

2º WORKSHOP DE
**credenciais
verificáveis**
2026

RELATÓRIO
EXECUTIVO-ANALÍTICO

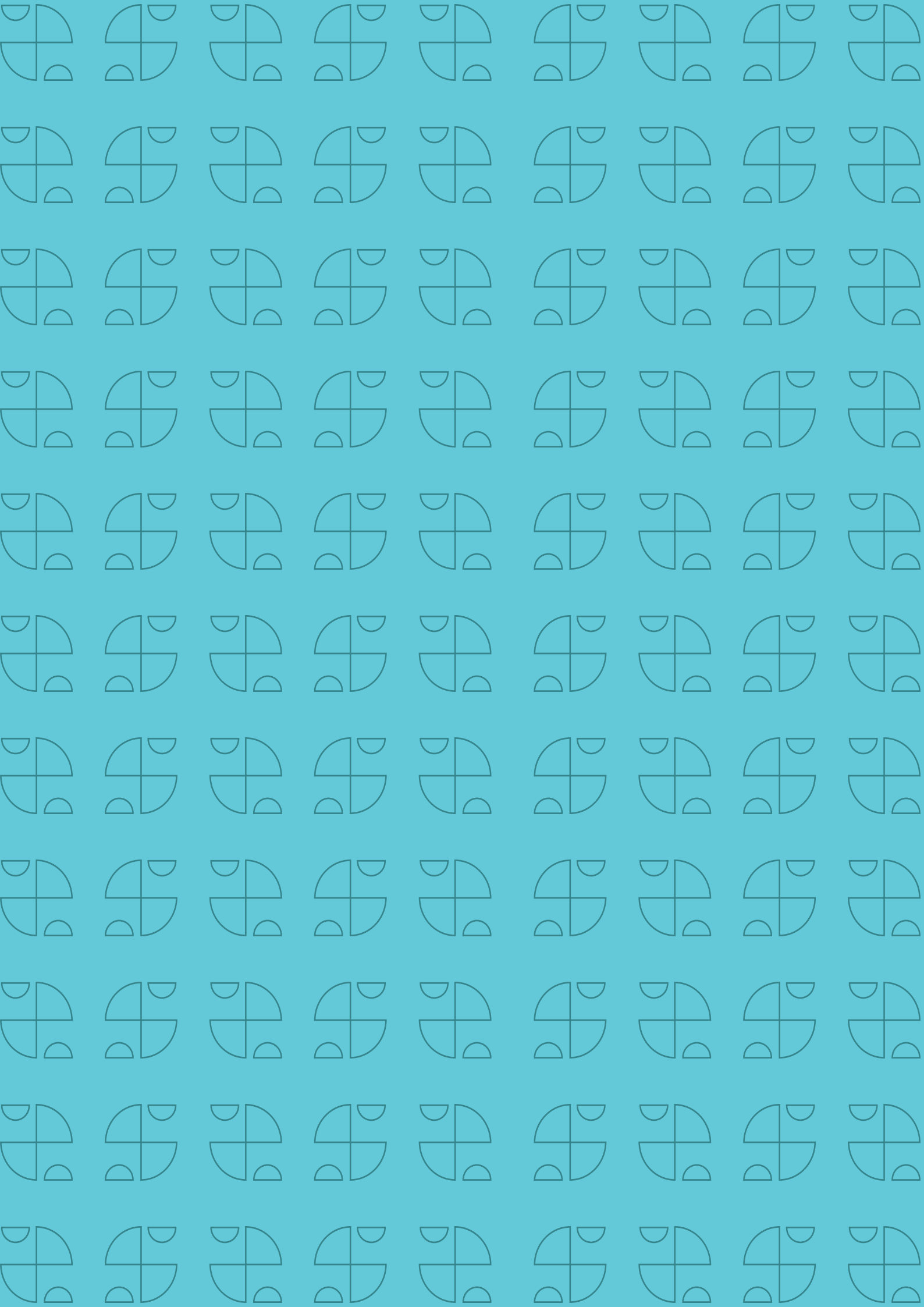
ceweb.br nic.br cgi.br



BANCO MUNDIAL
BIRD • AID | GRUPO BANCO MUNDIAL

MINISTÉRIO DA
GESTÃO E DA INOVAÇÃO
EM SERVIÇOS PÚBLICOS

GOVERNO DO
BRASIL
DO LADO DO POVO BRASILEIRO



2º WORKSHOP DE
credenciais
verificáveis
2026

RELATÓRIO
EXECUTIVO-ANALÍTICO

JUNHO 2026

ceweb.br nic.br cgi.br

CRÉDITOS

Núcleo de Informação e Coordenação do Ponto BR — NIC.br

Diretoria-Presidência

Demi Getschko

Diretoria Administrativa

Ricardo Narchi

Diretoria de Serviços e Tecnologia

Frederico Neves

Diretoria de Projetos Especiais e de Desenvolvimento

Milton Kaoru Kashiwakura

Diretoria de Assessoria às Atividades do CGI.br

Hartmut Richard Glaser

Centro de Estudos sobre Tecnologias Web — Ceweb.br

Coordenação Executiva

Vagner Diniz

Coordenação e Edição do Relatório

Beatriz Rocha, Diogo Cortiz, Henrique Xavier, Reinaldo Ferraz

Apoio à Adição – Comunicação NIC.br

Carolina Carvalho e Thiago Planchart

Projeto Gráfico e Editoração

Grappa Marketing Editorial

Agradecimentos

Este evento foi uma realização do NIC.br e contou com o apoio imprescindível do Banco Mundial e Ministério da Gestão e Inovação em Serviços Públicos na curadoria da programação e da Dataprev na cessão do auditório para as atividades.

Responsáveis pela Programação

Henrique Xavier e Beatriz Rocha – NIC.br

Cláudio Machado – Banco Mundial

Vinicius de Farias Silva – Ministério da Gestão e Inovação

SUMÁRIO

INTRODUÇÃO E ABORDAGEM METODOLÓGICA	7
1.1 Abordagem Metodológica	7
2. CONCEITOS APRESENTADOS	9
3. CASOS PRÁTICOS	10
4. POSICIONAMENTO DO BRASIL EM RELAÇÃO AOS TÓPICOS DISCUTIDOS	16
4.1 Fragmentação e Custos de Desconexão	21
4.2 Verificação Etária e Privacidade	21
4.3 Controle do Cidadão e Revogação	21
4.4 Interoperabilidade Transfronteiriça	21
4.5 Burocracia no Setor Produtivo Rural	21
4.6 Desafios Arquiteturais e Legados	22
4.7 Governança da Confiança na Educação	22
4.8 Inclusão Digital e Usabilidade	22
4.9 Riscos de Fraude e Sequestro de Contas	22
4.10 Adequação Normativa e Inovação Privada	22
5. PROVOCAÇÕES E PENSAMENTOS	23
6. TÓPICOS RELEVANTES DISCUTIDOS	24
6.1 Disputa de Arquitetura de Sistemas e Papel do Governo <i>versus</i> Setor Privado	24
6.2 Aferição e Verificação de Idade	24
6.3 Nível e Tipo de Implementação no Brasil por Padrão Tecnológico e Papel do Governo e Setor Privado	25
6.4 Perspectivas para o Desenvolvimento Técnico do Governo Diante da Situação Atual	25
6.5 Pontos de Entrada do Setor Privado	26
6.6 Atuação do Setor Privado	27
6.7 Camadas, Funções e Atores de Credenciais Verificáveis	28
7. POTENCIAIS TÓPICOS DE AGENDA FUTURA NÃO DISCUTIDOS NO WORKSHOP	29
8. CONCEITOS, ASSUNTOS E FREQUÊNCIA DE MENÇÕES	29
9. GLOSSÁRIO: LISTA DE ABREVIATURAS, SIGLAS E ACRÔNIMOS	30
APÊNDICE A: SISTEMA DE CLASSIFICAÇÃO DE CASOS PRÁTICOS APRESENTADOS SOBRE CREDENCIAIS VERIFICÁVEIS	36

1. INTRODUÇÃO E ABORDAGEM METODOLÓGICA

Este relatório tem o objetivo de sintetizar os conteúdos apresentados e discutidos durante o 2º Workshop de Credenciais Verificáveis¹, realizado entre as datas de 17 e 18 de Junho de 2026 no Auditório da DataPrev, em Brasília – Distrito Federal (Brasil). O evento insere-se em um contexto global de transformação digital, no qual cresce a necessidade de soluções seguras e interoperáveis para a comprovação automática de informações no ambiente *online*. As credenciais verificáveis (VCs) permitem que atributos como identidade, diplomas, comprovantes de renda, propriedade de imóveis, habilitação para dirigir ou registros de vacinação sejam emitidos por instituições confiáveis e apresentados digitalmente, com garantia criptográfica, preservação da privacidade e revelação seletiva de dados. Essas características contribuem para a simplificação da burocracia, o aumento da eficiência na prestação de serviços e o fortalecimento da confiança na economia digital.

No Brasil, a Lei 15.211/2025, que institui o Estatuto Digital da Criança e do Adolescente (ECA Digital), destaca-se como uma aplicação promissora dessa tecnologia ao estabelecer a necessidade de mecanismos eficazes de verificação de idade para a proteção de crianças e adolescentes no ambiente *online*. As credenciais verificáveis oferecem uma solução precisa e respeitosa à privacidade, permitindo comprovar a maioridade ou a faixa etária sem a exposição de dados pessoais desnecessários, reduzindo os riscos de vazamento de informações e promovendo maior segurança jurídica e tecnológica para plataformas digitais e seus usuários. Por outro lado, sua implementação ainda enfrenta desafios tecnológicos, como a definição de padrões interoperáveis comuns, e desafios de governança, como aqueles relacionados à confiança e adoção do público em geral.

O *workshop* abordou, de forma integrada, os fundamentos conceituais e técnicos das credenciais verificáveis, incluindo padrões internacionais e protocolos de implementação, o papel da infraestrutura pública digital e das carteiras digitais, além de aspectos de regulação, governança, experiência do usuário e inclusão digital. Também foram discutidos impactos sociais e éticos, bem como diversos casos de uso nos setores público e privado, contribuindo para ampliar o entendimento, a conscientização e a adoção das credenciais verificáveis no Brasil, fortalecendo um ecossistema digital mais seguro e eficiente.

1.1 Abordagem Metodológica

Este relatório analítico teve sua abordagem metodológica dividida em duas etapas principais: (i) transcrição, refinamento e consolidação do conteúdo do evento; e (ii) análise qualitativa da transcrição consolidada. Na primeira etapa, todo o conteúdo do evento foi transcrito e posteriormente revisado, com o objetivo de corrigir inconsistências inerentes ao processo de transcrição automática, padronizar a linguagem e consolidar as falas em um texto contínuo em terceira pessoa, preservando o conteúdo e o contexto das discussões. Na segunda etapa, foi realizada uma análise qualitativa baseada e adaptada da análise de conteúdo proposta por Bardin². Para isso, o texto foi segmentado em unidades menores de análise, permitindo uma classificação sistemática de cada unidade em três dimensões analíticas, compilados em uma Tabela nomeada de Tabela de Conceitos, Casos e Organizações:

- **Assunto ou conceito:** assunto principal ou conceito abordado na unidade de análise;
- **Caso ou exemplo:** experiências, estudos de caso, aplicações práticas ou exemplos apresentados pelos palestrantes;
- **Organização:** instituições, empresas, órgãos públicos ou demais atores e organizações mencionados na discussão.

¹ A programação completa está na página *web* <https://credenciaisdigitais.ceweb.br/>

² Metodologia das ciências sociais para estudos de conteúdo que parte de uma perspectiva quantitativa, analisando frequência de ocorrência de determinados termos, construções e referências em um dado texto. Análise de conteúdo – Wikipédia, a enciclopédia livre.

A categorização dessas unidades resultou em uma base de dados estruturada, que permitiu a aplicação de filtros temáticos e diferentes recortes analíticos. A partir dessa base, foram elaboradas tabelas sintéticas reunindo os principais conceitos, exemplos, organizações e demais informações consideradas relevantes para os objetivos deste relatório. Abaixo, dividimos e apresentamos em resumo as decisões metodológicas para criação do relatório para cada uma das seções.

Na Seção 2, foram identificados conceitos apresentados pelos participantes do *workshop*. Estes conceitos apresentados foram extraídos da Tabela de Casos Conceitos e Organizações. Definições com fundo colorido em amarelo possuem características das definições. Definições com fundo colorido em verde possuem definições completas apresentadas pelos participantes.

Na Seção 3, foram identificados os casos práticos apresentados sobre credenciais verificáveis. Estes casos foram extraídos da Tabela de Casos, Conceitos e Organizações. Foi criado um nível de maturidade para analisar superficialmente os casos de acordo com as apresentações dos participantes, apresentada no Quadro 3 – Nível de prontidão e maturidade dos casos de uso de credenciais verificáveis apresentados no *workshop*. O resultado dessa avaliação está apresentado no Quadro 4 - Casos práticos ordenados por região/país e nível de maturidade.

Na Seção 4, foram apresentados os posicionamentos do Brasil em relação aos tópicos discutidos no Workshop de Credenciais Verificáveis. O Quadro 5 elenca o posicionamento do Brasil em relação aos tópicos discutidos no *workshop*. A partir da análise de todas as contribuições apresentadas pelos participantes do *workshop*, foi possível identificar 20 desafios. A partir desses desafios, foi construída uma análise baseada em eixos, descrevendo quais os Desafio Específicos identificados, quais Propostas foram identificadas, quais Casos e Exemplos foram dados, e quais Pontos a Aprofundar foram apresentados, em um formato que não levou em consideração a frequência de menções sobre os assuntos e dimensões, mas a simples menção já bastou para ser considerada.

Na Seção 5, foi apresentada uma lista de Provocações e Pensamentos a partir dos materiais das seções acima descritas. Esta seção possui uma metodologia inspirada nos podcasts e textos do Prof. Galloway³. Desta forma, o Quadro 6 apresenta propostas de provocações e pensamentos sobre os temas e assuntos apresentados no Workshop que não tiveram propostas concretas para sua resolução. Esta seção auxilia na construção de pensamento crítico para tomada de decisões e conciliação de agenda dos atores e organizações envolvidas neste ecossistema de Credenciais Verificáveis.

Na Seção 6, foram apresentados Tópicos relevantes discutidos nos dois dias de *workshop*, em especial, no Quadro 9 sobre as camadas, funções e atores do ecossistema de credenciais verificáveis. Este Quadro 9 nos dá a dimensão de quais formatos, padrões, organizações estão trabalhando em quais camadas e oferecendo quais funções para o ecossistema de Credenciais Verificáveis. Este Quadro 9 também dá a oportunidade de estabelecer conversas para avançar em uma agenda de interesse comum entre os atores, e identificar consensos e dissensos, bem como os pontos a aprofundar para a boa governança de Credenciais Verificáveis.

Na Seção 7, foram identificadas propostas de uma agenda futura para o ecossistema de credenciais verificáveis. O Quadro 10 - Tópicos omissos do *workshop*, impacto e justificativas de apresentação de 20 propostas de tópicos a serem discutidos em Agenda Futura. Estes tópicos foram identificados através de uma análise de oportunidades, após *brainstorming* de especialistas no assunto. Esta agenda foi dividida em três eixos: 1- Governança, Regulação e Jurídica; 2- Técnica, Infraestrutura e Semântica; e, 3- Impacto Socioeconômico e Inclusão.

Na Seção 8, foram apresentadas as frequências dos conceitos e assuntos apresentados pelos participantes do Workshop de Credenciais Verificáveis. O Quadro 11 extraiu da Tabela de Casos, Conceitos e Organizações uma lista de 20 tópicos mais discutidos, sendo os cinco com maior frequência na ordem a seguir: 1- Verificação e Aferição etária (219); 2- Credenciais verificáveis (181); 3- Interoperabilidade (107); 4- Identidade digital (91); 5- Governança e estruturas de confiança (88). Estas e outras frequências nos dão outras pistas sobre quais assuntos discutir em agendas posteriores a este *workshop*.

³ <https://www.profgalloway.com/>

2. CONCEITOS APRESENTADOS

Para nivelar o debate e padronizar termos importantes que foram discutidos durante o evento, apresenta-se aqui os conceitos “Credenciais Verificáveis” e “Credencial Fundacional e Derivada”, a partir das perspectivas dos participantes. Os quadros 1 e 2 apresentam os conceitos, as definições e referências encontradas. A ordem de apresentação dos conceitos não representa ordem de relevância.

QUADRO 1

Definições Encontradas para “Credenciais Verificáveis”

#	Palestrante	Trecho de Menção da Definição ou de Elementos que Caracterizem a Definição do Objeto	Link YouTube
01	Yolanda Martínez	Intercâmbio seguro de dados entre cidadãos, instituições e países.	https://www.youtube.com/live/mB519auQuOY?si=L4VFtLrDBuCIWcAn&t=828
02	Esther Dweck	Elemento estratégico da infraestrutura pública digital por permitir a comprovação segura de direitos, atributos e autorizações emitidos por fontes confiáveis. Como exemplo da evolução desse modelo, mencionou a assinatura eletrônica do gov.br	https://www.youtube.com/live/mB519auQuOY?si=GmBBYnsKR226JLGJ&t=2548
03	Henrique Xavier	Credencial como um documento emitido por uma instituição ou indivíduo para atestar informações sobre uma entidade, ressaltando que toda credencial deve identificar claramente seu emissor. É uma prova criptográfica que irá garantir a integridade e autenticidade, sem necessidade de representação visual obrigatória.	https://www.youtube.com/live/mB519auQuOY?si=eAtAQjPeQp4jvKg5&t=3275
04	Luciano Charlita de Freitas	Credenciais são componentes essenciais para ampliar a segurança, a confiabilidade e a interoperabilidade dos serviços digitais, além de favorecer a integração entre ecossistemas digitais de diferentes países.	https://www.youtube.com/live/mB519auQuOY?si=aIM2TcnJOBQtp_Et&t=5582
05	Luana Roncaratti	Credenciais verificáveis como documentos digitais emitidos com base em padrões tecnológicos e criptográficos que asseguram maior segurança, incluindo garantias de integridade, autenticidade, confidencialidade e disponibilidade das informações. Esse modelo permite ao titular comprovar atributos pessoais de forma seletiva, sem a necessidade de compartilhar um volume excessivo de dados, o que tende a aumentar a confiança nas transações digitais.	https://www.youtube.com/live/mB519auQuOY?si=etRi-bnQBZv0_4Gd&t=7575
06	Isaac Montilla	A mesma carteira poderá ser utilizada em diferentes instituições, cabendo à própria empresa decidir quais informações deseja compartilhar e em que momento. Essa abordagem reduz a burocracia e os custos operacionais, fortalece a relação de confiança entre o Estado e o setor empresarial e representa um importante avanço na utilização nacional de credenciais verificáveis e no gerenciamento seguro de dados.	https://www.youtube.com/live/LZ_QmiP0G84?t=1517s
07	Jean Martina	A evolução [de credenciais verificáveis] depende de três elementos principais: legitimidade institucional, interoperabilidade real e governança clara.	https://www.youtube.com/live/LZ_QmiP0G84?si=AMKUndE1r23fYv09&t=10555
08	Marcelo Queiroz	O ecossistema [de credenciais verificáveis] envolve três elementos: emissores, responsáveis pela criação e disponibilização das credenciais; verificadores, que utilizam essas informações para validar identidades ou atributos; e a própria credibilidade dos participantes envolvidos, fator essencial para o funcionamento do modelo.	https://www.youtube.com/live/LZ_QmiP0G84?si=3n7uzpJZGwuxE_5c&t=11094
09	Marcelo Queiroz	[Elementos da] operacionalização de soluções baseadas em credenciais verificáveis, tanto no setor público quanto no privado: 1- Canais e jornada do usuário 2- Relação de confiança e autenticação 3- Governança do ecossistema.	https://www.youtube.com/live/LZ_QmiP0G84?si=3n7uzpJZGwuxE_5c&t=11094

QUADRO 2

Credenciais Fundacionais e Credenciais Derivadas

#	Palestrante	Trecho de Menção	Link Youtube
01	Germana Gladys	A arquitetura prevê a emissão de uma credencial fundacional, baseada em dados governamentais, denominada credencial gov.br, que servirá como base para a emissão de outras credenciais derivadas destinadas a diferentes aplicações.	https://www.youtube.com/live/Mlx9k2NM6ng?si=LXZn18Ebk0Ui3GYH&t=6235
02	Guilherme Funchal	Explicou que o processo começa com a emissão de uma credencial fundacional, vinculada inicialmente ao Cadastro de Pessoas Físicas (CPF) do cidadão, que serve como base para a emissão de outras credenciais derivadas. Em seguida, ocorre uma segunda etapa em que é solicitada uma prova da credencial fundacional para possibilitar a emissão de uma nova credencial, sendo ambas armazenadas na carteira digital do usuário.	https://www.youtube.com/live/Mlx9k2NM6ng?si=8cJQ2_TD-7L9GGn7&t=6749

3. CASOS PRÁTICOS

Durante o evento foram citados diversos casos práticos relacionados à credenciais verificáveis. O quadro 3 apresenta estes casos e os classifica pelo nível de maturidade. O apêndice A, ao final do documento, apresenta o sistema utilizado para classificação.

QUADRO 3

Casos Práticos Ordenados por Região/País e Nível de Maturidade

Caso Prático	País	Palestrante	Contexto	Nível de Maturidade
BRASIL				
Confiança Delegada na Educação	Brasil	Pierre-Antoine Champin	Cadeia de confiança onde o Ministério da Educação (MEC) atesta a universidade que, por sua vez, emite o diploma validável.	Maduro
Digitalização e Rastreabilidade de Diplomas	Brasil	Jean Martina	Consolidação dos diplomas digitais e construção da Rede de Rastreabilidade com Dataprev/MEC.	Maduro
Diploma Digital	Brasil	Henrique Xavier	Emissão de diplomas universitários em formato digital assinado por instituições de ensino superior.	Maduro
Documentos de Veículos	Brasil	Henrique Xavier	Digitalização e emissão de Certificado de Registro e Licenciamento de Veículo (CRLV) / Certificado de Registro de Veículo (CRV) em carteiras digitais de trânsito.	Maduro
Passaporte	Brasil	Henrique Xavier	Passaporte eletrônico e emissão de atestados digitais associados à identificação civil internacional.	Maduro
Aferição de Idade e Decreto 2.880/2026	Brasil	Marcos Moreira	Regulamentação do Ministério da Gestão e da Inovação em Serviços Públicos (MGI) para disponibilizar soluções públicas de verificação etária sem identificação.	Intermediário
Códigos de Barras para Credenciais Verificáveis	Brasil	Pierre-Antoine Champin	Codificação de VCs em QR Codes para leitura <i>offline</i> em cartões físicos ou <i>smartphones</i> .	Intermediário

► CONTINUA

Caso Prático	País	Palestrante	Contexto	Nível de Maturidade
Comprovação de Maioridade (ECA Digital / Agência Nacional de Proteção de Dados (ANPD))	Brasil	Miriam Wimmer / Victor Fernandes	Diretrizes e orientações regulatórias para aplicação de VCs em cumprimento às obrigações do ECA.	Intermediário
Confirmação de Faixa Etária sem Exposição de Dados Pessoais (ZKP)	Brasil	Beatriz Vasconcellos	Uso de Zero-Knowledge Proofs (ZKP) para respostas binárias (sim/não) para idade no contexto do ECA Digital.	Intermediário
Credenciais Verificáveis como Métodos de Aferição de Idade	Brasil	Henrique Xavier	Uso do recurso de revelação seletiva para atestar maioridade em transações <i>online</i> .	Intermediário
Divulgação Seletiva da Data de Nascimento	Brasil	Rafael Zanatta	Uso de Age Tokens para validar maioridade em serviços digitais preservando a data de nascimento.	Intermediário
Age Token no Gov.br	Brasil	Sanchi Singh	Emissão de <i>token</i> de idade derivado da conta Gov.br, identidade digital do cidadão brasileiro, para comprovação de elegibilidade.	Intermediário
Anoncreds no Gov.br	Brasil	Guilherme Funchal	Uso do protocolo AnonCreds para minimização de dados e preservação da privacidade.	Intermediário
Bitstring Status List - Revogação de Carteira Nacional de Habilitação (CNH) Cassada	Brasil	Pierre-Antoine Champin	Implementação do padrão do World Wide Web Consortium (W3C) para consulta instantânea de <i>status</i> de revogação de documentos.	Intermediário
Crédito para Trator Usando VCs no Banco do Brasil	Brasil	Anand Varada	Aplicação prática onde a apresentação de VCs acelerou o financiamento de maquinário agrícola.	Intermediário
Crédito Rural	Brasil	Beatriz Vasconcellos	Simplificação da análise cadastral para acesso a financiamento agrícola usando VCs.	Intermediário
Documentos de Identidade com Atributos Seleccionáveis	Brasil	Beatriz Vasconcellos	Modelo de compartilhamento parcial de campos da credencial dependendo do destinatário.	Intermediário
Financiamento de Jovens Agricultoras	Brasil	Carlos Guedes	Prova de conceito bem-sucedida de aprovação de crédito rural reduzindo burocracia com VCs.	Intermediário
Formatos <i>OpenID for Verifiable Credential Issuance</i> (OpenID4VCI), <i>OpenID for Verifiable Presentations</i> (OID4VP), ISO/IEC 18013-5 (mDoc) no Gov.br	Brasil	Fred Guth	Padronização arquitetural da carteira Gov.br para interoperabilidade técnica internacional.	Intermediário
Gov.br com Android, iOS, W3C, OID4VC e DIDComm	Brasil	Guilherme Funchal	Estruturação de carteira nativa no aplicativo Gov.br com armazenamento local e privado.	Intermediário

► CONTINUA

Caso Prático	País	Palestrante	Contexto	Nível de Maturidade
Gov.br em Rede Besu e QR Code	Brasil	Guilherme Funchal	Infraestrutura de emissão em <i>blockchain</i> Hyperledger Besu com suporte a validação <i>offline</i> .	Intermediário
<i>High Assurance Interoperability Profile</i> (HAIP)	Brasil	Joseph Heenan	Perfil de alta garantia e segurança para emissão de documentos críticos como Carteira Nacional de Habilitação (CNH) e Passaporte.	Intermediário
ID Pass	Brasil	Felipe Kenji Nishimura	Emissão de credencial digital pela Google baseada na leitura do <i>chip</i> NFC (Near Field Communication ou Comunicação por Campo de Proximidade) do ePassport.	Intermediário
Implementação Inji/ Modular Open Source Identity Platform	Brasil	Fred Guth / Sanchi Singh	Adoção da plataforma <i>open-source</i> Inji para o ecossistema brasileiro de verificação de idade.	Intermediário
(MOSIP) para Aferição de Idade	Brasil	Fred Guth / Sanchi Singh	Adoção da plataforma <i>open-source</i> Inji para o ecossistema brasileiro de verificação de idade.	Intermediário
Informação de Renda para Benefícios Sociais	Brasil	Beatriz Vasconcellos	Atributo de renda validado para concessão e elegibilidade em programas sociais governamentais.	Intermediário
Integração Gov.br e Carteiras digitais Serviço Federal de Processamento de Dados (SERPRO) / Centro de Pesquisa e Desenvolvimento em Telecomunicações (CPQD)	Brasil	Germana Gladys	Integração do módulo de verificação etária às soluções de carteira digital do governo.	Intermediário
Meu Imóvel Rural	Brasil	Luanna Roncaratti	Aplicativo e infraestrutura pública digital para integração de dados fundiários e acesso a crédito.	Intermediário
<i>OpenID Federation</i> para Credenciais Acadêmicas (Rede Nacional de Ensino e Pesquisa (RNP) / MEC)	Brasil	Emerson Ribeiro de Mello	Transição da infraestrutura acadêmica de <i>Security Assertion Markup Language</i> (SAML) para <i>OpenID Federation</i> com MEC como âncora.	Intermediário
Piloto de Crédito Rural com 100 Famílias (RS)	Brasil	Carlos Guedes	Projeto no Vale do Taquari aplicando VCs para crédito pós-enchentes. Desenvolvido por Ministério do Desenvolvimento Agrário e Agricultura Familiar (MDA), Agência Nacional de Assistência Técnica e Extensão Rural (ANATER), Empresa de Assistência Técnica e Extensão Rural (EMATER), Banco do Brasil (BB).	Intermediário
Plataforma Serasa / Bradesco IDEbra	Brasil	Andreza Lona	Soluções construídas em parceria com o CPQD transacionando milhares de credenciais no setor bancário.	Intermediário
Procura de emprego Utilizando Diplomas Verificáveis	Brasil	Beatriz Vasconcellos	Apresentação de credenciais educacionais diretamente a empregadores no mercado de trabalho.	Intermediário
Projeto Aries Bifold e Flutter (SERPRO/ CPQD)	Brasil	Guilherme Funchal	Adaptação de <i>frameworks</i> abertos de identidade soberana para o aplicativo <i>mobile</i> do Gov.br.	Intermediário

► CONTINUA

Caso Prático	País	Palestrante	Contexto	Nível de Maturidade
Credenciais Verificáveis para Concessão de Crédito Rural (CAR)	Brasil	Esther Dweck	Projeto piloto que integra o Cadastro Ambiental Rural (CAR) e bases fundiárias para emissão de VC para concessão de crédito a produtores rurais.	Intermediário
Distinção: Documentos Eletrônicos <i>versus</i> Credenciais Verificáveis	Brasil	Jean Martina	Modelo arquitetural que trata a VC como representação temporária emitida a partir da base oficial.	Intermediário
QRCode Android e Carteira Digital	Brasil	Joseph Heenan	Fluxos de teste e certificação de carteiras digitais em sistemas operacionais móveis.	Intermediário
Serasa Pass e Controle Parental	Brasil	Marcelo Queiroz	Solução de mercado derivada do Serasa Pass para suporte ao cumprimento do ECA Digital.	Intermediário
Validação de Documentos por Agentes Financeiros	Brasil	Luanna Roncaratti	Verificação direta de VCs por bancos para concessão de serviços e produtos financeiros.	Intermediário
Verificação de Idade em Ambientes Digitais	Brasil	Esther Dweck	Mecanismo governamental para comprovação de faixa etária sem exposição de dados pessoais adicionais.	Intermediário
Verificação Etária para Atendimento ao ECA Digital	Brasil	Luanna Roncaratti	Adaptação regulatória e técnica do ecossistema nacional para atendimento às exigências do ECA Digital.	Intermediário
Credenciais para Uso de Energia Solar	Brasil	Beatriz Vasconcellos	Certificação de geração e uso de energia fotovoltaica para transações entre mercados.	Inicial
Alvarás de Funcionamento	Brasil	Henrique Xavier	Emissão de licenças e alvarás operacionais em formato de credenciais digitais por órgãos municipais/estaduais.	Inicial
App Serasa, Tokenização de Cartões e VCs	Brasil	Marcelo Queiroz	Carteira de dados permitindo emissão de VCs cadastrais e financeiras no <i>app</i> Serasa.	Inicial
Certificados de Registro de Programas de Computador	Brasil	Henrique Xavier	Emissão de ativos e registros de propriedade intelectual pelo Instituto Nacional da Propriedade Industrial (INPI) na forma de credencial.	Inicial
Combate a <i>deepfakes</i> e Desinformação	Brasil	Beatriz Vasconcellos	Uso de VCs para certificar autoria, procedência e integridade de mídias e conteúdos digitais.	Inicial
Comprovação de Idade na Indústria de Jogos / Loot boxes	Brasil	Victor Fernandes	Mecanismo de verificação etária acionado pontualmente em etapas de compra dentro de <i>games</i> .	Inicial
Credenciais Multipropósito no Setor Público	Brasil	Andreza Lona	Proposta de emissão de VCs baseadas na base de 95 milhões de pessoas do Cadastro Único (CadÚnico).	Inicial
IA Agêntica – Agentes de Inteligência Artificial	Brasil	Beatriz Vasconcellos	Atribuição de credenciais e permissões para que robôs realizem transações em nome de usuários.	Inicial
Projeto Drex e Identidade Digital	Brasil	Marcelo Queiroz	Incorporação de VCs como camada de confiança e identidade no projeto de moeda digital do Banco Central do Brasil (Bacen).	Inicial

► CONTINUA

Caso Prático	País	Palestrante	Contexto	Nível de Maturidade
VC para Lei de Improbidade Administrativa	Brasil	Andreza Lona	Validação automatizada e privada da declaração de imposto de renda de servidores públicos via VCs.	Inicial
WhatsApp e Credenciais Verificáveis	Brasil	Marcelo Queiroz	Integração de fluxos de apresentação de credenciais diretamente na interface do WhatsApp.	Inicial
AMÉRICA LATINA				
Carteiras de Motorista Verificáveis	Argentina	Beatriz Vasconcellos	Emissão da habilitação de trânsito em formato de credencial digital interoperável.	Maduro
Abertura de Contas Bancárias com Carteira Digital Empresarial	República Dominicana	Isaac Montilla	Redução do tempo de validação de documentos de empresas de 30 dias para imediato usando VCs.	Intermediário
Adoção de Credenciais Digitais na Cidade Do México	México	Yolanda Martínez	Implementação municipal de credenciais com foco em desafios de interoperabilidade nacional.	Intermediário
Autenticar 2.0 na Argentina	Argentina	Sandra Negre / Julián Belistri	Evolução da plataforma nacional para emissão de VCs armazenadas em carteiras digitais.	Intermediário
Carteira Eletrônica Nacional	Honduras	Elmer Ferrera Padilla	Plataforma nacional para armazenamento de credenciais civis e eliminação do papel.	Intermediário
Consórcio Latino-Americano para Reconhecimento de Vcs	América Latina	Yolanda Martínez	Parceria transfronteiriça (+12 países, Banco Interamericano de Desenvolvimento (BID)/Banco Mundial) para validação mútua de credenciais.	Intermediário
Expansão do Diploma Digital Brasileiro no Mercosul	América Latina	Jean Martina	Adoção do padrão brasileiro de diploma digital pelo Uruguai e Paraguai.	Intermediário
Identidade Digital Transfronteiriça (Brasil/Uruguai)	América Latina	Germana Gladys	Mecanismo que permite aos cidadãos brasileiros acessar +300 serviços no Uruguai via Gov.br.	Intermediário
Prontuário Médico Transfronteiriço	Honduras	Ysaías Alvarez Castillo	Projeto de interoperabilidade de dados de saúde e histórico médico entre países da região.	Inicial
UNIÃO EUROPEIA				
Carteira Digital da União Europeia (EUDI Wallet)	União Europeia	Beatriz Vasconcellos / Joseph Heenan	Quadro regulatório (eIDAS 2) e arquitetura HAIP/OID4VC obrigatória para os 27 membros.	Maduro
Carteiras Digitais Governamentais (França, Alemanha e Finlândia)	União Europeia	Omer Shafiq	Carteiras digitais soberanas já em operação diária na França, Alemanha e Finlândia.	Maduro

► CONCLUSÃO

Caso Prático	País	Palestrante	Contexto	Nível de Maturidade
EUDI Wallet - Carteiras de Habilitação Digital	União Europeia	Joseph Heenan	Padronização e emissão da CNH em formato ISO mDoc dentro da carteira europeia.	Maduro
Carteira Digital de Médicos	União Europeia	Fernando Moreira	Credencial de atributo profissional permitindo a médicos atuar transfronteiramente na União Europeia (UE).	Intermediário
Modelos de Análise de Ameaças para Verificação Etária	União Europeia	Rafael Zanatta	Threat models publicados pela Comissão Europeia e Agencia Española de Protección de Datos (AEPD) para auditoria de VCs de idade.	Intermediário
Princípio “once-only” e VCs (Projeto TOOP)	União Europeia	Beatriz Vasconcellos	Aplicação de VCs para garantir que o cidadão preste informações ao governo apenas uma vez. https://ec.europa.eu/isa2/isa2conf8/once-only-principle-project-toop_en/	Intermediário
Reconhecimento Mútuo de Documentos Digitais (Brasil-UE)	União Europeia	Enylson Camolesi	Negociações e acordos internacionais de interoperabilidade técnica de VCs entre Brasil e UE.	Inicial
OUTRAS REGIÕES DO MUNDO / CENÁRIO INTERNACIONAL				
Aadhaar e Google Wallet	Índia	Felipe Kenji Nishimura	Integração do sistema de identificação civil indiano na carteira digital do Google.	Maduro
DigiLocker	Índia	Beatriz Vasconcellos	Ecossistema nacional massivo da Índia para emissão e armazenamento de documentos digitais.	Maduro
Ecossistema Inji / MOSIP	Mundo / África / Ásia	Sanchi Singh	Plataforma <i>open-source</i> adotada em +20 países para emissão de VCs de saúde e identidade.	Maduro
Open Badges	Mundo	Sanchi Singh	Padrão global consolidado para emissão e verificação de distintivos e conquistas educacionais.	Maduro
TSA e Google Wallet	Estados Unidos	Felipe Kenji Nishimura	Aceite do ID Pass (VC de passaporte) nos portões de embarque de aeroportos dos EUA.	Maduro
<i>Age Assurance Trial</i>	Austrália	Rafael Zanatta / Enya Costa	Programa governamental australiano de testes de tecnologias de verificação etária via VCs.	Intermediário
Bilhetes de Transporte Ferroviário	Japão	Joseph Heenan	Implementação do protocolo OID4VC para emissão de bilhetes de trem no Japão.	Intermediário
Global Digital Collaboration	Suíça	Ruth Puente	Iniciativa governamental suíça com a OpenWallet Foundation para testes globais de VCs.	Intermediário
Projeto Credencial Verificável	Benin	Cláudio Machado	Modernização da identidade nacional do Benin incorporando padrões W3C de VCs.	Intermediário
Registro Civil e VCs	Indonésia	Cláudio Machado	Projeto financiado pelo Banco Mundial emitindo VCs desde a certidão de nascimento.	Intermediário
Identidade Digital para Agentes de IA	Estônia	Fabro Steibel	Criação do “CPF do Robô” para identificação oficial de agentes autônomos na rede estatal.	Inicial

4. POSICIONAMENTO DO BRASIL EM RELAÇÃO AOS TÓPICOS DISCUTIDOS

O Quadro 4 elenca o posicionamento do Brasil em relação aos tópicos discutidos no *workshop*, que são detalhados na sequência.

QUADRO 4

Posicionamento do Brasil em Relação aos Tópicos Discutidos no *Workshop*

#	Assunto / Tema	Desafio Específico	Propostas	Casos e Exemplos	Pontos a Aprofundar
1	Fragmentação e Custos de Desconexão	Sistemas públicos e privados atuam em silos (bancos, órgãos governamentais, cartórios, hospitais e universidades).	Infraestruturas Públicas Digitais (IPDs) Criação de uma camada pública de confiança para integrar serviços sem centralizar dados.	- O Pix como infraestrutura pública digital que unificou o sistema financeiro. - A Plataforma Conecta integrando dados entre órgãos federais.	- Definição de âncoras de confiança (<i>trust anchors</i>) nacionais. - Modelo de participação de atores privados sem captura proprietária.
2		Custo elevado com redundância de dados e fraudes com documentos físicos/falsificados.	Identidade Digital Única e Infraestrutura de Chaves Públicas (ICP) Uso de chaves públicas consolidadas e identificador único civil.	- Consolidação do CPF como identificador único no gov.br. - O e-Notariado mantido pelos cartórios para assinaturas e atos notariais.	- Garantia de interoperabilidade técnica e semântica entre diferentes órgãos. - Redução do uso e do custo operacional do papel.
3	Verificação Etária e Privacidade	Cumprir exigências legais de proteção a crianças e adolescentes sem forçar o envio de documentos com foto/biometria a plataformas terceiras.	Age Tokens (Minimização por Design) Emissão de atestados etários temporários e restritos que respondem apenas "sim" ou "não" (ZKP).	- Regulamentação do ECA Digital pelo Decreto nº 2.880/2026 atribuindo soluções ao MGI. - Implementação piloto com a plataforma <i>open-source</i> Inji/MOSIP via gov.br.	- Publicação do guia regulatório e acreditação pela ANPD de entidades certificadoras independentes. - Garantia de acessibilidade para as pessoas com deficiência no Brasil.
4		Alto risco de vigilância, perfilamento excessivo e burla etária por menores em dispositivos dos pais.	Modelo de Dupla Camada Aferição na loja de <i>apps</i> /OS e verificação estrita pontual apenas no acesso a conteúdos restritos.	- Mapeamento de uso em <i>loot boxes</i> na indústria de jogos pela Secretaria Nacional de Direitos Digitais. - Pesquisas do Cetic.br sobre métodos de burla por menores.	- Proibição e fiscalização do uso de dados de checagem etária para perfilamento comercial. - Definição de responsabilidade solidária entre os agentes da cadeia digital.

CONTINUA ►

► CONTINUA

#	Assunto / Tema	Desafio Específico	Propostas	Casos e Exemplos	Pontos a Aprofundar
5	Controle do Cidadão e Revogação	No formato atual de imagens/PDFs, o cidadão entrega todos os seus dados sem controle de destinação.	Divulgação Seletiva (Selective Disclosure) Compartilhamento parcial de campos da credencial (<i>AnonCreds</i> e <i>Selective Disclosure</i> for JSON Web Tokens, <i>SD-JWT</i>) com armazenamento local.	- Carteira Digital gov.br (+180M de contas) com armazenamento seguro local no aplicativo móvel. - Desenvolvimento via SERPRO/CPQD utilizando a rede <i>blockchain Hyperledger Besu</i> .	▪ Transição gradual para o modelo de "governo agêntico" com IAs operando em nome dos cidadãos. ▪ Uso de VCs para certificação de autoria e combate a <i>deepfakes</i>.
6	Controle do Cidadão e Revogação	Falta de mecanismos eficientes para checagem imediata de documentos suspensos ou revogados.	Listas Dinâmicas de Revogação Uso da especificação <i>Bitstring Status List</i> para consulta instantânea sem rastrear a navegação.	- Consulta de revogação imediata de CNHs cassadas ou suspensas. - Verificação de <i>status</i> em tempo real por agentes financeiros e de trânsito.	▪ Escalonamento de consultas de <i>status</i> em larga escala mantendo o desempenho da carteira. ▪ Preservação da privacidade do cidadão durante a verificação do <i>status</i>.
7	Interoperabilidade Transfronteiriça	Dificuldade de validação de documentos civis e acadêmicos brasileiros em outros países da região sem burocracia consular.	Acordos Multilaterais e Reconhecimento Mútuo Uso de padrões abertos (W3C VC) e tradução técnica entre plataformas estatais de identidade.	- Consórcio Latino-Americano de Credenciais Digitais liderado por Brasil e Uruguai. - Acesso de cidadãos brasileiros a +300 serviços públicos do Uruguai via gov.br .	▪ Reconhecimento mútuo de credenciais acadêmicas e profissionais (médicos/engenheiros) no Mercosul. ▪ Acordos de interoperabilidade em negociação entre o Brasil e a União Europeia.
8		Incompatibilidade de formatos e padrões de dados entre diferentes blocos econômicos e países.	Adoção de Perfis Globais (HAIP) Implementação de perfis de alta garantia e padrões internacionais (OID4VC/mDoc).	- Expansão do padrão do Diploma Digital brasileiro para adoção no Uruguai e Paraguai. - Harmonização de carteiras digitais civis com os padrões eIDAS 2 da União Europeia.	▪ Alinhamento contínuo das especificações nacionais aos fóruns globais de padronização (W3C, <i>OpenID Foundation</i> (OIDF), <i>Internet Engineering Task Force</i> (IETF)). ▪ Manutenção da soberania sobre os dados e regras de negócio nacionais.

► CONTINUA

#	Assunto / Tema	Desafio Específico	Propostas	Casos e Exemplos	Pontos a Aprofundar
9	Burocracia no Setor Produtivo Rural	Jornada convencional de acesso ao crédito rural longa e burocrática (média de 73 dias para validação).	Automação de Atributos Fundiários Emissão automatizada de VCs baseadas nas bases do CAR, CNIR e CAF para comprovação em bancos.	- Aplicativo Meu Imóvel Rural (Dataprev/MGI) para integração de dados fundiários. - Piloto de concessão de crédito rural no Vale do Taquari (RS) com 100 famílias (MDA, ANATER, EMATER, Banco do Brasil).	- Engajamento e adesão nativa das cooperativas de crédito e bancos privados ao fluxo de VCs. - Simplificação das exigências bancárias por meio de atestados de conformidade digital.
10		Dificuldade do pequeno produtor e agricultor familiar em reunir e apresentar comprovantes pulverizados.	Credencial Única do Produtor Consolidação de atributos socioeconômicos e ambientais em um único ecossistema digital.	- Concessão de crédito para financiamento de tratores no Banco do Brasil via VCs do CAR. - Uso do Cadastro Nacional da Agricultura Familiar (CAF) como emissor de atributos.	- Ampliação do alcance do crédito consciente e redução do tempo da jornada do produtor. - Inclusão de pequenos agricultores com menor letramento digital.
11	Desafios Arquiteturais e Legados	<i>Frameworks</i> abertos legados (ex: Hyperledger Indy) eram incompatíveis com a arquitetura do <i>app gov.br</i> (Flutter) e redes Ethereum.	Agentes Nativos Besu Construção de agentes nativos em Kotlin e Swift para redes Hyperledger Besu em dispositivos móveis.	- Desenvolvimento pelo SERPRO/CPQD de agentes móveis compatíveis com Besu para iOS e Android no gov.br . - Alinhamento tecnológico com a infraestrutura do Drex (Banco Central).	- Sustentabilidade técnica e manutenção continuada dos componentes <i>open-source</i> pelo ecossistema nacional. - Interoperabilidade entre redes <i>blockchain</i> (Besu) e modelos sem <i>blockchain</i> (Web DIDs).
12		Dependência de redes e protocolos de federação acadêmica antigos e legados (SAML).	Migração para OpenID Federation Transição de federações acadêmicas e governamentais para a família de protocolos OpenID (<i>OID4VC</i>).	- Projeto de migração da rede acadêmica da Rede Nacional de Ensino e Pesquisa (RNP) e do MEC do SAML para OpenID Federation .	- Atualização do parque tecnológico das universidades públicas sem interromper serviços ativos. - Estabelecimento de novas redes de confiança dinâmicas para a educação.

► CONTINUA

#	Assunto / Tema	Desafio Específico	Propostas	Casos e Exemplos	Pontos a Aprofundar
13	Governança da Confiança na Educação	Dificuldade de um empregador em verificar se uma faculdade remota tinha autorização oficial para emitir determinado diploma.	Confiança Delegada (Trust Registries) Estruturação de uma cadeia onde o Ministério da Educação atua como âncora principal (<i>Trust Anchor</i>).	- Projeto da Rede de Rastreabilidade da Educação Superior desenvolvido pelo MEC em parceria com a Dataprev . - Modelo onde o MEC emite <i>Trust Marks</i> atestando a autoridade de emissão das universidades.	- Validação e persistência de longo prazo para diplomas caso a instituição de ensino seja extinta. - Distinção clara entre o documento eletrônico permanente e a VC temporária emitida sob demanda.
14		Risco de falsificação e venda de diplomas acadêmicos no mercado de trabalho.	Rastreabilidade e Validação Criptográfica Emissão obrigatoriamente assinada criptograficamente na origem da base de dados.	- Obrigatoriedade do Diploma Digital regulamentado pelo MEC em todas as instituições de ensino superior. - Verificação instantânea por recrutadores e empresas via leitura de QR Code.	- Expansão do modelo para certificações técnicas, ensino médio e microcredenciais (<i>Open Badges</i>). - Eliminação do mercado de fraudes de atestados escolares.
15	Inclusão Digital e Usabilidade	Riscos de exclusão para cidadãos de baixa maturidade digital, idosos ou pessoas de baixa escolaridade.	User Experience (UX) Invisível e VCs Impressas Abstração da criptografia na interface do usuário e suporte a QR Codes protegidos em papel.	- Testes de usabilidade com produtores rurais de baixa escolaridade e trabalhadoras autônomas no app Meu Imóvel Rural . - Padrão internacional de VC Barcodes para uso <i>offline</i> e impresso.	- Desenvolvimento de interfaces extremamente simples e acessíveis a diferentes públicos. - Garantia de funcionamento em cenários de baixa conectividade ou dispositivos mais simples.
16	Inclusão Digital e Usabilidade	Bloqueios de acesso por perda de senhas do gov.br e compartilhamento informal de contas com familiares ou contadores.	Mecanismos Formais de Delegação Criação de procurações digitais e papéis de representação sem necessidade de fornecer senhas pessoais.	- Relatos de compartilhamento indevido de códigos do gov.br com contadores para Imposto sobre a Renda de Pessoa Física (IRPF). - Mapeamento pelo Cetic.br (TIC Kids Online) do uso de celulares de terceiros em famílias vulneráveis.	- Implementação de fluxos formais de delegação (ex: representação por contadores) na carteira digital. - Proteção contra o sequestro indireto de contas por terceiros de boa ou má-fé.

► CONCLUSÃO

#	Assunto / Tema	Desafio Específico	Propostas	Casos e Exemplos	Pontos a Aprofundar
17	Riscos de Fraude e Sequestro de Contas	Engenharia social e sequestro de contas gov.br para alteração cadastral, emissão indevida e empréstimos fraudulentos.	Sinalizadores de Risco (Flags) Mecanismos de marcação de contas ou credenciais sob suspeita para exigir confirmações adicionais.	- Relatos de fraudes envolvendo acesso indevido ao gov.br para saques e empréstimos consignados. - Propostas de exportação dos mecanismos de sinalização de risco do Pix para o ecossistema de VCs.	▪ Criação de camadas adicionais de segurança dinâmica sem bloquear o acesso de usuários legítimos. ▪ Definição de responsabilidade civil para órgãos emissores em casos de alteração cadastral fraudulenta.
18		Aparelhamento de infraestruturas públicas digitais e mercados ilegais de dados em redes como Telegram.	Alertas Inter-Sistemas e Proteção de Dispositivos Comunicação rápida entre instituições em caso de comprometimento de aparelhos.	- Denúncias de uso indevido de dados de sistemas públicos (ex: sistema <i>Córtex</i> do Ministério da Justiça). - Proposta de integração do conceito do aplicativo Celular Seguro ao ecossistema de credenciais.	▪ Auditoria contínua de acessos e criação de registros de observabilidade ponta a ponta. ▪ Proteção contra vazamentos em massa em bases governamentais descentralizadas.
19	Adequação Normativa e Inovação Privada	Leis antigas que exigem o envio e arquivamento de cópias integrais de documentos em papel (ex: validação de declarações de Imposto de Renda, IR).	Modernização Regulatória e Checagem Atômica Adaptação de normas para aceitar validações atômicas e temporárias via VCs sem expor o documento integral.	- Proposta de uso de VCs para validação de IR na Lei de Improbidade Administrativa (Lei nº 8.429/1992). - Redução da exigência do arquivamento físico de declarações patrimoniais de servidores.	▪ Substituição formal do arquivamento permanente de papéis na Administração Pública por provas criptográficas. ▪ Adequação da legislação administrativa e tributária aos princípios da Lei Geral de Proteção de Dados (LGPD).
20	Adequação Normativa e Inovação Privada	Dificuldade de integração das empresas privadas, bancos e conselhos profissionais aos ecossistemas estatais.	Governo como Plataforma e Ecossistema Híbrido Plataformas privadas e conselhos integrados como emissores ao ecossistema do gov.br.	- Integração de conselhos profissionais (Ordem dos Advogados do Brasil (OAB), Enfermagem) ao gov.br. - Plataformas do CPQD operando com a Serasa Experian (<i>Serasa Pass</i>) e o Bradesco (<i>IDebra</i>). - Uso do Cadastro Único (+95M de pessoas) para VCs multipropósito.	▪ Fomento à livre concorrência entre carteiras públicas e privadas garantindo interoperabilidade. ▪ Estabelecimento de regras claras para o mercado privado emitir e verificar credenciais confiáveis.

4.1 Fragmentação e Custos de Desconexão

A atuação de sistemas em silos isolados gera duplicidade de dados e elevados custos com fraudes e burocracia analógica no setor público e privado. Para superar essa desconexão, a proposta central foca em Infraestruturas Públicas Digitais (IPDs) e na consolidação de chaves públicas. Casos como o **Pix**, a **Plataforma Conecta** do governo federal e o **e-Notariado** demonstram a viabilidade da integração de serviços e da adoção do CPF como identificador único nacional no **gov.br**. Os pontos críticos a aprofundar incluem a definição de âncoras de confiança (*trust anchors*) e a participação do setor privado sem a captura proprietária do valor público gerado.

4.2 Verificação Etária e Privacidade

Atender às exigências do ECA Digital e do Decreto nº 2.880/2026 para proteger crianças sem forçar a entrega de documentos completos exige soluções de minimização de dados, como os *Age Tokens* baseados em ZKPs e o modelo de dupla camada. Na prática, o MGI lidera soluções com a *stack open-source Inji/MOSIP* no **gov.br**, enquanto a Secretaria Nacional de Direitos Digitais mapeia o uso em *loot boxes* em jogos. O aprofundamento exige a publicação de guias regulatórios pela **ANPD**, a acreditação de entidades certificadoras, a garantia de acessibilidade e a proibição estrita do perfilamento comercial de dados etários.

4.3 Controle do Cidadão e Revogação

Para evitar a exposição desnecessária de dados em arquivos PDF e garantir o controle sobre documentos suspensos, propõe-se a Divulgação Seletiva (*AnonCreds* e *SD-JWT*) e o uso de listas dinâmicas de revogação (*Bitstring Status List*⁴). Essa arquitetura é aplicada na **Carteira Digital gov.br** (+180 milhões de contas), desenvolvida pelo **SERPRO/CPQD** em **Hyperledger Besu** (compatível com o **Drex**), viabilizando a consulta instantânea de CNHs cassadas. Os desdobramentos exigem avançar em modelos de “governo agêntico” com IAs operando sob permissão do cidadão, na certificação de mídias para combater *deepfakes* e no desempenho dessas verificações em larga escala.

4.4 Interoperabilidade Transfronteiriça

A validação de documentos civis e acadêmicos brasileiros no exterior enfrenta barreiras consulares e divergências de padrões. A solução passa por acordos multilaterais e pela adoção de perfis globais de alta garantia (HAIP da OpenID / W3C). O Brasil destaca-se ao liderar o **Consórcio Latino-Americano de Credenciais Digitais** com o Uruguai (permitindo acesso a +300 serviços uruguaios via **gov.br**) e na internacionalização do **Diploma Digital** no Mercosul. O aprofundamento do tema envolve estabelecer o reconhecimento mútuo de credenciais profissionais (como médicos e engenheiros), negociar a interoperabilidade com a União Europeia e preservar a soberania sobre os dados nacionais.

4.5 Burocracia no Setor Produtivo Rural

A jornada convencional para obter crédito rural no Brasil leva em média 73 dias devido à checagem manual de dados fundiários e ambientais. A proposta automatiza o envio de atributos de conformidade baseados nas bases do CAR, CNIR e CAF. Esse modelo foi aplicado no aplicativo **Meu Imóvel Rural** (Dataprev/MGI) e no piloto com 100 famílias no **Vale do Taquari (RS)**, em parceria com o MDA, EMATER e Banco do Brasil, agilizando inclusive o financiamento de tratores. Para escalar, é preciso engajar cooperativas e bancos privados na aceitação nativa dessas credenciais e garantir a inclusão de pequenos agricultores familiares.

⁴ https://ec.europa.eu/isa2/isa2conf18/once-only-principle-project-toop_en/

4.6 Desafios Arquiteturais e Legados

Frameworks de código aberto legados (como Hyperledger Indy) e protocolos antigos de federação acadêmica (SAML) criam gargalos de compatibilidade com o *app gov.br* (Flutter) e redes Ethereum. A proposta envolve a construção de agentes móveis nativos em Kotlin/Swift para redes Besu e a migração para a família **OpenID Federation**. O **SERPRO/CPQD** viabilizou esses agentes nativos no **gov.br** (alinhado ao **Drex**), enquanto a **RNP** e o **MEC** lideram a transição do SAML. O aprofundamento exige assegurar a manutenção sustentável desses *softwares* abertos no Brasil e harmonizar arquiteturas baseadas em *blockchain* com modelos sem *blockchain* (Web DIDs).

4.7 Governança da Confiança na Educação

Garantir a autenticidade de diplomas e a autoridade legal de instituições de ensino exige superar o risco de fraudes e a falta de rastreabilidade. Propõe-se o modelo de Confiança Delegada (*Trust Registries*), no qual o Ministério da Educação atua como âncora principal de confiança (*Trust Anchor*). Essa abordagem fundamenta a **Rede de Rastreabilidade da Educação Superior** (MEC/Dataprev) e a obrigatoriedade do **Diploma Digital**, permitindo a validação instantânea por empresas via QR Code. O aprofundamento requer criar regras para a persistência de diplomas caso a universidade seja extinta e expandir o modelo para certificações técnicas e *Open Badges*.

4.8 Inclusão Digital e Usabilidade

Soluções complexas de criptografia correm o risco de excluir cidadãos de baixa escolaridade, além de lidar com bloqueios por perda de senhas e o compartilhamento informal de contas com familiares ou contadores. A proposta aposta na abstração total da tecnologia (UX invisível), no uso de **VC Barcodes** (QR Codes protegidos em papel) e em mecanismos formais de procuração digital. Casos como os testes de usabilidade no *app Meu Imóvel Rural* e pesquisas do **Cetic.br** sobre o uso de celulares por terceiros ilustram o cenário. O aprofundamento exige criar fluxos seguros de delegação para contadores e garantir acessibilidade *offline*.

4.9 Riscos de Fraude e Sequestro de Contas

A engenharia social, o sequestro de contas **gov.br** para empréstimos fraudulentos e a comercialização ilegal de dados em redes como o Telegram ameaçam a confiança na infraestrutura pública. Como resposta, propõe-se a criação de sinalizadores dinâmicos de risco (*flags* anti-fraude) e protocolos de alerta de dispositivos comprometidos. As propostas inspiram-se nas **sinalizações de risco do Pix** e no modelo do aplicativo **Celular Seguro**, visando conter fraudes registradas no **gov.br** e usos indevidos de bases estatais. O aprofundamento foca na responsabilização civil dos emissores e no estabelecimento de auditorias contínuas sem bloquear acessos de usuários legítimos.

4.10 Adequação Normativa e Inovação Privada

Legislações ultrapassadas exigem a apresentação e o arquivamento físico de cópias integrais de documentos, enquanto empresas e conselhos profissionais enfrentam dificuldades de integração técnica. A proposta defende a modernização regulatória para aceitar validações atômicas e temporárias, adotando a visão de Governo como Plataforma. Na prática, sugere-se aplicar VCs na validação de IR na **Lei de Improbidade Administrativa**, além da integração de conselhos (**OAB, Enfermagem**) e plataformas privadas (**CPQD, Serasa Experian, Bradesco**) ao **gov.br**. O aprofundamento exige substituir a guarda física de papéis por auditorias criptográficas e aproveitar o **Cadastro Único** para VCs sociais.

5. PROVOCAÇÕES E PENSAMENTOS

O Quadro 5 apresenta um apanhado de perguntas provocadoras e conteúdos a serem discutidos a partir dos temas desenvolvidos no evento, no formato de organização proposto pelo Prof. Galloway.

QUADRO 5

Perguntas Provocadoras e Conteúdo a Ser Discutido no Formato Prof. Galloway

#	Tópico	Pergunta Questionadora	Palestrantes	Encruzilhadas para Tomada de Decisão
01	O Padrão W3C e a Descentralização Criptográfica	<i>A tecnologia é capaz de garantir a honestidade da origem?</i>	Henrique Xavier e Pierre-Antoine Champin	O choque entre a segurança matemática do JSON-LD e o risco real de automatização de fraudes por emissores privados fraudulentos.
02	A ICP-Brasil e a Validação Estatal de Chaves	<i>O instinto de controle do governo vai sufocar a inovação do setor privado?</i>	Enylson Camolesi, Miriam Wimmer e Fabro Steibel	A centralização burocrática <i>versus</i> a necessidade de flexibilidade e agilidade do mercado.
03	Conecta Gov.br e as Carteiras Digitais	<i>Quem vai cobrar o pedágio econômico da identidade nacional?</i>	Luanna Roncaratti	A soberania da Infraestrutura Pública Digital (IPD) diante da ameaça de <i>lock-in</i> das carteiras da Apple e do Google.
04	Casos Práticos e Projetos Piloto (Crédito Rural e CAR)	<i>Como escalar a tecnologia do laboratório para o abismo da desigualdade municipal?</i>	Yolanda Martínez e Luciano Charlita	O contraste entre o sucesso controlado dos testes e a assimetria tecnológica e orçamentária das prefeituras do interior.
05	O ECA Digital e a Emergência da Verificação Etária	<i>O governo vai descentralizar o acesso ou criar um oligopólio bilionário de verificadores privados?</i>	Victor Fernandes	A disputa pelo novo ambiente de disputa do novo ambiente de execução da regulação da Internet brasileira.
06	Provas de Conhecimento Zero (ZKP) e Limites da ANPD	<i>A regulação tem braço técnico para impedir a caça comercial aos metadados periféricos?</i>	Miriam Wimmer e Rafael Zanatta	A proteção de dados na ponta contra o modelo de negócios das plataformas, que vive do rastro de números IPs, geolocalização e horários de uso.
07	Governança e Responsabilidade no Ecossistema	<i>Quando o sistema falhar, de quem será a conta jurídica e financeira da fraude?</i>	Guilherme Almeida, Enylson Camolesi e Andreza Lona	A encruzilhada do vácuo de responsabilização em arquiteturas descentralizadas: a distribuição de culpa entre quem emite a credencial (ex: universidade ou banco), quem custodia o <i>app</i> (carteira) e quem verifica a informação, sob o risco de paralisia jurídica por judicialização em massa.
08	O Papel Estratégico do gov.br	<i>O gov.br é o catalisador da cidadania digital ou um futuro monopólio estatal com ponto único de falha?</i>	Luanna Roncaratti, Esther Dweck e Fabro Steibel	A faca de dois gumes do gov.br como catalisador e monopolista: ser o grande facilitador democrático de credenciais e verificação etária para o país <i>versus</i> o risco sistêmico de transformar 180 milhões de contas em um alvo único de sequestro de dados e dependência estatal centralizada.

6. TÓPICOS RELEVANTES DISCUTIDOS

6.1 Disputa de Arquitetura de Sistemas e Papel do Governo *versus* Setor Privado

- O PAPEL CENTRAL DO GOVERNO (INFRAESTRUTURA PÚBLICA DIGITAL - IPD):
 - **Provedor de Camada de Confiança:** O Estado deve atuar não apenas como emissor de documentos, mas proativamente como provedor e garantidor da infraestrutura pública e das fontes primárias de confiança (*Trust Anchors*).
 - **Bases Oficiais Fundacionais:** O Governo Federal utiliza bases de dados consolidadas para emitir credenciais fundacionais (como a conta *gov.br*, o CPF e a Carteira de Identidade Nacional – CIN). A partir destas, criam-se as credenciais derivadas para fins específicos.
 - **Autonomia Tecnológica e Soberania:** O MGI destaca que o foco do Estado é evitar a dependência de fornecedores (*vendor lock-in*) e garantir que os dados sensíveis dos cidadãos permaneçam sob regulação soberana e interesse público.
- A INSERÇÃO DO SETOR PRIVADO:
 - **Provedor de Serviços e Verificador Descentralizado:** As empresas privadas (plataformas digitais, *e-commerce*, agentes financeiros) operam no ecossistema primordialmente na ponta verificadora (*Verifiers*), consumindo as provas emitidas pelas fontes governamentais sem necessidade de criar bases paralelas.
 - **Inovação e Prestação de Serviços:** Abre-se mercado para que empresas privadas atuem como desenvolvedoras de carteiras digitais (*Wallets*) interoperáveis e provedoras de mercado de verificação (desde que respeitem os padrões regulados de governança e conformidade).

6.2 Aferição e Verificação de Idade

- MECANISMOS SEM MERCADO TERCEIRIZADO MASSIVO DE DADOS (*ZERO-KNOWLEDGE PROOFS* – ZKP):
 - Para cumprir o ECA Digital (Lei nº 15.211/2025 e Decreto nº 2.880/2026), a arquitetura desenhada pelo MGI/Dataprev adota o princípio de *Privacy by Design* e a minimização de dados.
 - Em vez de exigir envio de documentos completos, *selfies* ou criação de intermediários que colem dados para validar a idade em cada *site*, adota-se o uso de **Age Tokens** baseados em Provas de Conhecimento Zero (ZKPs).
- FUNCIONAMENTO DO MODELO PROPOSTO PELO GOVERNO (*AGE TOKEN*):
 - A partir das bases oficiais confiáveis (*gov.br/CIN*), a aplicação local do cidadão (sua carteira) obtém a validação etária.
 - Ao acessar um *site* ou *app* (como redes sociais, *e-commerce*, *streaming*), o titular envia apenas uma resposta binária e temporária (uma “prova seletiva” atestando se tem ou não maioridade ou determinado requisito etário), sem expor nome, data exata de nascimento ou CPF.
 - **Descentralização:** Não há consulta centralizada e em tempo real do Governo monitorando a navegação do cidadão. A verificação é efetuada localmente e de forma auditável diretamente entre a *wallet* do usuário e o verificador do *site/app*.

6.3 Nível e Tipo de Implementação no Brasil por Padrão Tecnológico e Papel do Governo e Setor Privado

O Quadro 6 apresenta os principais projetos e usos de credenciais verificáveis, bem como seu nível de implementação.

QUADRO 6

Nível e Tipo de Implementação de Credenciais Verificáveis no Brasil Elencadas por Padrão Tecnológico e o Papel do Governo e Setor Privado

Projeto / Caso de Uso	Estado de Implementação	Tipo / Padrão Tecnológico	Papel do Governo / Setor Privado
Identificação Civil (gov.br / CIN)	Produção / Operacional Mais de 177 milhões de contas; 120 milhões níveis Prata/Ouro.	Identidade digital unificada, validação biométrica e emissão de credencial fundacional (<i>Aries/Besu</i>).	Governo: Emissor e gestor da identidade.
Verificação Etária (ECA Digital)	Piloto / Em Implantação Aguardando regulamentação prática e integração.	Stack Inji/MOSIP, <i>Age Token</i> , ZKP e padrões W3C/OpenID (OID4VCI / OID4VP).	Governo: Emissor do <i>token</i> de idade. Privado: Verificador em <i>sites/apps</i> .
Acesso ao Crédito Rural	Piloto Ativo Região Sul / App "Meu Imóvel Rural".	Integração do CAR (Cadastro Ambiental Rural), CAF e bases fundiárias em credencial verificável no <i>app</i> .	Governo (MGI/Dataprev): Provedor do <i>app</i> /infraestrutura. Privado (Bancos): Verificadores automatizados.
Controle de Acesso Físico / Aeroportos	Fase de Teste Piloto Ações de validação de <i>rollout</i> e acesso a áreas restritas.	Credencial derivada <i>gov.br</i> , <i>blockchain Besu</i> , DIDComm v2.0, QR Code <i>offline</i> .	Governo (MGI/SERPRO/CPQD): Emissão e verificação.
Relações de Trabalho e Diplomas	Em estudo / Planejamento.	Credenciais qualificadas de vínculo profissional, habilidades e histórico educacional.	Misto: Instituições de ensino/ órgãos de classe como emissores.

6.4 Perspectivas para o Desenvolvimento Técnico do Governo Diante da Situação Atual

■ SOB O PONTO DE VISTA TÉCNICO

- **Padrões Internacionais Abertos:** Adoção rigorosa dos padrões W3C (*Verifiable Credentials Data Model v2.0, JSON-LD*) e da OpenID Foundation (*OID4VCI* para emissão e *OID4VP* para apresentação).
- **Redes e Armazenamento (*Blockchain* e Agentes *Mobile*):** Uso da rede *blockchain Hyperledger Besu* (alinhada à infraestrutura do Drex) para publicação de esquemas e suporte ao gerenciamento de DIDs e revogações. Desenvolvimento de agentes móveis em *Flutter* (utilizando frameworks Kotlin e Swift para iOS/Android) baseados na *stack Aries*.
- **Provas Criptográficas e Operacionalização *Offline*:** Utilização do protocolo *AnonCreds* para suporte a provas de conhecimento zero (ZKP). Suporte à validação presencial *offline* utilizando *QR Codes* dinâmicos/multicamadas e cache local com janela temporária de validação nos verificadores.

■ SOB O PONTO DE VISTA DE GOVERNANÇA

- **Estrutura Multissetorial e Federativa:** O ecossistema é alinhado entre MGI (SGD), Casa Civil, Dataprev, SERPRO, ITI e o apoio consultivo do Comitê Gestor da Internet no Brasil (CGI.br) / NIC.br e Banco Mundial.
- **Avanço Regulatório:** Respalado por marcos normativos como o Marco Civil da Internet (Lei nº 12.965/2014), a LGPD (Lei nº 13.709/2018), o ECA Digital (Lei nº 15.211/2025), e Decretos Federais de Identificação e Governo Digital (ex: Decreto 12.089/2024 e Decreto 2.880/2026).
- Organismos que Creditam/Atestam Emissores:
 - **ICP-Brasil / ITI:** Provê a Infraestrutura de Chaves Públicas para garantias e certificados criptográficos de alta confiança.
 - **Modelos de Autoridade de Confiança (*Trust Anchors e Recognized Entities*):** Regulamentação estatal e especificações do W3C (*Recognized Entities*) e OpenID (*HAIP / X.509*) para definir e encadear quem possui legitimidade para emitir cada tipo de credencial no ecossistema público e privado.

■ VOCABULÁRIOS CONTROLADOS PARA CAMPOS DE CREDENCIAIS

- Quem faz e Como faz:
 - **Proposição de Padrões:** O W3C elabora o modelo sintático e de ontologia aberta (*Linked Data / JSON-LD*).
 - **Definição Semântica Governamental:** A Infraestrutura Nacional de Dados (IND) da Secretaria de Governo Digital (SGD/MGI) padroniza a semântica e os esquemas oficiais dos atributos de dados do Estado brasileiro (como os campos oficiais da CIN, CAR e qualificações).
 - **Semântica Flexível:** Embora a tecnologia ofereça interoperabilidade técnica (*como trafegar o dado*), a definição de conceitos, regras de negócio e limites legais de cada campo cabe soberanamente às regulações de cada país e órgãos setoriais.

6.5 Pontos de Entrada do Setor Privado

■ CARTEIRAS DIGITAIS (*WALLETS*):

- O governo federal começou integrando as credenciais no próprio aplicativo *gov.br* (já presente em mais de 80 milhões de dispositivos).
- Contudo, o ecossistema é projetado para ser **aberto e interoperável**. Através da especificação *W3C Digital Credentials API* no nível do sistema operacional (Android / iOS) e da conformidade com perfis abertos (ex: *HAIP / OID4VP*), o setor privado e *Big Techs* (como *Google Wallet*, *Apple Wallet* e carteiras corporativas como a *Hovi*) poderão atuar como carteiras de armazenamento.

■ EMISSORES PRIVADOS:

- **Entrada de Entidades Classistas e Setor Privado:** Sim, órgãos de classe profissional (ex: Ordem dos Médicos, conselhos regionais), universidades privadas, bancos e seguradoras podem emitir credenciais verificáveis (diplomas, certificados de especialidade, apólices, dados de crédito).
- **Dependência Arquitetural:** A entrada dos emissores privados depende do credenciamento e do enquadramento das suas chaves nas regras de governança e emissores reconhecidos pelas autoridades de confiança (*Trust Framework*).

▪ **MERCADOS DE VERIFICADORES (POSSIBILIDADES):**

- **Validação Descentralizada e Sem Fricção:** Empresas privadas operam essencialmente no polo de verificadores, consumindo as provas dos usuários no *e-commerce*, setores bancários (*Know Your Customer* – *KYC*), plataformas digitais de entretenimento e logística.
- **Agentes de Inteligência Artificial e Automação:** Entrada estratégica para o setor privado na autenticação de Agentes de IA. As credenciais verificáveis servirão para atestar se um agente inteligente atuando em nome de uma empresa ou de um cidadão possui autorização legítima e limites regulados para realizar transações jurídicas ou financeiras.

6.6 Atuação do Setor Privado

O Quadro 7 sintetiza a atuação do setor privado em diferentes categorias de uso de credenciais verificáveis.

QUADRO 7

Matriz de Atuação do Setor Privado no Ecossistema de Credenciais Verificáveis

Categoria / Papel	Atores do Setor Privado	Principais Padrões e Tecnologias	Requisitos e Governança (<i>Trust Framework</i>)	Casos de Uso e Aplicações Práticas
Carteiras Digitais (Wallets)	▪ <i>Big Techs</i> (Google Wallet, Apple Wallet) ▪ <i>Wallets</i> Corporativas / Nativas (ex: Hovi)	▪ <i>W3C Digital Credentials API</i> (Nível de SO) ▪ <i>HAIP / OID4VP</i> ▪ Padrões Abertos e Interoperáveis	▪ Conformidade com perfis abertos de interoperabilidade ▪ Suporte a sistemas operacionais móveis (Android / iOS)	▪ Armazenamento seguro de credenciais pelo cidadão ▪ Apresentação de provas digitais diretamente no dispositivo
Emissores Privados (Issuers)	▪ Órgãos de Classe (ex: OAB, Conselhos de Medicina) ▪ Universidades Privadas ▪ Bancos e Seguradoras	▪ Padrões W3C de Credenciais Verificáveis (<i>Verifiable Credentials</i>) ▪ Modelos de Assinatura Criptográfica	▪ Credenciamento formal na Autoridade de Confiança (<i>Trust Anchor</i>) ▪ Validação e enquadramento de chaves públicas na estrutura de governança	▪ Diplomas digitais e certificados de especialização ▪ Atestados de vínculo profissional ▪ Apólices de seguro e dados para análise de crédito
Verificadores (Verifiers)	▪ Plataformas de <i>E-commerce</i> ▪ Instituições Financeiras ▪ Serviços de Logística e Entretenimento	▪ <i>OID4VP (OpenID for Verifiable Presentations)</i> ▪ Provas de Conhecimento Zero (ZKP)	▪ Aceite dos parâmetros de privacidade (<i>Privacy by Design</i>) ▪ Minimização da coleta de dados pessoais sensíveis	▪ Autenticação rápida e descentralizada (<i>KYC / Onboarding</i>) ▪ Validação de idade e atributos sem exposição de documentos
Automação e Agentes de IA	▪ Desenvolvedores de Inteligência Artificial ▪ Agentes de Automação Corporativa	▪ Protocolos de Autorização e Delegação Criptográfica ▪ Atribuição via DID (<i>Decentralized Identifiers</i>)	▪ Regulação de limites de autorização jurídica e financeira ▪ Registro e rastreabilidade da governança de agentes	▪ Validação da identidade e legitimidade de robôs/agentes de IA ▪ Execução autônoma de transações jurídicas e financeiras

6.7 Camadas, Funções e Atores de Credenciais Verificáveis

QUADRO 8

Camadas, Funções e Players do Ecossistema de Credenciais Verificáveis

Mencionado no evento		Incluído por análise dos consultores		Célula mista: evento + análise consultores		Sem item	
Camadas / Funções <i>OpenID Foundation</i>		W3C / W3C CCG IETF		ISO/IEC <i>Decentralized Identity Foundation (DIF)</i>		LF <i>Decentralized Trust</i> Outros players / Mecanismos	
1. Protocolo / Fluxo de Emissão da Credencial	OID4VCI 1.0 HAIP 1.0 (perfil transversal)	VCALM 1.0 (complementar)	OAuth 2.0 (base do OID4VCI)	ISO/IEC 23220-3	DIDComm Messaging	—	—
2. Modelo e Formato da Credencial Verificável	HAIP: seleciona SD-JWT VC + mdoc	VCDM 2.0 JSON-LD Data Integrity	SD-JWT VC SD-JWT (RFC 9901) JOSE / COSE / JWT	ISO/IEC 18013-5 (mDoc)	—	AnonCreds	—
3. Formato da Apresentação ou da Prova	HAIP: apresentação SD-JWT VC / mdoc	Verifiable Presentation Data Integrity / BBS	SD-JWT + KB-JWT	mDoc DeviceResponse	—	AnonCreds Proofs / ZKP	ZKP (família de técnicas)
4. Protocolo / Fluxo de Apresentação da Credencial	OID4VP 1.0	VCALM 1.0 VC Barcodes 1.0 (apresentação offline/QR)	—	Fluxo de apresentação mdoc	DIDComm Messaging	—	QR Code
5. Acesso e Seleção da Carteira	OID4VP (redirecionamentos e iniciação)	Digital Credentials API CHAPI (W3C CCG)	—	QR Code (ISO/IEC 18004) NFC em perfis mDoc	—	—	Deep link Seleção pelo sistema operacional
6. Transporte ou Canal de Comunicação	OID4VP sobre HTTP e perfis de proximidade	VC Barcodes / QR	HTTP TLS	mDoc via BLE/ NFC QR Code (ISO/IEC 18004)	DIDComm (agnóstico de transporte)	—	Bluetooth SIG: BLE NFC Forum: NFC FIDO Alliance: CTAP Câmera/QR
7. Modelo ou Estrutura de Confiança	<i>OpenID Federation</i> HAIP: X.509 / trust lists	DID Core Confidence Method Recognized Entities	PKIX / RFC 5280	X.509 / ISO/IEC 9594-8	—	Trust over IP Governance Metamodel	ETSI: Trust Lists GLEIF: vLEI
8. Ciclo de Vida e status da Credencial	HAIP: requisitos de revogação e status	Bitstring Status List 1.0 VCALM 1.0	Token Status List	—	—	AnonCreds revocation	—

7. POTENCIAIS TÓPICOS DE AGENDA FUTURA NÃO DISCUTIDOS NO *WORKSHOP*

A partir da revisão dos conteúdos discutidos durante o evento, elencam-se pontos adicionais para aprofundamento:

- Sustentabilidade Financeira das Listas de Revogação
- Gargalo de Latência na Verificação em Massa
- Interoperabilidade Semântica Federativa (Estados e Municípios)
- Padrões de Criptografia Pós-Quântica (PQC)
- Gestão de Chaves Criptográficas pelo Cidadão Comum
- Arquiteturas Híbridas de Armazenamento (*Backup* de Nuvem)
- Padrões para Rastreamento de Metadados de Apresentação

8. CONCEITOS, ASSUNTOS E FREQUÊNCIA DE MENÇÕES

O Quadro 9 apresenta a frequência de menção dos principais assuntos discutidos, visando elencar prioridades e tópicos de interesse para aprofundamento futuro. De maneira similar, a Figura 1 ilustra os principais termos usados.

QUADRO 9

Conceitos e Assuntos Mencionados no Evento e Frequência de Menções

#	Conceitos e Assuntos	Frequência de Menções
1	Verificação e aferição etária	219
2	Credenciais verificáveis	181
3	Interoperabilidade	107
4	Identidade digital	91
5	Governança e estruturas de confiança	88
6	Carteiras digitais	79
7	Segurança, autenticidade e integridade	71
8	Aferição e estimativa de idade	66
9	Padrões W3C para credenciais verificáveis	57
10	Plataforma gov.br	56
11	Privacidade e proteção de dados	56
12	Verificação e validação de credenciais	48
13	Governo como plataforma	41
14	Proteção de crianças e adolescentes no ambiente digital	40
15	Integração com plataformas móveis	38

CONTINUA ►

► CONCLUSÃO

#	Conceitos e Assuntos	Frequência de Menções
16	Infraestrutura pública digital	34
17	Adoção de credenciais verificáveis	33
18	Grupos de trabalho da OpenID Foundation	32
19	Padrões abertos e <i>software</i> livre	30
20	Carteira Europeia de Identidade Digital	29

FIGURA 1

Nuvem de Palavras Baseada na Frequência de Menções do Evento



9. GLOSSÁRIO

LISTA DE ABREVIATURAS, SIGLAS E ACRÔNIMOS

Abreviatura	Nome por extenso
AEPD	Agencia Española de Protección de Datos
ANATER	Agência Nacional de Assistência Técnica e Extensão Rural
AnonCreds	<i>Anonymous Credentials</i>
ANPD	Agência Nacional de Proteção de Dados
API	<i>Application Programming Interface</i>
app	Aplicativo
Bacen	Banco Central do Brasil
BB	Banco do Brasil
BBS	<i>Boneh-Boyen-Shacham</i> , esquema de assinatura criptográfica
BID	Banco Interamericano de Desenvolvimento
BLE	<i>Bluetooth Low Energy</i>

► CONTINUA

Abreviatura	Nome por extenso
CadÚnico	Cadastro Único para Programas Sociais do Governo Federal
CAF	Cadastro Nacional da Agricultura Familiar
CAR	Cadastro Ambiental Rural
CBOR	<i>Concise Binary Object Representation</i>
CCG	<i>Credentials Community Group</i>
Cetic.br	Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação
CGI.br	Comitê Gestor da Internet no Brasil
CHAPI	<i>Credential Handler API</i>
CIN	Carteira de Identidade Nacional
CNH	Carteira Nacional de Habilitação
CNIR	Cadastro Nacional de Imóveis Rurais
COSE	<i>CBOR Object Signing and Encryption</i>
CPF	Cadastro de Pessoas Físicas
CPQD	Centro de Pesquisa e Desenvolvimento em Telecomunicações
CRLV	Certificado de Registro e Licenciamento de Veículo
CRV	Certificado de Registro de Veículo
CTAP	<i>Client to Authenticator Protocol</i>
Dataprev	Empresa de Tecnologia e Informações da Previdência
DID	<i>Decentralized Identifier</i>
DIDComm	<i>DID Communication</i>
DIF	<i>Decentralized Identity Foundation</i>
ECA	Estatuto da Criança e do Adolescente
ECA Digital	Estatuto Digital da Criança e do Adolescente
eIDAS	<i>electronic Identification, Authentication and Trust Services</i>
EMATER	Empresa de Assistência Técnica e Extensão Rural
ETSI	<i>European Telecommunications Standards Institute</i>
EUA	Estados Unidos da América
EUDI	<i>European Union Digital Identity</i>
ex.	Exemplo
FIDO	<i>Fast Identity Online</i>
GLEIF	<i>Global Legal Entity Identifier Foundation</i>
HAIP	<i>OpenID4VC High Assurance Interoperability Profile</i>
HTTP	<i>Hypertext Transfer Protocol</i>
IA	Inteligência Artificial
ICP	Infraestrutura de Chaves Públicas
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
ID	identificação ou identidade
IETF	<i>Internet Engineering Task Force</i>

► CONTINUA

Abreviatura	Nome por extenso
IND	Infraestrutura Nacional de Dados
INPI	Instituto Nacional da Propriedade Industrial
IP	<i>Internet Protocol</i>
IPD	Infraestrutura Pública Digital
IR	Imposto de Renda
IRPF	Imposto de Renda da Pessoa Física
ISO/IEC	<i>International Organization for Standardization / International Electrotechnical Commission</i>
ITI	Instituto Nacional de Tecnologia da Informação
JOSE	<i>JavaScript Object Signing and Encryption</i>
JSON	<i>JavaScript Object Notation</i>
JSON-LD	<i>JSON for Linked Data</i>
JWT	<i>JSON Web Token</i>
KB-JWT	<i>Key Binding JSON Web Token</i>
KYC	<i>Know Your Customer</i>
LF	<i>Linux Foundation</i>
LGPD	Lei Geral de Proteção de Dados Pessoais
M	Milhões
mDoc	<i>mobile document</i>
MDA	Ministério do Desenvolvimento Agrário e Agricultura Familiar
MEC	Ministério da Educação
Mercosul	Mercado Comum do Sul
MGI	Ministério da Gestão e da Inovação em Serviços Públicos
MOSIP	<i>Modular Open-Source Identity Platform</i>
NFC	<i>Near Field Communication</i>
NIC.br	Núcleo de Informação e Coordenação do Ponto BR
OAB	Ordem dos Advogados do Brasil
OAuth	<i>Open Authorization</i>
OID4VC / OpenID4VC	<i>OpenID for Verifiable Credentials</i>
OID4VP / OpenID4VP	<i>OpenID for Verifiable Presentations</i>
OIDC	<i>OpenID Connect</i>
OIDF	<i>OpenID Foundation</i>
OpenID4VCI	<i>OpenID for Verifiable Credential Issuance</i>
OS	<i>Operating System</i>
PDF / PDFs	<i>Portable Document Format / Portable Document Formats</i>
PKIX	<i>Public Key Infrastructure using X.509</i>
PoC	<i>Proof of Concept</i>
PQC	<i>Post-Quantum Cryptography</i>
Prof.	Professor

► CONCLUSÃO

Abreviatura	Nome por extenso
QR	<i>Quick Response</i>
RFC	<i>Request for Comments</i>
RNP	Rede Nacional de Ensino e Pesquisa
RS	Rio Grande do Sul
SAML	<i>Security Assertion Markup Language</i>
SD-JWT	<i>Selective Disclosure for JSON Web Token</i>
SERPRO	Serviço Federal de Processamento de Dados
SGD	Secretaria de Governo Digital
SIG	<i>Special Interest Group</i>
SLA	<i>Service-Level Agreement</i>
SO	Sistema operacional
TIC	Tecnologias da Informação e Comunicação
TLS	<i>Transport Layer Security</i>
TOOP	<i>The Once-Only Principle</i>
TSA	<i>Transportation Security Administration</i>
UE	União Europeia
UX	<i>User Experience</i>
v	Versão
VC	<i>Verifiable Credential / credencial verificável</i>
VCALM	<i>Verifiable Credential API for Lifecycle Management</i>
VCDM	<i>Verifiable Credentials Data Model</i>
vLEI	<i>verifiable Legal Entity Identifier</i>
W3C	<i>World Wide Web Consortium</i>
ZKP	<i>Zero-Knowledge Proof</i>

NOMES, MARCAS E DENOMINAÇÕES SEM NATUREZA ABREVIATIVA

Nome ou marca	Identificação no relatório
Aadhaar	Sistema nacional de identificação civil da Índia.
Age Assurance Trial	Programa australiano de testes de tecnologias de verificação etária.
Age Token	Denominação usada para <i>tokens</i> ou provas digitais de faixa etária.
Android	Plataforma e sistema operacional móvel mantido pelo Google.
Apple Wallet	Carteira digital da Apple.
Bifold	<i>Framework</i> de carteira móvel associado ao ecossistema <i>Hyperledger Aries</i> .
Bitstring Status List	Especificação do W3C para publicação e consulta do <i>status</i> ou revogação de credenciais.
Bluetooth	Tecnologia de comunicação sem fio de curto alcance.
Bradesco	Instituição financeira mencionada em soluções de credenciais digitais.
Celular Seguro	Aplicativo e iniciativa governamental citados como referência de proteção de contas.

► CONTINUA

Nome ou marca	Identificação no relatório
Confidence Method	Modelo ou especificação de confiança citado na arquitetura de credenciais.
Córtex	Sistema do Ministério da Justiça citado no contexto de riscos de uso indevido de dados.
Data Integrity	Modelo de provas criptográficas empregado em credenciais verificáveis.
DigiLocker	Plataforma indiana de emissão e armazenamento de documentos digitais.
Digital Credentials API	Especificação de integração de credenciais digitais com navegadores e sistemas operacionais.
DID Core	Especificação central de identificadores descentralizados.
Drex	Nome do projeto brasileiro de moeda digital do Banco Central do Brasil.
e-Notariado	Plataforma brasileira para atos notariais eletrônicos.
ePassport	Denominação de passaporte eletrônico com <i>chip</i> .
EUDI Wallet	Carteira Europeia de Identidade Digital.
Flutter	<i>Framework</i> de desenvolvimento de aplicativos multiplataforma criada pelo Google.
Global Digital Collaboration	Iniciativa governamental suíça de colaboração em credenciais verificáveis.
Google Wallet	Carteira digital do Google.
gov.br	Plataforma federal brasileira de identidade e serviços digitais.
Hovi	Carteira corporativa citada como exemplo de solução privada.
Hyperledger Aries	Ecossistema de ferramentas para identidade descentralizada e credenciais digitais.
Hyperledger Besu	Cliente <i>blockchain</i> compatível com Ethereum utilizado na arquitetura descrita.
Hyperledger Indy	Tecnologia de registro distribuído voltada a identidade descentralizada.
ID Pass	Nome dado à credencial digital de passaporte mencionada no relatório.
IDebra	Solução mencionada no contexto da parceria entre Serasa e Bradesco.
Inji	Conjunto de códigos abertos para gestão de credenciais verificáveis do ecossistema MOSIP.
iOS	Sistema operacional móvel da Apple.
ISO/IEC 23220-3	Especificação das interfaces, protocolos e mecanismos de segurança/privacidade para instalação, emissão e derivação de credenciais eID baseadas em mDoc dentro de infraestruturas de sistemas eID móveis.
ISO/IEC 9594-8	Especificações de segurança para serviços de certificados de chaves públicas e de atributos.
Kotlin	Linguagem de programação multiplataforma citada no desenvolvimento de agentes móveis, priorizada no desenvolvimento para Android.
Linked Data	Modelo de dados conectados utilizado no ecossistema de credenciais.
Meu Imóvel Rural	Aplicativo brasileiro de integração de dados fundiários e acesso a crédito rural.
Open Badges	Padrão para emissão e verificação de distintivos e conquistas educacionais.
OpenID	Família de padrões abertos de identidade digital.
OpenID Federation	Especificação para federação de identidades e estabelecimento de confiança.
OpenWallet Foundation	Fundação dedicada a componentes abertos para carteiras digitais.
Pix	Nome do sistema brasileiro de pagamentos instantâneos.
Plataforma Conecta	Plataforma federal brasileira de integração e intercâmbio de dados.
Recognized Entities	Denominação de entidades reconhecidas em modelos de confiança.

► CONCLUSÃO

Nome ou marca	Identificação no relatório
RFC 5280	Definição do perfil dos certificados X.509 v3 e das listas de revogação de certificados (CRL) X.509 v2 para uso na Internet, incluindo formatos, extensões e o algoritmo de validação de caminhos de certificação.
Serasa Experian	Empresa de serviços de informação e análise de crédito citada no relatório.
Serasa Pass	Solução de identidade e verificação digital da Serasa mencionada no relatório.
Swift	Linguagem de programação citada no desenvolvimento de agentes para iOS.
Telegram	Serviço de mensagens citado no contexto de mercados ilegais de dados.
TIC Kids Online	Pesquisa sobre o uso da Internet por crianças e adolescentes no Brasil.
Token Status List	Especificação do IETF para representação e consulta do <i>status</i> de <i>tokens</i> ou credenciais.
Trust Anchors	Denominação de autoridades ou âncoras de confiança.
Trust Lists	Listas usadas para publicar ou reconhecer provedores e entidades confiáveis.
Trust over IP Governance Metamodel	Modelo de governança para ecossistemas de confiança digital.
VC Barcodes	Especificação ou abordagem para apresentação de credenciais por códigos de barras.
Verifiable Presentation Data Integrity	Modelo de prova de integridade aplicado a apresentações verificáveis.
WhatsApp	Serviço de mensagens citado como canal potencial para credenciais verificáveis.
X.509	Recomendação da <i>International Telecommunication Union</i> (ITU) para infraestrutura de chaves públicas e certificados digitais.

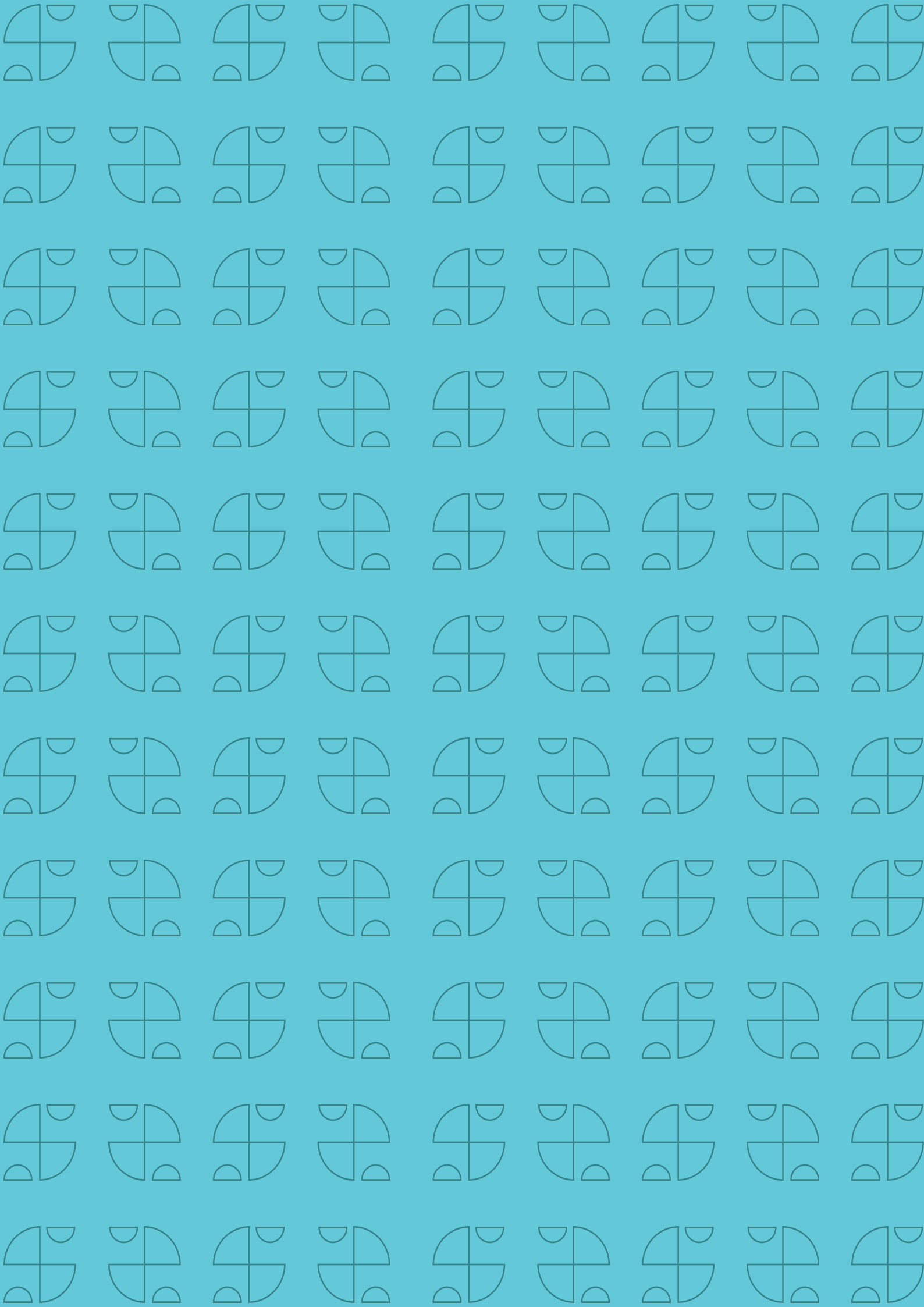
APÊNDICE A: SISTEMA DE CLASSIFICAÇÃO DE CASOS PRÁTICOS APRESENTADOS SOBRE CREDENCIAIS VERIFICÁVEIS

Sistema de classificação utilizado para desenvolvimento do conteúdo apresentado no Quadro 10.

QUADRO 10

Casos Práticos Ordenados por Região/País e Nível de Maturidade

Nível de Prontidão e Maturidade	Exemplo de Descrição de Caracterização	Arquitetura de Sistemas	Dimensões de Avaliação	
			Escala e Adoção de Uso	Governança e Legislação (Atos Normativos)
Inicial	Fase de Prospecção, Disputa de Padrões ou Desenho Inicial	Solução em fase de concepção técnica e <i>Proof of Concept</i> (PoC). Desenho lógico em aberto, com dependência de APIs de terceiros, componentes experimentais e falta de padronização nas camadas de integração.	Uso residual ou inexistente. Restrito a ambientes de testes laboratoriais, provas de conceito e validações pontuais por equipes técnicas internas.	Atos Normativos gerando a demanda, mas cujos critérios de governança, auditoria, testes de conformidade e responsabilidades legais ainda estão em definição.
Intermediário	Fase de Pilotos Avançados e Integração Tecnológica	Solução construída e funcional em ambiente de homologação. Arquitetura baseada em padrões abertos consolidados (ex: VCs, JSON-LD, OIDC), com barramentos e APIs de validação integrados às bases oficiais.	Adoção segmentada e controlada. Uso por públicos-alvo específicos, grupos focais ou órgãos piloto, transacionando dados e fluxos operacionais reais em volumes reduzidos.	Processo de articulação em andamento entre diferentes órgãos para implementação e definição de acordos operacionais (SLA).
Maduro	Produção em Larga Escala e Infraestrutura Estabelecida	Arquitetura implantada em produção resiliente e escalável. Infraestrutura centralizada ou federada de alta disponibilidade, com interoperabilidade plena, barramentos legados abstraídos e observabilidade ponta a ponta com padrões e melhores práticas definidas.	Uso massivo e recorrente. Adoção consolidada pelo ecossistema, com volume expressivo de transações e cobertura nacional de usuários ou órgãos usuários na rotina diária.	Amparado por atos normativos consolidados e vigentes (Ex: Leis consolidando o CPF como número único identificador, normas de privacidade e governança de dados ativos).



ceweb.br nic.br cgi.br



BANCO MUNDIAL
BIRD • AID | GRUPO BANCO MUNDIAL

MINISTÉRIO DA
GESTÃO E DA INOVAÇÃO
EM SERVIÇOS PÚBLICOS

GOVERNO DO
BRASIL
DO LADO DO POVO BRASILEIRO