REVISTA OWL (*OWL Journal*)
www.revistaowl.com.br – ISSN: 2965-2634

GOVERNANÇA DE ACESSO E PROTEÇÃO DE DADOS EM REDES ESCOLARES: PROTOCOLO CONCEITUAL A PARTIR DA EXPERIÊNCIA DO PROJETO CONECTAR

ACCESS GOVERNANCE AND DATA PROTECTION IN SCHOOL NETWORKS: A CONCEPTUAL PROTOCOL BASED ON THE CONECTAR PROJECT

DOI: 10.5281/zenodo.24432668

Laís da Rosa Lima Cunha[1]
Raira Aiúde Dias Ramos[2]
Thielly Kamilly Guedes Coelho[3]
Willian Vilhena da Cruz[4]
Eonay Barbosa Gurjão[5]
Célio do Nascimento Rodrigues[6]
Abymael Rennare Amaral dos Santos[7]
Klenilmar Lopes Dias[8]

RESUMO

Este artigo propõe um protocolo conceitual de avaliação de segurança de redes e proteção de dados para apoiar o uso escolar de tecnologias assistivas, tomando como contexto a implementação do Projeto CONECTAR em duas escolas públicas de Macapá (AP). Diferentemente de estudos anteriores

1 Graduanda em Tecnologia em Redes de Computadores, IFAP, Macapá, Amapá, Brasil. E-mail: llaislimaa21@gmail.com
2 Graduanda em Tecnologia em Redes de Computadores, IFAP, Macapá, Amapá, Brasil. E-mail: rraira357@gmail.com
3 Graduanda em Tecnologia em Redes de Computadores, IFAP, Macapá, Amapá, Brasil. E-mail: thiellyguedes441@gmail.com
4 Graduando em Tecnologia em Redes de Computadores, IFAP, Macapá, Amapá, Brasil. E-mail: williamvilhena3@gmail.com
5 Mestre em Computação Aplicada, FAP, Macapá, Amapá, Brasil. E-mail: eonay.gurjao@ifap.edu.br
6 Mestre em Educação, FAP, Macapá, Amapá, Brasil. E-mail: celio.rodrigues@ifap.edu.br
7 Licenciado em Informática, IFAP, Macapá, Amapá, Brasil. E-mail: rennare091@gmail.com
8 Doutor em Inteligência Computacional, IFPR, Umuarama, Paraná, Brasil. E-mail: klenilmar@gmail.com

A Revista OWL Journal está licenciada com uma Licença Creative Commons Atribuição (CC BY)

sobre funcionalidades, uso offline e infraestrutura geral, o foco recai na governança de acesso, no tratamento de informações e nas responsabilidades institucionais. Adotou-se abordagem qualitativa, documental e propositiva, com análise de relato de experiência de bolsista, publicações do projeto, literatura de segurança e legislação brasileira. A experiência documenta formação docente, instalação em tablets e aplicação pedagógica mediada, com continuidade das atividades mesmo diante de restrições de conectividade. A partir desse contexto, desenvolveu-se um protocolo de cinco etapas: delimitação de ativos e papéis, mapeamento de dados e fluxos, avaliação de riscos, priorização de controles e verificação. A contribuição é uma matriz de riscos e salvaguardas, acompanhada de arquitetura lógica de referência e indicadores para validação futura. Não foram conduzidos testes de intrusão nem auditoria de dados reais. Conclui-se que governança, segurança de rede e privacidade constituem condições organizacionais para expansão responsável de iniciativas inclusivas.

Palavras-chave: Segurança de redes; Proteção de dados pessoais; Tecnologia assistiva; Governança de acesso; Educação inclusiva.

ABSTRACT

This article proposes a conceptual protocol for assessing network security and data protection in school-based assistive technologies, using the implementation of the CONECTAR Project in two public schools in Macapá, Brazil, as context. Unlike prior studies addressing app features, offline use, and general infrastructure, this paper focuses on access governance, information processing, and institutional accountability. A qualitative, documentary, and proposal-oriented approach examined an undergraduate scholarship student's experience report, project publications, security literature, and Brazilian legislation. The documented experience includes teacher training, tablet deployment, and mediated educational activities, which continued despite connectivity constraints. The resulting protocol comprises five steps: defining assets and roles, mapping data and flows, assessing risks, prioritizing controls, and conducting verification. The contribution includes a risk-and-safeguard matrix, a logical reference architecture, and indicators for future validation. No penetration tests or audits of actual personal data were conducted. The study concludes that governance, network security, and privacy provide organizational foundations for responsibly scaling inclusive educational initiatives.

Keywords: Network security; Personal data protection; Assistive technology; Access governance; Inclusive education.

1. INTRODUÇÃO

A incorporação de tecnologias assistivas à escola pública produz benefícios potenciais para comunicação e participação, mas também torna relevante decidir quem administra dispositivos, como se organizam perfis, quais serviços exigem acesso externo e de que modo os registros relacionados a crianças são protegidos. Trata-se de questão distinta daquela que procura apenas verificar a existência de Internet ou a disponibilidade de equipamentos:

A Revista OWL Journal está licenciada com uma Licença Creative Commons Atribuição (CC BY)

segurança envolve relações entre pessoas, credenciais, sistemas, redes e responsabilidades institucionais (BRASIL, 2018; ROSE et al., 2020).

O Projeto CONECTAR, selecionado no Programa InovaEDUCAÇÃO da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES), Edital nº 3/2025, disponibiliza aplicativo Android que integra Comunicação Alternativa e Aumentativa (CAA), rotinas, jogos educativos e recursos de Inteligência Artificial. Seu desenvolvimento foi apresentado por Dias et al. (2026a). A utilização nas escolas envolveu formação de professoras, preparação e instalação em tablets, personalização de atividades e uso mediado em sala regular e no Atendimento Educacional Especializado (AEE). A continuidade dessas atividades demonstra viabilidade operacional de implantação no contexto relatado, sem constituir medição de efeito na aprendizagem.

Na experiência, em duas escolas de Macapá, as professoras e auxiliares conduziram a interação pedagógica com estudantes, enquanto bolsistas do projeto apoiaram instalação, demonstração e acompanhamento. Dificuldades de acesso à Internet foram contornadas pontualmente com conexão móvel da equipe, e equipamentos antigos exigiram atenção de suporte. Esses episódios não permitem concluir que o aplicativo apresenta falha de segurança; antes, tornam visíveis decisões de gestão relativas a dispositivos compartilhados, modalidades de conexão e condições de proteção de dados.

A questão de pesquisa é: como estruturar um protocolo verificável de avaliação de segurança de redes e governança de dados, adequado a projetos de tecnologia assistiva em escolas públicas, a partir de uma experiência de implementação já documentada? O objetivo é formular um método de avaliação e priorização de salvaguardas que contemple acesso, dispositivos, tráfego, registros e responsabilidades institucionais, sem apresentar proposta de topologia física ou novo modelo geral de continuidade pedagógica.

A contribuição é original em seu recorte: em vez de replicar o diagnóstico de infraestrutura e a arquitetura de rede já explorados em outros manuscritos do CONECTAR, oferece um artefato de governança orientado à ameaça e à conformidade, com etapas, evidências esperadas, matriz de riscos e critérios de aceitação. A solução é conceitual, ainda

A Revista OWL Journal está licenciada com uma Licença Creative Commons Atribuição (CC BY)

dependente de validação com gestores escolares, equipe técnica, encarregado de dados e profissionais pedagógicos.

2. FUNDAMENTAÇÃO TEÓRICA

2.1 Tecnologia assistiva, escola e o papel dos dados

A tecnologia assistiva reúne recursos e estratégias voltados à funcionalidade e à participação, conforme a Lei Brasileira de Inclusão (BRASIL, 2015). A CAA não se reduz a um conjunto de cartões ou telas: sua utilização exige seleção contextualizada e mediação dos interlocutores (BEUKELMAN; LIGHT, 2020; LIGHT; MCNAUGHTON, 2014). No CONECTAR, categorias, rotinas e jogos apoiam propostas educacionais desenvolvidas com professoras e auxiliares. Essa mediação é condição importante para adequação pedagógica, não evidência isolada de ganho de aprendizagem (DIAS et al., 2026a).

Em ambientes digitais, registros de atividades podem apoiar acompanhamento e planejamento; contudo, a finalidade pedagógica não autoriza coleta indiscriminada. É necessário distinguir dados indispensáveis ao funcionamento, identificadores para organização dos perfis, metadados técnicos de segurança e eventuais registros destinados à pesquisa. A política de tratamento depende do contexto, dos agentes envolvidos e das bases legais aplicáveis; especialmente no tratamento de dados de crianças deve prevalecer seu melhor interesse (BRASIL, 2018; ANPD, 2023).

Experiências de ensino e inclusão com tecnologias de custo reduzido reforçam a importância da adequação sociotécnica. Sousa e Dias (2023) discutem robótica alternativa e inclusão; Souza e Dias (2026) descrevem um laboratório remoto virtual; Dias et al. (2026b) apresentam pensamento computacional com computação desplugada e realidade aumentada; e Dias et al. (2023) analisam formação na licenciatura em informática. Essas publicações ajudam a situar a integração entre formação, recursos e prática educacional, sem serem tomadas como evidências de segurança do CONECTAR.

A Revista OWL Journal está licenciada com uma Licença Creative Commons Atribuição (CC BY)

2.2 Segurança em redes escolares: identidade, segmentação e observabilidade

Redes escolares articulam pontos de acesso, roteadores, equipamentos móveis e serviços internos ou externos. Kurose e Ross (2021) oferecem fundamentos para compreender protocolos e relações entre serviços e infraestrutura. Em WLAN, os mecanismos de autenticação e proteção do tráfego devem ser coerentes com a arquitetura e o perfil dos dispositivos, com políticas de atualização e controle de acesso (SOUPPAYA; SCARFONE, 2012). A segmentação lógica pode reduzir caminhos de comunicação indesejados, mas, isoladamente, não substitui autorização por identidade, gestão de credenciais e controles nos serviços.

A arquitetura de confiança zero descrita por Rose et al. (2020) sustenta a premissa de que um recurso não deve receber confiança apenas por estar conectado à rede interna. Em contextos escolares, o princípio pode ser traduzido proporcionalmente em perfis individualizados, privilégios mínimos, revisão periódica de acesso e autenticação adequada aos papéis, sem pressupor implantação integral de uma solução corporativa complexa. O planejamento também deve incluir inventário, ciclo de vida dos tablets, atualizações, configuração protegida e procedimentos de resposta a incidentes.

2.3 LGP, crianças e ciclo de vida de registros

A Lei nº 13.709/2018 estabelece princípios como finalidade, adequação, necessidade, transparência, segurança e prevenção. Para dados pessoais de crianças e adolescentes, o artigo 14 e a interpretação da ANPD impõem exame específico do melhor interesse, sem presumir que toda operação dependa de uma única hipótese legal (BRASIL, 2018; ANPD, 2023). A presença de informação potencialmente relacionada a condição de saúde requer atenção à classificação de dados sensíveis e às bases legais apropriadas, tema que deve ser analisado conforme a efetiva base de dados, não inferido apenas do público atendido.

Uma política de governança precisa tratar separadamente criação da conta, acesso por educadores, registro de atividades, eventual compartilhamento entre instituição e projeto, exportação para pesquisa, retenção e descarte. A desidentificação deve considerar risco de reidentificação, sobretudo quando conjuntos de dados pequenos, datas ou instituições possam

A Revista OWL Journal está licenciada com uma Licença Creative Commons Atribuição (CC BY)

permitir associação indireta. Também se exige evitar exposição em capturas do dashboard ou divulgação de registros individualizados.

2.4 Pesquisa aplicada e construção de artefatos de governança

Estudos documentais permitem extrair necessidades de situações registradas, mas não comprovam o estado efetivo de controles técnicos ausentes da documentação (GIL, 2008). A análise temática auxilia a organizar evidências qualitativas por categorias, distinguindo fatos relatados de inferências analíticas (BRAUN; CLARKE, 2006). Para dar forma ao artefato proposto, adotou-se raciocínio compatível com design science: explicitar o problema, formular o artefato, justificar seus requisitos e prever avaliação em contexto (HEVNER et al., 2004). Neste estudo, apenas a formulação e a avaliação argumentativa de coerência foram realizadas; não se reivindica validação em campo.

3. METODOLOGIA

3.1 Delineamento, corpus e unidade de análise

O estudo é qualitativo, documental e propositivo, com elaboração de artefato conceitual de governança. Seu ponto de partida é o relato de experiência da bolsista relativo às atividades de junho a setembro de 2026 nas escolas Mãe Angélica e Nancy Nina, em Macapá (AP). O corpus contextual inclui a publicação técnica do CONECTAR, os manuscritos correlatos disponibilizados para comparação e fontes normativas de segurança e proteção de dados. As unidades de análise foram os episódios ou decisões documentados com implicações para dispositivo, conta, conectividade, tratamento de registros ou atribuição de responsabilidade.

O relato descreve formação teórico-prática, demonstração, instalação e testes do aplicativo em tablets, uso assistido em sala regular e no AEE, reuniões de encerramento e existência de registros e formulários de avaliação. A bolsista explicita que não acessou respostas individuais do formulário nem analisou quantitativamente o banco de dados; essas fontes, portanto, não foram utilizadas para calcular desfechos ou riscos empíricos.

A Revista OWL Journal está licenciada com uma Licença Creative Commons Atribuição (CC BY)

3.2 Procedimento analítico e prevenção de sobreposição editorial

Primeiro, realizou-se leitura comparativa dos quatro manuscritos correlatos: um sobre uso offline, outro sobre apropriação escolar e continuidade pedagógica, um terceiro sobre método conceitual de infraestrutura de TI e um quarto sobre diagnóstico e arquitetura geral de redes. A partir dessa comparação, delimitaram-se como objetos já cobertos conectividade, capacidade, cabeamento, implantação e mediação. Reservou-se para o novo artigo o objeto "governança de segurança e privacidade", com requisitos e testes destinados à avaliação posterior, evitando reapresentar figuras e quadros dos estudos anteriores como resultados inéditos.

Segundo, os episódios do relato foram categorizados como: E1 — provisão e manutenção de dispositivos; E2 — uso de conexões alternativas; E3 — organização de perfis e papéis; E4 — acompanhamento de atividades; E5 — suporte e continuidade. Terceiro, cada categoria foi relacionada a um ativo, a uma possibilidade de ameaça, a uma salvaguarda e a uma evidência de verificação. A ameaça corresponde a cenário plausível a investigar, e não a ocorrência de incidente. Quarto, foi elaborado um protocolo de cinco etapas, acompanhado de arquitetura lógica e matriz de análise.

3.3 Critérios de construção e limites

A formulação adotou quatro critérios: rastreabilidade (cada recomendação identifica a origem documental ou normativa), proporcionalidade (controles ajustáveis ao porte da escola), separação entre fato e hipótese (nenhuma vulnerabilidade é declarada sem teste) e verificabilidade (cada ação prevê evidência objetiva). A matriz utiliza prioridades qualitativas indicativas, não um escore de risco calculado a partir de ocorrências observadas. Sua utilização real exige definir probabilidade e impacto com representantes das instituições.

Não foram realizadas varreduras de portas, captura de pacotes, testes de autenticação, análise de banco de dados, pentest, inspeção de rede ou consulta a dados pessoais dos estudantes. O trabalho não audita a conformidade LGPD do CONECTAR ou das escolas; propõe metodologia para avaliação futura. Nenhuma conclusão sobre tratamento efetivamente realizado pode ser derivada da mera existência de um dashboard.

A Revista OWL Journal está licenciada com uma Licença Creative Commons Atribuição (CC BY)

4. O CONECTAR COMO CONTEXTO DE APLICAÇÃO

4.1 Formação e operacionalização em ambientes escolares

O relato registra duas configurações de uso: na Escola Mãe Angélica, intervenções em sala regular com professoras e auxiliares conduzindo tablets e bolsistas atuando no apoio; na Escola Nancy Nina, ações no AEE, com menor número de estudantes por atendimento e acompanhamento individualizado. As equipes organizaram apresentações, exercícios práticos com professoras, preparação de dispositivos e adaptação de conteúdos pedagógicos. A experiência indica implementação efetiva em situações educativas e cooperação entre profissionais, sem afirmar aprendizagem mensurada ou eficácia clínica.

O CONECTAR foi desenvolvido como solução assistiva e educacional com recursos visuais, síntese de voz, personalização de categorias, rotinas, jogos e módulos de IA (DIAS et al., 2026a). Sua presença em sala de aula oferece um contexto pertinente para refletir sobre governança digital, pois há diversidade de usuários, dispositivos transportáveis e necessidade de continuidade pedagógica. O manuscrito não reprojeta a aplicação nem exige alteração de funcionalidades que não tenham sido tecnicamente avaliadas.

4.2 Situações de contexto com implicações para segurança

A disponibilização de tablets pelo IFAP permitiu viabilizar intervenções; a observação de equipamentos antigos com travamentos aponta necessidade de inventário e política de manutenção. O uso eventual de Internet móvel da própria equipe permitiu dar continuidade a atividades quando a conexão institucional não estava disponível, mas motiva, para uma implantação institucional futura, exame de autorização, configuração, proteção de tráfego e responsabilidades. Tais situações não provam transmissão insegura nem exposição de dados.

4.3 Da utilização exitosa à governança responsável

O êxito descritivo da implantação deve ser entendido como realização de formação, instalação, testes e intervenções mediadas nos dois ambientes, inclusive mediante soluções operacionais para garantir sua realização. A contribuição deste trabalho parte desse cenário

A Revista OWL Journal está licenciada com uma Licença Creative Commons Atribuição (CC BY)

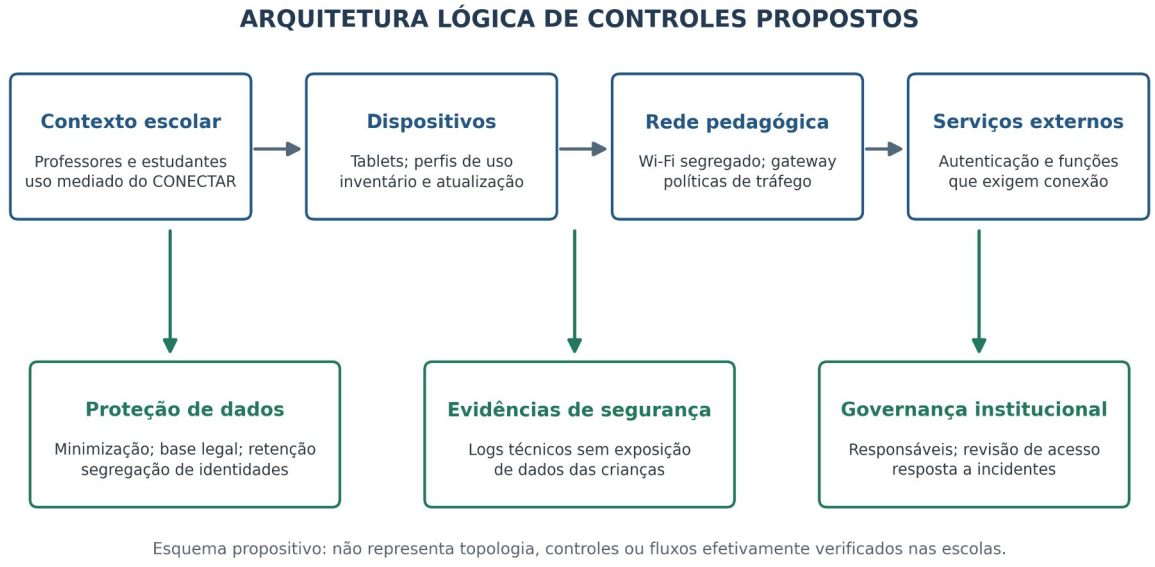
positivo para discutir requisitos de amadurecimento institucional. A inclusão de governança de acesso e práticas de privacidade é uma oportunidade de escalonamento responsável do CONECTAR, e não juízo negativo sobre o aplicativo ou as escolas.

5. PROPOSTA METODOLÓGICA DE SEGURANÇA E PROTEÇÃO DE DADOS

5.1 Arquitetura lógica de controles

A Figura 1 representa uma arquitetura lógica de controles para análise futura. O fluxo de uso vincula profissionais e estudantes aos dispositivos pedagógicos, à rede institucional e, quando necessário, a serviços externos. Em paralelo, três planos transversais estabelecem salvaguardas de dados, evidências técnicas e governança institucional. O diagrama não é um desenho da topologia real nem afirma utilização de VLANs, autenticação robusta ou centralização de logs nas escolas acompanhadas.

Figura 1 – Arquitetura lógica proposta de controles de segurança e privacidade para o uso escolar do CONECTAR.



Fonte: proposta conceitual dos autores (2026).

A escolha de controles deve decorrer de inventário e levantamento de fluxos: por exemplo, se não houver integração remota em determinada operação, não cabe pressupor

A Revista OWL Journal está licenciada com uma Licença Creative Commons Atribuição (CC BY)

transmissão de dados dessa função. Da mesma forma, a segmentação administrativa e pedagógica deve ser definida após conhecer os equipamentos, privilégios e necessidades de comunicação. Os princípios orientadores são necessidade de acesso, minimização e rastreabilidade (BRASIL, 2018; ROSE et al., 2020).

5.2 Protocolo em cinco etapas

O protocolo compreende uma sequência de avaliação repetível, concebida para execução conjunta por profissional de redes, docente responsável, equipe do projeto e representantes da instituição. A etapa 1 delimita finalidade, ambientes, dispositivos, perfis e responsáveis; a etapa 2 identifica, mediante entrevistas e inspeção autorizada, fluxos de dados locais e remotos; a etapa 3 transforma achados em cenários de ameaça e riscos; a etapa 4 seleciona salvaguardas proporcionais; e a etapa 5 valida controles e produz registros técnicos sem expor dados de crianças.

Figura 2 – Protocolo proposto de avaliação e validação de segurança de redes e privacidade.



Fonte: proposta conceitual dos autores (2026).

5.3 Matriz de riscos e salvaguardas

O Quadro 1 associa situações descritas no relato ou classes de ativos relevantes a perguntas de auditoria e a evidências verificáveis. As prioridades são apenas exemplos iniciais

A Revista OWL Journal está licenciada com uma Licença Creative Commons Atribuição (CC BY)

para planejamento e não níveis de risco medidos. Em aplicação futura, recomenda-se documentar impacto, probabilidade, responsáveis, custos e condições para aceitação de risco, com decisão colegiada.

Quadro 1 – Matriz propositiva de cenários, salvaguardas e verificação.

Contexto ou ativo	Risco a investigar (não comprovado)	Controle proposto	Evidência futura
Tablets móveis e compartilhados	Uso por perfil inadequado ou perda de dispositivo	Inventário, bloqueio, perfis e atualizações	Checklist por tablet; teste de bloqueio
Conexão alternativa por celular	Conexão sem política institucional documentada	Rede autorizada, proteção de sessão e orientação	Política aprovada; teste de configuração
Perfis de educadores e estudantes	Acesso além da finalidade pedagógica	Papéis, menor privilégio e revisão periódica	Matriz de acesso; revisão semestral
Registros de atividades	Retenção excessiva ou exportação identificável	Mapa de dados, minimização e prazo de retenção	Inventário de dados e política aprovada
Rede Wi-Fi pedagógica	Comunicação desnecessária entre dispositivos	Avaliar isolamento de clientes e segmentação	Testes autorizados de conectividade
Registros técnicos de incidentes	Exposição de identificadores em logs	Pseudonimização e acesso restrito	Amostras sintéticas e trilha de auditoria
Serviços externos eventualmente usados	Fluxos e terceiros insuficientemente documentados	Mapa de integrações e responsabilidades	Diagrama validado; contratos aplicáveis

Fonte: proposta conceitual dos autores (2026).

O foco não é encontrar vulnerabilidades por suposição. A matriz ajuda a organizar uma avaliação futura proporcional ao cenário: por exemplo, um equipamento cedido pode ser adequadamente protegido, mas isso só será confirmado mediante inspeção autorizada. Também não se confunde disponibilidade de Internet com proteção do conteúdo transmitido; são propriedades distintas.

5.4 Plano de verificação de indicadores

O Quadro 2 define uma estratégia de avaliação posterior, com indicadores que podem ser produzidos sem leitura de conteúdo sensível das atividades pedagógicas. A escolha e os limiares dos indicadores exigem validação institucional; os exemplos abaixo devem ser tratados como propostas de operacionalização, não metas já atingidas.

A Revista OWL Journal está licenciada com uma Licença Creative Commons Atribuição (CC BY)

Quadro 2 – Indicadores propostos para validação futura.

Indicador	Definição operacional	Fonte e periodicidade
Cobertura do inventário	Dispositivos inventariados / dispositivos em uso × 100	Inventário institucional; mensal
Perfis revisados	Contas revisadas / contas ativas × 100	Relatório de gestão de acesso; trimestral
Conformidade de atualização	Dispositivos conformes / dispositivos elegíveis × 100	Checklist técnico; mensal
Fluxos documentados	Integrações descritas / integrações identificadas × 100	Mapa de fluxos; por mudança de versão
Incidentes tratados	Incidentes encerrados conforme fluxo / incidentes registrados × 100	Registro técnico; trimestral
Revisão de retenção	Conjuntos de dados com prazo definido / conjuntos identificados × 100	Inventário de tratamento; semestral

Fonte: Elaborado pelos autores (2026).

Na avaliação futura, a inspeção de redes e dispositivos deve empregar contas de teste, dados sintéticos e autorização formal. Testes de acesso não devem envolver estudantes reais ou conteúdos identificáveis. Resultados serão registrados por controle e não por pessoa, preservando a privacidade do público atendido. O protocolo permite comparar o estado inicial e o estado após eventual adequação, mas essa comparação ainda não foi executada.

5.5 Responsabilidade e gorvernança

A governança não pode ser atribuída apenas à bolsista ou ao técnico de redes. A direção da escola, a coordenação do projeto, profissionais de TI e o responsável institucional pelo tratamento de dados devem definir papéis segundo instrumentos de cooperação e responsabilidades legais efetivamente aplicáveis. Cabe às equipes pedagógicas determinar finalidades educacionais e acesso necessário; à TI, operacionalizar controles; e aos responsáveis pela governança de dados, avaliar base legal, transparência, registros e respostas a incidentes (BRASIL, 2018; ANPD, 2023).

A bolsista de Tecnologia em Redes de Computadores contribui na elaboração do protocolo, na organização de requisitos e na definição de evidências técnicas, sob supervisão acadêmica. O desenho não implica que ela realizou auditoria, vistoria detalhada, engenharia de segurança implantada ou tratamento de dados pessoais. Essa delimitação preserva a natureza formativa e a responsabilidade institucional pelas decisões de implantação.

A Revista OWL Journal está licenciada com uma Licença Creative Commons Atribuição (CC BY)

6. DISCUSSÃO

Os manuscritos correlatos ao CONECTAR examinam a operação offline, a adaptação à escola, a infraestrutura geral ou um método multidimensional de continuidade. A presente proposta complementa — sem reproduzir — esses recortes ao perguntar não "quais equipamentos instalar?", mas "como controlar e comprovar que o acesso e o tratamento de dados permanecem proporcionais às finalidades educacionais?". A distinção tem relevância científica porque transforma princípios legais e recomendações técnicas em perguntas de avaliação, documentos exigíveis e procedimentos verificáveis.

A análise também evita associar automaticamente episódios de indisponibilidade de Internet a vulnerabilidades: conectividade insuficiente não prova quebra de confidencialidade, e um equipamento com travamento não comprova falha de autenticação. Tais situações funcionam como gatilhos para levantamento de ativos e políticas. A implantação do CONECTAR, viabilizada por formação, mediação e apoio técnico, oferece campo para estudar governança justamente porque representa uma utilização real de tecnologia assistiva, e não um cenário hipotético de laboratório.

A LGPD impõe que finalidades, bases legais, responsabilidades e segurança sejam avaliadas conforme operações efetivas. O protocolo não determina que o consentimento é sempre a única base cabível, tampouco presume que todos os dados de atividades sejam sensíveis. O melhor interesse de crianças orienta a análise concreta e a adoção de controles compatíveis com o risco, conforme entendimento da ANPD (2023). Uma metodologia de inventário e classificação reduz a chance de extrapolações jurídicas sem exame do tratamento efetivo.

A proposta possui três limites principais. Primeiro, o corpus registra atividades de formação e aplicação, não inventário técnico completo. Segundo, não houve acesso a dados pessoais, logs operacionais ou respostas docentes para avaliar conformidade real. Terceiro, o protocolo ainda não passou por avaliação de especialistas ou aplicação piloto. Portanto, os resultados correspondem à elaboração de artefato argumentado e rastreável; sua utilidade e viabilidade devem ser investigadas em etapa subsequente.

A Revista OWL Journal está licenciada com uma Licença Creative Commons Atribuição (CC BY)

7. CONSIDERAÇÕES FINAIS

O estudo apresentou um protocolo conceitual para avaliação de segurança de redes e proteção de dados no contexto de tecnologias assistivas escolares, tomando como referência a aplicação documentada do Projeto CONECTAR. A experiência de formação docente, instalação em dispositivos e uso mediado nas duas escolas demonstrou a realização das ações propostas e a possibilidade de continuidade operacional com apoio da equipe. A discussão de segurança foi construída como dimensão de amadurecimento e expansão responsável, não como crítica ao aplicativo.

A contribuição consiste em cinco etapas metodológicas, uma arquitetura lógica de controles, uma matriz de cenários e salvaguardas e um conjunto de indicadores para validação posterior. O resultado difere de propostas gerais de infraestrutura porque enfatiza identidades, finalidades, fluxos, retenção, evidências de controle e responsabilidade institucional. Como perspectivas futuras, recomenda-se validação do protocolo por equipe multidisciplinar, mapeamento autorizado de fluxos e aplicação piloto com dados sintéticos, após autorização institucional e exame ético pertinente.

FINANCIAMENTO

Este estudo apresenta resultados do Projeto CONECTAR, selecionado no Programa InovaEDUCAÇÃO – Edital nº 3/2025. Os autores agradecem o apoio financeiro da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) – Brasil, por meio do Processo nº 88887.180678/2025-00.

REFERÊNCIAS

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). Enunciado CD/ANPD nº 1, de 22 de maio de 2023. Brasília, DF: ANPD, 2023. Disponível em: https://bibliotecadigital.mj.gov.br/handle/1/10215. Acesso em: 11 nov. 2026.

BEUKELMAN, David R.; LIGHT, Janice C. Augmentative & alternative communication: supporting children and adults with complex communication needs. 5. ed. Baltimore: Paul H. Brookes Publishing, 2020.

A Revista OWL Journal está licenciada com uma Licença Creative Commons Atribuição (CC BY)

BRASIL. Lei nº 13.146, de 6 de julho de 2015. Institui a Lei Brasileira de Inclusão da Pessoa com Deficiência (Estatuto da Pessoa com Deficiência). Brasília, DF: Presidência da República, 2015. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13146.htm. Acesso em: 11 nov. 2026.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 11 nov. 2026.

BRAUN, Virginia; CLARKE, Victoria. Using thematic analysis in psychology. Qualitative Research in Psychology, v. 3, n. 2, p. 77-101, 2006. DOI: https://doi.org/10.1191/1478088706qp063oa.

COORDENAÇÃO DE APERFEIÇOAMENTO DE PESSOAL DE NÍVEL SUPERIOR (CAPES). Edital nº 3/2025 – InovaEDUCAÇÃO. Brasília, DF: CAPES, 2025. Disponível em: https://www.gov.br/capes/pt-br/acesso-a-informacao/acoes-e-programas/articulacao-e-inovacao-em-educacao-aberta/sistema-universidade-aberta-do-brasil/editais-uab/edital-no-3-2025-inovaeducacao. Acesso em: 11 nov. 2026.

DIAS, Klenilmar Lopes; BARROSO, Gabriel Canela; RAMOS, Raira Aiúde Dias; COELHO, Thielly Kamilly Guedes; VAZ, Anderson Nascimento; RODRIGUES, Célio do Nascimento; SANTOS, Abymael Rennare Amaral dos; GURJÃO, Eonay Barbosa. Infraestrutura de TI e educação inclusiva: o Projeto CONECTAR e um método conceitual de análise para continuidade pedagógica. Artefactum: Revista de Estudos Interdisciplinares, [S. l.], v. 25, n. 13, p. 1-16, 2026. DOI: https://doi.org/10.23900/artefactum.v25i13.121. Disponível em: https://artefactumjournal.com/index.php/artefactum/article/view/5275. Acesso em: 11 nov. 2026.

DIAS, Klenilmar Lopes; DIAS, Felipe V.; DIAS, Karla R. V.; ROCHA, Emellin R. S.; DIAS, Klessis L.; GURJÃO, Eonay B. Pensamento computacional nos anos iniciais: relato de experiência com computação desplugada e realidade aumentada. In: WORKSHOP SOBRE EDUCAÇÃO EM COMPUTAÇÃO, 34., 2026, Gramado. Anais [...]. Porto Alegre: Sociedade Brasileira de Computação, 2026. Disponível em: https://sol.sbc.org.br/index.php/wei/article/view/43158. Acesso em: 11 nov. 2026.

A Revista OWL Journal está licenciada com uma Licença Creative Commons Atribuição (CC BY)

DIAS, Klenilmar Lopes; SANTOS, Abymael Rennare Amaral dos; DIAS, Felipe Vilhena; GURJÃO, Eonay Barbosa; DIAS, Klessis Lopes. Conectar: aplicativo assistivo para crianças com TEA com IA, CAA, rotinas e jogos educativos. In: COMPUTER ON THE BEACH, 17., 2026, Florianópolis. Anais [...]. Itajaí: Universidade do Vale do Itajaí, 2026. p. 44-52. DOI: https://doi.org/10.14210/cotb.v17.p044-052.

DIAS, Klenilmar Lopes; SOBRINHO, Ana Carla de Jesus; GURJÃO, Eonay Barbosa; DIAS, Klessis Lopes. Prática como componente curricular no curso de licenciatura em informática: relato de experiência do estágio supervisionado no modelo de ensino remoto emergencial. Ensino de Ciências e Tecnologia em Revista – ENCITEC, v. 13, n. 2, p. 187-206, 2023. DOI: https://doi.org/10.31512/encitec.v13i2.1136.

GIL, Antonio Carlos. Métodos e técnicas de pesquisa social. 6. ed. São Paulo: Atlas, 2008.

HEVNER, Alan R.; MARCH, Salvatore T.; PARK, Jinsoo; RAM, Sudha. Design science in information systems research. MIS Quarterly, v. 28, n. 1, p. 75-105, 2004.

KUROSE, James F.; ROSS, Keith W. Computer networking: a top-down approach. 8. ed. [S. l.]: Pearson, 2021.

LIGHT, Janice; MCNAUGHTON, David. Communicative competence for individuals who require augmentative and alternative communication: a new definition for a new era of communication? Augmentative and Alternative Communication, v. 30, n. 1, p. 1-18, 2014. DOI: https://doi.org/10.3109/07434618.2014.885080.

RAMOS, Raira Aiúde Dias; COELHO, Thielly Kamilly Guedes; CUNHA, Laís da Rosa Lima; BARROSO, Gabriel Canela; CRUZ, Willian Vilhena da; VAZ, Anderson Nascimento; DIAS, Klessis Lopes; GURJÃO, Eonay Barbosa; RODRIGUES, Célio do Nascimento; SANTOS, Abymael Rennare Amaral dos; DIAS, Klenilmar Lopes. Infraestrutura de redes para a inclusão educacional: diagnóstico da realidade escolar e proposta de adequação tecnológica a partir da aplicação do Projeto Conectar. Revista OWL (OWL Journal): Revista Interdisciplinar de Ensino e Educação, [S. l.], v. 4, n. 11, p. 1-21, 2026. DOI: https://doi.org/10.5281/zenodo.24021580. Disponível em: https://revistaowl.com.br/index.php/owl/article/view/1232. Acesso em: 11 nov. 2026.

ROSE, Scott; BORCHERT, Oliver; MITCHELL, Stu; CONNELLY, Sean. Zero trust architecture. Gaithersburg: National Institute of Standards and Technology, 2020. (NIST Special Publication 800-207). DOI: https://doi.org/10.6028/NIST.SP.800-207.

A Revista OWL Journal está licenciada com uma Licença Creative Commons Atribuição (CC BY)

SOUPPAYA, Murugiah; SCARFONE, Karen. Guidelines for securing wireless local area networks (WLANs). Gaithersburg: National Institute of Standards and Technology, 2012. (NIST Special Publication 800-153). DOI: https://doi.org/10.6028/NIST.SP.800-153.

SOUSA, Elender Keuly de; DIAS, Klenilmar Lopes. Robótica alternativa educacional: promovendo a inclusão e a sustentabilidade na educação. In: WORKSHOP DE INFORMÁTICA NA ESCOLA, 29., 2023. Anais [...]. Porto Alegre: Sociedade Brasileira de Computação, 2023. DOI: https://doi.org/10.5753/wie.2023.234879.

SOUZA, Elender Keuly de; DIAS, Klenilmar Lopes. Aplicação da robótica alternativa e a experimentação do laboratório remoto virtual de robótica alternativa – labRVRA. Tecnologias, Sociedade e Conhecimento, Campinas, v. 11, p. 1-4, 2026. DOI: https://doi.org/10.20396/v9065j47.

Recebido em: 12/11/2026
Aprovado em: 16/11/2026
Publicado em: 21/11/2026

A Revista OWL Journal está licenciada com uma Licença Creative Commons Atribuição (CC BY)