Chamada Pública de Pesquisa, Desenvolvimento e Inovação da Rede Nacional de Ensino e Pesquisa (RNP)

PROJETO: Programa Hackers do Bem no Domínio Cibernético

INTRODUÇÃO

A segurança cibernética é crítica no mundo extremamente globalizado decorrente da virtual onipresença da Internet nas nações. Falhas em cibersegurança podem resultar em disrupção econômica, tensões geopolíticas e, em última instância, instabilidade social. Tratar de cibersegurança é, portanto, imperativo para qualquer nação.

A necessidade de investimento em cibersegurança é uma realidade presente tento no Brasil quanto no mundo. Com o avanço das tecnologias e a crescente dependência das empresas e governos em relação aos sistemas de informação, a cibersegurança se tornou um dos temas mais relevantes na atualidade.

Diante da pandemia de COVID-19, que impulsionou uma mudança mundial em direção ao trabalho remoto e ao aprendizado online, a cibersegurança se tornou um tópico ainda mais crítico. A transformação digital naturalmente resulta também em um conjunto de impactos positivos para os países, para os diferentes setores econômicos, para a sociedade e para os cidadãos. Em consequência, há também o aumento da dependência em cibersegurança, com a expansão dos impactos no caso de incidentes cibernéticos, que podem afetar a privacidade dos cidadãos, as operações de empresas e indústrias de variados setores, além da própria vida humana.

Somada à transformação digital, a interdependência entre infraestruturas críticas dos países leva à necessidade de profissionais qualificados para tratar das principais funções da cibersegurança, isto é, identificação, proteção, detecção, resposta e recuperação. A complexidade existente nas funções de cibersegurança aumenta com a multidisciplinaridade do tema, que envolve aspectos tecnológicos,

humanos e processuais, que se somam à multidimensionalidade que envolve diferentes camadas tecnológicas.

A cibersegurança emerge como uma nova disciplina da Computação que compreende muitas outras subáreas como o desenvolvimento de software, redes de computadores, banco de dados, sistemas distribuídos, hardware e outras. Adicionalmente, a cibersegurança também se configura como um curso interdisciplinar que inclui aspectos legais, políticas, fatores humanos, éticos e gestão de risco[1]. O reflexo mais evidente da relevância do mercado de cibersegurança é, apesar do aumento do número de incidentes cibernéticos, a falta de profissionais qualificados em cibersegurança.

De acordo com o estudo da força de trabalho em cibersegurança da (ISC)[2²], em 2020, o número de vagas não preenchidas no Brasil na área era de mais de 330 mil profissionais, enquanto no mundo esse número era de 3,1 milhões. Ao mesmo tempo, o número de startups de cibersegurança que recebem investimentos e outras que se tornam unicórnios é alto, se comparado com os mesmos números em outros setores, o que evidencia a preocupação de desenvolvimento tecnológico na área.

O **Programa Hackers do Bem no Domínio Cibernético** (ou apenas Hackers do Bem em sua forma reduzida) possui um valor estratégico para o Brasil ao contribuir diretamente com a capacitação profissional com o objetivo de fortalecer o ecossistema de cibersegurança. Os resultados esperados vão desde avanços do País em uma área crítica que afeta de uma forma holística diferentes setores econômicos e que refletem também na sociedade e na vida dos cidadãos.

GRUPO DE TRABALHO

Um Grupo de Trabalho (GT) é a designação dada a um projeto de pesquisa, desenvolvimento e inovação (PD&I) que tenha sido aprovado em resposta a uma chamada pública da RNP. Os GTs do Hackers do Bem têm como objetivo comum o desenvolvimento de projetos de PD&I colaborativos que possam demonstrar a viabilidade no uso de novos serviços, produtos e aplicações que possam beneficiar o processo de capacitação em cibersegurança, objetivo principal do Hackers do Bem.

Nesta presente chamada pública, a RNP convida a comunidade científica interessada em empreender em parceria para a criação de um Produto Minimamente Viável (do inglês MVP - Minimum Viable Product) como principal resultado do projeto de PD&I. Este MVP deve ser obrigatoriamente desenvolvido para a criação de um novo produto/serviço para o Hackers do Bem. Para tanto, a RNP irá disponibilizar seus serviços para experimentação, os chamados testbeds, que podem ser utilizados para as etapas de avaliação dos projetos de PD&I. Dessa forma, os bolsistas terão acesso a uma infraestrutura de ponta para testar e validar suas soluções, aumentando as chances de sucesso em suas iniciativas.

[1] ACM, IEEE-CS, AIS SIGSEC, IFIP WG 11.8. Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity, Chapter. 2: The cybersecurity discipline, pp. 17. 2017. [online] http://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf

[2] https://www.isc2.org/-/media/ISC2/Research/2020/Workforce-Study/ISC2ResearchDrivenWhitepaperFINAL.ashx

A composição de cada GT deve seguir as orientações descritas na seção **"Elegibilidade"** desta chamada. As propostas selecionadas deverão seguir o cronograma de entregas apresentado na seção **"Acompanhamento e Entregas"** desta chamada pública. Os componentes de software descritos na proposta, devem ser facilmente reutilizáveis, extensíveis e bem documentados, de forma a facilitar futuras atualizações. Os componentes utilizados no desenvolvimento dos resultados devem ter independência de licenças comerciais.

A duração de cada GT deve prever execução em 12 (doze) meses. Ao longo do GT, a RNP irá apoiar na adoção de ferramentas e técnicas de modelagem de negócio que auxiliem na orientação do novo serviço/produto proposto para uso no Hackers do Bem.

Espera-se que o desenvolvimento do GT seja realizado em etapas incrementais do serviço/produto e do projeto, etapas estas que permitam obter feedback de clientes/usuários reais em sucessivas iterações para a construção de relatórios e feedbacks desejados.

OBJETIVOS

O programa de bolsas de pesquisa tem como objetivo principal selecionar grupos de Pesquisa, Desenvolvimento e Inovação (PD&I) na área de cibersegurança. Essa iniciativa busca impulsionar o desenvolvimento de novos produtos e serviços de segurança da informação, abordando desafios específicos e promovendo soluções inovadoras nesse campo em constante evolução de forma a facilitar a capacitação dos alunos no Hackers do Bem.

Os grupos de pesquisa e os bolsistas selecionados terão a oportunidade de se envolver em projetos colaborativos, liderados por um coordenador de grupo de trabalho (GT), com o objetivo de desenvolver soluções e técnicas de segurança que garantam a integridade, confidencialidade e disponibilidade das informações em diferentes plataformas e ambientes digitais, com o objetivo de melhor capacitar os alunos do Hakers do Bem.

O objetivo central desta chamada pública é incentivar a submissão de propostas de produtos e artefatos que possam ser utilizados nas atividades de capacitação central em cibersegurança do projeto Hackers do Bem. Esses produtos devem estar alinhados com as necessidades de formação dos participantes e promover um ambiente de aprendizado eficaz. Alguns exemplos de propostas desejadas incluem simuladores de código aberto, emuladores de ambiente de ataques, geradores de conjuntos de dados entre outros.

Além disso, são esperadas propostas de ferramentas que possam ser utilizadas nos Pontos de Presença (POPs) da RNP e atividades relacionadas, especialmente durante as residências dos alunos. Essas ferramentas devem facilitar o desenvolvimento de habilidades práticas e oferecer suporte aos participantes durante suas experiências de trabalho. Exemplos de propostas desejadas nessa categoria incluem analisadores de tráfego, monitores especializados e detectores de ameaças.

Nesta iniciativa, busca-se alcançar o objetivo principal de prover soluções que auxiliam na formação dos alunos do Hackers do Bem. Para tanto, os seguintes objetivos secundários são elencados:

I. Identificar soluções para áreas de interesse em segurança da informação e cibersegurança.

II. Promover o desenvolvimento de artefatos tecnológicos baseados nas soluções identificadas.
III. Estimular a capacidade empreendedora e apoiar a concepção de novos empreendimentos.

Dessa forma, busca-se impulsionar a inovação e o avanço na capacitação em cibersegurança por meio da colaboração entre bolsistas, laboratórios de pesquisa e/ou startups, aproveitando a expertise da RNP e fomentando a criação de soluções eficazes e empreendimentos promissores nesse campo essencial para a proteção das informações e sistemas em um mundo cada vez mais digitalizado e interconectado.

PRODUTOS

Os GTs selecionados terão a responsabilidade de desenvolver e entregar uma série de produtos que contribuirão para o avanço na capacitação em cibersegurança. Esses produtos consistirão em:

1. **Códigos fonte dos artefatos desenvolvidos**: Os bolsistas deverão disponibilizar o código fonte dos artefatos tecnológicos desenvolvidos durante o projeto. Esses artefatos podem incluir aplicativos, sistemas, algoritmos, protocolos ou quaisquer outras soluções de segurança. O código fonte será armazenado em um repositório e estará acessível publicamente, permitindo a transparência e o compartilhamento de conhecimento.
2. **Documentação associada**: Além dos códigos fonte, os bolsistas deverão fornecer documentação associada aos artefatos desenvolvidos. Essa documentação terá o objetivo de descrever a arquitetura, funcionalidades, características técnicas e requisitos de uso dos artefatos de segurança. Essa documentação permitirá que outros pesquisadores, desenvolvedores e profissionais da área compreendam e utilizem efetivamente as soluções desenvolvidas.
3. **Relatórios Técnicos de Acompanhamento**: Os bolsistas selecionados serão responsáveis por entregar relatórios técnicos periódicos que descreverão o andamento dos seus trabalhos. Esses relatórios serão utilizados para acompanhar o progresso, identificar desafios enfrentados e discutir soluções adotadas. Eles também servirão como uma forma de comunicação efetiva entre os bolsistas, o coordenador do projeto e demais membros envolvidos.
4. **Relatórios de Avaliação de Resultados**: Ao final do projeto, os bolsistas deverão preparar relatórios de avaliação que apresentarão os resultados alcançados, destacando os benefícios e impactos das soluções desenvolvidas. Esses relatórios contribuirão para a disseminação do conhecimento gerado pelo projeto e poderão ser utilizados como base para futuras pesquisas e desenvolvimentos na área de cibersegurança.

É importante ressaltar que os produtos propostos devem estar mais próximos de soluções de produção, uma vez que serão utilizados diretamente nas atividades de capacitação e residência dos alunos. Isso significa que eles devem ser funcionais, confiáveis e capazes de atender às demandas do ambiente de aprendizado prático.

Busca-se selecionar propostas de alta qualidade que contribuam para uma experiência de capacitação enriquecedora, fornecendo recursos tecnológicos avançados e aplicáveis diretamente nas atividades do Hackers do Bem. Esses produtos e ferramentas impulsionarão a formação dos participantes,

capacitando-os a enfrentar desafios reais em cibersegurança e promovendo o desenvolvimento de competências práticas e teóricas essenciais para o setor.

CAPACITAÇÃO EMPREENDEDORA

Os projetos selecionados passarão por mentorias de capacitação empreendedora, visando fornecer suporte e orientação aos bolsistas durante o desenvolvimento de seus trabalhos. É importante ressaltar que o nível de exigência das mentorias será ajustado de acordo com as necessidades específicas de cada projeto, levando em consideração suas características e estágio de desenvolvimento.

Além das mentorias, os projetos serão acompanhados de perto pela RNP por uma equipe responsável. Esse acompanhamento será liderado por um coordenador de Pesquisa e Desenvolvimento (P&D) da RNP, que será o ponto focal para os bolsistas e estará envolvido no monitoramento e orientação dos projetos ao longo do processo. Além disso, membros do comitê gestor do Hackers do Bem ou pessoas designadas por eles também estarão envolvidos no acompanhamento, trazendo uma perspectiva adicional e contribuindo para a qualidade e alinhamento dos projetos com os objetivos do Hackers do Bem. Esse acompanhamento contínuo assegurará que os bolsistas dos grupos de pesquisa recebam a devida orientação e suporte para alcançar os melhores.

ELEGIBILIDADE

Esta chamada pública do Hackers do Bem está direcionada à comunidade científica especializada em segurança cibernética, englobando pesquisadores dedicados ao ensino e pesquisa nessa área. Além disso, startups também são bem-vindas devido ao potencial de exploração dos produtos desenvolvidos. A submissão das propostas deve ser obrigatoriamente liderada por pesquisadores da comunidade acadêmica.

Propostas que já possuam a participação de startups desde a submissão ou que indiquem a criação de uma startup ao longo do projeto terão preferência no processo de seleção. Essa abertura para startups visa estimular a transferência de tecnologia e o potencial de aplicação prática dos resultados da pesquisa em cibersegurança.

Uma proposta de GT precisa necessariamente indicar:

l. 1 (um) coordenador acadêmico
li. Equipe de bolsistas colaboradores

O coordenador acadêmico deve ser um pesquisador de uma instituição de ensino e/ou pesquisa, pública ou privada. Ele deve ser o líder da equipe, responsável pela indicação dos seus membros. O papel do coordenador acadêmico do GT é garantir que os resultados sejam o mais próximo possível da proposta aprovada.

Além do coordenador acadêmico, o GT deve ter uma equipe de colaboradores composta por alunos de doutorado, mestrado ou graduação. Estes colaboradores deverão atuar no desenvolvimento da proposta.

A coordenação acadêmica deve contribuir diretamente com os aspectos de inovação/negócio do projeto e estar atenta a estes aspectos e contribuir para que os resultados produzidos possam se aproximar ao máximo das características validadas ao longo do desenvolvimento do projeto junto aos segmentos de clientes priorizados no modelo de negócio.

A RNP irá indicar um (01) coordenador de pesquisa e desenvolvimento (P&D) de seu quadro de colaboradores, que será o responsável pelo acompanhamento da entrega dos produtos. O coordenador acadêmico estará em contato com o coordenador de P&D da RNP para acompanhamento e avaliação constante do andamento do GT.

É vedada a participação como membro do GT, seja como coordenador ou membro da equipe executora, pessoas que sejam:

i. Funcionários CLT da RNP;
ii. Membros do Conselho de Administração da RNP;
iii. Membros da Comissão de Avaliação do Contrato de Gestão (CA-MCTIC);
iiii. Membros da Comissão de Avaliação desta Chamada Pública.

STARTUPS

As propostas para esta chamada devem ser submetidas por grupos de pesquisas vinculados a Instituições de Ensino Superior (IES), tanto públicas quanto privadas. Caso haja startups associadas a essas instituições, elas também podem estar envolvidas nas propostas. No entanto, é importante ressaltar que esta chamada não se destina à seleção de startups individuais, mas sim a grupos de pesquisa que possuam parcerias com startups, ou até mesmo GTs que tenham criado startups para algum determinado produto focado nos temas dessa chamada de bolsa.

O objetivo é promover a colaboração entre laboratórios de pesquisa, instituições de ensino superior e startups, visando o desenvolvimento conjunto de novos produtos e serviços para capacitação em cibersegurança.

APRESENTAÇÃO DE PROPOSTAS

As propostas devem ter no máximo 12 páginas, usando fonte Arial 11 e espaçamento simples e devem ser submetidas utilizando o modelo disponível em https://www.rnp.br/inovacao/editais, contemplando os seguintes itens:

A. **Título** – Sigla e nome do projeto;
B. **Coordenador Acadêmico** – nome do coordenador, instituição, URL do currículo Lattes atualizado e dados de contato como e-mail e o número de telefone celular;

C. **Equipe de Colaboradores** – nome completo, instituição, URL do currículo Lattes atualizado e e-mail de contato;
D. **Tópicos de interesse** – indicação do(s) tópico(s) de interesse em que a proposta se enquadra, baseado na Seção 6 desta chamada pública;
E. **Parcerias e respectivas contrapartidas** – Informar quais as instituições participarão do projeto. Declarar explicitamente as contrapartidas financeiras e não financeiras de cada parte e como cada parte contribuirá para o sucesso do projeto. Este não é um requisito obrigatório, mas ter parcerias distribuídas no território nacional será um diferencial;
F. **Descrição da proposta**, identificando o problema e a solução – Deve ter no máximo sete (7) páginas descrevendo o problema e quem são os clientes afetados pelo problema, quais são as soluções existentes atualmente, quais os diferenciais da solução proposta neste projeto e indicar o grau de maturidade da solução em termos tecnológicos e de negócio.

O texto deve caracterizar quem são os atores atualmente impactados pelo problema, explicitando este(s) público(s) alvo. A solução proposta deve descrever os detalhes da visão de negócio e da visão do produto final do projeto que resolva minimamente o problema central identificado.

De forma mais ampla, as propostas devem conter informações suficientes para que o comitê de avaliação possa entender o que está sendo proposto, o escopo do trabalho, sua abrangência e impacto, destacando como o resultado poderá beneficiar o Hackers do Bem.

A descrição da proposta deve estar estruturada em 3 seções, distribuindo as 7 páginas da seguinte forma:

A. Sumário Executivo (máximo 1 página)
B. Desenvolvimento Tecnológico (máximo 4 páginas)
C. Modelo do Projeto (máximo 2 páginas)

No caso das parcerias indicadas, deve-se descrever o papel de cada parceiro no desenvolvimento do projeto, destacando-se em especial o papel de parceiros, se houver.

Ambiente de validação da solução proposta e documentação dos aprendizados – Descrever qual será o ambiente de validação, destacando a estratégia que será usada para tal durante o desenvolvimento.

A RNP oferece um Serviço de Testbeds composto por plataformas de experimentação, que fornecem recursos de computação e comunicação, as quais podem ser indicadas na proposta como parte do ambiente de validação.

As informações incluídas na seção de recursos financeiros também serão consideradas como parte do ambiente existente para que a RNP possa avaliar a viabilidade do projeto.

Cronograma de marcos – Apresentar um cronograma de marcos do projeto, fornecendo uma visão distribuída no tempo de como a equipe de projeto realizará o trabalho ao longo de 12 meses para alcançar a visão do projeto, a visão de produto e a entrega dos resultados.

Recursos Financeiros – A proposta deve informar os recursos necessários para a execução do projeto. Deverão ser detalhados e justificados os recursos destinados a:

Viagens – Ao longo do desenvolvimento do GT, a RNP poderá solicitar, a seu critério e arcando com todos os custos, a participação de membros do GT nas seguintes situações: em reuniões de projeto;

na representação da RNP em eventos; em eventos da RNP; e na realização de outros eventos considerados relevantes ao GT.

TÓPICOS DE INTERESSE

A cibersegurança é uma das áreas mais críticas da tecnologia atualmente, visto que as ameaças cibernéticas continuam a crescer em número e sofisticação. Diante desse cenário, a seleção de GTs é fundamental para o desenvolvimento de novos produtos e serviços na área. A lista não exaustiva de tópicos de interesse desta chamada inclui:

1. Criptografia e criptoanálise: algoritmos, protocolos e aplicações
2. Criptomoedas e mecanismos de consenso distribuído
3. Forense Computacional para análise criminalística em sistemas computacionais, Tradeoffs entre segurança e eficiência, usabilidade, custo e/ou ética
4. Auditoria e análise de riscos em sistemas computacionais
5. Análise de riscos na disseminação de informações para manipulação maliciosa, fake news, vigilância e censura em sistemas computacionais.
6. Cibersegurança abrangente e responsável na educação, engenharia social, ética, governança, proteção de propriedade intelectual e segurança centrada nas pessoas.
7. Segurança da informação baseada em aprendizado de máquina, Inteligência Artificial e privacidade em sistemas.
8. Segurança em Harware em RFIDs, cartões inteligentes, sensores, tamper-proof e tamper-evident modules
9. Segurança em Redes de Computadores, ambientes de computação em nuvem, em redes móveis e veiculares
10. Segurança em Internet das Coisas e Sistemas embarcados
11. Intrusão: detecção, prevenção e resposta
12. Segurança de sistemas para Votação Eletrônica
13. Segurança de aplicações para o Metaverso, sistemas operacionais, Banco de Dados, aplicações (e-banking, smart grids e redes sociais e etc.)
14. Ambientes de execução confiáveis
15. Controle de acesso, autenticação, biometria, confiança, gestão de identidades
16. Normatização e políticas de segurança
17. Segurança de software baseados no desenvolvimento, testes, certificação e análise de vulnerabilidades
18. Software malicioso (malware)
19. Segurança da informação no gerenciamento de dados e sistemas, proteção dos dados, anonimização e privacidade.
20. Criação de ambiente experimental para cibersegurança

SUBMISSÃO E SELEÇÃO

Os proponentes deverão enviar as propostas até o prazo máximo estipulado nesta chamada pública. Após a data limite de submissão, o comitê de avaliação avaliará as propostas enviadas e poderá

solicitar esclarecimento de dúvidas através de mensagem de e-mail. Os proponentes deverão enviar suas considerações sobre os eventuais pontos levantados pelos avaliadores em até 48h.

O arquivo texto em formato PDF contendo o projeto deverá usar o modelo de referência disponível na página de divulgação desta chamada pública. As submissões de propostas devem ser realizadas eletronicamente através do sistema JEMS no link https://jems3.sbc.org.br/hackersdobem.

A seleção dos GTs será baseada principalmente os seguintes critérios:

1. Potencial para gerar um novo produto/serviço para o Hackers do Bem
2. Viabilidade da oferta como plataforma/serviço
3. Potencial para avançar o estado-da-arte
4. Realizações e competência do grupo de pesquisa
5. Qualidade da proposta

DATAS IMPORTANTES

Divulgação da chamada pública: **30/06/2023**

Web-conferências públicas para esclarecimentos sobre a chamada pública e dúvidas. A URL onde todas as reuniões serão em https://conferenciaweb.rnp.br/rnp/chamada-pd-hackers-do-bem

Web Conferência 1: **14/07/2023 de 10h até 12h**

Web Conferência 2: **21/07/2023 de 15h até 16h**

Data limite para entrega das propostas**: 16/08/2023 até as 23h59**

Divulgação dos resultados: **24/08/2023**

Web-conferência de orientações iniciais e contratação das equipes dos GTs selecionados na sala virtual no dia **25/08/2023 de 10h até 12h**

Prazo para o envio de documentação completa para contratação: até **28/08/2023 até as 23h59**

Web-conferência de alinhamento de contrapartidas selecionados na sala virtual no dia **30/08/2023 de 10h até 12h**

Período de execução dos projetos é de 12 meses: **De 01/09/2023 até 01/09/2024**

CONTRATAÇÃO

Todos os projetos aprovados terão seus membros de equipe remunerados através do Programa de Bolsas de Incentivo à Pesquisa, Desenvolvimento e Inovação da RNP. Em havendo contrapartida por parte das proponentes, tal contrapartida poderá ser considerada para a definição da participação de cada parte na propriedade dos resultados.

GESTÃO E INFORMAÇÕES PÚBLICAS

As atividades de gestão do GT serão conduzidas pela RNP e as informações públicas serão lançadas em área determinada para a divulgação das atividades dos GTs.

Entre as informações públicas, tem-se:

l. Produtos;
li. Apresentações, artigos e demais bibliografias que sejam geradas a partir dos resultados do GT, durante a vigência do projeto, devem ser informadas ao respectivo coordenador de P&D e mencionar o apoio da RNP, e
lii. Atividades das reuniões técnicas e Workshop RNP.

Entre as informações restritas, tem-se:

liii. Listas de discussão;
liv. Documentos de trabalho e versões preliminares dos produtos, e
lv. Gerência de Projeto: ações, atividades, tarefas, status, etc

PROPRIEDADE INTELECTUAL

Propriedade dos Resultados

Conforme a Política de Propriedade Intelectual da RNP, todos os resultados intermediários e finais produzidos no âmbito do GT, envolvendo invenções, processos, métodos, programas de computador ou inovações técnicas, passíveis de proteção ou não, terão seus direitos divididos entre as instituições envolvidas na proporção e forma estabelecidas em instrumento específico. Em havendo contrapartida por parte das proponentes, esta poderá ser considerada para a definição da participação de cada parte na propriedade dos resultados.

No caso de as instituições participantes optarem por não participar como cotitulares no processo de tratamento da propriedade intelectual, os pesquisadores vinculados a elas terão garantida sua autoria e esta informação constará no registro/depósito no INPI. Em contrapartida, o pesquisador deverá fornecer todas as informações inerentes à tecnologia para que o registro da tecnologia no INPI possa ser feito.

Um acordo de entendimento será estabelecido, no início do projeto, em conjunto entre a RNP, as instituições envolvidas, a startup, quando houver, e a equipe do projeto, para descrever o entendimento inicial sobre a propriedade dos resultados, transferência de tecnologia, entre outros entendimentos com as respectivas instituições citadas na proposta.

Sigilo e Confidencialidade

As instituições envolvidas se comprometem em manter sigilo e confidencialidade sobre as informações trocadas e geradas durante e após a execução das atividades previstas na presente chamada pública e, não revelar, nem transmitir direta ou indiretamente, tais informações trocadas a terceiros que não estejam envolvidos/autorizados.

Para resultados intermediários e finais produzidos no âmbito do GT passíveis de proteção da propriedade intelectual, a RNP recomenda que sejam divulgados somente após o protocolo de pedido de proteção ao INPI, para que o requisito de novidade seja mantido. Neste caso, a RNP oferece apoio ao coordenador do GT para tomar as providências cabíveis.

Transferência de Tecnologia

Todos os resultados tecnológicos intermediários e finais produzidos no âmbito do GT, envolvendo invenções, processos, métodos, programas de computador ou inovações técnicas, passíveis de proteção ou não, com potencial de aplicação e de interesse por terceiros, terão sua transferência estabelecida em instrumento específico entre as instituições envolvidas e/ou interessadas.

Este processo acontecerá após o tratamento da proteção da propriedade intelectual dos resultados tecnológicos do GT e da identificação de empresa que tenha interesse em ser licenciada para explorar comercialmente, priorizando parceiros participante do projeto, se houver.

DÚVIDAS

Dúvidas podem ser enviadas para o e-mail: romulo.pinheiro@rnp.br

INFORMAÇÕES GERAIS

Eventuais casos omissos e situações não contempladas nesta chamada pública serão decididos pela Diretoria de Pesquisa e Desenvolvimento da RNP. A RNP se reserva ao direito de, a qualquer momento, alterar as datas do cronograma, bem como atividades relacionadas aos projetos e o prazo de entrega de candidaturas a esta chamada de bolsa.