EDITAL DE SELEÇÃO PARA COOPERAÇÃO E EXECUÇÃO

RNP/CAIS Nº. 01/2026

2ª Seleção de Instituições para o Estabelecimento de Centros de Operações de Segurança (SOC) nos estados Integrados à Rede Federada de Cibersegurança e Privacidade

06 de abril de 2026

A REDE NACIONAL DE ENSINO E PESQUISA, associação civil qualificada como Organização Social pelo Decreto nº 4.077 de 09 de janeiro de 2002, com sede à Rua Lauro Müller nº 116, sala 1103, Botafogo, Rio de Janeiro, RJ, CEP 22290-160, inscrita no Cadastro Nacional de Pessoa Jurídica do Ministério da Fazenda sob o nº 03.508.097/0001-36, por meio deste Edital, selecionará até 2 (dois) proponentes para, com cada um individualmente, firmar Acordo de Cooperação Técnica (ACT) com o objetivo de estabelecer 1 (um) Centro de Operações de Segurança (SOC) em um Estado, e por consequência participação na chamada Rede Federada de Cibersegurança e Privacidade.

1. CONTEXTUALIZAÇÃO

1.1. A RNP é a rede acadêmica brasileira para educação e pesquisa, com objetivo de promover o uso inovador de redes avançadas no país. Atua por meio da oferta de conectividade segura e de alta capacidade, serviços especializados e promove projetos de inovação, além de colaborar com redes internacionais de ensino e pesquisa, conhecidas como *National Research and Education Networks* (NRENs). Criada em 1989, foi fundamental para a chegada da Internet no Brasil, e hoje a Rede Ipê, seu backbone nacional, serve às instituições de todas as unidades da federação. A RNP está conectada às demais redes de educação e pesquisa na América Latina, América do Norte, África e Europa por meio de cabos de fibra óptica terrestres e submarinos. Com a Rede Ipê, seu backbone nacional de alta capacidade, mais de 1.800 campi são conectados, em centenas de localidades em todo o Brasil, incluindo universidades, centros de pesquisa, institutos educacionais e culturais, agências de pesquisa, hospitais de ensino, parques e polos tecnológicos. Somado ao desenvolvimento, sustentação

e oferta de serviços e aplicações de TIC, beneficia cerca de 4,5 milhões de alunos, professores e pesquisadores brasileiros. Implementa soluções de TIC próprias, construídas por meio de processos de desenvolvimento tecnológico envolvendo grupos e instituições de pesquisa brasileiros e setor privado.

1.2. O pioneirismo também existe em cibersegurança. Em 1995 a RNP criou o primeiro centro de segurança de redes brasileiro, que deu origem ao CAIS[1] em 1997, cujo papel é zelar pela segurança da rede e das instituições conectadas. Com mais de 28 anos de atuação, o CAIS foi um dos primeiros grupos de resposta a incidentes de segurança a atuar em nível nacional na detecção, resolução e prevenção de incidentes de segurança cibernética. Atualmente, o CAIS trata da segurança da informação de uma forma holística, com ações integradas e colaborativas de governança, identificação, proteção, detecção, resposta e recuperação. O CAIS possui um papel relevante[2] para a comunidade, com a publicação de estatísticas, alertas, notificações[3] e relatórios de segurança[4], e mantém um Catálogo de Fraudes[5]. Para o cumprimento dos objetivos estratégicos, a segurança da informação e a privacidade sempre foram e continuam sendo fundamentais para a RNP.

1.3. Nesse contexto, a segurança da informação e a privacidade consolidam-se como pilares estratégicos da atuação da RNP, alinhados às diretrizes nacionais, como a Estratégia Nacional de Segurança Cibernética (e-ciber)[6] direciona ações estratégicas que reforçam o papel de estados e municípios para a proteção e resiliência cibernética da sociedade, pessoas e instituições.

1.4. Os números de incidentes cibernéticos seguem aumentando, resultando em prejuízos para pessoas e instituições[7].

[1] 25 anos do CAIS. http://plataforma.rnp.br/cais/25-anos
[2] CAIS, inteligência em cibersegurança. https://www.rnp.br/cais/
[3] Estatísticas do CAIS. https://www.rnp.br/cais/#Estatisticas
[4] Pesquisas, relatórios e conteúdos ricos em informação. https://www.rnp.br/informe-se/publicacoes/
[5] Catálogo de Fraudes. https://catalogodefraudes.rnp.br
[6] Decreto N. 10.222, de 5 de fevereiro de 2020. https://www.gov.br/gsi/pt-br/ssic/estrategia-nacional-de-seguranca-cibernetica-e-ciber/e-ciber.pdf
[7] Estatísticas resultantes do trabalho de detecção, triagem, análise e resposta a incidentes cibernéticos. https://www.gov.br/ctir/pt-br/assuntos/ctir-gov-em-numeros

1.5. A cibersegurança é um pilar fundamental para alavancar o desenvolvimento econômico[8], principalmente devido ao aumento da conectividade e da digitalização, que resulta em uma maior superfície de ataques cibernéticos.

1.6. A privacidade e segurança é um dos objetivos da Estratégia Nacional de Governo Digital[9], visando ampliar a resiliência e a maturidade das estruturas tecnológicas governamentais com atenção à privacidade, proteção de dados pessoais, segurança da informação e segurança cibernética.

1.7. O Programa de Privacidade e Segurança da Informação (PPSI)[10], tem como objetivo elevar a maturidade e a resiliência dos órgãos e entidades, em termos de privacidade e segurança da informação, no âmbito do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP).

1.8. Diante do crescimento contínuo dos incidentes cibernéticos e da ampliação da superfície de ataque decorrente da digitalização, torna-se essencial a adoção de estruturas especializadas e permanentes de monitoramento e resposta. Nesse cenário, destaca-se o Centro de Operações de Segurança (SOC), que consiste em uma estrutura centralizada responsável por monitorar, detectar, analisar e responder a incidentes de segurança cibernética em tempo real, por meio da atuação integrada de pessoas, processos e tecnologias.

1.9. De forma complementar, o SOC atua a partir da coleta e análise contínua de dados provenientes de diferentes fontes, como redes, sistemas e aplicações, permitindo identificar padrões anômalos e potenciais ameaças. Essa atuação envolve, por exemplo, a investigação e priorização de alertas de segurança, a correlação de eventos para distinguir atividades legítimas de maliciosas e a coordenação de respostas a situações como acessos indevidos, presença de códigos maliciosos, exploração de vulnerabilidades ou vazamento de dados. Além disso, contribui para a geração de inteligência de ameaças e para o aumento da visibilidade sobre o ambiente digital, viabilizando uma atuação contínua, proativa e orientada à mitigação de riscos.

1.10. Alinhado ao PPSI e às necessidades correlatas em Segurança da Informação, a RNP inaugurou em 2023 seu SOC, implantado para proporcionar maior proteção, visibilidade, mitigação de

[8] Cybersecurity Economics for Emerging Markets. https://www.worldbank.org/en/topic/digital/publication/Cybersecurity-Economics-for-Emerging-Markets
[9] Estratégia Nacional de Governo Digital. https://www.gov.br/governodigital/pt-br/estrategias-e-governanca-digital/estrategianacional
[10] Portaria SGD/MGI Nº 852, de 28 de março de 2023. https://www.in.gov.br/en/web/dou/-/portaria-sgd/mgi-n-852-de-28-de-marco-de-2023-473750908

ataques cibernéticos e conformidade para as instituições que fazem parte do Sistema RNP. O modelo de custos compartilhados viabiliza o atendimento às instituições (atualmente em mais de 160) por meio de parcerias, processos estruturados, uso em escala de plataformas de cibersegurança e time especializado, que resultam em custos reduzidos se comparados aos de mercado.

1.11. Com a aderência às necessidades de cibersegurança das instituições, e diante dos desafios crescentes, a RNP estruturou a iniciativa do SOC nos estados como forma de ampliar sua atuação. O objetivo é de desenvolver capacidades de cibersegurança próprias nos estados brasileiros, de uma forma coordenada com o SOC da RNP, fortalecendo assim as instituições locais, que terão maior visibilidade, proteção e resiliência cibernética, avançando também no nível de maturidade e conformidade, em especial com a propagação de ações do PPSI.

1.12. Os SOCs nos estados representam os alicerces que sustentarão a construção de uma Rede Federada de Cibersegurança e Privacidade, representando uma estrutura colaborativa, descentralizada, expansiva e incremental de desenvolvimento de capacidades de cibersegurança.

1.13. Atuando de forma coletiva, integrada e coordenada, os SOCs nos estados atuarão com o SOC da RNP, que passa a exercer um papel central, como um SOC de Coordenação, trazendo toda a expertise e experiência exercida nos 28 anos de CAIS em cibersegurança.

1.14. Existe uma grande necessidade de fortalecimento dos estados brasileiros em segurança cibernética, que está alinhada com o propósito do SOC nos estados. Com o desenvolvimento de capacidades em cibersegurança e a construção da Rede Federada de Cibersegurança e Privacidade, esta iniciativa contribui para a evolução da cultura em cibersegurança, do nível de maturidade, da conformidade e da capacidade de proteção contra os ataques cibernéticos e resposta avançada a incidentes de segurança.

1.15. A ação do SOC nos estados integra o planejamento do Programa Conecta, iniciativa do Ministério da Ciência, Tecnologia e Inovação (MCTI), coordenada e executada pela RNP, que amplia o acesso a redes e serviços digitais avançados para instituições de ensino e pesquisa em todo o país. Dentre as ações previstas, está incluída a ampliação do Centro de Operações em Segurança (SOC). Nesse contexto, a ação do SOC nos estados representa uma forma de implementação dessa ampliação, por meio da descentralização da operação de cibersegurança e da expansão da Rede Federada de Cibersegurança e Privacidade, contribuindo para o fortalecimento das instituições atendidas e para o desenvolvimento de capacidades locais.

1.16. Ainda como parte da estratégia de fortalecimento das capacidades de cibersegurança nos estados, o SOC nos estados também busca criar condições para que as instituições abrigo

possam, quando houver interesse, viabilidade e com os respectivos controles necessários, utilizar informações derivadas da operação do SOC para fomentar pesquisa aplicada e desenvolvimento tecnológico na área de cibersegurança. Essa possibilidade tem como finalidade estimular o desenvolvimento tecnológico e a inovação nacional, apoiando a formação de competências e contribuindo para a evolução de soluções e processos relacionados à proteção digital.

2. FUNDAMENTAÇÃO

2.1. As necessidades de cibersegurança exigem uma atuação coletiva, com sinergias e ações em nível nacional, estadual e municipal. Adicionalmente, a atuação setorial reforça a assertividade das ações, permitindo a priorização, otimização e a escalabilidade. A RNP, por meio do CAIS, vem, ao longo dos anos, atuando com abrangência nacional na conectividade segura de todo o Brasil, tendo como parte essencial os Pontos de Presença (PoPs) distribuídos em todos os estados brasileiros.

2.2. O CAIS da RNP vem acompanhando as necessidades e evoluções de cibersegurança, com o desenvolvimento de capacidades relacionadas à gestão de segurança da informação, gestão de riscos cibernéticos e de vulnerabilidades, proteção e implementação de controles de segurança, monitoramento, resposta a incidentes e recuperação de desastres. O CAIS tem reforçado a atuação necessária no ecossistema de ensino, pesquisa e inovação com a estruturação de seu Centro de Operações de Segurança (SOC), trabalhando de forma integrada com as frentes complementares de segurança ofensiva (*Red Team*) e defensiva (*Blue Team*), governança, riscos, conformidade, privacidade, educação, conscientização, resposta a incidentes (CSIRT) e arquitetura de segurança.

2.3. O SOC da RNP vem contribuindo para a elevação do nível de cibersegurança das Organizações Usuárias do Sistema RNP, incluindo avanços relacionados aos controles do PPSI, aumento da resiliência cibernética, melhoria da visibilidade de cibersegurança, e redução de impactos financeiros e reputacionais decorrentes de ataques cibernéticos.

2.4. Diante do cenário atual, em que os impactos dos incidentes cibernéticos são cada vez mais representativos e as medidas legais exercidas pelos países continuam a evoluir, torna-se essencial o avanço das estratégias organizacionais e técnicas, que por sua vez exigem o desenvolvimento de capacidades e de medidas de cooperação.

2.5. A RNP busca estabelecer alianças estratégicas com os estados para fortalecer a cibersegurança com o estabelecimento de SOCs nos estados como elemento impulsionador

para a proteção cibernética de instituições e pessoas, fundamentais para o desenvolvimento local, a partir do desenvolvimento de capacidades em cibersegurança.

2.6. Os SOCs nos estados atuarão de forma coletiva e integrada com o SOC da RNP, que passará a exercer o papel de um SOC de Coordenação, contribuindo para os avanços locais.

2.7. A estruturação da RNP na forma de um sistema, o Sistema RNP, reformulado por meio da Portaria Interministerial n. 3.825, de 12 de dezembro de 2018, reflete uma proposta integradora, orientada pela articulação de iniciativas, recursos e capacidades em benefício das comunidades alcançadas e das organizações usuárias, integrantes do mencionado Sistema. Nesse mesmo sentido, portanto, no campo da cibersegurança, a RNP propõe uma atuação coletiva e coordenada, capaz de potencializar a proteção digital por meio de soluções compartilhadas e colaborativas, ampliando o alcance e a efetividade das ações de segurança.

2.8. Os SOCs nos estados, nesse sentido, constituem a primeira ação para a construção de uma Rede Federada de Cibersegurança e Privacidade, que visa implementar elementos da Estratégia Nacional de Cibersegurança (e-Ciber), agregando novas capacidades necessárias de segurança cibernética que refletirão em toda a sociedade, de uma forma sinérgica com as estratégias federais, estaduais e municipais. A Rede Federada de Cibersegurança e Privacidade visa instituir uma estrutura de governança e coordenação para implementação de medidas de reforço à privacidade, proteção de dados pessoais, segurança da informação e segurança cibernética, em articulação com estruturas de mesmo propósito de âmbito regional e nacional, em especial o Programa de Privacidade e Segurança da Informação (PPSI) do governo federal.

2.9. Adicionalmente, a operação dos SOCs nos estados tende a gerar informações relevantes sobre ameaças cibernéticas, padrões de ataques, vulnerabilidades exploradas e comportamentos maliciosos observados no ambiente digital das instituições atendidas. Quando tratadas de forma adequada e em conformidade com os normativos aplicáveis, essas informações podem subsidiar iniciativas de pesquisa aplicada e desenvolvimento tecnológico na área de cibersegurança. Nesse sentido, a possibilidade de utilização de dados derivados da operação do SOC para fins de pesquisa e inovação contribuindo para o fortalecimento do ecossistema nacional de segurança cibernética, permitindo que as instituições abrigo ampliem sua atuação em projetos de pesquisa, formação de recursos humanos especializados e desenvolvimento de novas soluções e metodologias voltadas à proteção digital.

2.10. O SOC nos estados possibilita a formação e a evolução profissional em cibersegurança, por meio da aproximação direta dos times dos SOCs com a cibersegurança em sua essência e na prática. Há a operação de plataformas de cibersegurança em múltiplas camadas, com a aplicação de processos e playbooks efetivos, que estão sempre em evolução.

2.11. O SOC nos estados caracteriza também um ambiente que estimula, viabiliza e acelera o desenvolvimento tecnológico na área de cibersegurança, em um ambiente prático que aproxima a pesquisa e desenvolvimento das operações de cibersegurança. Há o potencial das novas tecnologias, mecanismos, algoritmos, processos, métodos e metodologias desenvolvidos serem utilizados pelo SOC, e depois replicados para toda a Rede Federada de Cibersegurança e Privacidade.

3. BASE LEGAL

O presente edital encontra-se fundamentado nas seguintes normativas e dispositivos legais:

3.1. Decreto nº 4.077, de 09 de janeiro de 2002 – Qualificação da RNP como Organização Social.

3.2. Lei nº 12.846, de 1º de agosto de 2013 – Lei Anticorrupção, que define normas para integridade nas parcerias público-privadas.

3.3. Lei Complementar nº 101, de 4 de maio de 2000 – Lei de Responsabilidade Fiscal (LRF), que orienta o equilíbrio das contas públicas nas parcerias governamentais.

3.4. Marco Civil da Internet (Lei nº 12.965, de 23 de abril de 2014) – Estabelece princípios, direitos e deveres para o uso da Internet no Brasil, incluindo a proteção da segurança cibernética.

3.5. Lei Geral de Proteção de Dados (Lei nº 13.709, de 14 de agosto de 2018 – LGPD) – Regulamenta o tratamento de dados pessoais, essencial para a implementação do SOC.

3.6. Portaria Interministerial MEC/MCTIC nº 3.825, de 12.12.2018, que reformula o Programa Interministerial de Implantação e Manutenção da Rede Nacional para Ensino e Pesquisa - RNP e de seu Comitê Gestor.

4. DEFINIÇÕES

4.1. **Centro de Operações de Segurança da RNP (SOC da RNP**): O Centro de Operações de Segurança da RNP tem como objetivo fortalecer a segurança cibernética das Organizações Usuárias do Sistema RNP, elevando seu nível de maturidade e aprimorando a capacidade de detecção, prevenção e resposta a incidentes de segurança.

4.2. **Ciberinfraestrutura:** Plataforma digital distribuída, integrada por redes de comunicação, sistemas de computação e armazenamento, componentes de *hardware* e *software,*

dispositivos de sensoriamento e aquisição de dados que, em conjunto, habilitam e suportam a pesquisa científica, a educação e a inovação.

4.3. **Entidade:** pessoa jurídica pública ou privada, dotada de personalidade jurídica própria.

4.4. **Instituição Abrigo:** Instituição responsável por implantar e manter o SOC no estado, com atuação do time, processos e plataformas tecnológicas de cibersegurança, integrado e em colaboração com o SOC de Coordenação.

4.5. **Organização Usuária:** Instituição pública ou privada habilitada para compartilhar da ciberinfraestrutura para Educação, Pesquisa e Inovação provida pela RNP e, por adesão, compor o Sistema RNP, usufruindo de seus serviços. As instituições que compartilham esta ciberinfraestrutura da RNP, são, portanto, "Organizações Usuárias do Sistema RNP".

4.6. **Pontos de Presença (PoP):** Para operar seu backbone e garantir o atendimento às comunidades de educação, pesquisa, saúde e cultura, a RNP possui pontos de presença (PoPs) espalhados pelas 27 unidades da federação. Nesses, equipes técnicas e administrativas são responsáveis por garantir acesso à rede Ipê para seus usuários finais, que podem estar vinculados a organizações que se conectam ao backbone diretamente, através dos PoPs, ou indiretamente, através de redes metropolitanas ou infovias estaduais ou regionais.

4.7. **Rede Federada de Cibersegurança e Privacidade:** Estrutura colaborativa, descentralizada, expansiva e incremental de desenvolvimento de capacidades de cibersegurança que, inicialmente, é composta pelas instituições responsáveis por abrigar o SOC nos estados. Esse modelo fortalece a cultura de cibersegurança, contribui para a democratização da cibersegurança no Brasil, elevando a maturidade das operações e a capacidade de resposta avançada a incidentes de segurança.

4.8. **Sistema RNP[11]:** Sistema responsável pelo desenvolvimento, oferta e uso de serviços para atender às necessidades das comunidades de 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 Interministerial Rede Nacional de Ensino e Pesquisa – PRORNP, reformulado pela Portaria Interministerial nº 3.825, de 12 de dezembro de 2018. O Sistema RNP é composto por: (i) a Rede Nacional Ipê e seus Pontos de Presença (PoPs) e Pontos de Agregação; (ii) as Redes

[11] https://www.rnp.br/sistema-rnp

Metropolitanas Comunitárias; (iii) as Organizações Usuárias; e (iv) as Redes de Colaboração de Comunidades.

4.9. **SOC de Coordenação:** SOC da RNP, responsável por orquestrar os SOCs nos estados, garantindo as operações 24x7x365, as atualizações tecnológicas, definição de plataformas, o cumprimento dos processos, a qualidade nas entregas e uma atuação eficiente e rápida em casos de incidentes de segurança.

4.10. **SOC nos estados:** Infraestrutura física e tecnológica local nos estados, com times de cibersegurança com a missão de proteger e monitorar ativamente as instituições locais contra ameaças cibernéticas. É orquestrado, organizado e integrado com o SOC de Coordenação, seguindo padrões e processos que garantem uma operação homogênea e eficiente. Parte fundamental para o desenvolvimento de capacidades de cibersegurança local e para a Rede Federativa de Cibersegurança e Privacidade.

4.11. **Arranjos Locais:** Articulações e parcerias institucionais voltadas a viabilizar a implementação, a operação e a sustentabilidade do SOC nos estados. Essas colaborações podem envolver até 10 (dez) instituições que venham a ser beneficiadas pelo SOC nos estados, sem custo nos 2 (dois) primeiros anos do acordo, bem como outros órgãos e/ou entidades capazes de contribuir com recursos, infraestrutura ou profissionais qualificados. Os arranjos locais têm como principais objetivos estabelecer e manter a infraestrutura necessária ao funcionamento do SOC nos estados, viabilizar a contratação e/ou alocação de equipe técnica, além de apoiar a expansão e o fortalecimento da Rede Federada de Cibersegurança e Privacidade. Considerando que este edital não prevê repasse financeiro por parte da RNP à instituição abrigo, tais parcerias são consideradas fundamentais para garantir a efetividade, a continuidade e o sucesso da iniciativa.

5. PROPÓSITO DO EDITAL DE SELEÇÃO PARA COOPERAÇÃO E EXECUÇÃO

5.1. A finalidade deste Edital é a seleção de até 2 (dois) proponentes, de diferentes Estados, um por Estado, para a celebração de parceria, por meio de Acordo de Cooperação Técnica (ACT), para desenvolver capacidades em cibersegurança e implantar um SOC naquele Estado, visando proteger e monitorar instituições locais e fortalecer a construção de uma Rede Federada de Cibersegurança e Privacidade.

5.2. Será selecionada uma única proposta por proponente, a Instituição Abrigo do SOC no Estado, observada a ordem de classificação para a celebração do ACT, conforme Item 12 CLASSIFICAÇÃO DAS PROPOSTAS, deste Termo de Referência.

6. OBJETIVO DO ACORDO DE COOPERAÇÃO TÉCNICA

6.1. O Acordo de Cooperação Técnica (ACT) que será celebrado, após a realização da seleção, tem como objetivo formalizar a cooperação com a instituição selecionada como parceira, para o fortalecimento das capacidades em cibersegurança no Estado, mediante a integração com o CAIS, a implantação de um SOC no estado e a futura participação na Rede Federada de Cibersegurança e Privacidade, promovendo, de forma conjunta entre a RNP e instituição, ações coordenadas, escaláveis e sustentáveis voltadas à proteção e à resiliência cibernética de pessoas e instituições, em consonância com as diretrizes nacionais de segurança da informação e proteção de dados.

7. CRITÉRIOS DE ELEGIBILIDADE E CONDIÇÕES DE PARTICIPAÇÃO

7.1. São elegíveis para submissão de propostas as Organizações Usuárias do Sistema RNP, bem como outras instituições estaduais, tais como fundações, secretarias de governo, companhias estaduais de processamento de dados (PRODs) e entidades similares, público ou privado.

7.2. Arranjos locais são desejáveis e podem ser feitos para viabilizar a implantação do SOC nos estados e integração à Rede Federada de Cibersegurança e Privacidade.

7.3. Somente serão admitidas propostas que apresentem manifestação por escrito da alta gestão da instituição, assinada por dirigente com poderes legais para representação da instituição. O modelo de carta de anuência é apresentado no ANEXO I deste instrumento.

7.4. A participação das instituições interessadas neste Edital implica na aceitação de todas as condições aqui apresentadas.

8. RECURSOS E BENEFÍCIOS CONCEDIDOS

8.1. Não há previsão de repasse de recursos financeiros neste edital. No entanto, conforme descrito na Seção 12, são incentivados arranjos locais que promovam a cooperação entre instituições. Esses arranjos podem ter como objetivo o estabelecimento e a manutenção da infraestrutura necessária para a operação do SOC no estado, a **viabilização da contratação e/ou alocação da equipe técnica**, bem como o apoio à expansão da Rede Federada de Cibersegurança e Privacidade.

8.2. O proponente terá um Centro de Operações de Segurança (SOC) para atendimento próprio e de instituições do estado, com alinhamento direto com as necessidades locais, com a

Estratégia Nacional de Segurança Cibernética (e-ciber), visando o desenvolvimento de capacidades em cibersegurança necessários para evoluir a resiliência cibernética na região.

8.3. Para a execução da parceria decorrente desta seleção, serão fornecidos aos proponentes selecionados:

- Licenciamento e acesso às plataformas de cibersegurança, com a finalidade de viabilizar a operação de cibersegurança a ser realizada pelo SOC no Estado, no atendimento às instituições por ele protegidas, de acordo com a proposta designada para o Centro. Atualmente, as seguintes camadas de proteção são contempladas:
  - **Anti-DDoS**;
  - **Security Ratings**;
  - **Threat Intelligence**;
  - **WAAP**;
  - **Gestão de vulnerabilidades**;
  - **SIEM**.
- Processos utilizados no SOC de Coordenação que possibilitam o funcionamento da operação de segurança a ser conduzida;
- Manuais de operação das plataformas de cibersegurança fornecidas pelo SOC de Coordenação;
- Treinamento interno da equipe que irá compor o SOC nos estados;
- Certificações do curso Security+ da CompTIA para 2 (dois) analistas selecionados para as atividades do SOC no estado;
- Arte da marca a ser utilizada pelo SOC no estado, contendo logomarcas da RNP, CAIS, SOC da RNP, instituição abrigo e participantes do arranjo local.

8.4. Será disponibilizado o plano Intermediário do SOC da RNP para a Instituição Abrigo durante os 2 (dois) anos de vigência do acordo, no âmbito da atuação do SOC no Estado, em conjunto com o SOC de Coordenação. Atualmente, o plano Intermediário contempla o seguinte escopo (mais informações disponíveis no site do RNP+):

- **Anti-DDoS** – Análise do comportamento do tráfego da instituição, somente através dos links fornecidos pela RNP, a fim de identificar e mitigar de ataques de negação de serviço;
- **Security Ratings** – Avaliação mensal do nível de segurança cibernética e acompanhamento da evolução histórica, com base em vulnerabilidades, exposição de dados e práticas de segurança;
- **Threat Intelligence –** Monitoramento e detecção de credenciais corporativas vazadas na Surface Web, Deep Web e Dark Web;

- **WAAP** - Proteção de aplicações web e APIs, por meio da detecção e mitigação de ataques que exploram vulnerabilidades na camada de aplicação, como ataques de injeção e cross-site scripting. São fornecidas duas licenças, capazes de proteger múltiplas aplicações, conforme a infraestrutura a ser protegida;
- **Gestão de vulnerabilidades –** Varredura mensal de vulnerabilidades externas em 5 (cinco) IPs ou URLs públicas, expostas à internet, avaliando exclusivamente a superfície acessível publicamente a partir da rede externa, sem autenticação;
- **SIEM** – Monitoramento e detecção de ataques a partir da correlação de logs de serviços de diretório e autenticação (Active Directory/OpenLDAP/Samba).
- **Indicadores semanais**, evidenciando o quantitativo de alertas tratados;
- **Relatório mensal**, detalhando toda a operação de segurança realizada, análise de eventos significativos e ataques mitigados.

8.5. Também será disponibilizado o plano Intermediário do SOC da RNP para até 10 (dez) instituições do Estado, sem custo para as instituições beneficiadas, durante os 2 (dois) anos de vigência do acordo, no âmbito da atuação do SOC no Estado, em conjunto com o SOC de Coordenação. O processo de definição das instituições do estado que serão atendidas será realizado em conjunto com a gestão do SOC no Estado e SOC de Coordenação, priorizando o atendimento às instituições participantes do Sistema RNP.

8.6. A proponente passará a ter uma equipe técnica qualificada para executar a operação de segurança, incluindo o monitoramento, a análise e o tratamento de eventos e incidentes, bem como a condução de medidas de mitigação quando aplicáveis, de acordo com o escopo de atuação e camadas utilizadas pelos SOCs nos estados, em benefício próprio e de outras instituições do estado. Como parte dessas atribuições, os analistas serão responsáveis pela elaboração de relatórios técnicos, permitindo evidenciar a atuação do SOC e demonstrar o valor gerado pela operação.

8.7. O SOC de Coordenação ficará responsável pela evolução contínua dos processos e procedimentos operacionais, construção e atualização de manuais de operação das plataformas, bem como por implantações de novos clientes, configurações e ajustes das ferramentas. Compete ainda ao SOC de Coordenação apoiar a equipe dos SOCs nos estados na mitigação de ataques de maior severidade, realizar a validação técnica de relatórios e orientar a atuação do SOC no estado.

8.8. Uma vez constituído o SOC no Estado, o proponente e a RNP deverão construir e implantar, em conjunto, um modelo de atuação que viabilize sua sustentabilidade, seja através da expansão dos serviços, da continuidade das operações do SOC, bem como no

desenvolvimento tecnológico da área de cibersegurança através de projetos de pesquisa, dando sequenciamento ao plano estratégico da iniciativa após os 2 (dois) anos de vigência do acordo.

8.9. Caso haja interesse da instituição abrigo em utilizar dados gerados pela operação do SOC no estado para fins de pesquisa e desenvolvimento na área de cibersegurança, deverá ser realizado previamente um estudo para definir quais dados serão utilizados, de que forma e com qual finalidade, bem como os critérios e controles aplicáveis. Quando aplicável, o tratamento desses dados deverá contemplar medidas como pseudonimização, conforme critérios e controles definidos pelo SOC de Coordenação e em conformidade com os normativos vigentes. O uso desses dados será exclusivo da instituição abrigo e deverá observar integralmente os critérios definidos pelo SOC de Coordenação, de modo a prevenir uso indevido e evitar a exposição de informações não autorizadas ou não necessárias ao objetivo proposto.

8.10. O SOC de Coordenação irá fornecer apoio operacional durante o período de operação do SOC nos estados, garantindo uma redundância da operação de segurança.

8.11. Fora do horário de operação do SOC nos estados, as atividades de segurança serão gerenciadas pelo SOC de Coordenação, assegurando cobertura ininterrupta.

8.12. Poderá ser fornecido ainda, capacitações e cursos para a equipe do SOC nos estados, sem custo para a instituição abrigo, caso haja necessidade identificada pelo SOC de Coordenação.

9. DEVERES E RESPONSABILIDADES

INSTITUIÇÃO ABRIGO

A instituição abrigo deve atender aos seguintes itens, de acordo com o ACT que será estabelecido.

9.1. A instituição abrigo é responsável por prover a infraestrutura necessária para a implantação do SOC no Estado, seguindo os seguintes padrões:

9.1.1. Infraestrutura física destinada exclusivamente para comportar a sala do SOC na instituição abrigo, onde, por questões de segurança, a sala não pode ser compartilhada com nenhuma outra equipe que não a do SOC no estado. Essa infraestrutura deve possuir os seguintes itens:

- Metragem mínima de 25 m²;

- Parede adesivada com a arte da marca a ser utilizada pelo SOC no estado, contendo logomarcas da RNP, CAIS, SOC da RNP, instituição abrigo e participantes do arranjo local;
- Ar-condicionado;
- Mesas, Cadeiras e Gaveteiros;
- Fechadura com leitor biométrico;
- Porta com fechamento magnético;
- Câmera de vigilância;
- Vidro Polarizado;
- Smartphone com linha ativa para uso exclusivo do SOC no estado;
- Questões relacionadas à eletricidade, sobretudo sobre disponibilidade de energia elétrica, de preferência, ininterrupta (geradores e nobreaks), inclusive para ou com capacidade de manter o sistema de refrigeração para conforto dos alocados e equipamentos.

9.1.2. O ambiente escolhido para a implantação do SOC no estado, incluindo o layout de todos os itens definidos acima, deve ser aprovado pela equipe do SOC de Coordenação da RNP, a fim de garantir uma estrutura adequada e padronizada para comportar de maneira profissional a operação do SOC no estado.

9.1.3. Os requisitos mínimos do conjunto de equipamentos de TIC destinados à equipe que irá compor o SOC no estado e ao ambiente físico são:

- Equipamentos para Vídeo Wall:
  - 4 (quatro) TVs de 50 a 55 polegadas;
  - 1 (um) computador com processador i7, placa de vídeo com 4 (quatro) saídas HDMI, SSD 500GB, 32GB de memória RAM; **ou** 2 (dois) computadores com processador i5, placa de vídeo com 2 (duas) saídas HDMI, SSD 500GB, 16GB de memória RAM.
- Equipamento individual da equipe:
  - 1 (um) notebook com processador i5, SSD 500GB, 16GB de memória RAM e *webcam* integrada;
  - 2 (dois) monitores de tamanho entre 21 e 23 polegadas;
  - 1 (um) kit teclado e mouse sem fio;

- 1 (um) fone headset com microfone.
- Conectividade geral das estações de trabalho.

9.1.4. Outros equipamentos poderão ser instalados caso a RNP verifique a necessidade e a instituição abrigo concorde, para cumprimento dos objetivos do projeto. Neste caso, a instituição será previamente informada da possível demanda adicional.

9.2. A instituição abrigo deve custear todas as despesas operacionais (como água, energia elétrica, entre outros), além de garantir a manutenção e, se necessário, a substituição dos recursos essenciais para o pleno funcionamento do SOC no estado.

9.3. A instituição abrigo será integralmente responsável pela contratação e/ou alocação de, no mínimo, 2 (dois) analistas de segurança, com formação superior em andamento na área de Tecnologia da Informação ou áreas correlatas, os quais deverão atuar simultaneamente, de forma presencial, no SOC no estado, sendo expressamente vedado o regime remoto ou híbrido.

9.4. Deverá ser assegurada a sustentabilidade econômico-financeira do modelo de contrapartidas, em conformidade com as responsabilidades atribuídas à instituição abrigo quanto à alocação e cessão da equipe. Fica vedada a alocação de profissionais que recebam, direta ou indiretamente, remuneração, bolsa, incentivo, repasse financeiro ou qualquer outro benefício custeado pela RNP para atuação no SOC no estado, a qualquer título, não se aplicando tal vedação a vínculos ou participações do profissional em outros projetos ou iniciativas da RNP, desde que desvinculados das atividades desempenhadas no SOC.

9.5. É admitida a participação de profissionais com diferentes modalidades de vínculo com a instituição, inclusive bolsistas ou vínculos equivalentes, desde que seja assegurada a disponibilidade compatível com as atividades do SOC no estado. A organização interna das atividades e a gestão da alocação dos profissionais são de responsabilidade exclusiva da instituição abrigo, devendo esta garantir que, durante a execução das atividades relacionadas ao SOC, não haja conflito ou prejuízo decorrente da concomitância com outras atribuições.

9.6. O SOC no estado deverá operar em regime de funcionamento regular em dias úteis, em horário compatível com as necessidades operacionais e com a integração ao SOC de Coordenação, respeitados os feriados locais e nacionais. Compete à instituição abrigo definir a organização da jornada de trabalho e assegurar a disponibilidade de sua equipe durante o período de funcionamento do SOC (das 9h às 18h), de modo a garantir a continuidade e a adequada execução das atividades, observadas as diretrizes gerais estabelecidas neste edital.

9.7. A equipe do SOC nos estados não poderá operar nenhuma plataforma interna da instituição abrigo, que já não faça parte do escopo de monitoramento delimitado pelo SOC de Coordenação, a não ser em situações de desenvolvimento de plataformas para possíveis aplicações futuras nos SOC de Coordenação e de estado, bem como pela Rede Federada de Cibersegurança e Privacidade.

9.8. A substituição ou reposição dos analistas deve ocorrer no menor prazo possível, de forma a evitar descontinuidade nas atividades do SOC nos estados. O não cumprimento dessa obrigação poderá resultar em notificação formal pela equipe do SOC de Coordenação da RNP, concedendo um prazo para regularização da equipe.

9.9. A instituição abrigo deve contratar e/ou alocar um responsável técnico, podendo ser o gestor de TIC ou o gestor de cibersegurança, a fim de gerir a equipe de analistas do SOC nos estados.

9.10. O responsável técnico do SOC nos estados é o ponto central de contato para todas as questões gerenciais, atuando em conjunto com o responsável técnico do SOC de Coordenação.

9.11. Caso de ausência do responsável técnico, a instituição abrigo deve indicar um substituto qualificado que assumirá temporariamente as responsabilidades dele, garantindo a continuidade das operações do SOC nos estados;

9.12. Caso a ausência do responsável técnico seja prolongada ou definitiva, a instituição abrigo deve nomear um novo profissional no menor prazo possível, assegurando que o SOC nos estados não sofra prejuízos operacionais.

9.13. Em caso de ausência, de qualquer natureza, o responsável técnico da instituição deve comunicar o SOC de Coordenação via e-mail, com a maior brevidade possível.

9.14. A instituição abrigo deve fornecer informações sobre horários de funcionamento, recessos e feriados com, no mínimo, 48 horas de antecedência. Este informe deve ser enviado ao SOC de Coordenação, via e-mail soc@rnp.br.

9.15. O SOC nos estados deve cumprir integralmente os processos e procedimentos definidos pelo SOC de Coordenação, garantindo o mesmo nível de qualidade. Além disso, deve viabilizar a validação e análise contínua pelo SOC de Coordenação, assegurando a consistência na execução dos processos e a eficiência operacional.

9.16. O SOC nos estados deve manter o padrão de qualidade estabelecido pelo SOC de Coordenação.

9.17. O SOC nos estados deve passar anualmente por checagem de conformidade dos padrões de qualidade e maturidade nos processos e procedimentos provenientes da padronização do SOC de Coordenação. É necessário envio de documentações e evidências aderentes aos padrões pré-determinados.

9.18. Uma vez constituído o SOC no estado, a Instituição Abrigo deverá construir e implantar, em conjunto com a RNP, um modelo de atuação que viabilize sua sustentabilidade, seja através da expansão dos serviços, da continuidade das operações de SOC, bem como no desenvolvimento tecnológico da área de cibersegurança através de projetos de pesquisa, dando sequenciamento ao plano estratégico da iniciativa após os 2 (dois) anos de vigência do acordo.

9.19. Caso haja interesse em utilizar dados derivados da operação do SOC no estado para fins de pesquisa e desenvolvimento em cibersegurança, caberá à Instituição Abrigo realizar estudo prévio para definição do escopo, finalidade e forma de utilização dos dados, bem como assegurar que o tratamento dessas informações observe integralmente os critérios, controles e diretrizes estabelecidos pelo SOC de Coordenação e a legislação vigente. A Instituição Abrigo será responsável pela implementação das medidas técnicas e organizacionais necessárias para garantir a proteção das informações utilizadas, bem como por eventuais incidentes de segurança, uso indevido, exposição não autorizada ou vazamento de dados decorrentes da utilização desses dados, sem prejuízo da aplicação das medidas cabíveis previstas neste edital e na legislação aplicável.

9.20. Não está prevista a transferência de recursos financeiros para as instituições abrigo selecionadas. Quaisquer despesas relacionadas à ampliação da infraestrutura física ou à aquisição de equipamentos necessários é de responsabilidade integral da instituição abrigo.

RNP

9.21. A RNP deve custear o licenciamento das soluções utilizadas no SOC de Coordenação, que serão fornecidas ao SOC no estado, para atendimento da instituição abrigo e de até 10 (dez) instituições do estado, durante os 2 (dois) anos de vigência do acordo.

9.22. O SOC de Coordenação deve orquestrar toda a operação de segurança, fornecendo capacidade e inteligência em cibersegurança por meio das soluções, conhecimentos, processos e manuais fornecidos.

9.23. O SOC de Coordenação é responsável por manter a operação de segurança 24x7, visto que o SOC nos estados atua apenas em horário comercial. O SOC nos estados deve realizar a troca

de conhecimento com o SOC de Coordenação durante a troca de horário, a fim de manter a operação de segurança durante a madrugada, feriados e fins de semana.

9.24. O SOC de Coordenação é responsável por orquestrar e direcionar as atividades da equipe do SOC nos estados, seja para tratar de questões relacionadas à própria instituição abrigo ou às demais instituições monitoradas pelo SOC de Coordenação.

9.25. O SOC de Coordenação deve apoiar o processo de seleção dos analistas e responsável técnico que irão compor a equipe do SOC nos estados.

9.26. A equipe técnica do SOC de Coordenação da RNP deve avaliar a equipe do SOC nos estados, a fim de garantir a qualidade nas atividades, incluindo as respostas a incidentes de segurança.

9.27. O SOC de Coordenação deve avaliar periodicamente o padrão de qualidade e a efetividade do SOC nos estados (conformidade com os processos e procedimentos estabelecidos no SOC de Coordenação), incluindo uma análise do nível de maturidade, a partir de suas entregas.

9.28. A RNP poderá convidar, a seu critério e arcando com os custos de locomoção, estadia e alimentação, a participação de membros da equipe do SOC nos estados em reuniões de trabalho, ações de capacitação ou em eventos organizados pela RNP.

9.29. Uma vez constituído o SOC no estado, a RNP deverá construir e implantar, em conjunto com a Instituição Abrigo, um modelo de atuação que viabilize sua sustentabilidade, seja através da expansão dos serviços, da continuidade das operações de SOC, bem como no desenvolvimento tecnológico da área de cibersegurança através de projetos de pesquisa, dando sequenciamento ao plano estratégico da iniciativa após os 2 (dois) anos de vigência do acordo.

9.30. Definir os critérios, diretrizes e controles aplicáveis para eventual utilização de dados oriundos da operação do SOC no estado para fins de pesquisa e desenvolvimento em cibersegurança, incluindo orientações relacionadas à segurança da informação, privacidade e proteção de dados. Caberá à RNP avaliar e estabelecer as condições sob as quais tais dados poderão ser utilizados, bem como orientar a aplicação de mecanismos de proteção e restrições necessárias para prevenir o uso indevido ou a exposição de informações sensíveis.

10. APRESENTAÇÃO DA PROPOSTA E DA DOCUMENTAÇÃO

10.1. Apresentação da proposta:

10.1.1. A apresentação de candidaturas deverá ser realizada por meio do preenchimento e envio, por parte do proponente, do formulário eletrônico disponível no endereço: https://forms.office.com/r/93fTXPQmh7

10.1.2. A pessoa a ser identificada como proponente no formulário de submissão precisa pertencer ao quadro de funcionários da instituição, bem como deverá ser utilizado, necessariamente, seu endereço de e-mail institucional para envio da proposta.

- Recomenda-se que o proponente seja o gestor de segurança da informação ou de TI da instituição.

10.1.3. Cada proponente deverá apresentar uma manifestação favorável, em apoio à proposta, da alta gestão da instituição (dirigente com poderes legais para representação da instituição).

- Tal manifestação poderá ser comprovada por meio de ofício ou mensagem eletrônica enviada para o endereço soc@rnp.br.

10.1.4. Além do preenchimento do formulário eletrônico e do envio da carta de anuência do dirigente com poderes legais para representação da instituição, todos os itens pontuados no formulário, conforme a tabela constante no item 12.3, deverão ser devidamente comprovados por meio de documentação pertinente.

- Os documentos comprobatórios devem ser enviados via mensagem eletrônica para o endereço soc@rnp.br.

10.1.5. Serão consideradas as propostas enviadas até às 23:59 do dia 01/05/2026, no fuso horário GMT-3.

- Este mesmo prazo também é aplicável para o envio de informações comprobatórias e manifestações de anuência do dirigente e do gestor de segurança da informação/TI da instituição.

10.1.6. Após o término do prazo estabelecido, nenhuma outra proposta será recebida, assim como não serão aceitos adendos ou esclarecimentos que não forem solicitados pela RNP.

10.2. Envio de informações complementares:

10.2.1. A RNP se compromete a tratar de forma confidencial toda informação e documentação que venha a ter acesso por força desde edital, obrigando-se a utilizá-las apenas para a finalidade e nos limites aqui apresentados e a não permitir que nenhum de seus colaboradores, representantes ou terceiros sob sua

responsabilidade, façam quaisquer outros usos dessas informações confidenciais sem prévia autorização do proponente.

10.2.2. A Comissão de Seleção poderá entrar em contato com o proponente a qualquer tempo, se julgar necessário, para o esclarecimento de dúvidas técnicas que possam surgir durante a análise da proposta enviada.

11. PRAZOS

11.1. Prazos do cronograma deste Edital:

FASE	DATA
Publicação deste Edital	06/04/2026
Webconferência pública para tirar dúvidas sobre este Edital, a ser realizada no endereço: **https://conferenciaweb.rnp.br/sala/soc-rnp**	13/04/2026 às 15h (GMT -3)
Término do prazo para submissão de candidaturas.	01/05/2026
Visitas técnicas às proponentes.	11/05/2026 ao 15/05/2026
Publicação do resultado.	29/05/2026
Assinatura do Acordo de Cooperação Técnica (ACT).	Até 28/06/2026
Validade deste Edital	05/04/2027

11.2. O horário limite para a submissão das propostas e entrega de documentação se encerra às 23:59 (fuso horário GMT-3).

11.3. O prazo limite para a assinatura do Acordo de Cooperação Técnica é de até 30 (trinta) dias após a publicação do resultado.

11.4. O prazo limite para a adequação integral da infraestrutura do SOC no estado (seções 9.1, 9.3 e 9.8) é de até 3 (três) meses após a assinatura do ACT.

11.5. Após a publicação do resultado, a RNP entrará em contato com os proponentes selecionados para o agendamento de uma reunião inaugural (*kick-off*).

12. CLASSIFICAÇÃO DAS PROPOSTAS

12.1. A Comissão de Seleção analisará as propostas apresentadas pelas instituições que aplicarem para este edital. A análise e a seleção das propostas serão realizadas pela Comissão de Seleção, que terá total independência técnica para exercer seu julgamento.

12.2. A Comissão de Seleção será composta por analistas e gestores da RNP, incluindo aqueles que atualmente compõem o SOC de Coordenação da RNP, e representante do MCTI.

12.3. A classificação dos proponentes será realizada por meio da avaliação dos seguintes critérios:

Critério avaliado	Aspectos que serão considerados na avaliação	Pontuação atribuída
Instituição abriga um Ponto de Presença (POP) da RNP	Atualmente hospeda um Ponto de Presença (PoP) da RNP em sua infraestrutura.	0 ou 1 Peso 5
Instituição abriga uma unidade da Escola Superior de Redes (ESR)	Atualmente hospeda uma unidade da Escola Superior de Redes (ESR) em sua infraestrutura.	0 ou 1 Peso 3
Conectividade ao Sistema RNP	Proponente faz parte do Sistema RNP.	0 ou 1 Peso 4
Conectividade redundante	Possui redundância dos links de Internet.	0 ou 1 Peso 3
Instituição oferta cursos de segurança da informação	Proponente ou parceiros do arranjo local ofertam cursos de segurança da informação em sua grade curricular, promovendo a capacitação e o aprimoramento contínuo das equipes que podem integrar o SOC.	0 ou 1 Peso 3
Infraestrutura	A proponente já possui toda a infraestrutura necessária para implantação do SOC no estado, de acordo com os itens descritos na seção 9.1.	0 ou 1 Peso 10
Experiência em cibersegurança do responsável técnico	Pontuação de acordo com a experiência, em anos.	Até 2 anos – 2 2-4 anos – 3 Acima de 4 anos - 4

Critério avaliado	Aspectos que serão considerados na avaliação	Pontuação atribuída
Experiência em cibersegurança da equipe de analistas	Pontuação de acordo com a experiência, em anos, em média.	0-1 ano – 2 1-2 anos – 3 Acima de 2 anos - 4
Possui acordo de cooperação com a RNP ou o CAIS	Possui acordos de cooperação vigentes com a RNP ou o CAIS.	0 ou 1 Peso 1
Arranjos locais: equipe	A proponente possui toda a equipe de analistas já estabelecida, que será alocada exclusivamente para atuação no SOC no estado (seção 9.3).	0 ou 1 Peso 5
	A proponente possui o responsável técnico que irá coordenar o SOC no estado (seção 9.9).	0 ou 1 Peso 5
	A proponente dispõe de recursos financeiros próprios ou provenientes de cooperação e/ou acordos financeiros que assegurem o financiamento necessário para a manutenção da equipe responsável pela continuidade do SOC no estado (seções 9.3 e 9.9), a exemplo de financiamento do governo estadual.	0 ou 1 Peso 5
Arranjos locais: instituições	Possui relacionamentos institucionais com instituições que receberão os serviços. São aceitos para comprovação do item, documentos oficiais, como por exemplo, acordos institucionais, contratos, memorandos etc.	0 ou 1 Peso 3

Critério avaliado	Aspectos que serão considerados na avaliação	Pontuação atribuída
Arranjos locais: expansão	Possui relacionamentos institucionais que viabilizem a expansão da Rede Federada de Cibersegurança e Privacidade. São aceitos para comprovação do item, documentos oficiais, como por exemplo, acordos institucionais, contratos, memorandos etc.	0 ou 1 Peso 4
Diversidade de estados atendidos	Receberão pontuação adicional proponentes dos seguintes estados: • AC - Acre • AL - Alagoas • AM - Amazonas • BA - Bahia • CE - Ceará • ES - Espírito Santo • GO - Goiás • MA - Maranhão • MG - Minas Gerais • MS - Mato Grosso do Sul • MT - Mato Grosso • PA - Pará • PB - Paraíba • PE - Pernambuco • PR - Paraná • RJ - Rio de Janeiro • RN - Rio Grande do Norte • RO - Rondônia • RR - Roraima • SC - Santa Catarina • SE - Sergipe • TO - Tocantins	0 ou 1 Peso 10

12.4. A proponente deverá enviar documentação comprobatória de **todos os itens a serem pontuados**, via mensagem eletrônica, para o endereço soc@rnp.br, até o fim do período de submissão das propostas.

12.5. Será aceito como comprovação do critério "Arranjos locais: equipe", referente às pontuações da equipe de analistas e do responsável técnico, documentação que comprove a aprovação formal das vagas para início do processo de contratação e/ou alocação dos colaboradores. No caso de bolsistas (ou vínculos equivalentes), será aceita documentação que comprove a aprovação formal das bolsas/vagas, com o respectivo ato/instrumento autorizativo e previsão de custeio. Documentações apresentadas fora desses formatos poderão ser analisadas e deliberadas posteriormente pela Comissão de Seleção.

12.6. A Comissão de Seleção apresentará como resultado uma lista com a classificação das propostas recebidas, de acordo com a pontuação obtida.

12.7. Em caso de empate na classificação das propostas, o desempate considerará:

i. O maior potencial de impacto da proposta para o fortalecimento da cibersegurança no âmbito das instituições atendidas e da sociedade; e

ii. O maior grau de aderência às diretrizes estratégicas da RNP e do CAIS, conforme avaliação fundamentada da Comissão de Seleção.

12.8. Após recebimento das propostas, será realizada uma **etapa eliminatória,** onde os seguintes itens serão avaliados:

i. Recebimento de carta de anuência do Gestor de segurança da informação/TI (caso ele não seja o proponente).

ii. De acordo com o ranqueamento das proponentes baseado na pontuação previamente estabelecida na seção 12.3, será feita uma visita técnica às instituições com maior pontuação, a fim de avaliar a viabilidade técnica da implantação do SOC no estado. Como resultado, será elaborado um parecer de caráter eliminatório, declarando a organização usuária apta ou inapta a abrigar o SOC nos estados.

iii. O proponente que impossibilitar e/ou não disponibilizar agenda dentro do prazo previsto para a visita técnica será automaticamente desclassificada.

13. RESULTADO

13.1. Os 2 (dois) proponentes mais bem classificados e que tenham cumprido com êxito a fase de análise da documentação serão declarados aptos para a celebração do ACT, sendo o resultado do edital homologado e publicizado.

13.2. Não será admitido mais de um proponente selecionado por estado.

13.3. O resultado será publicizado por meio do envio aos endereços eletrônicos informados pelos proponentes participantes e da divulgação da lista com as instituições aprovadas em página do website público da RNP (www.rnp.br).

13.4. Caso alguma das proponentes declaradas aptas para a celebração do ACT, não cumpram os prazos definidos, fica a cargo da Comissão de Seleção, considerar a convocação das demais proponentes, além das 2 (duas) primeiras selecionadas, seguindo a ordem de classificação obtida no resultado deste edital, observado o prazo de validade.

14. RESCISÃO DO ACT

14.1. O Acordo de Cooperação Técnica (ACT) poderá ser rescindido caso o proponente deixe de atender aos requisitos técnicos e operacionais previamente estabelecidos, incluindo, mas não se limitando a:

14.1.1. Falha na manutenção da infraestrutura necessária para a operação do SOC no estado, incluindo conectividade;

14.1.2. Não substituição ou alocação de equipamentos essenciais à operação do SOC, comprometendo sua funcionalidade;

14.1.3. Caso a Instituição Abrigo não mantenha no mínimo 02 (dois) analistas atuando simultaneamente, de forma presencial e exclusiva para o SOC nos estados;

14.1.4. Descumprimento de exigências regulatórias e normativas, não se limitando a:

i. Atender às exigências da Lei Geral de Proteção Dados (LGPD - Lei n. 13.709/2018), garantindo boas práticas no tratamento de dados pessoais;

ii. Cumprir o Marco Civil da Internet (Lei n. 12.965/2014), respeitando os princípios de privacidade, segurança e governança da informação;

iii. Seguir as diretrizes de segurança da RNP e do SOC de Coordenação, aderindo a padrões de operação e boas práticas recomendadas;

iv. Atender aos critérios do Plano de Trabalho, que estabelecerá as etapas, atividades e metas para a implantação do SOC no estado.

14.2. O descumprimento dos requisitos de infraestrutura física ensejará notificação prévia para regularização, no prazo de 30 (trinta) dias. A rescisão imediata do ACT será aplicada prioritariamente em hipóteses que comprometam a operação essencial, tais como interrupção da conectividade, ausência de equipe técnica mínima presencial ou violação

grave de diretrizes de cibersegurança que coloquem em risco a integridade da Rede Federada de Cibersegurança e Privacidade.

14.3. Caso algum dos acordos firmados por meio desse processo de seleção pública venha a ser rescindido, poderão ser convocadas outras proponentes, além das 2 (duas) primeiras selecionadas, seguindo a ordem de classificação obtida no resultado deste edital, observado o prazo de validade.

15. DÚVIDAS E CONSULTAS

15.1. As consultas e os pedidos de esclarecimento referentes a este Edital deverão ser encaminhados à Comissão de Seleção, via Internet, para o e-mail soc@rnp.br, até a data da publicação do resultado.

15.2. A Comissão de Seleção terá prazo de 3 (três) dias úteis para responder as consultas e os pedidos de esclarecimentos encaminhados. As respostas serão enviadas para o e-mail do solicitante.

15.3. A RNP não se responsabiliza por quaisquer incorreções e/ou problemas de funcionamento dos endereços eletrônicos fornecidos pelas instituições interessadas.

16. DISPOSIÇÕES GERAIS

16.1. Será facultado à Comissão de Seleção promover, em qualquer fase do processo de análise e seleção, diligências destinadas a esclarecer ou complementar a instrução do presente Edital e a aferição dos critérios de habilitação de cada instituição.

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

16.3. A revogação ou anulação do presente chamamento não gera direito a indenizações de quaisquer naturezas.

16.4. A divulgação do resultado da seleção da instituição não implica relação de obrigatoriedade para a formalização da parceria, contudo, havendo a celebração do ACT, ele terá efeito vinculante.

16.5. Todos os custos decorrentes da elaboração das propostas e quaisquer outras despesas correlatas à participação neste edital serão de inteira responsabilidade das instituições, não cabendo nenhuma remuneração, apoio ou indenização por parte da RNP.

16.6. O proponente é responsável pela fidelidade e legitimidade das informações prestadas e dos documentos apresentados em qualquer fase da seleção.

16.7. No período entre a divulgação do resultado e a assinatura do ACT, o proponente fica obrigado a informar qualquer evento superveniente que possa prejudicar a celebração da parceria, sobretudo quanto ao cumprimento dos requisitos e exigências previstos para celebração do ACT.

16.8. As questões não previstas neste Edital serão decididas pela Comissão de Seleção e pela Diretoria Executiva da RNP, observadas as disposições legais aplicáveis.

17. DO FORO

17.1. Fica o foro do Rio de Janeiro, com renúncia a qualquer outro, por mais privilegiado que seja eleito para dirimir as dúvidas e questões oriundas do presente Edital que não possam ser resolvidas administrativamente.

ANEXO I

MODELO SUGESTIVO DE CARTA DE ANUÊNCIA

Eu, <nome>, <cargo>, na condição de dirigente do(a) <nome da instituição>, manifesto meu apoio à proposta submetida por <nome do proponente>, <cargo do proponente> desta instituição, em atendimento ao Edital de Seleção para Cooperação em Execução de Política Pública voltada ao estabelecimento de Centros de Operações de Segurança (SOC) nos estados integrados à Rede Federada de Cibersegurança e Privacidade.
Caso nossa proposta seja uma das selecionadas, estou ciente que será solicitado a assinatura de um Acordo de Cooperação Técnica em até 30 dias após a divulgação do resultado.