Política da
Comunidade Acadêmica Federada - CAFe

RNP - *Rede Nacional de Ensino e Pesquisa*

Código: CAFE.N.001 **Versão:** 1.0

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.

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 ampliação do escopo de utilização das contas institucionais e proporciona um ambiente para cooperação interinstitucional.

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

2. ESCOPO

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

3. TERMOS E DEFINIÇÕES

As seguintes definições são usadas nesse documento:

- **Federação:** federação de identidade. Uma associação de organizações que se reúnem para trocar informações de maneira segura sobre seus usuários e recursos, com a finalidade de permitir colaborações e transações;
- **Membro da Federação:** uma organização que aderiu à Federação por concordar e se comprometer formalmente com a Política da Federação;
- **Interfederações:** 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;
- **Operador da Federação:** organização que provê a infraestrutura para Autenticação e Autorização para os Membros da Federação. No contexto da CAFe a RNP desempenha esse papel;
- **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);
- **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;

- **Provedor de Serviço (SP):** componente que com base nas asserções de um Provedor de Identidade exerce o controle de acesso a um serviço protegido;
- **Usuário:** pessoa natural que possui vínculo formal com um Membro da Federação;
- **Contatos Registrados:** pessoas autorizadas a representar os Membros da Federação. Podem possuir diferentes papéis com diferentes atribuições;
- **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;
- **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; e
- **Organização Usuária (OU):** Instituição pública ou privada habilitada para compartilhar da Ciber Infraestrutura para Educação, Pesquisa e Inovação e, por adesão, compor o Sistema RNP. É também a quem um usuário final é afiliado e é a responsável por autenticar este usuário e gerenciar os dados de identidade digital dos seus usuários finais.

4. 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 Provedor de Serviço; e
- **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.

5. MODELO DE GOVERNANÇA

A governança na Federação é exercida através de modelo compartilhado e colaborativo entre o Operador da Federação e o Comitê Assessor de Gestão de Identidade. Cabe à Diretoria de Serviços da RNP desempenhar o papel de Operador da Federação.

5.1 COMITÊ ASSESSOR DE GESTÃO DE IDENTIDADE

Assessora o Operador na Federação nas questões que envolvem: políticas, padrões, requisitos, boas práticas, adesão de membros, inclusão de entidades, bem como elaboração de planos de ações.

6. SEGURANÇA DA INFORMAÇÃO E PROTEÇÃO DE DADOS

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

- Garantir a aderência à Lei 13.709/2018 - Lei Geral de Proteção de Dados nos processos relacionados a CAFe;
- Aplicar as recomendações de segurança da informação do Operador da Federação; e
- A avaliar periodicamente o cumprimento das recomendações de segurança.

7. REGRA PARA INGRESSO E SAÍDA DA FEDERAÇÃO

Para ingressar na federação 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; e

A saída voluntária da federação pode ocorrer a qualquer momento através de pedido encaminhado ao Operador da federação.

8. REGRAS PARA ORGANIZAÇÃO USUÁRIA

Entidade 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;
- Utilizar 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 na federação;
- Receber e auxiliar equipe designada pela 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;
- Deve cooperar com o Operador da Federação e outros Membros na resolução de incidentes e deve relatar incidentes 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; e
- Manter sempre vigente o certificado de metadados, para comunicação com a federação.

9. REGRAS PARA PROVEDORES DE SERVIÇO

Entidade 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, sem que haja consentimento formal;
- Receber e auxiliar equipe designada pela 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;
- Manter sempre vigente o certificado de metadados, para comunicação com a federação;
- Os provedores de serviços são responsáveis por decidir quais usuários podem acessá-los e quais direitos são designados aos usuários finais; e
- Deve cooperar com o Operador da Federação e outros Membros na resolução de incidentes e deve relatar incidentes 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.

10. AUDITORIA E CONFORMIDADE

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

11. RESPONSABILIDADES

11.1. 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 o regulamento para ingresso e saída dos Membros da Federação.

11.2. MEMBROS DA FEDERAÇÃO

- Designar e manter atualizados os Contatos Registrados junto ao Operador da Federação;
- Cooperar com o Operador da Federação, bem como com os outros Membros da Federação, na resolução e notificação de incidentes de segurança; e
- Seguir os regulamentos aplicáveis às Entidades.

12. EXCEÇÕES

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

13. 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 e a 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.