dos dados do serviço conta, minimizado aos dados de contato, e-mail telefone e endereço, e método de autenticação, por meio do piloto do Modelo de Governo como Plataforma, permite conectar **os setores governamental e não governamental por meio do empoderamento do titular no uso de seus dados pessoais para melhorar a experiência no consumo de serviços públicos e privados** de seu interesse, estimulando a inovação e a atividade econômica do país. Este modelo estabelece as regras e condições para o reuso dos dados que estão em posse do Poder Público.

- *Método de controle que os indivíduos exercem sobre seus dados*

Os titulares de dados pessoais podem autorizar o compartilhamento de seus dados, retirar

sua autorização e atualizar seus dados diretamente no Serviço conta gov.br e exercer outros direitos através do canal Fala.BR. Mais detalhamento no tópico 5.

Para o piloto do Modelo Governo como plataforma:

Os titulares de dados pessoais podem autorizar o login e revogar sua autorização diretamente no serviço de contas gov.br e consentir o compartilhamento de seus dados de contatos, além de exercer outros direitos previstos na LGPD, diretamente no aplicativo gov.br e do canal Fala.BR.

- *Expectativa do titular*

O Aviso de Privacidade, disponível no Serviço conta gov.br, visa esclarecer ao titular como seus dados pessoais serão tratados, além de seus direitos e deveres. Este relatório fornece transparência, credibilidade e confiança ao titular gerando uma expectativa positiva de que seus dados pessoais estão sob um viés regulamentar o que traz segurança ao detentor destes dados.

Para o piloto do Modelo Governo como plataforma, este papel cabe à solicitação de consentimento que traz o esclarecimento necessário para subsidiar a decisão do titular de dados pessoais quanto ao compartilhamento de seus dados.

- *Tecnologia e segurança para proteção dos dados pessoais*

O Ministério da Economia e o Serpro atuam em conjunto e constantemente na área de segurança de informação e seguem o Guia de Avaliação de Riscos de Segurança e Privacidade, elaborado pela equipe técnica de segurança da informação da SGD, com base na Lei Geral de Proteção de Dados.

O guia apresenta o embasamento teórico utilizado, a organização dos temas segurança da informação e privacidade com 113 controles propostos para avaliação dos riscos de segurança da informação e privacidade. Todas essas etapas não apenas servem como uma oportunidade de identificação de lacunas e evitar incidentes de segurança da área de tecnologia como também são insumos para a elaboração deste Relatório de Impacto à Proteção de Dados Pessoais.

O processo de análise e tratamento dos riscos, indicado por este Guia, tem como referência normas e práticas reconhecidas internacionalmente e algumas das principais referências são:

ABNT NBR ISO/IEC 27001:2013: Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da

informação

ABNT NBR ISO/IEC 27002:2013: Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação.

ABNT NBR ISO/IEC 27005:2019: Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação.

ABNT NBR ISO/IEC 27701:2019: Técnicas de segurança — Extensão da ABNT NBR ISO/IEC

27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes.

ABNT NBR ISO/IEC 31000:2018: Gestão de Riscos.

3.4 – FINALIDADE DO TRATAMENTO

Nesta seção, é detalhado o que se pretende alcançar com o tratamento dos dados pessoais, em harmonia com as hipóteses do arts. 7 º e 11 da LGPD), no que for aplicável, indicando:

- Finalidades e hipóteses de tratamento
- Resultados pretendido para os titulares dos dados pessoais, informando o quão importantes são esses resultados.
- Benefícios esperados para o Ministério da Economia.

- *Finalidades*

No âmbito do Serviço conta gov.br, os dados pessoais são tratados com as finalidades de:

- Provar a identidade do titular (identificação), por validação biométrica **(Identificar por biometria)** e validação biográfica **(Identificar por biografia);**
- Autenticar o titular para acesso aos serviços governamentais digitais **(Autenticar);**
- Compartilhar dados pessoais para preencher cadastros de serviços governamentais (**Preencher cadastro);**
- Enviar mensagens para recuperar conta por SMS ou e-mail, notificar sobre registros de ações na conta e notificar sobre incidentes de segurança **(Notificar);**
- Monitorar, detectar e investigar fraudes **(Monitorar).**

Para o projeto piloto do modelo Governo como Plataforma, o compartilhamento de dados será realizado para duas finalidades:

- Provar a identidade do titular, através da conta gov.br **(Identificar gaap)** e
- Obter dados para entrar em contato nas relações institucionais **(Entar em contato gaap)**

- *Hipóteses de tratamento*

O tratamento de dados pessoais para a finalidade de **Identificar por biometria** é realizado nas seguintes hipóteses da Lei nº 13.709, de 2018, Seção II Do Tratamento de Dados Pessoais Sensíveis, artigo 11:

- II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para**:**

  a) cumprimento de obrigação legal ou regulatória pelo controlador; **(Dado Sensível/Obrigação legal)**

b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em Leis ou regulamentos; **(Dado Sensível/Políticas Públicas)**
g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais. **(Dado Sensível/identificação e autenticação).**

Os tratamentos de dados para as finalidades de **Identificar por biografia, Autenticar, Preencher cadastro, Notificar e Monitorar** são realizados nas seguintes hipóteses da Lei nº 13.709, Seção I, artigo 7:

- II - para o cumprimento de obrigação legal ou regulatória pelo controlador. **(Obrigação legal)**

- III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em Leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV da Lei nº 13.709, de 2018. **(Políticas Públicas)**

Para o piloto do Modelo Governo como Plataforma, os tratamentos de dados para as finalidades de **Identificar Gaap** e **Entrar em contato Gaap** através do compartilhamento dos dados com o setor não governamental, são realizados na hipótese da Lei nº 13.709, Seção I, artigo 7:

- I - mediante o fornecimento de consentimento pelo titular. **(Consentimento)**

- *Resultados pretendidos para os titulares*

Alcançar a total autonomia do titular para exercer a sua cidadania de forma confiável e efetiva perante os órgãos públicos, ofertando ao titular o acesso a serviços públicos por meio digital, sem necessidade de solicitação presencial ou se utilizar de serviços terceiros.
Para o piloto do Modelo Governo como Plataforma:
Alcançar a autonomia do titular para exercer a sua cidadania de forma confiável e efetiva, ofertando ao titular o controle no processo de compartilhamento de dados com o setor não governamental.

- *Benefícios esperados para o Ministério da Economia*

Redução de custos e fraudes no oferecimento de vários serviços públicos, trazendo maior segurança à população. Cabe lembrar que não somente será o único beneficiário, pois o serviço envolve vários órgãos federais, estaduais e municipais.
Para o piloto do Modelo Governo como Plataforma:
Os principais benefícios pretendidos no projeto Governo como Plataforma são:
I - Para o governo:
a) Políticas públicas mais efetivas;
b) Serviços públicos simplificados; e

c) Relacionamento mais próximo ao cidadão.
II - Para o cidadão:
a) Maior satisfação e segurança no uso dos serviços públicos e privados;
b) Controle sobre seus dados; e
c) Ampliação da oferta de serviços personalizados, mediante consentimento específico, explícito e informado ao titular.
III - Para as empresas:
a) Maior entrega de valor ao cliente;
b) Geração de negócios inovadores;
c) Redução de fraudes; e
d) Melhoria do ambiente de negócios e do empreendedorismo.

4 – PARTES INTERESSADAS CONSULTADAS

Nessa seção, foi identificado:
• quais partes foram consultadas, e
• o que cada parte consultada indicou como importante de ser observado para o tratamento dos dados pessoais em relação aos possíveis riscos referentes às atividades de tratamento em análise. Também foram observados os riscos de não-conformidade ante a LGPD e os instrumentos internos de controle.

- *Encarregada*

Forneceu orientações quanto ao tratamento de dados pessoais no Serviço conta gov.br e ao processo de elaboração deste RIPD.

- *Partes gerenciais*

Coordenadores, servidores e diretores do Ministério da Economia, a fim de obter informações técnicas e administrativas sobre o processo de trabalho executado no âmbito do Serviço conta gov.br.

- *Partes operacionais*

Coordenação Geral de Segurança da Informação do Ministério da Economia, Serpro e Central IT, que indicaram oportunidades de melhoria para aperfeiçoamento da proteção dos dados pessoais a respeito da LGPD e dos critérios de segurança da informação.

- *Titulares*

Titulares que utilizam a plataforma não foram consultados mediante pesquisa, eles expressaram sua opinião na loja de aplicativos móveis e em canais oficiais do governo, como as ouvidorias, reclamando das autoridades ações para melhoria do Serviço conta gov.br

5 – NECESSIDADE E PROPORCIONALIDADE

Nesta seção, é descrito como é avaliada a necessidade e proporcionalidade dos dados, demonstrando que as operações realizadas sobre os dados pessoais limitam o tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados (LGPD, art. 6º, III). Nesse sentido, é destacado:

- A fundamentação legal para o tratamento dos dados pessoais;
- Como será garantida a qualidade [exatidão, clareza, relevância e atualização dos dados] e minimização dos dados;
- Quais controles são adotados a fim de assegurar que o operador (LGPD, art. 5º, VII) realize o tratamento de dados pessoais conforme a LGPD e respeite os critérios estabelecidos pela instituição que exerce o papel de controlador (LGPD, art. 5º, VI);
- Como estão implementadas as medidas que asseguram o direito de o titular dos dados pessoais obter do controlador o previsto pelos art. 18, 19 e 20 da LGPD.;
- Como são fornecidas informações de como ocorre o tratamento de dados pessoais para os titulares;
- Quais são as salvaguardas para as transferências internacionais de dados.

- *Fundamentação legal para o tratamento dos dados pessoais*

Para respaldar a necessidade do tratamento de dados, na hipótese de **Obrigação legal, Dado Sensível/Obrigação legal e Identificação e autenticação**, há previsão legal constante nos seguintes normativos:

> Decreto 10.900, de 2021:
> Art. 8º O Serviço de Identificação do Cidadão, para verificar a identidade das pessoas naturais, verificará os dados biográficos e biométricos disponíveis:
> I - na Base de Dados da Identidade Civil Nacional, de que trata a Lei nº 13.444, de 2017;
> II - no Cadastro Base do Cidadão, de que trata o Decreto nº 10.046, de 9 de outubro de 2019; e
> III - em outras bases biométricas de identificação do cidadão que estejam acessíveis ao Governo federal.
>
> Art. 10. As amostras biométricas das bases de dados sob a gestão dos órgãos e das entidades da administração pública federal serão interoperáveis entre si e com a base de dados da Identidade Civil Nacional por meio do Serviço de Identificação do Cidadão.
> § 1º As bases biométricas da administração pública federal terão ferramentas para integração com as bases biométricas dos órgãos de identificação dos Estados e do Distrito Federal.
> § 2º O número do CPF será utilizado como chave para interoperabilidade das bases biométricas.

Decreto 8.936, de 2016:
Art. 1º Fica instituída a Plataforma gov.br, no âmbito da administração pública federal direta, autárquica e fundacional, com a finalidade de: (Redação dada pelo Decreto nº 10.900, de 2021)
...
III - disponibilizar, em plataforma única e centralizada, mediante o nível de autenticação requerido, o acesso às informações e a prestação direta dos serviços públicos;
Art. 3º Compõem a Plataforma gov.br: (Redação dada pelo Decreto nº 10.900, de 2021)
...
II - o mecanismo de acesso digital único do usuário aos serviços públicos, com nível de segurança compatível com o grau de exigência, natureza e criticidade dos dados e das informações pertinentes ao serviço público solicitado;
III - a ferramenta de solicitação e acompanhamento dos serviços públicos, com as seguintes características:
a) identificação do serviço público e de suas principais etapas;
V - o painel de monitoramento do desempenho dos serviços públicos prestados, com, no mínimo, as seguintes informações para cada serviço, órgão ou entidade da administração pública federal:
VII - a ferramenta de notificações e mensageria aos usuários de serviços públicos de caixa postal eletrônica; (Redação dada pelo Decreto nº 10.900, de 2021)

Decreto nº 10.332, de 2020
Art. 9º O Anexo I ao Decreto nº 9.319, de 2018, passa a vigorar com as seguintes alterações:
Os objetivos a serem alcançados, por meio da Estratégia de Governo Digital incluem:
- promover a integração e a interoperabilidade das bases de dados governamentais;
- disponibilizar a identificação digital ao cidadão;
Iniciativa 6.1. Interoperar os sistemas do Governo federal, de forma que, no mínimo, seiscentos serviços públicos disponham de preenchimento automático de informações relacionadas ao Cadastro Base do Cidadão, ao Cadastro Nacional de Pessoa Jurídica e ao Cadastro de Endereçamento Postal, até 2022. (Redação dada pelo Decreto nº 10.996, de 2022)

Lei nº 13.709, de 2018, LGPD, que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.
Lei nº 12.965, de 2014 - Marco Civil da Internet – Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

> **Decreto n° 8.771/2016**, que regulamenta a Lei nº 12.965, de 23 de abril de 2014, (Marco Civil da Internet).

Para respaldar a necessidade de tratamento de dados, nas hipóteses de **Políticas Públicas** e **Dado sensível/Políticas Públicas**, há previsão legal constante no seguinte normativo:

> **Decreto nº 10.609, de 2021:**
> Art. 4º São diretrizes da Política Nacional de Modernização do Estado:
> …
> VII - ampliar o acesso e a qualidade dos serviços públicos; e
> VIII - promover a transformação digital da gestão e dos serviços.
> ...
> Art. 5º A Política Nacional de Modernização do Estado será implementada com observância aos seguintes eixos temáticos:
> III - evolução dos serviços públicos - desburocratização e simplificação na prestação dos serviços públicos, com ampliação da efetividade na ação governamental, de modo a garantir o atendimento das necessidades da sociedade;
> ...
> V - governo e sociedade digital - transformação digital do País, com atenção à governança de dados, à internet das coisas, à digitalização da economia, à digitalização de serviços, à integração das bases e à estrutura de conectividade.

Demais Normativos que autorizam o tratamento de dados encontram-se no Anexo B.

- *Garantia da qualidade e minimização dos dados*

No cadastro da conta, os dados de identificação são validados com entes do Governo, Bancos credenciados e Provedores de Certificados Digitais, conforme descrito no Tópico 3.1 deste relatório e os dados de contato são fornecidos pelo titular, que manifesta ciência do Termo de Uso do Serviço conta gov.br, no qual destaca-se a responsabilidade do titular informar dados verdadeiros e atualizados.
O controlador se responsabiliza por informar ao titular quando houver mudanças, referente ao tratamento de dados, no Aviso de Privacidade.
Para os dados de nome, de contato, foto selfie e imagem de perfil é possível alteração direto no Serviço conta gov.br e esses dados são apenas alterados na base de dados do Serviço conta gov.br, não havendo nenhuma alteração nas bases de dados da qual se originou o dado, RFB, Bancos e Provedores de serviços digitais. Os serviços integrados podem ter seus dados atualizados, de acordo com as regras de negócios do mesmo.
A escolha dos dados coletados para implementação do Serviço conta gov.br foi resultado de intensos estudos realizados pelo Ministério da Economia com a preocupação de coletar o mínimo de dados necessários para execução da política pública relacionados a esse programa.

- *Controles para assegurar a conformidade do operador*

Por ter toda a estrutura do Serviço conta gov.br dentro dos centros de processamento de dados do Serpro, o Ministério da Economia provê pontos de controle semanais a fim de acompanhar as conformidades com as diretrizes definidas pelo Ministério da Economia. Diretrizes estas que contêm a avaliação de risco presente neste relatório. Devido a esse modelo de negócio, o operador tem o compromisso de não fazer uso dos dados do Serviço conta gov.br para fins diversos do acordado com o controlador. Melhorias constantes são realizadas no Serviço conta gov.br, visando adequá-la aos preceitos expostos na LGPD sob o conceito *"Privacy-by-default"* e assim internalizando, cada vez mais, a proteção dos dados pessoais na plataforma proposta. Mais sobre os controles de segurança e privacidade no Anexo B.

- *Medidas que asseguram o direito do titular dos dados pessoais*

O titular é informado sobre o tratamento de seus dados pessoais e seus direitos através do Aviso de Privacidade. (https://p2.appgovbr.estaleiro.serpro.gov.br/api/legal)

A página https://consentimento.acesso.gov.br/, permite ao titular verificar seus dados compartilhados e pode desautorizar os compartilhamentos futuros.

Diretamente no Serviço conta gov.br é permitido ao titular consulta, exclusão e alteração de dados pessoais, conforme explicado no Tópico 3.2.
Para o titular exercer os demais direitos, como exclusão da conta, há o canal Fala.BR.

Marta Juvina de Medeiros, contato: Fala.BR (falabr.cgu.gov.br)
Endereço: Ministério da Economia. Esplanada dos Ministérios, Bloco P, 4º andar, sala 425. CEP 70048-900. Brasília/DF.

Para o Modelo Governo como Plataforma em sua fase piloto, os consentimentos e as consultas e/ou revogações a estes, bem como os históricos de consultas às bases de governo realizados pelas empresas/organizações participantes, poderão ser acessados através do aplicativo gov.br.

- *Salvaguardas para as transferências internacionais de dados*

O Ministério da Economia não realiza qualquer tipo de transferência internacional de dados, para os dados pessoais apresentados neste relatório de impacto.
Para o piloto do Modelo de Governo como Plataforma, no que se refere ao tem transferência internacional, as empresas/organizações participantes deverão considerar o disposto no Capítulo V da LGPD.

6 – IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS

O art. 5º, XVII da LGPD preconiza que o Relatório de Impacto deve descrever "medidas, salvaguardas e mecanismos de mitigação de risco ".
Antes de definir tais medidas, salvaguardas e mecanismos, é necessário identificar os riscos

que geram impacto potencial sobre o titular dos dados pessoais.

Os riscos elencados neste relatório foram adaptados da norma ISO/IEC 29134:2017, que trata de técnicas de segurança para a avaliação do impacto à privacidade.

Para cada risco, define-se: a probabilidade de ocorrência do evento de risco, o possível impacto caso o risco ocorra, avaliando o nível potencial de risco para cada evento.

A classificação dos riscos, os níveis de probabilidade, de impacto e de riscos indicados na Tabela 5 foram obtidos do resultado da ferramenta recomendada pela SGD. Esta ferramenta contém um questionário sobre as 113 medidas de segurança e privacidade, elencadas no Checklist do Anexo I do Guia de Avaliação de Riscos de Segurança e Privacidade da SGD.
Para cada medida, há três respostas: Sim, Não e Não se Aplica. Quando a resposta é **Sim**, quer dizer que a medida já foi implementada. Quando a resposta é **Não**, quer dizer que a medida está associada ao risco, mas ainda não foi implementada. Quando a resposta é **Não se aplica**, quer dizer que não cabe ao risco.
Cada medida deste questionário, tem um peso, de acordo com o tipo de Risco, conforme os anexos II.A, II.B e II.C do Guia da SGD.
Com as respostas ao Questionário e esses pesos das medidas, a ferramenta recomendada pela SGD calcula os valores de Probabilidade e Impacto, aplicando as fórmulas abaixo:

Probabilidade = Total de Pesos das Medidas de **Prevenção** Aplicadas ao Risco / (Total de Pesos dos Medidas de Prevenção Associados ao Risco – Total de Pesos das Medidas de Prevenção Que Não se Aplica ao Risco).

Impacto = Total de Pesos das Medidas de **Mitigação** Aplicadas ao Risco / (Total de Pesos das Medidas de Mitigação Associados ao Risco – Total de Pesos das Medidas de Mitigação Que Não se Aplica ao Risco).

Os resultados das fórmulas acima são referentes à porcentagem de medidas implementadas e elas serão representadas por valores escalares. Os valores serão de acordo com as Tabelas 2 e 3. Na tabela 2 é determinado se o resultado se classifica em Alta, Média ou Baixa para a Probabilidade e Alto ou Moderado para o Impacto.

Tabela 2- Parâmetros escalares

Medidas Implementadas	Probabilidade	Impacto
0% a 50%	Alta	
50% a 85%	Moderada	Alto
85% a 100%	Baixa	Moderado

Na Tabela 3, parâmetros escalares foram utilizados para representar os níveis de probabilidade e impacto que, após a multiplicação, resultarão nos níveis de risco, que direcionarão a aplicação de controles de segurança.

Tabela 3- Parâmetros escalares

Classificação	Valor
Baixo	5
Moderado	10
Alto	15

A Tabela 4 apresenta a Matriz Probabilidade x Impacto, instrumento de apoio para a definição dos critérios de classificação do nível de risco.

Tabela 4– Probabilidade x Impacto

Probabilidade (P)				
	15	75	150	225
	10	50	100	150
	5	25	50	75
		5	10	15
			Impacto (I)	

O produto da probabilidade pelo impacto de cada risco deve se enquadrar em uma região da matriz apresentada pela Tabela 4. Risco que se enquadra na região:

- verde, é entendido como baixo;
- amarelo, representa risco moderado; e
- vermelho, indica risco alto.>

A Tabela 5 apresenta os riscos inerentes, ou seja, todos os riscos ao qual o serviço está exposto, quando não há aplicação de nenhum controle. Ou seja, o questionário das 113 medidas foi respondido apenas com “Não” e “Não se aplica”, para demonstrar o nível de riscos altos a quais o serviço fica sujeito, caso as medidas não sejam implementadas.

Tabela 5 – Riscos Inerentes antes de qualquer medida implementada.

Id	Risco referente ao tratamento de dados pessoais	P	I	Nível de Risco (P x I)
R01	Acesso não autorizado	15	15	225 (Alto)
R02	Coleção Excessiva	15	15	225 (Alto)
R03	Compartilhar ou distribuir dados pessoais com terceiros fora da administração pública federal sem o consentimento do titular dos dados pessoais	15	15	225 (Alto)
R04	Falha em considerar os direitos do titular dos dados pessoais (Ex.: perda do direito de acesso)	15	15	225 (Alto)
R05	Falha ou erro de processamento (Ex.: execução de script de banco de dados que atualiza dado pessoal com informação equivocada, ausência de validação dos dados de entrada, etc.)	15	15	225 (Alto)
R06	Informação insuficiente sobre a finalidade do tratamento	15	15	225 (Alto)
R07	Modificação não autorizada	15	15	225 (Alto)
R08	Perda	15	15	225 (Alto)
R09	Reidentificação de dados pseudonimizados	15	15	225 (Alto)
R10	Remoção não autorizada	15	15	225 (Alto)
R11	Retenção prolongada de dados pessoais sem necessidade	15	15	225 (Alto)
R12	Roubo	15	15	225 (Alto)
R13	Tratamento sem consentimento do titular dos dados pessoais (Caso o tratamento não esteja previsto em legislação ou regulação pertinente)	15	15	225 (Alto)
R14	Vinculação ou associação indevida, direta ou indireta, dos dados pessoais ao titular	15	15	225 (Alto)

Legenda: P – Probabilidade; I – Impacto.

[1] Probabilidade: chance de algo acontecer, não importando se definida, medida ou determinada objetiva ou subjetivamente, qualitativa ou quantitativamente, ou se descrita utilizando-se termos gerais ou matemáticos (ISO/IEC 31000:2009, item 2.19).

[2] Impacto: resultado de um evento que afeta os objetivos (ISO/IEC 31000:2009, item 2.18).

[3] Nível de Risco: magnitude de um risco ou combinação de riscos, expressa em termos da combinação das consequências e de suas probabilidades (ISO/IEC 31000:2009, item 2.23 e IN SGD/ME nº 1, de 2019, art. 2º, inciso XIII).

7 – CONTROLES PARA TRATAR OS RISCOS

Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito (LGPD, art. 46.).

Os controles, apresentados neste relatório, são um conjunto de medidas de segurança e/ou privacidade, que implementados diminuem o nível do risco.

A Tabela 6 é resultado da última avaliação de riscos do acesso.gov.br, com a maioria dos controles de segurança e privacidade já implementados.

A classificação dos riscos, os níveis de probabilidade, de impacto e de riscos indicados na Tabela 5 foram obtidos através da ferramenta recomendada pela SGD, no dia 20/09/2022. Esta ferramenta contém um questionário, que foi respondido pelas equipes de segurança do Serpro e do Departamento de Canais e Identidade Digital do Ministério da Economia.

A utilização dos termos "controle" e "medidas" estão alinhados com o CIS Controls - controle (mais genérico, categoria), medida de segurança (ações mais específicas).

As medidas estão divididas e agrupadas em características comuns. Esses agrupamentos serão apresentados como Controles de segurança e de privacidade e têm como referência as normas ABNT NBR ISO/IEC 27002:2013 (escopo de segurança da informação) e ISO/IEC 29100:2011 (escopo de privacidade). Os Controles e as medidas aplicadas podem ser analisados na Planilha de Avaliação de Riscos.

O Efeito sobre o Risco é resultante do tratamento do risco com a aplicação do(s) Controles(s). As seguintes opções podem ser selecionadas: Reduzir, Evitar, Compartilhar e Aceitar.

As Colunas de Riscos é a mesma do Tópico 6, já os valores de Probabilidade, Impacto e Nível, comparadas com a tabela 5, apresentada no Tópico 6, foram alteradas, a maioria diminuindo seu nível, devido à implementação dos Controles. Os riscos apresentados na Tabela 7 não são residuais, visto que ainda há planejamento de medidas para redução dos riscos.

As medidas implementadas e a serem implementadas estão na Planilha de Avaliação de Riscos, com demandas abertas e prazos e/ou ações desempenhadas.

Tabela 6 – Controles e Medidas para tratar os Riscos

Risco ID	**Controle(s)**	**Efeito sobre o Risco**				**Medida (s) Aprovada (s)**
			P	**I**	**Nível (P x I)**	
R01	Responsabilização; Compliance com a Privacidade; Gestão de Mudanças; Gestão de Riscos; Resposta a Incidente; Cópia de Segurança; Controles de Acesso Lógico; Registro de Eventos, Rastreabilidade e Salvaguarda de Logs; Desenvolvimento Seguro; Controles de Segurança em Redes, Proteção Física e do Ambiente; Legitimidade e Especificação de	Reduzir	5	10	50	Sim

	Propósito; Controles Criptográficos; Segurança Web; Controle de Acesso e Privacidade; Continuidade de Negócio;					
R02	Responsabilização; Compliance com a Privacidade; Gestão de Mudanças; Gestão de Riscos; Resposta a Incidente; Cópia de Segurança; Controles de Acesso Lógico; Registro de Eventos, Rastreabilidade e Salvaguarda de Logs; Desenvolvimento Seguro; Controles de Segurança em Redes, Proteção Física e do Ambiente; Legitimidade e Especificação de Propósito; Controles Criptográficos; Segurança Web; Controle de Acesso e Privacidade; Continuidade de Negócio	Reduzir	5	15	75	Sim
R03	Responsabilização; Compliance com a Privacidade; Gestão de Mudanças; Desenvolvimento Seguro; Legitimidade e Especificação de Propósito	Reduzir	5	15	75	Sim
R04	Responsabilização; Compliance com a Privacidade; Gestão de Mudanças; Cópia de Segurança; Abertura, Transparência e Notificação; Legitimidade e Especificação de Propósito; Participação Individual e Acesso; Gestão de Riscos; Controles de Segurança em Redes, Proteção Física e do Ambiente; Desenvolvimento Seguro; Controles de Acesso Lógico; Segurança Web; Uso, Retenção e Limitação de Divulgação; Precisão e qualidade; Gestão de Capacidade e Redundância;	Reduzir	5	15	75	Sim
R05	Responsabilização; Compliance com a Privacidade; Gestão de Mudanças; Legitimidade e Especificação de	Reduzir	10	15	150	Sim

	Propósito; Cópia de Segurança; Precisão e qualidade; Gestão de Capacidade e Redundância; Continuidade de Negócio					
R06	Compliance com a Privacidade; Abertura, Transparência e Notificação; Responsabilização; Gestão de Mudanças; Gestão de Riscos; Legitimidade e Especificação de Propósito	Reduzir	10	10	100	Sim
R07	Responsabilização; Compliance com a Privacidade; Controles de Segurança em Redes, Proteção Física e do Ambiente; Gestão de Mudanças; Gestão de Riscos; Resposta a Incidente; Cópia de Segurança; Legitimidade e Especificação de Propósito; Controles de Acesso Lógico; Registro de Eventos, Rastreabilidade e Salvaguarda de Logs; Desenvolvimento Seguro; Controles Criptográficos; Segurança Web; Controle de Acesso e Privacidade; Continuidade de Negócio;	Reduzir	5	10	50	Sim
R08	Responsabilização; Compliance com a Privacidade; Gestão de Mudanças; Gestão de Riscos; Resposta a Incidentes; Cópia de Segurança; Legitimidade e Especificação de Propósito; Controles de Acesso Lógico; Desenvolvimento Seguro; Registro de Eventos, Rastreabilidade e Salvaguarda de Logs; Controles de Segurança em Redes, Proteção Física e do Ambiente; Controle de Acesso e Privacidade; Gestão de Capacidade e Redundância; Continuidade de Negócio; Controles Criptográficos; Segurança	Reduzir	5	10	50	Sim

	Web;					
R09	Responsabilização; Compliance com a Privacidade; Gestão de Mudanças; Desenvolvimento Seguro; Legitimidade e Especificação de Propósito; Uso, Retenção e Limitação de Divulgação;	Reduzir	10	15	150	Sim
R10	Responsabilização; Compliance com a Privacidade; Gestão de Mudanças; Gestão de Riscos; Resposta a Incidente; Cópia de Segurança; Controles de Acesso Lógico; Registro de Eventos, Rastreabilidade e Salvaguarda de Logs; Legitimidade e Especificação de Propósito; Controles de Segurança em Redes, Proteção Física e do Ambiente; Desenvolvimento Seguro; Controles Criptográficos; Segurança Web; Controle de Acesso e Privacidade; Continuidade de Negócio;	Reduzir	5	10	50	Sim
R11	Responsabilização; Compliance com a Privacidade; Gestão de Mudanças; Abertura, Transparência e Notificação; Gestão de Capacidade e Redundância; Cópia de Segurança; Legitimidade e Especificação de Propósito	Reduzir	5	15	75	Sim
R12	Responsabilização; Compliance com a Privacidade; Gestão de Mudanças; Gestão de Riscos; Resposta a Incidente; Cópia de Segurança; Legitimidade e Especificação de Propósito; Controles Criptográficos; Controles de Acesso Lógico; Registro de Eventos, Rastreabilidade e Salvaguarda de Logs; Desenvolvi-mento Seguro; Segurança Web; Controles de Segurança em Redes, Proteção Física e do Ambiente;	Reduzir	5	10	50	Sim

	Controle de Acesso e Privacidade; Uso, Retenção e Limitação de Divulgação; Minimização de Dados; Continuidade de Negócio;					
R13	Compliance com a Privacidade; Registro de Eventos, Rastreabilidade e Salvaguarda de Logs; Abertura, Transparência e Notificação; Responsabilização; Legitimidade e Especificação de Propósito; Gestão de Mudanças; Desenvolvimento Seguro; Controles de Acesso Lógico;	Reduzir	5	10	50	Sim
R14	Responsabilização; Compliance com a Privacidade; Gestão de Mudanças; Registro de Eventos, Rastreabilidade e Salvaguarda de Logs; Limitação de Coleta; Abertura, Transparência e Notificação; Desenvolvimento Seguro; Legitimidade e Especificação de Propósito; Controles de Acesso Lógico; Controle de Acesso e Privacidade; Uso, Retenção e Limitação de Divulgação; Minimização de Dados;	Reduzir	5	10	50	Sim

Legenda: P – Probabilidade; I – Impacto. Aplicam-se as mesmas definições de Probabilidade e Impacto da seção 6.

[1] Efeito resultante do tratamento do risco com a aplicação da(s) medida(s) descrita(s) na tabela. As seguintes opções podem ser selecionadas: Reduzir, Evitar, Compartilhar e Aceitar.
2 Controles aprovados pelo controlador dos dados pessoais. Preencher a coluna com: Sim ou Não.

- *Controles de segurança, de privacidade e medidas associadas*

Entre Controlador e Operador, há o Contrato 72/2017, que tem como objeto a concepção, implementação, implantação, manutenção e a operação do Serviço conta gov.br. Este contrato estabelece requisitos e obrigações no que diz respeito a segurança da informação e a privacidade dos dados.
Conforme o Contrato 72/2017:

> "A CONTRATADA deverá observar, rigorosamente, todas as normas e procedimentos de segurança implementados no ambiente de Tecnologia da Informação da CONTRATANTE e das suas unidades previamente orientado e comunicado pela CONTRATANTE."
>
> "O Gerenciamento de identidades deve estar conforme a Política de Segurança da Informação e Comunicação (PoSIC) do Ministério do Planejamento (MP), bem como suas normas complementares a fim de prover acesso aos sistemas somente a pessoas autorizadas, priorizando garantir a integridade, confidencialidade e autenticidade das informações."
>
> "Manter ambiente computacional funcional, sincronizado, íntegro, atualizado, observando o acordo de nível de serviço e indicadores de desempenho, disponível para os usuários e perfeitamente dimensionado para hospedar e processar todos os sistemas objetos deste Contrato, nas condições e nos níveis de serviços nele indicados e que atendam aos requisitos de segurança estabelecidos pelas unidades da CONTRATANTE, conforme política de segurança da CONTRATADA."
>
> "Recurso de segurança das informações das identidades, que permite flexibilidade para realização do acesso e atribuição de níveis conforme as normas de segurança do GSI/PR".

O Serviço conta gov.br está hospedado em centro de dados do Serpro. No Serpro, são implementadas normas para segurança e privacidade, conforme os requisitos que o Ministério da Economia estabelece no Contrato 72/2017, ou seja, o operador está de acordo com as regras estabelecidas pelo controlador. O Serpro está alinhado às determinações emitidas pelo GSI/PR, Ministério da Economia e outros padrões internacionais em suas normas. As normas são para uso interno e de uma forma geral são adequadas e aplicadas ao Serviço conta gov.br. Em algumas situações são estabelecidos requisitos específicos por parte do contrato, como por exemplo o tempo de retenção dos backups.

As tecnologias adotadas são flexíveis para atender o contrato.

Para os Controles de Segurança, elencados na Planilha de Avaliação de Riscos, são apresentadas algumas referências, como regras do Contrato 72/2017, estabelecidas pelo ME, normativos do Serpro e Normas complementares ou Instruções Normativas.

As normas do Serpro são iniciadas por: Segurança (SG), Risco Empresarial (RI) e Centro de Dados (CD). Há um breve resumo das normas do Serpro na Planilha de Avaliação de Riscos.

O Quadro 1 apresenta uma breve descrição para os Controles de segurança adotados para o Serviço conta gov.br. Mais detalhes do conjunto de medidas para cada Controle são encontrados na Planilha de Avaliação de Riscos.

Quadro 1 – Controles de Segurança

Controles de Segurança	**Descrição/Objetivo**
Continuidade de Negócio	Manter a operação da atividade, apesar das adversidades enfrentadas.
Controles Criptográficos	Oferecer um meio seguro para as comunicações e armazenamento de registros (dados, informações e conhecimento).
Controles de Acesso Lógico	Limitar os acessos indevidos ao sistema.
Controles de Segurança em Redes, Proteção Física e do Ambiente	Evitar acessos indevidos às estruturas internas.
Cópia de Segurança	Realizar e manter cópias com temporariedade de execução e testes (simulações) de que os procedimentos adequados foram implantados e estão funcionais.
Desenvolvimento Seguro	Atender critérios de segurança da informação, desde a concepção do produto.
Gestão de Capacidade e Redundância	Manter a disponibilidade do serviço.
Gestão de Mudanças	Acompanhar as mudanças, comunicar aos interessados e identificar potenciais riscos.
Gestão de Riscos	Identificar, avaliar, gerenciar e monitorar os riscos identificados.
Registro de Eventos, Rastreabilidade e Salvaguarda de Logs	Registrar eventos com atributos de rastreabilidade e proteger de alteração e acessos indevidos.

Resposta a Incidente	Realizar a coleta, a preservação de evidências, o tratamento e a resposta à incidentes de segurança.
Segurança Web	Elevar os níveis de segurança (da camada de front-end) nos serviços de acessos eletrônicos.

O Quadro 2 apresenta uma breve descrição para os Controles de Privacidade adotados para o Serviço conta gov.br. Mais detalhes do conjunto de medidas para cada Controle são encontrados na Planilha de Avaliação de Riscos.

Quadro 2- Controles de Privacidade

Controles de Privacidade	**Descrição/Objetivo**
Abertura, Transparência e Notificação	Atender o princípio de transparência da LGPD (art. 6º, inciso VI11).
Compliance com a Privacidade	Atender a legislação de proteção de dados, monitorar e auditar a privacidade.
Consentimento e Escolha	Obter consentimento do titular (art. 7º, I), desde que não se enquadre nas demais hipóteses previstas pelo art. 7º e 11 da LGPD.
Controles de Acesso e Privacidade	Limitar acessos indevidos às operações de tratamento de dados pessoais (LGPD, art. 6º, Incisos VII12 e VIII13).
Legitimidade e Especificação de Propósito	Realizar tratamento para propósitos legítimos, específicos, explícitos e informados ao titular (LGPD, art. 6º, I14).
Limitação da Coleta	Limitar a coleta ao mínimo necessário para a realização de suas finalidades (LGPD, art. 6º, III15).
Minimização dos Dados	Minimizar os dados utilizados no processamento (LGPD, art. 6º, III).
Participação Individual e Acesso	Assegurar que os direitos do titular dos dados pessoais são atendidos, a exemplo do livre acesso aos seus dados (LGPD, art. 6º, IV16).

Precisão e qualidade	Assegurar que os dados coletados são exatos e relevantes para o cumprimento da

- *Medidas Planejadas*

Na Planilha de Avaliação de Riscos, estão as medidas ainda não implementadas, mas em planejamento. Abaixo segue uma cópia resumida do dia 03/10/2022:

Descrição	**PRIORIZAÇÃO (DIAS)**	**RESPONSÁVEL (ÁREA)**	**PRAZO DE INÍCIO**	**PRAZO DE FIM**	**AÇÃO DESEMPENHADA**
Matriz de Responsabilidade	Médio Prazo (120)	Serpro/SGD	dez/22	mar/23	Previsão de iniciar em dezembro
PCN do Aplicativo	Longo Prazo (360)	Serpro/SGD			Previsão no novo contrato
Testes de Backup	Longo Prazo (360)	Serpro	jan/23		Previsão de início do planejamento depois da Migração AWS
Backup Offsite	Não Priorizado (+360)	Serpro			Necessário questionamento com outras áreas
Ripd	Longo Prazo (360)	SGD	out/21	dez/22	Ripd sendo elaborado.
Criptografia de fotos/selfie	Longo Prazo (360)	Serpro	jun/22	jan/23	Demanda 3246208 e 3285345
Controles de Dispositivos	Médio Prazo (120)	Serpro			Demanda 2787325
Separar credenciais de logs	Curto Prazo (40)	Serpro	jan/23		Previsão na Migração AWS
Cabeçalho SRI	Médio Prazo (120)	Serpro	jan/23		Previsão de início do planejamento depois da Migração AWS
Anonimização	Não Priorizado (+360)	Serpro/SGD			Necessita estudo
Notificação de Atualização do AP	Curto Prazo (40)	Serpro		dez/22	Demanda 3223850
Avaliar o resultado do piloto ao fim do projeto					Avaliação dos resultados do projeto, ajustes necessários ao modelo e a conclusão da viabilidade de

					implantação de forma permanente.

MINISTÉRIO DA ECONOMIA

8 – APROVAÇÃO E PARECER

Esta seção **formaliza a aprovação do RIPD.**

RESPONSÁVEL PELA ELABORAÇÃO DO RELATÓRIO DE IMPACTO	RESPONSÁVEL PELA ELABORAÇÃO DO RELATÓRIO DE IMPACTO
_____ <Nome do responsável> **Matrícula/SIAPE:** xxxxx <Local>, <dia> de <mês> de <ano>	_____ <Nome do responsável> **Matrícula/SIAPE:** xxxxx <Local>, <dia> de <mês> de <ano>

AUTORIDADE REPRESENTANTE DO CONTROLADOR	AUTORIDADE REPRESENTANTE DO OPERADOR
_____ <Nome do representante> **Matrícula/SIAPE:** xxxxx <Local>, <dia> de <mês> de <ano>	_____ <Nome do representante> **Matrícula/SIAPE:** xxxxx <Local>, <dia> de <mês> de <ano>

ANEXO A – Cookies estritamente necessários

Os cookies listados abaixo permitem funcionalidades essenciais tais como verificação de identidade, segurança e gestão acesso e rede.

Alguns cookies possuem informações do idtoken e do acesstoken, que tratam dados pessoais criptografados, como CPF, nome, e-mail e telefone. A coleta de dados pessoais por cookies é realizada nas hipóteses de Obrigação legal e de Políticas públicas, de acordo com o Tópico 4 deste RIPD. Os controles de Segurança e Privacidade adotados para essa coleta são os mesmos apresentados no tópico 7 deste RIPD.

O titular não tem permissão de desativar esses cookies através do Serviço conta gov.br. Caso o titular decida por apagá-los ou bloqueá-los, através de outros recursos, não permitirá o funcionamento correto do serviço conta gov.br.

Nome	Finalidade	Duração
Session_Gov_Br_Prod	Identificar a sessão do titular	Até terminar a sessão de navegação
INGRESSCOOKIE	Registrar recursos para balanceamento de carga otimizando a experiência do titular Distinguir entre humanos e bots.	Até terminar a sessão de navegação
Session	Armazenar a sessão do titular com o tempo de expiração Descrição: Armazena a sessão do titular com tempo de expiração, CSRF token, identificação do titular e uma chave criptográfica usada nos demais cookies (Session-Attr*).	Até terminar a sessão de navegação
Session-Attr*	Conter informações criptografadas do login, como access token e id token do acesso.gov.br.	Até terminar a sessão de navegação
XSRF-TOKEN	Impedir ataques de solicitação falsa entre sites	Até terminar a sessão de navegação
Sid-Govbr-Emp	Conter informações criptografadas do lado do titular	Até terminar a sessão de navegação
Reliabilities-Session	Armazena a sessão do titular com tempo de expiração, CSRF	Até terminar a sessão de navegação

	token, identificação do titular e uma chave criptográfica usada nos demais cookies (Session-Attr*).	
Reliabilities-Session-Attr*	Contém informações criptografadas do login, como access token e id token do acesso.gov.br	Até terminar a sessão de navegação
Govbr-Emp-SessionSession	Armazenar a sessão do titular com tempo de expiração	1 hora
Govbr-Emp-SessionU-Ssn	Conter informações criptografadas do acesso	1 hora
Govbr-Emp-SessionXsrf	Conter informações criptografadas do lado do servidor	1 hora
Ges_Prod_Session	Armazenar a sessão do titular com tempo de expiração	1 hora
Ges_Prod_U-Ssn	Conter informações criptografadas no acesso	1 hora
Ges_Prod_Xsrf	Conter informações criptografadas do lado do servidor	1 hora
Sid-Govbr-Gestao	Conter o csrf criptografado do lado do frontend.	Até terminar a sessão de navegação

MINISTÉRIO DA ECONOMIA

ANEXO B – Previsões Normativas que autorizam o tratamento de dados

- **Decreto nº 10.609, de 26 de janeiro de 2021** - Institui a Política Nacional de Modernização do Estado e o Fórum Nacional de Modernização do Estado.
- **Decreto nº 10.046, de 9 de outubro de 2019** - Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados.
- **Decreto 8.936, de 19 de dezembro de 2016** - Institui a Plataforma de Cidadania Digital e dispõe sobre a oferta dos serviços públicos digitais, no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional.
- **Decreto nº 9.745, de 08 de abril de 2019, Decreto nº 10.072, de 18 de outubro de 2019,** e posteriores alterações com a conversão da **MP na Lei nº 13.844, de 18 de junho de 2019,** contemplam as competências do Ministério da Economia e Secretaria do Governo Digital, nas quais se respalda o Serviço conta gov.br.
- **Decreto nº 10.332, de 28 de abril de 2020** - Institui a Estratégia de Governo Digital para o período de 2020 a 2022, no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional e dá outras providências.
- **Lei nº 13.444, de 11 de maio de 2017 -** Dispõe sobre a Identificação Civil Nacional (ICN), que possui o objetivo de identificar o brasileiro em suas relações com a sociedade e com os órgãos e entidades governamentais e privados.
- **Decreto nº 9.756, de 11 de abril de 2019 -** Institui o portal único "gov.br" e se propõe sobre as regras de unificação dos canais digitais do Governo federal.
- **Decreto nº 10.543, de 13 DE Novembro de 2020 -** Dispõe sobre o uso de assinaturas eletrônicas na administração pública federal e regulamenta o art. 5º da Lei nº 14.063, de 23 de setembro de 2020, quanto ao nível mínimo exigido para a assinatura eletrônica em interações com o ente público.
- **Portaria SEDGGME nº 2.154, de 23 de fevereiro de 2021** - Regulamenta o Decreto nº 10.543, de 13 de novembro de 2020, que estabelece níveis mínimos de exigência para as assinaturas em interações eletrônicas com entes públicos.

- **Lei nº 13.709, de 2018, LGPD,** que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

- **Lei nº 12.965, de 2014** - Marco Civil da Internet **–** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

- **Decreto n° 8.771/2016**, que regulamenta a Lei nº 12.965, de 23 de abril de 2014, (Marco Civil da Internet), para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de

dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações.

- **Lei n° 9.507/1997**, que regula o direito de acesso a informações e disciplina o rito processual do habeas data.
- **Lei n° 9.784/1999**, que regula o processo administrativo no âmbito da Administração Pública Federal.
- **Lei n° 12.527/2011 (Lei de Acesso à Informação)**, que regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências.
- **Decreto n° 7.724/2012**, que regulamenta a Lei nº 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso a informações previsto no inciso XXXIII do caput do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição. **Lei n° 13.460/2017**, que dispõe sobre participação, proteção e defesa dos direitos do usuário dos serviços públicos da administração pública.

- **Decreto n° 9.278/2018**, que regulamenta a Lei nº 7.116, de 29 de agosto de 1983, que assegura validade nacional às Carteiras de Identidade e regula sua expedição.
- **Lei n° 13.709/2018**, Lei Geral de Proteção dos Dados – LGPD.
- **Decreto n° 9.492/2018**, que regulamenta a Lei nº 13.460, de 26 de junho de 2017, que dispõe sobre participação, proteção e defesa dos direitos do usuário dos serviços públicos da administração pública federal, institui o Sistema de Ouvidoria do Poder Executivo federal, e altera o Decreto nº 8.910, de 22 de novembro de 2016, que aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança do Ministério da Transparência, Fiscalização e Controladoria-Geral da União.
- **Decreto n° 9.723/2019**, que altera o Decreto nº 9.094, de 17 de julho de 2017, o Decreto nº 8.936, de 19 de dezembro de 2016, e o Decreto nº 9.492, de 5 setembro de 2018, para instituir o Cadastro de Pessoas Físicas - CPF como instrumento suficiente e substitutivo da apresentação de outros documentos do cidadão no exercício de obrigações e direitos ou na obtenção de benefícios e regulamentar dispositivos da Lei nº 13.460, de 26 de junho de 2017.
- **Lei n° 13.853/2019**, que altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências.
- Derrubada de vetos da **Lei n° 13.853/2019** pelo Congresso Nacional.