GRUPO I – CLASSE V – Plenário
TC 015.635/2025-2.
Natureza: Relatório de Auditoria.
Órgãos/Entidades: Controladoria-Geral da União; Instituto Nacional do Seguro Social; Secretaria de Governo Digital; Serviço Federal de Processamento de Dados.
Representação legal: não há.

SUMÁRIO: AUDITORIA OPERACIONAL AUDITORIA NA GESTÃO DE IDENTIDADE DA CONTA GOV.BR. APROFUNDAMENTO DAS ANÁLISES. RECOMENDAÇÕES. COMUNICAÇÕES.

RELATÓRIO

Adoto como relatório, com os ajustes necessários, excerto da instrução da Unidade de Auditoria Especializada em Tecnologia da Informação[1], que contou com a anuência do corpo diretivo[2]:

"**INTRODUÇÃO**

1. Trata-se de relatório de auditoria operacional, com o objetivo de promover a melhoria nos processos de gestão de identidade da Conta Gov.br, por meio da avaliação de controles técnicos e administrativos existentes em relação às boas práticas, cujas principais conclusões são:

1.1. Desafios da inclusão digital e baixa habilidade digital pela população, aliados ao uso inadequado de credenciais de acesso induzem à diminuição das exigências de segurança pelos serviços públicos: a baixa inclusão digital da população, somada à baixa maturidade em SI pelos gestores, impõe a redução de critérios de segurança (nível da conta, verificação em duas etapas, métodos de acesso) para evitar a exclusão de usuários, fragilizando a proteção dos serviços públicos digitais.

1.2. Dificuldades e falhas no processo de validação biométrica impactam no acesso ao gov.br.: as limitações técnicas na prova de vida biométrica geram barreiras de acesso legítimo e frustração aos usuários, ao passo que a sofisticação de ataques com inteligência artificial explora fragilidades nessa validação. Essa dualidade compromete a disponibilidade do serviço público digital para o cidadão e, simultaneamente, a eficácia do controle na prevenção de fraudes avançadas.

1.3. A inconsistência dos mecanismos de segurança exigidos em cada nível da Conta Gov.br, aliada à baixa adoção, pelos gestores dos serviços públicos, de mecanismos de autenticação mais robustos aumenta o risco de uso indevido das Contas Gov.br dos cidadãos brasileiros: a desconexão entre o nível de confiança cadastral (identificação) e a não exigência de autenticação em duas etapas, somada à baixa exigência e uso dos critérios de segurança pelos serviços, ao baixo uso de verificação em duas etapas pelos usuários, e à permanência de contas em nível elevado de confiabilidade (ouro) indefinidamente torna os níveis de segurança ineficazes. Tal inconsistência estrutural permite que credenciais privilegiadas sejam exploradas por vetores de ataque básicos, expondo ativos críticos e dados sensíveis a acessos não autorizados.

1.4. Falhas na sincronização de dados entre as bases de registro civil e do CPF podem permitir fraudes no acesso ao Gov.br e em serviços públicos por meio de cadastro de cidadãos falecidos: a persistência de contas ativas de titulares falecidos, decorrente de falhas de sincronização entre

[1] Peça 148.
[2] Peças 149/150.

bases governamentais, viabiliza a continuidade de acessos indevidos e a materialização de fraudes, com prejuízos às organizações e aos cidadãos.

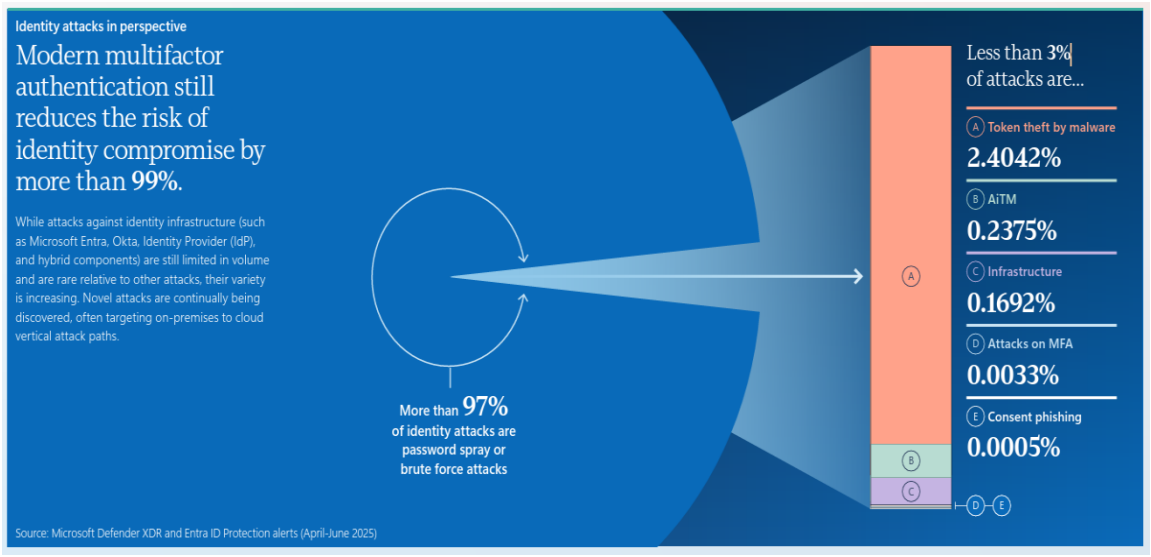
1.5. Adicionalmente, a segurança do ecossistema é comprometida pela incipiência dos processos de monitoramento e pela obsolescência dos requisitos de senhas.

2. A presente auditoria envolve conceitos técnicos e administrativos no que diz respeito a gestão de identidade. Assim, para melhor compreensão deste relatório, foi elaborado o Apêndice A – Conceitos relacionados ao objeto, que descreve os termos mais técnicos utilizados no presente relatório.

3. O objeto da fiscalização é a identificação e autenticação segura de usuários na Conta Gov.br, que fornece uma variedade de serviços para o cidadão, incluindo identificação e autenticação de usuários.

4. A Microsoft, em seu relatório 'Microsoft Digital Defense Report', de 2025, enfatiza a priorização da proteção de identidades, responsável por 80% dos vetores de ataque para obter acesso inicial ao ambiente de tecnologia da informação (TI) das organizações. A diretriz preconiza a imposição de Autenticação Multifator (MFA) resistente a phishing para todas as contas, inclusive as administrativas, destacando que o MFA moderno continua sendo o padrão-ouro de segurança, capaz de bloquear mais de 99% das tentativas de acesso não autorizado e de mitigar riscos como ataques de força bruta e pulverização de senhas (password spray).

Figura 1: MFA moderno reduz em 99% o risco de comprometimento de identidade



Fonte: Microsoft Digital Defense Report (2025).

5. Esse relatório apresenta dados estatísticos que fundamentam a necessidade de controles robustos na gestão de identidade, dentre eles a autenticação multifator. Identificou-se que menos de 0,3% dos ataques observados conseguem contornar o MFA (ex: via Token Theft ou MFA Fatigue), demonstrando que a falha de controle raramente está na tecnologia MFA em si, mas na sua ausência. Além disso, mais de 97% de todos os ataques de identidade observados são do tipo password spray (pulverização de senhas) ou força bruta, explorando a fragilidade do fator único de autenticação (apenas senha).

6. Além disso, o relatório aponta que as fraudes envolvendo biometria e identidade digital apresentam uma evolução crítica impulsionada pelo uso de Inteligência Artificial (IA). O relatório destaca que a IA está ampliando a escala, a velocidade e a sofisticação das fraudes, desafiando os métodos tradicionais de verificação. Segundo o relatório, o avanço dos deepfakes já possibilita burlar testes de vivacidade e autenticações de dois fatores, enquanto a criação de identidades sintéticas cresceu 195%, gerando documentos digitais extremamente convincentes. Esse ecossistema, exemplificado pela atuação de grupos que comercializam ferramentas de IA para fins ilícitos, facilita desde a personificação de vítimas em golpes de engenharia social até a

abertura massiva de contas fraudulentas, desafiando a eficácia das verificações biométricas atuais.

7. Esteve no escopo desta fiscalização avaliar:

7.1. A política de gestão de identidade na Conta Gov.br;

7.2. A gestão de riscos de segurança da informação em relação à Conta Gov.br;

7.3. Os processos de identificação, desabilitação e gestão de identidades privilegiadas em relação à Conta Gov.br;

7.4. A gestão de senhas e autenticação na Conta Gov.br;

7.5. O registro e monitoramento dos eventos de segurança na Conta Gov.br;

7.6. As diretrizes para orientar os gestores sobre integração e uso seguro do Conta Gov.br;

7.7. Iniciativas efetivas para proteger os cidadão e grupos vulneráveis, considerando o aspecto humano e cultural, contra o roubo de credenciais no âmbito da Plataforma Gov.br; e

7.8. A integração e uso seguro da Conta Gov.br pelas organizações;

8. Tudo o que não foi declarado no escopo está fora escopo desta fiscalização, em especial:

8.1. Atestar se a Conta Gov.br está efetivamente segura contra ataques cibernéticos;

8.2. Atestar se os serviços disponibilizados através da Plataforma Gov.br estão efetivamente seguros contra ataques cibernéticos;

8.3. Avaliar os controles de acessos implementados nos serviços integrados à Plataforma Gov.br;

8.4. Avaliar os controles de autorização implementados nos serviços integrados à Plataforma Gov.br;

8.5. Atestar a segurança de mecanismos e serviços prestados por terceiros à Conta Gov.br (cadeia de fornecedores);

9. A matriz de planejamento completa pode ser vista na peça 117.

10. Quanto aos critérios, foram utilizados como fontes frameworks e guias amplamente reconhecidos que tratam da gestão de identidades e autenticação. Entre eles, destacam-se:

10.1. O Programa de Auditoria de Gerenciamento de Identidade e Acesso da Isaca ;

10.2. NIST SP 800-63 Digital Identity Guidelines;

10.3. Norma técnica ABNT NBR ISO/IEC 27002:2022 – 5.16 Gestão de Identidade; e

10.4. Controles CIS Versão 8 - Controles críticos de segurança cibernética do Center for Internet Security (CIS).

11. A auditoria foi conduzida de acordo com as Normas de Auditoria do Tribunal de Contas da União e com o Manual de Auditoria Operacional do Tribunal.

12. O método empregado na auditoria está descrito no Apêndice B – Detalhamento do Método e pode ser sintetizado da seguinte forma:

12.1. Na fase de planejamento, a equipe de auditoria estudou a literatura e as boas práticas sobre gestão de identidades, desenvolvendo uma questão de auditoria abrangente que se desdobrou em procedimentos em cinco áreas críticas.

12.2. Essa fase incluiu a criação de papéis de trabalho e métodos de coleta de dados. Os métodos de coleta de dados abrangeram entrevistas, revisão documental, com a preparação dos Questionários de Avaliação de Controles Internos (QACI) para analisar os controles internos da organização.

13. Durante a execução, a equipe preencheu os QACIs e avaliou os controles a partir de evidências enviadas pelos gestores e outras coletadas diretamente, realizou entrevistas e solicitou evidências adicionais. As conclusões da auditoria foram documentadas em conformidade com as normas do TCU.

14. A conclusões preliminares das equipes foram compartilhadas com os gestores, que receberam versão com marca d´água ‘preliminar’ (peças 75-77 e 84), dando-lhes a oportunidade

de analisarem as avaliações feitas pela equipe, enviarem novas evidências e apresentarem comentários.

15. A fase de relatório compreende a confecção deste documento e o envio de sua versão preliminar para comentário dos gestores, que serão analisados em seção apartada.

16. Não houve limitações à auditoria.

17. As proposições centrais deste relatório priorizam o enfrentamento das causas raízes que comprometem a segurança, a inclusão e a eficiência da Conta Gov.br, destacando-se:

17.1. Ampliação e modernização dos métodos de autenticação: transição para métodos de autenticação baseados em biometria nativa e chaves físicas, visando eliminar a dependência de senhas e mitigar ataques de phishing e roubo de credenciais, além de melhorias na experiência do usuário e custos operacionais.

17.2. Melhorias na validação biométrica: aprimoramento tecnológico, operacional e de segurança das soluções de biometria facial e prova de vida (liveness) do ecossistema biométrico do Serpro, assegurando resistência contra ataques de apresentação e fraudes de personificação, além de melhorias na experiência do cidadão para acessos legítimos.

17.3. Melhorias na detecção e proteção contra ataques: implementação de ferramentas de detecção e resposta a ameaças de identidade para monitoramento comportamental em tempo real, permitindo a identificação de anomalias e acessos indevidos, além de fortalecimento da participação ativa do cidadão na sua segurança.

17.4. Melhoria nas diretrizes, orientações e segurança nativa na integração dos serviços: correção de vulnerabilidades e deficiências identificadas nas diretrizes e manuais para assegurar a coerência entre os instrumentos normativos, os formulários de integração e a documentação técnica.

18. Espera-se que a implementação das medidas propostas tenha como benefício um salto qualitativo na segurança e na inclusão da Plataforma Gov.br, assegurando que a modernização tecnológica caminhe em conjunto com a proteção efetiva do cidadão. Ao atacar as causas raízes — desde a fragilidade das senhas até a baixa inclusão digital —, o Estado brasileiro fortalece a confiança nas instituições digitais, mitiga vulnerabilidades críticas e consolida as bases para uma transformação digital resiliente, capaz de prevenir prejuízos e assegurar o exercício pleno da cidadania em ambiente virtual.

19. Este relatório está organizado em dez capítulos, sendo esta introdução o primeiro deles.

20. O capítulo dois traz uma visão geral da importância da Plataforma Gov.br no cenário nacional, seu arcabouço normativo e a relevância do tema da gestão de identidade e autenticação.

21. O capítulo três traz o resultado geral das avaliações realizadas a partir dos QACIs desta auditoria, enquanto os capítulos quatro, cinco, seis, sete e oito destacam os achados da fiscalização.

22. O capítulo nove apresenta as boas práticas identificadas na fiscalização.

23. O capítulo dez apresenta a análise dos comentários dos gestores.

24. Por fim, os capítulos onze e doze completam a conclusão e as propostas de encaminhamento.

25. Ao final, estão apresentados diversos apêndices, destacando-se o Apêndice C – Índice de documentos e análises de suporte dos achados de auditoria, que contém um índice que enumera todos os documentos e análises que serviram de suporte para as conclusões deste relatório.

2 VISÃO GERAL

26. Gestão de Identidade e Acesso (Identity and Access Management - IAM) é um conjunto de processos, políticas, tecnologias e ferramentas que têm como objetivo garantir que as identidades digitais dentro de uma organização ou de um sistema sejam devidamente gerenciadas e que o acesso aos recursos seja controlado de maneira segura, eficiente e em conformidade com as regulamentações.

27. A gestão de identidade e acesso (IAM) é um pilar essencial da cibersegurança, pois centraliza o controle de quem pode acessar quais recursos, reduzindo drasticamente a superfície de ataque por meio de autenticação robusta e permissões granulares. Ao implementar práticas como o controle de privilégios (PAM), a autenticação multifator e o Single Sign-On (SSO), o IAM não apenas mitiga ameaças internas e previne o escalonamento de acessos por fraudadores, mas também otimiza a eficiência operacional através da automação de processos. Além de proteger credenciais contra roubos e phishing, o sistema acelera a resposta a incidentes ao permitir a revogação imediata de acessos e o fornecimento de registros detalhados para auditoria, equilibrando uma segurança rigorosa com uma experiência de usuário fluida.

28. Uma solução completa de IAM integra componentes fundamentais que gerenciam todo o ciclo de vida do usuário, desde o registro e provisionamento de contas até a exclusão definitiva. O sistema opera através de mecanismos de autenticação (como MFA e SSO) para validar identidades, e de autorização (via RBAC ou ABAC) para definir permissões específicas baseadas em funções ou atributos. Complementarmente, a solução abrange o gerenciamento seguro de credenciais, o controle rigoroso de acessos privilegiados (PAM) e a revisão constante de direitos para garantir o princípio do privilégio mínimo. Todo esse ecossistema é sustentado por processos de monitoramento e auditoria, que rastreiam atividades e geram relatórios essenciais para a conformidade e a detecção de anomalias.

29. As principais diretrizes globais para a implementação de IAM fundamentam-se nos frameworks do CIS, NIST e na norma ISO/IEC 27002:2022, que estabelecem padrões rigorosos para o controle de acesso e proteção de dados. Enquanto os controles 5 e 6 do CIS v8.1 priorizam o gerenciamento técnico de contas e privilégios para reduzir riscos imediatos, o framework do NIST oferece uma abordagem estratégica e detalhada, desde o domínio de 'Proteção' no CSF até normas específicas como a SP 800-63, focada em identidades digitais e autenticação multifator. Complementarmente, a ISO 27002 fornece uma estrutura normativa para a governança da segurança da informação, reiterando princípios como o mínimo privilégio e a necessidade de revisões periódicas de acesso para garantir a confidencialidade e integridade organizacional.

30. A Conta Gov.br configura-se como o sistema central de identificação e autenticação para o acesso aos serviços públicos digitais no âmbito federal, com uma expansão progressiva para os níveis estadual e municipal. Sua relevância transcende a de um mero sistema de login, posicionando-se como um elemento fundamental no ecossistema de governo digital brasileiro .

31. A Plataforma oferece mais de 4,6 mil serviços digitais federais ao cidadão e chega a 173 milhões de usuários. A quantidade expressiva de usuários cadastrados e serviços integrados atesta sua centralidade na estratégia de transformação digital do Estado.

32. A Conta Gov.br usada para acessar a Plataforma Gov.br é uma identificação que comprova em meios digitais que você é você. Com ela, você se identifica com segurança na hora de acessar serviços digitais.

33. Os objetivos da plataforma Gov.br estão intrinsecamente alinhados com as diretrizes da Estratégia Nacional de Governo Digital (ENGD). Conforme a ENGD, busca-se ampliar e simplificar o acesso do cidadão aos serviços públicos, promover a transformação digital do setor público com foco em eficiência, transparência e acessibilidade, fortalecer a participação cidadã e impulsionar a inovação tecnológica.

34. A meta é a criação de uma administração pública mais moderna, ágil e centrada nas necessidades do cidadão. Um dos dez objetivos específicos da ENGD para o período 2024-2027 é, precisamente, a 'Identidade Única do Cidadão', o que coloca a Plataforma Gov.br no epicentro dessa estratégia. A funcionalidade de login único e a gestão centralizada de identidades digitais são os mecanismos primários pelos quais a plataforma contribui para esses desígnios, unificando a experiência do usuário e racionalizando o acesso a uma miríade de serviços governamentais.

35. A governança da plataforma Gov.br e da estratégia de governo digital no Brasil passou por diversas evoluções. Iniciativas pioneiras como o Comitê Executivo de Governo Eletrônico (CEGE), criado em 2000, deram lugar a estruturas mais recentes. O Decreto 10.332/2020

instituiu os Comitês de Governança Digital nos órgãos e entidades federais, mas partes significativas deste arranjo foram posteriormente revogadas, notadamente pelo Decreto 12.198/2024.

36. Atualmente, a Secretaria de Governo Digital (SGD) do Ministério da Gestão e da Inovação em Serviços Públicos (MGI) desempenha um papel central na formulação de políticas, coordenação e normatização da transformação digital, incluindo a plataforma Gov.br. O Decreto 12.069/2024 redefiniu a ENGD 2024-2027 e a Rede Nacional de Governo Digital (Rede Gov.br), alterando o Decreto 9.319/2018 (que trata do Sistema Nacional para a Transformação Digital) e revogando disposições anteriores sobre a Rede Gov.br contidas no Decreto 10.332/2020. A existência e as atribuições de um Comitê Gestor da Identidade Digital Federal também devem ser consideradas no contexto da legislação vigente, verificando-se o impacto das revogações mencionadas .

37. Em resumo, a plataforma Gov.br foi concebida para gerar valor para um amplo espectro de atores, centrada no cidadão, mas com impactos positivos relevantes para a eficiência da máquina pública e para o desenvolvimento da sociedade digital no Brasil. Foram identificados três grupos principais de partes beneficiárias da plataforma Gov.br: os cidadãos, o setor público e, potencialmente, o setor privado e a sociedade em geral.

38. O papel de trabalho 'PT0.1 - Visão Geral do Objeto' (peça 116) detalha os conceitos fundamentais de Gestão de Identidade e Acesso (Identity and Access Management - IAM), destacando sua importância para a cibersegurança e eficiência operacional, além de listar os critérios técnicos e normativos utilizados, como os padrões do NIST, CIS Controls e a norma ISO/IEC 27002:2022. Adicionalmente, descreve a estrutura da Plataforma Gov.br, seu complexo arcabouço legal, a governança exercida pela SGD/MGI e a execução tecnológica pelo Serpro, finalizando com uma análise da lógica de intervenção estatal, os benefícios para o cidadão e os riscos cibernéticos e operacionais inerentes ao sistema.

Grupo de controle	Pontuação obtida	Pontuação total possível	Nota obtida no grupo de controle	Interpretação
1. Política de gestão de identidade	37	40	92,5%	Muito alinhado às boas práticas
2. Gestão de riscos	20	30	66,6%	Parcialmente alinhado às boas práticas
3. Gestão de identidade	40	40	100%	Muito alinhado às boas práticas
4. Identificação	30	30	100%	Muito alinhado às boas práticas
5. Desativação/exclusão de contas de usuário encerrada/inativa	6	20	30%	Não alinhado às boas práticas
6. Contas privilegiadas	20	20	100%	Muito alinhado às boas práticas
7. Processo de autenticação	27	30	90%	Alinhado às boas práticas
8. Gestão de Senhas	26	40	65%	Parcialmente alinhado às boas práticas

Grupo de controle	Pontuação obtida	Pontuação total possível	Nota obtida no grupo de controle	Interpretação
9. Autenticação multifator	27	30	90%	Alinhado às boas práticas
10. Registro	37	40	92,5%	Muito alinhado às boas práticas
11. Monitoramento	3	20	15%	Não alinhado às boas práticas

Fonte: elaborada pela equipe de auditoria

40. Os achados de auditoria derivam das análises das avaliações dos QACIs (peças 118 a 121) e dos resultados das avaliações nos papéis de trabalho (peças 111, 114, e 115) relacionados às questões de auditoria cinco, seis e oito da matriz de planejamento (peça 117).

A EQUIPE DE AUDITORIA UTILIZOU O DIAGRAMA DE RELAÇÕES DE CAUSAS E EFEITOS (APÊNDICE E – DIAGRAMAS DE CAUSAS E EFEITOS)

41. para estruturar os achados e evidenciar as vulnerabilidades identificadas. Diferente de modelos lineares, esta técnica permite mapear a interdependência sistêmica entre falhas de governança, fragilidades operacionais e seus impactos sociais e financeiros. Por meio dessa abordagem, foi possível visualizar como as causas transversais — como a exclusão digital e a baixa maturidade em cibersegurança — desencadeiam efeitos em cascata que comprometem a integridade dos serviços públicos digitais e resultam em danos ao erário e à confiança na transformação digital do país.

4 DESAFIOS DA INCLUSÃO DIGITAL E BAIXA HABILIDADE DIGITAL PELA POPULAÇÃO, ALIADOS AO USO INADEQUADO DE CREDENCIAIS DE ACESSO INDUZEM À DIMINUIÇÃO DAS EXIGÊNCIAS DE SEGURANÇA PELOS SERVIÇOS PÚBLICOS.

4.1 Insuficiência de programas de inclusão digital e conscientização

42. Devido à insuficiência de ações de inclusão digital (capacitação para usar a internet de forma consciente e segura) e conscientização em segurança da informação, ocorre o desconhecimento dos cidadãos sobre riscos e boas práticas de segurança. Essa situação leva ao uso inadequado de credenciais de acesso e à maior exposição dos usuários a golpes digitais, impactando a segurança dos serviços, das organizações e a confiança na transformação digital no Brasil (PT06, peça 114, p. 4, itens 17-24).

43. Embora a Secretaria de Governo Digital (SGD/MGI) realize campanhas informativas em redes sociais e mantenha seções com jogos educativos e quizzes no portal de Governo Digital, essas iniciativas apresentam baixa efetividade e alcance limitado, além de ausência de direcionamento às necessidades de grupos vulneráveis. Constatou-se que a organização não comunica adequadamente a existência dessas páginas com orientações, nem fornece links acessíveis diretamente na plataforma Gov.br, dificultando o acesso do cidadão comum às orientações de proteção (PT06, peça 114, p. 9, itens 38-44; PT15, peça 112, itens 3-4).

44. A estratégia de disseminação depende do apoio das organizações do Sistema de Administração dos Recursos de Tecnologia da Informação (Sisp), o que limita o alcance ao público externo. A própria organização reconhece o cumprimento parcial das metas estabelecidas na Estratégia Federal de Governo Digital (EFGD), autoavaliando-se com nota 3 de 10 no quesito de alcance das campanhas. Até o momento da auditoria, não foram evidenciadas as ações de inclusão digital em privacidade e segurança para os cidadãos previstas na iniciativa 10.1 da referida estratégia (PT15, peça 112, itens 5, 21-22).

45. Assim, as iniciativas estatais de inclusão digital e segurança da informação carecem de estruturação dentro de um plano ou estratégia consolidada, evidenciando falhas de governança e fragmentação de esforços. Adicionalmente, constata-se a insuficiência de métricas para apurar a eficácia, eficiência e efetividade dessas ações, o que inviabiliza a avaliação de seu impacto real frente à contínua vulnerabilidade da população a ameaças cibernéticas. Por conseguinte, tais iniciativas apresentam alcance limitado, caracterizado pela baixa visibilidade nos portais governamentais (item 43), ausência de direcionamento adequado às necessidades de grupos vulneráveis (item 43) e dependência de canais de alcance restrito (item 44).

46. Embora a Lei de Diretrizes e Bases da Educação Nacional (Lei 9.394/1996) estabeleça, em seu art. 4º, inciso XII, o dever do Estado de garantir o desenvolvimento de competências voltadas à inclusão digital, incluindo a criação de conteúdo e segurança, a implementação dessa diretriz apresenta falhas estruturais de governança. A insuficiência e a fragmentação das ações estatais motivaram a determinação desta Corte para a criação do Plano Nacional de Inclusão Digital (PNID), dado que os debates atuais são pouco efetivos. Há, também, a necessidade de coordenar esforços para superar a exclusão digital e reduzir a vulnerabilidade da população a ameaças cibernéticas (Lei 9.394/1996; Acórdão 1.699/2025-TCU-Plenário, Rel. Min. Aroldo Cedraz).

47. O Plano Nacional de Inclusão Digital (PNID) é uma iniciativa do Governo Federal, coordenada pelo Ministério das Comunicações e pela Casa Civil, instituída com o objetivo de estruturar políticas públicas para mitigar a exclusão digital no Brasil. Sua formulação visa assegurar à população três pilares fundamentais: a expansão da infraestrutura de conectividade de alta qualidade, a facilitação do acesso a equipamentos adequados e a promoção da inclusão digital, democratizando o uso seguro e produtivo das tecnologias de informação e comunicação.

48. Para embasar tecnicamente a elaboração do plano, foram instituídas as Câmaras Setoriais no âmbito do Grupo de Trabalho Interministerial (GTI), atuando como fóruns consultivos que reúnem representantes do governo, da sociedade civil e do setor privado. Essas câmaras dividem-se primariamente em duas frentes: a Setorial de Oferta, focada na viabilidade técnica, expansão de redes e segurança cibernética; e a Setorial de Demanda, dedicada à formulação de estratégias para o desenvolvimento de habilidades digitais, educação tecnológica e acessibilidade financeira aos serviços.

49. Essa lacuna educacional reflete-se na disparidade entre o conhecimento teórico e a prática de segurança dos brasileiros. Dados indicam que, embora 96% dos usuários afirmem saber criar senhas fortes, apenas 19% utilizam métodos seguros de armazenamento. Além disso, somente 27% conseguem identificar tentativas de phishing e apenas 11% compreendem riscos de privacidade associados à coleta de metadados, evidenciando que a população permanece vulnerável a ataques de engenharia social devido à falta de competência técnica de segurança da informação defensiva (PT06, peça 114, item 27-28).

50. Não obstante, é necessário ressaltar que a dificuldade de acesso pode decorrer da complexidade do próprio serviço digital, como declarações de imposto de renda pessoa-física.

51. A ausência de iniciativas massivas e direcionadas, especialmente considerando aspectos humanos e culturais de grupos vulneráveis (idosos e pessoas com baixa habilidade digital), contribui para a exposição do cidadão ao risco de uso inseguro do ambiente digital. Práticas inseguras, como o compartilhamento de senhas com terceiros e a desativação de mecanismos de segurança, como a verificação em duas etapas (MFA), por conveniência, continuam recorrentes, sem uma contrapartida educativa robusta por parte do Estado para reduzir esses comportamentos.

4.2 Uso inadequado de credenciais de acesso

52. A baixa conscientização em segurança da informação (SI) por parte dos cidadãos reflete-se na proteção insuficiente de suas identidades digitais. (itens 49 e 51)

53. O uso inadequado de credenciais resulta na baixa utilização da ‘Verificação em Duas Etapas’ (uma segunda camada de proteção além da senha). A adesão, voluntária, é baixa e apenas 1% (25) dos serviços integrados à plataforma e que preencheram as informações de critérios de acesso (57%) exigem esse controle. Além disso, a restrição da ‘Verificação em Duas

Etapas' ser disponibilizada exclusivamente ao aplicativo em dispositivos móveis gera frustração e indisponibilidade de acesso quando ocorre perda, roubo ou troca do aparelho pelo usuário (PT08, peça 115, p. 6, item 12; peça 100, p. 2).

54. Em contraposição ao cenário histórico de baixo uso de controles de segurança, iniciativas recentes da SGD/MGI impulsionaram a adesão à 'Verificação em Duas Etapas'. Em fevereiro de 2026, o número de cidadãos que utilizam a funcionalidade atingiu a marca de 50 milhões, representando cerca de 29% do total de 173 milhões de usuários da plataforma (peça 100, p. 1-2).

55. Esse crescimento decorre de uma estratégia de incentivo implementada desde o ano anterior, na qual usuários com conta nível Ouro são convidados a ativar a camada extra de segurança no momento do login. Embora a ativação permaneça opcional, sendo possível ao usuário pular a etapa, a medida visa reduzir o risco de acesso indevido por terceiros, mesmo em casos de comprometimento de senha (peça 100, p. 1-2). Contudo, o método de 'Verificação em Duas Etapas' via código de acesso no aplicativo Gov.br não é resistente a phishing por não afastar a possibilidade do vazamento do próprio código de verificação mediante engenharia social – quando o usuário é enganado para entregar o código ao fraudador.

56. Para mitigar as vulnerabilidades inerentes ao uso de senhas e códigos de verificação, surge o padrão FIDO (Fast Identity Online), que viabiliza a autenticação sem senha (passwordless). Ao adotar chaves de acesso (passkeys) baseadas em criptografia de chave pública, o FIDO elimina a necessidade de o usuário memorizar sequências complexas ou digitar códigos temporários. Essa tecnologia aumenta significativamente a segurança por ser nativamente resistente a phishing, uma vez que a autenticação é vinculada ao domínio legítimo do serviço e exige a posse física do dispositivo ou verificação biométrica local. A implementação desse padrão não apenas simplifica a jornada do cidadão, reduzindo a fricção no acesso, mas também resolve gargalos de suporte técnico relacionados à recuperação de contas e perdas de dispositivos. O papel de trabalho 'Fido – autenticação sem senha' (peça 110) contém mais detalhes sobre este padrão.

4.3 Exclusão digital de brasileiros

57. A exclusão digital manifesta-se como um obstáculo estrutural à universalização do acesso aos serviços públicos digitais, afetando desproporcionalmente grupos vulneráveis. Dados do Banco Interamericano de Desenvolvimento (BID) indicam que, embora 90,7% da população adulta tenha acessado a internet recentemente, o uso efetivo de serviços públicos digitais cai drasticamente entre idosos, pessoas com baixa escolaridade e pessoas com deficiência, variando entre apenas 22,1% e 26,3% nestes grupos, respectivamente (peça 97, p. 9-10 e 30).

58. Essa disparidade é agravada pela desigualdade no acesso a dispositivos e pela qualidade da conexão. Enquanto o uso de celulares é quase universal (94,2%), a posse de computadores atinge apenas 14,4% das pessoas com ensino fundamental. Adicionalmente, 36,9% dos usuários de internet móvel enfrentam interrupções por atingirem o limite de dados, situação que afeta principalmente cidadãos com menor escolaridade (44,6%) e pessoas com deficiência (52,2%), limitando a capacidade desses cidadãos de realizar procedimentos complexos na Conta Gov.br, como o reconhecimento facial ou a recuperação de contas (peça 97, p. 18 e 20).

59. A falta de habilidade e inclusão digital gera insegurança e dependência de terceiros. Apenas 24% dos idosos e cidadãos com ensino fundamental sentem-se confiantes em suas habilidades digitais. Como reflexo, 57,2% dos usuários ainda preferem o atendimento presencial, citando falta de experiência (15,3%) e desconfiança na validade jurídica do digital (14,9%). Essa preferência impõe um custo significativo ao cidadão vulnerável, visto que o custo estimado para o usuário de um serviço presencial é de R$ 59,74, comparado com R$ 6,64 no meio digital, sem incluir os custos específicos de cada serviço (peça 97, p. 30 e 35-37).

60. A rede de suporte presencial, essencial para diminuir essas barreiras, apresenta cobertura insuficiente e distribuição geográfica desigual. O programa de atendimento presencial das Contas Gov.br (Balcão Gov.br), em parceria com redes credenciadas, está presente em apenas quinze estados e cobre somente 98 municípios. Observa-se uma concentração desproporcional em Minas Gerais (57 unidades), enquanto estados de grande extensão territorial, como o Pará,

possuem apenas uma unidade credenciada, e a Bahia conta com apenas três unidades, todas na capital. Essa lacuna deixa vastas regiões e populações rurais sem suporte para recuperação de acesso (peça 46, p. 2). No âmbito digital, o canal de atendimento digital via chat dedicado ao esclarecimento de dúvidas relacionadas à Conta Gov.br (Assistente Gov.br) apresenta uma alta demanda reprimida, evidenciada pela demora de horas no atendimento (PT06, peça 114, p. 19, Apêndice 1, seção 5.4) e pela espera de dias para resposta do órgão prestador do serviço via Fala.br, ambos frequentemente sem solução definitiva (PT06, peça 114, p. 24, Apêndice 2)

4.4 Diminuição das exigências de segurança em relação às boas práticas por parte das organizações

61. A baixa maturidade em segurança da informação nas organizações, aliada à necessidade de reduzir a exclusão digital entre os usuários, tem levado gestores de serviços críticos a flexibilizarem os controles de segurança para garantir a continuidade operacional. No caso do INSS, por exemplo, a adoção de regras mais restritivas bloquearia o acesso de milhares de usuários nos canais digitais, direcionando-os para as centrais telefônicas (como a Central 135) e agências físicas, que não têm capacidade para absorver essa demanda adicional. (PT13, peça 109, itens 8, 40-42; Acórdão 2.387/2024-TCU-Plenário, Rel. Min. Augusto Nardes)

62. Para evitar o congestionamento desses canais e o aumento de reclamações por dificuldades de acesso ou falhas na validação biométrica, opta-se pela manutenção de padrões mínimos de segurança da Conta Gov.br (nível Bronze). Essa estratégia preserva a disponibilidade do serviço, mas amplia o risco de roubo de credenciais (PT13, peça 109, itens 8, 40-42; Acórdão 2387/2024-Plenário, Rel. Min. Augusto Nardes; Achado 5).

63. Essa imposição de controles rígidos, como a obrigatoriedade da ‘Verificação em Duas Etapas’ ou a exigência exclusiva de contas que precisam de reconhecimento facial (Prata ou Ouro), pode criar barreiras de acesso para cidadãos com baixa habilidade ou inclusão digital ou com limitações tecnológicas em seus dispositivos.

64. No entanto, ressalta-se que após a ocorrência de incidentes de segurança, as organizações têm mudado a postura e aumentado as exigências de segurança, uma vez que os custos (incluindo resposta ao incidente e aos órgãos de controle, como a ANPD, CGU ou TCU) e prejuízos dos incidentes podem superar a maior inconveniência para os cidadãos e os riscos de exclusão digital, como ocorrido nos recentes incidentes no Siafi e no Suibe , principalmente em sistemas críticos. Além disso, percebe-se que parte das organizações ainda possuem baixa governança em SI, o que ocasiona avaliações de risco inadequadas e, consequentemente, controles de SI frágeis, conforme Acórdão 2.387/2024 – TCU-plenário, Rel. Min. Benjamin Zymler.

4.5 Evidências, critérios e causas

65. As evidências que suportam o achado estão no papel de trabalho sobre grupos vulneráveis (PT06, peça 106) e reuniões com gestores (PT09, peça 105; PT13, peça 109). Nelas, também podem ser encontradas análises aprofundadas, demonstrando como a falta de habilidade e inclusão digital impacta a eficácia das medidas de segurança implementadas.

66. A fontes dos critérios que serviram de base para a análise foram:

66.1. Decreto 12.198/2024, que institui a Estratégia Federal de Governo Digital para o período de 2024 a 2027, prevendo ações de inclusão digital em segurança da informação para os cidadãos.

67. As causas identificadas indicam que:

67.1. A análise do diagrama de relações de causas e efeitos (p. Erro! Indicador não definido.) demonstra que as situações encontradas não são eventos isolados, mas consequências de uma cadeia causal que se origina na falha de governança nas políticas públicas para combater a exclusão digital e na ausência de programas efetivos de inclusão digital (seção 4.1). Essa lacuna educacional gera a baixa conscientização dos cidadãos sobre riscos cibernéticos, criando um ambiente propício para a disseminação de práticas inseguras e dificultando a implementação de controles robustos.

67.2. A insuficiência de programas efetivos de inclusão digital e conscientização: a inexistência de campanhas massivas e eficazes de educação em segurança da informação resulta no desconhecimento generalizado sobre boas práticas de segurança e seus riscos envolvidos. Sem essa base, o cidadão não compreende os riscos aos quais está exposto, tornando-se o elo mais frágil da cadeia de segurança (seção 4.1).

67.3. Cultura de uso inadequado de credenciais (efeito direto da baixa habilidade digital): a baixa conscientização leva à prática disseminada de compartilhamento de senhas com terceiros (ex.: familiares) e à reutilização de credenciais fracas (seção 4.2). Para viabilizar esse compartilhamento, os usuários evitam ou desativam voluntariamente a autenticação de dois fatores (MFA), resultando no baixo uso desse mecanismo de segurança e na maior exposição a golpes.

67.4. Insuficiência do suporte presencial (barreira estrutural): a distribuição geográfica desigual e a cobertura limitada do atendimento presencial (Balcão Gov.br) impedem que cidadãos sem habilidade digital ou acesso à tecnologia recebam o auxílio necessário para superar as barreiras de autenticação. Isso consolida a exclusão digital e força o cidadão a depender de terceiros, perpetuando o ciclo de insegurança. (seção 4.3)

67.5. Diminuição dos padrões de segurança pelas organizações: diante da incapacidade do cidadão em lidar com controles complexos e das falhas de usabilidade da plataforma, os gestores públicos optam por nivelar a segurança por baixo; somado a isso, a diminuição dos padrões de segurança também é causada pela baixa maturidade em SI das organizações. Para evitar o colapso no atendimento e garantir a entrega do serviço, as organizações diminuem as exigências de autenticação em relação às boas práticas, aceitando um risco elevado de fraude em troca da disponibilidade operacional (seção 4.4).

4.6 Propostas de encaminhamento e benefícios

68. Para tratar da insuficiência de programas de inclusão digital, que leva à exclusão digital de brasileiros e à baixa conscientização em segurança da informação por parte dos cidadãos, o que, por sua vez, leva ao uso inadequado de credenciais de acesso e à diminuição das exigências de segurança por parte dos gestores (seções 4.1, 4.2, 4.3 e 4.4) e:

68.1. Considerando: a) a baixa inclusão digital (seção 4.1); b) baixa conscientização em SI pela população, com consequente uso indevido de credenciais (seção 4.2); c) a dificuldade no uso dos serviços digitais e dificuldade na disponibilização de atendimento (seção 4.3); d) os problemas com o processo de recuperação de MFA atuais (seção 5.1); e e) a taxa de cerca de 20% de insucesso no login à Conta Gov.br, demonstrado nos painéis de monitoramento (PT09, peça 105, p. 9, item 68), a AudTI propõe:

68.1.1. Recomendar à SGD/MGI, com fundamento no art. 11 da Resolução - TCU 315/2020, que realize estudo de viabilidade e de riscos para a disponibilização de SMS, e-mail ou aplicativos MFA como métodos alternativos de Autenticação de Múltiplos Fatores (MFA), mas nunca como único fator de recuperação das contas, para oferecer opções de autenticação mais segura para usuários no nível bronze.

68.1.2. Como benefício, espera-se que a adoção da medida aumente a taxa de sucesso de login, reduza a exclusão digital de usuários com baixa habilidade técnica e ofereça alternativas que equilibrem a necessidade de segurança com a viabilidade de acesso para a população em geral.

68.1.3. Além disso, espera-se que a implementação das medidas recomendadas promova o fortalecimento da resiliência cibernética da Administração Pública Federal, mediante a redução significativa da superfície de ataque e da probabilidade de incidentes de acesso não autorizado a sistemas sensíveis. Ao condicionar o acesso a serviços críticos a níveis de confiabilidade superiores (Prata ou Ouro) e ao uso da verificação em duas etapas, as instituições garantem a conformidade com as diretrizes da SGD/MGI, elevando a proteção dos dados dos cidadãos e assegurando a integridade e a continuidade dos serviços públicos digitais integrados à plataforma Gov.br.

5 DIFICULDADES E FALHAS NO PROCESSO DE VALIDAÇÃO BIOMÉTRICA IMPACTAM NO ACESSO AO GOV.BR.

5.1 Frustração do usuário, sobrecarga dos canais de atendimento, menos contas com nível melhor de segurança e indisponibilidade de acesso

69. Devido a problemas técnicos na implementação do processo de validação da biometria facial, ocorrem falhas na etapa de validação de vivacidade (conhecido como liveness), essencial para a prova de vida do cidadão, pois garante que o cidadão está fisicamente presente e interagindo em tempo real, impedindo fraudes por representação. Limitações relacionadas à iluminação do ambiente, qualidade das câmeras de dispositivos móveis de baixo custo e posicionamento do usuário geram altas taxas de rejeição no reconhecimento facial. Essa instabilidade técnica impede que usuários legítimos, especialmente aqueles com menor habilidade digital, concluam a autenticação no Gov.br, resultando em bloqueio de acesso a serviços essenciais e frustração generalizada (PT06, peça 114, p. 6, seção 3.2, seção 3.4 e Apêndices 1, 2 e 3).

70. A segurança do ecossistema é agravada pela restrição da 'Verificação em Duas Etapas' (MFA) exclusivamente ao aplicativo instalado no dispositivo móvel. Essa arquitetura cria um ponto único de falha: em caso de perda, roubo ou dano ao aparelho, o cidadão perde o acesso ao segundo fator de autenticação. Para recuperar o acesso, o usuário é frequentemente obrigado a realizar novamente o reconhecimento facial – justamente o processo sujeito a falhas técnicas e instabilidades. Esse ciclo vicioso desestimula a adesão ao MFA, levando muitos usuários a desativarem a proteção para evitar o risco de bloqueio de conta (lockout), o que, paradoxalmente, facilita a ação de fraudadores que utilizam vídeos falsos criados por inteligência artificial (deepfakes) para assumir contas desprotegidas (PT06, peça 114, p. 6, seção 3.2, seção 3.4 e Apêndices 1, 2 e 3).

71. O suporte e atendimento aos cidadãos relativos às Contas Gov.br possuem presença física limitada, cobertura desigual, presença digital com demanda reprimida (quando a população necessita de um serviço essencial, mas não consegue acessá-lo devido a barreiras como filas de espera) e falta de resolutividade (item 60). Diante dessas lacunas, a equipe de auditoria identificou que muitos cidadãos recorrem a canais não oficiais, como o 'Reclame Aqui', nos quais permanecem sem retorno. (PT06, peça 114, p. 16, Apêndice 1). As maiorias das reclamações identificadas são relacionadas à perda de MFA e falhas de biometria, alinhando-se com o que os gestores também apontaram em reuniões (PT06, peça 114, p. 16, Apêndice 1; PT10, peça 106, p. 17, item 146)

72. A fragmentação e a desatualização das bases de dados governamentais utilizadas para validação (e.g. Identificação Civil Nacional – ICN, Carteira Nacional de Habilitação – CNH e Carteira de Identificação Nacional – CIN) prejudica a eficácia da validação biométrica. A base da CNH, por exemplo, possui um ciclo de atualização longo (dez anos), resultando em imagens históricas de baixa resolução que dificultam a comparação com a foto atual do cidadão. Adicionalmente, a ausência de integração com bases para cidadãos residentes no exterior limita a cobertura do serviço, obrigando a adoção de fluxos alternativos menos seguros ou burocráticos (PT06, peça 114, seção 3.4, PT10, peça 106, p. 16, item 136; PT09, peça 105, p. 17, item 155).

5.2 Validações falsas da identidade do cidadão

73. Simultaneamente, vulnerabilidades nos controles de detecção de vivacidade permitem a ocorrência de validações falsas da identidade. A Operação Face Off da Polícia Federal revelou que organizações criminosas utilizam técnicas avançadas, como vídeos falsos criados por inteligência artificial (deepfakes) de alta fidelidade, máscaras 2D/3D e manipulação de imagens ('selfies trocadas'), para burlar os sistemas de segurança. A exploração dessas falhas possibilita que fraudadores elevem o nível das contas para 'Ouro' ou 'Prata', assumindo a identidade de terceiros para realizar fraudes financeiras e acessar dados sensíveis, como o desvio de benefícios sociais e a transferência de veículos (peças 94-96).

74. Para reduzir o risco de exclusão digital decorrente dessas falhas técnicas, gestores de serviços críticos, como o INSS, adiam a obrigatoriedade da validação biométrica em etapas iniciais de acesso. A organização relata que a imposição irrestrita dessa tecnologia poderia sobrecarregar os canais de atendimento presencial, devido à incapacidade de grande parte dos

segurados em superar as barreiras de usabilidade da ferramenta de reconhecimento facial atual (PT13, peça 109, itens 8, 40-42).

75. Como contramedida a essas vulnerabilidades e buscando equilibrar segurança com usabilidade, o mercado adota as certificações iBeta, fundamentadas na norma técnica ISO/IEC 30107-3, para atestar a eficácia dos sistemas na detecção de ataques de apresentação (Presentation Attack Detection - PAD). O padrão iBeta Level 1 estabelece a linha de defesa primária, garantindo o bloqueio de fraudes de baixa sofisticação, como o uso de fotografias impressas e vídeos reproduzidos em telas bidimensionais. Por sua vez, a certificação iBeta Level 2 exige a comprovação robusta de vivacidade (liveness) contra ataques avançados, a exemplo de máscaras 3D de silicone e deepfakes de alta fidelidade.

76. No âmbito regulatório governamental, a recente Resolução Cefic - Casa Civil 21/2025 padroniza essas exigências para o Serviço Biométrico Federal. O normativo estabelece que o serviço de prova de vivacidade facial (liveness passivo) deve estar apto a receber a certificação iBeta Level 1 para transações consideradas de baixo risco. Para as transações de médio a alto risco, exige-se a aptidão para as certificações iBeta Level 1 e 2, em estrita conformidade com a norma ISO 30107-3. Adicionalmente, para garantir a alta precisão do motor biométrico no reconhecimento de imagens faciais, a resolução estipula que o resultado da Taxa de Falsa Não Identificação (FNIR - correspondente ao falso negativo) máxima aceitável é de 0,0085, condicionada a uma Taxa de Falsa Identificação Positiva (FPIR) fixa de 0,001.

77. Durante a etapa de comentários, os gestores do Serpro informaram que a evolução constante das ameaças tecnológicas exige melhorias contínuas nas soluções de validação biométrica, ressaltando que os padrões ISO podem não acompanhar essa dinâmica — entendimento também compartilhado pela CGU (peça 147, p. 6, item 18.4).

78. O Serpro utiliza soluções certificadas de prova de vida (liveness) através de contratos com terceiros, em conjunto com soluções próprias. Porém, a certificação atende somente ao nível mínimo iBeta Level 1. Os gestores do Serpro informaram que a imposição de critérios de segurança mais rígidos em soluções de validação biométrica restringiria a competitividade, resultando em um direcionamento indevido em possíveis contratações de soluções de prova de vida usadas na solução final de validação biométrica do Serpro (peça 147, p. 6, item 18.2). Por fim, comunicaram que está em andamento um processo licitatório para uma nova solução de prova de vida, com o objetivo de aprimorar as métricas de autenticação e elevar o nível de segurança do sistema, mas sem informar o nível de segurança a ser exigido (peça 147, p. 6, item 18.1).

79. Constatou-se que a inclusão de camadas adicionais de segurança pelo Serpro altera negativamente as métricas da solução final — como a taxa de rejeição de usuários legítimos — em relação aos parâmetros da certificação internacional contratada. (peça 147, p. 6, item 18.3)

5.3 Evidências, critérios e causas

80. As evidências que suportam o achado estão relacionadas no papel de trabalho sobre grupos vulneráveis (PT06, peça 114) e nas atas de reunião com gestores da SGD/MGI, Serpro e do INSS (peça 105, 106 e 109). Nelas, encontram-se análises aprofundadas sobre as limitações da tecnologia de reconhecimento facial e relatos de incidentes de segurança envolvendo a burla desses controles, como os identificados na Operação Face Off (peça 94-96).

81. Os critérios específicos de cada deficiência estão relacionados no Questionário de Avaliação de Controles Internos (peça 120). As fontes dos critérios que serviram de base para a análise foram:

81.1. ABNT NBR ISO/IEC 27002:2022 – Controles 5.17 (Informações de autenticação) e 8.3 (Controle de acesso à informação);

81.2. NIST Special Publication 800-63B – Digital Identity Guidelines, especificamente a seção 3.2.3, que estabelece requisitos para detecção de ataque de apresentação (Presentation Attack Detection – PAD) e uso de biometria para níveis de garantia elevados (IAL3/AAL3);

82. Quanto às causas que teriam levado à situação encontrada, os gestores informaram, durante as reuniões técnicas (peça 105 e peça 106), o seguinte:

82.1. Limitações técnicas e de infraestrutura dos usuários: a diversidade de dispositivos móveis utilizados pela população, muitos com câmeras de baixa resolução, somada a condições ambientais inadequadas (iluminação ruim), prejudica a eficácia dos algoritmos de prova de vida (liveness), gerando altas taxas de rejeição para usuários legítimos (PT10, peça 106, p. 17, item 137);

82.2. Qualidade e fragmentação das bases biométricas: a desatualização das imagens nas bases governamentais (ex.: CNH com renovação a cada dez anos) e a falta de integração plena entre os acervos biométricos (TSE, CNH, CIN) dificultam a validação precisa, aumentando a vulnerabilidade a fraudes e falsos negativos (PT09, peça 105, p. 17, item 155);

82.3. Defasagem dinâmica dos padrões internacionais frente à evolução das ameaças: a evolução constante e célere das ameaças tecnológicas exige melhorias contínuas nas soluções de validação biométrica, superando a velocidade de atualização dos padrões normativos ISO, os quais podem não acompanhar o ritmo dessas novas vulnerabilidades (peça 147, p. 6, item 18.4); e

82.4. Risco de restrição à competitividade e direcionamento licitatório: a imposição imediata de critérios de segurança excessivamente rígidos ou estritos nas contratações de soluções de prova de vida, usadas na solução final de validação biométrica do Serpro, limitaria o mercado fornecedor apto, resultando no risco de direcionamento indevido do certame e prejuízo à ampla concorrência (peça 147, p. 6, item 18.2).

5.4 Propostas de encaminhamento e benefícios

83. Para tratar dos problemas técnicos no processo de validação da biometria facial (capítulo 5), e considerando: a) a taxa de rejeição de usuários legítimos acima das boas práticas no processo de validação da biometria facial (peça 104, p. 9), b) considerando a norma ISO/IEC 30107-3 e o laboratório de testes iBeta Quality Assurance, acreditado pelo NIST (via NVLAP) para realizar testes de conformidade de biometria, especificamente o teste de Detecção de Vivacidade (Liveness Detection / Presentation Attack Detection – PAD), baseado na norma ISO/IEC 30107-3; c) considerando os requisitos mínimos do motor biométrico especificados na Resolução Cefic - Casa Civil nº 21/2025 (item 76), e d) a análise da equipe de auditoria pós-comentários dos gestores (peça 147, p. 14, seção 6.6), a AudTI propõe:

83.1. Recomendar à SGD/MGI, com fundamento no art. 11 da Resolução - TCU 315/2020, que adote as medidas necessárias para promover o aprimoramento tecnológico, operacional e de segurança das soluções de biometria facial e prova de vida (liveness) do ecossistema Gov.br, de forma a:

83.1.1. assegurar que os níveis de desempenho de segurança e acurácia sejam compatíveis com padrões de boas práticas internacionalmente reconhecidos (NIST SP 63A 3.11 Rev. 4 e ISO/IEC 30107-3:2023);

83.1.2. identificar e mitigar eventuais disparidades de desempenho para grupos demográficos específicos; e

83.1.3. atualizar periodicamente as bases de validação sob controle da SGD/MGI.

84. Como exemplo, seguindo as boas práticas para garantir a manutenção de uma Taxa de Aceitação de Ataque de Impostor (IAPAR) inferior a 0,07 (NIST SP 63A 3.11 Rev. 4) ou utilizar métricas de APCER e BFCER calculadas em conformidade com a ISO/IEC 30107-3:2023, a exemplo de taxas adequadas de falsa rejeição (FNMR de 1:100 ou melhor) e de falso aceitação (FMR de 1:10.000 ou melhor), assegurando que a defasagem de desempenho para grupos demográficos específicos não ultrapasse 25% em relação à população geral, promovendo, ainda, a atualização periódica de suas bases de validação (NIST SP 63A 3.11 Rev. 4). De igual modo, a SGD/MGI pode, por exemplo, validar a robustez dos mecanismos de detecção de ataques de apresentação contra falsificações de alto nível baseadas em inteligência artificial, com o uso de soluções certificadas com os requisitos mínimos da certificação iBeta Level 2.

85. Como benefício, espera-se que essas ações inviabilizem a apropriação fraudulenta de identidades digitais, reduzindo, de forma significativa, o espaço para golpes de personificação

em serviços governamentais. Simultaneamente, as adequações visam mitigar as taxas de rejeição indevida de usuários legítimos, diminuindo a sobrecarga operacional dos canais de suporte e fomentando a adesão orgânica da população a níveis de conta com maior segurança.

6 A INCONSISTÊNCIA DOS MECANISMOS DE SEGURANÇA EXIGIDOS EM CADA NÍVEL DA CONTA GOV.BR, ALIADA À BAIXA ADOÇÃO, PELOS GESTORES DOS SERVIÇOS PÚBLICOS, DE MECANISMOS DE AUTENTICAÇÃO MAIS ROBUSTOS AUMENTA O RISCO DE USO INDEVIDO DAS CONTAS GOV.BR DOS CIDADÃOS BRASILEIROS

86. Os níveis de segurança da Conta Gov.br não garantem segurança na prática, pois há uma contradição em classificar contas como de alta confiabilidade quando sua segurança técnica é baixa (seção 6.1). Além disso, tanto os níveis quanto os demais critérios de segurança da Conta Gov.br são pouco adotados pelos serviços, inclusive os críticos e sensíveis (seção 6.2), e pelos usuários, apesar dos esforços da SGD/MGI terem aumentado o número de contas ouro que usam verificação em duas etapas (peça 100). Esse quadro é agravado pela fragmentação e deficiências nas diretrizes e orientações disponíveis para os gestores (seção 6.3).

87. Esse cenário leva à facilitação de ataques, como o uso de credenciais vazadas para acessar serviços críticos, e à ocorrência de fraudes digitais, impactando a segurança dos cidadãos e a confiabilidade dos serviços. A implementação de critérios ineficazes pelos gestores surge como uma consequência da inconsistência entre confiabilidade e segurança técnica. No entanto, essa falha também é alimentada por outros problemas relacionados, tornando-se, em conjunto, o principal motivo da fragilidade dos níveis de segurança da Conta Gov.br (peça 95, p. 2; peça 94, p. 2).

6.1 Inconsistência estrutural entre contas com alta confiabilidade (nível ouro), mas baixa segurança

88. Há uma inconsistência estrutural crítica no modelo de identidade da Plataforma Gov.br, caracterizada pelo desalinhamento entre o nível de confiança no cadastro do usuário (Nível de Garantia de Identidade - IAL) e a robustez do processo de login exigido (Nível de Garantia de Autenticação - AAL). Atualmente, uma conta de nível Ouro — que atesta com alto grau de certeza que o usuário é quem diz ser, permitindo acesso a serviços sensíveis e assinatura de documentos — pode ser acessada utilizando apenas CPF e senha (fator único de autenticação), o que corresponde ao nível de segurança mais baixo (AAL1) segundo as normas internacionais (NIST SP 800-63B). Essa brecha permite que o comprometimento de uma simples senha conceda a um fraudador privilégios elevados de acesso (PT03, peça 120, p. 5, item 4.1).

89. Embora a Secretaria de Governo Digital (SGD/MGI) incentive o uso da ‘Verificação em Duas Etapas’ (MFA) para contas ‘Ouro’, essa configuração não é tecnicamente obrigatória para todos os fluxos de acesso, criando um cenário onde a ‘chave’ (senha) para abrir a ‘porta blindada’ (serviços nível Ouro) é frágil. A Portaria - SGD/MGI 11.229/2025, que visa corrigir essa distorção, por meio da vinculação obrigatória do nível de confiabilidade da conta ao método de autenticação (ex: conta Ouro exigir MFA ou certificado digital), entrará em vigor apenas em 14/6/2026, prolongando a vulnerabilidade (PT03, peça 120, p. 5, item 1).

90. Adicionalmente, a equipe de auditoria identificou uma falha nos processos de revisão de ciclo de vida das credenciais. Enquanto os selos de confiabilidade bancária (conta ‘Prata’) expiram após 36 meses e os certificados digitais passam por verificação diária de revogação, os selos de nível Ouro obtidos via reconhecimento facial não possuem rotina de revalidação periódica definida. Na prática, uma vez que o cidadão obtém o nível Ouro por biometria, ele mantém esse status de privilégio elevado indefinidamente, sem a necessidade de renovar a prova de vida ou confirmar a posse do documento. Esse modelo contraria as boas práticas de gestão de identidade que recomendam a conferência regular dos atributos de confiança (PT02, peça 119, item 4.3).

6.2 Disponibilização de serviços críticos ou sensíveis com exigência de nível mínimo de segurança

91. A equipe de auditoria identificou a oferta de serviços de alta criticidade operando com requisitos de autenticação menos seguros (nível Bronze), sem a garantia de que o usuário não

negue ter feito a ação (não repúdio) ou a validação robusta da identidade. Serviços sensíveis nas áreas de segurança pública (autorização para aquisição de armas e produtos controlados), seguridade social e finanças (saque do FGTS e solicitação de benefícios previdenciários) e transportes (transferência de propriedade de veículos) permitem o acesso apenas com CPF e senha, expondo o Estado brasileiro e o cidadão a riscos elevados de fraudes patrimoniais e desvios de recursos (PT08, peça 115, p. 5, itens 9-11).

92. A análise do catálogo de serviços integrados ao Gov.br revelou a subutilização sistêmica dos critérios de segurança da plataforma. De 5.352 serviços, 64% dos que requerem autenticação exigem apenas o nível mínimo de conta (Bronze), enquanto somente 2% demandam o nível máximo de confiabilidade (Ouro). A exigência da 'Verificação em Duas Etapas' (MFA) é marginal, presente em apenas 1% dos serviços digitais integrados ao Gov.br, sendo que 92% desses casos concentram-se em apenas três organizações (Banco Central – BCB, Agência Nacional do Cinema – Ancine e Ministério do Trabalho e Emprego – MTE), evidenciando a falta de padronização na proteção de ativos críticos pela maioria dos órgãos (PT08, peça 115, p. 6, seção 2.3).

93. Além da baixa exigência formal, a equipe de auditoria identificou falhas nos controles de implementação técnica. Em testes substantivos, constatou-se a ocorrência de divergências entre os requisitos de segurança declarados no catálogo e a configuração efetiva da aplicação. Foi possível acessar com conta nível 'Bronze' no serviço digital Atendimento ao Consumidor de Serviços de Telecomunicações, que, em sua documentação e página oficial, exigia níveis 'Prata' ou 'Ouro'. Isso demonstra que a validação do token de acesso e dos atributos de segurança não foi implementada corretamente (PT05, peça 111, p. 3, item 11).

94. Essa implementação de critérios ineficazes ou desproporcionais aos riscos reais decorre, em parte, da ausência de formalidade metodológica (processo estruturado e sistemático) na análise de riscos por parte dos gestores dos serviços e da priorização da disponibilidade do serviço em vez da segurança, visando evitar o bloqueio de usuários com baixa inclusão digital. Contudo, tal prática amplia a superfície de ataque para fraudadores que exploram a fragilidade das credenciais de nível básico para cometer golpes em larga escala (PT05, peça 111, p. 5, seção 2.2 e Apêndices 1 e 2; seção 4.4).

6.3 Fragmentação e deficiências nas diretrizes e orientações

95. A fragmentação de diretrizes e as deficiências nas orientações de integração resultam na adoção de controles técnicos sem fundamentação adequada, com ausência de formalidade metodológica e de análise prévia de riscos na gestão de identidades. Consequentemente, ocorre uma incoerência entre o nível de risco aceito pelas organizações e as configurações implementadas, deixando os serviços digitais governamentais mais expostos (PT05, peça 111, p. 5, seção 2.2).

96. As orientações de segurança fornecidas pela SGD/MGI carecem de instrumentos práticos para apoiar a tomada de decisão dos gestores. A matriz de risco e impacto disponibilizada é subjetiva e binária (Alto/Baixo), ignorando cenários de risco médio onde se enquadram a maioria dos serviços digitais. A ausência de uma metodologia padronizada, como calculadoras de risco ou escalas objetivas, leva a classificações baseadas na opinião pessoal, sem critérios fixos que podem subestimar a criticidade dos ativos e a necessidade de controles mais seguros (PT05, peça 111, p. 5, item 63-66).

97. Identificaram-se inconsistências semânticas e operacionais entre as diretrizes estratégicas e as ferramentas de solicitação. Enquanto a página de orientações da SGD/MGI estabelece claramente que serviços envolvendo transações financeiras e bens e sistemas acessados somente por autoridades, pessoas politicamente expostas ou servidores do alto escalão devem adotar o nível Ouro com 'Verificação em Duas Etapas' (MFA), a orientação geral apresentada no formulário de integração do serviço ao Gov.br é genérica, sugerindo apenas que o nível seja 'no mínimo PRATA' para acesso a informações sensíveis ou pagamentos de benefícios. Essa falta de distinção explícita no momento do cadastro pode induzir o gestor ao erro, permitindo que serviços de alto impacto sejam configurados com requisitos de segurança inferiores (nível Prata) aos recomendados nas diretrizes (nível Ouro) (PT05, peça 111, p.6, itens 67-68).

98. Além da divergência nos níveis de conta, o formulário utiliza terminologias divergentes das normas publicadas, classificando o acesso como ‘ilimitado’, ‘restrito’ ou ‘sigiloso’, em vez de utilizar os níveis de confiabilidade (Bronze, Prata, Ouro) definidos na página de orientação sobre os critérios de segurança adotados na Conta Gov.br. Essas diferenças de nomenclaturas podem confundir o gestor no momento da configuração do serviço, dificultando a correta tradução do risco do negócio em parâmetros técnicos de autenticação (PT05, peça 111, seção 2.2, item 69).

99. O roteiro técnico de integração do serviço ao Gov.br apresenta deficiências que comprometem a segurança das implementações nos órgãos clientes. O único exemplo prático de código disponibilizado (em PHP) utiliza parâmetros estáticos (state e nonce) e não implementa a validação de tokens via chave pública (JWT). Tais vulnerabilidades violam o padrão OpenID Connect (OIDC) e expõem as aplicações a riscos de sequestro de sessão e ataques de repetição (PT05, peça 111, p. 3, item 12). Adicionalmente, a documentação não oferece exemplos práticos para a implementação da ‘Verificação em Duas Etapas’ (MFA), contribuindo para a baixa adesão ao mecanismo (PT05, peça 111, p. 3, item 9).

6.4 Evidências, critérios e causas

100. As evidências que suportam o achado estão consolidadas no papel de trabalho de integração, autorização e uso seguro dos serviços públicos digitais (PT08, peça 115), que demonstra a baixa exigência de segurança nos serviços, e no papel de trabalho de diretrizes da SGD/MGI (PT05, peça 111), que detalha as orientações de integração, atendimento e gestão de risco passadas pela SGD/MGI. Adicionalmente, o papel de trabalho de autenticação (PT03, peça 120, p. 5, item 4.1) evidencia a desconexão entre o nível da conta (identificação) e da autenticação.

101. Os critérios específicos para as deficiências identificadas estão relacionados nos Questionários de Avaliação de Controles Internos (peça 119 e 120). As fontes normativas e de boas práticas que serviram de base para a análise foram:

101.1. ABNT NBR ISO/IEC 27002:2022 – Controles 5.15 (Controle de acesso), 5.18 (Direitos de acesso) e 8.5 (Autenticação segura), que preconizam o gerenciamento rigoroso dos privilégios e métodos de autenticação fortes para acessos críticos; e

101.2. NIST Special Publication 800-63B – Digital Identity Guidelines, especificamente as definições de Níveis de Garantia de Autenticação (AAL), que recomendam AAL2 (MFA) ou AAL3 (hardware criptográfico) para transações de alto risco, em contraste com o uso disseminado de senha simples (AAL1).

102. As causas que levaram à inefetividade dos níveis de segurança são:

102.1. Priorização da disponibilidade em detrimento da segurança: organizações gestoras de serviços críticos, como o INSS, optam por manter requisitos mínimos (nível Bronze) para evitar o bloqueio massivo de usuários com baixa inclusão digital, o que poderia colapsar canais de atendimento presenciais e telefônicos (seção 4.4). Há uma percepção de que a implementação de controles de segurança, como o MFA, é uma barreira de usabilidade, levando gestores a não utilizarem as funcionalidades de segurança disponíveis na plataforma por receio de aumento de demandas de suporte (seção 4.4). Além disso, a baixa maturidade em SI por parte das organizações contribui para implementação de critérios mínimos de segurança (Acórdão 2.387/2024-TCU-Plenário, Rel. Min. Augusto Nardes);

102.2. Limitações técnicas da plataforma: a vinculação restritiva do segundo fator de autenticação (MFA) ao aplicativo no dispositivo móvel, sem opções flexíveis de recuperação, gera receio nos gestores de torná-lo obrigatório, pois a perda do celular pelo cidadão resulta em perda temporária do acesso à conta, sendo necessário requisitar, via formulário, a desativação do MFA (PT03, peça 120, p. 5, item 4.1).

102.3. Sistemas legados e controles internos: alguns serviços utilizam mecanismos próprios de autenticação, apesar de disponibilizarem o serviço no catálogo da plataforma (PT08, peça 115, p. 2, item 5) e outros serviços apresentam controles de segurança posteriores ao login, por exemplo, comparecimento presencial posterior para completar o fluxo do serviço (PT13, peça 109, p. 2, item 5-6).

102.4. Limitações de acesso aos usuários residentes no exterior: no caso do INSS, usuários no exterior representaram cerca de 4 milhões de acessos ao Meu INSS em 2024. Contudo, os recursos para elevar as credenciais de acesso são limitados fora do Brasil. A necessidade de soluções junto às representações diplomáticas ainda está sendo discutida pela SGD/MGI (peça 123, p. 6, item 37).

6.5 Propostas de encaminhamento e benefícios

103. Para tratar a situação de inconsistência entre contas com alta confiabilidade, mas baixa segurança, a AudTI propõe dois encaminhamentos, considerando:

103.1. a) a Portaria - SGD/MGI 11.229/2025, que estabelece diretrizes para a criação e gestão de contas digitais na Plataforma gov.br, visando a segurança, a usabilidade e a confiança no ambiente digital, em especial, o art. 5º, que estabelece que o acesso à Plataforma Gov.br exija diferentes critérios de autenticação conforme o nível da conta digital do cidadão (o nível bronze requer apenas autenticação de fator único, o nível prata exige autenticação multifator, e o nível ouro demanda autenticação multifator fornecida pela própria plataforma ou validação por meio de certificado digital ICP-Brasil);

103.2. b) a análise da equipe de auditoria pós-comentários dos gestores (peça 147, p. 15, seção 6.9), onde foi informado que a SGD/MGI pretende implementar a obrigatoriedade de atendimento à Portaria - SGD/MGI 11.229/2025 de maneira gradual, sem apresentar plano de ação ou planejamento específico.

104. Assim, a AudTI propõe:

104.1. Recomendar à SGD/MGI, com fundamento no art. 11 da Resolução - TCU 315/2020, que adote as medidas necessárias para:

104.1.1. instituir ciclos de validação e revalidação periódica para os selos de identidade obtidos via reconhecimento facial e Carteira de Identidade Nacional, alinhando a gestão do ciclo de vida das credenciais às boas práticas internacionais de gestão de identidade digital.

104.2. Determinar à SGD/MGI, com fundamento no art. 4º, inciso I, da Resolução - TCU 315/2020, que, no prazo de 180 dias:

104.2.1. implemente controles lógicos para assegurar o alinhamento entre nível de identificação da Conta Gov.br e os métodos de autenticação definidos na Portaria - SGD/MGI 11.229/2025;

104.3. Como benefício, espera-se que a adoção da medida assegure a integridade técnica do modelo de confiança da Conta Gov.br, garanta a conformidade automatizada com a Portaria - SGD/MGI 11.229/2025 e elimine inconsistências entre a confiabilidade declarada do nível da conta e a robustez efetiva do método de autenticação exigido, reduzindo o risco de que contas com nível elevado de confiança, eventualmente comprometidas ou obtidas de forma fraudulenta, permaneçam ativas indefinidamente, dificultando a perpetuação de fraudes de personificação baseadas em identidades digitais indevidamente elevadas.

105. Para tratar as divergências entre orientações fornecidas aos gestores no site e sistemas, considerando: a) que as inconsistências semânticas entre a página de orientações da SGD/MGI, o formulário de cadastro de serviços e o sistema de integração podem confundir o gestor do serviço; e b) a melhoria na redação da recomendação da equipe de auditoria pós-comentários dos gestores (peça 147, p. 11, seção 6.11); a AudTI propõe:

105.1. Recomendar à SGD/MGI, com fundamento no art. 11 da Resolução-TCU 315/2020, que adote as medidas necessárias para aprimorar, consolidar e alinhar as diretrizes de segurança e manuais de integração dos serviços ao Login Gov.br (Login Único).

105.2. Como benefício, espera-se que a adoção das medidas reduza as ocorrências de configurações incorretas por parte dos gestores, diminuindo a discrepância entre o nível de segurança declarado e o efetivamente implementado nos serviços digitais governamentais.

106. Além disso, após a etapa de comentários dos gestores e análise da equipe de auditoria (peça 147, p. 15, seção 6.10), e considerando que: a) 64% dos serviços integrados ao Login único requer o nível mínimo de conta (bronze) e apenas 2% dos serviços requerem o nível máximo de segurança na identificação (ouro); b) somente 1% dos serviços requerem a

verificação em duas etapas e c) há serviços críticos e sensíveis que exigem somente nível de segurança mínimo (conta bronze) (seção 6.2), a AudTI propõe:

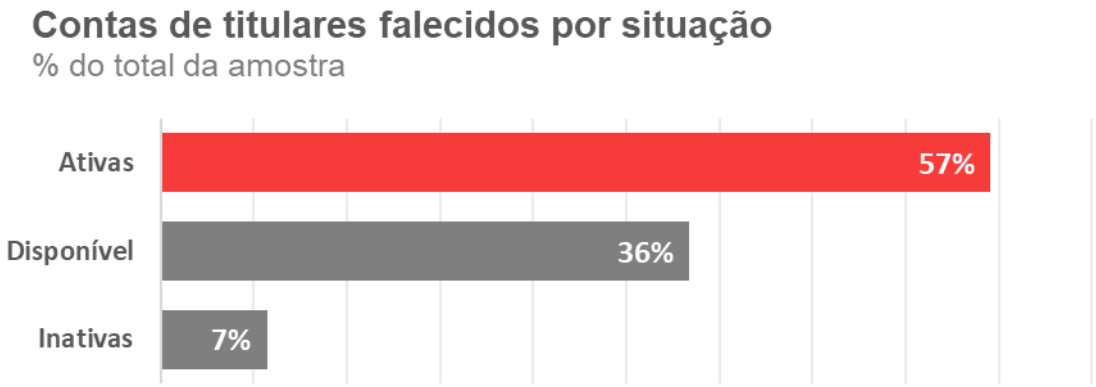
106.1. Dar ciência às unidades jurisdicionadas do TCU e gestoras de serviços integrados à plataforma Gov.br (conforme lista no Apêndice F), com fundamento no art. 9º, inciso I, da Resolução-TCU 315, de 2020, de que a definição dos níveis de confiabilidade das contas (Bronze, Prata ou Ouro) e dos métodos de acesso sem a prévia realização de avaliação de risco, especialmente para serviços classificados como críticos ou sensíveis, expõe a Administração Pública a incidentes de segurança e descumpre o dever de proteção de dados dos cidadãos, em decorrência da inobservância dos seguintes dispositivos: Lei 13.709/2018: Art. 50, § 2º, inciso I, d); e Portaria - SGD/MGI 11.229/2025: Art. 7º, incisos I e II.

106.2. Como benefício, espera-se que a implementação das medidas recomendadas promova o fortalecimento da resiliência cibernética da Administração Pública Federal, mediante a redução significativa da superfície de ataque e da probabilidade de incidentes de acesso não autorizado a sistemas sensíveis. Ao condicionar o acesso a serviços críticos a níveis de confiabilidade superiores (Prata ou Ouro) e ao uso da verificação em duas etapas, as instituições garantem a conformidade com as diretrizes da SGD/MGI, elevando a proteção dos dados dos cidadãos e assegurando a integridade e a continuidade dos serviços públicos digitais integrados à plataforma Gov.br.

7 FALHAS NA SINCRONIZAÇÃO DE DADOS ENTRE AS BASES DE REGISTRO CIVIL E DO CPF PODEM PERMITIR FRAUDES NO ACESSO AO GOV.BR E EM SERVIÇOS PÚBLICOS POR MEIO DE CADASTRO DE CIDADÃOS FALECIDOS

107. A equipe de auditoria identificou a existência de contas ativas no Conta Gov.br vinculadas a CPFs de pessoas com registro de óbito, o que representa 57% da amostra analisada, conforme a Figura 2. A manutenção indevida desses acessos decorre de atrasos significativos na sincronização de dados entre as bases de registro civil e a plataforma, resultando em prazos médios de inativação das contas elevadas, que variam de 65 dias para contas de nível Ouro a 70 dias para contas de nível Bronze. Essa deficiência nos controles de ciclo de vida da identidade permite a persistência e a exploração prolongada de acessos indevidos, viabilizando fraudes e o uso de serviços por terceiros em nome de titulares falecidos (PT12, peça 108, itens 8-9, 11 e 12-21).

Figura 2 - Gráfico de contas de titulares falecidos por situação



Fonte: Equipe de Auditoria

108. Além disso, foram identificadas a existência de titulares falecidos com a situação 'Disponível' no Contas Gov.br. Segundo as regras de negócio, são contas que não existem no cadastro do sistema, mas que não há qualquer restrição, ou seja, estão aptas para serem utilizadas por fraudadores. Assim, se alguém se passar por um usuário de CPF falecido, ele consegue criar uma conta nova, pois não há restrição no sistema. A permanência desses CPFs sem o devido bloqueio ou restrição no sistema de acesso digital eleva o risco de um criminoso se passar por outra pessoa (personificação) e, consequentemente, usar indevidamente

identidades de pessoas falecidas para possível prática de fraudes. Um caso concreto é o relatado na notícia sobre a Operação Krypteia (peça 95). O criminoso conseguia invadir a conta Gov.br do proprietário do veículo original e obtinha acesso à documentação veicular que era usada posteriormente para praticar outros crimes (PT12, peça 108, p. 5, itens 12-13).

7.1 Contas de titulares falecidos com nível de confiabilidade elevadas

109. Embora a maioria das contas ativas de titulares falecidos (representando 68%) pertença ao nível Bronze, constatou-se um volume relevante de credenciais com níveis elevados de privilégio: contas no nível 'Prata' e contas no nível 'Ouro'. A manutenção indevida dessas contas de níveis superiores é crítica, pois tais credenciais habilitam o acesso a serviços sensíveis, visualização de dados fiscais e bancários, além de permitirem a assinatura eletrônica de documentos com validade jurídica (PT12, peça 108, p. 3, itens 8-9).

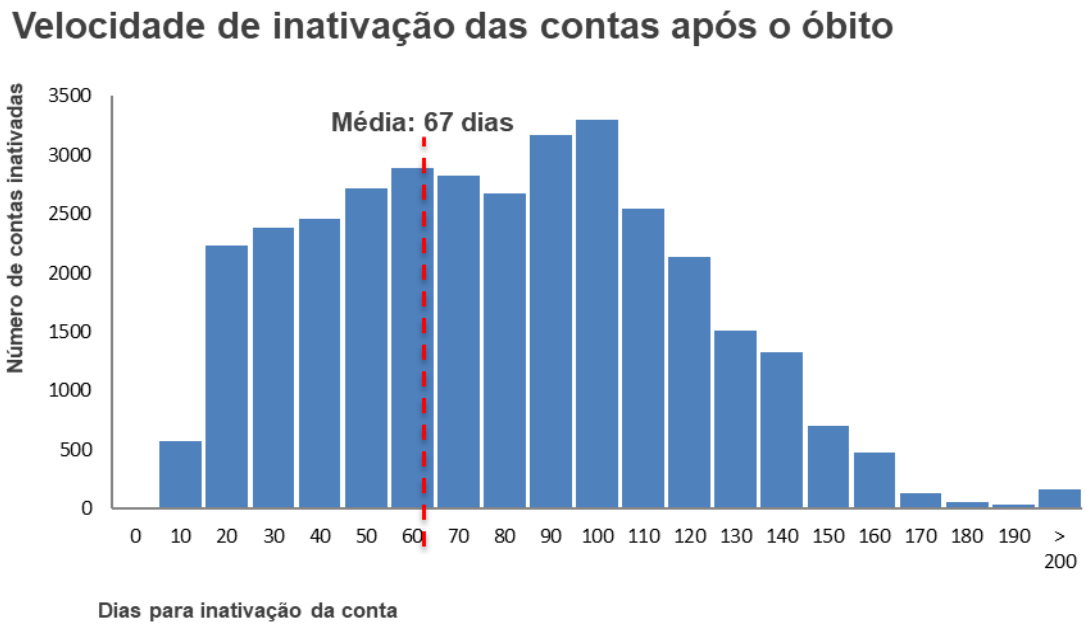
110. A equipe de auditoria também confirmou o uso de dispositivos de autenticação por terceiros em contas ativas de falecidos com a 'Verificação em Duas Etapas' (MFA) habilitada. Dessas, há contas que registraram acesso ao sistema após o óbito, indicando que os dispositivos móveis dos falecidos estão sob controle de terceiros (PT12, peça 108, p. 6, itens 19-20).

7.2 Criação e acessos indevidos após o óbito

111. Identificou-se a criação de novas contas (2% da amostra) no Contas Gov.br em data posterior ao registro do óbito do titular da conta no Sistema Nacional de Informações de Registro Civil (Sirc). Adicionalmente, os dados mostram a realização efetiva de login em contas (14%) após o registro do falecimento, confirmando que terceiros estão utilizando ativamente essas credenciais para acessar serviços públicos digitais em nome de pessoas falecidas (PT12, peça 108, p. 3, itens 10-11).

7.3 Demora no processo de inativação

112. A taxa de inativação automática mostrou-se insuficiente frente ao volume de óbitos. Apenas 7,32% das contas foram bloqueadas após o registro da certidão de óbito. O tempo de resposta do sistema apresenta atraso excessivo, com uma média geral de 67 dias para a inativação. Observou-se uma disparidade nos controles de atualização cadastral baseada no nível da conta: enquanto contas Prata e Ouro levam em média 65 dias para serem inativadas, as contas nível Bronze permanecem ativas por uma média de 70 dias após a certidão de óbito, expondo o sistema a janelas de vulnerabilidade prolongadas (PT12, peça 108, p. 4, itens 12 e 18-19).



113. Além disso, falhas de sincronização entre os sistemas foram detectadas: 31% das contas na amostra permanecem ativas no Gov.br mesmo constando com a situação cadastral 'Titular Falecido' na base da Receita Federal (RFB), evidenciando que a atualização na base fiscal não aciona o bloqueio automático na plataforma de acesso. No entanto, não foram detectados acessos indevidos após o registro da situação cadastral 'Titular falecido' na base da RFB (PT12, peça 108, p. 5, itens 22-23 e 26).

114. O processo de inativação de contas por motivo de óbito não ocorre mediante varredura periódica e proativa em toda a base de usuários, sendo acionado de forma reativa apenas no momento da tentativa de login. O mecanismo técnico adotado pelo Serpro, empresa que mantém a plataforma Gov.br, utiliza um sistema de fila que aguarda o agrupamento de CPFs (lote) para realizar a consulta de situação cadastral na base da Secretaria Especial da Receita Federal do Brasil (RFB). Essa arquitetura de processamento em lote visa otimizar o consumo de recursos computacionais, mas introduz um atraso no fluxo de autenticação (PT10, peça 106, itens 105-106; PT2, peça 119, item 4.3).

115. Além disso, há deficiência de controle na lógica de 'falha aberta' (fail-open) implementada nesse fluxo. Caso a fila de processamento não seja preenchida tempestivamente ou a consulta à RFB não retorne dentro do tempo limite da sessão, o sistema prioriza a disponibilidade do serviço em vez da segurança. Nessas situações, a verificação de óbito é ignorada e a autenticação é permitida, possibilitando que credenciais de titulares falecidos continuem operacionais caso a validação na RFB não seja concluída em tempo real (PT10, peça 106, item 106; PT2, peça 119, item 4.3).

116. Os gestores informaram que a atualização da base de CPFs é feita diariamente e o gestor responsável pela manutenção da base é a Secretaria Especial da Receita Federal do Brasil (RFB) (peça 147, p. 12, seção 6.5, item 40). Assim, a proposta de encaminhamento endereçada à SGD/MGI tem como objetivo promover medidas para gerir os riscos de falecidos permanecerem com contas ativas no Login Gov.Br.

117. Após a análise dos comentários dos gestores (peça 147, p. 12, seção 6.5, item 41), além dos manuais internos, a equipe de auditoria adicionou ciência à RFB, considerando que o órgão é o responsável pela base de dados de CPF e o relatório preliminar não foi enviado para comentários da RFB, o que inviabiliza proposta de determinação ou recomendação.

7.4 Evidências, critérios e causas

118. As evidências que suportam o achado estão consolidadas no papel de trabalho sobre contas ativas de falecidos (PT12, peça 108, p. 3-5), que demonstra a manutenção indevida de 445 mil

contas ativas de titulares falecidos e a ocorrência de logins póstumos. Adicionalmente, o papel de trabalho de monitoramento (PT04, peça 121, p. 5-6) e a ata de reunião com o Serpro (PT10, peça 106, p. 3 e 19) evidenciam as falhas técnicas nos processos de bloqueio automático e a inexistência de revisão proativa de anomalias.

119. Os critérios específicos para as deficiências identificadas estão relacionados nos Questionários de Avaliação de Controles Internos (PT04, peça 121). As fontes normativas e de boas práticas que serviram de base para a análise foram:

119.1. ABNT NBR ISO/IEC 27002:2022 – Controles 5.16 (Gestão de identidade) e 8.16 (Atividades de monitoramento), que preconizam a revogação tempestiva de direitos de acesso e a detecção de comportamentos anômalos;

119.2. CIS Controls v8.1, especificamente a Salvaguarda 5.3 (Disable Dormant Accounts), que recomenda a desativação automática de contas sem uso ou inválidas, e a Salvaguarda 6.2 (Establish an Access Revoking Process), que exige processos para revogar acessos imediatamente após o término da necessidade de uso ou alteração de status do usuário.

120. Quanto às possíveis causas que levaram à persistência de contas ativas de falecidos, os gestores informaram, durante as reuniões técnicas e nos levantamentos de auditoria (peça 99, p. 3, itens 105-106; peça 193, p. 5, itens 26-27), o seguinte:

120.1. Limitações na arquitetura de verificação de óbito: o bloqueio não ocorre por varredura proativa na base, mas apenas reativamente no momento do login, utilizando um sistema de filas (lotes de CPFs) para consulta à base da RFB. Esse processo possui lógica de 'falha aberta' (fail-open), permitindo o acesso caso a verificação externa falhe ou demore, priorizando a disponibilidade do serviço em detrimento da segurança (peça 99, p. 3);

120.2. Falhas de interoperabilidade entre bases: a atualização do status 'Titular Falecido' na base da RFB ou no Sirc não aciona gatilhos automáticos imediatos para a inativação da conta no Gov.br, resultando em janelas de vulnerabilidade onde o CPF consta como irregular na origem, mas permanece ativo na plataforma de acesso ao serviço (peça 108, p. 5).

120.3. Acórdão 2.919/2025-TCU-Plenário do TCU, Rel. Min. Benjamin Zymler: a fiscalização identificou que há um descompasso entre as informações de óbito registradas no Sistema Nacional de Informações de Registro Civil (Sirc) e a situação cadastral mantida na base de CPF da RFB. A informação de óbito constante no Sirc muitas vezes 'ainda não foi atualizada na base da RFB'. O relatório menciona que, após os testes, a RFB informou ter apropriado 574.297 óbitos do Sirc para o CPF entre julho e setembro de 2025. Devido à necessidade constante de manter as bases sincronizadas, o TCU recomendou à RFB que passe a avaliar e incorporar, de forma periódica ou recorrente, as informações de óbitos do Sirc à base de dados do CPF (peça 108, p. 6, itens 24-27).

7.5 Proposta de encaminhamento e benefícios

121. Para resolver o problema de contas ativas de titulares falecidos, considerando a análise da equipe de auditoria pós-comentários dos gestores (peça 147, p. 12, seção 6.5), a AudTI propõe:

121.1. Determinar à SGD/MGI, com fundamento no art. 4º, inciso I, da Resolução - TCU 315/2020, que, no prazo de 180 dias:

121.1.1. avalie as contas constantes da planilha 'Contas ativas.csv' (item não digitalizável da peça 108) cujos titulares encontravam-se ativos no Login Gov.Br em 29/1/2026 e simultaneamente na situação de falecidos na base do SIRC, para fins de inativação dessas contas, se for o caso.

121.2. Recomendar à SGD/MGI, com fundamento no art. 11 da Resolução TCU 315/2020, que:

121.2.1. apure as causas que geraram a permanência dessas contas ativas de pessoas falecidas no Login Gov.Br, com apoio do Serpro e da RFB, caso necessário; e

121.2.2. adote as medidas necessárias para gerir os riscos de falecidos permanecerem com contas ativas no Login Gov.Br.

121.2.1. Dar ciência à Secretaria Especial da Receita Federal do Brasil (RFB), com fundamento no art. 9º, inciso I, da Resolução-TCU 315, de 2020, que a falha de sincronização entre a base

de dados do Cadastro de Pessoas Físicas (CPF) e o Sistema Nacional de Informações de Registro Civil (Sirc) — evidenciada por defasagens que abrangem registros desde 2020, apesar da previsão de atualização diária —, compromete a fidedignidade da base do CPF para a prestação de serviços e a regular execução de políticas públicas, em decorrência da inobservância dos seguintes dispositivos: Lei 14.129/2021: Art. 3º, inciso XIV; Art. 4º, inciso X; Art. 29, § 1º, inciso III; e Art. 39, inciso II, VI; Decreto 9.929/2019: Art. 2º, incisos I e III; Art. 3º, § 1º, incisos II e VII; e Decreto 10.046/2019: Art. 1º, inciso IV; Art. 16, inciso II; e Art. 18, §§ 4º e 5º.

121.3. Como benefício, espera-se que a adoção da medida identifique e solucione os gargalos técnicos de sincronização entre as bases do Sirc e do CPF, acelere a atualização da situação cadastral de falecidos e reduza a janela de oportunidade para fraudes e usurpação de identidade, garantindo maior qualidade e fidedignidade às bases de dados da Administração Pública e limitando o risco de acesso indevido a serviços sensíveis e de assinatura de documentos em nome de pessoas falecidas.

8 A SEGURANÇA DO ECOSSISTEMA É COMPROMETIDA PELA INCIPIÊNCIA DOS PROCESSOS DE MONITORAMENTO EM TEMPO REAL E PELA OBSOLESCÊNCIA DOS REQUISITOS DE SENHAS

8.1 Falhas na gestão e segurança de senhas

122. A equipe de auditoria identificou que o tamanho da senha é inferior ao recomendado pelas boas práticas de segurança. A política atual da plataforma exige um mínimo de apenas oito caracteres, contrariando referenciais técnicos (NIST SP 800-63B e CIS Controls v8) que recomendam, na ausência de autenticação multifator obrigatória (MFA), senhas mais longas (mínimo de catorze caracteres) para se proteger a ataques modernos. Essa configuração permite a criação de credenciais vulneráveis a ataques de força bruta, facilitando a quebra de sigilo por tentativa e erro (PT3, peça 120, p. 5-6).

123. Constatou-se, ainda, a ausência de processos para identificar senhas vazadas no momento da criação ou da alteração da credencial. Testes de auditoria demonstraram que o sistema permite a definição de senhas presentes em dicionários de vazamentos conhecidos (ex: ‘P@ssword1’), sem emitir alerta ou bloqueio ao usuário. Dada a tendência de reutilização de senhas pelos usuários em múltiplos serviços, essa lacuna gera o risco de utilização de credenciais já expostas em incidentes anteriores (PT3, peça 120, p. 6).

124. A combinação dessas falhas expõe a plataforma à vulnerabilidade contra ataques de uso em massa de credenciais vazadas (credential stuffing), onde fraudadores utilizam listas de usuários e senhas vazadas de outros sites para automatizar o acesso não autorizado. Consequentemente, ocorre o comprometimento facilitado de contas de usuários em caso de vazamento de dados, permitindo que agentes maliciosos assumam a identidade digital dos cidadãos e acessem serviços sem enfrentar barreiras de segurança robustas.

125. A criticidade dessas lacunas na política de senhas é confirmada pelos dados do Microsoft Digital Defense Report 2025, em que a identidade se apresenta como a principal forma de ataque cibernética atual. O relatório aponta que mais de 97% dos ataques de identidade observados globalmente são do tipo password spray (teste de senhas comuns em múltiplas contas) ou força bruta, explorando justamente a fragilidade do fator único de autenticação: a senha. Além disso, análises indicam que 85% dos nomes de usuários alvo dessas ofensivas já constavam em bases de credenciais vazadas, o que torna a ausência de verificação contra dicionários de vazamentos no Gov.br uma vulnerabilidade crítica. Nesse contexto, a baixa adesão ao segundo fator de autenticação (MFA) na plataforma é alarmante, visto que a implementação dessa camada de proteção, segundo o mesmo relatório, bloqueia mais de 99% das tentativas de acesso não autorizado, neutralizando a eficácia de senhas comprometidasxi.

8.2 Falhas no monitoramento

126. A identificação rápida de irregularidades é prejudicada por falhas estruturais no monitoramento da Conta Gov.br. Constatou-se a inexistência de um processo automatizado para a revisão de logs de auditoria, gerando uma dependência de análises manuais ou reativas, muitas vezes iniciadas apenas após provocação externa (ex.: denúncias policiais). Essa abordagem é

incompatível com o atual cenário de ameaças cibernéticas, no qual a velocidade de resposta é determinante. Segundo o Microsoft Digital Defense Report 2025, a defesa cibernética moderna exige o uso de algoritmos avançados de detecção de anomalias (e.g. casos de uso próprios, aprendizado de máquina ou inteligência artificial) para processar trilhões de sinais diários e detectar anomalias comportamentais em tempo real, reduzindo o tempo de permanência (dwell time) dos fraudadores no ambiente da conta da vítima, que hoje é crítico para evitar a roubo ou vazamento de dados e a consolidação de fraudes (QACI 4, peça 121, q. 5-6; PT9, peça 105, p. 9 e 19; Microsoft Digital Defense Report 2025, p. 61).

8.3 Evidências, critérios e causas

127. As evidências que suportam as situações encontradas estão consolidadas no papel de trabalho 'PT03 - QACI 3 - Autenticação' (peça 120) e 'PT04 - QACI 4 - Monitoramento' (peça 121).

128. Os critérios específicos para as deficiências identificadas estão relacionados nos Questionários de Avaliação de Controles Internos (peças 120 e 121).

129. Quanto às possíveis causas que levaram às situações encontradas:

129.1. Falhas na gestão e segurança de senhas: A SGD/MGI justificou a inexistência de processos para identificação de senhas vazadas citando a falta de garantias sobre a confiabilidade, integridade e atualização das bases de dados públicas de senhas de credenciais vazadas. Além disso, destacou que as tais bases não suprem os requisitos institucionais devido à sua dimensão e ao elevado custo operacional e administrativo (peça 91, p. 3, item 18-20). Adicionalmente, segundo os gestores, os requisitos de senhas são adaptados para o contexto brasileiro para não criar barreiras para os cidadãos, especialmente grupos vulneráveis, ou sobrecarregar os canais de atendimento (peça 105, p. 21, itens 217-219); e

129.2. Falhas no monitoramento: a equipe de auditoria não aprofundou as causas, no entanto, os gestores apontaram que há ferramenta em desenvolvimento focada na detecção de fraudes (PT10, peça 106, p. 8, item 47-50).

8.4 Propostas de encaminhamento e benefícios

130. Considerando as recomendações do item 68.1.1, acredita-se que o investimento em inclusão digital e uso seguro do ambiente digital, além do reforço dos controles de verificação em duas etapas, incluindo o uso de autenticação sem senha (mais seguro, menos custoso e com melhor experiência do usuário) são mais adequados, portanto a equipe propõe deixar de recomendar em relação aos requisitos de senha.

131. Para tratar a situação encontrada de inexistência de um processo automatizado para monitoramento de logs, e considerando que: a) o principal vetor de ataque é a identidade, e mais de 97% dos ataques é do tipo password spray ; b) a evolução do cenário de ameaças cibernéticas transformou a identidade no componente central da estratégia de defesa moderna , a AudTI propõe:

131.1. Recomendar à SGD/MGI, com fundamento no art. 11 da Resolução - TCU 315/2020, que:

131.1.1. realize estudos técnicos para identificar as lacunas e deficiências no monitoramento das Contas Gov.br, incluindo monitoramento de módulos de gestão e aprimoramento de deficiências que podem impactar processos formais de comunicação e resposta a incidentes, como falta de rastreabilidade ou impossibilidade de reconstrução de incidentes de segurança;

131.1.2. implante os mecanismos técnicos necessários ao monitoramento das Contas Gov.br; e

131.1.3. oriente e, se necessário, elabore normatização acerca do seu papel e do papel dos gestores dos serviços nas atividades de monitoramento das Contas Gov.br.

131.2. Como benefício, espera-se que a adoção da medida reduza o tempo de detecção e resposta a acessos indevidos, ampliando tanto a capacidade institucional de identificar fraudes em curso quanto a capacidade de o próprio cidadão atuar como linha de defesa ativa contra o roubo de sua identidade digital.

9 BOA PRÁTICA – AUTENTICAÇÃO SEM SENHA (PASSWORDLESS)

132. A SGD/MGI iniciou estudos para adoção de autenticação sem senha. O uso de passkey passou a ser adotado no módulo de gestão da conta Gov.br, que é acessada por servidores da Secretaria e pela equipe da central de atendimento. A Polícia Federal e o Ministério Público Federal, que também usam o módulo de gestão, adotaram o passkey. Essa é uma primeira etapa, que tem por objetivo mapear as principais dificuldades na jornada, visto que a experiência muda de acordo com o sistema operacional e o navegador. A partir dos resultados obtidos, será definida estratégia de expansão para uso de autenticação na conta Gov.br. (peça 144, p. 2, item 8)

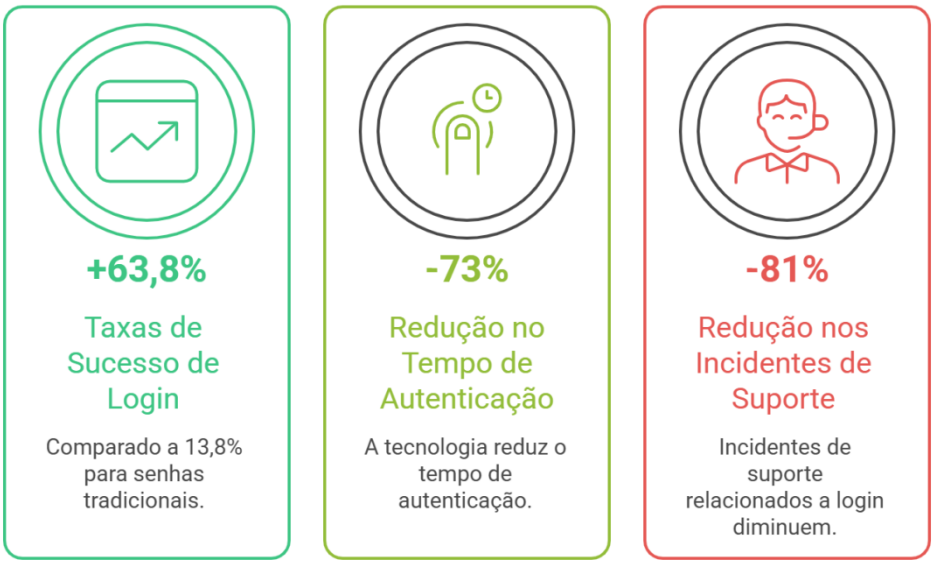
133. A segurança digital fundamentada em senhas apresenta vulnerabilidades, sendo o uso de credenciais comprometidas a forma inicial de ataque em 22% das violações de dados em 2025. O uso de métodos de autenticação multifator (MFA) tradicionais (SMS, E-mail, TOTP) são tecnicamente vulneráveis à interceptação e engenharia social por dependerem de segredos compartilháveis, embora eles reduzam o risco de acessos não autorizados (PT14, peça 110, p. 2, item 1). Por outro lado, o uso de MFA moderno (Passkeys, FIDO2, Biometria) bloqueia 99,9% das tentativas de acesso não autorizado (item 5).

134. A tecnologia FIDO (Fast Identity Online) surge como uma alternativa moderna para substituir as senhas por um sistema de chaves digitais mais seguro e eficiente.

135. Ao contrário dos certificados digitais tradicionais (físicos ou em nuvem), que frequentemente exigem a instalação de softwares externos, drivers ou sistemas complicados para gerenciar as chaves, as passkeys (chaves de acesso) são integradas nativamente aos celulares e computadores atuais. Na prática, o usuário substitui a senha pelo reconhecimento biométrico ou pelo PIN de desbloqueio do próprio aparelho. Esse modelo é mais seguro porque os dados de acesso nunca saem do dispositivo do usuário e não trafegam pela rede, o que impede que fraudadores capturem informações durante o login ou utilizem sites falsos para enganar o cidadão (PT14, peça 110, p. 2, item 4-7).

136. A figura a seguir apresenta graficamente como funciona a tecnologia FIDO e os seus benefícios.

Figura 3: Tecnologia Fido e passkeys sincronizadas: segura e conveniência.



Fonte: Fido Alliance .

137. A democratização dessa tecnologia ocorre por meio das passkeys (chaves de acesso), que integram a segurança FIDO nativamente aos principais celulares e computadores. Elas podem ser 'sincronizadas' em nuvem para maior conveniência do usuário ou 'vinculadas ao dispositivo' (device-bound) para setores de alta segurança que exigem prova de posse física. A eficácia das passkeys é absoluta contra a engenharia social, pois a credencial é vinculada criptograficamente ao endereço oficial do site. Esse modelo impede, por exemplo, que o

navegador apresente uma chave legítima em um site fraudulento, evitando que os usuários caiam em golpes (PT14, peça 110, p. 3, item 8-10).

138. Os impactos operacionais e econômicos da transição para o modelo sem senha são significativos, com taxas de sucesso de login atingindo 63,8% em comparação aos 13,8% das senhas tradicionais. Além de reduzir o tempo de autenticação em até 73%, a tecnologia demonstrou ser capaz de diminuir em 81% os incidentes de suporte relacionados a login. Casos práticos em empresas como Target, Mercado Livre e Aflac confirmam que a intuitividade do método, baseada no simples desbloqueio biométrico do dispositivo, elimina a resistência dos usuários no acesso e reduz os custos de manutenção de TI (PT14, peça 110, p. 4, itens 11-19).

Tabela - Comparação entre métodos de autenticação modernos

Critério	*Passkey* Sincronizada	*Passkey* Presa ao Dispositivo	App Vinculado (Gov.br)	Certificado A3 (Físico)	Certificado A1 (Software)	MFA Tradicional (SMS/OTP)
Mecanismo de Acesso	Biometria nativa ou PIN do dispositivo.	Biometria ou PIN no *hardware* local.	Código exibido no *app* após *login* e clique.	PIN + Conexão de *Token* / *Smartcard* físico.	Senha de acesso ao arquivo do certificado.	Inserção manual de código recebido.
Nível de Segurança	Médio/Elevado: Criptografia ponta a ponta na nuvem.	Crítico/Máximo: Chave privada impossível de exportar.	Médio/Elevado: Vínculo lógico ao smartphone.	Elevado: *Hardware* criptográfico e PIN.	Médio: Arquivo de software protegido por senha.	Básico/Médio: Vulnerável a interceptação.
Facilidade para o Usuário	Muito Alta: Sincroniza entre dispositivos.	Alta: Autenticação em ~8,5s via biometria.	Média: Clique em botão via app. Gov.br no smartphone.	Baixa: Exige drivers e conexão física.	Média: Exige instalação no navegador/SO, pode ser exportado e compartilhado.	Média: Exige troca de *apps* e digitação.
Resistência a *Phishing*	Absoluta: Vínculo técnico ao domínio (RP ID).	Absoluta: Vínculo técnico ao domínio (RP ID).	Média/Alta: Código pode ser compartilhado.	Absoluta.	Média: O arquivo pode ser usado em sites fraudulentos, exportado.	Inexistente: Código pode ser inserido em sites falsos.
Tipo de Vínculo	Lógico/Nuvem (Ecossistema da plataforma).	*Hardware* (Chip TPM ou *Token* Físico).	Lógico (Instalação e ativação no smartphone).	*Hardware* (*Token* USB ou *Smartcard*).	Software (Arquivo instalado no computador/celular).	Lógico (Número de telefone ou aplicativo).
Recuperação de Conta	Facilitada: Via conta da plataforma (Apple/Google).	Rigorosa: Chaves de *backup* ou prova de identidade.	Moderada: Nova ativação biométrica facial no app.	Complexa: Requer nova emissão e validação.	Moderada: Requer nova instalação do arquivo.	Insegura: *Reset* via e-mail ou SMS.

Fonte: Elaborado pela equipe (2026).

139. Portanto, usar a autenticação sem senha (FIDO) no Contas Gov.br amplia a segurança e a usabilidade do sistema mediante um método acessível e de baixo custo. Adicionalmente, a solução diminui a demanda por suporte técnico ao reduzir problemas recorrentes do modelo atual de verificação em duas etapas.

140. O papel de trabalho 'FIDO – autenticação moderna sem senha' (peça 110) apresenta fundamentos técnicos, impactos positivos, estudos de casos de uso e desafios na implementação da tecnologia FIDO.

10 ANÁLISE DOS COMENTÁRIOS DOS GESTORES

141. Este capítulo do relatório de auditoria atende ao disposto nas Normas de Auditoria do TCU, itens 144 a 148. Também atende ao disposto no art. 14 da Resolução - TCU 315, de 2020, no sentido de oportunizar aos destinatários das deliberações a apresentação de comentários

sobre as propostas da equipe de auditoria, solicitando, em prazo compatível, informações quanto às consequências práticas da implementação das medidas aventadas e eventuais alternativas.

142. Dessa forma, a oportunidade de apresentar comentários foi viabilizada mediante o envio do relatório preliminar da fiscalização com as propostas de determinação ou recomendação à SGD/MGI, INSS e Serpro. Adicionalmente, a equipe de auditoria consultou a Controladoria Geral da União (CGU), que também realizou ciclos de fiscalização nas Contas Gov.br em trabalhos anteriores (peças 18-23) e colaborou com o planejamento desta fiscalização.

143. Como resultado, as organizações enviaram documentos contendo comentários sobre as conclusões do trabalho, as propostas de encaminhamento e os papéis de trabalho que sustentam os achados, conforme documentos citados no item 2 do PT17 (peça 147, p. 2, item 2).

144. O PT17 – Análise dos comentários dos gestores aos resultados preliminares (peça 147) contém a consolidação das análises feitas aos comentários dos gestores e os detalhes das mudanças propostas no relatório de auditoria.

145. Em síntese, os comentários sugeriram:

145.1. Aprimoramento dos mecanismos de gestão de senhas e da autenticação da Conta Gov.br (peça 147, p. 4, seção 3, item 12.2);

145.2. Reconhecimento do Sistema Balcão Gov.br como potencial vetor de ataque cibernético (peça 147, p. 4, seção 3, item 12.3);

145.3. Garantia de que a emissão e a recuperação de credenciais ocorram exclusivamente por meios seguros (peça 147, p. 4, seção 3, item 12.5);

145.4. Validação contínua da identidade e do vínculo funcional dos atendentes (peça 147, p. 4, seção 3, item 12.6);

145.5. Implementação de trilhas de auditoria completas para assegurar a rastreabilidade integral das ações (peça 147, p. 4, seção 3, item 12.8);

145.6. Adoção de rastreabilidade ampliada (forward completo) a partir da identificação de endereços de rede suspeitos (peça 147, p. 4, seção 3, item 12.10);

145.7. Revisão das políticas de acesso ao Programa Balcão Gov.br para restringir a atuação de estagiários (peça 147, p. 4, seção 3, item 12.11);

145.8. Instituição de fluxo formal de bloqueio e desbloqueio de credenciais em incidentes cibernéticos (peça 147, p. 4, seção 3, item 12.12);

145.9. Validação obrigatória da localização e do ambiente de acesso em atendimentos do Programa Balcão Gov.br (peça 147, p. 4, seção 3, item 12.13);

145.10. Sugestão de utilização do termo habilidade digital e/ou inclusão digital, em substituição ao termo letramento digital (peça 147, p. 7, seção 6.1);

145.11. Alteração dos cinco títulos dos achados de auditoria (peça 147, p. 7, seção 6.1);

145.12. Remoção da recomendação para implementar autenticação sem senha (peça 147, p. 9, seção 6.2);

145.13. Remoção da recomendação para aprimorar e otimizar a visualização do histórico de acessos da conta (peça 147, p. 7, seção 6.3);

145.14. Revisão textual da recomendação para correção de falhas de monitoramento (peça 147, p. 7, seção 6.4);

145.15. Alteração do direcionamento da determinação relacionada a contas ativas de falecidos (peça 147, p. 11, seção 6.5);

145.16. Revisão textual da recomendação para aprimoramento do processo de validação biométrica (peça 147, p. 13, seção 6.6);

145.17. Revisão da recomendação para implementação de métodos alternativos de verificação em duas etapas (peça 147, p. 14, seção 6.7); e

145.18. Classificação de sigilo para a totalidade do processo ou para os trechos sensíveis do relatório (peça 147, p. 14, seção 6.8).

146. A equipe analisou o conteúdo enviado pelos gestores (peça 147, p. 7-17) e:

146.1. Acolheu totalmente seis comentários: itens 145.10, 145.11, 145.12, 145.13, 145.14 e 145.15; e

146.2. Acolheu parcialmente três comentários: itens 145.16, 145.17 e 145.18;

147. As demais sugestões a equipe de auditoria entendeu que é necessário avaliar em maior profundidade através de procedimentos adicionais de auditoria (itens 145.2, 145.4, 145.5, 145.6, 145.7, 145.8 e 145.9), e outras medidas são endereçadas nas propostas de encaminhamento ou já são adotadas (itens 145.1 e 145.3). Considerando o cronograma da auditoria, não serão realizados procedimentos adicionais. Contudo, recomenda-se que a SGD/MGI avalie a implementação dos controles sugeridos, uma vez que se mostram adequados e o INSS pode apresentar maior familiaridade operacional com a matéria, e, consequentemente, dos riscos, devido à sua atuação relevante no atendimento das Contas Gov.br.

148. Os ajustes previstos na análise dos comentários não alteraram a versão final dos questionários de avaliação (peças 118-121), mas ajustes foram incorporados ao relatório preliminar em recomendações não diretamente relacionadas aos questionários.

11 CONCLUSÃO

149. A conclusão do relatório é:

149.1. Desafios da inclusão digital e baixa habilidade digital pela população, aliados ao uso inadequado de credenciais de acesso induzem à diminuição das exigências de segurança pelos serviços públicos: a baixa inclusão digital da população, somada à baixa maturidade em SI pelos gestores, impõe a redução de requisitos de controle para evitar a exclusão de usuários, fragilizando a proteção dos serviços públicos.

149.2. Dificuldades e falhas no processo de validação biométrica impactam no acesso ao gov.br.: as limitações técnicas na prova de vida biométrica geram barreiras de acesso legítimo e frustração aos usuários, ao passo que a sofisticação de ataques com inteligência artificial explora fragilidades nessa validação. Essa dualidade compromete a disponibilidade do serviço para o cidadão e, simultaneamente, a eficácia do controle na prevenção de fraudes avançadas.

149.3. A inconsistência dos mecanismos de segurança exigidos em cada nível da Conta Gov.br, aliada à baixa adoção, pelos gestores dos serviços públicos, de mecanismos de autenticação mais robustos aumenta o risco de uso indevido das Contas Gov.br dos cidadãos brasileiros: a desconexão entre o nível de confiança cadastral (identificação) e a não de exigência autenticação em duas etapas, somada à baixa exigência e uso dos critérios de segurança pelos serviços, baixo uso de verificação em duas etapas pelos usuários e permanência indefinida de contas em nível elevado de confiabilidade (ouro) , torna os níveis de segurança do Gov.br ineficazes. Tal inconsistência estrutural permite que credenciais privilegiadas sejam exploradas por vetores de ataque básicos, expondo ativos críticos e dados sensíveis a acessos não autorizados.

149.4. Falhas na sincronização de dados entre as bases de registro civil e do CPF podem permitir fraudes no acesso ao Gov.br e em serviços públicos por meio de cadastro de cidadãos falecidos: a persistência de contas ativas de titulares falecidos, decorrente de falhas de sincronização entre bases governamentais, viabiliza a continuidade de acessos indevidos ao Gov.br e a materialização de fraudes com prejuízos aos serviços, às organizações e aos cidadãos.

149.5. Adicionalmente, a segurança do ecossistema é comprometida pela incipiência dos processos de monitoramento e pela obsolescência dos requisitos de senhas.

150. Em resposta às questões de auditoria propostas na matriz de planejamento, tem-se:

150.1. (QST-01: Em que medida as práticas de governança que impactam a gestão de identidade (IdM) estão alinhadas às boas práticas?) As práticas de governança que impactam a gestão de identidade estão alinhadas às boas práticas (peça 118)

150.2. (QST-02: Em que medida o processo de gestão de identidade está alinhado às boas práticas?) O processo de gestão de identidade está alinhado às boas práticas (peça 119);

150.3. (QST-03: Em que medida o processo de autenticação está alinhado às boas práticas?) O processo de autenticação está alinhado às boas práticas (peça 120);

150.4. (QST-04: Em que medida o monitoramento dos processos que envolvem a gestão de identidade (IdM) está alinhado às boas práticas?) O monitoramento dos processos que envolvem a gestão de identidade está parcialmente alinhado às boas práticas (peça 121);

150.5. (QST-05: Há diretrizes, alinhadas às boas práticas, para orientar os gestores sobre integração e uso seguro do Conta Gov.br?) Existem diretrizes, porém não estão plenamente alinhadas às boas práticas, apresentando falhas críticas nos exemplos técnicos de integração (como uso de parâmetros estáticos e ausência de validação de tokens) e inconsistências entre as orientações de segurança e os formulários operacionais, além de carência de ferramentas objetivas para a análise de riscos (peça 111);

150.6. (QST-06: Há iniciativas efetivas para proteger os cidadão e grupos vulneráveis, considerando o aspecto humano e cultural, contra o roubo de credenciais no âmbito da plataforma Gov.br?) Existem iniciativas estruturadas, como o Balcão Gov.br e melhorias de acessibilidade, mas sua efetividade é mitigada por barreiras técnicas (falhas na biometria), cobertura presencial geograficamente desigual e pela decisão estratégica de flexibilizar requisitos de segurança (como a não obrigatoriedade do MFA) para evitar a exclusão digital (peça 114);

150.7. (QST-07: Em que medida a autorização aos serviços é fornecida com base nos riscos?) A autorização não é fornecida com base nos riscos na maioria dos casos, visto que 64% dos serviços exigem apenas o nível mínimo (Bronze) e somente 1% demanda duplo fator de autenticação, permitindo que serviços críticos (como aquisição de armas e benefícios sociais) operem com requisitos de segurança insuficientes (peça 115);

150.8. (QST-08: Em que medida as organizações promovem a integração e uso seguro do Conta Gov.br?) A promoção do uso seguro é baixa, pois as organizações tendem a priorizar a disponibilidade do serviço em detrimento da segurança para evitar o colapso de canais de atendimento, resultando na subutilização dos controles disponíveis (níveis Prata/Ouro e MFA) e na falta de preenchimento dos requisitos de segurança no catálogo de serviços. (peça 115);

151. Desta forma, conclui-se que o objetivo dessa auditoria foi alcançado, ao passo que serão propostos encaminhamentos para endereçar as deficiências identificadas nos achados.

152. Considerando o interesse público e a ausência de elementos que justifiquem a restrição de acesso nos termos do art. 23 da Lei 12.527/2011, propõe-se a classificação como público para este processo. Tal classificação estende-se ao presente relatório da unidade técnica, ao voto e à decisão proferida, assegurando o pleno acesso à informação, conforme a Resolução-TCU 294/2018, ressalvando-se as peças sigilosas especificadas na proposta de encaminhamento (Capítulo 12).

153. Quanto aos benefícios do controle, espera-se que a implementação das medidas propostas promova um salto qualitativo na segurança e na inclusão da Plataforma Gov.br, assegurando que a modernização tecnológica caminhe em conjunto com a proteção efetiva do cidadão. Ao atacar as causas raízes — desde a fragilidade das senhas até a baixa inclusão digital —, o Estado brasileiro fortalece a confiança nas instituições digitais, mitiga vulnerabilidades críticas e consolida as bases para uma transformação digital resiliente, capaz de prevenir prejuízos e assegurar o exercício pleno da cidadania em ambiente virtual.

12 PROPOSTA DE ENCAMINHAMENTO

154. Ante o exposto, submete-se o presente relatório à consideração superior com as seguintes propostas.

155. Determinar à Secretaria de Governo Digital do Ministério da Gestão e da Inovação em Serviços Públicos (SGD/MGI), com fundamento no art. 4º, inciso I, da Resolução - TCU 315/2020, que, no prazo de 180 dias:

155.1. implemente controles lógicos para assegurar o alinhamento entre nível de identificação da Conta Gov.br e os métodos de autenticação definidos na Portaria - SGD/MGI 11.229/2025; e

155.2. avalie as contas constantes da planilha ‘Contas ativas.csv’ (item não digitalizável da peça 108) cujos titulares encontravam-se ativos no Login Gov.Br em 29/1/2026 e simultaneamente na situação de falecidos na base do SIRC, para fins de inativação dessas contas, se for o caso;

156. Recomendar à Secretaria de Governo Digital do Ministério da Gestão e da Inovação em Serviços Públicos (SGD/MGI), com fundamento no art. 11 da Resolução TCU 315/2020, que:

156.1. apure as causas que geraram a permanência dessas contas ativas de pessoas falecidas no Login Gov.Br, com apoio do Serpro e da RFB, caso necessário;

156.2. adote medidas necessárias para gerir os riscos de falecidos permanecerem com contas ativas no Login Gov.Br;

156.3. realize estudo de viabilidade e de riscos para a disponibilização de SMS, e-mail ou aplicativos MFA como métodos alternativos de Autenticação de Múltiplos Fatores (MFA), mas nunca como único fator de recuperação das contas, para oferecer opções de autenticação mais segura para usuários no nível bronze;

156.4. adote as medidas necessárias para:

156.4.1. promover o aprimoramento tecnológico, operacional e de segurança das soluções de biometria facial e prova de vida (liveness) do ecossistema Gov.br, de forma a:

156.4.1.1. assegurar que os níveis de desempenho de segurança e acurácia sejam compatíveis com padrões de boas práticas internacionalmente reconhecidos (NIST SP 63A 3.11 Rev. 4 e ISO/IEC 30107-3:2023);

156.4.1.2. identificar e mitigar eventuais disparidades de desempenho para grupos demográficos específicos; e

156.4.1.3. atualizar periodicamente as bases de validação sob controle da SGD/MGI.

156.4.2. instituir ciclos de validade e revalidação periódica para os selos de identidade obtidos via reconhecimento facial e Carteira de Identidade Nacional, alinhando a gestão do ciclo de vida das credenciais às boas práticas internacionais de gestão de identidade digital;

156.4.3. aprimorar, consolidar e alinhar as diretrizes de segurança e manuais de integração dos serviços ao Login Gov.br (Login Único).

156.5. realize estudos técnicos para identificar as lacunas e deficiências no monitoramento das Contas Gov.br, incluindo monitoramento de módulos de gestão e aprimoramento de deficiências que podem impactar processos formais de comunicação e resposta a incidentes, como falta de rastreabilidade ou impossibilidade de reconstrução de incidentes de segurança;

156.6. implante os mecanismos técnicos necessários ao monitoramento das Contas Gov.br; e

156.7. oriente e, se necessário, elabore normatização acerca do seu papel e do papel dos gestores dos serviços nas atividades de monitoramento das Contas Gov.br.

157. Dar ciência às unidades jurisdicionadas do TCU e gestoras de serviços integrados à plataforma Gov.br listadas no Apêndice F deste relatório, com fundamento no art. 9º, inciso I, da Resolução-TCU 315, de 2020, de que a definição dos níveis de confiabilidade das contas (Bronze, Prata ou Ouro) e dos métodos de acesso sem a prévia realização de avaliação de risco, especialmente para serviços classificados como críticos ou sensíveis, expõe a Administração Pública a incidentes de segurança e descumpre o dever de proteção de dados dos cidadãos, em decorrência da inobservância dos seguintes dispositivos: Lei 13.709/2018: Art. 50, § 2º, inciso I, d); e Portaria SGD/MGI 11.229/2025: Art. 7º, incisos I e II.

158. Dar ciência à Secretaria Especial da Receita Federal do Brasil (RFB), com fundamento no art. 9º, inciso I, da Resolução-TCU 315, de 2020, que a falha de sincronização entre a base de dados do Cadastro de Pessoas Físicas (CPF) e o Sistema Nacional de Informações de Registro Civil (Sirc) — evidenciada por defasagens que abrangem registros desde 2020, apesar da previsão de atualização diária —, compromete a fidedignidade da base do CPF para a prestação de serviços e a regular execução de políticas públicas, em decorrência da inobservância dos seguintes dispositivos: Lei 14.129/2021: Art. 3º, inciso XIV; Art. 4º, inciso X; Art. 29, § 1º, inciso III; e Art. 39, inciso II, VI; Decreto 9.929/2019: Art. 2º, incisos I e III; Art. 3º, § 1º, incisos II e VII; e Decreto 10.046/2019: Art. 1º, inciso IV; Art. 16, inciso II; e Art. 18, §§ 4º e 5º.

159. Classificar como sigiloso em grau reservado, com fulcro no art. 23, VII, da Lei 12.527/2011 e nos arts. 8º, § 3º, inciso I e 9º, inciso VII, ambos da Resolução-TCU 294/2018, o seguinte:

159.1. as peças 18-23, 29-31, 41, 56, 68, 78-79, 91, 102-104, enviadas pelos auditados, referendando a classificação dada pelo auditado; e

159.2. as peças 34, 66, 75-77, 81, 84, 87, 105-109, 112, 118-121, contendo as análises que evidenciam o descrito neste relatório.

160. Nos termos do art. 8º da Resolução-TCU 315, de 2020, fazer constar, na ata da sessão em que estes autos forem apreciados, comunicação do relator ao colegiado no sentido de autorizar o monitoramento das recomendações propostas neste relatório.

161. Nos termos do art. 8º da Resolução-TCU 315, de 2020, fazer constar, na ata da sessão em que estes autos forem apreciados, comunicação do relator ao colegiado no sentido de encaminhar cópia do relatório para a Unidade de Auditoria Especializada em Comunicações (AudComunicações) para embasar o acompanhamento do desenvolvimento do Plano Nacional de Inclusão Digital (PNID) no que se refere ao quesito acesso seguro ao ambiente digital, nos termos do Acórdão 1.699/2025–TCU-Plenário, Rel. Min. Aroldo Cedraz.

162. Informar à Secretaria de Governo Digital do Ministério da Gestão e da Inovação em Serviços Públicos (SGD/MGI), à Secretaria Especial da Receita Federal do Brasil (RFB) à Controladoria-Geral da União (CGU) e às unidades jurisdicionadas do TCU e gestoras de serviços integrados à plataforma Gov.br listadas no Apêndice F deste relatório sobre o acórdão que vier a ser proferido, destacando que o relatório e o voto que fundamentam a deliberação ora encaminhada podem ser acessados por meio do endereço eletrônico www.tcu.gov.br/acordaos.

163. Arquivar o presente processo, com base no art. 169, inciso V, do Regimento Interno do TCU."

É o relatório.

VOTO

Em exame, auditoria realizada para avaliar a maturidade, a segurança e a efetividade dos processos de gestão de identidade da Conta Gov.br, sistema central de identificação e autenticação para acesso aos serviços públicos digitais federais.

2. A finalidade da Conta Gov.br – que oferece mais de 4,6 mil serviços digitais federais ao cidadão e chega a 173 milhões de usuários – é assegurar a identificação confiável dos usuários no ambiente digital, permitindo que cidadãos, empresas e demais interessados acessem serviços públicos sem a necessidade de múltiplos cadastros ou comparecimentos presenciais, tais como serviços previdenciários, trabalhistas, educacionais e de saúde, realização de prova de vida digital, documentos eletrônicos e assinatura eletrônica com validade jurídica.

3. A plataforma opera sob o conceito de login único, por meio do qual uma única credencial permite acesso a diferentes sistemas governamentais. Esse modelo reduz custos administrativos, simplifica a experiência do usuário, amplia a interoperabilidade entre órgãos públicos e fortalece a segurança das transações eletrônicas.

4. Para garantir níveis adequados de segurança, a conta Gov.br adota uma estrutura de graduação de confiabilidade baseada em três níveis: Bronze, Prata e Ouro, definidos a partir de regulamentações e normas técnicas editadas pela Secretaria de Governo Digital do Ministério da Gestão e da Inovação em Serviços Públicos (SGD/MGI). Essa classificação busca compatibilizar o grau de certeza sobre a identidade do usuário com o risco e a sensibilidade do serviço acessado.

5. O nível Bronze é o grau básico de confiabilidade, obtido mediante validações cadastrais em bases governamentais e autenticação simples. O nível Prata exige formas adicionais de verificação, como reconhecimento facial ou validação por instituições credenciadas, proporcionando maior segurança. O nível Ouro tem o mais elevado grau de confiabilidade, podendo ser obtido mediante certificado digital da ICP-Brasil ou validações biométricas mais robustas em bases governamentais, sendo exigido para determinados serviços de maior sensibilidade ou impacto jurídico.

6. Além da autenticação, a conta Gov.br possibilita que cidadãos assinem documentos em ambiente digital com respaldo jurídico, funcionalidade que contribui para a eliminação de procedimentos presenciais, redução do uso de papel e maior eficiência na tramitação de processos administrativos.

7. A operacionalização da conta Gov.br envolve diversos órgãos e entidades. A coordenação estratégica é exercida pelo Ministério da Gestão e da Inovação em Serviços Públicos, por intermédio da SGD/MGI, responsável pela gestão da plataforma e pela definição das políticas de identidade digital do Governo Federal. O Serviço Federal de Processamento de Dados (Serpro) garante a infraestrutura tecnológica e o processamento dos serviços digitais. A Receita Federal do Brasil participa por meio da utilização do CPF como identificador único do cidadão, enquanto os institutos de identificação dos estados colaboram na validação biométrica e na integração com a Carteira de Identidade Nacional (CIN). Também participam instituições financeiras e outros provedores de identidade credenciados que auxiliam nos procedimentos de validação necessários para a elevação dos níveis de confiabilidade das contas.

8. A conta Gov.br é parte da estratégia de modernização dos sistemas de identificação civil do País, especialmente à implementação da Carteira de Identidade Nacional (CIN), que utiliza o CPF como número único de identificação. Essa integração fortalece os mecanismos de autenticação digital, reduz fraudes cadastrais e contribui para a construção de um ecossistema unificado de identidade digital para os cidadãos brasileiros.

9. A principal fundamentação jurídica da conta Gov.br encontra-se na Lei 14.129/2021 (Lei do Governo Digital), que estabelece princípios, regras e instrumentos para a digitalização dos serviços públicos e para a disponibilização de uma plataforma integrada de acesso à Administração Pública. A operacionalização da plataforma também observa as disposições da Lei 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), bem como da Lei 14.063/2020, que disciplina o uso de assinaturas eletrônicas nas interações com entes públicos.

II

10. Na presente auditoria, foram examinados os controles administrativos e técnicos relacionados à política de gestão de identidade, gestão de riscos, identificação, autenticação, monitoramento e integração dos serviços públicos à plataforma Gov.br, utilizando como critérios os parâmetros do National Institute of Standards and Technology (NIST)[1], CIS Controls[2], ISO/IEC 27002:2022[3] e o Programa de Auditoria de Gerenciamento de Identidade e Acesso da ISACA[4].

11. A equipe de auditoria identificou cinco achados estruturais, fundamentados em evidências técnicas e normativas, que revelam algumas fragilidades no ecossistema de identidade digital federal.

12. Esses achados derivam de análises relacionadas às questões de auditoria[5]. Inicialmente, procurou-se avaliar se há diretrizes alinhadas às boas práticas para orientar os gestores sobre integração e uso seguro do login Gov.br. Em segundo lugar, foi avaliado se há iniciativas para proteger os cidadãos e os grupos vulneráveis, considerando o aspecto humano e cultural contra o roubo de credenciais no âmbito da plataforma Gov.br. A terceira questão investigou em que medida a autorização aos serviços é fornecida com base em riscos e, por último, em que medida as organizações promovem a integração e uso seguro do login Gov.br.

13. Feitas as considerações iniciais, exponho, de forma sintética e sistematizada, com vistas a facilitar a compreensão das questões examinadas, os achados de auditoria e as respectivas propostas de encaminhamento formulados pela Secretaria de Controle Externo de Tecnologia da Informação (AudTI).

1. Desafios de inclusão digital e uso inadequado de credenciais

14. Constatou-se que a baixa inclusão digital da população brasileira – caracterizada por limitações de acesso à internet, baixa escolaridade digital e reduzida familiaridade com práticas básicas de segurança – induz ao uso inadequado de credenciais, como senhas fracas, reutilização de credenciais e compartilhamento indevido, além de maior exposição a golpes cibernéticos. Foram identificadas falhas na efetividade e no alcance das campanhas informativas realizadas pela SGD/MGI, bem como a ausência de direcionamento às necessidades de grupos mais vulneráveis. Ademais, verificou-se que a comunicação sobre orientações de segurança disponíveis no portal Gov.br é inadequada, e dificulta o acesso do cidadão comum às informações de proteção.

15. As iniciativas estatais de inclusão digital e segurança da informação carecem de estruturação dentro de um plano ou estratégia consolidados, com ações fragmentadas entre os diversos órgãos e entidades, além de falhas de governança. Esse contexto é agravado pela ausência de métricas para avaliar a eficácia, eficiência e efetividade das ações, o que inviabiliza a mensuração de seu impacto frente à vulnerabilidade da população a ameaças cibernéticas.

---

[1] Agência governamental dos Estados Unidos que cria padrões de tecnologia, regras de medição e guias de cibersegurança.
[2] Os Controles Críticos de Segurança do CIS (CIS Controls) são um conjunto de recomendações elaboradas por meio de um processo de consenso comunitário por milhares de profissionais de cibersegurança ao redor do mundo para que o usuário fortaleça sua atitude de cibersegurança.
[3] Norma internacional com orientações para organizações que buscam estabelecer, implementar e melhorar um Sistema de Gestão de Segurança da Informação (SGSI) focado em cibersegurança, sobretudo controle de acesso, criptografia, segurança de recursos humanos e resposta a incidentes.
[4] A ISACA é uma associação profissional global, sem fins lucrativos, dedicada ao avanço da confiança digital.
[5] Peça 117.

16. A baixa conscientização em segurança da informação reflete-se, também, na proteção insuficiente das identidades digitais dos cidadãos, com baixa adesão à "Verificação em Duas Etapas", exigida por apenas 1% dos serviços integrados à plataforma Gov.br.

17. Apesar de iniciativas recentes da SGD/MGI terem impulsionado a adesão, alcançando 50 milhões de usuários em fevereiro de 2026 (29% do total de 173 milhões de usuários da plataforma), a funcionalidade apresenta limitações, como vulnerabilidade a ataques de *phishing* mediante vazamento do código de verificação por meio de engenharia social[6].

18. Conclui-se que, embora haja avanços, persistem desafios na conscientização e na implementação de mecanismos mais robustos para mitigar riscos de acesso indevido.

19. A ausência de iniciativas massivas e direcionadas, especialmente para grupos vulneráveis, como idosos e pessoas com baixa habilidade digital, contribui para a exposição do cidadão ao risco de uso inseguro do ambiente digital.

20. Essa realidade pressiona gestores públicos a reduzirem exigências de segurança para evitar exclusão de usuários, resultando em serviços que aceitam níveis mínimos de autenticação, mesmo quando tratam dados sensíveis, com vulnerabilidades que se propagam por todo o ecossistema Gov.br.

21. A equipe de auditoria propõe, portanto, recomendar à SGD/MGI, que "realize estudos de viabilidade e de riscos para a disponibilização de SMS, e-mail ou aplicativos de MFA como métodos alternativos de Autenticação de Múltiplos Fatores (MFA), mas nunca como único fator de recuperação das contas, para oferecer opções de autenticação mais segura para usuários no nível bronze".

22. A proposta de ampliar os métodos alternativos de autenticação de múltiplos fatores pode representar avanços significativos para a segurança da conta digital. No entanto, e-mail e SMS são ferramentas vulneráveis a ataques de engenharia social, frequentemente utilizados por agentes mal-intencionados para enganar usuários e obter informações sensíveis, como credenciais de acesso ou outras informações pessoais.

23. Assim, considero que a recomendação deve contemplar a realização de estudos de viabilidade e riscos para a implementação de métodos alternativos e seguros de autenticação multifatores priorizando tecnologias modernas e resistentes a ataques de engenharia social.

2. Falhas e dificuldades na validação biométrica

24. A auditoria constatou que o mecanismo de validação facial apresenta instabilidades relevantes na etapa de verificação de vivacidade (*liveness*), decorrentes de limitações de iluminação, baixa qualidade de câmeras e dificuldades de posicionamento do usuário.

25. Tais fatores elevam a taxa de rejeição de usuários legítimos, especialmente aqueles com menor habilidade digital, e validações falsas decorrentes de ataques sofisticados com uso de inteligência artificial, que exploram fragilidades na validação biométrica.

26. A MFA também está restrita ao dispositivo móvel do usuário, criando vulnerabilidade estrutural: perda, roubo ou dano do aparelho impede o acesso ao segundo fator de autenticação. A recuperação da conta exige frequentemente nova validação facial – justamente o procedimento sujeito a falhas técnicas. Esse ciclo vicioso leva usuários a desativarem a verificação em mais de um etapa para evitar bloqueios, o que reduz o nível de segurança das contas e amplia a exposição a fraudes sofisticadas, inclusive por meio de *deepfakes*.

27. Essas falhas frustram o usuário, sobrecarregam os canais de atendimento e acabam por reduzir o nível de segurança das contas.

---

[6] É a arte de manipular psicologicamente as pessoas para que elas tomem ações ou revelem informações confidenciais. Em vez de explorar falhas em *softwares* ou *firewalls*, o atacante explora falhas no comportamento humano – como confiança, medo, urgência ou vontade de ajudar.

28. O processo de validação biométrica facial do Gov.br apresenta, portanto, um desequilíbrio entre usabilidade e segurança.

29. Além disso, a combinação entre falhas técnicas e ataques avançados compromete simultaneamente a disponibilidade do serviço para acessos legítimos e a eficácia dos controles para impedir fraudes e gera sobrecarga dos canais de atendimento, que não conseguem absorver a demanda reprimida gerada por falhas recorrentes no processo de autenticação.

30. Identificou-se, também, que a fragmentação e a desatualização das bases de dados governamentais utilizadas para validação biométrica, como a Identificação Civil Nacional, a Carteira Nacional de Habilitação (CNH) e a Carteira de Identificação Nacional (CIN), comprometem a eficácia do processo.

31. A base da CNH, por exemplo, apresenta um ciclo de atualização de dez anos, o que resulta em imagens históricas de baixa resolução, dificultando a comparação com a foto atual do cidadão. Além disso, a ausência de integração com bases de dados de cidadãos residentes no exterior reduz a cobertura do serviço, forçando a adoção de fluxos alternativos menos seguros ou mais burocráticos.

32. Gestores de serviços críticos, como o INSS, têm adiado a obrigatoriedade da validação biométrica nas etapas iniciais de acesso para mitigar o risco de exclusão digital. A medida visa evitar a sobrecarga dos canais de atendimento presencial, considerando que muitos segurados enfrentam dificuldades para superar as barreiras de usabilidade da ferramenta de reconhecimento facial atualmente disponível.

33. Com relação a esse achado, a equipe de auditoria propõe:

> "81.1. Recomendar à SGD/MGI (...) que adote as medidas necessárias para promover o aprimoramento tecnológico, operacional e de segurança das soluções de biometria facial e prova de vida (liveness) do ecossistema Gov.br, de forma a:
>
> 81.1.1. assegurar que os níveis de desempenho de segurança e acurácia sejam compatíveis com padrões de boas práticas internacionalmente reconhecidos (NIST SP 63A 3.11 Rev. 4 e ISO/IEC 30107-3:2023);
>
> 81.1.2. identificar e mitigar eventuais disparidades de desempenho para grupos demográficos específicos; e
>
> 81.1.3. atualizar periodicamente as bases de validação sob controle da SGD/MGI."

34. A recomendação de aprimorar a validação biométrica me parece adequada e alinhada com boas práticas. A proposta não aborda, contudo, como será garantida a inclusão de grupos com dispositivos de baixa qualidade ou residentes em áreas com infraestrutura limitada. Assim, entendo que as recomendações dos itens 81.1.2 e 81.1.3 devem ter o seguinte teor:

- identificar e mitigar eventuais disparidades de desempenho para grupos demográficos específicos, incluindo aqueles que utilizam dispositivos de baixa qualidade ou residem em áreas com infraestrutura limitada;
- atualizar periodicamente as bases de validação sob controle da SGD/MGI, garantindo que sejam inclusivas e representativas da diversidade populacional brasileira.

35. Como benefício, espera-se que essas ações promovam maior equidade no acesso aos serviços digitais, reduzam as barreiras tecnológicas enfrentadas por grupos vulneráveis e fortaleçam a segurança e a confiabilidade do ecossistema Gov.br.

3. Inconsistência dos mecanismos de segurança entre níveis de segurança da Conta Gov.br

36. A auditoria pontuou que o nível de confiabilidade cadastral (Bronze, Prata, Ouro) não se traduz em níveis equivalentes de segurança operacional. Contas classificadas como nível Ouro – que conferem elevado grau de confiança na identidade do usuário e permitem acesso a serviços sensíveis –

podem ser acessadas mediante simples combinação de CPF e senha, correspondente ao nível mais baixo de segurança.

37. Tal configuração possibilita que o comprometimento de uma única senha conceda a terceiros privilégios indevidos de acesso, situação agravada pela ausência de obrigatoriedade imediata da MFA, cuja exigência somente será implementada com a entrada em vigor da Portaria SGD/MGI 11.229/2025, em 30/11/2026.

38. Além disso, serviços de alta criticidade vêm sendo disponibilizados com exigência de segurança mínima, incompatível com o risco associado. Serviços sensíveis relacionados à segurança pública, seguridade social, finanças e transportes – tais como autorização para aquisição de armas, saque de FGTS, solicitação de benefícios previdenciários e transferência de propriedade de veículos – admitem acesso apenas com CPF e senha. A equipe de auditoria reporta que a análise do catálogo de serviços revelou que 64% dos serviços que requerem autenticação exigem apenas nível Bronze, enquanto somente 2% demandam nível Ouro.

39. A adoção de MFA é residual, presente em apenas 1% dos serviços, concentrados em poucas organizações. Testes substantivos demonstraram falhas de implementação, permitindo acesso com conta Bronze em serviços que declaravam exigir níveis superiores, fato que evidencia deficiência na validação dos atributos de segurança. Constatou-se, ainda, que a baixa exigência decorre da ausência de metodologia estruturada de análise de riscos e da priorização da disponibilidade em detrimento da segurança, o que amplia a superfície de ataque para fraudadores.

40. Identificou-se, ainda, que a fragmentação de diretrizes e deficiências nas orientações de integração resultam na adoção de controles técnicos sem fundamentação adequada, com ausência de formalidade metodológica e análise prévia de riscos na gestão de identidades. Essa incoerência entre o nível de risco aceito pelas organizações e as configurações implementadas expõe os serviços digitais governamentais a vulnerabilidades.

41. A equipe de auditoria identificou, ainda, que os selos de nível Ouro, obtidos por reconhecimento facial, não têm rotina de revalidação periódica definida. Diferentemente dos selos Prata, que expiram após 36 meses, e dos certificados digitais, que passam por verificação diária de revogação, o *status* Ouro é mantido indefinidamente após sua obtenção, sem necessidade de renovação da prova de vida ou confirmação da posse do documento.

42. Conclui-se, portanto, que o modelo de identidade digital do Gov.br apresenta fragilidades estruturais significativas, caracterizadas pelo desalinhamento entre confiabilidade e segurança, pela disponibilização de serviços críticos com requisitos insuficientes de autenticação e pela fragmentação das diretrizes técnicas que orientam a integração dos serviços. Tais deficiências ampliam riscos operacionais e de segurança, favorecem fraudes e comprometem a proteção de ativos sensíveis da Administração Pública, impondo a necessidade de revisão normativa, padronização técnica e fortalecimento dos mecanismos de autenticação e revalidação.

43. Com relação a esse achado, a equipe de auditoria propôs:

> **"102.1. Recomendar** à SGD/MGI (...) que adote as medidas necessárias para:
>
> 102.1.1. instituir ciclos de validação e revalidação periódica para os selos de identidade obtidos via reconhecimento facial e Carteira de Identidade Nacional, alinhando a gestão do ciclo de vida das credenciais às boas práticas internacionais de gestão de identidade digital.
>
> **102.2. Determinar** à SGD/MGI (...) que, no prazo de 180 dias:
>
> 102.2.1. implemente controles lógicos para assegurar o alinhamento entre nível de identificação da Conta Gov.br e os métodos de autenticação definidos na Portaria - SGD/MGI 11.229/2025;

103.1. Recomendar à SGD/MGI (...) que adote as medidas necessárias para aprimorar, consolidar e alinhar as diretrizes de segurança e manuais de integração dos serviços ao Login Gov.br (Login Único).

(...)

104.1. Dar ciência às unidades jurisdicionadas do TCU e gestoras de serviços integrados à plataforma Gov.br (...) de que a definição dos níveis de confiabilidade das contas (Bronze, Prata ou Ouro) e dos métodos de acesso sem a prévia realização de avaliação de risco, especialmente para serviços classificados como críticos ou sensíveis, expõe a Administração Pública a incidentes de segurança e descumpre o dever de proteção de dados dos cidadãos, em decorrência da inobservância dos seguintes dispositivos: Lei 13.709/2018: Art. 50, § 2º, inciso I, d); e Portaria - SGD/MGI 11.229/2025: Art. 7º, incisos I e II.

44. À vista do exposto, concordo com as propostas de recomendação formuladas nos autos, considerando que estão devidamente fundamentadas e alinhadas às disposições normativas aplicáveis. Entendo, contudo, que a proposta de determinação constante do item 102.2 deve ser reclassificada como recomendação, por se revestir a medida sugerida de caráter orientativo e visar ao aprimoramento da gestão pública, sem impor obrigação de cumprimento imediato, em conformidade com o disposto no art. 11 da Resolução 315/2020.

4. Falhas na sincronização entre bases de registro civil e CPF

45. A equipe de auditoria também identificou inconsistências entre bases de registro civil e CPF que permitem a manutenção de contas ativas de titulares falecidos, criação de contas fraudulentas após o óbito e acessos indevidos a serviços públicos.

46. A demora na inativação dessas contas decorre de falhas de integração/sincronização atrasada com base de registro civil, ausência de processos automatizados e inconsistências cadastrais.

47. A falta de sincronização entre bases governamentais, no entender da equipe de auditoria, pode criar brechas estruturais para fraudes, comprometendo a confiança do cidadão e a integridade dos serviços públicos.

48. Diante disso, a equipe de auditoria propõe:

"119.1. Determinar à SGD/MGI (...) que, no prazo de 180 dias:

119.1.1. avalie as contas constantes da planilha "Contas ativas.csv" (...) cujos titulares encontravam-se ativos no Login Gov.Br em 29/1/2026 e simultaneamente na situação de falecidos na base do SIRC, para fins de inativação dessas contas, se for o caso.

119.2. Recomendar à SGD/MGI (...) que:

119.2.1. apure as causas que geraram a permanência dessas contas ativas de pessoas falecidas no Login Gov.Br, com apoio do Serpro e da RFB, caso necessário; e

119.2.2. adote as medidas necessárias para gerir os riscos de falecidos permanecerem com contas ativas no Login Gov.Br.

119.2.1. Dar ciência à Secretaria Especial da Receita Federal do Brasil (...) que a falha de sincronização entre a base de dados do Cadastro de Pessoas Físicas (CPF) e o Sistema Nacional de Informações de Registro Civil (Sirc) – evidenciada por defasagens que abrangem registros desde 2020, apesar da previsão de atualização diária –, compromete a fidedignidade da base do CPF para a prestação de serviços e a regular execução de políticas públicas, em decorrência da inobservância dos seguintes dispositivos: Lei 14.129/2021: Art. 3º, inciso XIV; Art. 4º, inciso X; Art. 29, § 1º, inciso III; e Art. 39, inciso II, VI; Decreto 9.929/2019: Art. 2º, incisos I e III; Art. 3º, § 1º, incisos II e VII; e Decreto 10.046/2019: Art. 1º, inciso IV; Art. 16, inciso II; e Art. 18, §§ 4º e 5º."

49. Divirjo, neste ponto, dos encaminhamentos propostos, ao menos por ora. A análise de fontes oficiais revela que diversos serviços públicos permanecem dependentes do CPF do falecido, seja para acesso, cancelamento, transferência, regularização ou encerramento das obrigações.

50. A Receita Federal do Brasil, por exemplo, exige o CPF do falecido para que o inventariante ou sucessor possa ter acesso serviços digitais em nome da pessoa morta, tais como regularização de pendências tributárias, acesso ao eSocial, e a abertura de processos digitais. Ainda que o acesso à conta de pessoa falecida seja feito por meio de procuração digital, esta é sempre vinculada ao CPF do falecido.

51. Por essa razão, entendo que esse achado deve ser mais explorado e amadurecido antes de que se mostre apropriado formular algum encaminhamento para o auditado.

5. Monitoramento insuficiente e requisitos de senha obsoletos

52. Atualmente, a política de senhas exige um mínimo de apenas oito caracteres, contrariando boas práticas de segurança, que recomendam senhas mais longas (mínimo de 14 caracteres) na ausência de MFA.

53. Essa configuração permite a criação de credenciais vulneráveis a ataques de força bruta e *password spray*[7]. Além disso, não há processos para identificar senhas vazadas no momento da criação ou alteração, o que possibilita o uso de credenciais já expostas em incidentes anteriores, como "P@ssword1". Essa lacuna aumenta o risco de ataques de "credenciais vazadas"[8], compromete contas de usuários e facilita o acesso não autorizado a serviços digitais.

54. A baixa adesão ao MFA agrava o problema, uma vez que esse mecanismo bloqueia mais de 99% das tentativas de acesso não autorizado[9]. A ausência dessa camada de proteção deixa a plataforma mais suscetível a ataques baseados na fragilidade do fator único de autenticação.

55. Adicionalmente, foram constatadas falhas estruturais no monitoramento da Conta Gov.br. Não há processos automatizados para revisão de logs de auditoria, o que gera dependência de análises manuais ou reativas, frequentemente iniciadas apenas após denúncias externas. Essa abordagem é incompatível com o cenário atual de ameaças cibernéticas, que exige o uso de algoritmos avançados de detecção de anomalias, como aprendizado de máquina, para identificar irregularidades em tempo real e reduzir o tempo de permanência de fraudadores no ambiente da conta.

56. Essas vulnerabilidades comprometem a segurança das identidades digitais dos cidadãos e a integridade dos serviços digitais governamentais, demandam ações urgentes para fortalecer a política de senhas, como ampliar a adoção do MFA, e requerem a implementação de monitoramento automatizado e proativo.

57. Acerca desse achado, a equipe de auditoria propõe:

> 131.1. Recomendar à SGD/MGI (...) que:
>
> 131.1.1. realize estudos técnicos para identificar as lacunas e deficiências no monitoramento das Contas Gov.br, incluindo monitoramento de módulos de gestão e aprimoramento de deficiências que podem impactar processos formais de comunicação e resposta a incidentes, como falta de rastreabilidade ou impossibilidade de reconstrução de incidentes de segurança;
>
> 131.1.2. implante os mecanismos técnicos necessários ao monitoramento das Contas Gov.br; e

[7] No jargão da cibersegurança, *password spray* é um tipo de ataque de força bruta, mas com uma estratégia bem específica e silenciosa. Enquanto o ataque tradicional tenta muitas senhas diferentes contra uma única conta (o que a bloqueia rapidamente), o *password spray* faz exatamente o oposto: ele testa poucas senhas comuns (geralmente 1 ou 2) contra contas de muitos usuários.

[8] No universo da cibersegurança, credenciais vazadas são combinações de usuário (login/e-mail) e senha (ou chaves de API, *tokens* de autenticação e certificados digitais) que foram expostas, roubadas ou tornadas públicas sem a autorização do dono.

[9] Segundo dados do segundo do Microsoft Digital Defense Report 2025.

131.1.3. oriente e, se necessário, elabore normatização acerca do seu papel e do papel dos gestores dos serviços nas atividades de monitoramento das Contas Gov.br.

58. A análise evidencia a criticidade das falhas identificadas, especialmente no que tange à ausência de processos automatizados para revisão de logs e à fragilidade na gestão de senhas, que expõem o ecossistema digital a riscos significativos.

59. O investimento no aprimoramento no monitoramento contas Gov.br, conforme sugerido, é essencial para mitigar os riscos associados ao tempo de permanência de agentes maliciosos no ambiente digital. A recomendação de realizar estudos técnicos para identificar lacunas e deficiências no monitoramento, bem como implantar mecanismos técnicos e normatizar responsabilidades, é pertinente e está em consonância com o cenário atual de ameaças cibernéticas.

III

60. A auditoria realizada evidenciou fragilidades significativas na gestão de identidade e autenticação da plataforma Gov.br, comprometendo a segurança, a inclusão digital e a eficiência dos serviços públicos digitais. As inconsistências nos níveis de segurança, a baixa adoção de autenticação multifator e as falhas no monitoramento em tempo real expõem os cidadãos e a Administração Pública a riscos elevados de fraudes e acessos indevidos. Tais deficiências contrariam os princípios da eficiência e da segurança previstos no art. 37 da Constituição Federal, bem como os deveres de proteção de dados pessoais estabelecidos pela Lei Geral de Proteção de Dados (Lei 13.709/2018).

61. Verifico, também, que os achados convergem em três fragilidades sistêmicas:

62. Desalinhamento estrutural entre segurança e inclusão: a necessidade de facilitar o acesso para evitar a exclusão digital levou à redução de exigências de segurança, como a não obrigatoriedade da autenticação multifator (MFA) para contas de nível Ouro. Essa flexibilização fragiliza a proteção dos serviços públicos digitais, expondo-os a riscos de fraude e comprometem a confiança no sistema. Além disso, a baixa inclusão digital da população e a falta de programas eficazes de conscientização em segurança da informação agravam o problema.

63. Incoerência entre políticas, diretrizes e implementação: apesar da existência de normativos robustos, como a Portaria SGD/MGI 11.229/2025, sua aplicação é irregular e fragmentada. Há inconsistências entre as diretrizes estratégicas e os formulários de integração, além de falhas nos exemplos técnicos fornecidos, como a ausência de validação de *tokens* e o uso de parâmetros estáticos. Essa incoerência dificulta a implementação de controles adequados pelos gestores e aumenta a exposição a riscos.

64. Controles tecnológicos insuficientes diante da evolução das fraudes: os controles tecnológicos atuais não acompanham a evolução das fraudes, especialmente aquelas baseadas em inteligência artificial. Exemplos incluem a exploração de falhas na validação biométrica por meio de *deepfakes* e a ausência de monitoramento em tempo real para detecção de anomalias. A falta de ferramentas avançadas de monitoramento e a obsolescência dos requisitos de senhas tornam o ecossistema vulnerável a ataques.

65. As fragilidades identificadas no relatório de auditoria estão interligadas e refletem problemas estruturais que comprometem a segurança, a inclusão e a eficiência da gestão de identidade na Conta Gov.br. As propostas de encaminhamento visam mitigar essas vulnerabilidades e fortalecer a resiliência do sistema.

Ante o exposto, VOTO para que o Tribunal aprove a minuta de acórdão que ora submeto à deliberação deste Colegiado.

TCU, Sala das Sessões, em 29 de julho de 2026.

ODAIR CUNHA
Relator

DECLARAÇÃO DE VOTO

Acompanho o eminente Relator, Ministro Odair Cunha, e louvo sua decisão de afastar o eventual bloqueio das contas Gov.br de titulares falecidos. Como bem destacou S. Exa., a eventual inativação paralisaria procedimentos indispensáveis conduzidos por inventariantes e sucessores, como acertos tributários na Receita Federal, obrigações no eSocial e partilhas digitais, atos que ainda dependem do CPF do *de cujus*.

2. A ausência de sincronização em tempo real entre o Registro Civil (Sirc) e o CPF gera vulnerabilidade sistêmica, abrindo margem para credenciais indevidamente ativas e fraudes por personificação póstuma. Trata-se de gargalo estrutural no governo digital que compromete a fidedignidade das bases públicas e a segurança da informação, exigindo acompanhamento prioritário por este Tribunal.

3. Com vistas a amadurecer a matéria sem impor prejuízos ao cidadão, proponho determinar à unidade instrutora que aprofunde o achado referente à governança e à segurança da plataforma Gov.br no contexto de titulares falecidos.

Assim, manifesto apoio irrestrito ao entendimento do Relator e reforço a urgência de modelagem de alternativas tecnológicas seguras para a gestão de identidades digitais no contexto sucessório.

TCU, Sala das Sessões, em 29 de julho de 2026.

Ministro BRUNO DANTAS

ACÓRDÃO Nº 2019/2026 – TCU – Plenário

1. Processo TC 015.635/2025-2.
2. Grupo: I – Classe: V – Assunto: Relatório de Auditoria.
3. Interessados/Responsáveis: não há.
4. Órgãos/Entidades: Controladoria-Geral da União; Instituto Nacional do Seguro Social; Secretaria de Governo Digital; Serviço Federal de Processamento de Dados.
5. Relator: Ministro Odair Cunha.
6. Representante do Ministério Público: não atuou.
7. Unidade Técnica: Unidade de Auditoria Especializada em Tecnologia da Informação (AudTI).
8. Representação legal: não há.
9. Acórdão:

VISTO, relatado e discutido este processo de auditoria operacional realizada pela Secretaria de Controle Externo de Tecnologia da Informação (AudTI), com o objetivo de avaliar a maturidade, a segurança e a efetividade dos processos de gestão de identidade da Conta Gov.br, sistema central de identificação e autenticação para acesso aos serviços públicos digitais federais.

ACORDAM os Ministros do Tribunal de Contas da União, reunidos em sessão do Plenário, por unanimidade, ante as razões expostas pelo Relator, em:

9.1. com fundamento no art. 250, III, do Regimento Interno do TCU, e no art. 11 da Resolução 315/2020, recomendar à Secretaria de Governo Digital do Ministério da Gestão e da Inovação em Serviços Públicos (SGD/MGI) que:

9.1.1. realize estudo de viabilidade e de riscos para a implementação de métodos alternativos e seguros de autenticação multifatores priorizando tecnologias modernas e resistentes a ataques de engenharia social;

9.1.2. adote as medidas necessárias para:

9.1.2.1. promover o aprimoramento tecnológico, operacional e de segurança das soluções de biometria facial e prova de vida (*liveness*) do ecossistema Gov.br, de forma a:

9.1.2.1.1 assegurar que os níveis de desempenho de segurança e acurácia sejam compatíveis com padrões de boas práticas internacionalmente reconhecidos (NIST SP 63A 3.11 Rev. 4 e ISO/IEC 30107-3:2023);

9.1.2.1.2 identificar e mitigar eventuais disparidades de desempenho para grupos demográficos específicos, incluindo aqueles que utilizam dispositivos de baixa qualidade ou residem em áreas com infraestrutura limitada;

9.1.2.1.3 atualizar periodicamente as bases de validação sob controle da SGD/MGI, garantindo que sejam inclusivas e representativas da diversidade populacional brasileira;

9.1.2.2. instituir ciclos de validade e revalidação periódica para os selos de identidade obtidos via reconhecimento facial e Carteira de Identidade Nacional, alinhando a gestão do ciclo de vida das credenciais às boas práticas internacionais de gestão de identidade digital;

9.1.2.3. aprimorar, consolidar e alinhar as diretrizes de segurança e manuais de integração dos serviços ao Login Gov.br (Login Único);

9.1.2.4. implemente controles lógicos para assegurar o alinhamento entre nível de identificação da Conta Gov.br e os métodos de autenticação definidos na Portaria - SGD/MGI 11.229/2025;

9.1.2.5. realize estudos técnicos para identificar as lacunas e deficiências no monitoramento das Contas Gov.br, incluindo monitoramento de módulos de gestão e aprimoramento de deficiências que podem impactar processos formais de comunicação e resposta a incidentes, como falta de rastreabilidade ou impossibilidade de reconstrução de incidentes de segurança;

9.1.2.6. implante os mecanismos técnicos necessários ao monitoramento das Contas Gov.br; e

9.1.2.7. oriente e, se necessário, elabore normatização acerca do seu papel e do papel dos gestores dos serviços nas atividades de monitoramento das contas Gov.br.

9.2. Dar ciência às unidades jurisdicionadas do TCU e gestoras de serviços integrados à plataforma Gov.br listadas no Apêndice F deste relatório, com fundamento no art. 9º, inciso I, da Resolução 315, de 2020, de que a definição dos níveis de confiabilidade das contas (Bronze, Prata ou Ouro) e dos métodos de acesso sem a prévia realização de avaliação de risco, especialmente para serviços classificados como críticos ou sensíveis, expõe a Administração Pública a incidentes de segurança e descumpre o dever de proteção de dados dos cidadãos, em decorrência da inobservância dos seguintes dispositivos: Lei 13.709/2018: Art. 50, § 2º, I, d); e Portaria SGD/MGI 11.229/2025: Art. 7º, I e II.

9.3. Classificar como sigiloso em grau reservado, com base no art. 23, VII, da Lei 12.527/2011 e nos arts. 8º, § 3º, I e 9º, VII, ambos da Resolução 294/2018, o seguinte:

9.3.1. as peças 18-23, 29-31, 41, 56, 68, 78-79, 91, 102-104, enviadas pelos auditados, referendando a classificação dada pelo auditado; e

9.3.2. as peças 34, 66, 75-77, 81, 84, 87, 105-109, 112, 118-121, contendo as análises que evidenciam o descrito neste relatório.

9.4. Informar à Secretaria de Governo Digital do Ministério da Gestão e da Inovação em Serviços Públicos (SGD/MGI), à Secretaria Especial da Receita Federal do Brasil (RFB) à Controladoria-Geral da União (CGU) e às unidades jurisdicionadas do TCU e gestoras de serviços integrados à plataforma Gov.br listadas no Apêndice F deste relatório sobre este acórdão, destacando que a íntegra da deliberação (relatório, voto e acórdão) ora encaminhada pode ser acessada em www.tcu.gov.br/acordaos.

9.5. ordenar à Unidade de Auditoria Especializada em Tecnologia da Informação que aprofunde a análise achado referente à governança e à segurança da plataforma Gov.br no contexto de titulares falecidos sem prejuízo do monitoramento das deliberações constantes deste acórdão.

10. Ata n° 29/2026 – Plenário.
11. Data da Sessão: 29/7/2026 – Ordinária.
12. Código eletrônico para localização na página do TCU na Internet: AC-2019-29/26-P.
13. Especificação do quórum:
13.1. Ministros presentes: Jorge Oliveira (na Presidência), Walton Alencar Rodrigues, Bruno Dantas, Antonio Anastasia, Jhonatan de Jesus e Odair Cunha (Relator).
13.2. Ministros-Substitutos presentes: Augusto Sherman Cavalcanti, Marcos Bemquerer Costa e Weder de Oliveira.

(Assinado Eletronicamente)
JORGE OLIVEIRA
Vice-Presidente, no exercício da Presidência

(Assinado Eletronicamente)
ODAIR CUNHA
Relator

Fui presente:

(Assinado Eletronicamente)
CRISTINA MACHADO DA COSTA E SILVA
Procuradora-Geral