**CAIS - RFC 2350**

**1. Informações do documento**

 Este documento contém uma descrição do CAIS/RNP de acordo com a RFC 2350.

**1.1 Data da última atualização**

15 de abril de 2025.

**1.2 Lista de distribuição para notificações**

Não há lista de distribuição para notificações de novas versões deste documento.

**1.3 Locais onde este documento pode ser encontrado**

 A versão atual deste documento pode ser encontrada em https://plataforma.rnp.br/cais/rfc2350. A chave utilizada para a assinatura é a chave CAIS/RNP listada abaixo de 2.8.

**2. Informações de contato**

**2.1 Nome do CSIRT**

 English: CAIS/RNP – RNP Security Incident Response Team

Português: CAIS/RNP – Centro de Atendimento a Incidentes de Segurança da RNP

**2.2 Endereço de correspondência**

Rua Dr. Ricardo Benetton Martins, 1000 – Parque II do Polo de Alta Tecnologia, Campinas – SP – 13086-902

**2.3 Fuso horário**

America/Sao\_Paulo (GMT-0300)

**2.4 Número de telefone**

Não aplicável. O CAIS/RNP não recebe notificações de incidentes via telefone.

**2.5 Número de fac-símile**

Não aplicável.

**2.6 Outras telecomunicações**

iNOC-DBA: 1916\*800 (veja mais em https://inoc.nic.br).

**2.7 Endereço eletrônico de e-mail**

Notificações de incidentes devem ser enviados para cais@cais.rnp.br.

**2.8 Chaves públicas e informações de criptografia**

A chave CAIS/RNP pode ser encontrada em: https://plataforma.rnp.br/cais/cais-pgp.key

**2.9 Membros da equipe**

Não são fornecidas informações públicas sobre os membros do CAIS/RNP.

**2.10 Outras informações**

Informações adicionais podem ser encontradas em: https://www.rnp.br/cais.

O CAIS/RNP é membro do FIRST, mais detalhes em: https://www.first.org/members/teams/cais-rnp

**2.11 Pontos de contato com o cliente**

Para entrar em contato com o CAIS/RNP sobre incidentes de segurança relacionados às redes de ensino e pesquisa, envie um e-mail para <cais@cais.rnp.br>.

A operação padrão CAIS/RNP é de segunda a sexta-feira, das 09:00 às 18:00h, UTC-0300.

**3. Carta**

**3.1 Declaração da missão**

Atuar na detecção, resolução e prevenção de incidentes de segurança na rede acadêmica brasileira, além de elaborar, promover e disseminar práticas de segurança em redes.

**3.2 Eleitorado**

O CAIS/RNP coordena a resposta e o tratamento de incidentes de segurança ligadas à rede acadêmica brasileira (NREN) operada pela Rede Nacional de Ensino e Pesquisa (RNP).

**3.3 Patrocínio e/ou filiação**

O CAIS/RNP foi criado em 1997 e é mantido pela RNP, associação sem fins lucrativos criada para operar a rede nacional de pesquisa e educação (NREN). A RNP é regida por seu estatuto e suas atribuições e compromissos são definidos em contrato com o Ministério da Ciência e Tecnologia (MCTI). A coordenação de resposta a incidentes dentro da rede é uma das responsabilidades da RNP.

**3.4 Autoridade**

CAIS/RNP não tem autoridade sobre seu público-alvo, todas as atividades são baseadas em colaboração com outras entidades.

**4. Políticas**

**4.1 Tipos de incidentes e nível de suporte**

O CAIS/RNP atua como ponto focal para a notificação de incidentes da rede acadêmica brasileira, proporcionando a coordenação e suporte necessários para o tratamento de incidentes, através dos seguintes serviços:

• Coordenação no tratamento de incidentes, análise de incidentes e artefatos, mitigação e recuperação de incidentes;

• Detecção e análise de vulnerabilidades;

• Ações de conscientização em segurança;

• Treinamentos e compartilhamento de materiais, técnicas e tecnologias de segurança.

O CAIS/RNP também proporciona ao seu público-alvo informações e atualizações quanto a acontecimentos e tendências de segurança através de alertas e informes, relatórios, webinars e eventos.

**4.2 Cooperação, interação e divulgação de informações**

O CAIS/RNP não compartilha informações específicas sobre incidentes com partes externas.

Os dados podem ser agregados para estatísticas, desde que as informações não identifiquem pessoas ou organizações envolvidas.

O CAIS/RNP adere ao Protocolo de Compartilhamento de Informações de Semáforo conforme orientações do FIRST:

https://www.first.org/tlp/. As informações rotuladas com as tags WHITE, GREEN, AMBER ou RED serão tratadas adequadamente.

**4.3 Comunicação e autenticação**

O CAIS/RNP usa e-mail não criptografado na maioria das comunicações não sensíveis.

Para mensagens confidenciais, recomenda-se o uso de criptografia PGP (ver itens 2.7 e 2.8). Alertas de vulnerabilidade enviados pela lista de discussão podem ser assinados digitalmente. A autenticação pode ocorrer por comunidades existentes (ex: FIRST) ou outros métodos como call-back, mail-back ou reunião presencial.

**5. Serviços**

**5.1 Resposta incidente**

 O CAIS/RNP auxilia na resolução de incidentes de segurança com um sistema de gerenciamento, agregação de notificações e acompanhamento técnico.

**5.1.1 Triagem de incidentes**

Triagem de incidentes ou vulnerabilidades detectadas ou reportadas; auxílio na validação, avaliação e priorização pelo público-alvo.

**5.1.2 Coordenação de incidentes**

Ponto de contato principal para sistemas conectados à rede brasileira de pesquisa e educação. Notificações recebidas são encaminhadas aos contatos apropriados e, se necessário, agregadas.

**5.1.3 Resolução de incidentes**

 O CAIS/RNP atua diretamente na resolução de incidentes em sua rede e serviços mantidos pela RNP. Para redes externas, fornece suporte às equipes locais sem autoridade direta de resolução.

**5.2 Atividades proativas**

Serviços incluem:

• Alertas de vulnerabilidade sobre softwares e hardwares comuns;

• Apoio à criação de CSIRTs;

• Realização e participação em eventos de segurança;

• Varreduras de vulnerabilidade.

**6. Formulários de notificação de incidentes**

Não há formulários disponíveis. Consulte a seção 2.7.

**7. Isenção de responsabilidade**

 O CAIS/RNP não assume responsabilidade por erros, omissões ou danos causados pelo uso das informações fornecidas.