DPI-Lab
Infraestrutura Pública Digital

NOTA TÉCNICA
Nº 01/2026

INFRAESTRUTURA PÚBLICA COMO BEM COMUM



Infraestruturas Públicas Digitais e Bens Públicos Digitais

Aprendizados da Experiência Indiana e Perspectivas de Aplicação nas Políticas Públicas Brasileiras

INSTITUIÇÃO NEES / Universidade Federal de Alagoas

LOCAL E DATA Maceió/AL, outubro de 2026

REALIZAÇÃO NEES 15 anos

2026

NOTA TÉCNICA Nº 01/2026

Infraestruturas Públicas Digitais e Bens Públicos Digitais: Aprendizados da Experiência Indiana e Perspectivas de Aplicação nas Políticas Públicas Brasileiras

AUTORIA

André Magno Costa de Araújo
NEES/UFAL

Ana Beatriz Moreira Santos Fernandes
NEES/UFAL

Alisson Werner Arruda de Arruda
NEES/IFPB

José Vitor de Abreu Silva
NEES/UFAL

Márcio Alexandre Pereira da Silva
NEES/UFAL

Maria Andreza Correia da Silva
NEES/UFAL

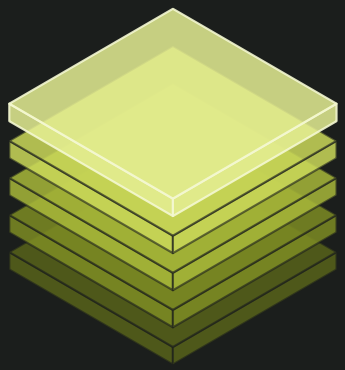
Patrick Henrique da Silva Brito
NEES/UFAL

→ Biografias completas em Sobre os autores, na última página.

ISBN
978-65-02-48803-4

COMO CITAR

ARAÚJO, André Magno Costa de et al. Infraestruturas Públicas Digitais e Bens Públicos Digitais: aprendizados da experiência indiana e perspectivas de aplicação nas políticas públicas brasileiras. Nota Técnica nº 01/2026. Maceió: DPI-Lab, NEES/UFAL, 2026. ISBN 978-65-02-48803-4.



REALIZAÇÃO

DPI-Lab
Infraestrutura Pública Digital

NEES 15 anos

Universidade Federal de Alagoas
Maceió/AL · 2026

Sumário

Prefácio 5

Sumário Executivo 6

01 Introdução 7

1.1 Transformação digital e desafios das políticas públicas 7
1.2 Infraestruturas públicas digitais como abordagem tecnológica 8
1.3 Contextualização da missão técnica Brasil-Índia 9
1.4 Objetivo e escopo da nota técnica 10
1.5 Organização do Documento 10

02 Fundamentos de DPI e DPG 12

2.1 Conceitos e evolução das infraestruturas públicas digitais 12
2.2 Bens públicos digitais e ecossistemas de software aberto 14
2.3 Princípios arquiteturais: modularidade, interoperabilidade, escalabilidade e reutilização 15
2.4 Governança, privacidade, segurança e proteção de dados 16
2.5 Modelos de sustentabilidade e colaboração em ecossistemas digitais 17

03 Experiência Indiana: Ecossistema e Aprendizados 19

3.1 O ecossistema Sunbird: origem, composição e evidências de escala 19
3.2 Blocos em destaque: Spark, RC e Obsrv 21
3.3 Aprendizados sobre engenharia de software, governança e sustentabilidade 22

04 Oportunidades de Aplicação em Políticas Públicas Educacionais 25

4.1 Contexto das políticas públicas educacionais e seus ecossistemas digitais 25
4.2 Casos de uso e oportunidades de experimentação 27

05 Arquitetura de Referência e Diretrizes Técnicas 32

5.1 Premissas e requisitos arquiteturais 32
5.2 Modelo conceitual de uma arquitetura baseada em DPI/DPG 33
5.3 Componentes compartilhados e integração com sistemas de software existentes 34
5.4 Governança de dados, segurança e observabilidade 35
5.5 Diretrizes de engenharia de software e evolução tecnológica 35
5.6 Critérios de validação e avaliação técnica 35

06 DPI e DPG na Prática: Um Exemplo com Credenciais Verificáveis - Sunbird RC 37

6.1 O cenário: comprovar o percurso durante o curso . . . 38
6.2 Implementação e execução da prova de conceito . . . 38
6.3 Resultados e alcance da prova de conceito . . . 39

07 Cooperação Continuada e Apoio à Adoção 44

7.1 Alinhamento continuado com o ecossistema . . . 44
7.2 Capacidades disponíveis para apoio a instituições . . . 45
7.3 Colaboração institucional e participação no ecossistema . . . 46

08 Considerações Finais 47

Referências 49

APÊNDICES

A Cenário ilustrado: a trajetória de Luana 53

Prefácio

Cara leitora, caro leitor,

Ao longo dos últimos anos, tenho acompanhado de perto como a pesquisa científica e o desenvolvimento tecnológico podem contribuir para enfrentar desafios concretos das políticas públicas brasileiras. Essa experiência tem reforçado uma convicção: a tecnologia alcança seu maior valor quando o conhecimento produzido na academia se transforma em soluções que beneficiam a sociedade.

É com essa perspectiva que apresento o DPI Lab, uma iniciativa do Núcleo de Excelência em Tecnologias Sociais (NEES), da Universidade Federal de Alagoas (UFAL), dedicada à pesquisa e ao desenvolvimento de Infraestruturas Públicas Digitais (DPI) e Bens Públicos Digitais (DPG). Nossa intenção é contribuir para uma agenda tecnológica que valorize a colaboração, o compartilhamento de conhecimentos e o desenvolvimento de soluções sustentáveis para o setor público.

Esta primeira nota técnica nasce também de uma experiência muito significativa de cooperação internacional. A aproximação com o International Institute of Information Technology Bangalore (IIIT-B) e o Centre for Open Societal Systems (COSS), na Índia, permitiu reunir diferentes experiências e perspectivas sobre o desenvolvimento de tecnologias de interesse público. Mais do que conhecer abordagens utilizadas em outro país, buscamos construir uma colaboração duradoura, na qual o conhecimento e as capacidades desenvolvidas por nossas instituições possam contribuir mutuamente.

Ao iniciar esta série de publicações, queremos compartilhar não apenas resultados, mas também reflexões, aprendizados e questões que orientarão nossas próximas pesquisas. Acreditamos que o avanço das Infraestruturas Públicas Digitais no Brasil depende do diálogo entre universidades, governos e outras instituições comprometidas com o interesse público.

Espero que esta leitura desperte novas ideias, estimule discussões e abra oportunidades de colaboração. Acima de tudo, que contribua para aproximar ainda mais o conhecimento científico das necessidades da sociedade brasileira.

Boa leitura!

Prof. Dr. André Magno Costa de Araújo
Diretor Executivo - NEES
Maceió, novembro de 2026

Resumo

A evolução das políticas públicas exige soluções tecnológicas capazes de integrar informações, compartilhar capacidades e acompanhar as mudanças nas necessidades da administração pública. Nesse contexto, as Infraestruturas Públicas Digitais (DPI) e os Bens Públicos Digitais (DPG) oferecem oportunidades para ampliar a interoperabilidade e a reutilização de componentes de software, aproveitando os investimentos e as capacidades tecnológicas já existentes. Esta nota técnica analisa essas possibilidades com base na experiência indiana no ecossistema Sunbird, combinando fundamentos científicos, análise arquitetural e experimentação prática para identificar caminhos de aplicação no contexto brasileiro.

A análise evidencia que o principal valor dessa abordagem reside na construção de capacidades digitais compartilhadas, sustentadas por padrões abertos, responsabilidades institucionais bem definidas e mecanismos de governança que assegurem sua evolução. A experiência com o Sunbird demonstra como componentes modulares podem apoiar diferentes serviços e políticas públicas, preservando a autonomia das instituições responsáveis pelos dados e pelos processos. Também evidencia que a reutilização tecnológica requer mais do que a disponibilização de código: depende de especificações interoperáveis, de manutenção contínua e de participação ativa no ecossistema de desenvolvimento.

No contexto brasileiro, foram identificadas oportunidades de aplicação em políticas públicas educacionais, abrangendo a emissão e a verificação de credenciais, o compartilhamento seguro de informações e a observabilidade de dados. A análise considera iniciativas como o Programa Nacional do Livro e do Material Didático (PNLD) e os ecossistemas de dados educacionais e propõe possibilidades de integração que preservam os sistemas de software existentes. Como contribuição técnica, foi elaborada uma arquitetura de referência e desenvolvida uma prova de conceito com o Sunbird RC, demonstrando o fluxo de emissão, apresentação e verificação de credenciais digitais em ambiente controlado.

Os resultados indicam caminhos para a adoção progressiva dessas tecnologias, mediante experimentações delimitadas, avaliação da interoperabilidade e definição de responsabilidades relativas a dados e componentes compartilhados. A continuidade do trabalho prevê a integração com aplicações de software em produção, a ampliação dos cenários experimentais e o aprofundamento da cooperação com o ecossistema internacional. Essas atividades orientarão a próxima nota técnica, com foco na avaliação das abordagens em condições reais de aplicação.

SEÇÃO 01

Introdução

Esta seção apresenta os desafios da transformação digital no setor público, introduz os conceitos de Infraestruturas Públicas Digitais (*Digital Public Infrastructure*, DPI) e Bens Públicos Digitais (*Digital Public Goods*, DPG) e contextualiza a missão técnica Brasil–Índia, com destaque para o ecossistema Sunbird. Por fim, são apresentados os objetivos, o escopo e a organização desta nota técnica.

1.1 Transformação digital e desafios das políticas públicas

A forma como os governos desenvolvem e oferecem serviços públicos tem passado por mudanças significativas com o avanço das tecnologias digitais [1]. Processos antes conduzidos de maneira isolada passaram a contar com aplicações de software capazes de apoiar a gestão de informações, automatizar atividades e ampliar o alcance das políticas públicas [2, 3]. Nesse cenário, a transformação digital representa não apenas a incorporação de novas tecnologias, mas também uma mudança na forma como as instituições públicas organizam seus processos, utilizam dados e se relacionam com a sociedade [4, 1].

A transformação digital tem ampliado o uso de aplicações de software na administração pública, especialmente em políticas que envolvem diferentes instituições, grandes volumes de dados e milhões de cidadãos. Essas aplicações desempenham funções essenciais na execução, no acompanhamento e na avaliação de programas governamentais, contribuindo para a gestão de processos e a oferta de serviços públicos em larga escala [5]. Nesse cenário, a crescente dependência de tecnologias digitais reforça a necessidade de assegurar a continuidade operacional, a capacidade de evolução e a interoperabilidade entre sistemas de software. Isso inclui a adoção de mecanismos de monitoramento contínuo, capazes de acompanhar o funcionamento das aplicações e identificar possíveis falhas [6, 4].

Um dos desafios desse cenário está relacionado à forma como as aplicações de software utilizadas pelo setor público são concebidas e desenvolvidas [7]. Historicamente, muitas delas foram construídas para atender às necessidades específicas de órgãos, programas ou políticas públicas. Embora essa abordagem tenha possibilitado avanços importantes, ela também pode resultar em ambientes tecnológicos fragmentados, caracterizados pela adoção de padrões distintos, por dificuldades de interoperabilidade e pela necessidade de desenvolver mecanismos específicos de integração entre plataformas computacionais [6]. Além disso, a implementação de funcionalidades semelhantes em diferentes aplicações de software pode gerar redundâncias e duplicação de dados mestres, dificultando a consistência das informações e aumentando os esforços necessários à manutenção e à evolução dos sistemas computacionais [4, 8].

Esses desafios tornam-se particularmente relevantes em políticas públicas de grande abrangência,

cujas necessidades tecnológicas evoluem continuamente em função de mudanças nos processos, nas regras de funcionamento e nas demandas da sociedade [6]. Nessas condições, a sustentabilidade das aplicações de software depende não apenas da infraestrutura computacional disponível, mas também de sua capacidade de adaptação, escalabilidade e integração com outras aplicações de software. Isso exige abordagens que considerem a evolução tecnológica de forma contínua, buscando equilibrar as necessidades específicas de cada política pública com a possibilidade de aproveitar capacidades e componentes já existentes [9].

A governança de dados constitui outra dimensão importante desse processo. A implementação e o acompanhamento de políticas públicas dependem de informações produzidas, compartilhadas e utilizadas por diferentes instituições [10]. Para que esses dados possam apoiar adequadamente a execução dos programas governamentais, torna-se necessário estabelecer padrões, responsabilidades e mecanismos que assegurem sua qualidade, segurança e uso apropriado [11, 12]. Dessa forma, a integração entre aplicações de software não representa apenas um desafio tecnológico, mas também envolve aspectos institucionais e organizacionais relacionados à gestão e ao compartilhamento de informações [4, 13].

No contexto brasileiro, essas questões podem ser observadas em diferentes iniciativas governamentais, especialmente na área da educação, em que programas de grande abrangência demandam soluções tecnológicas capazes de apoiar processos complexos e integrar informações provenientes de diferentes fontes [14]. Iniciativas como o Programa Nacional do Livro e do Material Didático (PNLD), o MEC Gestão Presente e o Pé-de-Meia ilustram a diversidade de necessidades tecnológicas envolvidas na implementação de políticas públicas educacionais. Nesse cenário, o Núcleo de Excelência em Tecnologias Sociais (NEES) da Universidade Federal de Alagoas (UFAL), por meio de sua colaboração com o Ministério da Educação (MEC), acumula experiência no desenvolvimento e na evolução de aplicações de software que apoiam essas políticas [2, 3, 5, 11, 7], contribuindo para a compreensão dos desafios relacionados à integração, à escalabilidade e à sustentabilidade tecnológica.

1.2 Infraestruturas públicas digitais como abordagem tecnológica

As DPIs representam uma abordagem para o desenvolvimento de serviços digitais baseada no compartilhamento de capacidades tecnológicas que podem ser utilizadas por diferentes aplicações de software, instituições e políticas públicas [6, 9]. Em vez de desenvolver soluções inteiramente independentes para cada necessidade, essa abordagem propõe a construção de uma base comum de componentes e serviços digitais, permitindo que diferentes aplicações aproveitem funcionalidades já disponíveis. Entre os exemplos de capacidades compartilhadas estão os mecanismos de identificação digital, os sistemas de pagamento e as plataformas de intercâmbio de dados [15].

Um dos princípios dessa abordagem é a reutilização de componentes tecnológicos, que permite aproveitar soluções já existentes no desenvolvimento de novos serviços. Associada à modularidade, essa característica favorece a organização dos sistemas em componentes com responsabilidades bem definidas, que podem ser desenvolvidos, mantidos e atualizados de forma independente. A

interoperabilidade, por sua vez, permite que esses componentes e as aplicações de software que os utilizam se comuniquem por meio de padrões e interfaces comuns, facilitando a integração entre diferentes plataformas e instituições [9, 16].

Além dos aspectos tecnológicos, a implementação de DPI envolve questões de governança, segurança e sustentabilidade das soluções. O compartilhamento de capacidades digitais entre diferentes instituições exige a definição de responsabilidades, regras de acesso, mecanismos de proteção de dados e modelos de manutenção que assegurem a continuidade dos serviços. Nesse sentido, a adoção de DPI não se limita à escolha de uma arquitetura tecnológica, mas também envolve a organização de um ecossistema no qual diferentes atores possam desenvolver, utilizar e evoluir capacidades digitais de maneira coordenada [6, 10, 17, 18].

Nesse contexto, os DPGs mantêm uma relação complementar com as DPIs. Os DPGs compreendem recursos digitais, como softwares de código aberto, padrões abertos e outros artefatos que atendam a critérios específicos de abertura, privacidade e interesse público [19]. Esses recursos podem contribuir para a implementação de infraestruturas digitais ao disponibilizar soluções adaptáveis e reutilizáveis em diferentes contextos, embora nem todo DPG constitua necessariamente uma DPI [6, 9].

1.3 Contextualização da missão técnica Brasil-Índia

A busca por abordagens tecnológicas capazes de apoiar a transformação digital das políticas públicas tem motivado o NEES/UFAL a ampliar sua cooperação internacional nas áreas de DPI e DPG. Nesse contexto, foi estabelecida uma parceria com o International Institute of Information Technology Bangalore (IIIT-B)[1], na Índia, envolvendo também o Centre for Open Societal Systems (COSS)[2], com o propósito de promover o intercâmbio de conhecimentos e experiências no desenvolvimento de soluções digitais voltadas ao setor público.

A cooperação parte do reconhecimento de que Brasil e Índia possuem experiências relevantes no uso de tecnologias digitais para apoiar políticas públicas de grande abrangência. No contexto brasileiro, o NEES/UFAL acumula experiência no desenvolvimento e na evolução de soluções tecnológicas que apoiam programas governamentais, especialmente na área da educação. Por sua vez, a experiência indiana oferece referências importantes sobre a construção de infraestruturas digitais compartilhadas, de arquiteturas modulares e de ecossistemas de colaboração. A aproximação entre essas experiências possibilita a troca de conhecimentos, considerando tanto os avanços já alcançados quanto os desafios enfrentados em cada contexto.

Como parte dessa parceria, foi realizada uma missão técnica à Índia, que possibilitou o compartilhamento de experiências entre pesquisadores e especialistas das instituições envolvidas. As atividades permitiram aprofundar os conhecimentos sobre o ecossistema Sunbird [20] e discutir abordagens relacionadas à interoperabilidade, à reutilização de componentes e ao desenvolvimento de capacidades digitais compartilhadas. Ao mesmo tempo, a experiência brasileira no

[1] Instituição de ensino superior e pesquisa em tecnologia da informação sediada em Bengaluru, na Índia, fundada em 1999 e reconhecida como universidade (*Deemed University*) desde 2005.

[2] Centro vinculado ao IIIT-B responsável pela manutenção e pela evolução do ecossistema Sunbird e de outras iniciativas de bens públicos digitais.

desenvolvimento de aplicações de software para políticas públicas contribuiu para o intercâmbio de conhecimentos e para a identificação de oportunidades de colaboração. A missão também marcou o início de uma agenda de cooperação internacional de longo prazo, orientada ao desenvolvimento conjunto de projetos, ao intercâmbio de pesquisadores e à construção de iniciativas científicas e tecnológicas que deverão se estender pelos próximos anos.

Além do intercâmbio técnico, a missão fortaleceu a cooperação científica e institucional entre as organizações, criando oportunidades para a experimentação de soluções baseadas em DPI e DPG e para a ampliação de iniciativas conjuntas. Essa aproximação representa uma oportunidade de combinar conhecimentos e experiências complementares, contribuindo para a investigação de novas abordagens tecnológicas e de suas possibilidades de aplicação nas políticas públicas brasileiras. Os aprendizados decorrentes dessa cooperação constituem uma das bases das reflexões e análises apresentadas nesta nota técnica.

1.4 Objetivo e escopo da nota técnica

Esta nota técnica tem como objetivo sistematizar os conhecimentos e as experiências compartilhadas durante a missão técnica Brasil–Índia, articulando-os a fundamentos científicos e a referências internacionais sobre DPI e DPG. Nesse contexto, destaca-se o ecossistema Sunbird, que constituiu um dos principais focos das discussões e das atividades técnicas realizadas durante a missão. A partir dessa experiência, busca-se discutir oportunidades de aplicação dessas abordagens no contexto brasileiro, considerando os desafios tecnológicos e institucionais envolvidos no desenvolvimento, na integração e na evolução de soluções digitais que apoiam políticas públicas.

O documento combina fundamentação conceitual, aprendizados da experiência internacional e reflexões sobre as possibilidades de aplicação em políticas públicas brasileiras. São examinadas oportunidades de compartilhamento de capacidades digitais, de reutilização de componentes de software e de interoperabilidade entre instituições. Essas oportunidades são aprofundadas no domínio da educação, no qual o NEES/UFAL acumula experiência, sem que os conceitos e a arquitetura aqui propostos se restrinjam a esse setor. As análises têm caráter exploratório e propositivo, respeitando as particularidades de cada política pública e as capacidades tecnológicas já existentes.

1.5 Organização do Documento

Além desta introdução, a nota técnica está organizada em sete seções. A Seção 2 apresenta os fundamentos conceituais e tecnológicos de DPI e DPG. A Seção 3 sistematiza os principais aprendizados da experiência indiana, com destaque para o ecossistema Sunbird. A Seção 4 examina oportunidades de aplicação no domínio da educação. A Seção 5 propõe uma arquitetura de referência e as diretrizes técnicas correspondentes. A Seção 6 descreve a prova de conceito desenvolvida com o Sunbird RC. A Seção 7 trata da cooperação continuada e do apoio à adoção. Por fim, a Seção 8 reúne as considerações finais.

SÍNTESE DA SEÇÃO

A transformação digital ampliou o papel das aplicações de software na execução de políticas públicas, mas também expôs a fragmentação tecnológica, as dificuldades de interoperabilidade e os desafios de sustentabilidade de soluções concebidas para necessidades isoladas. As DPIs e os DPGs oferecem uma abordagem baseada em capacidades digitais compartilhadas, interoperáveis e reutilizáveis, cuja adoção envolve também a governança, a segurança e a organização de um ecossistema de colaboração. A missão técnica Brasil–Índia permitiu examinar essa abordagem em operação, com destaque para o ecossistema Sunbird, e orienta esta nota técnica, que articula fundamentos, aprendizados e propostas de aplicação no contexto brasileiro, com ênfase na educação.

SEÇÃO 02

Fundamentos de DPI e DPG

Esta seção apresenta os fundamentos conceituais e técnicos que sustentam as discussões desenvolvidas ao longo desta nota técnica. Inicialmente, são apresentadas as definições de DPI e DPG, com base nas referências de organismos internacionais e no marco normativo brasileiro. A discussão avança para os princípios arquiteturais, os requisitos de governança e de proteção de dados, e os modelos de sustentabilidade necessários à implementação e à evolução dessas iniciativas.

2.1 Conceitos e evolução das infraestruturas públicas digitais

A transformação digital do setor público exige a integração de sistemas de software, dados e instituições para ampliar a eficiência, a segurança e o acesso aos serviços. Nesse contexto, as DPIs constituem capacidades digitais compartilhadas que podem ser utilizadas por diferentes organizações na prestação de serviços à sociedade, reduzindo a fragmentação tecnológica [6, 9].

O conceito ganhou contornos próprios a partir da experiência indiana com o chamado *India Stack*, conjunto de camadas fundacionais formado por identidade digital, sistema de pagamentos e camada de intercâmbio de dados. Mais do que cada componente isoladamente, o que essa experiência evidenciou foi uma abordagem de projeto: blocos compartilhados mantidos pelo Estado sobre os quais governos, empresas e sociedade civil passam a construir serviços próprios, estimulando inovação e competição em todo o ecossistema [21, 22].

Em 2023, sob a presidência indiana, o G20 consolidou essa leitura ao descrever as DPIs como um conjunto de sistemas digitais compartilhados cuja ideia central é projetar blocos de construção mínimos, utilizáveis de forma modular por governos, empresas, academia e sociedade civil [23]. No mesmo ano, o Programa das Nações Unidas para o Desenvolvimento (PNUD) publicou um guia de referência para a adoção da abordagem [9], e, em 2024, as Nações Unidas lançaram um referencial de salvaguardas voltado especificamente aos riscos dessas infraestruturas [10].

A Organização para a Cooperação e Desenvolvimento Econômico (OCDE) define as DPIs como sistemas digitais compartilhados, seguros e interoperáveis, destinados a apoiar a oferta inclusiva de serviços públicos e privados. Entre seus componentes estão a identidade digital, os pagamentos, o compartilhamento de dados e os registros governamentais. A composição dessas infraestruturas, contudo, varia conforme as necessidades e as condições institucionais de cada contexto [6, 15]. A literatura acadêmica acrescenta a essa definição uma dimensão normativa: nenhuma infraestrutura é neutra quanto à direção que imprime aos serviços que sustenta, e o caráter “público” de uma DPI depende menos de quem a desenvolve do que dos valores explicitados em seu desenho e de como sua governança é conduzida [18].

No Brasil, a Estratégia Nacional de Governo Digital para o período de 2024 a 2027 incorporou o conceito ao ordenamento jurídico, definindo as infraestruturas públicas digitais como soluções estruturantes de aplicação transversal, orientadas pelos princípios da universalidade e da interoperabilidade, que podem ser utilizadas por entidades públicas e privadas [24]. O mesmo decreto atribui à Secretaria de Governo Digital a condução do desenvolvimento e da implementação dessas infraestruturas e reconhece a identificação civil, apoiada na Plataforma gov.br, como uma DPI nacional [24, 25].

Tabela 1. Definições de referência adotadas nesta nota.

Termo	Definição de referência (fonte)	Interpretação da equipe
DPI (Infraestrutura Pública Digital)	Sistemas digitais compartilhados, seguros e interoperáveis que apoiam a oferta inclusiva de serviços públicos e privados [6]; no Brasil, soluções estruturantes de aplicação transversal orientadas pela universalidade e pela interoperabilidade [24].	Capacidades digitais compartilhadas que integram componentes tecnológicos, dados e governança para apoiar diferentes serviços e políticas públicas.
DPG (Bem Público Digital)	Recurso digital aberto (software, dados, modelos, padrões ou conteúdos) que atende aos critérios do padrão de bens públicos digitais, incluindo licenciamento aberto, documentação e conformidade legal [1, 19].	Recurso digital aberto que pode ser reutilizado ou adaptado para compor soluções de interesse público, desde que avaliado no contexto em que será empregado.

Fonte: Elaboração própria com base em OCDE [6], PNUD [9], Brasil [24], ONU [1] e DPGA [19].

Um conceito relacionado é o de DPG. O Roteiro para a Cooperação Digital do Secretário-Geral das Nações Unidas apresenta os DPGs como softwares de código aberto, dados abertos, modelos abertos de inteligência artificial, padrões abertos e conteúdos abertos que observam a privacidade e as normas aplicáveis e não causam danos [1]. A Aliança para os Bens Públicos Digitais (DPGA) operacionalizou essa noção em um padrão de verificação, segundo o qual esses recursos devem atender a critérios como relevância para os Objetivos de Desenvolvimento Sustentável (ODS), licenciamento aberto, documentação e conformidade com requisitos legais e de proteção de dados. Assim, a disponibilização gratuita de uma solução não é suficiente, por si só, para caracterizá-la como bem público digital [19].

Embora complementares, DPI e DPG não são equivalentes. As DPIs representam sistemas e capacidades compartilhadas que sustentam serviços digitais, enquanto os DPGs correspondem a recursos abertos que podem ser reutilizados e adaptados conforme suas respectivas condições de uso. Esses recursos podem integrar uma infraestrutura, mas sua adoção exige a avaliação de aspectos como interoperabilidade, segurança e adequação técnica [6, 19]. A composição de uma DPI pode incluir software proprietário. Por outro lado, a classificação de um recurso como DPG não implica que ele fará parte de uma infraestrutura compartilhada. Com base nessas referências, esta nota distingue as definições institucionais da interpretação adotada pela equipe, apresentada na Tabela 1.

A Figura 1 sintetiza essa relação, reunindo os componentes típicos das DPI, os critérios que caracterizam os DPG e os princípios arquiteturais, discutidos na Subseção 2.3, que articulam as duas categorias.

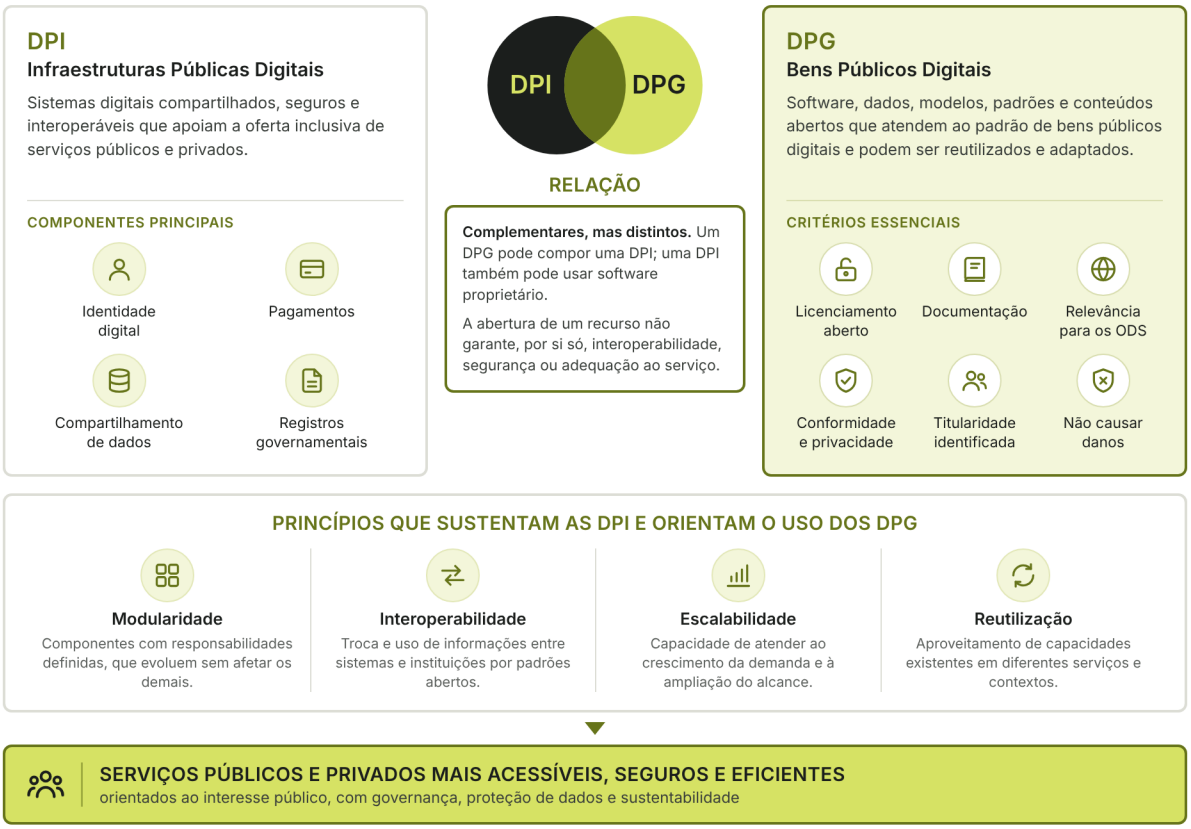


Figura 1. Relação conceitual entre infraestruturas públicas digitais e bens públicos digitais.

Fonte: Elaboração própria com base em OCDE [6], PNUD [9] e DPGA [19].

2.2 Bens públicos digitais e ecossistemas de software aberto

Os Bens Públicos Digitais constituem recursos que podem contribuir para ampliar o acesso a soluções tecnológicas, favorecer a reutilização de componentes e reduzir a dependência de desenvolvimentos exclusivos de cada organização. Seu caráter aberto, entretanto, não decorre apenas da disponibilidade gratuita de um recurso. A classificação como DPG depende do atendimento a critérios específicos, incluindo licenciamento aberto, identificação da titularidade, documentação, relevância para os ODS e observância de requisitos de privacidade, segurança e conformidade legal [19].

A adoção de recursos abertos pode favorecer a colaboração entre organizações, a adaptação a diferentes contextos e o compartilhamento de melhorias. A DPGA destaca que esses recursos podem ser adotados e adaptados por países e instituições de acordo com suas necessidades, além de contribuir para o desenvolvimento de capacidades locais e para a colaboração entre diferentes atores [19]. As Nações Unidas, por sua vez, situam a promoção dos DPGs entre as ações prioritárias para uma cooperação digital mais equitativa, reconhecendo a origem aberta

e pública de boa parte da infraestrutura que sustenta a internet [1]. Esses benefícios, contudo, dependem das características de cada solução, das condições de licenciamento e da capacidade institucional para sua implantação e manutenção.

No contexto das DPIs, os DPGs podem funcionar como componentes reutilizáveis, desde que sejam compatíveis com os requisitos da infraestrutura e possam ser integrados aos demais elementos do ecossistema. A relação entre essas categorias não é automática: a abertura de um recurso, isoladamente, não garante interoperabilidade, segurança, escalabilidade ou adequação ao serviço pretendido. Tais propriedades precisam ser avaliadas no contexto da arquitetura e das condições concretas de utilização [19, 9]. O ecossistema Sunbird, examinado na Seção 3, ilustra essa relação: trata-se de um conjunto de blocos de construção abertos, distribuídos sob licença MIT e reconhecidos como bens públicos digitais [26, 27], que só se tornam infraestrutura quando são configurados, integrados e operados para atender a uma política pública concreta.

2.3 Princípios arquiteturais: modularidade, interoperabilidade, escalabilidade e reutilização

Os referenciais internacionais convergem em torno de um conjunto relativamente estável de princípios para o desenho de DPI. O marco do G20 enumera, entre outros, inclusão, interoperabilidade, modularidade e extensibilidade, escalabilidade, segurança e privacidade, colaboração, governança orientada ao benefício público e sustentabilidade [23], e o guia do PNUD retoma esses mesmos elementos como orientações práticas para implementação [9]. Os quatro princípios tratados nesta subseção são aqueles com implicações mais diretas sobre a arquitetura técnica, os demais são discutidos nas subseções seguintes.

A modularidade consiste em organizar a infraestrutura em componentes com responsabilidades definidas, que possam ser desenvolvidos, mantidos e evoluídos de forma coordenada. A ideia tem raízes antigas na engenharia de software: a decomposição de um sistema em módulos que ocultam suas decisões internas de projeto e expõem apenas interfaces estáveis permite que cada parte seja modificada sem exigir alterações nas demais [28]. O referencial do PNUD associa esse princípio à extensibilidade, permitindo que componentes sejam modificados ou ampliados sem provocar interrupções desnecessárias nos demais elementos da infraestrutura [9]. Essa organização favorece a adaptação às mudanças nos requisitos e a incorporação progressiva de novas capacidades.

A interoperabilidade corresponde à capacidade de diferentes sistemas de software trocarem e utilizarem informações de forma compatível [16]. Sua implementação envolve a adoção de padrões, especificações, interfaces e modelos de dados que permitam a comunicação entre soluções heterogêneas. O Quadro Europeu de Interoperabilidade mostra, contudo, que a dimensão técnica é apenas uma das quatro [16]. A troca efetiva de informações entre administrações depende também de compatibilidade jurídica, organizacional e semântica: de normas que autorizem o compartilhamento, de processos alinhados entre as instituições e de um significado comum atribuído aos dados trocados.

No contexto das DPIs, a interoperabilidade reduz as barreiras à integração entre instituições e favorece o uso compartilhado de componentes. O PNUD e o G20 recomendam a adoção de padrões e especificações abertos, com uma abordagem tecnologicamente neutra, considerando as salvaguardas necessárias e as restrições legais e técnicas aplicáveis [9, 23]. O modelo de dados de credenciais verificáveis do W3C[3], retomado nas Seções 3 a 5, é um exemplo de padrão aberto desse tipo [29]. No Brasil, a Lei do Governo Digital já inclui a interoperabilidade de sistemas e a promoção de dados abertos entre os princípios e as diretrizes da administração pública [30].

A escalabilidade diz respeito à capacidade de uma solução atender ao crescimento da demanda ou à ampliação de seu alcance sem exigir, necessariamente, a substituição integral da estrutura existente. Segundo o PNUD [9] e o G20 [23], uma infraestrutura deve ser concebida com flexibilidade para acomodar aumentos de demanda, inclusive os inesperados, e necessidades de expansão. Para isso, o planejamento arquitetural precisa considerar a capacidade dos componentes, os limites operacionais, os requisitos de desempenho e as condições de continuidade dos serviços. A Estratégia Nacional de Governo Digital incorpora a mesma preocupação ao priorizar, para as DPI brasileiras, padrões tecnológicos interoperáveis, seguros, escaláveis e economicamente sustentáveis no longo prazo [24].

A reutilização permite empregar capacidades já existentes em diferentes serviços e contextos, evitando que cada instituição desenvolva, de forma independente, soluções para necessidades semelhantes. A OCDE destaca que as infraestruturas compartilhadas podem favorecer maior coerência na prestação de serviços digitais [6], e a experiência indiana mostra que o ganho decorre justamente de oferecer blocos comuns sobre os quais diferentes atores constroem suas próprias aplicações [21]. A reutilização, portanto, depende diretamente dos outros três princípios: um componente só é reaproveitável se tiver fronteiras bem definidas, se puder se comunicar por padrões conhecidos e se suportar a carga adicional de novos usos.

2.4 Governança, privacidade, segurança e proteção de dados

A governança de dados compreende políticas, processos, responsabilidades e estruturas organizacionais destinadas a orientar o gerenciamento das informações ao longo de seu ciclo de vida. Nas DPIs, ela é relevante para estabelecer critérios de acesso, compartilhamento, qualidade, integridade, armazenamento e uso dos dados. A definição desses elementos contribui para reduzir ambiguidades entre instituições e assegurar que o intercâmbio de informações ocorra de acordo com as finalidades, responsabilidades e condições previamente estabelecidas [4]. O marco do G20 situa essa dimensão entre os componentes constitutivos das DPIs, ao lado da tecnologia, e a associa à proteção dos direitos humanos, dos dados pessoais e da privacidade [23]. Na área da educação, essa preocupação já se traduz em estruturas formais, como o Comitê de Governança de Dados da Educação, instituído pelo Ministério da Educação em 2024 [14].

O compartilhamento de dados deve ser acompanhado de mecanismos de proteção proporcionais aos riscos envolvidos. A integração entre sistemas não deve ser interpretada como autorização irrestrita de acesso ou utilização de informações. É necessário estabelecer regras de acesso,

[3] *World Wide Web Consortium*, consórcio internacional responsável pela elaboração de padrões abertos para a web.

controles de segurança, registro de operações e procedimentos para tratamento de incidentes, considerando a natureza dos dados e as obrigações legais aplicáveis. A OCDE destaca que os sistemas de compartilhamento de dados devem contar com salvaguardas apropriadas, incluindo medidas relacionadas à privacidade e à segurança [6]. O Referencial Universal de Salvaguardas para DPI, publicado pelas Nações Unidas, aprofunda esse ponto ao propor orientações aplicáveis a todo o ciclo de implementação, voltadas a mitigar riscos tanto para os indivíduos quanto para a sociedade [10].

No Brasil, a Lei Geral de Proteção de Dados Pessoais (LGPD) estabelece regras para o tratamento de dados pessoais, inclusive em meios digitais, com o objetivo de proteger os direitos fundamentais à liberdade e à privacidade e o livre desenvolvimento da personalidade da pessoa natural [17]. Dessa forma, iniciativas de DPI que envolvam dados pessoais devem considerar as bases legais aplicáveis, os princípios do tratamento, os direitos dos titulares e as responsabilidades dos agentes de tratamento. A Estratégia Nacional de Governo Digital reforça essa exigência ao determinar o mapeamento prévio de riscos e a adoção de práticas de privacidade, proteção de dados e segurança ao longo de todo o ciclo de vida das DPIs [24].

A segurança da informação também precisa ser considerada desde a concepção da infraestrutura. Isso envolve identificar riscos, estabelecer controles adequados, restringir acessos conforme as responsabilidades, proteger os dados durante o armazenamento e a transmissão e preparar procedimentos de resposta a incidentes. O PNUD recomenda que a segurança e a privacidade sejam incorporadas ao desenho dos sistemas, associando esses requisitos à proteção de dados, à resiliência e à confiança dos usuários [9]. O G20, de forma semelhante, preconiza que as tecnologias de proteção da privacidade e os recursos de segurança estejam embutidos no núcleo do projeto, e não acrescentados posteriormente [23]. A confiança, nesse sentido, não é um resultado automático da tecnologia empregada, mas depende de governança transparente e de valores públicos explicitados desde o início [18].

2.5 Modelos de sustentabilidade e colaboração em ecossistemas digitais

O referencial do PNUD inclui a sustentabilidade entre os princípios para a estruturação das DPIs e relaciona sua concretização à existência de financiamento adequado, suporte tecnológico e aprimoramentos que permitam a continuidade das operações e a prestação dos serviços [9, 23]. Essa perspectiva indica que a sustentabilidade deve ser tratada desde o planejamento, em vez de ser considerada apenas após a entrada da infraestrutura em funcionamento.

Os bens públicos digitais podem contribuir para esse objetivo ao possibilitar a adoção e a adaptação de recursos existentes. Entretanto, o uso de uma solução aberta não elimina os custos associados à sua implantação, operação e manutenção. Mesmo quando não há cobrança pela licença de uso, podem existir despesas com infraestrutura computacional, integração, capacitação, suporte, segurança, atualização e adequação às exigências institucionais. Por isso, a avaliação de uma solução deve considerar seu custo ao longo de todo o ciclo de vida, e não apenas o custo inicial de aquisição ou desenvolvimento [19, 6]. A literatura sobre software aberto mostra que esse risco

é concreto: componentes amplamente utilizados como infraestrutura costumam depender de um número reduzido de mantenedores, muitas vezes sem financiamento estável, o que os expõe a falhas de segurança e à descontinuidade [31].

A colaboração entre organizações também constitui um fator relevante para a continuidade e a evolução das DPIs. O G20 inclui entre seus princípios o estímulo à participação de atores da comunidade nas diferentes etapas do ciclo de vida da infraestrutura [23]. A experiência com software aberto, por sua vez, indica que a manutenção de longo prazo depende menos do controle exercido por uma única organização do que de uma relação de cuidado com as comunidades que já mantêm os componentes [31].

Para que a colaboração produza resultados consistentes, é necessário definir responsabilidades, processos decisórios e condições de participação. A governança do ecossistema deve estabelecer quem mantém os componentes compartilhados, como as alterações são propostas e aprovadas, quais critérios orientam a seleção de soluções e como as falhas, vulnerabilidades e necessidades de atualização são tratadas. Nesse arranjo, o Estado assume um papel ativo de coordenação, garantindo que a infraestrutura permaneça orientada ao interesse público mesmo quando parte de seus componentes é mantida por terceiros [18].

Diante desses aspectos, a sustentabilidade de uma DPI deve ser analisada de forma integrada, considerando as dimensões financeira, tecnológica, institucional e operacional. A colaboração favorece a articulação entre os participantes; a governança estabelece responsabilidades e regras; e o planejamento de longo prazo permite prever recursos e ações necessários à continuidade dos serviços. Em conjunto, esses elementos contribuem para que a infraestrutura permaneça funcional, segura e alinhada ao interesse público ao longo de sua evolução [6, 9].

SÍNTESE DA SEÇÃO

DPI e DPG são conceitos complementares, mas distintos: as DPIs descrevem capacidades compartilhadas que sustentam serviços, e os DPGs, recursos abertos que podem compô-las. A abertura de um componente não garante, por si só, interoperabilidade, segurança ou sustentabilidade. Essas propriedades dependem da arquitetura adotada, da governança dos dados e de um modelo de manutenção definido desde o planejamento.

SEÇÃO 03

Experiência Indiana: Ecossistema e Aprendizados

A missão técnica permitiu observar, em operação, um ecossistema de bens públicos digitais construído ao longo de quase uma década e aplicado a políticas públicas em escala nacional. Esta seção sistematiza o que foi observado nas sessões conduzidas pelo *Centre for Open Societal Systems* (COSS), mantenedor do Sunbird, cotejando-o com a documentação pública do ecossistema, com ênfase nos blocos de construção que concentraram as demonstrações técnicas e nas práticas de engenharia, governança e sustentabilidade que os sustentam.

Esta seção apresenta um estudo inicial sobre três dos vinte e um componentes do ecossistema Sunbird. A escolha considera as prioridades de pesquisa e desenvolvimento do DPI Lab, bem como as possibilidades de aplicação dessas tecnologias no contexto brasileiro. A análise busca compreender suas principais características, funcionalidades e contribuições ao desenvolvimento de soluções baseadas em DPI e DPG. Como desdobramento desse estudo, a Seção 6 apresenta um exemplo prático de aplicação utilizando credenciais verificáveis.

3.1 O ecossistema Sunbird: origem, composição e evidências de escala

O Sunbird nasceu de um esforço da EkStep Foundation[4] voltado à construção de uma infraestrutura digital confiável para ampliar as oportunidades de aprendizagem na educação básica indiana, distribuída sob licença MIT [26]. O que começou como resposta a uma necessidade setorial específica evoluiu para um conjunto de componentes configuráveis, aplicáveis a domínios distintos e mantidos de forma colaborativa: o ecossistema reúne hoje vinte e um blocos de construção, que podem ser utilizados isoladamente ou combinados para formar capacidades maiores [27].

A característica arquitetural mais relevante do ecossistema não está em nenhum bloco isoladamente, mas na forma como eles se compõem. A Figura 2 ilustra esse modelo. Na base, situa-se a infraestrutura computacional, que permanece sob controle de quem adota: as soluções são auto-hospedadas e não dependem de serviços mantidos pelo mantenedor do código. Sobre ela organizam-se os blocos de construção, que oferecem capacidades genéricas e independentes de setor. Acima deles, uma camada de contexto incorpora o vocabulário e as regras próprios de cada domínio, seguida por uma camada de customização e integração, na qual cada adotante ajusta o comportamento dos componentes às suas necessidades. No topo, situam-se as soluções

[4] A EkStep Foundation é uma organização sem fins lucrativos sediada em Bengaluru, na Índia, fundada em 2015 por Nandan Nilekani, Rohini Nilekani e Shankar Maruwada, dedicada a ampliar oportunidades de aprendizagem por meio de plataformas digitais abertas e colaborativas.

efetivamente oferecidas aos cidadãos.



Figura 2. Modelo de composição do ecossistema Sunbird.

Fonte: Elaboração própria com base em Sunbird (2026a, 2026b).

Convém destacar um aspecto desse modelo que raramente é explicitado em iniciativas semelhantes: os blocos não são publicados da mesma forma. Alguns são disponibilizados como especificação, cabendo a quem adota implementá-la; é o caso dos blocos de telemetria, de descoberta de oportunidades educacionais e de credenciais verificáveis; outros, como código executável; outros, ainda, como composição de blocos preexistentes, como os blocos de aprendizagem e de mentoria [27]. Essa distinção tem consequência prática direta, pois determina o que pode ser substituído sem comprometer a interoperabilidade. Quando o que se publica é a especificação, duas implementações distintas permanecem compatíveis entre si; quando se publica apenas o código, a compatibilidade depende da permanência daquela implementação.

As evidências de escala sustentam a afirmação de que o modelo opera em condições reais, e não apenas em ambiente experimental. A plataforma DIKSHA[5], construída sobre os blocos de aprendizagem e adotada por quarenta estados indianos, alcança mais de cento e oitenta milhões de usuários e sete milhões de professores. A infraestrutura de certificação sanitária DIVOC[6], que sustenta a solução CoWIN[7], emitiu mais de dois bilhões de certificados de vacinação em cinco países [32]. Já a plataforma iGOT Karmayogi[8] ultrapassou os dez milhões de servidores públicos registrados [33]. Esses números importam menos como demonstração de desempenho do que como indicação de maturidade operacional: componentes submetidos a essa ordem de grandeza

[5] *Digital Infrastructure for Knowledge Sharing*, plataforma nacional de educação básica da Índia, mantida pelo Conselho Nacional de Pesquisa e Formação Educacional (NCERT), vinculado ao Ministério da Educação indiano, e lançada em 2017.
[6] *Digital Infrastructure for Verifiable Open Credentialing*, infraestrutura de código aberto para emissão de credenciais verificáveis, utilizada na emissão de certificados de vacinação contra a COVID-19.
[7] Plataforma do governo indiano para gestão e registro da vacinação contra a COVID-19.
[8] Plataforma de capacitação de servidores públicos do governo indiano, vinculada à Missão Karmayogi.

tiveram seus limites de projeto efetivamente testados.

3.2 Blocos em destaque: Spark, RC e Obsrv

Entre os blocos do ecossistema, três concentram hoje o esforço de manutenção e evolução conduzido pelo COSS e foram objeto das demonstrações técnicas realizadas durante a missão. A Figura 3 ilustra a relação entre eles, tomando o bloco de aprendizagem como exemplo de composição: ele recorre aos demais por meio de interfaces públicas, sem que isso os torne dependentes dele.

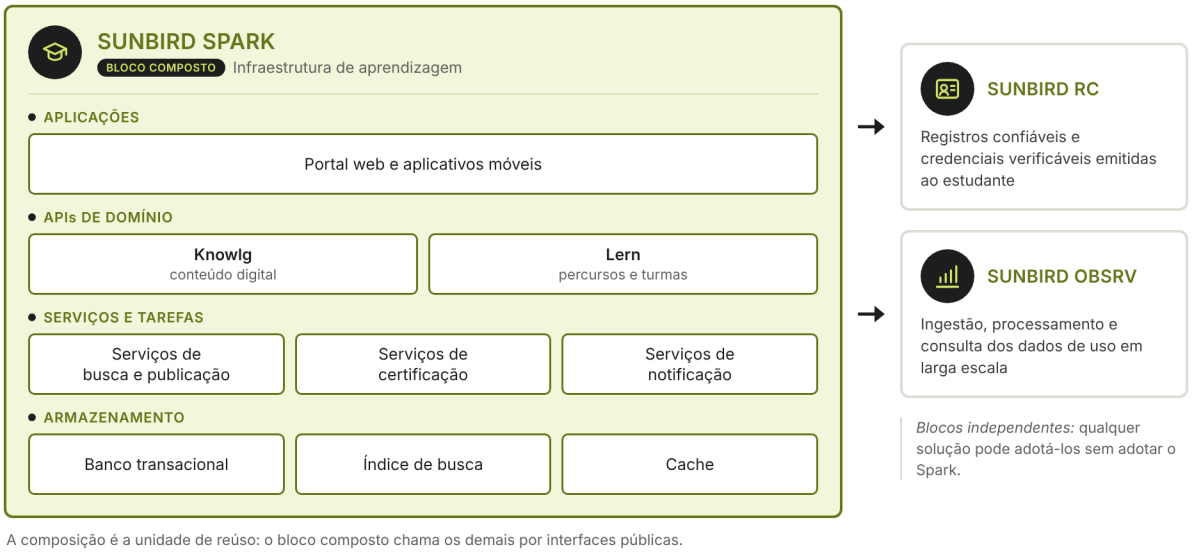


Figura 3. Composição entre os três blocos em destaque.

Fonte: Elaboração própria com base em Sunbird (2026b), Sunbird Ed (2026), Sunbird RC (2026) e Sunbird Obsrv (2026a).

3.2.1 Sunbird Spark

O Sunbird Spark é a versão 9.0 do bloco anteriormente denominado Sunbird Ed, publicada em abril de 2026, e constitui uma infraestrutura de aprendizagem, capacitação e desenvolvimento de competências [34]. Trata-se de um bloco composto [27], que reúne serviços de gestão de conteúdo digital, de percursos formativos e de turmas, de busca e descoberta, de avaliação e de emissão de certificados, além de aplicações web e móveis prontas para uso.

Sua propriedade mais relevante para os fins desta nota é a configurabilidade: o mesmo componente atende a contextos tão distintos quanto a educação escolar, a formação de servidores públicos e a capacitação de profissionais de saúde, mediante configuração, e não por meio do desenvolvimento de novas versões. A incorporação de capacidades de inteligência artificial segue a mesma lógica, sendo tratada como infraestrutura configurável, indexação de conteúdo, geração de transcrições, recomendação por competências, e não como funcionalidade acoplada ao produto.

3.2.2 Sunbird RC

O Sunbird RC responde por duas capacidades complementares, que podem ser utilizadas em conjunto ou separadamente: a manutenção de registros confiáveis e a emissão de credenciais verificáveis a partir deles [35]. Um registro, nessa acepção, distingue-se de um banco de dados por três atributos: possui um esquema padronizado e identificadores únicos, é atestado por uma autoridade responsável e constitui a fonte única de verdade sobre pessoas, instituições, ativos ou eventos. A credencial verificável é a prova portátil de um fato contido nesse registro, assinada pelo emissor e apresentada pelo próprio titular, de modo que o verificador possa conferi-la sem consultar a instituição emissora a cada apresentação.

A trajetória do bloco é instrutiva quanto ao modo como esses componentes evoluem. O bloco foi originado como motor de registros orientado a esquema e aplicado, em seguida, à infraestrutura de credenciamento sanitário. Nas versões mais recentes, incorporou os padrões internacionais consolidados ao longo da última década: a emissão, a atualização e a revogação seguem o modelo de dados de credenciais verificáveis do W3C, e a entrega a carteiras digitais apoia-se nos protocolos de emissão e apresentação da OpenID Foundation[9] [35, 29]. A evolução, portanto, foi conduzida por implantações reais e pela convergência a padrões externos, e não por um roteiro definido a priori.

3.2.3 Sunbird Obsrv

O Sunbird Obsrv constitui a infraestrutura de engenharia de dados do ecossistema [36]. Seu objeto é a cadeia que vai da ingestão à consulta analítica: conectores de origem levam os dados, em lote ou em fluxo contínuo, a um encadeamento de processamento que executa validação contra esquema, remoção de duplicidades, transformação e desnormalização de metadados; o resultado é armazenado e disponibilizado para consulta [37]. A unidade de configuração é o conjunto de dados, definido por suas origens, tabelas derivadas e métricas próprias de acompanhamento, o que permite tratar a observabilidade como propriedade de cada conjunto, e não do sistema como um todo. O componente foi dimensionado em condições exigentes: no âmbito da plataforma DIKSHA, processou médias da ordem de quinhentos milhões de eventos diários, com picos superiores a dois bilhões [36]. A Tabela 2 resume a função de cada um dos três blocos no ecossistema e as evidências de adoção que sustentam sua maturidade.

3.3 Aprendizados sobre engenharia de software, governança e sustentabilidade

Os aprendizados organizam-se em três planos, que demandam respostas institucionais distintas.

No plano da **engenharia de software**, o primeiro aprendizado diz respeito ao deslocamento do esforço de adoção. Nos blocos observados, instanciar uma capacidade não significa programá-la, mas descrevê-la: um registro é criado pela definição de seu esquema, a partir do qual as

[9] Organização internacional sem fins lucrativos responsável pelos padrões de identidade digital da família OpenID, incluindo os protocolos de emissão e apresentação de credenciais verificáveis.

Tabela 2. Blocos em destaque e evidências de adoção.

Bloco	Função no ecossistema	Evidência de adoção
Sunbird Spark	Infraestrutura de aprendizagem, capacitação e desenvolvimento de competências	DIKSHA e iGOT Karmayogi, em âmbito nacional na Índia
Sunbird RC	Registros confiáveis e emissão de credenciais verificáveis	Mais de dois bilhões de certificados de vacinação emitidos em cinco países (DIVOC)
Sunbird Obsrv	Ingestão, processamento, armazenamento e consulta de dados em escala, com identificação de campos de dados pessoais e sua proteção por mascaramento e criptografia [38]	Médias de quinhentos milhões de eventos diários na plataforma DIKSHA

Fonte: Elaboração própria com base em Sunbird (2026a, 2026b), Sunbird RC (2026) e Sunbird Obsrv (2026a).

interfaces de consulta e manutenção são geradas; uma plataforma de aprendizagem é adaptada por configuração. O esforço migra da escrita de código para a especificação do que se deseja, o que reduz o custo de implantação, mas desloca a exigência técnica para a modelagem.

O segundo refere-se à separação entre especificação e implementação: é ela que permite substituir um componente sem comprometer a interoperabilidade, e sua ausência é o que transforma o reúso em dependência.

O terceiro diz respeito à existência de caminhos de adoção que não exigem substituir o que já existe. Além da implantação em um ambiente novo, o bloco de registros permite importar acervos existentes e, sobretudo, utilizar apenas os serviços de credenciamento, mantendo o sistema atual como fonte de dados [35]. Essa última modalidade é a de maior interesse para o contexto brasileiro, no qual os sistemas de origem já existem e operam. Cabe registrar, contudo, que a integração com essas aplicações pré-existentes não é fornecida pelo bem público digital e constitui um trabalho específico de cada implantação.

No plano da **governança**, destaca-se a existência de um mantenedor identificável, com equipe dedicada e instâncias próprias de decisão técnica e estratégica. A distinção importa: código aberto sem mantenedor designado não é infraestrutura, pois não garante continuidade. A própria transição do ecossistema, concebido no âmbito da EkStep Foundation [26] e hoje mantido pelo COSS, evidencia que infraestruturas digitais precisam sobreviver à troca de quem as mantém e, portanto, precisam de propriedade institucional. Um terceiro aspecto diz respeito à arquitetura de padrões: no campo das credenciais verificáveis, nenhuma organização detém o conjunto, pois o modelo de dados, os protocolos de emissão e apresentação, os formatos de token e o reconhecimento legal são responsabilidade de corpos distintos [29, 35]. A interoperabilidade efetiva resulta de perfis que combinam padrões de origens diversas, e não da adesão a um padrão único, o que recomenda cautela diante de soluções apresentadas como integralmente padronizadas.

No plano da **sustentabilidade**, a continuidade do ecossistema não decorre da licença de uso, mas de um conjunto de atores com papéis distintos: adotantes, parceiros de implementação, integradores, fornecedores independentes e comunidade de desenvolvimento. A licença aberta e a aderência a padrões abertos são requisitos verificáveis de um bem público digital [19] e tornam a adoção possível; é o ecossistema que a torna sustentável. Soma-se a isso a soberania tratada

como propriedade técnica: as soluções são auto-hospedadas e nada é enviado ao mantenedor. Por fim, cabe reconhecer o risco do modelo: adotar componentes mantidos externamente reduz o custo inicial, mas cria dependência de um roteiro de evolução sobre o qual o adotante não decide por conta própria. A mitigação observada na prática indiana não é evitá-la, e sim participar de sua construção, contribuindo com código, casos de uso e especificações.

SÍNTESE DOS APRENDIZADOS

O valor de uma DPI está menos na qualidade isolada de seus componentes do que na combinação de três condições. A primeira são especificações publicadas, que preservam a interoperabilidade quando a implementação muda. A segunda é um mantenedor institucional, capaz de sobreviver à troca de equipes. A terceira é um ecossistema de atores que torne a manutenção viável. Sem elas, o reúso converte-se em dependência.

SEÇÃO 04

Oportunidades de Aplicação em Políticas Públicas Educacionais

Esta seção examina oportunidades de aplicação de DPI e DPG nas políticas públicas educacionais brasileiras. A Subseção 4.1 descreve o contexto em que essas oportunidades surgem: a organização federativa da educação, os ecossistemas digitais que a sustentam e o arcabouço de governança de dados que o Ministério da Educação vem construindo nos últimos anos.

A Subseção 4.2 reúne cinco casos de uso. Os dois primeiros tratam da emissão de credenciais verificáveis, aplicadas à habilitação de avaliadores e de editoras do PNLD e à comprovação da trajetória do estudante na educação básica. O terceiro examina o desenvolvimento de novos hubs de dados, voltados à educação profissional e tecnológica e à educação superior. O quarto estende as credenciais à trajetória integrada do estudante, da creche à pós-graduação. O quinto trata da observabilidade dos fluxos de dados que alimentam essa infraestrutura.

Cada caso é apresentado em três movimentos: a contextualização do processo, a forma como ele se realiza hoje e a forma como assumiria com o uso de registros confiáveis e credenciais verificáveis. A seção encerra com uma síntese comparativa dos cinco casos, acompanhada de uma estimativa da complexidade de implantação de cada um.

4.1 Contexto das políticas públicas educacionais e seus ecossistemas digitais

A educação brasileira é estruturada de forma federativa, o que significa que a informação sobre um mesmo estudante é produzida e mantida por entes distintos ao longo de sua trajetória. Trata-se de um universo da ordem de cinquenta e seis milhões de matrículas, das quais cerca de quarenta e seis milhões na educação básica, nas redes públicas e privadas [39], e dez milhões e duzentas mil na graduação, em cursos presenciais e a distância, em instituições públicas e privadas [40].

A educação profissional, com cerca de três milhões e duzentas mil matrículas registradas no Censo Escolar, entre cursos técnicos e de formação inicial e continuada, está contida nesses totais e não se soma a eles [39]. Esse universo, que na educação básica conta ainda com cerca de dois milhões e quatrocentos mil professores e cento e oitenta mil escolas [39], está distribuído entre redes municipais, estaduais, a rede federal e instituições privadas, cada qual com seus próprios sistemas de gestão. Essa arquitetura institucional não é um defeito a corrigir, mas uma característica a acomodar: qualquer solução tecnológica que pressuponha a centralização dos sistemas de origem encontra, desde o início, um obstáculo de natureza política e jurídica, e não apenas técnica.

A consequência prática é conhecida. Um fato comprovado em um sistema de gestão educacional, de que o estudante está matriculado, de que concluiu determinada etapa, de que atingiu certa frequência, precisa ser comprovado de novo, por meio de documentos em papel ou de consultas interinstitucionais, sempre que outro órgão dele necessita. O custo dessa recomprovação recai sobre o cidadão, que se desloca e coleta documentos, e sobre a administração, que mantém rotinas de conferência manual e assume o risco de decidir com base em informações desatualizadas.

O Ministério da Educação vem, nos últimos anos, construindo o arcabouço institucional para enfrentar esse desafio. Em 2024, foi instituído o Comitê de Governança de Dados da Educação, de caráter estratégico e deliberativo, com a atribuição de formular a política de governança de dados do Ministério e de suas entidades vinculadas e, entre suas competências expressas, a de promover a interoperabilidade dos dados da educação [14]. Em 2025, a Portaria nº 234 instituiu o MEC Gestão Presente como plataforma de dados da educação básica [42]. A norma estabelece a interoperabilidade de sistemas de gestão educacional como diretriz e prevê interfaces de integração com os sistemas administrativos das redes. Cria, ainda, um Comitê Tripartite com representação da União, dos estados, do Distrito Federal e dos municípios, e determina que a plataforma integre a Política Nacional de Governança de Dados para a Educação.

Esse arcabouço ganhou maior densidade com a Lei Complementar nº 220, de 31 de outubro de 2025, que instituiu o Sistema Nacional de Educação (SNE) e a Infraestrutura Nacional de Dados da Educação (Inde), denominada pelo MEC como Educadados, vinculando a cooperação federativa à interoperabilidade, ao compartilhamento, à qualidade e à segurança dos dados educacionais, com proteção dos dados pessoais [43]. Sob coordenação do MEC, a Educadados compreende a definição de padrões nacionais de interoperabilidade e de conjuntos mínimos de dados de gestão a serem compartilhados. Nesse contexto, a Portaria MEC nº 832, de 16 de dezembro de 2025, instituiu o conteúdo e a estrutura do Conjunto Mínimo de Dados da Educação Básica (CMDEB), no âmbito do MEC Gestão Presente, abrangendo informações sobre estudantes, matrículas, turmas, disciplinas, desempenho escolar, frequência, profissionais da educação e instituições de ensino [44]. A norma prevê a transmissão preferencial por meio de interfaces de programação de aplicações (APIs) e a coleta gradual, respeitando a diversidade e a capacidade técnica das redes de ensino.

Há, portanto, política, instância de governança e plataforma. O que esse conjunto ainda não resolve é o problema técnico de fundo: como fazer com que um fato comprovado na origem possa ser utilizado, com confiança, por quem não tem acesso ao sistema que o produziu. É nesse ponto específico que os conceitos tratados nas seções anteriores se aplicam, e não como substitutos do que já existe.

Dois programas de grande alcance ilustram o tipo de ganho em questão. O Pé-de-Meia condiciona o pagamento do incentivo financeiro-educacional à verificação simultânea da matrícula em série do ensino médio da rede pública, da inscrição da família no Cadastro Único, da inscrição do estudante no Cadastro de Pessoas Físicas, da frequência mínima de oitenta por cento da carga horária e, ao final do ano, da aprovação e da participação em avaliações externas [45]. Cada uma dessas condições é verificada em uma base diferente, mantida por um órgão distinto, o que torna o programa um caso quase didático de dependência de interoperabilidade: a política existe e opera, mas sua execução consome esforço considerável de conciliação entre bases.

O PNLD apresenta uma dependência de natureza distinta, ligada não a dados do estudante, mas a atributos de pessoas e organizações. O programa organiza-se em fases que incluem a adesão das redes, a inscrição das obras por titulares de direitos autorais, a avaliação pedagógica e a escolha pelas escolas [46]. A avaliação pedagógica é conduzida por equipes formadas por professores das redes públicas e privadas de ensino superior e da educação básica, que devem firmar declaração de inexistência de conflito de interesse [46]; o ingresso no banco de avaliadores exige comprovação de licenciatura plena ou magistério reconhecido pelo Ministério da Educação e a conclusão de curso de formação específico [47]. São atributos que hoje se comprovam por meio do envio de documentos e da autodeclaração.

4.2 Casos de uso e oportunidades de experimentação

Os casos a seguir foram selecionados por combinarem três características: apoiam-se em processos já existentes e operacionais, não exigem a substituição dos sistemas de origem e podem ser experimentados em escala reduzida antes de qualquer decisão de implantação ampla. Para cada um, descreve-se o processo tal como hoje se realiza e a forma que assumiria com o uso de registros confiáveis e credenciais verificáveis. A Figura 4 situa os casos relativos ao estudante ao longo de sua trajetória, distinguindo os momentos em que uma credencial é emitida dos momentos em que é verificada.

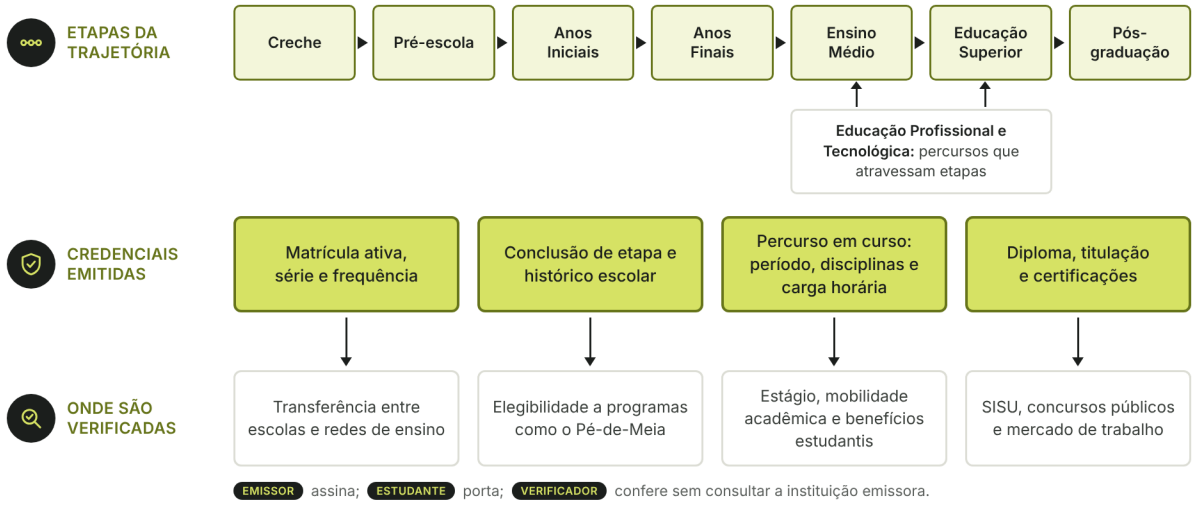


Figura 4. Pontos de emissão e de verificação de credenciais na trajetória do estudante.

Fonte: Elaboração própria.

4.2.1 Credenciais verificáveis para avaliadores e editoras do PNLD

A avaliação pedagógica do PNLD mobiliza um número expressivo de professores e especialistas, cuja habilitação depende de atributos verificáveis: titulação, vínculo institucional, conclusão da formação exigida e ausência de conflito de interesse em relação aos titulares de direitos autorais cujas obras serão avaliadas [46, 47].

Hoje, esses atributos são comprovados por meio de documentos enviados pelo próprio candidato

e de declarações firmadas por ele. A conferência é trabalhosa, depende de inspeção documental e, no caso de conflito de interesses, apoia-se essencialmente na boa-fé de quem declara, já que não há como cruzar automaticamente a lista de avaliadores com os vínculos profissionais existentes no mercado editorial.

Com credenciais verificáveis, o diploma passaria a ser emitido pela própria instituição formadora e apresentado pelo avaliador como prova assinada, dispensando o envio de cópias e a conferência manual. O certificado do curso de formação seria emitido pela própria plataforma de avaliação. E o vínculo com editoras poderia ser tratado como credencial emitida pela organização empregadora, de modo que a ausência de conflito deixasse de ser apenas declarada e passasse a ser comprovável. O ganho mais relevante não é a redução do esforço de conferência, embora ela ocorra, mas a elevação do padrão probatório de um processo cuja legitimidade depende da idoneidade de quem avalia.

4.2.2 Credenciais da trajetória do estudante na educação básica

A comprovação de escolaridade é, provavelmente, o documento mais solicitado ao estudante da educação básica. Ela é exigida na transferência entre escolas e redes, na habilitação a programas sociais e educacionais, em processos seletivos e no acesso a benefícios e incentivos sociais. Hoje, cada solicitação implica procurar a secretaria da escola, aguardar a emissão de uma declaração ou de um histórico escolar e entregá-lo em papel ou em arquivo digitalizado, cuja autenticidade o destinatário não tem como verificar senão entrando em contato com a escola emissora.

Com credenciais verificáveis, a escola ou a rede emitiria, no momento do registro, uma credencial assinada que atestasse a matrícula ativa, a série, a frequência ou a conclusão de etapa. O estudante ou seu responsável a manteria consigo e a apresentaria quando necessário; o destinatário a verificaria criptograficamente, sem precisar contatar a escola de origem.

A diferença torna-se mais evidente em dois cenários concretos. Na transferência entre redes, a escola de destino poderia confirmar de imediato a etapa e o histórico do estudante, em vez de aguardar a tramitação de documentos, o que hoje retarda a efetivação da matrícula e, em alguns casos, interrompe temporariamente a escolarização. Na habilitação ao Pé-de-Meia, a verificação de matrícula e de frequência deixaria de depender exclusivamente da conciliação periódica entre bases administrativas, podendo apoiar-se em credenciais emitidas pela própria rede no momento do registro [45]. Cabe ressalvar que a credencial não substitui o registro administrativo nem a base de origem: ela é a prova portátil de um fato que continua a residir no sistema que o produziu.

4.2.3 Novos hubs de dados da EducaDados: educação profissional e tecnológica e educação superior

A EducaDados organiza-se em camadas: os sistemas transacionais das redes e instituições permanecem onde estão, hubs por modalidade padronizam e publicam os dados de cada segmento, e uma plataforma integradora oferece a visão da trajetória completa [41]. A Figura 5 representa esse arranjo e situa os dois hubs ainda a desenvolver.

Hoje, a educação profissional e tecnológica e a educação superior dispõem de instrumentos

próprios de registro e de censo, mas não de uma camada padronizada que publique seus dados em formato comum e com semântica estável. A consequência é que cada integração entre esses segmentos e os demais é negociada caso a caso, com esquemas e vocabulários próprios, o que multiplica o custo de cada novo consumidor de dados.

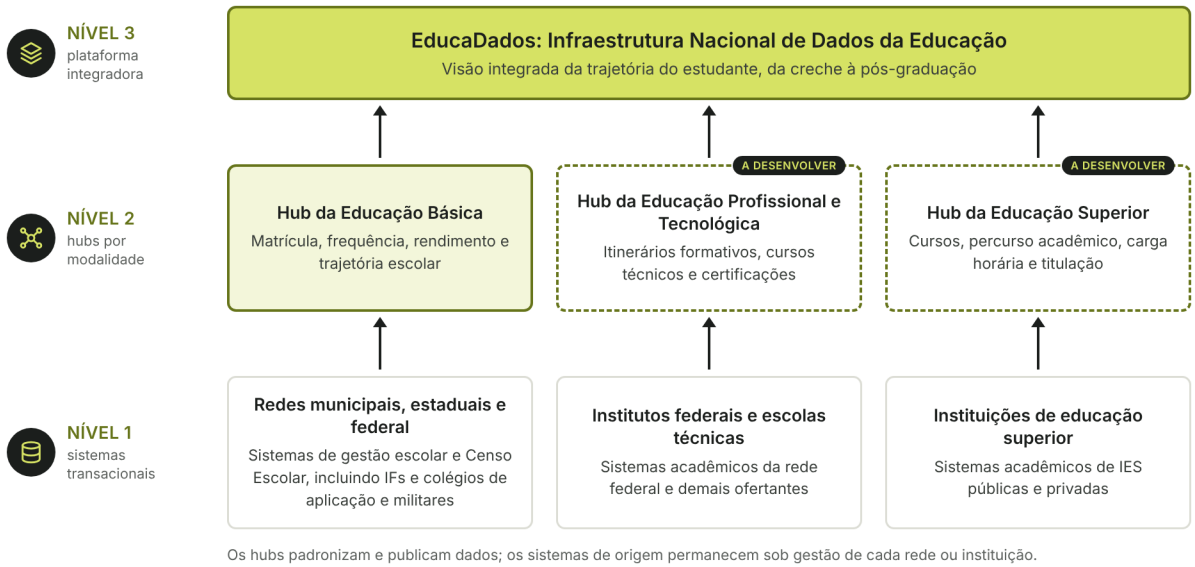


Figura 5. Arranjo em camadas da EducaDados e hubs a desenvolver.

Fonte: Elaboração própria.

O desenvolvimento dos hubs da educação profissional e tecnológica e da educação superior constitui, nesse quadro, uma oportunidade de aplicar o que a experiência indiana demonstrou: construir cada hub a partir de blocos reutilizáveis, publicando esquemas e interfaces antes de implementar integrações. A contribuição concreta dos blocos observados é dupla. De um lado, a definição do hub como um conjunto de dados com esquema declarado, origens identificadas e métricas próprias de acompanhamento oferece um modelo de construção aplicável diretamente [36]. De outro, o fato de que ambos os hubs tratam de percursos, itinerários formativos na educação profissional, percurso acadêmico na educação superior, sugere que seus esquemas sejam projetados desde o início para suportar a emissão de credenciais, e não apenas a produção de estatísticas.

4.2.4 Credenciais da trajetória integrada, da creche à pós-graduação

A EducaDados tem como objetivo possibilitar o acompanhamento integrado da trajetória educacional dos estudantes, desde a educação infantil até a pós-graduação [41]. Atualmente, essa iniciativa está voltada principalmente à produção de informações estatísticas e institucionais que apoiam o planejamento, o monitoramento e a avaliação das políticas educacionais, além de oferecer oportunidades para o desenvolvimento de novos serviços e funcionalidades voltados diretamente aos estudantes.

A oportunidade consiste em atribuir à mesma trajetória uma segunda função, voltada ao cidadão. Ao longo da vida escolar e acadêmica, o estudante acumularia um conjunto de credenciais emitidas

pelas instituições pelas quais passou, conclusão de etapas da educação básica, certificações técnicas, disciplinas e carga horária cursadas na educação superior, diploma e titulação, formando um registro portátil e verificável de sua formação.

O contraste com o instrumento existente hoje é esclarecedor. O diploma digital, regulado desde 2019, trata exclusivamente do diploma de graduação, emitido ao final do curso, com assinatura por meio de infraestrutura de chaves públicas [48]. É um instrumento consolidado e adequado ao seu propósito, mas que nada atesta sobre o percurso: não há meio padronizado de comprovar que um estudante está regularmente matriculado, em que curso, em que período e com que percentual de integralização da carga horária. São precisamente esses os fatos exigidos em estágios, em programas de mobilidade, na concessão de benefícios e em processos seletivos. Uma credencial de percurso pode, inclusive, tratar com precisão a situação dos estudantes em fluxo individual, que cursam disciplinas de períodos distintos, mediante comparação entre o projeto pedagógico do curso e o registro das disciplinas já integralizadas.

Convém registrar que a extensão à trajetória completa amplia, proporcionalmente, as exigências de proteção de dados. A divulgação seletiva, que permite comprovar um fato sem revelar os demais atributos contidos na credencial, deixa de ser um refinamento técnico para se tornar um requisito de projeto.

4.2.5 Observabilidade dos fluxos de dados educacionais

Uma infraestrutura federativa de dados depende da qualidade do que cada ente publica, e essa qualidade não é observável sem instrumentação. Hoje, problemas de completude, de atraso ou de inconsistência nos fluxos de dados tendem a ser percebidos tardiamente, quando já afetaram um relatório, um indicador ou a execução de um programa.

Com um componente de observabilidade, cada conjunto de dados publicado por um hub passaria a ter métricas próprias de acompanhamento, volume recebido, defasagem em relação ao evento de origem, proporção de registros rejeitados na validação contra o esquema, apuradas de forma contínua e visíveis tanto ao gestor nacional quanto à rede que origina o dado [36]. A diferença em relação a um painel de indicadores convencional está no objeto: não se trata de medir a educação, mas de medir o próprio fluxo de dados sobre ela, o que torna a qualidade da informação um atributo gerenciado e não presumido. A Tabela 3 sintetiza os cinco casos, indicando, para cada um, a capacidade requerida, a dependência institucional envolvida e a complexidade estimada de implantação.

CRITÉRIO DE SELEÇÃO DOS CASOS

Os cinco casos compartilham uma propriedade que convém explicitar: nenhum deles exige substituir as aplicações de software que hoje operam as políticas públicas educacionais. Todos acrescentam uma camada de prova ou de padronização aos registros que continuam sob a gestão de quem os produz. É essa característica que os torna experimentáveis em escala reduzida e reversíveis, condições necessárias para que a experimentação preceda

Tabela 3. Síntese dos casos de uso propostos.

Caso de uso	Capacidade requerida	Dependência institucional	Complexidade
Avaliadores e editoras do PNLD	Registro de pessoas e organizações; emissão e verificação de credenciais	Adesão de instituições formadoras como emissoras	Baixa
Trajetória na educação básica	Emissão de credenciais a partir dos sistemas de registro das redes	Pactuação federativa sobre esquema e responsabilidade de emissão	Alta
Hubs de EPT e de educação superior	Conjuntos de dados com esquema declarado e métricas próprias	Definição de esquemas e vocabulários por modalidade	Média
Trajetória integrada do estudante	Credenciais encadeadas entre modalidades, com divulgação seletiva	Integração entre os hubs e tratamento de dados pessoais	Alta
Observabilidade dos fluxos de dados	Ingestão, validação contra esquema e métricas por conjunto de dados	Acordo sobre indicadores de qualidade e sua publicidade	Baixa

Fonte: Elaboração própria. A coluna de complexidade expressa avaliação dos autores, considerando o esforço técnico e a articulação federativa requerida.

a decisão de implantação.

SEÇÃO 05

Arquitetura de Referência e Diretrizes Técnicas

A arquitetura apresentada nesta seção é uma proposta conceitual e deliberadamente independente de domínio. Seu propósito não é especificar uma implantação, mas estabelecer o vocabulário e as decisões estruturantes que organizam a adoção de bens públicos digitais em relação a sistemas que já existem e operam, quaisquer que sejam. As particularidades de cada política pública e os resultados das provas de conceito deverão confirmar ou rever essas decisões.

5.1 Premissas e requisitos arquiteturais

Quatro premissas delimitam o espaço de soluções admissíveis. A primeira é a preservação dos sistemas de software existentes: as aplicações que hoje operam as políticas permanecem em produção, sob a gestão de quem as mantém e com seus próprios bancos de dados, e a arquitetura acrescenta camadas sobre elas, em vez de substituí-las. No caso brasileiro, essa premissa tem fundamento adicional no arranjo federativo, que distribui a titularidade dos sistemas entre entes autônomos. A segunda é a reversibilidade: cada componente deve ser desativado sem comprometer o funcionamento dos sistemas de origem, condição para que a experimentação preceda a decisão de implantação. A terceira é a soberania como propriedade técnica: os componentes são auto-hospedados em infraestrutura sob controle do órgão adotante, sem dependência operacional de serviços de terceiros. A quarta é a primazia da especificação sobre a implementação: o que se padroniza são esquemas, vocabulários e interfaces, não produtos.

Dessas premissas decorrem cinco requisitos. A **interoperabilidade semântica** exige que cada conjunto de dados publicado tenha um esquema declarado e um vocabulário estável, de modo que seu significado não dependa de um acordo bilateral entre as partes. A **verificabilidade sem consulta ao emissor** exige que uma prova apresentada pelo titular possa ser conferida criptograficamente, inclusive quando o sistema emissor estiver indisponível. A **minimização** exige que cada verificação revele apenas o atributo necessário, o que torna a divulgação seletiva um requisito de projeto, e não um refinamento posterior. A **substituibilidade** exige que qualquer componente possa ser substituído por outra implementação conforme a mesma especificação. A **rastreabilidade** exige que todo dado publicado permita identificar sua origem, o momento de sua produção e as transformações a que foi submetido.

5.2 Modelo conceitual de uma arquitetura baseada em DPI/DPG

O modelo arquitetural representado na Figura 6, descreve a adoção de blocos de construção como acréscimo a um conjunto de sistemas de software em operação, e não como sua substituição.

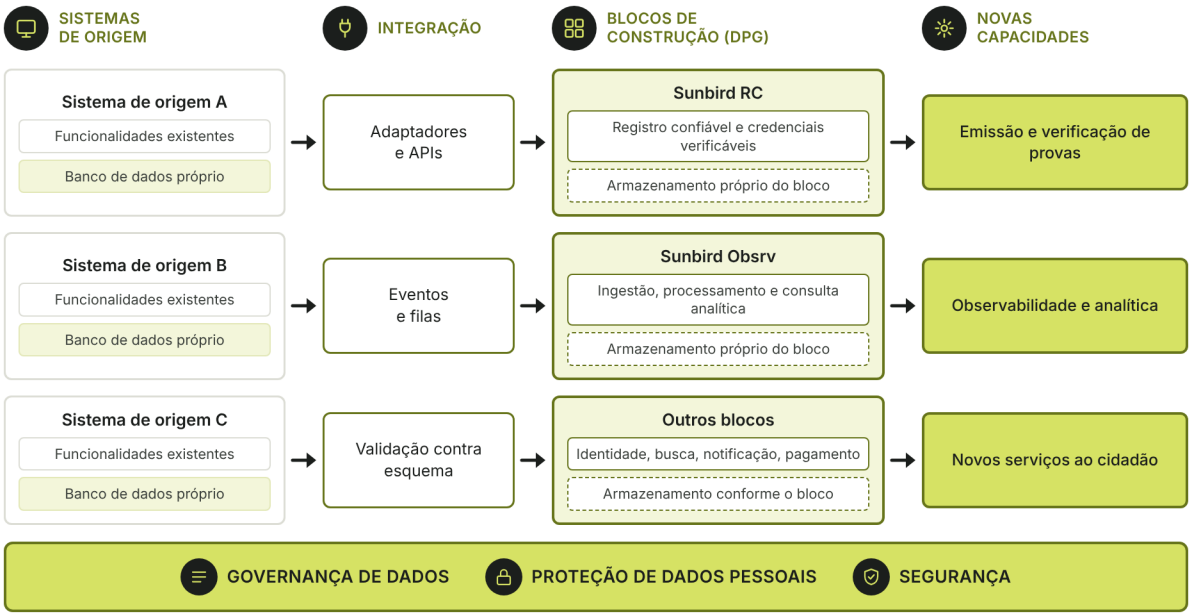


Figura 6. Modelo conceitual de arquitetura baseada em DPI/DPG.

Fonte: Elaboração própria.

À esquerda situam-se os sistemas de origem. Cada um deles já possui suas funcionalidades e seu próprio banco de dados, e continua a ser a autoridade sobre os fatos que registra. A arquitetura não lhes retira atribuições nem exige migração de acervo: o que se acrescenta é a possibilidade de que esses fatos sejam expostos de forma padronizada e utilizados por capacidades que o sistema de origem não oferece.

A camada de integração reúne o que liga um ao outro: adaptadores e interfaces de programação específicos de cada sistema, a publicação de eventos quando o dado muda e a validação do que é publicado contra o esquema declarado. É uma camada fina, mas é nela que se concentra o esforço específico de cada implantação.

Os blocos de construção constituem a camada que efetivamente acrescenta capacidades. Cada bloco é um componente autônomo, com funcionalidades próprias e, quando sua natureza o exige, armazenamento próprio. Um bloco de registros confiáveis mantém as entidades que administra e o estado das credenciais que emitiu. Um bloco de observabilidade mantém os conjuntos de dados processados e as séries históricas derivadas deles. Blocos de identidade, busca ou notificação mantêm o que lhes é necessário. À direita, finalmente, situam-se as capacidades que daí resultam e que não existiam antes, emissão e verificação de provas, observabilidade e analítica, novos serviços ao cidadão. Ao longo de todo o conjunto, a governança de dados, a proteção de dados pessoais e a segurança não pertencem a nenhuma camada isoladamente.

Dessa estrutura decorre a decisão mais consequente do modelo, relativa à duplicação de ar-

mazenamento. Quando um bloco mantém base própria, passam a existir dois lugares em que o mesmo fato aparece, e é indispensável declarar qual deles é autoritativo. A regra proposta é simples: o sistema de origem permanece autoritativo sobre os fatos que já registrava; a base do bloco é autoritativa apenas sobre o que ele próprio cria, o identificador de uma credencial emitida, seu estado de revogação, a série analítica derivada de um fluxo de eventos. Violar essa regra, permitindo que a base do bloco se torne uma fonte paralela de fatos já registrados na origem, reintroduz exatamente o problema de divergência entre bases que a arquitetura pretende resolver.

Uma segunda decisão separa dois fluxos que partem da mesma origem e que não devem ser confundidos. O **fluxo agregado** leva dados padronizados aos painéis, estudos e processos de decisão; seu destinatário é a administração, e seu requisito dominante é a comparabilidade. O **fluxo individual** conduz provas assinadas pelo emissor ao titular, que as apresenta a quem precise verificá-las; seu destinatário é o cidadão e seu requisito dominante é a minimização. Tratá-los como um só produz, previsivelmente, dois defeitos: bases analíticas que acumulam dados pessoais desnecessários e comprovações que dependem da disponibilidade de uma base central.

5.3 Componentes compartilhados e integração com sistemas de software existentes

Quatro componentes concentram o potencial de reúso entre domínios e políticas, e, para cada um deles, o ecossistema examinado na Seção 3 oferece uma implementação de referência. O **registro confiável** mantém dados estruturados sobre pessoas, instituições ou objetos, com esquema padronizado e autoridade identificada, e, a partir deles, emite e verifica provas portáteis; é a função do Sunbird RC [35]. A **ingestão e observabilidade** trata a cadeia que vai da origem à consulta analítica, com métricas próprias por conjunto de dados; é a função do Sunbird Obsrv [36]. O **catálogo de metadados** descreve o que existe, quem é responsável e sob que condições pode ser utilizado. Os demais blocos — identidade, busca, notificação e pagamento — seguem a mesma lógica e são adotados conforme a necessidade de cada caso.

A integração com os sistemas de software existentes admite três caminhos, em ordem crescente de intervenção. No mais leve, utiliza-se apenas o serviço de emissão de credenciais, mantendo-se o sistema atual como fonte de dados. No intermediário, importa-se o acervo existente para um registro, que passa a operar em paralelo. No mais profundo, implanta-se o bloco como sistema de origem para um novo domínio, situação em que a questão da duplicação de armazenamento não se coloca. Para um parque de sistemas já em operação, o primeiro caminho é o de melhor relação entre benefício e risco, por não exigir migração nem alterações no que está em produção.

Convém explicitar uma delimitação de escopo evidenciada pela experiência indiana: os conectores e adaptadores que ligam cada sistema de origem aos blocos não são fornecidos por eles e constituem um trabalho específico de cada implantação. É nesse ponto que se concentra o custo real de uma adoção. Daí a importância da padronização de esquemas: ela converte um problema de ordem quadrática, em que cada par de sistemas negocia seu próprio acordo, em um problema linear, em que cada sistema se adapta uma única vez a um esquema público.

5.4 Governança de dados, segurança e observabilidade

A regra de atribuição de responsabilidade decorre da decisão sobre autoridade tomada na subseção anterior: emite a credencial quem detém competência administrativa sobre o fato atestado, que é, em geral, quem opera o sistema de origem em que o fato foi registrado. Deslocar a emissão para uma instância central que não detém essa competência enfraquece o valor probatório da prova e transfere a essa instância um risco que não lhe cabe.

O tratamento de dados pessoais segue o regime da LGPD [17], com três consequências de projeto. A base legal deve ser identificada por finalidade, e não por sistema. A minimização implica que o verificador receba a resposta à pergunta feita, e não o conjunto de atributos do titular. E o compartilhamento de dados entre órgãos, previsto como diretriz no marco do governo digital [30], exige registro de quem acessou o quê e com que fundamento.

Três mecanismos costumam ser subestimados no projeto de infraestruturas de credenciamento e merecem uma decisão explícita. A **revogação** permite invalidar uma credencial emitida por erro ou por mudança da situação atestada. A **rotação de chaves** preserva a verificabilidade de credenciais antigas após a substituição do material criptográfico do emissor. A **expiração** delimita o período em que uma prova permanece aceitável. A observabilidade, por sua vez, aplica-se ao fluxo de dados e não apenas aos sistemas: cada conjunto de dados publicado deve ter métricas de volume, de defasagem e de rejeição na validação, visíveis tanto a quem consome o dado quanto a quem o origina [36].

5.5 Diretrizes de engenharia de software e evolução tecnológica

A arquitetura proposta é construída com base em cinco diretrizes técnicas. A primeira recomenda priorizar a configuração em vez da programação, utilizando esquemas e regras para definir as funcionalidades sempre que os componentes permitirem. Essa abordagem reduz a necessidade de desenvolver código específico e valoriza a capacidade da equipe de modelar dados e processos. A segunda diretriz trata do versionamento dos esquemas, buscando preservar a compatibilidade com as aplicações existentes à medida que os componentes evoluem. A terceira destaca a importância de disponibilizar não apenas o código-fonte, mas também as especificações técnicas, fundamentais para manter a interoperabilidade entre diferentes implementações [19]. A quarta recomenda verificar essa interoperabilidade por meio de testes com implementações independentes, permitindo avaliar se os padrões definidos funcionam na prática [29]. Por fim, a quinta diretriz incentiva a contribuição para a evolução dos componentes já existentes, evitando a criação de versões paralelas que possam aumentar os custos de manutenção e dificultar o aproveitamento das melhorias desenvolvidas pela comunidade.

5.6 Critérios de validação e avaliação técnica

As provas de conceito devem produzir evidência, e não apenas demonstração. A Tabela 4 reúne os critérios propostos para sua avaliação, cada qual associado a uma evidência verificável.

Tabela 4. Critérios de avaliação técnica das provas de conceito.

Critério	O que verificar	Evidência esperada
Conformidade a padrões	Aderência ao modelo de dados e aos protocolos adotados	Credencial emitida verificada por implementação independente
Custo de integração	Esforço efetivo de ligação ao sistema de origem	Registro de horas e de pontos de alteração no sistema existente
Consistência entre bases	Convergência entre a base do bloco e o sistema de origem	Divergência medida após operação concorrente por período definido
Reversibilidade	Possibilidade de desativar o componente sem efeito sobre a origem	Procedimento de desativação executado e documentado
Proteção de dados pessoais	Base legal, minimização e registro de acesso	Verificação que revele apenas o atributo consultado
Desempenho	Comportamento sob carga representativa da operação prevista	Medição com volume projetado, não com amostra
Sustentabilidade do componente	Mantenedor identificável, licença e atividade da comunidade	Histórico de versões e de correções no período

Fonte: Elaboração própria.

SÍNTESE DA SEÇÃO

A arquitetura proposta acrescenta capacidades a sistemas de software já existentes, sem substituí-los, e apoia-se em quatro premissas: preservação das aplicações de software de origem, reversibilidade, soberania técnica e primazia da especificação sobre a implementação. Sua decisão central é a regra de autoridade: o sistema de origem continua responsável pelos fatos que registra, e o bloco de construção responde apenas pelo que cria, evitando divergências entre bases. A separação entre o fluxo agregado, voltado à gestão, e o fluxo individual, voltado ao cidadão, preserva a minimização de dados pessoais. Para ambientes já em operação, o caminho mais seguro é usar apenas o serviço de emissão de credenciais, mantendo o sistema atual como fonte de dados. A validação por meio de provas de conceito, avaliadas segundo critérios verificáveis, deve preceder qualquer decisão de implantação em larga escala.

SEÇÃO 06

DPI e DPG na Prática: Um Exemplo com Credenciais Verificáveis - Sunbird RC

Esta seção apresenta uma prova de conceito desenvolvida pelo DPI Lab utilizando o componente Sunbird RC. O experimento demonstra, em ambiente controlado e com dados sintéticos, as etapas de emissão, apresentação e verificação de uma credencial digital, permitindo observar, na prática, a aplicação das decisões arquiteturais discutidas na Seção 5. Para essa demonstração, foi escolhido um cenário da educação superior, embora o mesmo processo possa ser aplicado a outras credenciais institucionais, como licenças, registros profissionais e comprovantes de participação em programas públicos. O exemplo apresenta uma situação fictícia envolvendo Luana, estudante de Ciências Sociais da Universidade Federal do DPI, que deseja participar de uma seleção de estágio e precisa comprovar sua matrícula ativa e a conclusão de metade da carga horária do curso. A Figura 7 ilustra dois momentos dessa situação, enquanto a narrativa completa está disponível no Apêndice A.



Figura 7. Dois momentos do cenário: o problema e a verificação.

Fonte: Elaboração própria. Cenário fictício, com dados de teste.

6.1 O cenário: comprovar o percurso durante o curso

A situação de partida é conhecida e foi caracterizada na Seção 4. Cada processo seletivo define sua própria lista de documentos, e cabe ao estudante obtê-los, um a um, na secretaria, em formatos que variam conforme quem os solicita. O destinatário recebe arquivos cuja autenticidade não pode conferir senão entrando em contato com a instituição emissora. E, com frequência, recebe muito mais do que precisa: para comprovar que metade do curso foi cumprida, costuma-se entregar o histórico escolar completo, com todas as notas obtidas. O instrumento digital hoje disponível na educação superior não resolve esse caso, pois o diploma digital trata do documento emitido ao final do curso, e não do percurso em andamento [48].

Com credenciais verificáveis, o mesmo processo assume outra forma. A universidade, que detém competência administrativa sobre o fato, emite uma credencial assinada; Luana a mantém em uma carteira digital sob seu controle; o verificador declara quais informações precisa e recebe apenas essas; Luana confere o pedido e decide se autoriza; e o verificador confere a origem e a integridade da prova sem precisar consultar a universidade. Cada um dos requisitos enunciados na Seção 5, verificabilidade sem consulta ao emissor, minimização, autoridade na origem, aparece aqui como um passo concreto do fluxo.

6.2 Implementação e execução da prova de conceito

A prova de conceito materializa os três papéis do ciclo em três aplicações independentes, que se comunicam por protocolos abertos. A primeira é o sistema de gestão da secretaria acadêmica da Universidade DPI, que emite. A segunda é a carteira do estudante, executada no celular, que guarda e apresenta. A terceira é o portal de carreiras de uma empresa fictícia, que verifica. Por trás delas operam, de forma integrada, os serviços de identidade, de gerenciamento de esquemas, de gestão de credenciais e de emissão por protocolo aberto do Sunbird RC. A Tabela 5 sintetiza as fases do ciclo e sua correspondência com a implementação.

Tabela 5. Fases do ciclo e correspondência com a implementação.

Fase	O que a prova de conceito executa	Padrão ou serviço
Preparação	Identidade do emissor e declaração do esquema da credencial	Identificadores descentralizados; JSON Schema
Emissão	Conferência da ficha, certificação nominal pelo servidor e geração da oferta	OID4VCI
Armazenamento	Leitura da oferta pela carteira e guarda sob controle do titular	Carteira da prova de conceito
Requisição	Pedido com declaração explícita dos campos necessários e dos dispensados	OID4VP
Autorização	Conferência das duas listas pelo titular, decisão e verificação de origem e integridade	OID4VP; modelo de dados do W3C [29]
Revogação	Invalidação de credencial anterior quando a situação ou o histórico mudam	Sunbird RC [35]

Fonte: Elaboração própria, a partir da prova de conceito.

6.3 Resultados e alcance da prova de conceito

6.3.1 Emissão: conferência e assinatura pela instituição

A emissão começa pela constituição do emissor: a universidade recebe um identificador descentralizado e um par de chaves com o qual assinará as credenciais. Em seguida, declara-se o esquema da credencial em JSON Schema, com os campos que ela conterá, seus tipos e sua obrigatoriedade, e publica-se esse esquema habilitado para emissão. É aqui que a diretriz de configuração em vez de código, discutida na Seção 5, se manifesta de forma mais visível: o que define a credencial é um documento declarativo, não um programa.

A Figura 8 ilustra o que ocorre no sistema de gestão da secretaria. O servidor tem diante de si a ficha completa da estudante: dados cadastrais, vínculo de matrícula com situação, período atual e validade, e o histórico escolar período a período, com carga horária, notas e situação de cada disciplina. Antes de emitir, ele firma um termo nominal, declarando que conferiu aqueles dados e que estão corretos para a emissão da credencial assinada pela universidade.

Esse passo merece destaque porque não é uma mera formalidade de interface. Ele materializa a regra enunciada na Seção 5: emite a credencial quem detém competência administrativa sobre o fato atestado. O valor probatório da credencial não decorre apenas da assinatura criptográfica da instituição, mas também do ato registrado de um servidor identificado que conferiu o que está sendo atestado. A mesma tela adverte quando já existem credenciais válidas para aquele estudante e orienta a revogar a anterior caso a situação ou o histórico tenham mudado, o que traz a revogação para dentro do fluxo cotidiano, e não para um procedimento excepcional.

Concluída a conferência, a emissão gera uma oferta de credencial destinada àquela titular, materializada em um QR code conforme o protocolo de emissão da OpenID Foundation [49]. A carteira do estudante lê o código, obtém a credencial e a guarda. A partir desse momento, a prova está sob controle da titular, e a carteira é o único lugar onde ela precisa estar para ser apresentada.

6.3.2 Apresentação seletiva: o pedido e a decisão

No portal de carreiras, o formulário de inscrição no estágio oferece duas alternativas ao candidato: anexar o histórico escolar em PDF, como se faz hoje, ou preencher a inscrição a partir da carteira digital. A segunda alternativa abre o pedido reproduzido na Figura 9.

Os dois lados da figura são o aspecto mais instrutivo do experimento. À esquerda, o verificador declara, antes de qualquer coisa, exatamente o que receberá: nome completo, curso, situação da matrícula, histórico escolar e os identificadores do emissor e da credencial, estes últimos para confirmar a origem e verificar se a credencial não foi revogada. E declara também o que não pede: CPF, data de nascimento, endereço eletrônico e número de matrícula. À direita, a carteira apresenta à titular as mesmas duas listas, agora como decisão sua, o que será compartilhado e o que não será, com os botões de autorizar e recusar.

A apresentação seletiva aparece aqui como propriedade do pedido, e não do documento [50]. Quem pede é obrigado a enunciar o mínimo de que precisa, e é essa enunciação que o titular



Figura 8. Emissão: a secretaria acadêmica confere a ficha e certifica o que foi conferido.

Fonte: Prova de conceito do DPI Lab, executada em ambiente local com dados de teste.

avalia. Convém registrar uma limitação que a própria carteira já explicita na tela: o pedido informa que a identidade do verificador não está confirmada. O protocolo garante a origem da credencial, não a identidade de quem a solicita, o que remete a um problema distinto, o do credenciamento de verificadores, que a prova de conceito não aborda.

6.3.3 Resultado: o formulário preenchido e conferido

Autorizada a apresentação, o verificador confere a assinatura do emissor e a integridade dos dados recebidos, e preenche o formulário com eles. A Figura 10 mostra o resultado.

O que antes exigia anexar um arquivo em formato PDF, agora chega como campo preenchido e marcado como verificado, com o registro de quem emitiu e de quando foi conferido. Nome, instituição e curso aparecem assim, e o portal ainda oferece a alternativa de preenchimento manual para quem não dispõe da credencial.

A Figura 11 mostra a continuação da mesma tela. O histórico escolar não chega como anexo, mas renderizado no próprio formulário, período a período, com código, disciplina, carga horária, nota e situação de cada componente, inclusive as disciplinas em curso, marcadas como tal. À candidata resta completar apenas o que a credencial não traz.

Duas observações fecham o ciclo. A primeira é de natureza probatória: o recrutador deixa de receber um arquivo que não pode conferir e passa a receber dados cuja origem está demonstrada,



Figura 9. Apresentação seletiva: o verificador declara de que precisa e a titular decide.

Fonte: Prova de conceito do DPI Lab, executada em ambiente local com dados de teste.

sem precisar contatar a universidade. A segunda diz respeito à proteção de dados. A credencial atende à comprovação, mas não dispensa a base legal para o tratamento posterior: o formulário mantém o consentimento expresso do candidato para que a empresa trate tais dados exclusivamente no processo seletivo, nos termos da LGPD [17]. São camadas distintas, e a presença de uma não substitui a outra.

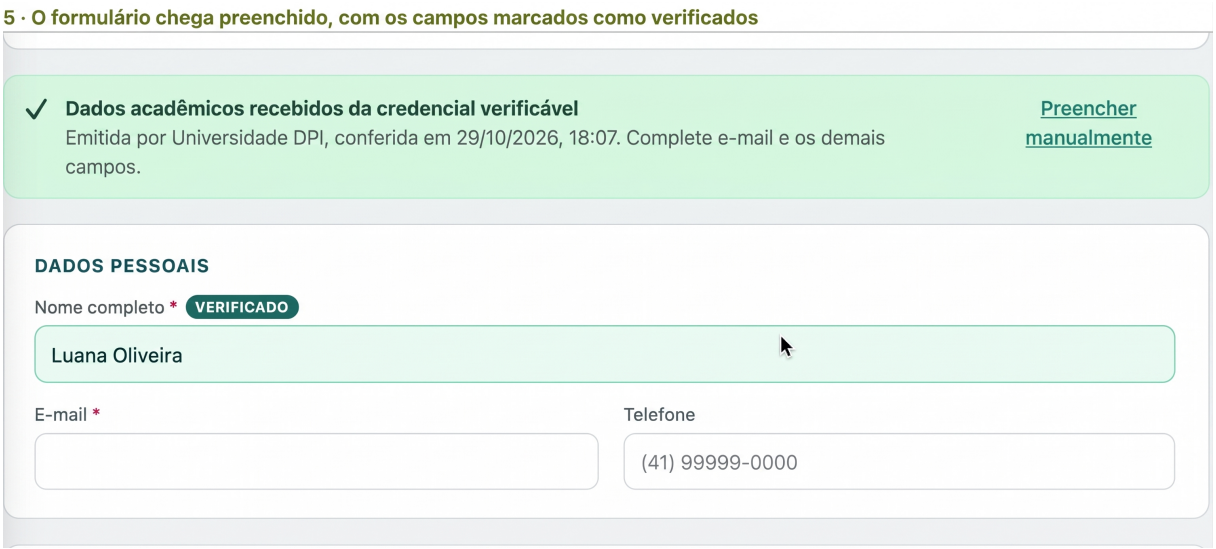


Figura 10. Resultado: campos preenchidos e marcados como verificados no portal do verificador.

Fonte: Prova de conceito do DPI Lab, executada em ambiente local com dados de teste.

Quatro resultados merecem registro. O primeiro é que a emissão foi obtida por declaração: definir uma nova credencial consistiu em escrever um esquema e publicá-lo, sem alterar o código do bloco de construção, o que significa que credenciais de outros domínios obtêm-se pelo mesmo caminho,

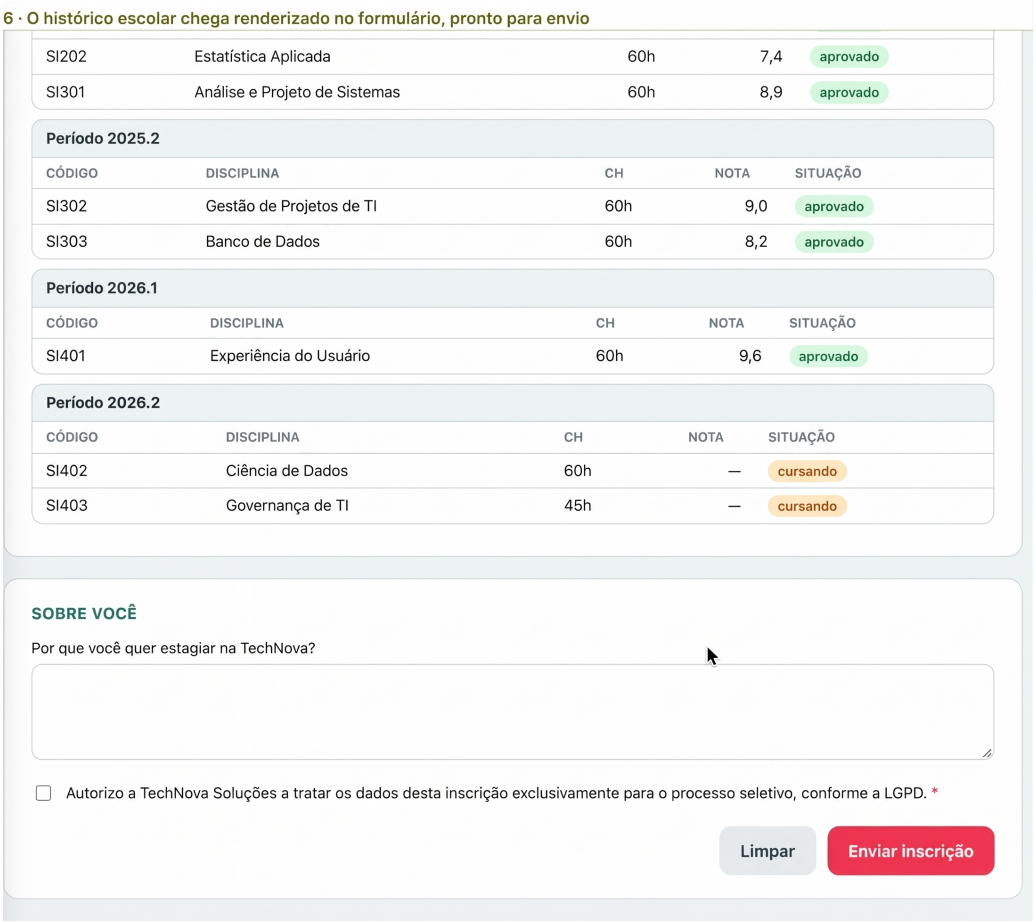


Figura 11. Histórico escolar importado da credencial e exibido no formulário de inscrição.

Fonte: Prova de conceito do DPI Lab, executada em ambiente local com dados de teste.

com outro esquema. O segundo é que o ciclo ocorreu entre três aplicações independentes, que se comunicavam por protocolos públicos, o que sustenta a expectativa de que outras carteiras e outros verificadores, conformes aos mesmos protocolos, possam participar do fluxo. O terceiro é que a minimização mostrou-se operacional, e não apenas declarada: o pedido obriga quem verifica a enunciar o mínimo necessário, e a carteira apresenta ao titular tanto o que será compartilhado quanto o que será retido. O quarto é que a revogação foi exercida como parte do fluxo de trabalho da secretaria, e não como procedimento à parte.

Considerando o caráter inicial e exploratório da prova de conceito, o experimento concentrou-se na demonstração das principais funcionalidades do Sunbird RC, utilizando dados sintéticos e um ambiente controlado. A evolução desse trabalho contempla a integração com sistemas acadêmicos em produção, permitindo avaliar os requisitos técnicos e operacionais discutidos na Seção 5. Também estão previstas análises relacionadas à gestão e à rotação das chaves criptográficas do emissor, à identificação e ao credenciamento dos verificadores e à avaliação de desempenho sob diferentes condições de uso. Outra etapa importante será a realização de testes de conformidade com implementações independentes, visando verificar a interoperabilidade entre diferentes soluções, conforme os critérios apresentados na Seção 5. Essas atividades permitirão ampliar a avaliação da arquitetura proposta e orientar sua aplicação progressiva em cenários reais.

Uma das próximas etapas de evolução da prova de conceito consiste em ampliar as informações disponibilizadas pela credencial digital. Na versão atual, a credencial já inclui o histórico escolar completo, com disciplinas cursadas, carga horária, notas e situação acadêmica por período. Como aprimoramento, está prevista a inclusão do percentual de integralização da carga horária do curso, informação necessária para atender plenamente ao cenário apresentado. Esse cálculo requer a integração entre os dados do histórico escolar e o projeto pedagógico do curso, considerando também as particularidades dos estudantes que cursam disciplinas de períodos distintos. A implementação dessa funcionalidade permitirá ampliar as possibilidades de uso da credencial e oferecer informações ainda mais relevantes aos estudantes.

PRINCIPAIS RESULTADOS E PERSPECTIVAS DE EVOLUÇÃO

A prova de conceito demonstrou a viabilidade técnica do ciclo completo de credenciais verificáveis em ambiente controlado, abrangendo emissão, guarda, apresentação seletiva, verificação e revogação entre três aplicações independentes. O experimento evidenciou, em particular, que a minimização e a decisão informada do titular são propriedades que se materializam na interface gráfica, e não apenas no protocolo. Os resultados constituem uma contribuição técnica para a aplicação de DPI e DPG em políticas públicas, especialmente na reutilização de componentes de software e na integração entre sistemas de software existentes.

SEÇÃO 07

Cooperação Continuada e Apoio à Adoção

As seções anteriores apresentaram o ecossistema, a arquitetura e os resultados da experimentação realizada. Esta seção aborda as perspectivas de continuidade desse trabalho, destacando o compromisso do NEES/UFAL, por meio do Laboratório de Infraestrutura Pública Digital (DPI Lab), com o avanço das pesquisas, a cooperação científica e o desenvolvimento de soluções baseadas em DPI e DPG. Essa atuação contempla a colaboração continuada com o IIIT-B e COSS, bem como o apoio a instituições interessadas na adoção dessas abordagens, seja no desenvolvimento de novas soluções, seja na integração de componentes a sistemas e ambientes tecnológicos existentes.

7.1 Alinhamento continuado com o ecossistema

O acompanhamento contínuo da evolução do ecossistema constitui um compromisso do NEES/UFAL, por meio do DPI Lab, fundamentado nos aprendizados apresentados na Seção 3. A adoção de componentes de software mantidos por terceiros pode reduzir os esforços iniciais de desenvolvimento, mas também implica acompanhar decisões e mudanças tecnológicas que não estão inteiramente sob o controle das instituições que os utilizam. A experiência indiana demonstra que uma forma de lidar com essa dependência é participar ativamente da evolução do ecossistema, contribuindo para o desenvolvimento e o aprimoramento de seus componentes. É nessa perspectiva que o NEES/UFAL, por meio do DPI Lab, pretende orientar sua atuação contínua.

Esse alinhamento se organiza em quatro frentes. A primeira é o **acompanhamento técnico** das versões, das especificações e das decisões de projeto dos blocos de construção, de modo que as recomendações formuladas no Brasil não se tornem defasadas em relação ao que efetivamente se mantém e evolui. Como registrado na Seção 3, os blocos são publicados sob formas distintas, especificação, código ou composição, e é essa distinção que determina o que pode ser substituído sem romper a interoperabilidade [27]; acompanhar essa evolução é condição para orientar escolhas de adoção com segurança.

A segunda frente é a **validação de conformidade**. A Seção 5 propôs que a interoperabilidade só se considera demonstrada quando uma credencial emitida por uma implementação é verificada por outra, de forma independente. Exercitar essa validação de forma sistemática, e não apenas no âmbito de uma prova de conceito, é um trabalho técnico contínuo que gera tanto confiança para o adotante quanto retorno para o mantenedor.

A terceira frente é a **contribuição de requisitos e de casos de uso do contexto brasileiro**. As prioridades de evolução de um bem público digital refletem as necessidades de quem o utiliza e de quem com ele contribui. Algumas características do caso brasileiro não se refletem automaticamente nas prioridades de um mantenedor sediado em outro país. É o caso da organização

federativa, que distribui a titularidade dos sistemas entre entes autônomos; da exigência, comum a vários setores, de comprovar situações em curso e não apenas situações concluídas; e do regime estabelecido pela LGPD [17]. Levá-las à comunidade, na forma de requisitos, de casos de uso documentados e de contribuições de código, é a maneira de assegurar que a evolução dos componentes acompanhe as necessidades de quem os adota aqui.

A quarta frente é a **formação de competência técnica**. Projetar, implantar e operar soluções baseadas nesses componentes exige conhecimento que hoje é escasso no país: modelagem de esquemas e vocabulários, protocolos de credenciais verificáveis, engenharia de dados em escala, governança de infraestruturas compartilhadas. Ampliar o número de pessoas capazes de realizar esse trabalho é condição para que a adoção não dependa de um grupo restrito.

A cooperação com o IIIT-B e COSS é o canal por meio do qual essas quatro frentes se tornam efetivas. Iniciada com a missão técnica que deu origem a esta nota, vem sendo convertida em uma agenda conjunta de trabalho, atualmente em construção. Essa agenda contempla a realização de provas de conceito de interesse comum, o intercâmbio técnico entre as equipes e a participação do NEES na discussão das especificações dos blocos. O formato importa menos do que a continuidade: o valor de uma cooperação dessa natureza não está em um acordo pontual, e sim na permanência do contato técnico ao longo dos ciclos de evolução dos componentes.

7.2 Capacidades disponíveis para apoio a instituições

Instituições públicas e privadas que considerem adotar DPI encontram-se, em geral, em uma de duas situações que demandam abordagens distintas.

A primeira é a de quem vai **desenvolver uma solução nova**. Aqui a oportunidade é considerável, porque incorporar blocos de construção desde a concepção evita o custo de reconstruir depois o que foi feito sem eles. O trabalho concentra-se nas decisões iniciais. Quais fatos a solução precisa registrar e com que esquema? Quais capacidades podem ser obtidas por blocos já existentes, em vez de desenvolvidas? Como se distribuem a autoridade e o armazenamento entre os componentes? E como a proteção de dados pessoais é incorporada ao projeto, em vez de ser acrescentada ao final? A arquitetura proposta na Seção 5 serve como ponto de partida para essas decisões.

A segunda é a de quem já tem um **ambiente em operação** e pretende acrescentar-lhe capacidades. Essa é a situação mais comum e, por isso mesmo, a mais sensível: a adoção precisa ser incremental e reversível, sem exigir migração de acervo nem alteração dos sistemas em produção. O trabalho começa por um diagnóstico do parque existente e pela identificação dos fatos já registrados que teriam valor se pudessem circular como prova ou como dados padronizados. Segue-se a escolha do caminho de adoção entre os três descritos na Seção 5, com preferência pelo menos intrusivo, a construção dos adaptadores, a decisão sobre qual base permanece autoritativa e a instrumentação dos fluxos.

Em ambos os casos, o percurso recomendado passa por uma prova de conceito delimitada, avaliada pelos critérios apresentados na Tabela 4, antes de qualquer decisão de implantação ampla. E, em ambos, parte relevante do trabalho é a formação da equipe da própria instituição, para

que a capacidade de operar e evoluir a solução permaneça nela e não dependa indefinidamente de apoio externo. A Tabela 6 resume essas duas situações e acrescenta outras duas formas de apoio, a avaliação preliminar de casos específicos e a formação de equipes, indicando a natureza do trabalho e o resultado esperado em cada uma.

Tabela 6. Situações de adoção e natureza do apoio.

Situação	Natureza do trabalho	Resultado esperado
Solução nova	Modelagem de esquemas, escolha de blocos, definição de arquitetura e de proteção de dados	Projeto arquitetural e primeira versão construída sobre componentes reutilizáveis
Ambiente em operação	Diagnóstico do parque existente, escolha do caminho de adoção, adaptadores e instrumentação	Capacidade nova acrescentada sem alteração dos sistemas de origem
Avaliação preliminar	Exame de viabilidade técnica, institucional e jurídica de um caso específico	Parecer com alternativas, riscos e estimativa de esforço
Formação	Capacitação da equipe em esquemas, credenciais verificáveis e engenharia de dados	Equipe própria capaz de operar e evoluir a solução

Fonte: Elaboração própria.

7.3 Colaboração institucional e participação no ecossistema

O NEES/UFAL, por meio do DPI Lab, mantém aberta uma agenda de colaboração com instituições públicas e privadas interessadas na adoção, no desenvolvimento e na disseminação de DPI e DPG. Essa colaboração pode envolver pesquisas conjuntas, intercâmbio de conhecimentos, desenvolvimento de provas de conceito e apoio à integração de componentes tecnológicos a sistemas existentes.

As instituições interessadas em estabelecer parcerias ou conhecer as iniciativas em andamento podem acompanhar as atividades, os projetos e as publicações do DPI Lab por meio de seu site institucional: https://dpilab.nees.ufal.br.

CONVITE

O NEES/UFAL, por meio do DPI Lab, está aberto à construção de parcerias que contribuam para ampliar a adoção de DPI e DPG no Brasil, promovendo a colaboração entre academia, governo e setor produtivo e o desenvolvimento de tecnologias de interesse público.

Contato: `dpi-lab@nees.ufal.br`

SEÇÃO 08

Considerações Finais

Esta nota técnica partiu dos fundamentos conceituais de infraestruturas públicas digitais e bens públicos digitais, examinou um ecossistema em operação há quase uma década, identificou oportunidades de aplicação no domínio da educação e propôs uma arquitetura de referência, submetida a um primeiro experimento.

O achado central é de natureza institucional, mais do que tecnológica. O problema que esses componentes resolvem não é a ausência de registros confiáveis: organizações públicas e privadas já registram, com autoridade, os fatos que lhes competem, e o marco jurídico brasileiro já estabelece a interoperabilidade como princípio e a proteção de dados como limite. O que falta é a camada capaz de tornar um fato comprovado na origem utilizável, com confiança, por quem não tem acesso ao sistema que o produziu. É essa camada, e não a substituição do que já existe, que os componentes examinados oferecem. Por isso, a mesma oportunidade reaparece em setores tão distintos quanto educação, saúde e qualificação profissional, como mostram as adoções em escala examinadas na Seção 3.

Os resultados apresentados devem ser compreendidos à luz do escopo definido nesta nota técnica. A análise concentrou-se no ecossistema estudado durante a missão técnica à Índia, enquanto a arquitetura de referência foi desenvolvida em nível conceitual e a prova de conceito demonstrou o ciclo completo de uma credencial verificável em ambiente controlado. Essas etapas forneceram subsídios técnicos para avaliar a aplicabilidade das abordagens investigadas e estabelecer uma base para sua evolução. Como próximos passos, estão previstas experimentações em aplicações de software em produção, com a ampliação dos cenários de uso e a avaliação de aspectos de integração, conformidade e interoperabilidade. Os resultados dessa nova etapa serão apresentados na próxima nota técnica, dando continuidade à agenda de pesquisa aplicada e de desenvolvimento tecnológico iniciada nesta publicação.

Uma das principais conclusões técnicas desta nota é que a adoção de DPI e DPG vai além da mera escolha de tecnologias ou componentes de software. Seu sucesso depende de três decisões: sobre os padrões e especificações que assegurem a interoperabilidade; sobre as responsabilidades pela produção e validação das informações; e sobre a participação na evolução dos componentes adotados. Essas decisões envolvem tanto aspectos tecnológicos quanto de governança e são fundamentais para a sustentabilidade das soluções. Conforme apresentado na Seção 7, a continuidade desse trabalho contempla o aprofundamento das questões identificadas durante a experimentação, o acompanhamento da evolução do ecossistema e a colaboração com instituições interessadas na adoção dessas abordagens.

SÍNTESE

- A especificação publicada vale mais do que a implementação adotada: sem ela, o reúso converte-se em dependência.
- O dado permanece na origem; circula a prova ou o dado padronizado, emitindo a prova quem detém competência sobre o fato.
- Reúso só se sustenta com mantenedor institucional e ecossistema de atores: adotar sem participar terceiriza o roteiro de evolução.

Referências

[1] UNITED NATIONS. **Roadmap for digital cooperation**: report of the Secretary-General. Nova York: United Nations, 2020. (A/74/821). Disponível em: https://www.un.org/techenvoy/content/roadmap-digital-cooperation. Acesso em: 28 out. 2026.

[2] SILVA, L. de F. *et al.* Digital transformation in a Brazilian public policy: a case study of pedagogical evaluation within the National Textbook Program. In: ANNUAL INTERNATIONAL CONFERENCE ON DIGITAL GOVERNMENT RESEARCH, 25., 2024. **Proceedings** [...]. New York: Association for Computing Machinery, 2024. p. 515–524. DOI: https://doi.org/10.1145/3657054.3657261.

[3] SILVA, L.; ARAÚJO, A.; ARAÚJO, R. An augmented intelligence framework as an enabler of digital transformation and innovation in the pedagogical evaluation of the Brazilian National Textbook Program (PNLD). In: INTERNATIONAL CONFERENCE ON ARTIFICIAL INTELLIGENCE IN EDUCATION, 2024. **Proceedings** [...]. Cham: Springer, 2024. p. 409–417.

[4] ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. **Digital Government Outlook 2026**: from foundations to transformational impact. Paris: OECD Publishing, 2026. DOI: https://doi.org/10.1787/0496b2bc-en.

[5] ARAÚJO, A. *et al.* Data-driven analysis for improving educational policies: a case in Brazil's Textbook Program. In: ANNUAL INTERNATIONAL CONFERENCE ON DIGITAL GOVERNMENT RESEARCH, 26., 2025. **Proceedings** [...]. [S.l.: s.n.], 2025. v. 26. DOI: https://doi.org/10.59490/dgo.2025.1023.

[6] ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. **Digital public infrastructure for digital governments**. Paris: OECD Publishing, 2024. (OECD Public Governance Policy Papers). DOI: https://doi.org/10.1787/ff525dc8-en.

[7] SILVA, J. *et al.* Agile project management in government software development: addressing challenges in education public policy. In: INTERNATIONAL CONFERENCE ON ENTERPRISE INFORMATION SYSTEMS, 27., 2025. **Proceedings** [...]. Setúbal: SciTePress, 2025. v. 2, p. 340–347. DOI: https://doi.org/10.5220/0013434800003929.

[8] PEREIRA, G. *et al.* Master data management in practice: an empirical analysis of architectural and governance capability. [Veículo, local e ano de publicação].

[9] UNITED NATIONS DEVELOPMENT PROGRAMME. **The DPI approach**: a playbook. Nova York: UNDP, 2023. Disponível em: https://www.undp.org/publications/dpi-approach-playbook. Acesso em: 27 out. 2026.

[10] UNITED NATIONS. Office of the Secretary-General's Envoy on Technology; UNITED NATIONS DEVELOPMENT PROGRAMME. **Universal DPI Safeguards Framework**: a guide to building safe and inclusive DPI for societies. Nova York: United Nations, 2024. Disponível em: https://www.dpi-safeguards.org/. Acesso em: 28 out. 2026.

[11] MEDEIROS, T. *et al.* Data governance in education: addressing challenges and unlocking opportunities for effective data management. In: INTERNATIONAL CONFERENCE ON ENTERPRISE INFORMATION

SYSTEMS, 27., 2025. **Proceedings** [...]. Setúbal: SciTePress, 2025. v. 1, p. 367–374. DOI: https://doi.org/10.5220/0013468300003929.

[12] FERRO, M. R. da C. *et al.* DGMA: a method for assessing the level of data governance maturity. In: ACM/SIGAPP SYMPOSIUM ON APPLIED COMPUTING, 41., 2026. **Proceedings** [...]. New York: Association for Computing Machinery, 2026. p. 548–550.

[13] FERRO, M. *et al.* An evidence-based method for assessing data governance maturity. In: INTERNATIONAL CONFERENCE ON DATABASE AND EXPERT SYSTEMS APPLICATIONS, 2026. **Proceedings** [...]. Cham: Springer, 2026. p. 289–304.

[14] BRASIL. Ministério da Educação. **Portaria nº 664, de 18 de julho de 2024**. Institui o Comitê de Governança de Dados da Educação. Brasília: MEC, 2024.

[15] ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. **Government at a Glance 2025**. Paris: OECD Publishing, 2025. Disponível em: https://www.oecd.org/en/publications/government-at-a-glance-2025_0efd0bcd-en/full-report/digital-public-infrastructure_1cee4220.html. Acesso em: 27 out. 2026.

[16] EUROPEAN COMMISSION. **New European Interoperability Framework**: promoting seamless services and data flows for European public administrations. Luxemburgo: Publications Office of the European Union, 2017. Disponível em: https://interoperable-europe.ec.europa.eu/collection/iopeu-monitoring/european-interoperability-framework-eif. Acesso em: 28 out. 2026.

[17] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília: Presidência da República, 2018.

[18] EAVES, D.; MAZZUCATO, M.; VASCONCELLOS, B. **Digital public infrastructure and public value**: what is 'public' about DPI? Londres: UCL Institute for Innovation and Public Purpose, 2024. (IIPP Working Paper Series, WP 2024-05). Disponível em: https://www.ucl.ac.uk/bartlett/public-purpose/wp2024-05. Acesso em: 28 out. 2026.

[19] DIGITAL PUBLIC GOODS ALLIANCE. **Digital Public Goods Standard**. 2026. Disponível em: https://www.digitalpublicgoods.net/standard. Acesso em: 28 out. 2026.

[20] SUNBIRD. **Sunbird overview**. Sunbird Knowledge Hub. Bengaluru: Centre for Open Societal Systems, [s.d.]. Disponível em: https://sunbird.gitbook.io/coss. Acesso em: 30 out. 2026.

[21] ALONSO, C. *et al*. **Stacking up the benefits**: lessons from India's digital journey. Washington, D.C.: International Monetary Fund, 2023. (IMF Working Paper, n. 23/78). DOI: https://doi.org/10.5089/9798400240416.001.

[22] DESAI, A.; MANOHARAN, A. P. Digital transformation and public administration: the impacts of India's digital public infrastructure. **International Journal of Public Administration**, v. 47, n. 9, p. 575–578, 2024. DOI: https://doi.org/10.1080/01900692.2024.2350762.

[23] G20. **G20 framework for systems of digital public infrastructure**. Anexo 1 ao documento final da Reunião de Ministros da Economia Digital do G20. Bengaluru, 19 ago. 2023. Disponível em: https://g7g20-documents.org/fileadmin/G7G20_documents/2023/G20/India/Sherpa-Track/Digital%20Economy%20Ministers/2%20Ministers'%20Annex/G20_Digital%20Economy%20Ministers%20Meeting_Annex1_19082023.pdf. Acesso em: 28 out. 2026.

[24] BRASIL. **Decreto nº 12.069, de 21 de junho de 2024**. Dispõe sobre a Estratégia Nacional de Governo Digital e a Rede Nacional de Governo Digital (Rede Gov.br) e institui a Estratégia Nacional de Governo Digital para o período de 2024 a 2027. Brasília: Presidência da República, 2024.

[25] BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. **O que são Infraestruturas Públicas Digitais (IPDs)?** Brasília: MGI, 2024. Disponível em: https://www.gov.br/governodigital/pt-br/estrategias-e-governanca-digital/estrategianacional/faq/o-que-sao-infraestruturas-publicas. Acesso em: 27 out. 2026.

[26] BANCO INTERAMERICANO DE DESENVOLVIMENTO. **Sunbird**. Washington, D.C.: BID, [s.d.]. Código para o Desenvolvimento - Soluções de código aberto. Disponível em: https://knowledge.iadb.org/en/open-knowledge/code-development/open-source-solution/sunbird. Acesso em: 28 out. 2026.

[27] SUNBIRD. **Building blocks**. Bengaluru: Centre for Open Societal Systems, 2026b. Disponível em: https://sunbird.org/building-blocks. Acesso em: 28 out. 2026.

[28] PARNAS, D. L. On the criteria to be used in decomposing systems into modules. **Communications of the ACM**, v. 15, n. 12, p. 1053–1058, 1972. DOI: https://doi.org/10.1145/361598.361623.

[29] WORLD WIDE WEB CONSORTIUM. **Verifiable credentials data model v2.0**. [S.l.]: W3C, 2025. W3C Recommendation. Disponível em: https://www.w3.org/TR/vc-data-model-2.0/. Acesso em: 28 out. 2026.

[30] BRASIL. **Lei nº 14.129, de 29 de março de 2021**. Dispõe sobre princípios, regras e instrumentos para o Governo Digital e para o aumento da eficiência pública. Brasília: Presidência da República, 2021.

[31] EGHBAL, N. **Roads and bridges**: the unseen labor behind our digital infrastructure. Nova York: Ford Foundation, 2016. Disponível em: https://www.fordfoundation.org/work/learning/research-reports/roads-and-bridges-the-unseen-labor-behind-our-digital-infrastructure/. Acesso em: 28 out. 2026.

[32] SUNBIRD. **Sunbird**: open source digital public goods. Bengaluru: Centre for Open Societal Systems, 2026a. Disponível em: https://sunbird.org. Acesso em: 28 out. 2026.

[33] NEWS ON AIR. **iGOT Karmayogi platform crosses mark of 1 cr registered civil servants**. Nova Délhi: Akashvani News, 21 maio 2025. Disponível em: https://www.newsonair.gov.in/igot-karmayogi-platform-crosses-mark-of-1-cr-registered-civil-servants. Acesso em: 28 out. 2026.

[34] SUNBIRD ED. **Sunbird Ed 9.0 - Spark**. Bengaluru: Centre for Open Societal Systems, 2026. Disponível em: https://ed.sunbird.org/sb-ed-releases/sunbird-ed-9.0-spark. Acesso em: 28 out. 2026.

[35] SUNBIRD RC. **Core capabilities**. Bengaluru: Centre for Open Societal Systems, 2026. Disponível em: https://rc.sunbird.org/learn/readme-1/core-capabilities. Acesso em: 28 out. 2026.

[36] SUNBIRD OBSRV. **Obsrv overview**. Bengaluru: Centre for Open Societal Systems, 2026a. Disponível em: https://obsrv.sunbird.org/core-concepts/obsrv-overview. Acesso em: 28 out. 2026.

[37] SUNBIRD OBSRV. **Data pipeline**. Bengaluru: Centre for Open Societal Systems, 2026b. Disponível em: https://obsrv.sunbird.org. Acesso em: 28 out. 2026.

[38] SUNBIRD OBSRV. **Dataset management console**. Bengaluru: Centre for Open Societal Systems, 2026c. Disponível em: https://obsrv.sunbird.org/guides/management-console-guide. Acesso em: 31 out. 2026.

[39] INSTITUTO NACIONAL DE ESTUDOS E PESQUISAS EDUCACIONAIS ANÍSIO TEIXEIRA. **Censo Escolar da Educação Básica 2025**: resultados. Brasília: Inep, 2026. Disponível em: https://www.gov.br/inep/pt-br/areas-de-atuacao/pesquisas-estatisticas-e-indicadores/censo-escolar/resultados. Acesso em: 31 out. 2026.

[40] INSTITUTO NACIONAL DE ESTUDOS E PESQUISAS EDUCACIONAIS ANÍSIO TEIXEIRA. **Censo da Educação Superior 2024**: resultados. Brasília: Inep, 2025. Disponível em: https://www.gov.br/inep/pt-br/areas-de-atuacao/pesquisas-estatisticas-e-indicadores/censo-da-educacao-superior/resultados. Acesso em: 31 out. 2026.

[41] AGÊNCIA GOV. **Startup GOV.BR, Gestão e MEC lançam plataforma nacional de dados da educação**. Brasília, 24 mar. 2026. Disponível em: https://agenciagov.ebc.com.br/noticias/202603/startup-gov-br-gestao-e-mec-lancam-plataforma-nacional-de-dados-da-educacao. Acesso em: 28 out. 2026.

[42] BRASIL. Ministério da Educação. **Portaria nº 234, de 2 de abril de 2025**. Institui o MEC Gestão Presente - Plataforma de Dados da Educação Básica. Brasília: MEC, 2025.

[43] BRASIL. **Lei Complementar nº 220, de 31 de outubro de 2025**. Institui o Sistema Nacional de Educação (SNE). Brasília: Presidência da República, 2025. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/lcp/Lcp220.htm. Acesso em: 31 out. 2026.

[44] BRASIL. Ministério da Educação. **Portaria nº 832, de 16 de dezembro de 2025**. Institui o Conjunto Mínimo de Dados da Educação Básica (CMDEB). Brasília: MEC, 2025.

[45] BRASIL. **Decreto nº 11.901, de 26 de janeiro de 2024**. Regulamenta a Lei nº 14.818, de 16 de janeiro de 2024, que institui incentivo financeiro-educacional a estudantes do ensino médio público. Brasília: Presidência da República, 2024.

[46] BRASIL. **Decreto nº 9.099, de 18 de julho de 2017**. Dispõe sobre o Programa Nacional do Livro e do Material Didático. Brasília: Presidência da República, 2017.

[47] AGÊNCIA GOV. **Ministério convida professores para avaliar livros didáticos**. Brasília, 12 ago. 2026. Disponível em: https://agenciagov.ebc.com.br/noticias/202608/ministerio-convida-professores-para-avaliar-livros-didaticos. Acesso em: 28 out. 2026.

[48] BRASIL. Ministério da Educação. **Portaria nº 554, de 11 de março de 2019**. Dispõe sobre a expedição e o registro do diploma de graduação por meio digital. Brasília: MEC, 2019.

[49] OPENID FOUNDATION. **OpenID for Verifiable Credential Issuance 1.0**. 2025. Disponível em: https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html. Acesso em: 28 out. 2026.

[50] OPENID FOUNDATION. **OpenID for Verifiable Presentations 1.0**. 2025. Disponível em: https://openid.net/sg/openid4vc/specifications/. Acesso em: 28 out. 2026.

APÊNDICE A

Cenário ilustrado: a trajetória de Luana

As páginas a seguir apresentam, na íntegra, o cenário resumido na Seção 6. Trata-se de material didático, construído sobre uma universidade fictícia e com dados de teste, destinado a comunicar a estudantes, gestores e instituições o que muda com a adoção de credenciais verificáveis. As Figuras 12 a 14 reúnem os oito quadros da narrativa, organizados em três partes.



Figura 12. Cenário ilustrado, parte 1. Da esquerda para a direita: Universidade DPI; Mais um comprovante? O problema da comprovação repetida e a solução com DPI; Receber, escolher, comprovar: o ciclo da credencial verificável.

Fonte: Elaboração própria. Cenário fictício, com dados de teste.



Figura 13. Cenário ilustrado, parte 2. Da esquerda para a direita: Onde isso pode ajudar: possíveis aplicações para as próximas etapas; Meu caminho no curso: evolução proposta com integração acadêmica; Meu histórico, mais oportunidades: um enorme potencial de possibilidades.

Fonte: Elaboração própria. Aplicações e evoluções propostas, não implementadas.



Figura 14. Cenário ilustrado, parte 3. Da esquerda para a direita: Os heróis dessa história: DPI e DPG em ação; Minha trajetória, minhas conquistas: mais acesso, mais oportunidades.

Fonte: Elaboração própria. Evolução proposta, não implementada.

Sobre os autores



André Magno Costa de Araújo NEES/UFAL
andre.araujo@nees.ufal.br

André Magno Costa de Araújo é professor da Universidade Federal de Alagoas (UFAL) e doutor em Ciência da Computação. Atualmente, exerce a função de diretor executivo do Núcleo de Excelência em Tecnologias Sociais (NEES). Sua trajetória acadêmica reúne atividades de ensino na graduação e na pós-graduação, formação de pesquisadores e uma expressiva produção científica em periódicos e em conferências internacionais. Desenvolve pesquisas nas áreas de Engenharia de Software, Governança de Dados e Infraestruturas Públicas Digitais (DPI). Possui experiência na liderança de projetos de pesquisa, desenvolvimento e inovação em larga escala e de impacto nacional, voltados à criação de soluções tecnológicas para problemas reais da sociedade. Sua atuação internacional é marcada pelo estabelecimento de parcerias com universidades e centros de pesquisa no exterior, que fortalecem a colaboração científica, o desenvolvimento de projetos conjuntos e o intercâmbio de pesquisadores.



Ana Beatriz Moreira Santos Fernandes NEES/UFAL
anabeatriz.fernandes@nees.ufal.br

Ana Beatriz Moreira Santos Fernandes é gestora de políticas públicas, bacharela em Gestão de Políticas Públicas pela Universidade de Brasília (UnB) e especialista em Gerenciamento de Projetos pela Universidade Federal Fluminense (UFF). É aluna do Public Leadership Credential, da Harvard Kennedy School. Como Gerente de Implementação de Políticas Públicas do NEES/UFAL, atua no relacionamento governamental e na articulação entre o Ministério da Educação, a universidade e as redes de ensino, coordenando ações do Programa Pé-de-Meia, com mais de 4 milhões de estudantes beneficiados, e do ecossistema MEC Gestão Presente. Participou da definição de um conjunto mínimo de dados para políticas educacionais e do debate sobre infraestrutura pública de dados na educação, e liderou mais de cem profissionais em oito coordenações.



Alisson Werner Arruda de Arruda NEES/IFPB
alisson.werner@nees.ufal.br

Alisson Werner Arruda de Arruda é doutorando em Ciência da Computação, com ênfase em Sistemas de Computação, mestre e graduado em Ciência da Computação. No NEES/UFAL, atua desde 2021 em projetos tecnológicos que apoiam políticas públicas brasileiras de grande escala, como o Programa Nacional do Livro e do Material Didático (PNLD) e o Pé-de-Meia. Além disso, é professor do Instituto Federal da Paraíba (IFPB). Sua experiência profissional dialoga com os campos da engenharia de software, da arquitetura de software, da qualidade de software e da segurança da informação.



José Vitor de Abreu Silva NEES/UFAL
vitor.abreu@nees.ufal.br

José Vitor de Abreu Silva é doutorando em Ciência da Computação pela Universidade Federal de Uberlândia (UFU), mestre em Informática e bacharel em Sistemas de Informação pela Universidade Federal de Alagoas (UFAL). Também possui especializações em Gestão de Projetos e Negócios em Tecnologia da Informação, pelo Instituto Federal do Rio de Janeiro (IFRJ), e em Gestão de Políticas Públicas Educacionais, pela UFAL. No NEES/UFAL, atua como gerente de projetos na área de políticas públicas educacionais. Além disso, é professor de cursos técnicos na área de tecnologia da informação no Senac. Suas linhas de pesquisa dialogam com os campos da interação humano-computador (IHC), da blockchain e das infraestruturas públicas digitais (DPI).



Márcio Alexandre Pereira da Silva NEES/UFAL
marcio.pereira@nees.ufal.br

Márcio Alexandre Pereira da Silva é doutor em Ciência da Computação e pesquisador de pós-doutorado na Universidade Federal de Alagoas (UFAL). Também atua como engenheiro de software em uma empresa multinacional e como professor. Seus interesses de pesquisa incluem arquitetura de software, sistemas de software autoadaptativos e padrões de projeto e de desenvolvimento de software.



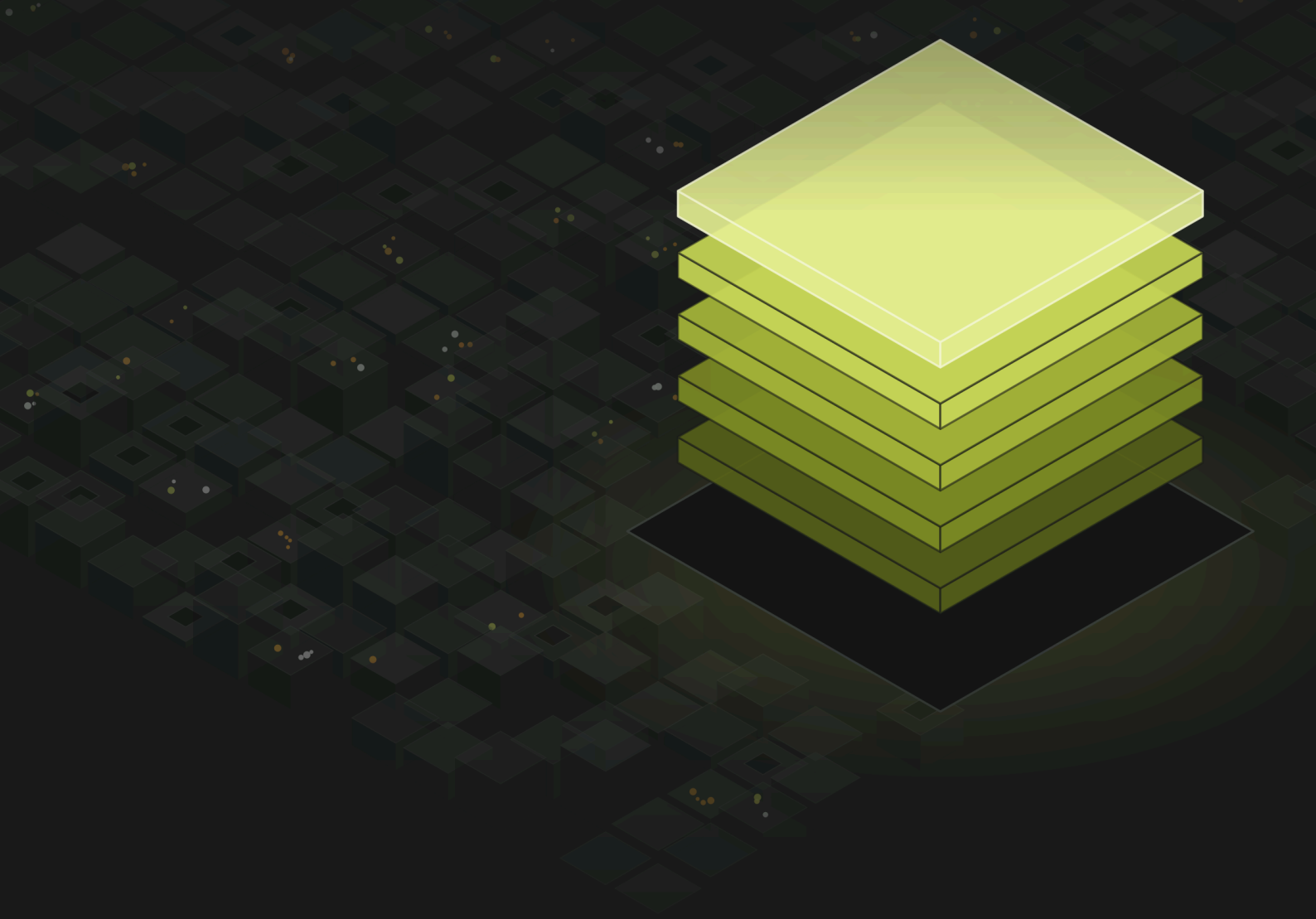
Maria Andreza Correia da Silva NEES/UFAL
maria.andreza@arapiraca.ufal.br

Maria Andreza Correia da Silva é graduada em Sistemas de Informação e mestranda em Informática pela Universidade Federal de Alagoas (UFAL), com especializações em Gerenciamento de Projetos de Tecnologia da Informação e em Segurança da Informação. Atua como analista de Governança, Risco e Compliance (GRC) em Segurança da Informação, unindo formação acadêmica e experiência prática na segurança e na governança de sistemas e dados.



Patrick Henrique da Silva Brito NEES/UFAL
patrick.brito@nees.ufal.br

Patrick Henrique da Silva Brito é Professor da Universidade Federal de Alagoas (UFAL) e pesquisador do Núcleo de Excelência em Tecnologias Sociais (NEES), onde atua em infraestruturas públicas digitais (DPI) e bens públicos digitais (DPG), com foco em arquiteturas de interoperabilidade, credenciais verificáveis e governança de dados em escala nacional. Possui mestrado e doutorado em Ciência da Computação pela Universidade Estadual de Campinas (UNICAMP). Sua pesquisa concentra-se no projeto rigoroso de arquiteturas de software para sistemas críticos e em estruturas de governança de dados, incluindo qualidade de dados, padrões de interoperabilidade e privacidade desde a concepção (*privacy by design*).



Infraestruturas Públicas Digitais e Bens Públicos Digitais

Aprendizados da experiência indiana com o ecossistema Sunbird e caminhos para que capacidades digitais compartilhadas, interoperáveis e reutilizáveis fortaleçam as políticas públicas brasileiras.

SITE dpilab.nees.ufal.br

CONTATO dpi-lab@nees.ufal.br

REALIZAÇÃO

DPI-Lab Infraestrutura Pública Digital

NEES 15 anos

Universidade Federal de Alagoas
Maceió/AL · 2026