

CARTA-CONVITE 03/2025

Chamada de trabalhos para o Programa de Gestão de Identidades (PGId) 2025

1. INTRODUÇÃO

O Comitê Técnico de Gestão de Identidade (CT-GId), criado pela RNP em 2010, tem como objetivo realizar recomendações técnicas e apresentar uma visão de futuro à RNP na temática de gestão de identidades. A participação como membro do CT-GId é aberta a qualquer pessoa que tenha conhecimento e atuação nas áreas relacionadas, visando dar a maior diversidade possível em seus componentes e com isso ampliar a visão e as contribuições em todas as áreas. Para requisitar a inscrição na lista de discussão do comitê, o interessado deve acessar o endereço: <https://listas.rnp.br/mailman/listinfo/ct-gid>.

2. OBJETIVOS

O programa de gestão de identidades (PGId) é uma iniciativa do CT-GId voltada ao fomento de projetos de curta duração, com foco na realização de estudos técnicos ou no desenvolvimento de provas de conceito relacionados à gestão de identidade e de acesso.

O objetivo principal do programa é ampliar a capacidade de prospecção tecnológica do CT-GId, contribuindo para a análise e validação de novas tecnologias, modelos ou aplicações emergentes na área. Espera-se que os projetos apoiados gerem subsídios para evolução dos serviços da RNP que possuam relação com GId, além de orientar futuros investimentos em pesquisa, desenvolvimento e inovação.

3. ESCOPO

Esta chamada tem como foco o apoio a pesquisadores com bolsas de curta duração para condução de iniciativas alinhadas ao conteúdo do Relatório de Visão de Futuro em GId 2025. Serão contempladas propostas voltadas à condução de estudos técnicos sobre temas estratégicos ou desenvolvimento de provas de conceito que envolvam o uso ou integração de tecnologias emergentes na área de gestão de identidade.

Espera-se que os trabalhos desenvolvidos contribuam para aprofundar o entendimento sobre os principais desafios e oportunidades; testem e validem novas abordagens tecnológicas; ofereçam subsídios relevantes para decisões estratégicas do CT-GId e apoiem a construção de futuras versões do relatório de visão de futuro. Além disso, os resultados poderão servir como materiais de referência para as demais áreas técnicas da RNP.

4. RECURSOS E BENEFÍCIOS CONCEDIDOS

As candidaturas aprovadas nesta chamada serão contempladas com bolsas individuais de R\$ 3.200,00 mensais, por um período de 3 (três) meses, conforme as regras do Programa de Bolsas de Pesquisa, Desenvolvimento e Inovação da RNP.

As bolsas são destinadas exclusivamente aos pesquisadores proponentes, não sendo permitida a destinação de recursos para: pagamento de equipe adicional; aquisição de licenças de software, bens ou serviços; qualquer outra despesa relacionada à execução do projeto.

5. CRONOGRAMA

Os prazos do cronograma desta chamada são:

FASE	DATA
Divulgação da chamada	1/08/2025
Data limite para submissão das candidaturas	10/08/2025
Divulgação do resultado da seleção	18/08/2025
Data limite para envio da documentação dos candidatos para implantação das bolsas	22/08/2025
Período de execução dos projetos e vigência das bolsas	1/10/2025 a 31/12/2025

6. CANDIDATURAS

- A submissão de candidaturas deverá ser realizada por meio do preenchimento e envio do formulário eletrônico disponível no endereço: <https://forms.office.com/r/G4p8m4iK89>;
- Serão consideradas as submissões enviadas até às 23:59 do dia 10/08/2025, no fuso horário UTC-3;
- Não serão aceitas candidaturas submetidas por qualquer outro meio, tampouco após o prazo final de recebimento aqui estabelecido;
- O pesquisador poderá se candidatar a mais de um dos projetos listados no Anexo I. Caso opte por se candidatar mais de um, deverá obrigatoriamente indicar a ordem de preferência entre eles;
- Na ocorrência de mais de uma submissão pelo mesmo candidato, será considerada para análise apenas a última submissão recebida.

7. CRITÉRIOS DE ELEGIBILIDADE E CONDIÇÕES DE PARTICIPAÇÃO

O candidato deverá atender obrigatoriamente aos seguintes requisitos:

- Possuir título de doutor e ter vínculo empregatício como efetivo (como docente ou pesquisador) com uma instituição de ensino ou pesquisa sediada no Brasil;
- Estar cadastrado, no momento da inscrição, na lista de discussão do Comitê Técnico de Gestão de Identidade (CT-GId) da RNP, caracterizando-se como membro ativo do comitê.

Não poderão participar desta chamada candidatos que:

- Estejam atualmente recebendo bolsas financiadas pela RNP cuja carga horária combinada ultrapasse os limites permitidos pelo programa de bolsas da RNP;
- Sejam funcionários da RNP contratados sob regime CLT;
- Façam parte do conselho de administração da RNP;
- Sejam membros da comissão de avaliação de contratos de gestão (CA-MCTI);
- Participem da comissão de avaliação desta chamada;
- Mantenham qualquer vínculo contratual ativo com a RNP, incluindo: prestadores de serviço (pessoa física ou jurídica); estagiários; ou adolescentes aprendizes.

A não observância de qualquer um dos critérios listados acima acarretará o indeferimento da candidatura. A verificação da elegibilidade será realizada no momento da análise da submissão, e pode ser complementada com a solicitação, ao candidato, de documentos comprobatórios.

8. AVALIAÇÃO

O processo de avaliação e seleção das candidaturas será realizado por um comitê designado pelo CT-GId e levará em consideração os seguintes critérios:

- Engajamento prévio com o CT-GId
 - Participação em reuniões presenciais ou online;
 - Contribuições para documentos, relatórios técnicos ou outros documentos produtos do comitê;
 - Realização de apresentações em workshops, reuniões técnicas ou eventos promovidos pelo comitê.
- Histórico de projetos de pesquisa financiados pela RNP
 - Serão analisados projetos anteriores em que o candidato tenha atuado como coordenador ou bolsista principal, com ênfase na qualidade dos resultados entregues (relatórios, publicações, etc); cumprimento dos objetivos e prazos estabelecidos.
- Projetos em andamento financiados pela RNP

- Serão considerados projetos atualmente em execução com participação ativa do candidato, seja como coordenador, bolsista principal ou membro técnico da equipe.
- Produção técnica e científica na área de GId
 - Será realizada uma análise do CV Lattes, como foco em publicações e realizações diretamente relacionadas à área de GId;

O resultado da avaliação será uma lista ranqueada de candidatos, agrupada por projeto. Candidatos inscritos em mais de um projeto poderão ocupar a primeira colocação em no máximo um deles, respeitando a priorização indicada no momento da inscrição.

9. ACOMPANHAMENTO E ENTREGAS

O acompanhamento dos projetos será feito com base em relatórios mensais, conforme previsto no Programa de Bolsas da RNP, além de reuniões mensais, que serão realizadas via Conferência Web RNP.

No último mês da vigência da bolsa, o bolsista deverá apresentar os resultados finais em uma reunião do CT-GId, com data previamente acordada.

Ao final do terceiro (e último) mês da bolsa, deverá ser entregue um relatório técnico no formato de artigo científico, contendo: resumo, introdução, revisão bibliográfica, descrição do desenvolvimento, resultados e conclusões.

Para projetos de natureza experimental, o código fonte desenvolvido e a documentação necessária para implantação, compilação e execução, deverão ser disponibilizados no sistema de controle de versão da RNP (<https://git.rnp.br/>).

Todos os resultados gerados pelos projetos apoiados serão tornados públicos pela RNP.

10. DÚVIDAS E CONSULTAS

As consultas e os pedidos de esclarecimento referentes a esta Chamada Pública deverão ser encaminhados ao Comitê de Avaliação, via internet, para o e-mail pgid2025@rnp.br, até a data da publicação do resultado.

11. DISPOSIÇÕES GERAIS

A RNP poderá revogar a presente Chamada Pública, no todo ou em parte, por conveniência e interesse público, ou por fato superveniente, devidamente justificado, ou anulá-lo, em caso de ilegalidade.

A revogação ou anulação da presente chamada não gera direito a indenizações de quaisquer naturezas.

Todos os custos decorrentes da elaboração das propostas e quaisquer outras despesas correlatas à participação nesta chamada serão de inteira responsabilidade dos proponentes, não cabendo nenhuma remuneração, apoio ou indenização por parte da RNP.

As questões não previstas nesta chamada serão decididas pelo Comitê de Avaliação e pela Diretoria Executiva da RNP e, caso necessário, por autoridade superior, observadas as disposições legais aplicáveis.

Anexo I

Lista de projetos contemplados por essa chamada

Projeto 1

Autenticação biométrica e como minimizar as implicações para a privacidade dos usuários

Contexto

A crescente adoção de soluções de controle de acesso utilizando autenticação biométrica, tanto em espaços físicos como digitais, pode trazer implicações de privacidade para os usuários. Como os dados biométricos são coletados, processados e armazenados inclui riscos de vazamentos e usos indevidos. Ao contrário de senhas, por exemplo, que podem ser alteradas em caso de vazamento, dados biométricos são únicos e permanentes. Por isso, eventuais vazamentos ou usos indevidos desses dados têm consequências mais severas e duradouras. Além disso, a legislação de dados pessoais, como a LGPD e a GDPR, classifica os dados biométricos como dados pessoais sensíveis, impondo restrições adicionais ao seu tratamento e exigindo justificativas legais mais rigorosas.

Objetivos

1. Investigar estratégias de implementação de autenticação biométrica com foco em privacidade:
 - a. Como pode ser implementada minimizando os riscos à privacidade e à segurança dos usuários.
2. Comparar abordagens técnicas, legais e de governança para a implementação da biometria:
 - a. Soluções nativas aos dispositivos do usuário;
 - b. Soluções que delegam para terceiros, com processamento em servidores ou nuvem
3. Mapear práticas, soluções e padrões adotados pelo mercado:
 - a. Considerar soluções empregadas em instituições de ensino, na segurança pública, por empresas de tecnologia e por instituições financeiras.
4. Identificar e caracterizar os principais riscos e implicações do tratamento de dados biométricos:
 - a. Considerar riscos relacionados à vazamento e reutilização não autorizada, discriminação algorítmica e interação com inteligência artificial;
5. Estudar a interoperabilidade entre diferentes canais de autenticação:

- a. Interfaces digitais (web, aplicativos móveis);
 - b. Interfaces físicas (catracas e outros relacionados a controle de acesso físico).
6. Investigar, de forma exploratória, como questões legais e éticas vêm sendo tratadas em relação ao uso de dados biométricos, incluindo potenciais exemplos de casos judiciais relevantes e seus desdobramentos, a fim de contextualizar possíveis riscos técnicos do ponto de vista regulatório;
7. Recomendações e direções futuras:
 - a. Sugerir diretrizes iniciais para governança, conformidade e controle ético no uso de biometria nos serviços providos pela RNP para suas instituições usuárias.

Entregável

Um relatório técnico que contemple os riscos, desafios técnicos, jurídicos e éticos associados ao tratamento de dados biométricos; um panorama das abordagens de implementação e das práticas adotadas pelo mercado; a interoperabilidade entre diferentes canais de autenticação; exploração de casos judiciais relevantes; recomendações e direções futuras, conforme objetivos do estudo.

Materiais de apoio

1. Keyless Named as Representative Vendor in Gartner Hype Cycle for Digital Identity 2025 - <https://keyless.io/news/keyless-named-as-representative-vendor-in-gartner-hype-cycle-for-digital-identity-2025>
2. Biometria é tema do segundo volume da série Radar Tecnológico - <https://www.gov.br/anpd/pt-br/assuntos/noticias/biometria-e-tema-do-segundo-volume-da-serie-radar-tecnologico>
3. NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software - https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software?utm_source=chatgpt.com
4. The Interplay of AI and Biometrics: Challenges and Opportunities - <https://www.computer.org/csdl/magazine/co/2021/09/09524669/1wpqdbENTlc>
5. Opinion 11/2024 on the use of facial recognition to streamline airport passengers' flow (compatibility with Articles 5(1)(e) and(f), 25 and 32 GDPR - https://www.edpb.europa.eu/system/files/2024-05/edpb_opinion_202411_facialrecognitionairports_en.pdf
6. TECNOLOGIAS DE VIGILÂNCIA E EDUCAÇÃO - um mapeamento das políticas de reconhecimento facial em escolas públicas brasileiras - Diagnósticos e recomendações - https://internetlab.org.br/wp-content/uploads/2023/06/Educacao-na-mira-PT_06.pdf

7. ANPD abre Tomada de Subsídios sobre Tratamento de Dados Biométricos - <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-abre-tomada-de-subsidios-sobre-tratamento-de-dados-biometricos>

Projeto 2

O uso de agentes de IA autônomos e sua relação com identidade digital

Contexto

A expectativa para os próximos anos é que agentes de IA autônomos se tornem cada vez mais comuns, atuando em nome de usuários humanos ou de sistemas computacionais em diversas tarefas. Esse avanço levanta novos desafios para os sistemas de gestão de identidade e acesso, que precisarão evoluir para lidar com questões como:

- Limitações dos protocolos atuais de autenticação e autorização;
- Delegação de identidade;
- Estabelecimento e verificação de confiança entre agentes;
- Efemeridade e rotatividade dessas identidades;
- Mecanismos de rastreabilidade, monitoramento e auditoria.

Objetivos

1. Mapeamento conceitual:
 - a. Identificar as principais nomenclaturas e terminologias em uso (ex.: *agentic identity*, *agentic AI identity*);
 - b. Diferenciar identidades digitais para humanos e para agentes autônomos, evidenciando suas particularidades;
 - c. Levantar os principais desafios associados a esse novo paradigma.
2. Análise de protocolos e tecnologias atuais:
 - a. Realizar um levantamento de soluções existentes para autenticação, autorização e auditoria em sistemas com agentes autônomos;
 - b. Analisar protocolos relevantes, como o *Model Context Protocol (MCP)*, *OAuth 2.0 Extension: On-Behalf-Of User Authorization for AI Agents*, entre outros.
3. Recomendações e direções futuras:
 - a. Propor caminhos para evolução dos serviços de Gld da RNP frente ao avanço dos agentes de IA;
 - b. Sugerir diretrizes iniciais para governança, conformidade e controle ético no uso de agentes autônomos nos serviços institucionais da RNP e internos das instituições usuárias.

Entregável

Um relatório analítico que contemple: os conceitos e terminologias; os desafios técnicos e regulatórios relacionados à gestão de identidades de agentes autônomos, conforme os objetivos do estudo; um panorama com as soluções existentes ou emergentes; recomendações práticas e estratégicas para a RNP.

Materiais de apoio:

1. A New Identity Playbook for AI Agents: Securing the Agentic User Flow:

<https://www.strata.io/blog/agentic-identity/new-identity-playbook-ai-agents-not-nhi-8b/>

2. Agentic AI Identity Management Approach -

<https://cloudsecurityalliance.org/blog/2025/03/11/agentic-ai-identity-management-approach>

3. What is Model Context Protocol (MCP)? <https://www.ibm.com/think/topics/model-context-protocol>

4. What Are AI Identities? Understanding Agentic Systems & Governance -

<https://www.youtube.com/watch?v=AuV62XbiZcw>

5. Artificial Intelligence Identity Management Community Group -

<https://openid.net/cg/artificial-intelligence-identity-management-community-group/>

Projeto 3

Material educativo sobre o impacto da computação quântica nos serviços de gestão de identidade RNP

Contexto

Computadores quânticos práticos ainda estão sendo desenvolvidos, com grandes empresas de tecnologia como Google, IBM, Microsoft investindo fortemente para conseguir vencer a corrida. A IBM, por exemplo, espera lançar um computador quântico prático até 2029. Com o avanço tecnológico, surgem impactos diretos sobre os sistemas de segurança atuais que dependem de algoritmos de criptografia clássica, muitos dos quais poderão se tornar obsoletos diante da capacidade computacional dos computadores quânticos.

Nesse contexto, os serviços de gestão de identidade mantidos pela RNP, como a CAFe, eduROAM e principalmente a ICPedu, precisam avaliar a adoção de algoritmos criptográficos resistentes a ataques quânticos. A transição para criptografia pós-quântica é estratégica para garantir as propriedades básicas de segurança da informação, como a confidencialidade e integridade, além da autenticidade.

Para este projeto espera-se a elaboração de um material educativo de base técnica e com linguagem acessível, em formato de cartilha, que permita disseminar o conhecimento sobre computação quântica e suas implicações para os serviços de GId da RNP, auxiliando assim tanto equipes técnicas da RNP quanto instituições usuárias na compreensão dos desafios e soluções para este cenário.

Objetivos

1. Apresentar fundamentos da computação quântica, explicando seus princípios básicos e como ela difere da computação clássica em termos de modelo de processamento;
2. Realizar um levantamento dos principais algoritmos pós-quânticos atualmente considerados seguros e padronizados (ou em processo de padronização) e indicando suas aplicações em criptografia assimétrica, assinatura digital e troca segura de chaves;
3. Apresentar uma revisão sobre as estratégias que o Brasil e outros países estão se preparando para o advento dos computadores quânticos práticos;
4. Realizar um levantamento das ferramentas, bibliotecas e frameworks que possibilitem a implementação de soluções de criptografia híbrida (clássica e pós-quântica), incluindo exemplos como o Open Quantum Safe (OQS), entre outros;

5. Analisar os requisitos técnicos, operacionais e desempenho para incorporação de algoritmos pós-quânticos nos atuais serviços da RNP, como foco em compatibilidade com a infraestrutura atual, interoperabilidade e minimização de impacto.

Entregável

A principal entrega deste projeto será uma cartilha técnica e educativa, com uma linguagem acessível e foco prático, devendo contemplar os objetivos apresentados acima. A cartilha deverá ser estruturada de modo a atender tanto profissionais das áreas responsáveis por manter os serviços de Gld da RNP quanto das instituições usuárias. Espera-se assim, que a cartilha seja uma referência para ações de capacitação e planejamento estratégico no tema.

Material de Apoio

1. Roadmap for the migration to post-quantum cryptography for the Government of Canada. <https://www.cyber.gc.ca/en/guidance/roadmap-migration-post-quantum-cryptography-government-canada-itsm40001>
2. A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography. <https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography>
3. Timelines for migration to post-quantum cryptography. <https://www.ncsc.gov.uk/guidance/pqc-migration-timelines>
4. Post-quantum cryptography. <https://www.nist.gov/pqcrypto>