

REVISTA DO



27

Workshop RNP

maio
2026

WRNP 2026 destaca

tecnologias quânticas,
inteligência artificial
e cibersegurança

Entrevistas

**Diretor-geral da RNP,
Lisandro Granville**
fala sobre soberania digital

MCTI e o Plano Brasileiro de IA
Redes de pesquisa,
supercomputação e formação
de especialistas: o Brasil
na corrida da inteligência artificial

E mais:

Conheça nossas iniciativas
em plataformas
para experimentação,
monitoramento de redes,
blockchain, redes abertas
e inovação

RNP

25 maio
a **27**
BAHIA

**Confira o material compartilhado
no 27º WRNP em**



RNP TECH NEWS

**Testando o futuro das redes
abertas e inteligentes —
e muitos outros temas
importantes para você!**

A RNP Tech News é a newsletter técnico-científica da RNP, disseminada na rede social profissional LinkedIn. Com periodicidade bimestral, você encontra artigos do interesse de pesquisadores da área de redes de computadores que façam Pesquisa, Desenvolvimento e Inovação. Além disso, a newsletter acompanha tendências sobre os principais avanços em Tecnologias da Informação e Comunicação (TICs), dentro e fora do Brasil.

**Assine
e acompanhe em:**



RNP

MINISTÉRIO DA
CULTURA

MINISTÉRIO DA
DEFESA

MINISTÉRIO DA
SAÚDE

MINISTÉRIO DAS
COMUNICAÇÕES

MINISTÉRIO DA
EDUCAÇÃO

MINISTÉRIO DA
CIÊNCIA, TECNOLOGIA
E INOVAÇÃO

GOVERNO DO
BRASIL
DO LADO DO POVO BRASILEIRO



REVISTA DO

27° Workshop RNP

maio
2026

Mensagem da Diretora de Pesquisa, Desenvolvimento e Inovação	04
Mensagem do Organizador do 27º WRNP	05
Entrevista Lisandro Granville	06
O Brasil na corrida da Inteligência Artificial	12
Comunicação segura na era quântica	15
A nova geração das redes acadêmicas	18

Experimentação e Monitoramento	21	Rede de e-Ciência	28	Colaboração e Futuro	35
Redes Abertas	40	Block chain	44	Cibersegurança	57
				PD&I Serviços Avançados	65

EXPEDIENTE
● Revista 27º WRNP

Rede Nacional de Ensino e Pesquisa
Diretor-geral: Lisandro Zambenedetti Granville

Comitê de Organização do WRNP 2026:
Coordenação Geral: Iara Machado
Coordenação Executiva: Leandro Ciuffo e Luciana Ferreira
Coordenação do Comitê de Programa: José Ferreira de Rezende e Davi Gemmer
Gerência de Comunicação e Marketing: Stela Tsirakis
Coordenação de Comunicação e Marketing: Fábio Falcão Cazes e Rafael Haruo Horigome
Arena Startups, Exposição e Demonstrações: Rafael Valle e Ana Georgia Barbosa

Projeto Editorial, Gráfico e Criação: Corcovado Comunicação Estratégica
Projeto gráfico: Andréa Miranda
Diagramação: F/damatta Design
Produção de Conteúdo e Revisão Técnica: Larriza Thurler, Ana Carolina Landi, Jaime Sousa Jr.
Fotografias: Shutterstock e banco de imagens RNP

RNP

MINISTÉRIO DA CULTURA MINISTÉRIO DA DEFESA MINISTÉRIO DA SAÚDE MINISTÉRIO DAS COMUNICAÇÕES MINISTÉRIO DA EDUCAÇÃO

GOVERNO DO
BRASIL
DO LADO DO POVO BRASILEIRO

Bem-vindos ao 27° WRNP na Praia do Forte na Bahia

É com grande satisfação que damos as boas-vindas a todos os participantes do WRNP, realizado este ano neste cenário inspirador da Praia do Forte, na Bahia. Ao reunir pesquisadores, gestores, especialistas, empreendedores e parceiros do ecossistema de inovação, este encontro reafirma o compromisso da comunidade de ensino e pesquisa com o avanço da tecnologia e com a construção de um futuro digital mais colaborativo e sustentável.

O Workshop RNP é, há mais de duas décadas, um espaço de convergência de ideias, experiências e projetos que impulsionam o desenvolvimento das tecnologias de informação e comunicação aplicadas à educação e à ciência. Ao longo desses dias, teremos a oportunidade de conhecer iniciativas inovadoras, acompanhar apresentações de projetos de pesquisa e desenvolvimento, participar de painéis estratégicos e dialogar sobre temas que estão moldando o futuro das redes avançadas e de seus serviços.



Foto: Divulgação/RNP

A programação deste ano foi cuidadosamente construída para promover a troca de conhecimento e fortalecer a conexão entre academia, governo, empresas e startups. Debates sobre inteligência artificial aplicada às redes acadêmicas, cooperação internacional, comunicação quântica e o papel das universidades no desenvolvimento de tecnologias nacionais são alguns dos destaques que irão enriquecer nossas discussões.

Mais do que um evento técnico, o WRNP é um ambiente de colaboração. Aqui, ideias encontram parceiros, projetos ganham visibilidade e novas possibilidades de cooperação surgem. É também um espaço para fortalecer nossa comunidade e ampliar o impacto das iniciativas que desenvolvemos em benefício da educação, da pesquisa e da sociedade.

Esperamos que cada participante aproveite intensamente esta oportunidade de aprendizado, networking e inspiração. Que as conversas iniciadas aqui se transformem em novas parcerias, projetos e soluções capazes de impulsionar a inovação no Brasil e além.

Sejam todos muito bem-vindos ao WRNP 2026. ●

IARA MACHADO
DIRETORA DE PESQUISA,
DESENVOLVIMENTO
E INOVAÇÃO DA RNP



27° WRNP: de olho no futuro

CAROS LEITORES,

Em 2026 trouxemos mudanças estruturais e simbólicas que refletem a evolução contínua do evento.

Pela primeira vez, o WRNP foi organizado em **duas sedes**. Nos dias **25 e 26 de maio**, as atividades se concentraram no Centro de Convenções de Praia do Forte. Já na manhã de **27 de maio**, fomos acolhidos pela **Escola Municipal Angelina Rodrigues**, marcando um gesto inédito de aproximação com a comunidade local e reforçando o compromisso da RNP com a democratização da ciência e tecnologia. Como contrapartida pela utilização do espaço, a organização do WRNP deixou como legado algumas melhorias na infraestrutura das salas utilizadas pelo evento.

O WRNP tipicamente sempre foi realizado nos primeiros dois dias do SBRC. Este ano, também inovamos ao estender nossas atividades para um **terceiro dia**, realizando uma sessão dedicada às **atualizações sobre projetos de implantação de infraestruturas regionais de pesquisa** e um **encontro da Rede de Colaboração RNP & Startups**, com foco no desenvolvimento de soluções inovadoras a partir da academia.

Temos ainda a alegria de “repatriar” momentaneamente nossa colega Daniela Brauner, ex-gerente de P&D da RNP e figura atuante na organização de edições anteriores do WRNP. Hoje atuando na



Foto: Divulgação/RNP

Géant (associação europeia de redes acadêmicas), Daniela traz uma perspectiva internacional sobre Inteligência Artificial, enriquecendo significativamente nossa programação.

Outra novidade fundamental é a implantação de uma **ação estruturada de promoção da diversidade de gênero**. Pela primeira vez, concedemos **bolsas de isenção da taxa de inscrição para alunas do sexo feminino**, incentivando a participação de jovens mulheres nas áreas de TIC e ampliando a representatividade no evento.

Por fim, celebramos uma conquista editorial: produzimos a **quinta edição desta revista**, distribuída aos participantes do WRNP, e pela primeira vez lançamos também uma versão digital em inglês, ampliando o alcance internacional das ações de P&D da RNP e fortalecendo nossa presença no cenário global.

Que o WRNP 2026 seja inspirador, inclusivo e repleto de conexões transformadoras! ●

LEANDRO CIUFFO
COORDENADOR EXECUTIVO
DO 27° WRNP



Lisandro Granville,
diretor-geral da RNP

Foto: Divulgação/RNP

‘Soberania digital não é isolamento, é autonomia de escolha’,
diz **Lisandro Granville**

PARA O DIRETOR-GERAL DA RNP, BRASIL PRECISA
ESTAR PREPARADO PARA MOMENTOS CRÍTICOS

POR **HENRIQUE GIMENES**

As discussões sobre soberania digital vêm ganhando força nos últimos anos, impulsionadas, principalmente, pela crescente dependência de dados, plataformas e infraestruturas tecnológicas. O assunto passou a integrar as agendas de desenvolvimento de países que buscam fortalecer sua capacidade científica e inovadora, como o Brasil.

Nas áreas de ciência e educação, a soberania digital assume um papel ainda mais estratégico, já que é preciso garantir conectividade avançada, segurança, identidade digital e capacidade de processamento. Para o diretor-geral da RNP, Lisandro Granville, alcançar essa soberania não significa que um país precise se isolar do cenário internacional. É justamente a cooperação que permite ampliar capacidades, compartilhar conhecimento e construir alternativas tecnológicas mais seguras e sustentáveis.

Em entrevista à **REVISTA DO WRNP**, Granville analisa os desafios da soberania digital no Brasil e discute como redes acadêmicas e infraestruturas compartilhadas podem contribuir para reduzir dependências tecnológicas e fortalecer a capacidade de inovação do país. Confira a entrevista:

REVISTA DO WRNP: Soberania digital é um tema que tem aparecido com frequência na mídia. O que significa, na prática, soberania digital para o Brasil hoje?

LISANDRO GRANVILLE: É a capacidade de um país de fazer escolhas informadas, sustentáveis e executáveis sobre infraestruturas, dados e tecnologias críticas — e sustentar essas escolhas com governança, segurança, competência técnica e previsibilidade de investimentos. Isso inclui desde conectividade, identidade e cibersegurança até armazenamento, processamento, plataformas digitais e gestão de dados. Não se trata de “produzir tudo localmente” nem de negar a interdependência global; trata-se de reduzir dependências que, em momentos críticos, se transformam em gargalos operacionais, custos imprevisíveis ou limitações de decisão.

No caso brasileiro, a soberania digital é especialmente relevante porque a economia e o setor público caminham para uma digitalização cada vez mais profunda, ao mesmo tempo em que dados e capacidade computacional se tornam insumos estratégicos. Ter soberania, portanto, é conseguir estabelecer requisitos (por exemplo, continuidade, auditabilidade, proteção de dados, interoperabilidade, portabilidade e conformidade) e ter alternativas reais quando uma tecnologia, fornecedor ou arranjo contratual deixa de

atender ao interesse público. Em outras palavras: soberania não é isolamento, é autonomia de escolha com responsabilidade.

No contexto das redes acadêmicas e do sistema de ciência, tecnologia e inovação, isso se traduz em garantir que a infraestrutura que sustenta ensino, pesquisa e inovação (conectividade avançada, federação de identidade, serviços digitais, dados e segurança) esteja alinhada aos objetivos nacionais, com arranjos de confiança compatíveis com a missão pública das instituições.

RW: Por que esse tema se tornou estratégico nos últimos anos, especialmente diante da aceleração da transformação digital e da inteligência artificial?

LG: A transformação digital já vinha avançando, mas a inteligência artificial acelerou e elevou o patamar das exigências: mais dados, mais computação, mais conectividade e mais segurança. Modelos de IA dependem de grandes volumes de dados, ambientes de processamento intensivo e cadeias complexas de software, serviços e infraestrutura. Quando esses componentes ficam concentrados em poucos atores, isso influencia não apenas o preço, mas também prazos, disponibilidade, requisitos técnicos, padrões de interoperabilidade e até as condições de uso. Para um país, isso vira um tema estratégico porque mexe com a competitividade

econômica, a capacidade científica e a continuidade de serviços críticos.

Além disso, o cenário internacional tornou mais evidente que dependências tecnológicas podem se transformar rapidamente em vulnerabilidades, por restrições comerciais, mudanças unilaterais de política de plataformas, descontinuidade de produtos, variações abruptas de custo, ou exigências contratuais difíceis de conciliar com o interesse público. O debate, então, deixou de ser apenas técnico: passou a envolver estratégia de desenvolvimento, formação de competências, sustentabilidade de longo prazo e capacidade de coordenação entre governo, academia e setor produtivo.

RW: Quais são os principais riscos para um país que depende excessivamente de tecnologias estrangeiras? E como evitar que esse debate seja tratado de forma simplista, como se soberania significasse isolamento?

LG: Os riscos se manifestam em três dimensões principais. A primeira é técnica e operacional: continuidade de serviço, capacidade de resposta a incidentes, auditoria, transparência e controle sobre componentes críticos. A segunda é econômica: a dependência pode levar a custos crescentes, pouca previsibilidade orçamentária e lock-in tecnológico, quando a migração se torna cara ou inviável. A terceira é estratégica: as dependências críticas reduzem a margem de decisão em cenários de crise, tensões geopolíticas ou mudanças regulatórias e comerciais.

Para evitar simplificações, é importante afirmar com clareza: soberania digital não é fechar portas. A ciência é colaborativa e internacional por natureza; as redes acadêmicas existem para viabilizar essa colaboração. O ponto é construir alternativas, portabilidade e capacidade de negociação, reduzindo as dependências de componentes estruturais. Em vez de “nacional versus estrangeiro” apenas, a discussão deve incluir quais ativos são críticos, quais requisitos são inegociáveis (segurança, conformidade, continuidade, interoperabilidade), quais partes

podem ser terceirizadas com segurança e quais exigem arranjos de confiança e governança mais próximos do interesse público.

RW: Soberania digital significa buscar autossuficiência total ou é possível pensar em modelos híbridos, com diversificação de parcerias e fornecedores?

LG: Autossuficiência total é, em última instância, utópica e, não raramente, indesejável. Um caminho mais consistente é o de modelos híbridos, combinando diversificação de fornecedores e rotas tecnológicas; fortalecimento de competências locais; investimento em pesquisa e inovação; e governança e contratos que evitem dependências irreversíveis.

A diversificação reduz o risco sistêmico: quando uma solução falha, encarece ou muda suas regras, o sistema não fica refém de um único caminho. E o fortalecimento de competências locais é essencial para que o país seja capaz de avaliar, operar, integrar, auditar e evoluir

Foto: Divulgação/Elea



Geradores do Centro Nacional de Dados da RNP na Elea, em São Paulo

tecnologias, mesmo quando parte delas é adquirida externamente. Soberania, nesse sentido, é menos sobre “fabricar tudo” e mais sobre ter capacidade de arquitetura, engenharia e governança: decidir, integrar e sustentar escolhas tecnológicas coerentes com o longo prazo.

RW: Como equilibrar a busca por autonomia tecnológica com a necessidade de eficiência econômica nas universidades e nas instituições públicas?

LG: Instituições públicas e universidades precisam de eficiência e sustentabilidade. Nem sempre desenvolver tudo localmente é o melhor caminho no curto prazo e, muitas vezes, nem é o papel de cada instituição individualmente. O equilíbrio exige olhar para o custo total e o risco: não apenas o preço inicial, mas também a manutenção, a capacidade de evolução, as dependências, a conformidade, a segurança e a continuidade. Soluções “baratas” no início podem se revelar caras quando a instituição fica presa a uma tecnologia, quando o orçamento oscila ou quando a exigência de segurança aumenta. É aí que entram infraestruturas compartilhadas e arranjos cooperativos: quando o sistema se organiza, ganha escala, padroniza o que faz sentido padronizar e distribui o custo de forma racional. Uma infraestrutura nacional como a RNP existe justamente para reduzir duplicações, elevar o nível de segurança e permitir que universidades e centros de pesquisa não precisem “reinventar” componentes complexos isoladamente. Autonomia, nesse modelo, não significa cada um

fazer o seu; significa o sistema ter capacidade coletiva de sustentar serviços estratégicos com qualidade e governança.

RW: Por que a soberania digital é especialmente relevante para o ambiente de educação, ciência e inovação?

LG: Porque educação e ciência lidam com produção de conhecimento, dados sensíveis e pesquisa estratégica, inclusive dados pessoais, propriedade intelectual, resultados de pesquisa e projetos de alto valor científico e tecnológico. Se a infraestrutura digital que sustenta essas atividades é frágil, insegura ou excessivamente dependente, o impacto se reflete diretamente na capacidade de inovar: desde vazamentos e interrupções até restrições no uso de dados e limitações à colaboração em grande escala.

Além disso, é nas universidades que formamos os profissionais que irão projetar, operar e proteger as infraestruturas digitais do país. Portanto, soberania digital passa por capacitação e formação de competências, mas também por oferecer um ambiente real para experimentação e evolução tecnológica. A infraestrutura acadêmica não é obviamente só “meio”; ela é parte do próprio ecossistema de inovação.

RW: Como a RNP contribui, de forma estruturante, para fortalecer a soberania digital no Brasil?

LG: A RNP contribui de forma estruturante ao combinar três dimensões: infraestrutura nacional, mecanismos de confiança e serviços avançados compartilhados. Ao operar uma

“A ECONOMIA E O SETOR PÚBLICO CAMINHAM PARA UMA DIGITALIZAÇÃO CADA VEZ MAIS PROFUNDA.”

rede acadêmica nacional de alta capacidade, interligando instituições em todo o país, a RNP sustenta um ativo estratégico para o ensino, a pesquisa e a inovação. Mas a contribuição vai além da conectividade: a RNP viabiliza arranjos de confiança para o ecossistema (como identidade e federações), além de serviços e plataformas que reduzem custos, elevam a maturidade e reforçam a autonomia do sistema.

Há também um componente essencial: a RNP atua como ambiente de integração e experimentação para a comunidade acadêmica e para projetos estratégicos, ajudando a transformar as necessidades do sistema em soluções evolutivas, com escala e governança. Isso reduz dependências críticas não por decreto, mas por construção: padrões, cooperação, capacidade de engenharia, segurança e continuidade.

RW: Em termos práticos, como a RNP apoia universidades e centros de pesquisa nesse processo?

LG: Na prática, a RNP oferece conectividade de alta capacidade e opera os Centros Nacionais de Dados (CNDs), que apoiam a oferta de serviços avançados e de ambientes de infraestrutura para necessidades compartilhadas. Em cibersegurança, a RNP mantém o Centro de Operações de Segurança (SOC) e iniciativas que apoiam a elevação da maturidade institucional, além de ações de coordenação e de resposta em rede. Soma-se a isso a oferta de soluções de identidade digital, colaboração e suporte a projetos de grande porte, elementos fundamentais para viabilizar a pesquisa colaborativa, a operação segura e a interoperabilidade entre instituições.

Esse conjunto só é possível porque a RNP tem capilaridade em todo o território nacional, por meio de seus Pontos de Presença (PoPs). E essa capilaridade, por sua vez, depende de arranjos de cooperação com instituições hospedeiras

— tipicamente universidades e institutos de pesquisa — que viabilizam a operação local, a integração com os campi e o relacionamento com a comunidade usuária. Há também um componente crítico de recursos humanos distribuídos, com equipes que operam e sustentam os PoPs nas 27 unidades federativas, garantindo a continuidade, a resposta a incidentes, a evolução técnica e a aderência aos requisitos de segurança e governança.

O resultado é duplo: por um lado, universidades e centros de pesquisa conseguem focar em sua missão, sem precisar construir do zero toda a base tecnológica; por outro, avançam em processos e capacitação, com mais governança, previsibilidade e autonomia no uso das tecnologias. Em soberania digital, esse arranjo é relevante porque cria uma infraestrutura de confiança e escala que dificilmente seria obtida de forma fragmentada.

RW: Como a RNP dialoga com redes acadêmicas internacionais e que aprendizados essa troca traz para a autonomia tecnológica do Brasil?

LG: A interação com redes acadêmicas internacionais é essencial para manter a pesquisa brasileira conectada a grandes projetos globais. Mas esse diálogo vai muito além de enlacs de alta capacidade: envolve troca contínua sobre governança, segurança, arquitetura de serviços, modelos operacionais e sustentabilidade. Ao acompanhar o que outras redes nacionais de pesquisa e educação fazem, conseguimos comparar estratégias, aprender com incidentes e decisões difíceis e adotar práticas mais sólidas e sustentáveis.

Ao mesmo tempo, compartilhar iniciativas brasileiras fortalece nossa inserção internacional e ajuda a calibrar prioridades internas: o país amplia sua capacidade de decisão ao entender, com profundidade, os trade-offs e



Foto: Divulgação/RNP

Granville: a importância da infraestrutura, pessoas e coordenação institucional para a soberania digital

as alternativas. Para a soberania digital, isso é fundamental: autonomia não se constrói no vácuo; constrói-se com conhecimento, padrões, cooperação e capacidade de escolha.

RW: Na sua visão, quais são os principais desafios para os próximos cinco a dez anos? E que mensagem o senhor deixaria para os leitores sobre o papel da RNP nesse cenário?

LG: Nos próximos cinco a dez anos, vejo três desafios centrais. O primeiro é a infraestrutura: precisamos de investimento contínuo e previsível em conectividade, segurança, dados e ambientes de computação, acompanhando a demanda crescente por IA e ciência orientada a dados. O segundo é pessoas: formação e retenção de competências em engenharia, dados, IA e cibersegurança, com trilhas de capacitação e ambientes de prática real. O terceiro é coordenação institucional: soberania digital exige alinhamento de longo prazo entre governo, academia e setor produtivo, com políticas consistentes, governança clara e sustentabilidade.

A mensagem que eu deixaria é que soberania digital não é um projeto com começo, meio e fim. É uma agenda contínua que se constrói com decisões técnicas bem fundamentadas e cooperação institucional. A RNP seguirá como infraestrutura pública de articulação do sistema de ensino e pesquisa, conectando instituições, provendo mecanismos de confiança, elevando a maturidade em segurança e sustentando serviços compartilhados. Em um mundo cada vez mais dependente de dados e IA, essa base é o que permite ao país inovar com mais autonomia, responsabilidade e capacidade de escolher. ●

“AUTONOMIA [...] SIGNIFICA O SISTEMA TER CAPACIDADE COLETIVA DE SUSTENTAR SERVIÇOS ESTRATÉGICOS COM QUALIDADE E GOVERNANÇA.”

Henrique Miguel:
"As redes acadêmicas
e a infraestrutura nacional
de pesquisa ocupam papel
estruturante no PBIA"



O Brasil na corrida da inteligência artificial

COM INVESTIMENTOS DE R\$ 23 BILHÕES ATÉ 2028, O PLANO BRASILEIRO DE INTELIGÊNCIA ARTIFICIAL IRÁ AMPLIAR REDES DE PESQUISA, SUPERCOMPUTAÇÃO E FORMAÇÃO DE ESPECIALISTAS

POR **HENRIQUE GIMENES**

Como assegurar autonomia tecnológica em um momento em que o avanço da inteligência artificial (IA) está cada vez mais concentrado em poucas empresas e países? A busca por uma infraestrutura própria de dados e capacidade computacional tornou-se uma das principais estratégias de ampliação da soberania digital. No Brasil, esse esforço vem sendo estruturado pelo Plano Brasileiro de Inteligência Artificial (PBIA), que reúne iniciativas voltadas ao desenvolvimento da tecnologia no país.

Com previsão de investimento de R\$ 23 bilhões até 2028, o PBIA foi estruturado em cinco eixos estratégicos, com iniciativas voltadas ao desenvolvimento da tecnologia no país. Entre as frentes estão o fortalecimento da infraestrutura computacional, a formação de profissionais, a aplicação da IA em serviços públicos e o estímulo à inovação empresarial. Segundo o Ministério da Ciência, Tecnologia e Inovação (MCTI), parte relevante dessas ações já começou a ser executada.

"Com base no monitoramento concluído em novembro de 2025, o plano já registrava execução financeira de R\$ 6,47 bilhões – o equivalente a 28% do total previsto. Das 54 ações estruturantes, 30 já apresentavam entregas concretas, enquanto as demais estavam em fase inicial ou de preparação", afirma Henrique Miguel, secretário de Ciência e Tecnologia para Transformação Digital do MCTI.

Um dos principais avanços está na ampliação da infraestrutura de computação de alto desempenho do país. O supercomputador Santos Dumont, operado pelo Laboratório Nacional de Computação Científica (LNCC), foi atualizado e passou de 4,6 para 18,85 petaflops de capacidade de processamento. O sistema agora conta com nova arquitetura e unidades de processamento gráfico voltadas a aplicações de IA ampliando o acesso da comunidade científica a recursos avançados de computação.

"Existe hoje uma dependência crítica de tecnologias estrangeiras, que não é um problema apenas do Brasil. O fortalecimento da infraestrutura nacional de computação de alto desempenho e de IA precisa ser tratado como uma política consistente e de longo prazo. Acompanhar a velocidade dos investimentos e das inovações associadas à inteligência artificial também é um desafio, e, por isso, é fundamental fortalecer o ecossistema nacional de ciência, tecnologia e inovação", aponta Miguel.

A expansão dessa capacidade tecnológica também está ligada ao debate sobre soberania digital, que busca dar ao país condições de desenvolver e operar tecnologias estratégicas, como infraestrutura de dados, computação de alto desempenho e sistemas de IA.

Nesse cenário, as redes acadêmicas e a infraestrutura nacional de pesquisa têm papel central ao conectar instituições de ensino e pesquisa distribuídas pelo país. Essa conexão permite que pesquisadores de diferentes regiões tenham acesso a recursos computacionais avançados e colaborem em projetos científicos que demandam grande capacidade de processamento e troca de dados.

"As redes acadêmicas e a infraestrutura nacional de pesquisa ocupam papel estruturante no PBIA, na medida em que sustentam tanto a agenda de pesquisa, desenvolvimento e inovação quanto a formação de talentos indispensáveis ao avanço da IA no país. A Rede Nacional de Ensino e Pesquisa (RNP) é a espinha dorsal da conectividade da pesquisa, ciência e educação no Brasil", ressalta o secretário.

RUMO A UMA IA BRASILEIRA

Uma infraestrutura nacional robusta também pode abrir caminho para o desenvolvimento de sistemas de IA adaptados ao contexto brasileiro, treinados com dados e conteúdos do próprio país. Isso deve ampliar a capacidade de criar ferramentas que compreendam melhor o português e detalhes da sociedade brasileira, reduzindo a dependência de plataformas desenvolvidas no exterior. Outra frente envolve organizar bases de dados nacionais para treinamento das IAs e dar suporte a projetos conduzidos por empresas e instituições de ensino e pesquisa no desenvolvimento dessas tecnologias.

“Para viabilizar esse tipo de iniciativa, é necessário apoiar instituições de ciência e tecnologia e empresas que atuam na área, com condições para sustentar equipes qualificadas e investimentos contínuos em pesquisa e desenvolvimento.”

Foto: Divulgação/RNP



“Outro desafio é acompanhar a velocidade dos investimentos e das inovações tecnológicas associadas à IA. É preciso apoiar todo o ecossistema nacional de ciência, tecnologia e inovação, priorizando as rotas tecnológicas que podem trazer maior retorno para o país”, destaca.

A formação de profissionais capazes de atuar no desenvolvimento e na aplicação da inteligência artificial é um dos pilares centrais do PBIA. A ampliação dessa base de talentos é vista como condição essencial para que o país acompanhe o ritmo acelerado das inovações no setor.

“É o eixo com maior percentual de ações com entregas”, explica Miguel. “Na educação básica, a 1ª Olimpíada Nacional de IA mobilizou 716 mil estudantes, e quatro representantes brasileiros participaram da competição internacional em Pequim, em agosto de 2025. No ensino superior, foram criadas 8.104 novas vagas em graduação em IA em 2024, superando a meta anual de 5 mil. Entre 2022 e 2025, o CNPq apoiou 773 mestrandos e 500 doutorandos na área. Há previsão de R\$ 194,2 milhões em bolsas de graduação e pós-graduação e R\$ 152 milhões em doutoramentos no exterior até 2028”, detalha o secretário. •

Comunicação segura na era quântica

AVANÇOS NA COMPUTAÇÃO IMPULSIONAM O DESENVOLVIMENTO DE NOVAS FORMAS DE PROTEGER DADOS

POR **HENRIQUE GIMENES**

Em um mundo cada vez mais digitalizado, manter dados protegidos deixou de ser apenas uma preocupação técnica para se tornar uma questão estratégica. Da internet doméstica às redes acadêmicas e governamentais, a criptografia é um dos pilares que sustentam a comunicação digital e as transações online. No entanto, a próxima geração de processamento – em especial a computação quântica – pode redefinir os padrões de segurança que hoje estruturam a proteção de dados.

Para lidar com esse potencial cenário, pesquisadores trabalham na chamada comunicação quântica, um conjunto de técnicas que usa propriedades da física quântica para tornar a troca de informações mais segura. Uma das aplicações mais conhecidas é a criptografia quântica, usada principalmente na geração e distribuição de chaves criptográficas. Diferentemente dos sistemas tradicionais, baseados em algoritmos matemáticos, esse modelo foi pensado para um cenário em que o poder computacional cresce rapidamente. Nesse contexto, proteger dados sensíveis, como transações bancárias

Foto: Divulgação/RNP



e comunicações governamentais, torna-se cada vez mais importante, assim como garantir maior soberania digital.

“Na criptografia quântica, a segurança está baseada nas leis da Física. Não importa quanto poder de computação você tenha, não é possível quebrar essa chave sem alterar o sistema e ser detectado. Hoje os computadores quânticos ainda não conseguem romper as chaves mais robustas, mas a evolução é rápida. Por isso, essa transição precisa ser planejada. E não é só comprar um equipamento e conectar que está tudo resolvido. É um processo trabalhoso, que exige organização e estratégia”, explica Valéria Loureiro, coordenadora do Centro de Competências Embrapii (Empresa Brasileira de Pesquisa e Inovação na Indústria) em Tecnologias Quânticas no Senai Cimatec.



Foto: Divulgação/RNP

Para Valéria, há necessidade de preparar o Brasil para uma nova era de segurança digital

O desafio não está apenas na tecnologia, mas também no preparo para que ela seja adotada. Um dos primeiros passos é entender quais mecanismos de segurança já estão em uso e onde estão as fragilidades. Muitas organizações ainda operam com soluções antigas, sem ter clareza do nível de proteção que oferecem. Além disso, é preciso garantir que a infraestrutura de comunicação esteja pronta para esse desafio. O Brasil já conta com um grande volume de fibras ópticas conectando o país, incluindo redes acadêmicas e projetos de infovias em diferentes regiões, como as operadas pela RNP (Rede Nacional de Ensino e Pesquisa). Ainda assim, a expansão e a modernização dessas redes podem ser necessárias para acompanhar as tecnologias emergentes.

“Uma das grandes questões é a formação de pessoal. Existem poucas pessoas formadas no mercado nessa área. Quem domina a parte de quântica vem da Física e não sabe fazer Engenharia, e os engenheiros não sabem da Física. Juntar esses dois mundos é essencial para levar essa tecnologia ao mercado. Se a gente não fizer isso, corre o risco de ficar dependente de tecnologia totalmente importada e ter que fazer essa transição às pressas”, aponta Valéria.

O FUTURO DA COMUNICAÇÃO SERÁ QUÂNTICO?

A comunicação quântica é vista como uma evolução das tecnologias atuais de segurança digital, mas não deve substituir o modelo clássico de transmissão de dados. A tendência é que os dados continuem circulando pelos sistemas de comunicação tradicionais, enquanto as chaves criptográficas passam a ser geradas por métodos quânticos. Na prática, essa combinação pode ampliar a segurança das redes sem a necessidade de substituir a infraestrutura que já está em funcionamento.

Apesar de ser uma tecnologia em desenvolvimento, a comunicação quântica já está sendo utilizada em alguns países. Governos, universidades

e empresas de telecomunicações vêm testando diferentes modelos de rede e avaliando como essas soluções podem ser integradas às infraestruturas de comunicação existentes.

A China está entre os países mais avançados nesta área e já tem redes sendo usadas, inclusive no setor bancário. Os chineses construíram uma rede de longa distância que interliga várias cidades e, dentro delas, redes metropolitanas que geram essas chaves criptográficas para proteger as comunicações. Na Europa também existem várias iniciativas em andamento para testar como essa tecnologia pode funcionar na prática”, afirma a coordenadora do Centro de Competências Embrapii em Tecnologias Quânticas no Senai Cimatec.

Outro ponto em discussão trata de como essas tecnologias devem chegar aos usuários. Uma possibilidade é a criação de redes quânticas privadas por organizações que já possuem infraestrutura própria de fibra óptica, como bancos ou instituições governamentais. Outra alternativa seria a oferta de geração de chaves quânticas como um serviço adicional de segurança por parte das operadoras de telecomunicações.

Pesquisadores também já trabalham em soluções para lidar com a segurança digital na era da comunicação quântica. Uma frente que vem ganhando atenção é a chamada criptografia pós-quântica. Diferentemente da comunicação quântica, que gera chaves criptográficas usando propriedades da física, essa abordagem busca criar novos algoritmos capazes de resistir a ataques de futuros computadores quânticos.

“Muita gente acha que os sistemas pós-quânticos seriam a evolução da comunicação quântica, mas não é bem assim. Eles ainda usam algoritmos clássicos, só que de uma forma muito mais complexa do que a usada atualmente, na expectativa de que um computador quântico não consiga quebrar. Mas é importante considerar que, quando se fala em uma internet quântica, isso ainda está relativamente distante. É algo que pode levar de 10 a 15 anos. E a tendência é que a comunicação quântica seja usada apenas em aplicações que realmente exijam um nível de segurança muito mais alto, enquanto a maior parte do tráfego continuará utilizando os sistemas de comunicação tradicionais”, destaca Valéria Loureiro. ●

“MUITAS ORGANIZAÇÕES AINDA OPERAM COM SOLUÇÕES ANTIGAS, SEM TER CLAREZA DO NÍVEL DE PROTEÇÃO QUE OFERECEM.”



A nova geração das redes acadêmicas

POR LARRIZA THURLER E ANA CAROLINA LANDI

Durante décadas, redes acadêmicas foram associadas sobretudo à conectividade. Garantir links estáveis entre universidades, centros de pesquisa e instituições científicas era a missão central dessas infraestruturas. Hoje, porém, esse papel vem se ampliando rapidamente, acompanhando a transformação da própria ciência.

Uma das pessoas que acompanhou essa evolução de perto foi Daniela Brauner. Professora da UFRGS e coordenadora de IA da rede acadêmica europeia GÉANT, em Cambridge (Reino Unido), ela conhece a RNP desde o início da sua carreira, tendo atuado na instituição e, posteriormente, como pesquisadora colaboradora em projetos ligados à rede acadêmica brasileira.

“Conheço a RNP desde a fase em que ela era essencialmente uma infraestrutura de rede”, lembra. Na época, trabalhando com suporte de redes em uma universidade, a RNP aparecia nas conversas principalmente quando havia problemas de conectividade.

COM O AVANÇO DA IA, AS NRENS EVOLUEM DE INFRAESTRUTURAS DE CONECTIVIDADE PARA PLATAFORMAS DIGITAIS QUE INTEGRAM DADOS, COMPUTAÇÃO AVANÇADA E NOVOS SERVIÇOS DIGITAIS PARA A CIÊNCIA

Desde então, no entanto, o papel das redes nacionais de pesquisa e educação, as chamadas NRENs, ampliou-se significativamente. “As NRENs deixaram de ser apenas provedoras de conectividade e passaram a atuar como plataformas digitais integradas para ciência e educação”, afirma. “Elas atualmente têm a possibilidade de se posicionarem como atores estratégicos na transformação digital do ecossistema de educação e pesquisa em seus países e terem papel atuante no ecossistema nacional de IA”.

O IMPACTO DA INTELIGÊNCIA ARTIFICIAL

A ascensão da inteligência artificial está acelerando essa transformação. Modelos de IA demandam grandes volumes de dados, infraestrutura computacional intensiva e redes de alto desempenho capazes de conectar centros de supercomputação, repositórios científicos e instituições de pesquisa distribuídas.

Na Europa, esse movimento tem sido acompanhado por uma estratégia coordenada que combina regulação, investimento em infraestrutura e fortalecimento do ecossistema de inovação.

Entre os marcos recentes estão o EU AI Act, que estabelece diretrizes para o desenvolvimento da tecnologia, e iniciativas como o EuroHPC Joint Undertaking, voltado ao financiamento de supercomputadores e infraestrutura avançada para IA.

As redes acadêmicas já ocupavam uma posição central, mas nesse cenário seu papel também está evoluindo. “Agora, muitas dessas organizações que já operavam serviços de *cloud* ou HPC estão evoluindo para GPUs, plataformas de dados e até oferecendo outros serviços, tais como IA generativa para ensino e pesquisa”, comenta Daniela. “As NRENs estão participando de importantes consórcios com outras organizações, colaborando em grandes projetos de infraestrutura de IA na Europa”.

O DESAFIO DA SOBERANIA DIGITAL

A expansão dessas capacidades também está ligada ao debate sobre a soberania digital e a atração e retenção de talentos. “As NRENs já operam infraestruturas de conectividade soberanas para universidades e institutos de pesquisa. Expandir essa ideia para outros serviços digitais parece um caminho natural”, observa Daniela.

Na prática, muitas NRENs estão atuando como integradoras de serviços, como ambientes digitais de pesquisa (Digital Research Environments), e plataformas que permitem a estudantes e pesquisadores utilizarem ferramentas de IA generativa escolhendo entre diferentes modelos, muitas vezes baseados em tecnologias abertas.

Outro elemento importante é a coordenação europeia na negociação com grandes provedores

“AS NRENS PODEM SE POSICIONAR COMO ATORES ESTRATÉGICOS NA TRANSFORMAÇÃO DIGITAL DO ECOSSISTEMA DE EDUCAÇÃO E PESQUISA.”

de nuvem, com frameworks contratuais comuns que fortalecem o poder de negociação das instituições acadêmicas. Ao mesmo tempo, políticas públicas têm incentivado o desenvolvimento de modelos de IA abertos e o fortalecimento do ecossistema de inovação europeu, incluindo startups e pequenas empresas que desenvolvem tecnologias estratégicas para ciência e educação.

COOPERAÇÃO INTERNACIONAL E DIVERSIDADE DE DADOS

A cooperação internacional ganha, portanto, ainda mais relevância. Para Daniela, a colaboração entre Brasil e Europa pode contribuir para o desenvolvimento de modelos de IA mais robustos e representativos. “A diversidade cultural e científica entre Europa e América Latina é extremamente valiosa para o desenvolvimento de modelos de IA menos enviesados”, afirma.

O compartilhamento de dados científicos também aparece como uma oportunidade relevante. Informações provenientes de áreas como biodiversidade, clima e agricultura, nas quais o Brasil possui grande riqueza de dados, são altamente valorizadas em pesquisas internacionais.

Além disso, o país apresenta características que podem favorecer a experimentação tecnológica. “O Brasil possui um mercado digital de escala continental sob um arcabouço regulatório relativamente unificado”, destaca Daniela. Esse cenário pode facilitar a adoção e o teste de novas soluções baseadas em inteligência artificial em grande escala.

Fortalecer colaborações entre universidades, centros de pesquisa e ecossistemas de startups pode ampliar as oportunidades de inovação e acelerar o desenvolvimento de tecnologias estratégicas para ciência e educação. •

Foto: Divulgação/RNP



Daniela destaca que a IA está acelerando a transformação do papel das NREns

EXPERIMENTAÇÃO E MONITORAMENTO

- 22 Testbeds **Laboratório Nacional Multiusuário da RNP**
- 23 **MonIPê:** Plataforma de Homologação da Rede Ipê
- 24 **Comitê Técnico** de Monitoramento de Redes (CT-Mon)
- 25 **Dados de Rede** para pesquisa
- 26 **A Evolução** dos mapas RNP
- 27 **SCIERA:** Colaboração Internacional para uma Nova Arquitetura da Internet

Testbeds

O Laboratório Nacional Multiusuário da RNP

INFRAESTRUTURA MULTITECNOLÓGICA PARA PESQUISA E INOVAÇÃO

O Laboratório Nacional Multiusuário, operado pela RNP, é uma infraestrutura multi-tecnológica e estratégica voltada à pesquisa, ao desenvolvimento e à inovação que permite validação de experimentos em ambientes controlados e interconectados em escala nacional. Seu propósito é oferecer a comunidade acadêmica, centros de pesquisa, startups e parceiros institucionais um ambiente distribuído, flexível e de alto desempenho para experimentação em tecnologias da informação e comunicação (TICs). O Laboratório viabiliza testes e validações em múltiplos domínios das TICs, como redes avançadas, 5G/6G, IoT, computação em nuvem, edge computing, blockchain, cibersegurança, inteligência artificial, aplicações distribuídas e novas arquiteturas de Internet. As experimentações ocorrem em infraestruturas reais, o que possibilita avaliações técnicas, provas de conceito e análises de desempenho em condições próximas ao mundo real. Ao integrar infraestrutura, suporte especializado, conhecimento técnico e articulação nacional, o Laboratório amplia as possibilidades de pesquisa aplicada e formação de recursos humanos qualificados. A iniciativa contribui para reduzir barreiras de acesso a ambientes complexos, estimular a colaboração entre instituições e fortalecer o papel da RNP como habilitadora da ciência, do ensino e da inovação em TICs no Brasil.



**TECNOLOGIAS,
PESSOAS E PROPÓSITO
EM APOIAR PESQUISA,
ENSINO E INOVAÇÃO
EM TICS NO BRASIL**



FICHA TÉCNICA

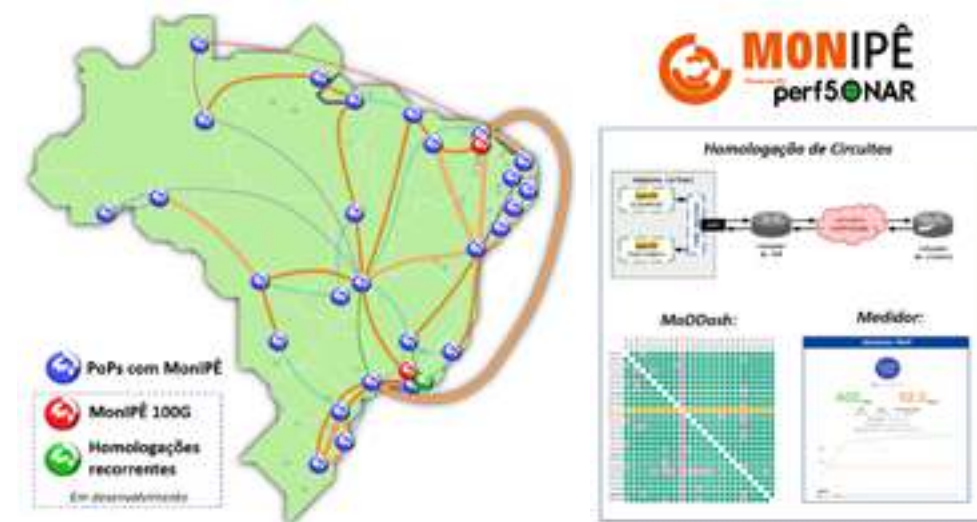
COORDENADOR-GERAL/ACADÊMICO:
Gustavo Neves Dias (RNP),
gustavo.dias@rnp.br

COORDENADOR-ASSISTENTE:
Leandro Mondin (RNP), leandro.mondin@rnp.br

EQUIPE:
Maria Elenice Pedrosa, Janssen Martins, Cesar Gama, Bruno Nascimento



QR CODE



MonIPÊ: Plataforma de Homologação da Rede Ipê

EVOLUÇÃO CONTÍNUA NA MEDIÇÃO DE QUALIDADE DAS REDES

O MonIPÊ é a plataforma da RNP para medições e homologações de circuitos que conectam as organizações usuários do Sistema RNP à Rede Ipê. Inicialmente utilizado para aferições de latência e jitter entre os Pontos de Presença (PoPs), o sistema evoluiu gradualmente e se consolidou como ferramenta de referência para validação de novos enlaces, upgrades de capacidade e mudanças de fornecedor. Sua adoção foi impulsionada pelas customizações desenvolvidas pela equipe de P&D que trouxeram flexibilidade da solução permitindo padronizar e dar maior transparência ao processo de certificação de circuitos. Entre as suas principais funcionalidades estão a criação de roteiros de homologação, o agendamento e a execução automatizada de testes, a definição de critérios objetivos de aprovação, a geração de relatórios detalhados e o armazenamento do histórico completo das medições. Acessível por meio de interface Web simples e centralizada, o MonIPÊ garante rastreabilidade, comparabilidade de resultados e maior eficiência operacional. Essas funcionalidades foram viabilizadas pelo domínio técnico da RNP sobre o perfSONAR e pela participação ativa no consórcio internacional responsável por sua manutenção e evolução. O roadmap 2026/2027 prevê novas melhorias, incluindo ampliação da capacidade de homologação de enlaces de até 10 Gbps em mais PoPs, avaliação contínua de vazão sem impacto às instituições e suporte à certificação de circuitos de até 100 Gbit/s.



FICHA TÉCNICA

COORDENADOR-GERAL/ACADÊMICO:
Gustavo Neves Dias (RNP),
gustavo.dias@rnp.br

COORDENADOR-ASSISTENTE:
Marcos Felipe Schwarz (RNP),
marcos.schwarz@rnp.br

EQUIPE:
Leandro Mondin, Daniel Neto, Elenice Pedrosa, Janssen Martins, Cesar Gama, João Bitencourt, Rafaela Fonseca, Robson Santos, Ronan Oliveira, Elder Storck, Thais Fernandes

**MEDIÇÕES
AVANÇADAS
GARANTINDO
A QUALIDADE
DAS REDES**

Comitê Técnico de Monitoramento de Redes (CT-Mon)

CT-MON IMPULSIONANDO PESQUISA COM DADOS DE MONITORAMENTO

Desde 2011, a necessidade de acompanhar mudanças técnicas e científicas no monitoramento de tráfego impulsiona as atividades do Comitê Técnico de Monitoramento (CT-Mon) da RNP. O grupo reúne pesquisadores, profissionais de operação de redes e representantes do serviço MonIPÊ para prospectar tecnologias e formular recomendações para os serviços de monitoramento. A infraestrutura operada pela RNP gera e armazena dados de desempenho de redes. Para transformar essas informações em oportunidades de pesquisa, o comitê promoveu, em 2025, o segundo Desafio de Dados de monitoramento do backbone da RNP, que contou com a participação de 15 equipes de universidades brasileiras, das quais três foram vencedoras. Os resultados foram publicados

em conferências internacionais. Outra iniciativa importante foi a realização de encontros com pesquisadores internacionais renomados sobre medições e monitoramento de redes, como Lin Wang (Paderborn University), Fabrício Murai (WPI), Aruna Balasubramanian (SUNY Stonybrook), Lucianna Kiffer (IMDEA, Espanha), Amir Houmansadr (UMass-Amherst) e Adrian Perrig (ETH Zürich). Em 2026, o CT-Mon direciona seu escopo para desafios de monitoramento levantados pela RNP, visando ao fornecimento de ferramentas de acesso aos dados, à padronização de métricas e à aplicação de soluções que permitam às instituições analisarem o tráfego de suas infraestruturas de forma interoperável, além da realização do 3º Data Challenge do CT-Mon/RNP. •

TRANSFORMANDO DADOS DE MONITORAMENTO DA RNP EM PESQUISA



FICHA TÉCNICA

COORDENADOR-GERAL/ACADÊMICO:

Antônio Augusto de Aragão Rocha (UFF),
arocha@ic.uff.br

COORDENADOR-ASSISTENTE:

Daniel Otavio da Cunha Cota (UFF),
danielotavio@id.uff.br

EQUIPE:

Gustavo Araújo (RNP) e José Ferreira de Rezende (RNP)



ENTIDADES PARCEIRAS

UFF



QR CODE

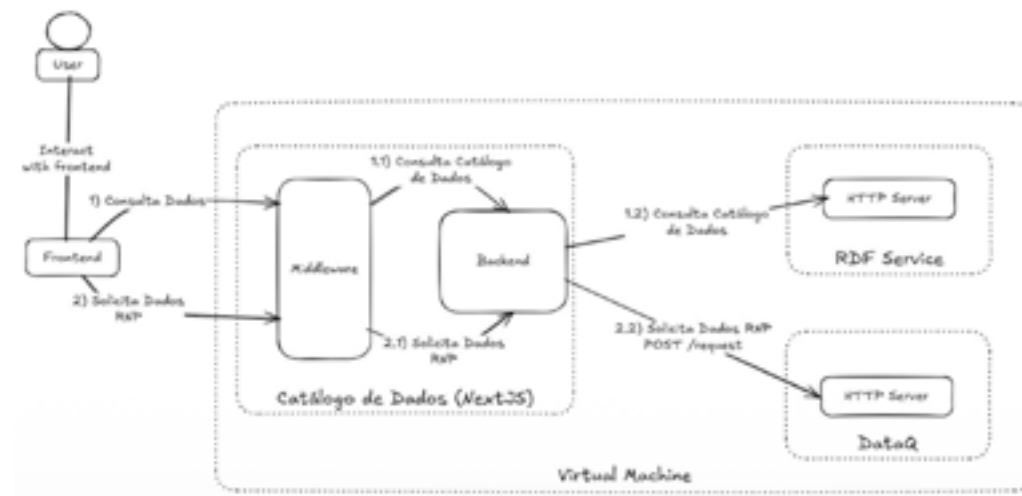


Dados de Rede para pesquisa

RNP TRANSFORMA DADOS OPERACIONAIS EM ATIVOS PARA A CIÊNCIA

A Rede Nacional de Ensino e Pesquisa (RNP) opera uma infraestrutura complexa e de capilaridade nacional que gera continuamente volumes massivos de dados operacionais. Esses dados representam um ativo estratégico subutilizado para fins científicos, criando uma lacuna entre o potencial gerado pela operação da RNP e as necessidades da comunidade de pesquisa brasileira em Inteligência Artificial e ciência de dados. Este projeto visa preencher essa lacuna por meio de objetivos específicos e mensuráveis. O objetivo geral é fomentar, promover e facilitar o uso eficiente de dados de rede para pesquisa em IA e ciência de dados, transformando dados operacionais brutos em um ativo estratégico para a comunidade científica. Em parceria

com o CT-Mon, o projeto busca: (i) catalogar, processar e transferir um recorte qualificado de informações para a plataforma Lakehouse da RNP, tratando e anonimizando os dados de forma estruturada e segura; (ii) desenvolver e implantar um portal web centralizado que permita pesquisadores descobrir conjuntos de dados, acessar dicionários e solicitar acesso; (iii) promover a disseminação ativa do repositório em eventos acadêmicos, workshops e congressos; e (iv) validar a relevância dos dados através da publicação de artigos científicos que demonstrem sua aplicabilidade em pesquisas de IA e redes. Esses objetivos ampliam o papel da RNP no ecossistema de CT&I, posicionando-a como fomentadora direta de pesquisas de ponta no Brasil. •



FICHA TÉCNICA

COORDENADOR-GERAL/ACADÊMICO:

Antônio Augusto de Aragão Rocha (UFF),
arocha@ic.uff.br

COORDENADOR-ASSISTENTE:

Lucas Bondan (RNP),
lucas.bondan@rnp.br

EQUIPE:

Marcos Laje, Daniel Oliveira, Nilson Damasceno, Rodrigo Chimelli, Marcelo Nobrega, João de Moraes, Gustavo Araújo, Marcos Schwarz, Daniel Neto, Filippio Venturini



ENTIDADES PARCEIRAS

UFF



A Evolução dos Mapas RNP

INOVAÇÕES DO CHAMELEON MAP E GREN MAP PARA REDES ACADÊMICAS

Desde 2022, a necessidade de aprimorar o alcance, a visibilidade e a comunicação das diversas iniciativas desenvolvidas pela RNP impulsionou a criação do projeto Mapa de Infraestruturas. O projeto visa oferecer uma ferramenta de visualização geolocalizada para representar esses projetos, demonstrando seu alcance nacional e como os pontos de interesse se interconectam. Atualmente, a iniciativa é dividida em dois pilares principais: Chameleon Map e GREN Map. A ferramenta Chameleon Map já é aplicada em diversos contextos, como cibersegurança, blockchain e a própria rede da RNP, entre outros. No momento, o Chameleon passa por uma transformação estrutural: em vez de atuar como um software stand-alone,

está sendo adaptado para o modelo SaaS (Software as a Service). Com a introdução de um painel administrativo, os usuários poderão criar seus mapas com muito mais simplicidade e autonomia. Além disso, estamos adotando o modelo Open Source (código aberto), disponibilizando o código ao público para incentivar o engajamento de novos contribuidores. Em paralelo, também atuamos no GREN Map, que funciona como um hub de colaboração focado na compreensão da topologia das redes acadêmicas. O grupo dedica-se à padronização, ao armazenamento e à visualização de dados, superando a fragmentação histórica dessas informações e permitindo que diferentes redes acadêmicas descrevam suas infraestruturas de forma interoperável. ●

**MAPAS RNP EVOLUEM
TRAZENDO VISIBILIDADE,
AUTONOMIA E COLABORAÇÃO
COM REDES ACADÊMICAS**



FICHA TÉCNICA

COORDENADOR-GERAL/ACADÊMICO:
Luciano Gaspari (UFRGS), paschoal@inf.ufrgs.br

COORDENADOR-ASSISTENTE:
Gustavo Araújo (RNP), gustavo.araujo@rnp.br

EQUIPE:
Gabriel Vassoler (RNP), Lisandro Granville (RNP), Eduardo Peretto (UFRGS), Leonardo Lauryel (UFRGS), Narciso Filho (UFRGS), Hugo Romão (UFRR)



ENTIDADES PARCEIRAS

RNP, UFRGS, UFRR e GNA-G



QR CODE



SCIARA: Colaboração Internacional para uma Nova Arquitetura da Internet

A REDE DE COLABORAÇÃO PARA EDUCAÇÃO E PESQUISA EM SCION

Já é possível que instituições de ensino e pesquisa no Brasil realizem experimentações e pesquisas na rede de colaboração SCIARA (SCION Education, Research and Academic), uma infraestrutura global dedicada ao desenvolvimento e à avaliação da arquitetura de Internet baseada em SCION (Scalability, Control and Isolation On Next-Generation Network). A iniciativa reúne importantes redes acadêmicas e instituições de pesquisa, como GÉANT, Internet2 e KREONET, criando um ambiente colaborativo para experimentação em redes de próxima geração. Por meio do Laboratório Nacional Multiusuário, a RNP tem viabilizado a adesão de instituições brasileiras à rede SCIARA, permitindo que participem com seus próprios ASes SCION nesse ambiente global de testes.

Nesse contexto, pesquisadores e estudantes podem desenvolver estudos diretamente sobre a arquitetura SCION, explorando temas como segurança de roteamento interdomínios, resiliência a falhas e ataques, comunicação multicaminhos, controle de rotas e soberania de dados. A rede SCIARA também promove a colaboração entre universidades e centros de pesquisa de diferentes países, possibilitando experimentos conjuntos e o desenvolvimento de soluções em redes seguras, cibersegurança e aplicações de baixa latência. Com essa iniciativa, a RNP fortalece a inserção do Brasil no ecossistema internacional de pesquisa em redes e consolida o papel do país na transição para arquiteturas de Internet mais seguras, transparentes e resilientes. ●



**RNP CONECTANDO
INSTITUIÇÕES BRASILEIRAS
À REDE GLOBAL
DE PESQUISA SCIARA**



FICHA TÉCNICA

COORDENADOR-GERAL/ACADÊMICO:
Leandro Mondin (RNP), leandro.mondin@rnp.br

COORDENADORA-ASSISTENTE:
Maria Elenice Pedrosa (RNP), elenice.pedrosa@rnp.br

EQUIPE:
Janssen Martins (RNP) e Cesar Gama (RNP)



QR CODE



E-CIÊNCIA

- 29 Rede de **e-Ciência**
- 31 **P&D e Prospecção Tecnológica** na Rede de e-Ciência
- 32 Repositórios de Dados de Pesquisa **para a Rede de e-Ciência**
- 34 **P&D para Gestão de Identidade** e Acesso para Rede de e-Ciência

Rede de e-Ciência

REDE DE ALTO DESEMPENHO PARA DADOS CIENTÍFICOS

A Rede de e-Ciência é uma infraestrutura digital segura de alto desempenho dedicada a centros de pesquisa que possuem demandas avançadas de processamento, análise, transmissão e armazenamento de grandes volumes de dados. Diferentemente da Rede Ipê, a Rede de e-Ciência oferecerá políticas e serviços especializados para grandes fluxos de dados científicos, com robustas medidas de segurança. Essa infraestrutura conectará principalmente Instituições de Ciência e Tecnologia (ICTs) de ponta, como centros de supercomputação, laboratórios multiusuários e outros ambientes de pesquisa intensiva em dados. Para viabilizar essa conectividade de altíssimo desempenho, a

RNP está renovando sua infraestrutura óptica nacional, tornando o backbone escalável para múltiplos canais de 100 Gbps. Com isso, cada instituição participante contará com largura de banda abundante, experiência otimizada e serviços sob medida para suas demandas específicas. A construção da Rede de e-Ciência está ocorrendo através de três frentes de financiamento. A principal delas integra o programa estruturante Conecta (MCTI/FNDCT, prioritário do Novo PAC 2023-2026) para conexão de 12 ICTs. Além disso, uma cooperação RNP-Petrobras integrará seis novos laboratórios de pesquisa, enquanto um acordo com o Ministério da Saúde agregará outros cinco até 2028. •

Rede Ipê	A primeira rede de Internet do Brasil, em evolução desde 1992	Em construção, com previsão de conclusão em 2027	Rede de e-Ciência
	+1300 pontos conectados	~20 pontos conectados	
	Com acesso aberto à Internet	Sem acesso à Internet	
	Acessível globalmente a partir de qualquer ponto de conexão à Internet	Acessível apenas a partir dos servidores de transferência de dados homologados das instituições participantes da rede	
	Conectividade até a borda da instituição	Conectividade até o servidor de armazenamento de dados científicos da instituição	
	Não otimizada para transferência de dados Configuração padrão para aplicações convencionais (e-mail, vídeo, serviços online etc)	Nativamente otimizada para transferências de dados com alto desempenho	
	Disponível para todas as organizações usuárias do Sistema RNP	Requer o cumprimento de políticas de segurança específicas para a instituição fazer parte da rede	



FICHA TÉCNICA

COORDENADOR-GERAL/ACADÊMICO:
Leandro Ciuffo (RNP), leandro.ciuffo@rnp.br

COORDENADORES-ASSISTENTES:
Débora Reis (RNP), debora.reis@rnp.br,
Kesley Silva (RNP), kesley.silva@rnp.br

EQUIPE:
Jeferson Souza,
Carlos Zilves,
Edemir Matos,
Luciana Ferreira,
Ari Frazão, Aluizio Hazin, Allan Oliveira,
Luiz Teixeira e
Humberto Forsan



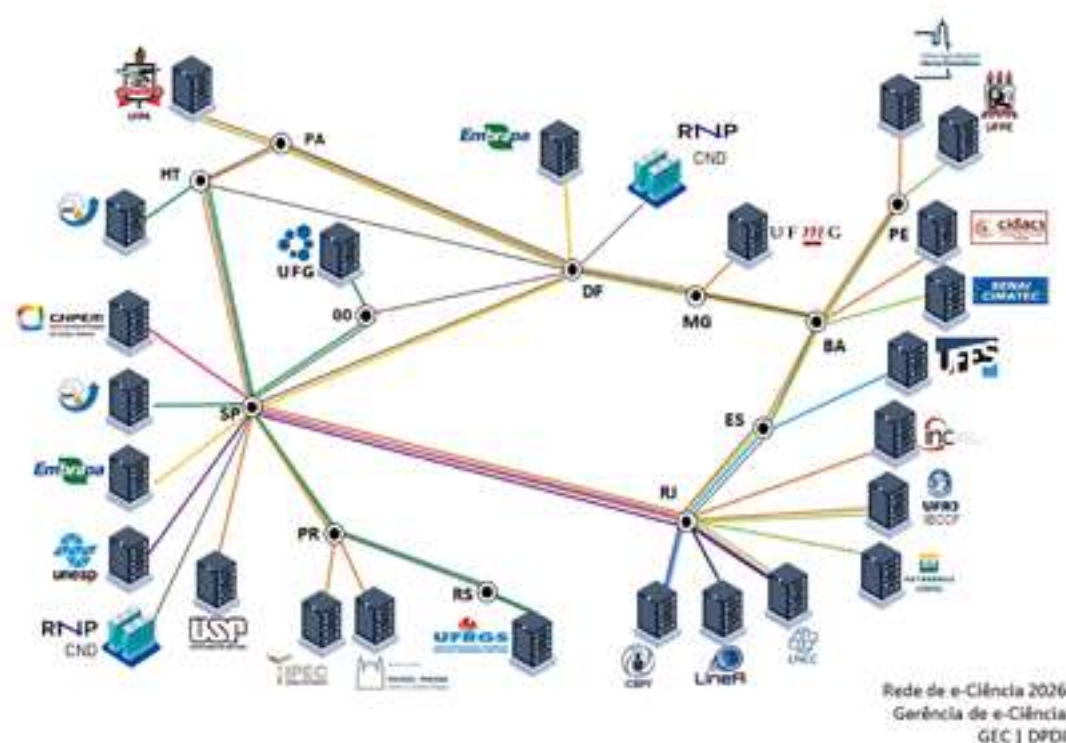
ENTIDADES PARCEIRAS

CBPF, CENPES, CNPEM, Embrapa, Fiocruz, INC, INPE, LIneA; LNCC, Senai-Cimatec, UFES, UFG, UFMG, UFPA, UFRGS, UFRJ, UNESP



QR CODE





CONECTIVIDADE DE ALTA VELOCIDADE PARA IMPULSIONAR O FUTURO DAS COLABORAÇÕES CIENTÍFICAS

DEMANDAS CIENTÍFICAS E CONEXÕES

AGRICULTURA E GENÔMICA
EMBRAPA

GENÔMICA
UFPA - UFPA - UFRJ - IREC - INC - USP (SP e RP) - FIOCRUZ (PR, CIOACS e PE)

NANOTECNOLOGIA BIORRENOVÁVEIS
CNPq - LNCC

COSMOLOGIA FÍSICA DE ALTAS ENERGIAS ASTRONOMIA
Unesp - CBPF - UFES - LineA-LNCC

GEOCIÊNCIA
LNCC - CENPES - SENAI-CIMATEC - UFRJ - UFPA - UFPE

METEOROLOGIA
LFG - INPE - UFRGS - INPE



P&D e Prospecção Tecnológica na Rede de e-Ciência

OTIMIZANDO A MOVIMENTAÇÃO DE DADOS EM LARGA ESCALA

No âmbito do termo de cooperação RNP-Petrobras, o projeto REPESQ expande a Rede de e-Ciência para novas ICTs com demandas crescentes de movimentação de grandes volumes de dados geológicos, geofísicos e de simulação de reservatórios para o centro de pesquisa da Petrobras (CENPES). O programa contempla três objetivos de pesquisa em quatro frentes de trabalho. A primeira desenvolve um sistema automatizado de gerenciamento de workflows científicos para acesso remoto dos pesquisadores do CENPES a supercomputadores localizados em outras instituições. A segunda frente, com duas linhas complementares, atua na otimização integrada de hardware, rede e armazenamento para transferências de alta vazão em longas

distâncias – em 100G e prospectando 400G – com foco em escalabilidade, segurança, integridade e eliminação de falhas. A quarta frente realiza prospecção tecnológica em Sensoriamento Acústico Distribuído (DAS), levantando desafios para estruturar um futuro programa de P&D em processamento e transmissão dos dados gerados pelo DAS em unidades de produção. Os objetivos combinados permitirão o desenvolvimento de novos fluxos de trabalho automatizados para a transferência eficiente de grandes volumes de dados para o CENPES e entre um conjunto de oito ICTs que desenvolvem pesquisas em parceria com a Petrobras, consolidando a Rede de e-Ciência como uma ciberinfraestrutura estratégica para a ciência brasileira. •



FICHA TÉCNICA

COORDENADOR-GERAL/ACADÊMICO:
Adriano da Silva Ferreira (RNP),
adriano.silva@rnp.br

EQUIPE:
Antônio Tadeu,
Vivian Medeiros,
Welber Paraizo (LNCC), Fernando Redigolo, Vinicius Medeiros, Fernanda Lopes (USP), Aderson Farias (UFRN), Marcelo Bianchi (USP)



ENTIDADES PARCEIRAS

CENPES, LNCC,
USP, UFRN,
SENAI-CIMATEC

Repositórios de Dados de Pesquisa **para a Rede de e-Ciência**

UM ESTUDO DE CASO COM DADOS CLIMATOLÓGICOS DO CEMPA-CERRADO/UFG

Ao longo de 2025, a RNP em parceria com a UFG, por meio de seu Centro de Excelência em Estudos, Monitoramento e Previsões Ambientais do Cerrado – CEMPA-Cerrado, avançou com uma iniciativa para melhorar a governança e gestão de dados climatológicos em repositórios digitais. A principal motivação foi ampliar o acesso e(re)uso para dados de pesquisa gerados por workflows científicos da rede de e-Ciência da RNP. Buscou-se interoperabilidade e compreensão da informação científica por pesquisadores de diferentes áreas – não necessariamente pares científicos. Inicialmente, a tentativa de ingestão de grandes volumes de dados, caracterizados por matrizes complexas em formato científico, resultou em sobrecarga da infraestrutura. Como solução, aplicou-se

rotinas de transformação originando dados derivados em formatos menores e estruturados, facilitando o consumo por usuários sem experiência em repositórios digitais. O enriquecimento dos dados oriundos de workflows científicos ampliou o acesso, mantendo o rigor científico e viabilizando o reuso destes em repositórios digitais por pesquisadores ou consumo por ferramentas de análise baseadas em inteligência artificial. O acesso sobre dados climatológicos em Goiás foi democratizado, eliminando a necessidade de ferramentas científicas específicas. Espera-se ampliar esse estudo de caso para outros domínios e ICTs da rede de e-Ciência da RNP de forma que também possam se beneficiar de uma melhor gestão e governança de dados de pesquisa em repositórios digitais. •

REPOSITÓRIOS DIGITAIS PARA UMA MELHOR GESTÃO E GOVERNANÇA DE DADOS CIENTÍFICOS DE PESQUISA



FICHA TÉCNICA

COORDENADORA-GERAL/ACADÊMICA:

Prof. Dra. Laura Vilela Rodrigues Rezende (UFG),
laura_rezende@ufg.br

COORDENADORA TÉCNICA:

Prof. Dra. Kátia Kelvis (UFG),
katiakelvis@ufg.br

COORDENADORA DE P&D:

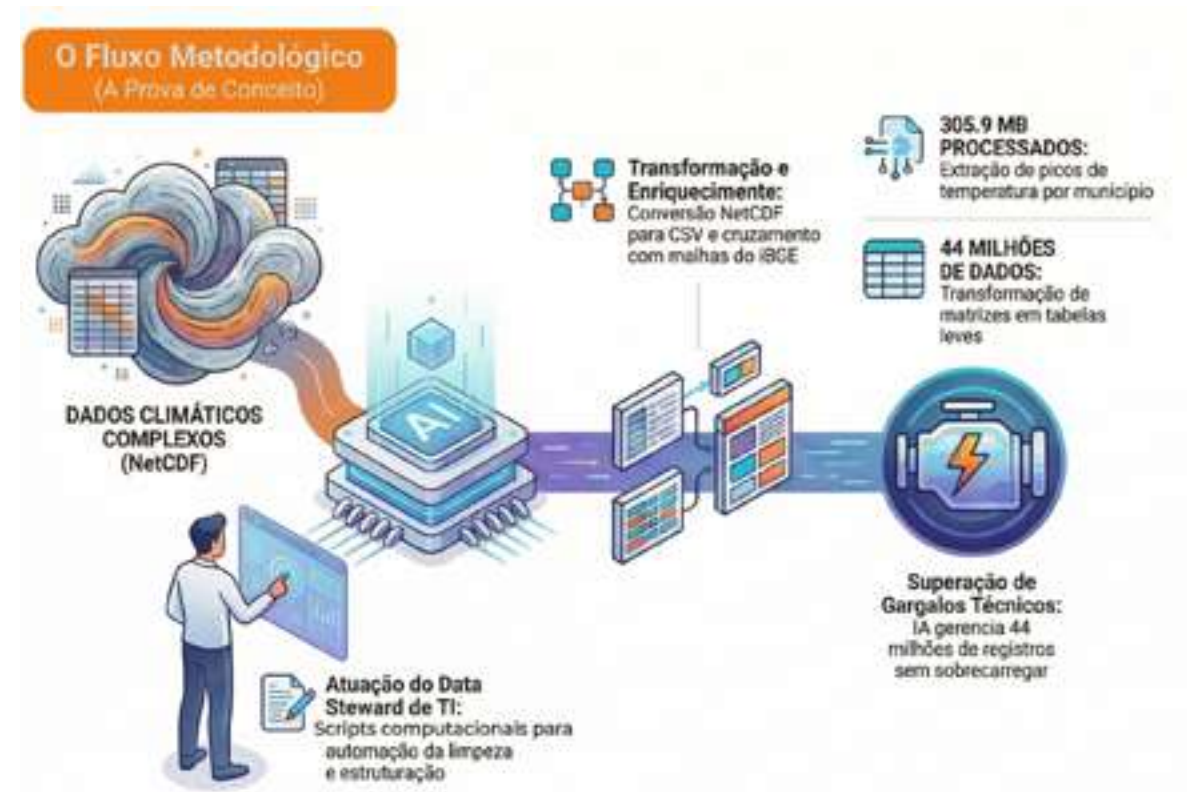
Carolina Howard Felicissimo (RNP),
carolina.felicissimo@rnp.br

EQUIPE:

Angel Chovert,
Anne Oliveira,
Breno de Lima,
Geisa Ribeiro

IA na Ciência Aberta: Da Curadoria de Dados à Democracia da Informação

Fluxo Metodológico e Resultados da Prova de Conceito (PoC) para Dados Climáticos Complexos



P&D para Gestão de Identidade e Acesso para Rede de e-Ciência

PROVA DE CONCEITO E ESTUDO DE CASO COM ICTS

Infraestruturas de Pesquisa dependem cada vez mais de mecanismos seguros e interoperáveis para a autenticação e autorização de usuários. Muitas vezes, uma colaboração de pesquisa é formada por pesquisadores de múltiplas instituições e até de empresas, o que aumenta a complexidade do controle de acesso. Para tanto, é necessário o uso de um ambiente que gerencie todo o ciclo de vida das Organizações Virtuais – um grupamento lógico e temporário de pessoas, muitas vezes de diferentes instituições, que colaboram em torno de um projeto. Esse ambiente permite que pesquisadores de várias instituições acessem serviços e espaços de colaboração usando apenas a credencial de sua própria instituição. A partir dessa necessidade, e mantendo o alinhamento com iniciativas internacionais, os Grupos de Trabalho envolvidos neste

projeto estão analisando plataformas já existentes (CILogon e MyAccessID) e propondo soluções de Gestão de Identidade – GId considerando a realidade das instituições da Rede de e-Ciência. Entre as principais soluções avaliadas, destaca-se uma arquitetura que integra o CILogon a protocolos modernos de autenticação, como o OpenID Connect (OIDC), além de uma prova de conceito baseada na AARC Blueprint Architecture, modelo amplamente adotado pela comunidade internacional para organizar serviços de identidade federada.

Além disso, está sendo conduzida uma prova de conceito de integração com a ferramenta Globus, uma solução que visa facilitar e automatizar a execução de transferências de dados entre as instituições da Rede de e-Ciência. ●



CILogon

FICHA TÉCNICA

PESQUISADOR PRINCIPAL:

Walter Priesnitz Filho (UFSM),
walter.filho@ufsm.br

EQUIPE:

Heitor Scalco Neto,
Renato Preigschadt de Azevedo, José Carlos Lacerda Lopes Neto,
Gustavo Peretti,
Gabriel Denarde



MyAccessID

FICHA TÉCNICA

PESQUISADOR PRINCIPAL:

Edelberto Franco Silva (UFJF),
edelberto.franco@ufjf.br

PESQUISADOR ADJUNTO:

Bruno Dembogurski,
bruno.dembogurski@ufrj.br

EQUIPE:

Allan Marcelino,
Leonan Louvem,
Pedro Henrique Silva, Bruno José Dembogurski

SOLUÇÕES EM GID: CILOGON, MYACCESSID E GLOBUS

Log in

Use your organizational login
e.g., university, national lab, facility, project



By selecting Continue, you agree to Globus terms of service and privacy policy.

[Continue](#)

COLABORAÇÃO
E
FUTURO

- 36 Rede de Colaboração RNP & Startups: **experimentação e inovação em rede**
- 37 Presente! **Sua sala de aula inteligente**
- 38 O CT-CDIA: **Articulando P&D, Infraestrutura e Inovação em IA**
- 39 **Comitê Técnico de Gestão de Identidade** (CT-GId)

Rede de Colaboração RNP & Startups: **experimentação e inovação em rede**

PROVAS DE CONCEITO CONECTAM PESQUISA, STARTUPS E ORGANIZAÇÕES USUÁRIAS

A Rede de Colaboração RNP & Startups foi criada para fortalecer a conexão entre resultados de pesquisa desenvolvidos nos programas de P&D da RNP e o ecossistema de inovação, apoiando startups surgidas a partir de grupos de trabalho e projetos de pesquisa. Um dos avanços recentes da iniciativa é a realização de Provas de Conceito (PoCs) que permitem testar soluções tecnológicas em ambientes reais de uso junto às organizações integrantes do Sistema RNP. Essas experimentações ajudam a validar tecnologias, compreender necessidades institucionais e gerar evidências para adoção ou expansão das soluções. Um exemplo é a PoC realizada com a startup Reabnet, que avaliou um modelo de cuidado digital gamificado para idosos em parceria com o Hospital de

Clínicas da Universidade Federal de Uberlândia e a Unimed Uberlândia. Os resultados indicaram alta adesão dos participantes e melhorias relevantes em indicadores clínicos e funcionais, evidenciando o potencial de escalabilidade da solução. Outras PoCs estão em andamento, incluindo projetos com a MetaHealth, em parceria com a UFMG e a Univates, e uma colaboração internacional entre a startup Ring0 e a RENU, rede acadêmica de Uganda. A Rede também promove mentorias especializadas, apoio na captação de recursos e aproximação com parceiros e *early adopters*, ampliando o papel da RNP como plataforma de experimentação tecnológica e contribuindo para transformar resultados de pesquisa em soluções inovadoras com impacto social e econômico. •



FICHA TÉCNICA

GERENTE:
Rafael Valle (RNP),
rafael.valle@rnp.br

COORDENADORA:
Ana Geórgia Damasceno Barbosa (RNP),
ana.barbosa@rnp.br

EQUIPE:
Felipe Nascimento,
Henrique Ferraz,
José Henrique Diéguez, John Forman



QR CODE



POCS CONECTAM STARTUPS, PESQUISA E ORGANIZAÇÕES PARA VALIDAR SOLUÇÕES INOVADORAS



Presente! **Sua sala de aula inteligente**

ENGAJAMENTO EM SALA ANALISADO POR IA E 5G PARA APOIAR O ENSINO

O projeto Presente! Sua sala de aula inteligente explora o uso de inteligência artificial e visão computacional para compreender o engajamento dos estudantes em sala e apoiar a melhoria do processo de ensino-aprendizagem. Implementada no Inatel, a solução opera sobre uma rede privativa 5G, garantindo baixa latência, alta confiabilidade e capacidade de processamento em tempo quase real. A arquitetura do sistema utiliza processamento na borda da rede para tratar dados multimodais provenientes de múltiplas câmeras na sala. Por meio de modelos de aprendizado de máquina e visão computacional, a plataforma identifica padrões de comportamento, interação e participação ao longo das atividades, permitindo estimar níveis coletivos de engajamento. As análises são realizadas com base em dados agregados e anonimizados, sem identificação individual dos alunos, preservando a privacidade dos participantes. O processamento ocorre em tempo real e sem necessidade de armazenamento permanente das imagens, garantindo maior segurança no tratamento das informações. A partir dessas análises, o sistema gera indicadores que podem apoiar professores e gestores educacionais na avaliação de estratégias pedagógicas e na compreensão da dinâmica de participação

em sala. Além da análise de engajamento, o projeto também investiga aplicações complementares, como controle de acesso inteligente e lista de presença automatizada por reconhecimento facial, contribuindo para a modernização da gestão acadêmica. •

TECNOLOGIA TRANSFORMA DADOS DA SALA DE AULA EM EVIDÊNCIAS PARA APRIMORAR O APRENDIZADO



FICHA TÉCNICA

COORDENADOR-GERAL/ACADÊMICO:
José Ferreira de Rezende (RNP),
jose.rezende@rnp.br

COORDENADOR-ASSISTENTE:
Clayton Reis da Silva (RNP),
clayton.reis@rnp.br

EQUIPE:
RNP: Iara Machado, Leonardo Ribeiro
UFRJ: Sergio L. Netto, Eduardo da Silva, Thadeu Dias
INATEL: Cristiani Guimarães, Douglas Pereira, Murilo Lopes, Ana Serafim



ENTIDADES PARCEIRAS

INATEL e UFRJ

O CT-CDIA: Articulando P&D, Infraestrutura e Inovação em IA

CONECTANDO UNIVERSIDADES E CENTROS DE P&D NA NOVA ERA DA IA

O mundo vive uma nova era tecnológica marcada pelo avanço da inteligência artificial, que está transformando rapidamente a ciência, a indústria e a educação, e impactando todos os setores da sociedade. Assim como ocorreu nos primórdios das redes de computadores, o Brasil enfrenta desafios importantes, como a falta de infraestrutura adequada para a IA. Ao mesmo tempo, a formação de recursos humanos capazes de compreender, desenvolver e utilizar as tecnologias de IA de forma responsável permanece insuficiente. A rápida evolução desse campo é impulsionada por tendências como o surgimento de agentes capazes de tomar decisões de forma autônoma ou agir de forma coordenada. A RNP, que conecta instituições brasileiras e oferece serviços essenciais à

pesquisa e à educação, pode desempenhar um papel estratégico ao oferecer serviços de pesquisa em IA que estimulem a colaboração e a inovação. Uma iniciativa alinhada a esse esforço é o CT-CDIA. O comitê promoverá palestras, workshops e painéis com especialistas do Brasil e do exterior para discutir tecnologias emergentes de IA e seus potenciais benefícios à sociedade. Entre seus objetivos estão identificar as necessidades da comunidade em pesquisa, educação e implantação, além de debater como a RNP pode desenvolver plataformas para avaliar sistemas de IA em condições realistas, integrando a infraestrutura e os dados distribuídos no país. Essas ações podem fortalecer a capacidade brasileira em tecnologias digitais avançadas. •



FICHA TÉCNICA

COORDENADOR-GERAL/ACADÊMICO:

Edmundo de Souza e Silva (UFRJ),
edmundo@land.ufrj.br

EQUIPE:

Altigran Soares da Silva, Andre Carlos Ponce de Leon, Claudia Bauzer Medeiros, Flávio Rech Wagner, Teresa Ludermir, Wagner Meira

A RNP FOI ESSENCIAL PARA O DESENVOLVIMENTO DAS REDES E PODE SER ESTRATÉGICA NA ERA DA IA



Comitê Técnico de Gestão de Identidade (CT-GId)

PROSPECÇÃO TECNOLÓGICA EM GESTÃO DE IDENTIDADE

Instituído pela RNP em 2010, tem por finalidade elaborar recomendações técnicas e projetar uma visão de futuro para a RNP no âmbito da gestão de identidades. A participação no CT-GId é aberta a especialistas e profissionais atuantes em áreas correlatas, buscando promover a pluralidade técnica e ampliar as contribuições para o setor. O comitê atua em ciclos anuais, acompanhando os principais avanços da academia e da indústria na área. São promovidas iniciativas importantes, como palestras, estudos técnicos e desenvolvimento de provas de conceito. O relatório de visão de futuro,

atualizado bianualmente, identifica tendências que podem evoluir serviços atuais, originar novos serviços ou modelos de negócio para a RNP no âmbito da gestão de identidade e de acesso. O relatório de 2025 indica tendências nas áreas como o modelo de identidade digital descentralizada, IA agêntica, identidade para carga de trabalho e software, arquitetura de confiança zero. Em 2026, o comitê está trabalhando em um novo formato para o relatório de visão, uma versão no estilo resumo executivo e uma com mais detalhes que possam ajudar a academia e a RNP identificarem tendências na área. •



FICHA TÉCNICA

COORDENADOR-GERAL/ACADÊMICO:

Emerson Ribeiro de Mello (IFCS),
mello@ifsc.edu.br

COORDENADORA-ASSISTENTE:

Shirlei Aparecida de Chaves (IFSC),
shirlei.chaves@ifsc.edu.br

EQUIPE:

Secretário:
Fiterlinge Martins de Sousa (RNP)



QR CODE



IDENTIDADE DIGITAL DESCENTRALIZADA E IA AGÊNTICA SÃO DESTAQUES NA ÁREA DE GID

REDES ABERTAS

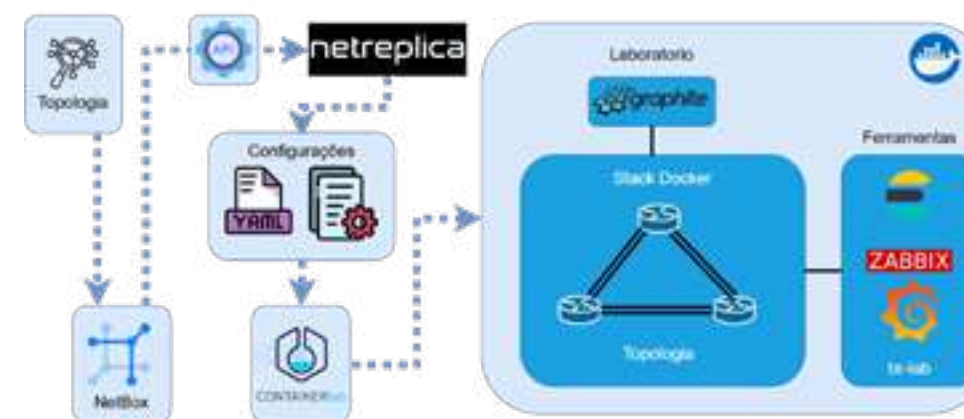
- 41 **Gêmeos Digitais**
de Redes da RNP
- 42 **Brasil acelera rumo
ao 6G** com infraestrutura
de ponta e inteligência artificial
- 43 Programa
OpenRAN@Brasil

Gêmeos Digitais de Redes da RNP

LABORATÓRIOS VIRTUAIS DAS DIFERENTES REDES DO SISTEMA RNP

Essa iniciativa tem como objetivo a criação de laboratórios de rede virtuais usando gêmeos digitais das diferentes redes do sistema RNP, como o backbone nacional (Rede Ipê) e redes metropolitanas. Utilizando como força de trabalho analistas de redes dos Pontos de Presença da RNP e pesquisadores da academia, são criados tutoriais abertos para explorar e disseminar novas metodologias, paradigmas e ferramentas de rede, relevantes ao mesmo tempo para a operação da rede, pesquisa e experimentação. Para 2026, a proposta do projeto é focar em serviços de rede fim a fim, servindo como ambiente de desenvolvimento,

teste e capacitação do 1) sistema de monitoramento unificado de redes da RNP, 2) criação de cenários práticos aplicando o uso de IA para redes e 3) solução de circuitos dinâmicos fim a fim entre redes metropolitanas passando por PoPs e Rede Ipê. O principal impacto é permitir que a evolução das redes da RNP possa ser colaborativa, com equipes que vão além das de operação, facilitando a execução de projetos de P&D em parceria com a academia e viabilizando a replicação de ambientes em topologias reais para transferência tecnológica e de conhecimento entre as equipes de P&D e produção. •



EVOLUÇÃO COLABORATIVA DAS REDES DA RNP ENTRE OPERADORES E PESQUISADORES



FICHA TÉCNICA

COORDENADOR-GERAL/ACADÊMICO:
Marcos Schwarz
(RNP),
marcos.schwarz@rnp.br

COORDENADOR-ASSISTENTE:
Gustavo Araújo
(RNP),
gustavo.araujo@rnp.br

EQUIPE:
UFRR/PoP-RR:
Kaio Guilherme
UFRA/PoP-PA:
Eduardo Castro
PoP-RJ: Rafael
Brandão
UFC/PoP-CE:
Felipe Anjos
RNP:
Lucas Borges



QR CODE



Brasil acelera rumo ao 6G com infraestrutura de ponta e inteligência artificial

INFRAESTRUTURA HPC AMPLIA PESQUISA BRASILEIRA EM REDES 6G

Iniciado em 2021, o Programa Brasil 6G consolidou-se como uma iniciativa estratégica para posicionar o país não apenas como consumidor, mas também como desenvolvedor de tecnologias e padrões para a próxima geração de redes móveis. Financiado pelo MCTI no âmbito do PPI/Internet Avançada da RNP, o projeto é executado em parceria com o Inatel e o CPQD. Atualmente, o programa está em sua 3ª fase, mantendo o foco na integração de Inteligência Artificial (IA) e no desenvolvimento da Plataforma de Experimentação em 6G. Para apoiar essa etapa, a iniciativa conta com investimentos superiores a R\$ 5 milhões em equipamentos de ponta. Essa infraestrutura engloba rádios definidos por software, analisadores de protocolos e de espectro,

além de uma solução avançada de computação de alto desempenho (HPC) com IA. Com esses recursos, é possível validar tecnologias de acesso e núcleo de rede, permitindo aos pesquisadores processar grandes volumes de dados para treinar modelos de aprendizado de máquina aplicados às redes 6G. Até a 3ª fase, já mobilizou cerca de 144 profissionais e 77 bolsistas, acumulando resultados expressivos em produção científica, registro de softwares, patentes, formação de talentos e desenvolvimento de protótipos. Ao reunir instituições de excelência como UFPA, UFC, Unicamp, UFSC, UFRJ, Unisinos e UFG, o Programa Brasil 6G fortalece a cooperação científica nacional e prepara o país para os desafios de um futuro cada vez mais conectado. •

Brasil 6G

3ª FASE FOCA EM HPC E IA PARA GARANTIR A SOBERANIA TECNOLÓGICA E INOVAÇÃO NACIONAL EM 6G



FICHA
TÉCNICA

COORDENADOR-GERAL/ACADÊMICO:

Fernando N. N. Farias (RNP),
fernando.farias@rnp.br

COORDENADOR-ASSISTENTE:

Bárbara Évellyn (RNP), barbara.santos@rnp.br

EQUIPE:

Michelle Wangham,
Bruno Ciro,
Diego Abreu,
José Rezende,
José Brito,
Daniely Gomes,
Luciano Mendes,
Juliano Ferreira



ENTIDADES
PARCEIRAS

UFG, UFC, UNISINOS,
UFSC, UFPA,
UFRJ, UNICAMP,
INATEL, CPQD



QR CODE



Programa OpenRAN@Brasil

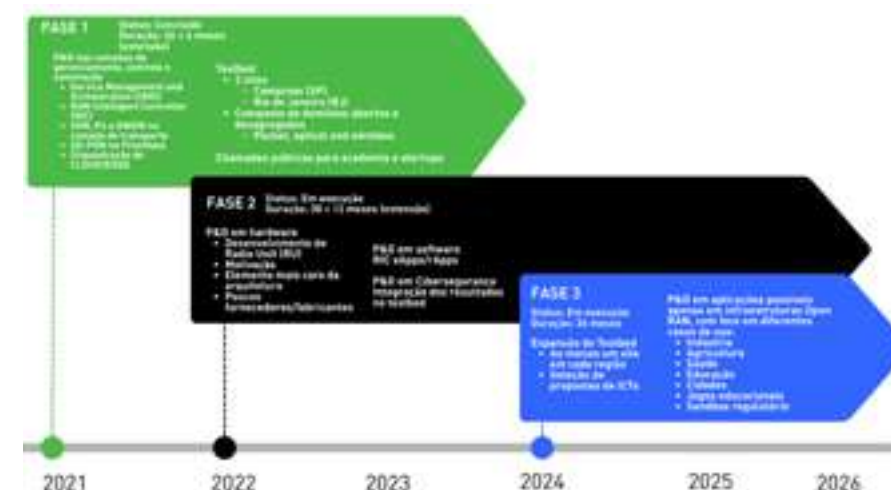
INFRAESTRUTURA ABERTA, INOVAÇÃO E COLABORAÇÃO EM REDES MÓVEIS

O Programa OpenRAN@Brasil consolida-se como a principal iniciativa nacional para pesquisa, desenvolvimento e validação de tecnologias Open RAN em ambiente realista e interoperável. Estruturado como um testbed multi-institucional, o programa integra universidades, centros de pesquisa e parceiros industriais para acelerar a maturidade de soluções abertas para redes móveis.

Ao longo de sua evolução, organizada em três fases complementares, o OpenRAN@Brasil avançou da implantação de infraestrutura laboratorial para a integração de módulos de rádio, software de controle, orquestração e gerenciamento, enfrentando desafios

concretos de interoperabilidade, desempenho e automação. O ambiente permite experimentação em arquitetura desagregada, testes de integração ponta a ponta e avaliação de casos de uso alinhados às demandas do país. Mais do que uma plataforma tecnológica, o programa atua como catalisador de formação de recursos humanos especializados, cooperação internacional e desenvolvimento de competências estratégicas. Ao promover padrões abertos e ecossistemas colaborativos, o OpenRAN@Brasil contribui para ampliar a competitividade nacional e fortalecer a soberania tecnológica em redes móveis. •

TESTBED NACIONAL IMPULSIONA INOVAÇÃO E SOBERANIA EM REDES OPEN RAN



FICHA
TÉCNICA

COORDENADOR DE INTEGRAÇÃO:

Lucas Bondan (RNP),
lucas.bondan@rnp.br

COORDENADOR DE PROJETOS:

Leonardo Carvalho Ribeiro (RNP),
leonardo.ribeiro@rnp.br

EQUIPE:

Fernando Farias,
Gustavo Araújo,
Daniel Marques,
Elaine Barioni,
Érico Bastos,
Francisco Portelinha,
Fábio Takaki



ENTIDADES
PARCEIRAS

CPQD, Inatel,
Eldorado, UFG, UnB,
UFRGS, UNISINOS,
UFPA, UFRJ, UFCG,
UFF, UFSCAR, UFRN,
PUCRS, UFCSPA



QR CODE



BLOCK CHAIN

45 **Observatório Nacional de Blockchain:** um modelo de disseminação científica

46 **Ilíada:** Integrando Livros-razão, Infraestrutura e Aplicações Descentralizadas

48 **CarbonID**

49 **ChainGuard:** Solução de preservação da cadeia de custódia de vestígios digitais

50 Valorizando a cadeia produtiva e aumentando **a segurança alimentar brasileira**

51 **GT-SWARM**

52 Tecnologia financeira on-chain com **conformidade para instituições reguladas**

53 **LedgerNFT:** Plataforma de modelagem, emissão e controle de NFT de Ciclo Preditivo

54 Blockchain para Governança Analítica em **Cadeias Produtivas**

55 **GT-Acredita:** Credenciais verificáveis para identidade digital e acesso

56 **Do papel ao digital:** IA e Blockchain na Gestão de Acervos Acadêmicos



CURADORIA DE DADOS, ENGAJAMENTO DE COMUNIDADE E INTERESSE PÚBLICO

O Observatório Nacional de Blockchain vem se consolidando como um modelo institucional de disseminação científica orientado por curadoria de dados, engajamento de comunidade e foco em informação de interesse público. De abril de 2025 até março de 2026, a plataforma mapeou mais de 580 iniciativas em blockchain; indexou cerca de 2,2 mil produções científicas sobre o tema – entre teses, dissertações e artigos –; promoveu mais de 10 encontros da Comunidade de Especialistas; relatou aproximadamente 130 casos de uso da tecnologia e alcançou 1,7 mil seguidores no LinkedIn. A equipe do Observatório entrevistou 11 pesquisadores da área, firmou cinco parcerias institucionais e participou de 13 eventos para divulgar ações e os objetivos relativos ao fortalecimento do ecossistema blockchain no Brasil. Ao todo, a produção de conhecimento e a governança de dados resultaram na produção de sete publicações, entre artigos, relatórios técnicos e materiais

Observatório Nacional de Blockchain: um modelo de disseminação científica



FICHA TÉCNICA

COMITÊ EDITORIAL: Bárbara Evellyn e Lariza Thurler (RNP); Luana Cruz (jornalista); Glauber Gonçalves (UFPI); Ismael Ávila e Sílvia Marion (CPQD), contato@observatorioblockchain.org.br



ENTIDADES PARCEIRAS

Ibict/BrCris, iColab, Polkadot Education, Cardano Academy



QR CODE



OBSERVATÓRIO PROMOVERÁ EXPANSÃO DOS INDICADORES E AUMENTARÁ ENFOQUE NAS CONEXÕES GERADAS

Ilíada: Integrando Livros-razão, Infraestrutura e Aplicações Descentralizadas

PESQUISA,
EXPERIMENTAÇÃO
E INOVAÇÃO
EM BLOCKCHAIN

Coordenado pela Softex e executado pela RNP e pelo CPQD, no âmbito do Programa de PPISoftex, o Projeto Ilíada lançou três chamadas públicas e selecionou 13 grupos de trabalho e quatro startups para desenvolver aplicações e ampliar o conhecimento científico sobre blockchain. As atividades de P&D mobilizaram 106 bolsistas, além da equipe da RNP. As soluções foram validadas em um testbed multiplataforma que permite a pesquisadores e desenvolvedores experimentarem diferentes plataformas e arquiteturas de blockchain em um contexto controlado e colaborativo. Foi desenvolvida, ainda, a ferramenta EasyLedger, que facilita e automatiza

a criação de redes blockchain nos ambientes de experimentação. A infraestrutura inclui oito servidores dedicados hospedados em pontos de presença da RNP distribuídos pelo país, totalizando uma capacidade computacional superior a 500 cores de CPU, mais de 2 TB de memória RAM e cerca de 40 TB de armazenamento, formando uma infraestrutura efetiva para experimentação em escala nacional. Outro resultado do Ilíada é o Observatório Nacional de Blockchain, plataforma que reúne dados, pesquisa e comunidade para mapear e dar visibilidade ao ecossistema da tecnologia no Brasil. A seguir, destacamos algumas iniciativas do projeto. •

**AS ATIVIDADES DE P&D
MOBILIZARAM 106 BOLSISTAS
DE 23 INSTITUIÇÕES, ALÉM
DA EQUIPE DA RNP**



FICHA TÉCNICA

COORDENADOR- GERAL/ACADÊMICO:

Leandro Ciuffo
(RNP), leandro.ciuffo@rnp.br

COORDENADORA- ASSISTENTE:

Bárbara Évellyn
(RNP), barbara.santos@rnp.br

EQUIPE:

Iara Machado,
Michelle
Wangham, Ana
Landi, Estefânia
Arata, Giovana
Barbosa, Kauane
Cordeiro, Larissa
Salles, Larriza
Thurler, Luiz Folly,
Marcos Schwarz,
Pedro Neves,
Reinaldo Gomes

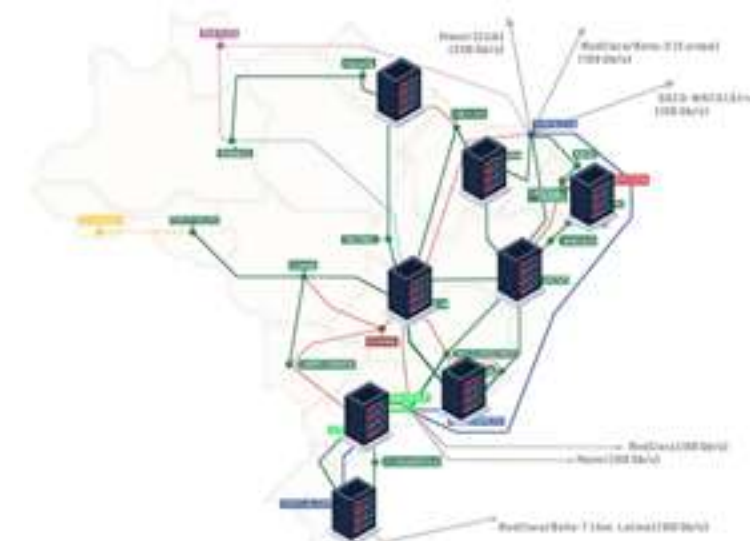


ENTIDADES PARCEIRAS

CPQD, UFPR,
UFPA, UFC, UFF,
IFBA, IFPI, UFPI,
Unioeste, PUC-MG,
UnB e Amachains



QR CODE



Pesquisadores de
23 universidades

Mais de
100 bolsas
de incentivo à PD&I

2 bolsas
de jornalismo científico

13 grupos
de pesquisa
utilizando o testbed

5 startups
envolvidas

CarbonID

PLATAFORMA PARA GESTÃO E RASTREABILIDADE DE ATIVOS DIGITAIS

A CarbonID é uma plataforma tecnológica concebida para ampliar a transparência, a rastreabilidade e a confiabilidade no ciclo de vida de projetos e ativos digitais, como créditos de carbono. A solução integra tecnologias emergentes, incluindo blockchain, contratos inteligentes e Identidade Digital Descentralizada (IDD), com o objetivo de registrar, validar e acompanhar as diferentes etapas associadas à geração, certificação e utilização desses ativos. A utilização de blockchain possibilita o registro imutável e auditável de informações e metadados dos projetos, constituindo um repositório confiável que contribui para reduzir inconsistências, fortalecer a confiança entre os participantes do ecossistema e apoiar processos de auditoria e verificação por

diferentes instituições e partes interessadas. Adicionalmente, a adoção de mecanismos de IDD permite garantir a autenticidade e a responsabilização das entidades envolvidas nas operações da plataforma, como desenvolvedores de projetos, auditores, certificadoras e compradores; assegurando que cada registro esteja vinculado a identidades digitais verificáveis. A plataforma também oferece recursos para acompanhamento do histórico e do estado dos projetos e ativos, promovendo maior visibilidade, governança e integridade das informações. Dessa forma, a CarbonID contribui para o fortalecimento da credibilidade e da transparência em mercados de carbono e em outros ativos digitais rastreáveis. •



**A CARBONID
INTEGRA
BLOCKCHAIN E IDD
PARA GARANTIR
RASTREABILIDADE
DE ATIVOS
AMBIENTAIS**



FICHA TÉCNICA

COORDENADOR- GERAL/ACADÊMICO:

Leobino
Nascimento
Sampaio (UFBA),
leobino@gmail.com

COORDENADOR- ASSISTENTE:

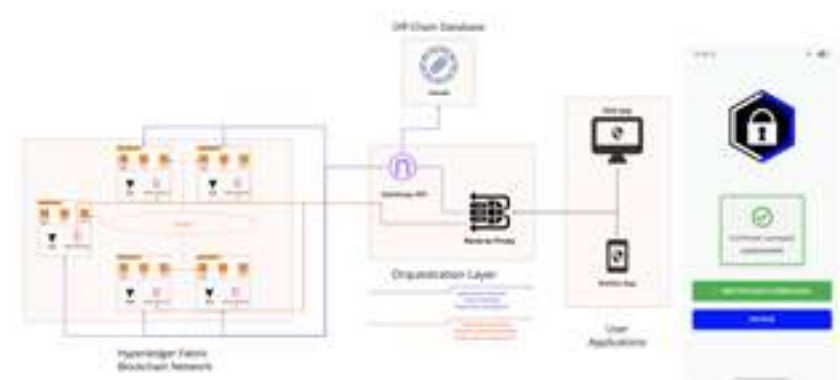
Silvio José de
Queiroz Pereira
(UFBA), silvio.queiroz@gmail.com

EQUIPE:

Leobino Sampaio,
Silvio Pereira,
Oswaldo Santana
Filho, Igor Santos,
Anderson Carvalho,
Ederson Assunção



QR CODE



ChainGuard: Solução de preservação da cadeia de custódia de vestígios digitais

A cadeia de custódia foi incorporada ao ordenamento jurídico brasileiro pela Lei nº 13.964/2019, que introduziu no Código de Processo Penal dispositivos voltados à garantia da rastreabilidade, integridade e autenticidade de vestígios utilizados como prova em investigações e processos judiciais. Nesse contexto, é essencial assegurar que evidências digitais sejam preservadas e documentadas ao longo de todo o seu ciclo de vida. Com o objetivo de apoiar esses requisitos, o projeto ChainGuard desenvolveu uma infraestrutura digital baseada em blockchain para gestão da cadeia de custódia de evidências digitais, reproduzindo fluxos operacionais de órgãos de segurança pública, além de desenvolver aplicações voltadas à coleta, registro e auditoria de vestígios. A solução é composta por três componentes: aplicações de usuário, incluindo um aplicativo móvel para coleta de vestígios em campo e uma aplicação web para gestão administrativa; uma camada de

orquestração responsável pela integração e controle das requisições do sistema; e uma rede blockchain permissionada baseada em Hyperledger Fabric, utilizada como registro imutável das transações. Complementarmente, uma base imutável off-chain armazena evidências e metadados. Ao integrar registro distribuído, assinaturas digitais e rastreabilidade criptográfica, o ChainGuard demonstra o potencial da tecnologia blockchain para fortalecer a integridade e a auditabilidade da cadeia de custódia de evidências digitais. •

**BLOCKCHAIN REFORÇA
CONFIABILIDADE DA
CADEIA DE CUSTÓDIA
DE EVIDÊNCIAS
DIGITAIS NO BRASIL**

SOLUÇÃO BLOCKCHAIN
DE CENTRAL DE CUSTÓDIA



FICHA TÉCNICA

COORDENADOR- GERAL/ACADÊMICO:

Renato Hidaka
Torres (UFPA),
renatohidaka@ufpa.br

COORDENADOR- ASSISTENTE:

Roberto Samarone
(UFPA), rsa@ufpa.br

EQUIPE:

João Santos, Kevin
Cruz, Sainy Dias
Antonio, Yasmim
Yosano, Roberto
Samarone, Renato
Hidaka Torres



ENTIDADES PARCEIRAS

Ministério Público
do Estado do Pará



QR CODE



Valorizando a cadeia produtiva e aumentando a segurança alimentar brasileira

BLOCKCHAIN A SERVIÇO DA AGRICULTURA FAMILIAR

A agricultura familiar corresponde a 77% dos estabelecimentos rurais brasileiros, desempenhando papel estratégico para o que chega à mesa da população. Apesar de sua relevância, o setor enfrenta o desafio de conciliar tradição e inovação para atender a exigências legais como a Instrução Normativa Conjunta INC 02/2018 (MAPA/ANVISA). O GT Smart Agro RAF investiga o uso de blockchain e contratos inteligentes como infraestrutura de confiança para a rastreabilidade agroalimentar na agricultura familiar. O projeto propõe uma arquitetura descentralizada, interoperável e de código aberto que garante aos produtores a soberania sobre seus dados, evitando a dependência de plataformas centralizadas e custos incompatíveis com a realidade do pequeno agricultor. Dessa forma, contribui para avanços em governança de dados, certificação de origem e inclusão digital, além de fomentar modelos replicáveis de rastreabilidade voltados para políticas públicas e cadeias produtivas distribuídas. A solução atende aos requisitos obrigatórios da INC 02/2018, que regulamenta a rastreabilidade de vegetais frescos. Validada por meio do Programa de Rastreabilidade da Agricultura Familiar (PRORAF), em implantação na

UNIPAMPA em Alegrete-RS, a plataforma está operacional e disponível publicamente (proraf.com.br). Sua arquitetura aberta permite que outros sistemas de rastreabilidade adotem seus componentes, contribuindo para a disseminação de soluções acessíveis e em conformidade regulatória. •

TECNOLOGIA ABERTA E FLEXÍVEL PARA PROVER RASTREABILIDADE E FOMENTAR A SEGURANÇA ALIMENTAR



FICHA TÉCNICA

COORDENADOR-GERAL/ACADÊMICO:

Rodrigo Brandão Mansilha (Unipampa), mansilha@unipampa.edu.br

EQUIPE:

Diego Kreutz, Roben Lunardi, Henrique Fan, Rafael Nogueira, Bruno Neves



ENTIDADES PARCEIRAS

Instituto Federal do RS



QR CODE



GT-SWARM

SELF-SOVEREIGN WI-FI AUTHENTICATION ROAMING

O GT-SWARM (Self-sovereign Wi-Fi Authentication Roaming) surgiu no contexto de preocupações com privacidade de usuários no acesso a serviços da Internet. As novas tecnologias de Identidade Digital Descentralizada (IDD) aprimoram a privacidade individual na autenticação de serviços. Nessa visão, o projeto desenvolveu um método EAP, para autenticação 802.1x em redes WiFi com o framework IDD Hyperledger Identus, sobre a blockchain Cardano, visando integração com a eduroam. A solução adota mecanismos de IDD, com credenciais verificáveis (VC) guardadas nas carteiras digitais dos usuários e criação de apresentações verificáveis (VP) sob demanda para autenticar o acesso à rede. O software desenvolvido é o módulo EAP-DID na implementação de referência do EAP

(hostap) e um proxy, chamado Hermes proxy, para comunicação entre o módulo e o Identus. Também foi concebida uma arquitetura para integrar os componentes e modelados os dados para viabilizar a autenticação dos usuários. O desempenho da implementação foi avaliado em comparação com o método EAP-MD5, para estimar o sobrecusto, que subiu de 2s para 4s, em média. O projeto segue com desafios em aspectos como a padronização do novo método EAP, implementação de suplicantes, integração com carteiras, avaliações de desempenho mais aprofundadas e modelagem de governança para emissão de VC, contribuindo para um ecossistema mais seguro, respeitando a privacidade e alinhado à soberania digital dos usuários. •



FICHA TÉCNICA

COORDENADORA-GERAL/ACADÊMICA:

Carla Merkle Westphall (LRG - UFSC), carla.merkle@westphall.ufsc.br

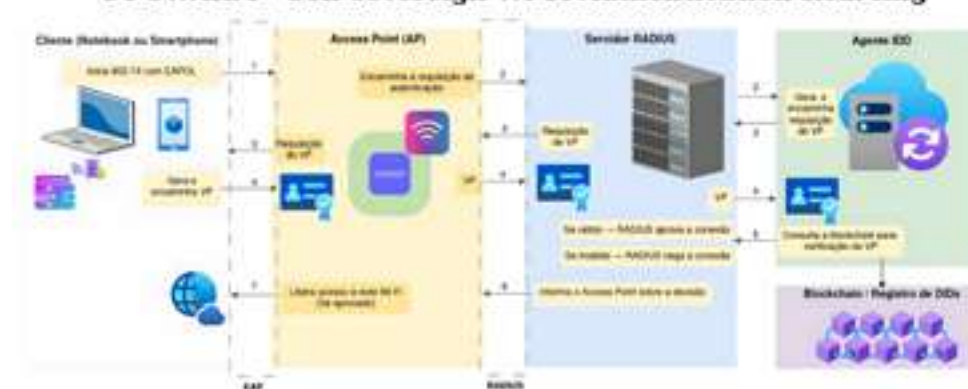
COORDENADOR-ASSISTENTE:

Caciano dos Santos Machado (CPD - UFRGS), caciano@cpd.ufrgs.br

EQUIPE:

Carla Merkle Westphall, Caciano dos Santos Machado, Cristian Alves dos Santos, Eduardo Freitas Hoffmann

GT-SWARM - Self-sovereign Wi-Fi Authentication Roaming



O GT-SWARM VIABILIZOU AUTENTICAÇÃO 802.1X COM IDENTIDADES DIGITAIS DESCENTRALIZADAS



Tecnologia financeira on-chain com **conformidade para instituições reguladas**

SOLUÇÃO WHITE-LABEL PARA NEGOCIAÇÃO DE ATIVOS TOKENIZADOS

A tecnologia financeira descentralizada abriu novas possibilidades para a negociação de ativos, com programabilidade e liquidação verificável, mas ainda enfrenta um impasse no mercado regulado. *Exchanges* centralizadas seguem dependentes de custódia, conciliação interna e controles concentrados, enquanto *venues* on-chain, abertos por padrão, não atendem às exigências de conformidade de instituições financeiras e PSAVs. É nessa lacuna que a Levery se posiciona. Como uma *stack DEX white-label* com foco em conformidade, a plataforma permite que instituições criem e operem ambientes próprios de negociação de ativos tokenizados e stablecoins. A solução abstrai a complexidade de conexão e de autorização de transações on-chain: o cliente pode criar sua *wallet*

dentro da experiência da instituição, com *passkey* e sem depender de extensão ou *wallet* externa, enquanto a instituição mantém supervisão com gestão de credenciais, políticas de uso e recuperação de acesso, sem custodiar a chave privada do usuário. KYC, KYB, AML, políticas de elegibilidade e limites de risco são verificados pelos *smart contracts* auditados da Levery antes de negociações ou movimentações de liquidez. Somam-se a isso console administrativo, políticas de ativos e mercados, monitoramento, integrações via API e oráculos para ajuste de taxas. O resultado é uma arquitetura desenhada para ampliar a governança institucional, reduzir a complexidade para o cliente final e aproximar a DeFi das exigências do mercado regulado. •



FICHA TÉCNICA

COORDENADOR-GERAL:
Cristiano Polcarpo
(Wireshape),
cristiano@
wireshape.com

COORDENADORA-ASSISTENTE:
Ingrid Gomes
(Wireshape),
ingrid@
wireshape.com



QR CODE



LEVERY UNE LIQUIDAÇÃO ON-CHAIN, COMPLIANCE E GOVERNANÇA INSTITUCIONAL



LedgerNFT: Plataforma de modelagem, emissão e controle de NFT de Ciclo Preditivo

GESTÃO TOKENIZADA DE DOCUMENTOS DIGITAIS RELEVANTES (DDR)

A tecnologia patenteada de NFT de Ciclo Preditivo (NFT-CP) da LedgerTec, associada à sua plataforma low-code/no-code de modelagem, emissão e controle de *smart contracts* e tokens, redefine a gestão de ativos digitais, sobretudo os associados com Documentos Digitais Relevantes (DDR) ao transformar o conceito de NFT de um simples colecionável em um instrumento robusto de governança e conformidade. Diferentemente de NFTs comuns, um NFT-CP estabelece previamente quem pode interagir com um dado token, em que momento e quais atributos podem ser alterados, garantindo um fluxo pré-definido, finito e auditável. Tal abordagem habilita governança multi-institucional, permitindo que várias entidades (Emissoras e Controladoras) colaborem na construção de um

único ativo digital, mantendo uma “instância digital única” de referência desde a emissão até a entrega ao destinatário final. Adicionalmente, a âncora digital do token permite que mudanças de estado e ações de preservação digital que gerem novas versões do ativo digital não afetem a integridade da visão dos detentores e eventuais destinatários do DDR. O projeto envolveu a modelagem de aplicações piloto baseadas em NFT-CP, usando a plataforma Ledger NFT, para investigar como NFTs podem incorporar lógica, temporalidade e dados ao longo de seu ciclo de vida em cenários práticos. A ideia é fomentar o uso de NFTs como componentes complementares de sistemas para prover rastreabilidade, cooperação e integração entre dados e ativos digitais. •



FICHA TÉCNICA

COORDENADOR-GERAL:
Caio Souza
Florentino
(Ledgertec),
caio@ledgertec.
com.br

EQUIPE:
Caio Souza, Rodolfo
Costa, Sebastião
Mateus Marques,
João Heitor Lopes,
Lucas Barbotin,
Rostand Costa



QR CODE



LEDGERNFT

**LEDGER
TEC**

GESTÃO TOKENIZADA DE ATIVOS DIGITAIS GOVERNADOS POR FLUXOS MULTI INSTITUCIONAIS FINITOS

Blockchain para Governança Analítica **em Cadeias Produtivas**

INFRAESTRUTURA DE VALIDAÇÃO E RASTREAMENTO DE TESTES RÁPIDOS

A confiabilidade de dados analíticos é essencial em cadeias produtivas sujeitas a forte regulação, como agricultura, meio ambiente e comércio internacional. Nesses setores, métodos laboratoriais considerados padrão-ouro continuam sendo referência para certificações e auditorias, embora sua aplicação em larga escala seja limitada por custos, tempo de resposta e complexidade operacional. Para ampliar a capacidade de monitoramento analítico ao longo dos processos produtivos foi desenvolvido o Sollytchain, uma infraestrutura digital baseada em blockchain voltada à rastreabilidade e à governança de dados analíticos. O projeto foi desenvolvido no âmbito do programa ILIADA da RNP. A solução integra três componentes principais: uma rede blockchain

permissionada baseada em Hyperledger Fabric para registro imutável das evidências analíticas; um módulo de aprendizado de máquina responsável pela avaliação automática de testes de aferição; e um painel de integração que conecta dispositivos analíticos, usuários e a infraestrutura distribuída. Diferente de aplicações tradicionais de blockchain focadas apenas no armazenamento seguro de dados, a arquitetura incorpora lógica analítica ao fluxo transacional por meio de contratos inteligentes capazes de executar inferências de modelos treinados off-chain. Assim, medições realizadas em campo passam a gerar evidências verificáveis e auditáveis ao longo do tempo, ampliando a transparência e fortalecendo processos de controle de qualidade. •

**BLOCKCHAIN
TORNANDO MEDIÇÕES
ANALÍTICAS
EM EVIDÊNCIAS
AUDITÁVEIS DE
CADEIAS PRODUTIVAS**



FICHA TÉCNICA

COORDENADORA-GERAL:

Mônica Santana Vianna (Sollytch – Soluções Analíticas Inteligentes),
monicaviann@gmail.com

EQUIPE:

Mônica Vianna,
Wilson Melo Júnior,
Walter Spolidoro,
Kledison Oliveira,
Rebeca Cruz,
Carlos Oliveira,
Eduardo Martins



ENTIDADES PARCEIRAS

Sollytch e INMETRO



QR CODE



GT-**Acredita**: Credenciais verificáveis para identidade digital e acesso

APLICAÇÃO DO MODELO DE IDENTIDADE DIGITAL DESCENTRALIZADA

Hoje, a maioria dos sistemas de informação utilizam modelos de gestão de identidade centralizados ou “em silos”. Nesse modelo, os dados pessoais dos usuários ficam guardados em instituições que atuam como provedoras de identidade e, embora o consentimento exista, o controle real do usuário sobre suas informações é limitado. Para romper com essa dependência, surge o modelo de Identidade Digital Descentralizada (IDD). O objetivo é inverter o poder: o usuário passa a gerir suas próprias informações, decidindo o que compartilhar e com quem. Através de técnicas como provas de conhecimento zero e divulgação seletiva, é possível realizar transações comprovando apenas o dado estritamente necessário. Neste projeto, desenvolvemos duas Provas de Conceito (PoCs) para validar o uso de

Credenciais Verificáveis como fator de autenticação de usuários:

1. A primeira PoC utilizou a Hyperledger Indy como base de dados verificáveis, aproveitando a maturidade tecnológica de iniciativas anteriores dentro do contexto do projeto Iliada;
2. A segunda foi construída com o framework walt.ID. Por ser uma ferramenta consolidada e bem documentada, essa etapa serviu para criar um modelo de referência para desenvolvedores que buscam implementar a IDD em aplicações reais. Complementando o estudo, realizamos um levantamento de carteiras digitais (wallets) de código aberto, identificando as opções com melhor usabilidade e com maior aderência às escolhas tecnológicas que fizemos no projeto. •



FICHA TÉCNICA

COORDENADOR-GERAL/ACADÊMICO:

Emerson Ribeiro de Mello (IFSC),
mello@ifsc.edu.br

EQUIPE:

João Vitor (UFRGS),
Kauan Freitas (IFSC), Marcos
Wagner (IFSC),
Rodrigo Lira (IFPE)



**DESENVOLVIMENTO
DE APLICATIVOS EMISSOR
E VERIFICADOR
DE CREDENCIAIS
VERIFICÁVEIS**

Do Papel ao Digital: IA e Blockchain na Gestão de Acervos Acadêmicos

AUTOMAÇÃO INTELIGENTE DA DIGITALIZAÇÃO DOCUMENTAL EM IES

Instituições de ensino superior brasileiras acumulam, ao longo de décadas, grandes volumes de documentos acadêmicos físicos, como históricos escolares, registros administrativos e outros documentos institucionais. A digitalização e organização desses acervos representam um grande desafio para universidades e centros acadêmicos, tanto pela complexidade operacional quanto pela necessidade de garantir integridade e preservação das informações. O projeto DAIESEB, desenvolvido no âmbito da iniciativa ILIADA, propõe uma solução tecnológica que utiliza Inteligência Artificial, visão computacional e blockchain para apoiar a digitalização e organização desses acervos acadêmicos. A plataforma permite processar documentos digitalizados, realizar a extração automática

de texto por meio de técnicas de OCR e estruturar metadados que facilitam a organização e recuperação das informações acadêmicas. Como mecanismo adicional de segurança, evidências criptográficas dos documentos processados são registradas em uma rede blockchain baseada em Hyperledger Fabric, permitindo verificar a integridade e rastreabilidade das informações ao longo do tempo. A solução foi desenvolvida com uma arquitetura baseada em microsserviços, o que permite escalabilidade e integração com sistemas acadêmicos existentes. Dessa forma, a iniciativa contribui para apoiar processos de transformação digital na educação superior brasileira, alinhando-se a iniciativas nacionais como o Diploma Digital e a Jornada do Estudante. ●

**IA
E BLOCKCHAIN
APLICADAS À
PRESERVAÇÃO
E GESTÃO DE
DOCUMENTOS
ACADÊMICOS**



FICHA
TÉCNICA

COORDENADOR-GERAL:
Rafael de Oliveira
Durá Eschrich
(Certisecure
Serviços Digitais
Ltda.), rafael.eschrich@gmail.com

COORDENADORA-ASSISTENTE:
Kamila Estevam
(Certisecure
Serviços
Digitais Ltda),
kamilaestevam@gmail.com

EQUIPE:
Rafael de Oliveira
Durá Eschrich,
Kamila Estevam,
Jean Martina,
Lucas Palma



QR CODE



CI BER SE GU RAN ÇA

58 **Hackers do Bem**

59 **Videobot:** quando aprender cibersegurança vira uma experiência interativa

60 **We Got Hacked!**
Um jogo educacional sobre resposta a incidentes cibernéticos

61 **Learn From Incidents:**
incidentes reais viram treino para defesa cibernética

62 Invada o **CASTELO**

63 A Nova Frente na Detecção de cibernética
Vulnerabilidades da RNP

64 Comitê Técnico de
Cibersegurança



CAPACITAÇÃO, INOVAÇÃO E COLABORAÇÃO PARA FORTALECER A CIBERSEGURANÇA NO PAÍS

Hackers do Bem

FORMAÇÃO DE PROFISSIONAIS E DESENVOLVIMENTO DE SOLUÇÕES EM CIBERSEGURANÇA

O programa Hackers do Bem foi criado com o objetivo de capacitar profissionais em cibersegurança e apoiar o desenvolvimento de soluções inovadoras para o setor, fortalecendo o ecossistema nacional de cibersegurança.

A formação é estruturada em uma trilha progressiva que combina aulas online, atividades teóricas e práticas e uma residência tecnológica onde os alunos aplicam os conhecimentos adquiridos em um ambiente real. Além da capacitação, o programa promove eventos como cybergames, hackathons e competições de Capture The Flag (CTF), que unem desafios técnicos e atividades colaborativas voltadas à geração e compartilhamento de conhecimento.

No campo de PD&I, o programa fomenta projetos voltados ao desenvolvimento de novas

ferramentas educacionais. Essa iniciativa contou com 12 Grupos de Trabalho executados em 2 ciclos, que envolveram mais de 80 bolsistas em atividades de pesquisa aplicada e resultando em ferramentas de código aberto que podem potencializar a formação de recursos humanos em cibersegurança. Nesta edição, apresentaremos os detalhes dos 5 GTs do segundo ciclo de PD&I do programa.

Complementando essas ações, o programa estrutura um hub nacional de cibersegurança que conecta estudantes, pesquisadores, empresas e instituições públicas, promovendo cooperação e oportunidades profissionais. Ao integrar capacitação, pesquisa aplicada e articulação institucional, o Hackers do Bem contribui para reduzir o déficit de especialistas e fortalecer a cibersegurança no país. ●



FICHA TÉCNICA

COORDENADORA-GERAL/ACADÊMICA:
Iara Machado (RNP),
iara.machado@rnp.br

COORDENADORA-ASSISTENTE:
Alessandra Poubel (RNP),
alessandra.poubel@rnp.br

EQUIPE:
Leandro Guimarães,
Emílio Nakamura,
Michelle Wangham,
Lisandro Granville,
Stela Toti, Luciana F.,
Rômulo P., Yve M., Renato D., Cristian G.



QR CODE



Videobot: quando aprender cibersegurança vira uma experiência interativa

APLICAÇÕES MULTIMÍDIA E IA PODEM TRANSFORMAR O APRENDIZADO

Em um cenário em que a educação em tecnologia cresce rapidamente, mas o engajamento dos estudantes nem sempre acompanha esse ritmo, novas formas de ensinar tornam-se essenciais. Nesse contexto surge o Videobot, uma abordagem que combina aplicações multimídia interativas, narrativa digital e análise de dados de aprendizagem para apoiar o ensino de cibersegurança. A iniciativa integra o projeto ViTuRi, desenvolvido no âmbito do Programa Hackers do Bem, e parte de uma ideia simples: transformar pequenos intervalos do cotidiano em oportunidades de aprendizado. Em vez de longas sessões de estudo, o estudante interage com episódios curtos projetados, nos quais as decisões tomadas ao longo da experiência influenciam o desenrolar da

narrativa. Diferentemente das aulas em vídeo tradicionais, em que o estudante é passivo, o Videobot utiliza aplicações multimídia interativas que respondem às escolhas do usuário. Cada decisão gera feedback dentro da própria narrativa, permitindo visualizar consequências, e aprender por experimentação. Por trás da experiência, o sistema registra dados de interação — como tempo de decisão, percursos escolhidos e padrões de resposta — que podem ser analisados para compreender o comportamento de aprendizagem. Essa infraestrutura abre espaço para o uso de inteligência artificial na recomendação de conteúdos, esclarecimento de dúvidas e adaptação de trilhas de aprendizagem possibilitando uma nova geração de ferramentas de ensino digital. ●



NO VIDEOBOT, CADA ESCOLHA MUDA A NARRATIVA E AJUDA A PERSONALIZAR O APRENDIZADO



FICHA TÉCNICA

COORDENADORA-GERAL/ACADÊMICA:
Danielle Rousy Dias Ricarte (Universidade Federal da Paraíba - UFPB / LAVID),
danielle@lavid.ufpb.br

COORDENADOR-ASSISTENTE:
Raoni Kulesza (Universidade Federal da Paraíba - UFPB / LAVID),
raoni@lavid.ufpb.br

EQUIPE:
Barbara Cavalcante,
Clarrissa Santos,
Gustavo Campos,
Herick Freitas,
Matheus Honório,
Pedro Alves,
Pedro Silveira,
Raissa Maiara



ENTIDADES PARCEIRAS

Laboratório de Aplicações de Vídeo Digital (LAVID) / Workverse



QR CODE



We Got Hacked! Um jogo educacional sobre resposta a incidentes cibernéticos

JOGO AUXILIA À TOMADA DE DECISÕES!

O We Got Hacked! é um jogo de simulação inspirado na rotina de um SOC para ensinar os processos de resposta a incidente e desenvolver a capacidade de tomada de decisões. O projeto busca equilibrar elementos lúdicos de um jogo com um cenário realista de um incidente cibernético. Para isso, o jogo apresenta o conflito entre uma organização petrolífera e um grupo hacktivista, em que o jogador assume diversos papéis no time de resposta a incidentes de um provedor de serviços de segurança, contratado pela petrolífera para monitorar os seus ativos. O jogo está organizado em três fases com complexidade crescente, cada uma representando um incidente cibernético distinto.



O OBJETIVO DO JOGO É APOIAR A FORMAÇÃO DE PROFISSIONAIS PARA ATUAR EM UM SOC

Na primeira fase, o jogador se depara com um ataque de pichação no site da organização petrolífera. Para resolver este incidente, o jogador deve tomar decisões, guiado por um *playbook* e pela troca de mensagens entre os personagens. A segunda fase simula um ataque de *ransomware* originado através da abertura indevida de um *phishing* na empresa petrolífera. Na fase final, o jogador precisa responder um incidente de vazamento resultante da exfiltração de dados confidenciais pelo grupo hacktivista. O We Got Hacked! é um projeto inovador para educação em cibersegurança e foi concebido para o cenário nacional, por isso o jogo foi desenvolvido em língua portuguesa. ●



FICHA TÉCNICA

COORDENADOR-GERAL/ACADÊMICO:

Luciano Ignaczak
(Unisinos),
lignaczak@
unisinos.br

EQUIPE:

Bernardo Klein,
Frank Veja, Igor
Flores, Jairo
Augusto de
Campos Alff,
Maurício Bammann
Gehling, Rodrigo
Steigleder, Tiago
Umberto Gazzola



ENTIDADES PARCEIRAS

Universidade
do Vale do Rio dos
Sinos (UNISINOS),
Atomic Rocket
Solutions,
ServiceIT Security,
DropReal, CAIS RNP



QR CODE



INCIDENTES REAIS ANONIMIZADOS VIRAM TREINO PRÁTICO COM IA E VALIDAÇÃO HUMANA

Learn From Incidents: incidentes reais viram treino para defesa cibernética

SOLUÇÃO INTEGRA CAPACITAÇÃO PRÁTICA E APOIO OPERACIONAL

Aprender a responder a incidentes de segurança exige mais do que teoria. Exige contato com situações reais, decisões sob pressão e compreensão dos fluxos usados pelas equipes que atuam na linha de frente. O GT-LFI foi criado justamente para aproximar formação e prática operacional, transformando incidentes reais anonimizados em experiências de aprendizagem e apoio à resposta. Desenvolvido no Programa Hackers do Bem, o projeto integra quatro frentes: anonimização de dados sensíveis, classificação automática de incidentes com IA, validação humana por estagiários e analistas e uma plataforma gamificada orientada ao desenvolvimento

de competências. O resultado é uma solução que ajuda a treinar novos profissionais e, ao mesmo tempo, contribui para tornar mais ágil e padronizado o tratamento de tickets de segurança em PoPs e CSIRTs. Em 2025, o GT-LFI entregou um MVP funcional, validado com incidentes reais, e acumulou resultados expressivos de pesquisa e inovação, com trabalhos aceitos em conferências científicas nacionais e internacionais. A próxima etapa é ampliar a base de incidentes, refinar a experiência da plataforma e avançar na consolidação da solução como referência em capacitação e apoio à resposta a incidentes. ●



FICHA TÉCNICA

COORDENADOR-GERAL/ACADÊMICO:

Rodrigo Sanches
Miani (UFU),
miani@ufu.br

EQUIPE:

Silvio Ereno
Quincozes, Diego
Luis Kreutz,
Leandro Bertholdo



ENTIDADES PARCEIRAS

UFU, UNIPAMPA,
UFRGS



QR CODE



Invada o CASTELO

ENSINANDO ATAQUE E DEFESA EM SISTEMAS E REDES



UMA PLATAFORMA COMPLETA E FLEXÍVEL PARA COMPETIÇÕES E TREINAMENTOS EM CIBERSEGURANÇA!

A plataforma CASTLE foi projetada para oferecer eficiência na hospedagem e no gerenciamento simultâneo de diversos desafios, trilhas e eventos. Para isso, utiliza estratégias leves de virtualização, ajustando dinamicamente os recursos conforme o perfil e a demanda dos usuários ativos, com opções para a criação de cenários de ataque e defesa. Embora esse modelo exija maior consumo de recursos computacionais, ele proporciona um nível superior de isolamento em ambientes de CTF, essencial para alguns tipos de desafios. Considerando as ameaças cibernéticas atuais, enfrenta-se um importante desafio: garantir a segurança digital diante da volatilidade das tecnologias emergentes e do alto valor agregado das operações executadas e dos dados

armazenados. Enfrentar esse desafio requer a formação de recursos humanos especializados em cibersegurança, capazes de identificar vulnerabilidades e desenvolver contramedidas eficazes e eficientes. Nesse contexto, a plataforma CASTLE surge oferecendo desafios didáticos e práticos de cibersegurança, relacionados às atividades de red, blue e purple team. A plataforma inclui atividades de treinamento e competições voltadas a atender, de forma personalizada, as necessidades de indivíduos, grupos e instituições interessadas. Entre os diferenciais da plataforma, destacam-se um sistema de gamificação baseado em níveis de conhecimento e um sistema de sugestão de atividades, competições e adversários com base nesses níveis. ●



FICHA TÉCNICA

COORDENADOR-GERAL/ACADÊMICO:

André Ricardo
Abed Grégio
(Universidade Federal do Paraná - UFPR),
gregio@ufpr.br

COORDENADOR-ASSISTENTE:

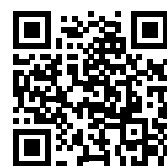
Vinicius
Fülber Garcia
(Universidade Federal do Paraná - UFPR),
viniciusfulber@ufpr.br

EQUIPE:

André Grégio,
Vinicius Garcia,
Nadia Lobkov,
Jorge Correia,
João Andreotti,
Claudio Torres Jr.,
Fernando Kiotheka,
Matheus Herbele



QR CODE



A Nova Frente na Detecção de cibernética Vulnerabilidades da RNP

VALIDAÇÃO RÁPIDA DE VULNERABILIDADES NO SISTEMA RNP

O aumento das vulnerabilidades em redes e aplicações exige soluções ágeis e automatizadas. O GT-SITV, desenvolvido pela UFRN a partir do 2º Hackathon RNP, surge com o propósito de fortalecer a segurança digital do Sistema RNP por meio de uma plataforma web voltada à identificação e mitigação de vulnerabilidades. A ferramenta permite que gestores e analistas de PoPs validem vulnerabilidades reportadas pelo SGIS em minutos, sem necessidade de expertise técnica. O processo inclui login federado via CAFe, seleção da vulnerabilidade, validação

automatizada e geração de relatórios profissionais com recomendações específicas de correção. Com suporte a APIs para integração com outros sistemas, o GT-SITV promove validação contínua e interoperabilidade. Resultados da Prova de Conceito com PoPs da Bahia, Pernambuco e Paraná mostraram ganhos em tempo, autonomia e compliance. Assim, o projeto consolida-se como um avanço significativo rumo a uma gestão de segurança simples, auditável e eficiente em todo o Sistema RNP. ●



FICHA TÉCNICA

COORDENADOR-GERAL/ACADÊMICO:

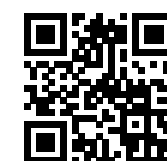
Rildo Antonio
de Souza (RNP),
rildo.souza@rnp.br

EQUIPE:

Matheus Vidal,
Paula Marinho,
Isabela Gomes



QR CODE



GT-SITV VALIDA NOTIFICAÇÕES SGIS EM MINUTOS PARA POPS RNP VIA WEB

Comitê Técnico de Cibersegurança

DADOS DE CIBERSEGURANÇA DISPONÍVEIS PARA A COMUNIDADE

A Chamada Pública de Trabalhos de Prospeção Tecnológica para o Comitê Técnico de Cibersegurança (CT-Cibersegurança) teve como objetivo desenvolver uma infraestrutura de coleta, anonimização e publicação de conjuntos de dados de cibersegurança. Relatórios de vulnerabilidades e incidentes coletados pela RNP foram disponibilizados pelo Centro de Atendimento a Incidentes de Segurança (CAIS). Com objetivo de anonimizar tais relatórios, quatro projetos foram desenvolvidos por pesquisadores da UFCG, UFF, UFRJ e Unipampa. Os projetos envolveram o desenvolvimento de um fluxo de trabalho com ferramentas de código aberto que implementam métodos para transformar dados e métodos para analisar a utilidade dos

dados de saída anonimizados, de um método semiautomatizado de anonimização de dados que aplica k-anonimato por supressão em atributos estruturados e regex com otimização bayesiana, de um algoritmo de anonimização baseado em Transformers para agrupamento semântico e em grandes modelos de linguagem para rotulação de dados e de um método de pseudonimização baseada em HMAC-SHA256 para gerar pseudônimos fortes e reversíveis. O próximo passo será disponibilizar o resultado dos projetos à comunidade e também os conjuntos de dados de cibersegurança anonimizados, já que esta é uma demanda levantada pelos membros do CT-Cibersegurança para realização de pesquisas pela comunidade científica. ●



FICHA TÉCNICA

COORDENADOR-GERAL/ACADÊMICO:
Igor Moraes (UFF),
igor@ic.uff.br

COORDENADOR-ASSISTENTE:
Ian Bastos (UERJ), ian.bastos@eng.uerj.br

EQUIPE:
Secretário:
Reinaldo Gomes



QR CODE



PROJETOS DE PROSPECÇÃO TECNOLÓGICA DESENVOLVERAM SOLUÇÕES PARA ANONIMIZAÇÃO DE DADOS

PD&I SERVIÇOS AVANÇADOS

- 66 **MaisAção:** Gamificando a Inserção Curricular da Extensão
- 67 **Rumo à CAFe 2.0:** GT-BAITA propõe nova infraestrutura federada
- 68 Gestão Acadêmica Inteligente com a **Plataforma AVIDA.AI**
- 69 **SIGAME:** do vídeo ao material de estudo em minutos
- 70 **IoTedu:** conectividade segura com inteligência artificial para IoT acadêmica
- 71 **GT LLMestre**
- 72 **Sokrates.AI**

MaisAção:

Gamificando a Inserção Curricular da Extensão

UMA PLATAFORMA BASEADA EM INTELIGÊNCIA ARTIFICIAL

A inserção curricular da extensão configura-se como estratégia central para integrar ensino, pesquisa e extensão, promovendo formação socialmente referenciada e comprometida com a transformação da realidade. Contudo, persiste a carência de ferramentas tecnológicas que ofereçam suporte integrado à sua implementação, especialmente quanto à gestão sistemática de evidências institucionais e ao engajamento discente na integralização de, no mínimo, 10% da carga horária dos cursos em atividades extensionistas.

Nesse contexto, o GT MaisAção propõe uma plataforma para organizar a inserção curricular de forma integrada. A solução permite que a comunidade externa registre demandas para a Instituição de Ensino Superior (IES), as quais passam por triagem e são encaminhadas

a docentes ou armazenadas em um banco de oportunidades. A partir dessas demandas, o professor cria ações de extensão, abre inscrições para estudantes, registra evidências e atribui insígnias como estratégia de engajamento. A plataforma oferece ainda APIs para integração com sistemas acadêmicos, *dashboards* para monitoramento da carga horária, recursos de inteligência artificial para agilizar cadastros e um módulo público de divulgação de resultados. A ferramenta está em fase de testes na UFSM, Universidade Federal do Rio Grande do Sul (UFRGS), Universidade Federal de Ciências da Saúde de Porto Alegre (UFCSPA), Universidade Estadual do Norte Fluminense Darcy Ribeiro (UENF) e Universidade Federal do Espírito Santo (UFES). ●



FICHA TÉCNICA

COORDENADOR-GERAL/ACADÊMICO:

Ricardo Tombesi Macedo
(Universidade Federal de Santa Maria),
ricardotombesi@ufsm.br

LÍDER DE INOVAÇÃO:

Betania Vahl de Paula (Startup Performance Vegetal), contato@performancevegetal.com.br

EQUIPE:

Arthur Guarizi de Godoy, Eliane Cristina Amoretti, Karina Lira Ohara, Leon Tassinari Julião, Marco André Babinski



QR CODE



UMA PLATAFORMA QUE ORGANIZA TODO O PROCESSO DA INSERÇÃO CURRICULAR DA EXTENSÃO



Rumo à CAFe 2.0:

GT-BAITA propõe nova infraestrutura federada

PROJETO MODERNIZA A FEDERAÇÃO ACADÊMICA

A Comunidade Acadêmica Federada (CAFe) conecta mais de 320 instituições de ensino e pesquisa no Brasil, permitindo que estudantes, professores e pesquisadores utilizem suas identidades institucionais para acessar serviços digitais oferecidos por diferentes organizações. Muitos usuários finais desconhecem os serviços disponibilizados na CAFe. O compartilhamento de aplicações e recursos ainda ocorre de forma limitada. Assim, a CAFe é percebida como um meio de acesso a serviços da RNP, e não como um ambiente amplo de cooperação digital.

Diante desse cenário, o Grupo de Trabalho Barramento de Interoperabilidade Acadêmica (GT-BAITA) propõe uma evolução da federação. A iniciativa busca, além de atualizar tecnologicamente a federação, reposicionar

a CAFe como um ecossistema de interoperabilidade acadêmica, promovendo integração e ampliando o compartilhamento de serviços e recursos digitais entre instituições. Entre os componentes do barramento estão: um Sistema de Gestão da Federação, que simplifica o onboarding e a administração de provedores de identidade e de serviço; um Portal de Benefícios voltado aos usuários finais, que integra serviços da própria instituição e da RNP em um único ambiente, utilizando autenticação federada, além da coleta automática de métricas e observabilidade dos serviços; e um novo Portal Where Are You From (WAYF), que, além de seu papel tradicional, também desempenha a função de normalizador sintático e semântico de atributos da identidade do usuário. ●



FICHA TÉCNICA

COORDENADOR-GERAL/ACADÊMICO:

Frederico Schar Dong
(Instituto Federal do Rio Grande do Sul), frederico.schar Dong@ifrs.edu.br

LÍDER DE INOVAÇÃO:

Eduardo Perottoni (Universidade Federal de Santa Catarina), edu.perottoni@gmail.com

EQUIPE:

Ricardo Custódio, Brendon V. Silva, Giulia Manno Lima, Alison De Rozado Batista, Leonardo M. dos Passos, Charlie E. Terra, Raissa M. Lima, Rayane M. Castilhos



ENTIDADES PARCEIRAS

IFRS e UFSC



QR CODE



PROJETO PROPÕE NOVA ARQUITETURA PARA AMPLIAR O PAPEL DA CAFe NA COLABORAÇÃO ACADÊMICA





TRANSFORME DADOS ACADÊMICOS EM INTELIGÊNCIA DE GESTÃO

Gestão Acadêmica Inteligente com a Plataforma AVIDA.AI

DADOS CIENTÍFICOS INTEGRADOS PARA DECISÕES ESTRATÉGICAS

A Plataforma AVIDA.AI apoia coordenadores de curso e programas de pós-graduação na tomada de decisões baseadas em dados consolidados. Integrando automaticamente múltiplas bases acadêmicas nacionais e internacionais, a solução organiza, cruza e interpreta informações científicas de forma estratégica. Com recursos de análise automatizada, processamento de linguagem natural e inteligência artificial, a AVIDA permite acompanhar indicadores de produção, avaliar impacto nacional e internacional, monitorar orientações, mapear colaboração entre pesquisadores e identificar oportunidades

de melhoria do seu programa de pós-graduação. O coordenador deixa de agir apenas no momento da avaliação formal e passa a realizar autodiagnósticos contínuos, antecipando riscos e fortalecendo o planejamento do programa. A interface conversacional funciona como um copiloto de gestão, respondendo perguntas estratégicas em linguagem natural e transformando dados dispersos em diagnósticos objetivos sobre a real situação do programa. Mais do que gerar relatórios, a AVIDA promove governança orientada por evidências e eleva o desempenho institucional de forma contínua. ●



FICHA TÉCNICA

COORDENADOR-GERAL/ACADÊMICO:
Reginaldo Santos
(Universidade Federal do Pará),
regicsf@ufpa.br

LÍDER DE INOVAÇÃO:
Sintia Silva de Almeida
(Universidade Federal do Pará),
sintiaalmeida@gmail.com

EQUIPE:
Vinícius Abreu,
Marcelle Mota,
Victor Pinto,
José Perdígão,
Thiago Correa,
Cristiano Monteiro,
Helder Matos,
Atilio Azevedo



STARTUP PARCEIRA

Katu Data
Visualization



QR CODE



SIGAME: do vídeo ao material de estudo em minutos

IA PARA TRANSFORMAR AULAS GRAVADAS EM CONTEÚDO SUPLEMENTAR



Aulas gravadas, webinários e treinamentos se multiplicam nas instituições de ensino, mas o conteúdo ainda permanece restrito a horas de vídeo. Revisar, localizar um trecho específico e transformar a gravação em material de estudo ou consulta costuma exigir tempo e esforço. O SIGAME (Sistema Inteligente de Geração Automática de Materiais Educacionais) resolve esse gargalo: a partir de um vídeo enviado como arquivo ou link, a solução produz materiais prontos para estudo e pesquisa. Quando o usuário anexa um PDF de slides, as imagens são incorporadas ao longo do texto como referência, facilitando a leitura, a navegação e a compreensão.

Com o SIGAME, o mesmo conteúdo pode virar notas de aula organizadas por seções, resumos objetivos, flashcards e listas de exercícios, além de uma versão de texto tratado, ideal para busca e para bases de conhecimento. Em avaliações iniciais, a solução reduziu em torno de 60% o tempo gasto na revisão e organização do material, quando comparada ao fluxo comum de transcrição e ao tratamento com ferramentas genéricas de IA. O SIGAME é desenvolvido no âmbito do Programa de PD&I Serviços Avançados da RNP, voltado à comunidade de ensino e pesquisa, em parceria com o CRIAR, do CIn-UFPE. ●



FICHA TÉCNICA

COORDENADOR-GERAL/ACADÊMICO:
Tsang Ing Ren
(CIn-UFPE), tir@cin.ufpe.br

LÍDER DE INOVAÇÃO:
Paulo Borba (CIn-UFPE), phmb@cin.ufpe.br

EQUIPE:
Érico Medeiros,
João Oliveira, Kauã Lima,
Lígia Padilha,
Lucas Gonçalves,
Mateus Baltazar,
Rafael Barros



ENTIDADES PARCEIRAS

CRIAR - Centro de Inovação em Robótica e Inteligência Artificial Responsável



QR CODE



DO VÍDEO AO MATERIAL SUPLEMENTAR: FIEL AO CONTEÚDO ORIGINAL, COM SLIDES INTEGRADOS

IoTedu: conectividade segura com inteligência artificial para IoT acadêmica

PLATAFORMA AUTOMATIZA CADASTRO E MONITORA RISCOS EM IOT

Levar de dois a seis dias úteis para liberar um dispositivo IoT na rede ainda é realidade em muitas universidades brasileiras. Em alguns casos, a alternativa é ainda mais preocupante: redes abertas, sem controle adequado sobre os equipamentos conectados. O IoTedu surge para transformar esse cenário. Desenvolvido no âmbito do GT-IoTEdu da RNP, coordenado pela UNIPAMPA em parceria com UFRGS, UFU e UFF, o projeto oferece uma plataforma de conectividade especializada para ambientes acadêmicos com IoT. A solução permite o onboarding rápido de dispositivos por meio de autenticação federada, inventário centralizado e aplicação de políticas de acesso alinhadas aos contextos de ensino e pesquisa.



DISPOSITIVOS IOT CADASTRADOS EM SEGUNDOS E MONITORADOS POR INTELIGÊNCIA ARTIFICIAL

Em poucos minutos, docentes e pesquisadores podem cadastrar dispositivos de forma autônoma, enquanto as equipes de TI passam a contar com um painel unificado para acompanhar conectividade, conformidade e comportamento dos equipamentos conectados. O núcleo tecnológico da plataforma é uma arquitetura de segurança multicamadas baseadas na integração de IDSs consolidados com técnicas de aprendizado de máquina, capaz de detectar ataques conhecidos e identificar comportamentos anômalos na rede. Pilotos estão previstos para 2026 na UNIPAMPA, UFRGS e UFU, com potencial de expansão para hospitais universitários, ambientes de indústria 4.0 e o agronegócio. ●



FICHA TÉCNICA

COORDENADOR-GERAL/ACADÊMICO:
Diego Kreutz (Unipampa), diegokreutz@unipampa.edu.br

LÍDER DE INOVAÇÃO:
Vagner Quincozes (UFF), vequincozes@id.uff.br

EQUIPE:
Leandro Bertholdo, Rodrigo Mansilha, Rodrigo Miani, Silvío Quincozes, Angelo N., Anna R., Douglas F., Emanuel C., Joner A., Leonardo B., Matheus C.



ENTIDADES PARCEIRAS

UNIPAMPA, UFRGS, UFU, UFF



QR CODE

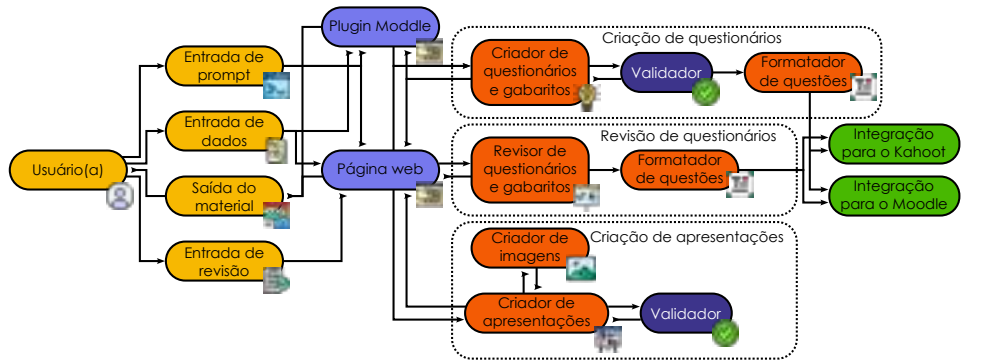


GT LLMestre

DISPONIBILIZAÇÃO E CRIAÇÃO DE CONTEÚDO ACADÊMICO COM AGENTES DE IA

Professores universitários enfrentam uma significativa carga de trabalho ao elaborar novas disciplinas, como planejar conteúdos e preparar materiais didáticos. Essa carga reduz a possibilidade de atualizar os cursos com frequência e limita a diversidade de disciplinas ofertadas. Para solucionar esse problema, o GT LLMestre desenvolve uma plataforma para automatizar a criação de conteúdos didáticos, utilizando agentes de IA especializados integrados a LLMs (Grandes Modelos de Linguagem). A plataforma do GT LLMestre é desenvolvida no framework de agentes LangFlow, com a qual criam-se fluxos que envolvem agentes de IA para executar as diferentes tarefas necessárias. Na arquitetura da solução, o usuário pode

acessar a plataforma por uma interface web. Além disso, há a possibilidade de utilizar o sistema diretamente no Moodle como um plugin. Para a criação de apresentações e questionários, o usuário detalha seu pedido pela entrada de prompt e insere documentos com informações importantes pela entrada de dados. Os resultados são recebidos pela saída de material. Uma das preocupações da plataforma desenvolvida é criar conteúdo apenas com o material que o professor fornece, evitando a inserção de informações incorretas causadas por alucinações dos LLMs. Ao fim da criação de um questionário, o usuário pode revisá-lo, utilizando a entrada de revisão. Assim, os agentes podem atuar na revisão a partir das solicitações do usuário. ●



O GT LLMESTRE DESENVOLVE UMA PLATAFORMA PARA AUTOMATIZAR A CRIAÇÃO DE CONTEÚDOS DIDÁTICOS



FICHA TÉCNICA

COORDENADOR-GERAL/ACADÊMICO:
Rodrigo de Souza Couto (UFRJ), rodrigo@gti.ufrrj.br

LÍDER DE INOVAÇÃO:
Leonardo Picciani (Black Bear Bytes), leo@blackbearbytes.com

EQUIPE:
Felipe Táparo, Fernando Silva, Guilherme Silva, João Sobrinho, Lucas Souza, Luís Costa, Maria Sales, Miguel Campista, Pedro Cruz, Pedro Rubinstein



QR CODE



Sokrates.AI

PLATAFORMA SOCRÁTICA DE CONHECIMENTO

O Sokrates.AI é um mentor inteligente para o ensino superior, baseado em Inteligência Artificial Generativa e no Método Socrático para promover aprendizagem ativa, pensamento crítico e autonomia intelectual. Diferente de tutores tradicionais, ele não fornece apenas respostas, mas conduz o estudante através de perguntas, reflexões e desafios que estimulam a Construção do Conhecimento. A solução responde a desafios centrais do ensino superior. Para estudantes, oferece motivação e aprendizagem personalizada, tornando-o protagonista no processo de ensino-aprendizagem. Para instituições, contribui para aumentar o engajamento e reduzir a evasão escolar. Sua tecnologia proprietária, LearningFlow, organiza a Construção do Conhecimento, através

de jornadas adaptativas de estudo baseadas no Diálogo Socrático, enquanto um gêmeo digital do aluno modela competências, lacunas e preferências de aprendizagem para orientar a personalização. Inspirado na Teoria da Autodeterminação, ele estimula autonomia, competência e pertencimento. O aprendizado é consolidado por meio de exercícios, autoavaliações e desafios integrados ao diálogo. Tecnicamente, o Sokrates.AI utiliza uma arquitetura “agentic”, baseada em múltiplos agentes inteligentes, serviços especializados e modelos de linguagem de grande escala (LLMs). Assim, o Sokrates.AI transforma o estudo passivo e a memorização em um processo contínuo de descoberta e construção ativa do conhecimento. ●



FICHA TÉCNICA

COORDENADOR-GERAL/ACADÊMICO:

Geraldo Bonorino
Xexéo (COPPE/UFRJ), xexeo@cos.ufrj.br

LÍDER DE INOVAÇÃO:

Claudio Dipolitto
(InoveLab: Inovação, Cultura e Desenvolvimento LTDA), claudiodipolitto@gmail.com

EQUIPE:

Claudia Susie
Camargo Rodrigues,
Débora de Oliveira
Souza, Gabriele
Iwashima, Luiz
Felipe Cantanhede
Cristino, Vitória
Nazareth, Thomas
Cardoso



QR CODE



ESTUDO PERSONALIZADO E MENTORIA COM IA SOCRÁTICA PARA TRANSFORMAR O APRENDIZADO



27
Workshop
RNP



OpenRAN@Brasil é um programa do MCTI que impulsiona redes abertas no país com pesquisa, inovação e capacitação em 5G e além. Coordenado pela RNP, conta com a execução da RNP, CPQD, Inatel e Eldorado, amplia testes e infraestrutura nacional, fomentando aplicações em indústria, agro, cidades e educação. Faz parte do Programa Prioritário de Informática [PPI] Internet Avançada, com recursos da Lei nº 8.248, de 23 de outubro de 1991 [Lei de Informática].

Conheça e descubra como sua instituição pode utilizar o testbed do programa.

<https://openranbrasil.org.br/>



EXECUÇÃO

RNP

cpqd

ELDORADO
INSPIRAÇÃO PELO NOVO

Inatel

COORDENAÇÃO

RNP

ORGANIZAÇÃO

MINISTÉRIO DA
CIÊNCIA, TECNOLOGIA
E INOVAÇÃO

GOVERNO DO
BRASIL
DO LADO DO POVO BRASILEIRO

Projeto apoiado pelo Ministério da Ciência, Tecnologia e Inovação, com recursos da Lei nº 8.248, de 23 de outubro de 1991, conforme orientação da Secretaria de Empreendedorismo e Inovação.