Relatório de Visão de Futuro

Resumo Executivo – 2026

Comitê Técnico de Gestão de Identidade

SUMÁRIO

Sumário

Impulsionadores de mudança **3**

Tecnológicos *3*

Regulatórios *3*

Sociais *3*

Cenários de Futuro **4**

Inovações imediatas (2026-2028) *4*

Visão 2030: transformações e novos paradigmas *5*

Considerações Finais **5**

Referências **5**

Resumo

Neste documento são apresentados impulsionadores de mudança e cenários futuros para a gestão de identidade digital no contexto acadêmico brasileiro, com foco no período entre 2026 e 2030. O objetivo é fornecer uma visão estratégica que possa orientar as ações da RNP e da comunidade acadêmica diante das transformações tecnológicas, regulatórias e sociais que impactam a gestão de identidade.

Impulsionadores de mudança

Os impulsionadores de mudança são forças ou fatores com potencial de moldar o futuro do campo de maneiras distintas. No contexto da gestão de identidade, os impulsionadores de mudança podem incluir avanços tecnológicos, mudanças regulatórias, transformações sociais e outras forças que impactam a forma como as identidades digitais são gerenciadas e utilizadas.

Tecnológicos

A OpenID Federation, versão 1.0 lançada em 2026, tem potencial para se tornar o novo padrão para federações acadêmicas, fazendo com que o ecossistema acadêmico se alinhe às práticas do mercado e facilite a integração com provedores de identidade e serviços comerciais. Paralelamente, a ascensão da inteligência artificial generativa e dos chamados deepfake desafia os métodos tradicionais de prova de identidade remota, exigindo a adoção de soluções determinísticas, como credenciais verificáveis e mecanismos criptográficos, para garantir autenticidade nas interações digitais. Ao mesmo tempo, cresce a necessidade de distinguir humanos de agentes inteligentes, impulsionando propostas inovadoras como as Credenciais de Pessoalidade e o Human Challenge Oracle, que apostam em provas contínuas e escassez cognitiva para assegurar a legitimidade das interações. A era da IA agêntica demanda, ainda, protocolos robustos de delegação de direitos e identificação de agentes, com níveis de garantia que atestem propriedades essenciais como auditabilidade e integridade.

Regulatórios

O cenário regulatório brasileiro está em rápida evolução, impulsionado pela Lei federal nº 15.211/2026 (ECA Digital), que exige verificação de idade para acesso a serviços online, sem abrir mão da privacidade, e pela crescente maturidade da Lei Geral de Proteção de Dados (LGPD), que reforça práticas como minimização de dados e consentimento verificável. Soma-se a isso o avanço do Marco Regulatório da IA (PL 2338/2023), em tramitação no Congresso Nacional, que acompanha tendências internacionais ao propor regras para biometria, identificação, monitoramento e transparência em sistemas de inteligência artificial, ampliando as exigências de identidade verificável tanto para usuários humanos quanto para agentes automatizados e fortalecendo o combate a deepfake.

Sociais

Enquanto soluções comerciais de gestão de identidade oferecem conveniência e ampla adoção, seu uso em ambientes acadêmicos esbarra em barreiras como privacidade, controle de dados e dependência tecnológica. Concomitantemente, a crescente digitalização da vida impõe desafios inéditos, como a necessidade de mecanismos confiáveis para delegação e transferência de autoridade em situações de incapacidade ou morte. Assim, a evolução dos modelos de identidade digital exige não só autenticação robusta e garantia sobre a identidade, mas também soluções nativas para gestão e delegação ao longo de todo o ciclo de vida.

Cenários de Futuro

A construção de cenários futuros permite preparar respostas estratégicas para reorganizar a gestão de identidade digital para automação, inovação e resiliência sem ampliar os riscos de segurança ou privacidade. Este esforço exige o fortalecimento da governança e o alinhamento com iniciativas internacionais de referência, como REFEDS, eduGAIN, FIM4R[1] e AARC[2], garantindo a adoção de frameworks de confiança e o cumprimento de expectativas operacionais mínimas.

A seguir, são apresentados possíveis caminhos para a evolução da gestão de identidade, visando assegurar a relevância da RNP frente à pressões comerciais e novos paradigmas tecnológicos e consolidando-a como uma infraestrutura crítica para a colaboração científica e acadêmica no Brasil e alinhada às melhores práticas internacionais. Esses possíveis caminhos consideram tanto o curto prazo, com foco em adaptações tecnológicas e regulatórias imediatas, quanto o horizonte de 2030, onde inovações e novos paradigmas podem redefinir práticas e modelos estabelecidos.

Inovações imediatas (2026-2028)

- Ecossistema nacional de identidade e confiança para as redes de e-Ciência e acadêmica
    - Fortalecer a governança e alinhar-se às Baseline Expectations da eduGAIN, para criar um ecossistema de identidade para as redes de e-Ciência e acadêmicas interoperável com iniciativas internacionais.
- Transição de federações acadêmicas baseadas em SAML para OpenId Federation
    - Atuar como emissora de Trust Marks para indicar conformidade, alinhando-se a frameworks como RAF, SIRTFI ou perfis tecnológicos em construção, como o eduGAIN OpenID Federation.
- Malha de identidade para elevar maturidade das instituições acadêmicas
    - Promover uma malha de identidade que integre governança, monitoramento e automação para elevar o nível de maturidade dos serviços de autenticação e autorização das instituições acadêmicas.
- Adoção de credenciais verificáveis em interações remotas ou presenciais
    - Servir de âncora de confiança no ambiente acadêmico para viabilizar o desenvolvimento de novos modelos de negócio que dependam de prova de identidade.
- Identidade digital para agentes de IA e mecanismos de delegação de direitos
    - Conduzir estudos sobre identidade digital de agentes, delegação de direitos, controle de acesso e rastreabilidade, para assegurar uma governança adequada ao ciclo de vida dessas identidades.
- Nível de garantia de identidade ou de pessoalidade para acesso a serviços online
    - Incentivar e facilitar a adoção de frameworks de níveis de garantia de identidade, como foi feito com o Workgroup Assurance Access da InCommon.
- Identificadores persistentes como ativos para a comunidade acadêmica
    - Considerar o uso de identificadores persistentes, como ORCID para pessoas, como parte dos serviços de GId, facilitando a gestão de identidades ao longo do tempo e em diferentes contextos.

[1] https://fim4r.org/

[2] https://aarc-community.org/

Visão 2030: transformações e novos paradigmas

- Autorização federada tendo o Provedor de Identidade (IdP) como o ponto central de controle e responsabilidade, ao invés do Provedor de Serviços (SP)
    - Permitir que a autorização de acesso seja feita no IdP, de modo que, em modelos de assinatura mensal por usuário, o SP cobre apenas pelos usuários efetivamente autorizados pelo IdP a acessar o serviço.
- Migração da WebPKI para Merkle Tree Certificates (MTCs)
    - Acompanhar experimentos com chaves e algoritmos pós-quânticos em certificados SSL, avaliando os impactos e benefícios para a ICPEdu.

Considerações Finais

Neste documento foram apresentados impulsionadores e casos de futuro para a gestão de identidade digital no contexto acadêmico brasileiro, considerando tanto ações imediatas quanto tendências para 2030. As análises e recomendações aqui reunidas visam subsidiar decisões da RNP e orientar a comunidade acadêmica diante das transformações tecnológicas, regulatórias e sociais em curso. Este documento servirá como referência inicial para a próxima revisão do relatório de visão de futuro do Comitê Técnico de Gestão de Identidade.

Referências

[1] GEANT. OpenID Technical Profile Mapping. 2026. url: https://wiki.geant.org/spaces/eduGAIN/pages/1116831798/OpenID+Technical+Profile+Mapping.

[2] Nicole Harris. REFEDS Entity Category: Anonymous Access. Fev. de 2023. url: https : / / zenodo . org /records/7816828.

[3] Nicole Harris. REFEDS Entity Category: Pseudonymous Access. Fev. de 2023. url: https://doi.org/10.5281/zenodo.7684488.

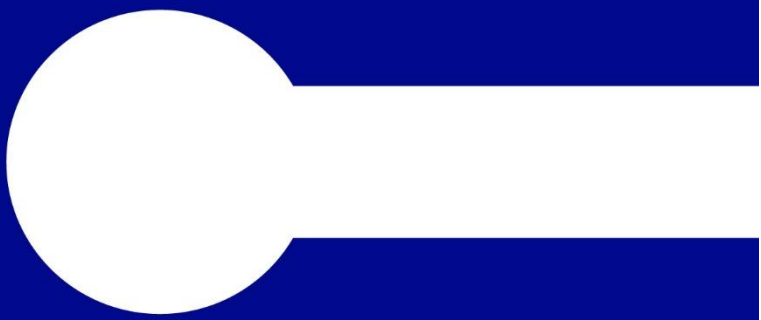
[4] Homayoun Maleki, Nekane Sainz e Jon Legarda. Human Challenge Oracle: Designing AI-Resistant, Identity-Bound, Time-Limited Tasks for Sybil-Resistant Consensus. 2026. arXiv: 2601 . 03923 [cs.CR]. url: https://arxiv.org/abs/2601.03923.

[5] Emerson Ribeiro de Mello et al. Relatório de visão de futuro em Gestão de Identidade. Fev. de 2025. url: https://plataforma.rnp.br/arquivos/documents/CT-GId-2025-relatorio-de-visao-futuro.pdf.

[6] REFEDS. REFEDS Assurance Framework. 2026. url: https://refeds.org/assurance.

[7] REFEDS. Security Incident Response Trust Framework for Federated Identity (SIRTFI). 2026. url: https://refeds.org/sirtfi.

[8] Luke Valenta et al. Keeping the Internet fast and secure: introducing Merkle Tree Certificates. Out. de 2025. url: https://blog.cloudflare.com/bootstrap-mtc.



RNP
MINISTÉRIO DA CULTURA
MINISTÉRIO DA DEFESA
MINISTÉRIO DA SAÚDE
MINISTÉRIO DAS COMUNICAÇÕES
MINISTÉRIO DA EDUCAÇÃO
MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO
GOVERNO DO BRASIL
DO LADO DO POVO BRASILEIRO