Política da
Comunidade Acadêmica Federada - CAFe

RNP - *Rede Nacional de Ensino e Pesquisa*

Código: CAFE.N.001 **Versão:** 2.0

CONTROLE DE VERSÕES

Versão	Data	Responsável	Natureza das Modificações
1	julho de 2011	RNP / DAGSer	Criação do serviço
2	janeiro de 2021	RNP / DAGSer	Ajustes de segurança, nova estrutura, inclusão de regras para possibilitar a exclusão de um Membro da Federação, novas regras para Provedores de Serviço, mudança da nomenclatura dos Provedores de Identidades para Organização Usuária e novas regras para Organizações Usuárias.
2	Dezembro de 2021	RNP / DAGSer	Ajustes nos itens de governança, segurança, regras de ingresso e saída e inclusão do anexo de política de privacidade. Foi também incluído o item “Aprovação e Manutenção”.

1. APRESENTAÇÃO

A Comunidade Acadêmica Federada (CAFe) consiste em uma federação de identidade que reúne instituições de ensino e pesquisa brasileiras.

Através da CAFe é possível que os usuários vinculados aos Membros da Federação, utilizando suas contas institucionais, possam acessar serviços fora do perímetro administrativo da sua instituição. Dessa forma é estabelecida uma rede de confiança que promove a oferta de serviços de forma distribuída, onde cada usuário utiliza as credencias de sua respectiva instituição.

Este documento estabelece a Política da Comunidade Acadêmica Federada (CAFe), que determina o conjunto de direcionadores que devem ser seguidos para garantir seu funcionamento adequado.

2. APROVAÇÃO E MANUTENÇÃO

Essa política foi aprovada pelo Comitê Assessor de Gestão de Identidade (CA-GID). Uma vez em vigor, esta política será mantida e revisada pelo Operador da Federação que, diante da eventual necessidade de alterações significativas, apresentará uma nova versão para aprovação do referido Comitê.

3. ESCOPO

Aplica-se a todos os Membros da Federação e ao Operador da Federação.

4. TERMOS E DEFINIÇÕES

As seguintes definições são usadas nesse documento:

- **Contatos Registrados:** pessoas autorizadas a representar os Membros da Federação. Podem possuir diferentes papéis com diferentes atribuições;
- **Contato de Segurança:** pessoa responsável por realizar os tratamentos de incidentes que venham a ocorrer na federação ou em algum cliente;
- **Comitê Assessor de Gestão de Identidade:** grupo responsável pelo assessoramento da RNP nas questões que envolvem políticas, padrões, requisitos, boas práticas, adesão de provedores de serviços/identidade, bem como elaboração de planos de ações;

- **Comitê Técnico de Gestão de Identidade:** grupo responsável pelo provimento de subsídios técnicos para a formulação de recomendações junto ao comitê assessor da CAFe;
- **Edugain:** reúne as federações de gestão de identidade integrantes da GÉANT (Rede de Pesquisa Pan-Europeia), organização gestora de uma rede de alta capacidade;
- **Entidade:** componente que um Membro da Federação deseja registrar e descrever no metadado. Em geral é um Provedor de Identidade (IdP) ou Provedor de Serviço (SP);
- **Federação:** uma associação que reúne diferentes organizações para trocar informações de maneira segura sobre seus usuários e recursos, com a finalidade de permitir colaborações e transações;
- **Grupo de Boas Práticas:** Grupo temporário que é definido pelo Comitê Assessor de Gestão de Identidade, para executar ações específicas;
- **Inter federações:** colaboração voluntária de duas ou mais Federações de Identidade, para permitir que usuários tenham acesso a Provedores de Serviços que não são os da sua própria federação de origem;
- **Membro da Federação:** uma organização que aderiu à Federação por concordar e se comprometer formalmente com sua Política;
- **Operador da Federação:** organização que provê a infraestrutura para Autenticação e Autorização para os Membros da Federação. No contexto da CAFe, a Diretoria de Serviços da RNP desempenha esse papel;
- **Organização Usuária (OU):** Instituição pública ou privada habilitada para compartilhar da ciberinfraestrutura para Educação, Pesquisa e Inovação e, por adesão, compor o Sistema RNP;
- **Provedor de Serviço (SP):** componente que, com base nas asserções de um Provedor de Identidade, exerce o controle de acesso a um serviço protegido fazendo sua gestão, implantação, operação e segurança;
- **Programa RNP (PRO-RNP):** Programa Interministerial Rede Nacional de Ensino e Pesquisa, definido pela Portaria Interministerial nº 3.825 de 12/12/2019, coordenado pelo Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC) e pelo Ministério da Educação (MEC), com participação de outros ministérios e entes federativos, com o objetivo de planejar e executar atividades de desenvolvimento tecnológico, inovação, operações de meios e serviços, envolvendo tecnologias de informação e comunicação para educação, ciência, tecnologia e inovação, e suas aplicações em políticas públicas setoriais;
- **Provedor de Identidade (IdP):** componente que emite asserções em nome de um usuário para viabilizar o acesso a um serviço disponibilizado através de um Provedor de Serviço;

- **Sistema RNP:** Sistema responsável pelo desenvolvimento, oferta e uso de serviços para atender às necessidades da pesquisa, educação e inovação. Explora tecnologias de informação e comunicação emergentes, disponibilizando uma ciberinfraestrutura de recursos federados, seguros, de alta capacidade e desempenho, por meio de mecanismos de governança multi-institucional, estabelecidos pelo Programa RNP;
- **Usuário:** pessoa natural que possui vínculo formal com um Membro da Federação.

5. MEMBROS DA FEDERAÇÃO

Existe duas categorias de Membros da Federação:

- **Pleno**: instituição qualificável como Organização Usuária do Sistema RNP. Possui o direito de registrar entidades do tipo Provedor de Identidade ou de Serviço;
- **Parceiro**: instituição que deseja apoiar a federação e possui serviços de interesse do Sistema RNP. Possui o direito de registrar apenas entidades do tipo Provedor de Serviço.

6. MODELO DE GOVERNANÇA

A governança na Federação é exercida através de modelo compartilhado e colaborativo entre o Operador da Federação, o Comitê Assessor de Gestão de Identidade, o Comitê Técnico de Gestão de Identidade e o Grupo de Políticas e Boas Práticas (grupo temporário que pode ser escolhido pelo CA-GID).

7. SEGURANÇA DA INFORMAÇÃO E PROTEÇÃO DE DADOS

Os Membros da Federação, da categoria Pleno e Parceiro, e o Operador da Federação comprometem-se a:

- Adotar a Política de Privacidade da CAFe;
- Garantir aderência à Lei Geral de Proteção de Dados (13.709/2018) nos processos relacionados a CAFe;
- Informar contato do Encarregado pelo Tratamento de Dados;
- Estabelecer o processo de governança de privacidade;
- Aplicar as recomendações de segurança da informação do Operador da Federação;
- Avaliar periodicamente o cumprimento das recomendações de segurança;
- Executar periodicamente avaliação de riscos na infraestrutura local da CAFe.

8. REGRA PARA INGRESSO E SAÍDA DA FEDERAÇÃO

- Para ingressar na federação CAFe, a instituição interessada deve satisfazer os critérios de Membro Pleno ou Parceiro. O pedido de ingresso deve ser encaminhado ao Operador da federação indicando a categoria de membro pretendida;
- Pedidos especiais de ingresso na federação serão analisados pelo Comitê Assessor de Gestão de Identidade;
- A saída voluntária da federação pode ocorrer a qualquer momento através de pedido encaminhado ao Operador da federação;
- A saída por decisão do Comitê Assessor de Gestão de Identidade e do Operador da Federação, pode ocorrer sempre que a instituição deixar de cumprir as regras da federação.

9. REGRAS PARA ORGANIZAÇÃO USUÁRIA

As entidades do tipo "Provedor de Identidade" devem atender às seguintes regras:

- Associar a cada usuário um atributo de identidade com valor único e persistente, evitando que esses atributos sejam reutilizados;
- Manter atualizadas e fidedignas as informações dos usuários utilizando o esquema breduperson para montar a base de usuários e popular minimamente os atributos para nome, apelido, e-mail, data de nascimento e CPF;
- Aderir aos padrões técnicos estabelecidos (https://ajuda.rnp.br/cafe), mantidos e divulgados pelo Operador da Federação;
- Adotar um serviço de autenticação de usuários seguro e confiável utilizando, no mínimo, login e senha únicos para cada usuário;
- Garantir que somente pessoas naturais possuam contas passíveis de autenticação;
- Receber e auxiliar equipe designada pela Governança da CAFe para realização de avaliação de segurança da informação;
- Aderir aos padrões técnicos estabelecidos, mantidos e divulgados pelo Operador da Federação;
- Atualizar os metadados da Federação, no mínimo, a cada trinta dias;
- Cooperar na resolução de incidentes relatando-os ao Operador da Federação nos casos em que esses incidentes possam afetar negativamente a segurança, confiabilidade e/ou reputação da Federação ou de qualquer de seus membros;
- Manter sempre vigente o certificado de metadados, para comunicação com a federação;
- Fornecer e manter informações de contatos precisas, incluindo pelo menos um contato de segurança que deve oferecer suporte em nome do serviço.

10. REGRAS PARA PROVEDORES DE SERVIÇO

As entidades do tipo "Provedor de Serviço" devem atender às seguintes regras:

- Respeitar a privacidade e quaisquer outras restrições associadas às informações de identidade recebidas dos usuários;
- Não compartilhar, divulgar ou armazenar de forma permanente as informações recebidas dos usuários, salvo quando houver uma base legal para tratamento de dados pessoais que permita, ao serviço, o armazenamento de dados pessoais;
- Receber e auxiliar equipe designada pela CAFe para realização de avaliação de segurança da informação;
- Aderir aos padrões técnicos estabelecidos (https://ajuda.rnp.br/cafe), mantidos e divulgados pelo Operador da federação;
- Atualizar os metadados da Federação no mínimo a cada trinta dias;
- Manter vigente o certificado de metadados, para comunicação com a federação;
- Gerir a autorização de acesso dos usuários finais;
- Cooperar na resolução de incidentes relatando-os ao Operador da Federação nos casos em que esses incidentes possam afetar negativamente a segurança, confiabilidade e/ou reputação da Federação ou de qualquer de seus membros
- Fornecer e manter informações de contatos precisas, incluindo pelo menos um contato de segurança que deve oferecer suporte em nome do serviço;
- Operar o serviço de forma segura e protegida evitando que ele prejudique a federação ou a qualquer um de seus clientes;
- Seguir as melhores práticas de segurança de TI, incluindo a aplicação proativa de atualizações ou alterações de configuração relacionadas à segurança. Responder apropriadamente, e dentro do período de tempo especificado, ao receber avisos de segurança;

11. AUDITORIA E CONFORMIDADE

O cumprimento desta norma deve ser realizado, periodicamente, por meio de avaliações de conformidade.

12. RESPONSABILIDADES

12.1. OPERADOR DA FEDERAÇÃO

- Fornecer e operar a infraestrutura central necessária para o funcionamento da Federação;
- Prestar suporte técnico para os Membros da Federação através de seus Contatos Registrados para a resolução de problemas relacionados à Federação;
- Elaborar documentação técnica contendo guias para implantação dos softwares necessários para uso da Federação; e
- Definir junto ao Comitê Assessor de Gestão de Identidade, o regulamento para ingresso e saída dos Membros da Federação.

12.2. MEMBROS DA FEDERAÇÃO

- Seguir as regras descritas para Provedor de Identidade e/ou Provedor de Serviço, conforme apresentadas respectivamente nos itens 9 e 10 deste documento.

13. EXCEÇÕES

Todo assunto que eventualmente não tenha sido tratado neste documento deve ser analisado pelo Comitê Assessor de Gestão de Identidade e pelo Operador da Federação.

14. CONSEQUÊNCIAS DAS VIOLAÇÕES

Violações desta política podem resultar na suspensão, bloqueio ou exclusão da federação, sempre que tais medidas forem necessárias para garantir a disponibilidade, integridade, confidencialidade, proteção e privacidade dos dados pessoais dos usuários sem prejuízo da aplicação de sanções administrativas, penais e cíveis por parte da RNP ou ente externo.