SELEÇÃO DE PROJETOS DE PESQUISA E DESENVOLVIMENTO DO PROGRAMA HACKERS DO BEM NO DOMÍNIO CIBERNÉTICO - CICLO 2025/2026

Chamada Pública de Projetos de Pesquisa e Desenvolvimento em Cibersegurança

05 de Agosto de 2024

1. INTRODUÇÃO

A cibersegurança é uma área crítica num mundo extremamente globalizado decorrente da virtual onipresença da Internet. Falhas de segurança podem resultar em disrupção econômica, tensões geopolíticas e instabilidade social. Tratar de cibersegurança é, portanto, imperativo para qualquer nação. A necessidade de investimentos nesta área é uma realidade presente tanto 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 da sociedade no uso da tecnologia e, portanto, na cibersegurança, graças à 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 é uma disciplina da Computação que por sua vez 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, políticos, sobre fatores humanos, éticos e de 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)[2], 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 necessidade de desenvolvimento tecnológico na área.

O Programa Hackers do Bem possui um valor estratégico para o Brasil ao contribuir diretamente com a formação profissional com o objetivo de fortalecer o ecossistema de cibersegurança. Os resultados esperados incluem 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.

2. GRUPO DE TRABALHO

No contexto da Rede Nacional de Ensino e Pesquisa (RNP), um Grupo de Trabalho (GT) é a designação dada a um projeto de pesquisa e desenvolvimento (P&D) que tenha sido aprovado em resposta a uma chamada pública da RNP ou através de carta convite. Os GTs do Programa Hackers do Bem têm como objetivo comum o desenvolvimento de projetos de P&D que que possam beneficiar o processo de formação qualificada em cibersegurança.

Nesta presente chamada pública, a RNP convida a comunidade científica interessada em desenvolver um Produto Minimamente Viável (do inglês MVP - *Minimum Viable Product*) como principal resultado do projeto de P&D. Este MVP deve ser obrigatoriamente desenvolvido para a criação de um novo produto/serviço para o Programa Hackers do Bem. A RNP disponibilizará seus

[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

serviços para experimentação, o Serviço de Testbeds[3] e o GidLab[4], que poderão ser utilizados nas etapas de avaliação dos projetos de P&D.

3. OBJETIVOS

O objetivo desta chamada é selecionar Grupos de Trabalho (GTs) para desenvolver novos produtos e serviços que abordem desafios específicos e promovam soluções inovadoras para a formação qualificada e prática dos participantes do Programa Hackers do Bem. Esses produtos devem estar alinhados com as necessidades de capacitação dos participantes e devem promover um ambiente de ensino e aprendizagem eficaz. Além disso, são esperadas propostas de ferramentas que possam ser utilizadas nos Pontos de Presença (PoPs) da RNP, 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. Como objetivo secundário, esta chamada visa estimular a capacidade empreendedora e apoiar a concepção de soluções educacionais inovadoras.

Os proponentes deverão submeter, em resposta à esta chamada, propostas aderentes com os interesses do Programa, listados na seção “Eixos Temáticos e de Interesse”. 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.

Após a seleção das propostas, a execução dos projetos selecionados terá a duração de 1 ano (12 meses). Ao longo do GT, a RNP irá apoiar na adoção de ferramentas e técnicas de modelagem de negócio que auxiliem na orientação do serviço/produto proposto para uso no Programa Hackers do Bem.

4. EIXOS TEMÁTICOS E DE INTERESSE

Tema 1: Plataformas de Desafios

As plataformas de desafios oferecem um ambiente dinâmico onde os alunos podem aprender e praticar habilidades em cibersegurança através de problemas reais disponibilizados através de ambientes simulados. Estas plataformas, como as competições *Capture the Flag* (CTF), permitem

[3] https://www.rnp.br/servicos/testbeds/gidlab
[4] https://www.rnp.br/servicos/testbeds

que os participantes resolvam quebra-cabeças de segurança e desenvolvam uma compreensão aprofundada das táticas e técnicas utilizadas pelos atacantes, enquanto praticam a implementação de medidas de defesa eficazes em um ambiente controlado e replicável.

Desafios:

- Criar uma interface de usuário intuitiva e atraente que facilite a navegação dos alunos pela plataforma de desafios.
- Desenvolver trilhas de aprendizado personalizadas que se adaptem ao nível de habilidade e progresso do aluno.
- Criar sistemas que avaliem automaticamente as respostas dos alunos aos desafios, fornecendo feedback imediato.
- Incorporar elementos de gamificação, como pontos, *badges* e *rankings*, para aumentar a atratividade e o engajamento dos alunos.
- Criar conteúdo didático e desafios que abordem uma ampla gama de tópicos em cibersegurança, desde conceitos básicos até técnicas avançadas.

Tema 2: Games - Grupo de Apoio e Modelo Educacional em Cibersegurança

A gamificação tem se mostrado uma ferramenta poderosa de conscientização e de engajamento de alunos no aprendizado de cibersegurança. Tal abordagem utiliza jogos educativos e oficinas práticas para criar um ambiente de aprendizado interativo. Através de simulações de ameaças cibernéticas e sessões de mentoria, os alunos desenvolvem tanto habilidades técnicas quanto competências de trabalho em equipe e resolução de problemas, promovendo um modelo educacional inovador e eficaz.

Desafios:

- Criar jogos que ensinem conceitos de cibersegurança de maneira envolvente e interativa.
- Desenvolver programas de treinamento que ajudem os educadores a integrar a gamificação em suas práticas pedagógicas.
- Estruturar atividades que sejam educativas e divertidas, ao mesmo tempo, garantindo que os conceitos técnicos sejam compreendidos.
- Criar conteúdo didáticos e desafios que abordem uma ampla gama de tópicos em cibersegurança, desde conceitos básicos até técnicas avançadas.
- Criar soluções configuráveis, permitindo adaptar os jogos e oficinas de cibersegurança para que possam ser incorporados aos currículos escolares existentes e em atividades de conscientização.
- Possibilitar parcerias com instituições para apoiar a práticas pedagógicas colaborativas.

Tema 3: Aplicação móvel de código aberto

Desenvolvimento de aplicação móvel gratuita para conscientização e ensino que combina teoria e prática de cibersegurança de forma gamificada. Oferecendo cursos e módulos interativos sobre uma ampla gama de tópicos, a aplicação móvel deve permitir aos usuários aprender e aplicar conceitos de cibersegurança em cenários práticos. Seu código aberto promove a cocriação e colaboração entre desenvolvedores, especialistas e educadores, garantindo que a aplicação esteja sempre atualizada com as últimas tendências e práticas do mercado.

Desafios:

- Criar uma interface intuitiva e atraente para facilitar a navegação dos usuários.
- Desenvolver cursos e módulos interativos que cubram uma ampla gama de tópicos de cibersegurança.
- Incorporar elementos de gamificação, como níveis, *badges* e recompensas, para aumentar o engajamento dos usuários.
- Criar sistemas que avaliem automaticamente o progresso dos usuários e forneçam feedback imediato.
- Ser desenvolvido seguindo as boas práticas de desenvolvimento seguro de software e de design de jogos.
- Assegurar que a aplicação seja inclusiva e acessível a todos, independentemente de habilidades técnicas ou deficiências.

Tema 4: Plataforma Digital Colaborativa: Uma Jornada Imersiva no Aprendizado em Cibersegurança

Plataforma digital de ensino remoto que permite aos alunos personalizar sua jornada de aprendizado em cibersegurança. Integrando diversas plataformas educativas e utilizando metodologias ativas, o programa oferece recursos educativos variados que os alunos podem escolher com base em seus interesses. A cocriação de conteúdos e a integração com outras plataformas educativas são diferenciais que enriquecem a experiência de aprendizado e preparam os alunos para enfrentar os desafios do mundo cibernético.

Desafios:

- Criar módulos de aprendizado que possam ser personalizados para atender às necessidades e interesses individuais dos alunos.
- Criar sugestões de perfis de formação com recomendações de módulos a serem cursados.

- Garantir que o programa possa se integrar facilmente com plataformas como YouTube, Discord e outras utilizadas pelos alunos.
- Utilizar metodologias ativas para engajar os alunos e promover uma aprendizagem participativa.
- Permitir que os alunos contribuam para o desenvolvimento do conteúdo educativo, promovendo uma aprendizagem colaborativa, através de sugestões, feedbacks e pesquisa NPS.
- Utilizar infraestrutura em nuvem para suportar a plataforma de ensino remoto e garantir sua escalabilidade.
- Desenvolver métricas e métodos de avaliação que forneçam insights úteis e acionáveis para avaliação da eficácia de um programa de ensino e aprendizagem.

5. ELEGIBILIDADE

Esta chamada pública do Hackers do Bem está direcionada à comunidade científica especializada em educação em cibersegurança, englobando pesquisadores dedicados ao ensino e pesquisa nessa área pesquisas, vinculados a Instituições de Ensino Superior (IES), tanto públicas quanto privadas.

Nos GTs, a parceria com startups é estimulada devido ao potencial de exploração dos produtos desenvolvidos. 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. Entretanto, a submissão das propostas deve ser obrigatoriamente liderada por pesquisadores da comunidade acadêmica.

Uma proposta de GT precisa necessariamente indicar:

I. 1 (um) coordenador acadêmico
II. 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 ou jovens profissionais com menos de dois anos de obtenção da última formação. 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 indicará 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:

1. Funcionários CLT da RNP;
2. Funcionários CLT do SENAI-SP;
3. Membros do Conselho de Administração da RNP;
4. Membros da Comissão de Avaliação do Contrato de Gestão (CA-MCTIC);
5. Membros da Comissão de Avaliação desta Chamada Pública;
6. Pessoa que esteja atuando sob qualquer vínculo contratual com a RNP, como prestadores de serviços com contratos de pessoa física ou pessoa jurídica, estagiários ou adolescente aprendiz.

Não será permitido que um mesmo coordenador acadêmico e integrantes participem em mais de 01 (um) projeto de GT desta chamada.

6. RECURSOS E BENEFÍCIOS CONCE/DIDOS

Os recursos financeiros disponibilizados para o cumprimento dos objetivos desta Chamada Pública serão:

- **Pessoal**: o valor total máximo mensal para pessoal por Grupo de Trabalho no total é de R$11.000,00.
- I**nfraestrutura de TIC**: Esta Chamada Pública não prevê o financiamento de despesas com aquisição de equipamentos. Entretanto, há um recurso anual disponível de R$ 15.000,00 para serviços em nuvem pública, o qual pode ser utilizado no desenvolvimento dos projetos.
- **Software**: Esta Chamada Pública não prevê o financiamento de despesas com software, entretanto, deverá ser especificado na proposta a necessidade de aquisição de licenças de software, bibliotecas ou APIs que sejam imprescindíveis para a realização do projeto. A depender da justificativa e do valor da despesa, a RNP poderá considerar a inclusão desse item de despesa no projeto.
- **Viagens**: Esta Chamada Pública não prevê o repasse de recursos para despesas de viagens dos Grupos de Trabalho selecionados. Entretanto, ao longo do desenvolvimento dos GTS

selecionados, a RNP poderá convidar, a seu critério e arcando com todo os custos de viagem, membros das equipes para participarem presencialmente em workshops ou eventos organizados pela RNP.

7. APRESENTAÇÃO DE PROPOSTAS

As propostas devem ter no máximo 10 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:

1. Título – Sigla e nome do projeto;
2. Coordenador Acadêmico – nome do coordenador, instituição, URL do currículo Lattes atualizado e dados de contato como e-mail e o número de telefone celular;
3. Equipe de Colaboradores – nome completo, instituição, URL do currículo Lattes atualizado e e-mail de contato;
4. Eixo temático de interesse – indicação do(s) eixo(s) temático de interesse em que a proposta se enquadra, baseado na Seção 4 desta chamada pública;
5. 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. Deve-se descrever o papel de cada parceiro no desenvolvimento do projeto Este não é um requisito obrigatório, mas ter parcerias distribuídas no território nacional será um diferencial;
6. Descrição da proposta, identificando o problema e a solução – Deve ter no máximo cinco (5) páginas descrevendo o problema, 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 do produto final do projeto que resolva minimamente o problema central identificado. 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 serviços para experimentação, que podem ser indicados na proposta como parte do ambiente de validação.

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 Programa Hackers do Bem.
A descrição da proposta deve estar estruturada em 2 seções, distribuindo as 5 páginas da seguinte forma:

- Sumário Executivo (máximo 1 página)

- Desenvolvimento Tecnológico (máximo 4 páginas)

7. Cronograma de marcos – Deverá ser apresentado um cronograma de marcos do projeto, fornecendo uma visão distribuída no tempo de como a equipe do projeto realizará o trabalho ao longo de 12 (doze) meses para alcançar a visão da solução e a entrega dos resultados.

8. Recursos Financeiros – A proposta deve informar os recursos necessários para a execução do projeto. Apresentar o fluxo de caixa para pagamento de pessoal, informando:

- Componentes da equipe, suas respectivas funções, modalidade da bolsa solicitada, o número de horas mensais que o membro da equipe irá dedicar ao projeto e o valor em reais (R$) mensal de cada um, respeitando os limites máximo e mínimo de carga-horária e remuneração estabelecidos no Anexo I do Regulamento do Programa de Bolsas de incentivo à P&D da RNP.
- Especificar a previsão de uso dos recursos em nuvem. A soma dos recursos solicitados por GT não deve exceder R$ 15.000,00 anuais. Usar como referência as informações sobre IaaS descritas no "Catálogo de equipamentos e Serviços de nuvem pública IaaS[5]".
- O coordenador acadêmico, proponente do Grupo de Trabalho, deverá ser enquadrado na modalidade de "Pesquisador Principal".

8. DATAS IMPORTANTES

Os prazos do cronograma deste Edital são:

FASE	DATA
Divulgação desta Chamada Pública	05/08/2024
Webconferência pública para tirar dúvidas sobre este chamada, a ser realizada no endereço: https://conferenciaweb.rnp.br/rnp/chamada-pd-hackers-do-bem	26/08/2024, de 10h até 12h

[5] Catálogo de equipamentos e Serviços nuvem pública_IaaS_2021.pdf (rnp.br)

Webconferência pública 2 para tirar dúvidas sobre este chamada, a ser realizada no endereço: https://conferenciaweb.rnp.br/rnp/chamada-pd-hackers-do-bem	13/09/2024, de 15h até 16h
Data limite para entrega das propostas.	16/09/2024, até as 23h59
Divulgação do resultado da seleção	A partir de: 16/10/2024
Webconferência para orientações iniciais aos GTs selecionados. https://conferenciaweb.rnp.br/rnp/chamada-pd-hackers-do-bem	05/09/2024 às 14h
Prazo para o envio da documentação completa para a implantação das bolsas.	23/10/2024, de 10h até 12h
Período de execução dos projetos e vigência das bolsas (12 meses)	02/01/2025 até 31/12/2025.

9. SUBMISSÃO E SELEÇÃO

Os proponentes deverão enviar as propostas até o prazo máximo estipulado nesta chamada pública (16/09/2024). O processo de seleção será conduzido por um comitê de avaliação composto por especialistas da RNP, da academia e de entidades externas convidadas.

Durante o processo de avaliação, o comitê de avaliação poderá solicitar esclarecimento de dúvidas através de mensagem de e-mail enviadas pelo moderador do sistema JEMS. Os proponentes deverão enviar suas considerações sobre os eventuais pontos levantados pelos avaliadores em até 48h (quarenta e oito) após o recebimento das dúvidas, acessando a página da respectiva proposta e submetendo sua resposta através da opção *rebuttal* dentro do sistema JEMS.

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/hackersdobem2024/

A seleção dos GTs será baseada principalmente os seguintes critérios:

1. Aderência temática: este critério verifica se a proposta é pertinente com os eixos temáticos definidos na chamada.

2. Potencial para gerar um novo produto/serviço aderente ao Programa Hackers do Bem.
3. Potencial para avançar o estado-da-arte.
4. Qualidade da proposta: este critério avalia a qualidade da proposta enviada com relação aos seus objetivos e motivações, à clareza, à objetividade, à complexidade e aos resultados esperados.
5. Viabilidade técnica: este critério avalia se a proposta é viável de ser executada no prazo de 12 meses.
6. Realizações e competência do grupo de pesquisa na área de cibersegurança e ensino de cibersegurança. Este critério é avaliado por meio da análise do Currículo Lattes do(s) proponente(s).

10. CONTRATAÇÃO

Todos os projetos aprovados terão seus membros de equipe remunerados através do Programa de Bolsas de Incentivo à Pesquisa e Desenvolvimento 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.

11. ACOMPANHAMENTOS E ENTREGAS

O acompanhamento será realizado por meio da entrega de uma série de produtos e da realização de reuniões, em periodicidade a ser definida com cada GT. Nestes encontros haverá a presença do Coordenador de P&D e de uma comissão de especialistas da RNP e do Programa Hackers do Bem, de acordo com a necessidade. As responsabilidades do proponente do GT selecionado, também chamado de coordenador acadêmico, englobam a gestão do projeto, fazendo uso, bem como sua equipe, das ferramentas de apoio à gestão do projeto disponibilizadas pela RNP.

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

Os produtos consistirão em:

1. **Códigos fonte dos artefatos desenvolvidos:** Os bolsistas deverão disponibilizar os códigos 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 de códigos da RNP.

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, casos de testes, tutoriais de configuração e documentação de implantação.
3. **Demonstradores:** vídeos apresentando as soluções implementadas em funcionamento e descrevendo suas principais funcionalidades.
4. **Relatórios Técnicos e de Avaliação de Resultados:** Os bolsistas selecionados serão responsáveis por entregar Relatórios Técnicos de Acompanhamento periódicos que descreverão o andamento dos seus trabalhos, permitindo acompanhar o progresso, identificar desafios enfrentados e discutir soluções adotadas. Além disso, ao final do projeto, serão elaborados Relatórios de Avaliação de Resultados 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. Mais detalhes sobre esses relatórios e outros entregáveis estão listados a seguir:

4.1. Especificação da equipe

Antes do início do projeto, o Grupo do Trabalho deverá submeter este relatório, que deverá listar de forma completa os membros da equipe, o papel de cada um no projeto e os dados necessários para a implantação das bolsas, incluindo a modalidade e o valor solicitado para cada bolsa, respeitando os limites máximo e mínimo de carga-horária e remuneração estabelecidos no Anexo I do Regulamento do Programa de Bolsas de incentivo à P&D da RNP.

Deverá ser observado o valor máximo mensal de R$11.000,00 para despesas de pessoal, já considerando todo o Grupo de Trabalho, conforme descrito na seção “Recursos e Benefícios concedidos” deste documento. A documentação e os procedimentos necessários para a implantação das bolsas serão apresentados na webconferência para orientações iniciais aos GTs selecionados.

4.2. Relatórios de Acompanhamento

Os GTs deverão informar nestes relatórios as atividades realizadas durante um determinado período. Cada relatório deverá apresentar um conjunto de planejamentos, documentos e atividades solicitados. Outras ações podem ser incluídas nos relatórios, caso o Grupo de Trabalho julgue necessário.

4.3. 1º Relatório de Acompanhamento

É o relatório de prospecção referente ao período de janeiro até fevereiro de 2025. Neste documento deverá estar presente as seguintes atividades:

- **Cronograma de Marcos:** Apresentar um cronograma detalhado com os principais marcos do projeto, incluindo etapas de desenvolvimento, prazos, entregáveis e responsabilidades.
- **Estudo do Estado da Arte:** Analisar as tecnologias e inovações mais recentes em cibersegurança a nível nacional e internacional para fundamentar o projeto.
- **Comparativo Tecnológico:** Comparar as opções tecnológicas disponíveis para identificar as mais adequadas em termos de desempenho, custo e integração.
- **Análise das Soluções de Mercado Concorrentes:** Avaliar as soluções concorrentes existentes para identificar diferenciais e oportunidades de inovação para a proposta do projeto.

4.4. 2º Relatório de Acompanhamento

Relatório referente ao período de março de 2025 até junho de 2025. Neste documento deverá estar presente as seguintes atividades:

- Modelagem de Protótipo ou prova de conceito
- Planejamento de implementação
- Plano de testes
- Cronograma detalhado e atualizado

4.5. Relatórios Mensais de Atividades por Bolsista

- Cada Bolsista deve entregar um relatório mensal contendo uma breve descrição das atividades realizadas por cada membro contratado da equipe. Estes relatórios deverão ser assinados pelo coordenador geral do projeto para que o coordenador P&D envie para o GRH da RNP.
- O modelo do documento pode ser baixado pela URL: https://www.rnp.br/programadebolsasPDI

4.6. Relatório Final de Acompanhamento

Relatório referente ao período de julho de 2025 até dezembro de 2025. Neste documento deverá estar presente as seguintes atividades:

- Avaliação dos Resultados do Protótipo ou prova de conceito.
- Artefatos de Software
- Demonstradores produzidos

Como parte do processo de acompanhamento, os GTs também deverão apresentar nestas entregas: a documentação associada (modelagem, descrição arquitetura, casos de testes, etc.), participação em eventos (workshops, demonstrações, conferências e afins) entre outras ações que compõe a elaboração do projeto.

4.7. Landing Page – 1ª versão:

O GT deve publicar uma landing page sobre o projeto e solução proposta. Esta Landing Page poderá ser atualizada ao longo do desenvolvimento do projeto, como instrumento de validação da solução. Essencialmente a landing page deve permanecer no ar ao longo de todo o projeto como página pública e aberta como uma página de entrada sobre o GT para que qualquer pessoa na internet consiga acessá-la

4.8. Landing Page – 2ª versão:

O GT deve publicar uma segunda versão da landing page com as atualizações após o fim da capacitação empreendedora, esta LP deve ficar online até o fim do projeto.

4.9. Whitepaper

Whitepaper apresentando os resultados alcançados e descrição da solução desenvolvida. Deve apresentar também o posicionamento da solução na comunidade ou no mercado, incluindo soluções relacionadas identificadas ao longo do desenvolvimento do projeto.

O documento também deve indicar características e funcionalidades da solução, de forma ordenada conforme sua importância, identificando claramente as características e funcionalidades que ainda podem ser desenvolvidas para a evolução da solução.

4.10. Código-fonte

O código-fonte deverá ser atualizado continuamente, de acordo com o desenvolvimento dos artefatos de software e entregue no ambiente de desenvolvimento colaborativo disponibilizado pela RNP.

1.1. Eventos

Os grupos de trabalho selecionados deverão estar disponíveis para apresentações de resultados e seminários em datas que serão marcadas no decorrer da execução do projeto.

1.2. Cronograma de Entregas

Abaixo segue o cronograma de entregas idealizado para esta chamada:

Atividade	Prazo
Especificação da equipe	Até 16/09/2024
Especificação da Infraestrutura	Até 01/10/2024

1o Relatório de Acompanhamento	31/01/2025
2o Relatório de Acompanhamento	30/06/2025
Relatórios Mensais de Atividades por Bolsista	Envio Mensal
Landing Page - 1ª Versão	30/04/2025
Landing Page - 2ª Versão	30/05/2025
White Paper	15/12/2025
Relatório Final de Acompanhamento	01/12/2025

12. 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.

13. GESTÃO E INFORMAÇÕES PÚBLICAS

As atividades de gestão dos projetos serão conduzidas pela RNP e as informações públicas serão lançadas em área determinada para a divulgação das atividades dos Grupos de Trabalhos. As informações que podem ser consideradas públicas poderão ser utilizadas em ações de disseminação da RNP, SENAI-SP, SOFTEX e MCTI, bem como pelas assessorias de imprensa das instituições relacionadas aos GTs. Abaixo, listamos as informações que são consideras públicas.

Entre as informações públicas, tem-se:

- 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.
- Resultados derivados do projeto, como: manuais, código, documentação e afins.
- Notamos que não são consideradas informações públicas:
- Troca de mensagens entre participantes.
- Gravações de reuniões de acompanhamento.
- Informações gerenciais sobre o projeto

Outras informações que não foram incluídas neste escopo inicial deverão ser debatidas com o coordenador de P&D.

14. PROPRIEDADE INTELECTUAL

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.

15. PUBLICAÇÕES

Publicações científicas e qualquer outro tipo de divulgação das propostas desenvolvias com o apoio da presente Chamada deverão citar, obrigatoriamente, o apoio da RNP e demais entidades/órgãos financiadores.

a) Na seção de agradecimentos deve constar a seguinte indicação: “O presente trabalho foi realizado com o apoio do Programa Hackers do Bem no Domínio Cibernético, financiado pelo MCTI com recursos oriundos da Lei das TICs -Lei nº 8.248, de 23 de outubro de 1991, no âmbito do PPI-SOFTEX, coordenado pela Softex e publicado PDI 03, DOU 01245.023862/2022-14”.

Qualquer divulgação deverá consultar anteriormente a RNP para a verificação se os resultados a serem apresentados possuem valor comercial ou possam levar ao desenvolvimento de um produto ou método envolvendo o estabelecimento de uma propriedade intelectual.

16. DÚVIDAS

Dúvidas podem ser enviadas para o e-mail: **pd_hackersdobem@rnp.br**

17. INFORMAÇÕES GERAIS

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

A revogação ou anulação da presente chamada não gera direito a indenizações de quaisquer naturezas.

Todos os custos decorrentes da elaboração das propostas e quaisquer outras despesas correlatas à participação nesta chamada serão de inteira responsabilidade dos proponentes, não cabendo nenhuma remuneração, apoio ou indenização por parte da RNP.

As questões não previstas nesta chamada serão decididas pelo Comitê de Avaliação e pela Diretoria Executiva da RNP e, caso necessário, por autoridade superior, observadas as disposições legais aplicáveis.