CARTILHA

PROJETO DE EXTENSÃO: CIDADANIA E PROTEÇÃO INTEGRAL: IMPLEMENTAÇÃO DE REDES SEGURAS E PROMOÇÃO DO ECA DIGITAL

PROJETO DE
CURRICULARIZAÇÃO DA EXTENSÃO

CIDADANIA E PROTEÇÃO INTEGRAL: Implementação de Redes Seguras e Promoção do ECA Digital

CST REDES DE COMPUTADORES

DISCIPLINA

SEGURANÇA DE REDES

Orientadores
Vivaldo de Albuquerque Pinto
Sergio de Araujo Vilela

Autores

Ane Caroline da Silva Carvalho
Cibely Souza Chuinca
Emily Soares da Silva
Fábio Júnior Gomes de Lima
Halbert Xavier da Silva
Jhon Jetson de Souza Gomes
Josiele de Aguiar Gomes Moura
Laís Cristina Domingues Marques
Magdiel da Silva Moreno Lopes
Maria Luiza Flores As
Paulo Ricardo Claro
Ramon Silas Shockness Alfonsin
Rômulo Garcia Tibúrcio
Ryan Carvalho Galvão
Ryan Ribeiro Martins
Yasmin Fernandes Pereira
Yasmin Leal de Oliveira

Apresentação

A tecnologia tem se tornado cada vez mais presente no cotidiano das instituições de ensino, contribuindo para a realização de atividades acadêmicas, administrativas e de comunicação. Com a crescente utilização de computadores, sistemas, plataformas digitais e acesso à internet, surge também a necessidade de proteger informações e recursos tecnológicos contra ameaças que podem comprometer a segurança dos dados e a continuidade dos serviços.

Diante dessa realidade, esta Cartilha Digital foi desenvolvida com o objetivo de apresentar, de forma clara e acessível, os principais conceitos, práticas e ferramentas relacionados à segurança em redes. O material reúne informações essenciais para a compreensão dos riscos existentes nos ambientes educacionais e das medidas que podem ser adotadas para prevenir incidentes e fortalecer a proteção das informações.

Ao longo desta cartilha, são abordados temas como os fundamentos da Segurança da Informação, a infraestrutura das redes, as principais ameaças e vulnerabilidades, a análise e o gerenciamento de riscos, além de boas práticas voltadas à proteção de sistemas e redes. Também são apresentados procedimentos de configuração, monitoramento, hardening de servidores, auditoria e validação das medidas de segurança implementadas.

Mais do que apresentar conceitos técnicos, este material busca incentivar a conscientização sobre a importância da segurança digital no ambiente educacional. A proteção das informações não depende apenas de tecnologias avançadas, mas também da adoção de boas práticas por todos os usuários que utilizam os recursos computacionais da instituição.

Sumário

INTRODUÇÃO

Segurança em Redes Escolares e Análise de Riscos

1 INTRODUÇÃO

A transformação digital tem promovido mudanças significativas nos ambientes educacionais, tornando as tecnologias da informação e comunicação recursos indispensáveis para o desenvolvimento das atividades pedagógicas e administrativas. Nesse contexto, as redes de computadores desempenham um papel fundamental ao possibilitar o compartilhamento de informações, o acesso à internet, a utilização de plataformas educacionais e a integração entre usuários, dispositivos e sistemas. Entretanto, à medida que a dependência dessas tecnologias aumenta, também crescem os desafios relacionados à proteção das informações e à segurança dos recursos computacionais presentes nas instituições de ensino.

As redes escolares armazenam e processam uma grande quantidade de dados, incluindo informações acadêmicas, registros administrativos e dados pessoais de alunos, professores e colaboradores. Dessa forma, torna-se essencial a adoção de práticas e mecanismos capazes de garantir a confidencialidade, a integridade e a disponibilidade dessas informações, reduzindo os riscos associados a incidentes de segurança. Além disso, o ambiente educacional apresenta características específicas que o tornam suscetível a ameaças cibernéticas, exigindo atenção especial quanto à proteção da infraestrutura tecnológica.

Diante desse cenário, este trabalho tem como objetivo apresentar os principais conceitos relacionados à segurança em redes escolares, abordando aspectos fundamentais para a proteção dos ativos de informação e para a manutenção da continuidade dos serviços tecnológicos nas instituições de ensino. Inicialmente, são discutidos os fundamentos da segurança da informação e os princípios que orientam a proteção dos dados. Em seguida, são apresentados os elementos que compõem a infraestrutura de redes escolares, incluindo equipamentos, segmentação e mecanismos de controle de acesso.

Posteriormente, são analisadas as principais ameaças e vulnerabilidades presentes em ambientes educacionais, bem como os conceitos relacionados à análise e ao gerenciamento de riscos em segurança da informação. Por fim, são apresentadas medidas de proteção e boas práticas que podem ser adotadas pelas instituições de ensino para fortalecer a segurança de suas redes e minimizar os impactos causados por incidentes cibernéticos.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 Fundamentos de Segurança em Redes Escolares

Nas instituições de ensino públicas e privadas, a utilização de recursos tecnológicos tornou-se essencial para apoiar as atividades acadêmicas, administrativas e de pesquisa. Nesse contexto, os órgãos responsáveis pela educação, como o Ministério da Educação (MEC), estabelecem diretrizes que orientam o funcionamento das instituições, enquanto normas técnicas e regulamentações específicas contribuem para a construção de ambientes tecnológicos seguros e adequados.

Ao projetar e implementar uma rede escolar, é fundamental garantir que a infraestrutura atenda aos requisitos de segurança, confiabilidade e desempenho

necessários para as atividades desenvolvidas pela instituição. Isso inclui a utilização de equipamentos adequados para laboratórios, salas de aula, ambientes administrativos e projetos de pesquisa, bem como dispositivos de telecomunicações devidamente certificados pela Agência Nacional de Telecomunicações (Anatel), órgão responsável pela regulamentação desses equipamentos no Brasil.

Além da proteção da infraestrutura física e dos equipamentos, a segurança das redes escolares também envolve a proteção das informações armazenadas e compartilhadas nos sistemas institucionais. Dados acadêmicos, documentos administrativos, informações pessoais de estudantes e professores e conteúdos educacionais devem ser protegidos por meio de controles de acesso, políticas de segurança e mecanismos de proteção que garantam a confidencialidade, a integridade e a disponibilidade das informações.

2.1.1 Conceito de Segurança da Informação

A segurança da informação consiste no conjunto de práticas, políticas, procedimentos, mecanismos e tecnologias destinados à proteção das informações contra acessos não autorizados, alterações indevidas, vazamentos, perdas ou qualquer incidente que possa comprometer sua confidencialidade, integridade e disponibilidade. Isso corrobora as leis da legislação para a tecnologia da informação (TI).

2.1.2 Conceito de Legislação de TI

A Legislação de Tecnologia da Informação (TI) corresponde ao conjunto de leis, normas e regulamentações que orientam o uso, a proteção e o tratamento das informações em ambientes digitais. Seu objetivo é garantir que organizações e usuários utilizem os recursos tecnológicos de forma segura, ética e em conformidade com a legislação vigente, protegendo dados, sistemas e direitos dos cidadãos.

No contexto da segurança da informação, a legislação de TI estabelece diretrizes relacionadas à privacidade, proteção de dados pessoais, utilização da internet, crimes cibernéticos e responsabilidade sobre as informações armazenadas e compartilhadas por meio de sistemas computacionais.

As instituições de ensino devem observar essas normas, pois realizam diariamente o tratamento de dados pessoais de estudantes, responsáveis, professores e servidores. Para atender às exigências legais, as escolas devem adotar medidas de segurança que garantam a proteção dessas informações, controlar o acesso aos sistemas institucionais, manter os dados atualizados e armazená-los de forma segura.

Entre as principais legislações aplicáveis ao ambiente escolar destacam-se a Lei Geral de Proteção de Dados Pessoais (LGPD), que regulamenta o tratamento de dados pessoais, e o Estatuto da Criança e do Adolescente (ECA), complementado pela Lei nº 14.811/2024, que fortalece a proteção de crianças e adolescentes no ambiente digital.

Dessa forma, o cumprimento da legislação de TI não se limita apenas à adoção de tecnologias de segurança, mas também à implementação de políticas, procedimentos e boas práticas que contribuam para a proteção das informações e para a construção de um ambiente digital seguro para toda a comunidade escolar.

2.1.3 Princípios da Confidencialidade, Integridade e Disponibilidade (CID)

A Tríade CID é formada por três princípios fundamentais da Segurança da Informação: Confidencialidade, Integridade e Disponibilidade. Esses princípios servem como base para a proteção das informações em ambientes digitais e físicos, garantindo que os dados sejam utilizados de forma segura e adequada.

A confidencialidade garante que as informações sejam acessadas apenas por pessoas autorizadas, evitando a divulgação indevida de dados. A integridade assegura que as informações permaneçam corretas, completas e sem alterações não autorizadas durante seu armazenamento ou transmissão. Já a disponibilidade garante que os dados e sistemas estejam acessíveis sempre que forem necessários aos usuários autorizados.

No ambiente escolar, esses princípios podem ser observados em diversas situações do cotidiano. A confidencialidade protege dados pessoais de alunos, professores e servidores, impedindo que pessoas não autorizadas tenham acesso a essas informações. A integridade garante que notas, frequências, históricos escolares e documentos acadêmicos não sejam alterados indevidamente. Por sua vez, a disponibilidade assegura que sistemas acadêmicos, plataformas de aprendizagem, bibliotecas digitais e demais recursos tecnológicos estejam acessíveis quando necessários para o desenvolvimento das atividades educacionais.

Dessa forma, a aplicação da Tríade CID contribui para a proteção das informações e para a manutenção de um ambiente digital seguro, confiável e adequado às necessidades da comunidade escolar.

2.1.4 Importância da Segurança em Ambientes Educacionais

No ambiente escolar, a segurança da informação assume papel fundamental, pois as instituições de ensino armazenam e processam uma grande quantidade de dados pessoais de estudantes, professores, servidores e responsáveis. Esses dados estão presentes em diversos sistemas e serviços, como ambientes virtuais de aprendizagem, portais acadêmicos, sistemas de matrícula, fóruns educacionais, calendários acadêmicos e plataformas para solicitação de documentos e requerimentos.

Dessa forma, as instituições de ensino devem adotar medidas de segurança adequadas e atuar em conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD), garantindo a proteção das informações sob sua responsabilidade. A ausência de mecanismos de segurança nas redes e sistemas institucionais pode resultar no vazamento de dados, no comprometimento da privacidade dos usuários e em prejuízos às atividades acadêmicas e administrativas da comunidade escolar.

A adoção dessas medidas é especialmente importante em ambientes educacionais, onde são armazenadas informações de crianças, adolescentes, professores e demais membros da comunidade escolar.

2.1.5 Principais Ativos de Informação em uma Rede Escolar

Os ativos de informação correspondem a todos os recursos que possuem valor para a instituição de ensino e que, por esse motivo, devem ser protegidos contra acessos não autorizados, perdas, alterações indevidas ou indisponibilidade. Em uma rede escolar, esses ativos não se limitam apenas às informações armazenadas, mas também incluem os recursos tecnológicos responsáveis por seu processamento, armazenamento e transmissão.

Entre os principais ativos de informação de uma instituição de ensino estão os sistemas acadêmicos, ambientes virtuais de aprendizagem, portais institucionais, fóruns educacionais, bancos de dados, servidores, equipamentos de rede, computadores, dispositivos móveis e as próprias informações de alunos, professores, responsáveis e servidores administrativos.

A identificação e a proteção desses ativos são fundamentais para garantir a continuidade das atividades educacionais, a privacidade dos usuários e a segurança das informações armazenadas e compartilhadas no ambiente escolar. O modelo PMBOK pode ser utilizado como referência para a identificação e classificação dos ativos presentes em uma rede escolar, auxiliando no gerenciamento dos riscos associados à infraestrutura tecnológica. Por meio de suas práticas de gerenciamento de riscos, é possível identificar ameaças e vulnerabilidades, avaliar seus impactos e definir medidas de mitigação adequadas, contribuindo para a segurança e a continuidade dos serviços oferecidos pela instituição de ensino. Com isso, conforme demonstrado na Figura 1, nota-se os ativos de uma rede escolar e seus principais riscos conforme a abordagem de identificação e gerenciamento de riscos inspirada nas práticas descritas pelo Guia PMBOK.

Figura 1 - Ativos de uma Rede Escolar

TABELA 1 **PRINCIPAIS ATIVOS DE INFORMAÇÃO EM UMA REDE ESCOLAR**

Identificação dos ativos de informação de acordo com as boas práticas de gerenciamento de projetos (PMBOK®).

CATEGORIA DO ATIVO	ATIVO	DESCRIÇÃO	IMPORTÂNCIA PARA A INSTITUIÇÃO	EXEMPLOS	NÍVEL DE CRITICIDADE*
DADOS	Dados dos alunos e responsáveis	Informações pessoais, documentos, matrículas e registros acadêmicos.	Garantir a privacidade, a segurança das informações e o cumprimento da LGPD.	Nome, CPF, endereço, contato, histórico escolar, autorizações.	ALTA
	Dados de professores e servidores	Informações funcionais, cadastrais e administrativas.	Apoiar a gestão acadêmica e administrativa da instituição.	Dados pessoais, cargos, salários, formação, avaliações.	ALTA
	Dados acadêmicos e administrativos	Notas, frequências, planos de ensino, relatórios, documentos institucionais.	Essenciais para a tomada de decisão e prestação de contas.	Boletins, atas, planos, relatórios gerenciais.	MÉDIA
SISTEMAS E APLICAÇÕES	Sistema Acadêmico	Plataforma para matrículas, notas, frequência e histórico escolar.	Essencial para a gestão escolar e acompanhamento dos alunos.	Sistemas ERP educacionais, módulos acadêmicos.	ALTA
	Ambiente Virtual de Aprendizagem (AVA)	Plataforma utilizada para atividades educacionais online.	Suporte ao ensino e aprendizagem, com interação e conteúdos digitais.	Moodle, Google Classroom, Microsoft Teams.	MÉDIA
	Portal Institucional e Sites	Site oficial e sistemas de comunicação da instituição.	Divulgação de informações, serviços e comunicação.	Site institucional, área do aluno, área do professor.	MÉDIA
	Fóruns e Comunidades Educacionais	Ambientes colaborativos para interação entre alunos e professores.	Fomentar a colaboração, o compartilhamento de conhecimento e a aprendizagem.	Fóruns de discussão, grupos de estudo online.	BAIXA
INFRAESTRUTURA DE TI	Servidores	Equipamentos responsáveis pelo armazenamento e processamento de dados.	Garantem a disponibilidade dos sistemas e dados institucionais.	Servidores físicos, máquinas virtuais.	ALTA
	Equipamentos de Rede	Dispositivos que permitem a comunicação e o tráfego de dados.	Essenciais para a conectividade e o funcionamento da rede.	Switches, roteadores, firewalls, access points.	MÉDIA
	Estações de Trabalho e Dispositivos	Computadores, notebooks, tablets e outros dispositivos utilizados na instituição.	Permitem a execução das atividades acadêmicas e administrativas.	PCs administrativos, notebooks de professores, tablets de alunos.	MÉDIA
	Conexão com a Internet	Serviço de comunicação com redes externas.	Necessária para acesso a recursos educacionais e administrativos.	Links dedicados, banda larga, provedores de internet.	MÉDIA
SEGURANÇA DA INFORMAÇÃO	Contas de Usuários	Credenciais de acesso aos sistemas e recursos institucionais.	Controlam o acesso às informações de acordo com o perfil do usuário.	Contas de alunos, professores, administradores.	ALTA
	Senhas e Credenciais	Mecanismos de autenticação dos usuários.	Protegem contra acessos não autorizados.	Senhas, tokens, autenticação de dois fatores.	ALTA
	Backups	Cópias de segurança dos dados e sistemas institucionais.	Garantem a recuperação de informações em caso de falhas ou incidentes.	Backups locais, backups em nuvem.	ALTA

* Nível de criticidade: avaliação do impacto do ativo caso ocorra perda, indisponibilidade ou comprometimento.

ALTA MÉDIA BAIXA

Fonte: Elaborado pelos Autores (2026).

2.2 Infraestrutura de Redes Escolares

A infraestrutura de redes escolares constitui o alicerce técnico e estratégico indispensável para a operação das instituições de ensino contemporâneas, atuando como suporte para a convergência de sistemas pedagógicos e administrativos. Com a digitalização crescente, a rede deixa de ser um mero utilitário para se tornar a base tecnológica que garante o acesso a serviços digitais e o armazenamento centralizado de informações. Segundo o Plano Estratégico de TIC (PETI 2025-2028), essa infraestrutura deve ser gerida para assegurar a disponibilidade dos ambientes e a segurança das conexões, sendo um pilar para a promoção da educação digital.

2.2.1 Estrutura e Interconexão de Dispositivos

A composição de uma rede escolar caracteriza-se pela heterogeneidade de dispositivos interconectados, incluindo estações de trabalho, servidores, notebooks, tablets e smartphones. Essa estrutura permite que recursos físicos e lógicos sejam compartilhados eficientemente, processando inúmeros sistemas que gerenciam as atividades de cada setor da instituição. Nesse ecossistema, os servidores assumem um papel central, sendo responsáveis pelo gerenciamento de identidades, hospedagem de aplicações institucionais e controle de serviços essenciais. A robustez dessa arquitetura é vital, pois a carência de planejamento e manutenção pode levar à subutilização de laboratórios e à fragilidade dos serviços oferecidos à comunidade escolar.

2.2.2 Equipamentos Fundamentais e suas Funções

Para viabilizar a comunicação, a infraestrutura depende de equipamentos com funções técnicas distintas nas camadas de conectividade. Os switches são responsáveis pela interligação direta dos equipamentos dentro de uma rede local (LAN), permitindo a troca de dados de forma comutada e eficiente. Para a comunicação externa, utilizam-se os roteadores, que gerenciam o fluxo de tráfego e interligam a rede interna à internet de maneira controlada. Complementando a estrutura, os pontos de acesso sem fio (APs) estendem a conectividade via Wi-Fi, provendo a mobilidade necessária para que o aprendizado ocorra em diferentes espaços físicos da escola.

2.2.3 Segmentação Lógica e Otimização da Rede

Um dos pilares de uma arquitetura segura é a segmentação de rede, técnica que divide a infraestrutura física em áreas lógicas distintas, independentes da topologia física. A utilização de VLANs (Virtual Local Area Networks) permite isolar o tráfego de diferentes perfis, como o administrativo, docentes e discentes, garantindo que informações sigilosas de um setor não sejam acessíveis por usuários não autorizados de outro segmento. Além de otimizar o desempenho ao reduzir o congestionamento de pacotes broadcast, a segmentação é vital para a segurança, pois limita o "raio de alcance" de possíveis incidentes: caso um segmento de alunos seja comprometido por um vírus, a propagação para servidores administrativos sensíveis é dificultada.

2.2.4 Controle de Acesso e Proteção de Ativos

O controle de acesso à rede estabelece as barreiras necessárias para garantir que apenas entidades autorizadas utilizem os recursos institucionais. Isso envolve a implementação de mecanismos robustos de Gestão de Identidade e Acesso (IAM), que verificam credenciais e restringem permissões conforme as atribuições funcionais de cada usuário. A adoção de políticas rigorosas de autenticação e o cadastro de dispositivos mitigam riscos de acessos indevidos e uso não autorizado de informações sensíveis. Conforme orienta o Centro de Inovação para a Educação Brasileira (CIEB), esses controles são fundamentais para que as secretarias de educação estejam em conformidade com a Lei Geral de Proteção de Dados (LGPD), zelando pela privacidade de crianças e adolescentes.

2.2.5 A Infraestrutura como Pilar da Segurança da Informação

Em última análise, uma infraestrutura de rede bem planejada é o principal vetor de fortalecimento da segurança da informação escolar. O Laboratório Nacional de Computação Científica (LNCC) enfatiza que uma gestão eficaz e a conformidade com requisitos técnicos são essenciais para proteger os ativos digitais contra ameaças crescentes, como o ransomware.

Ao integrar equipamentos apropriados, segmentação lógica e controle rigoroso de acesso, a instituição preserva o tripé da confidencialidade, integridade e disponibilidade. Assim, a rede deixa de ser apenas um meio de conexão e torna-se um componente estratégico que garante a continuidade das atividades educacionais e a sustentabilidade institucional frente aos desafios do mundo conectado.

2.3 Ameaças e Vulnerabilidades em Redes Escolares

O ecossistema escolar abriga vulnerabilidades técnicas e comportamentais específicas que são exploradas sistematicamente por atacantes cibernéticos. A relação de risco envolvida na segurança de uma rede escolar pode ser formalizada por meio de uma equação matemática de risco absoluto (R), determinada pelo produto da probabilidade de ocorrência de uma Ameaça ativa (A), da taxa de Vulnerabilidades de sistema e comportamento existentes (V) e da Severidade do Impacto gerado no funcionamento da instituição de ensino (I): **R=A×V×I**

No ambiente educacional de nível básico, o fator V (Vulnerabilidade) é expandido pela diversidade de perfis de usuários acessando a rede ao mesmo tempo. Muitos alunos jovens não possuem discernimento sobre engenharia social e consentem facilmente com termos de uso intrusivos ao instalar aplicativos de entretenimento ou utilitários Essa falta de conscientização se traduz em uma exposição diária a golpes eletrônicos via canais digitais variados. O fator de impacto I também é severo, uma vez que dados de menores de idade, quando vazados, permanecem utilizáveis para fins ilícitos, como a abertura de linhas de crédito fraudulentas, por períodos de tempo muito maiores do que os dados de adultos, que monitoram seus extratos financeiros com maior regularidade.

Em termos de investimentos e custos associados a essas vulnerabilidades, a edição de 2025 do relatório do Consortium for School Networking (CoSN) apontou que mais de 78% dos líderes de tecnologia em educação entrevistados relataram que suas instituições estão realizando investimentos dedicados em monitoramento, detecção e resposta a incidentes de segurança. No entanto, esses orçamentos continuam sob severa pressão devido à escalada contínua nos prêmios de seguros cibernéticos e nos custos diretos de contratação de serviços técnicos especializados de proteção.

Para compreender detalhadamente a dinâmica das ameaças mais comuns encontradas nas redes de ensino básico, a tabela abaixo categoriza as principais ocorrências e seus impactos correspondentes:

Tabela 1 - Ameaças e Vulnerabilidade

Tipo de Vetor de Ataque	Mecanismo de Exploração Técnica	Impacto Operacional e Financeiro no Ambiente Escolar
Ransomware	Infiltração na rede interna para criptografar bases de dados de estudantes e servidores administrativos vitais.	Paralisação total das atividades administrativas e acadêmicas, extorsão financeira e vazamento de dados caso o resgate não seja pago.
Phishing / Smishing / Vishing	Envio de mensagens de correio eletrônico, SMS ou chamadas telefônicas fraudulentas imitando comunicações oficiais da escola.	Captura de credenciais de acesso de docentes e funcionários administrativos para invasão de contas com altos privilégios.
Vulnerabilidades	Exploração de	Acesso não autorizado

Conhecidas Não Corrigidas	falhas públicas de segurança em servidores web e dispositivos de rede desprovidos de patches de correção. [4]	ao núcleo da infraestrutura escolar e implantação de spywares de coleta silenciosa de informações.
Vazamento e Exposição de Dados	Coleta inadequada e vazamento de registros confidenciais decorrente de más configurações de privacidade em aplicativos de terceiros.	Comprometimento permanente de históricos escolares e dados médicos, resultando em multas e processos judiciais.

Fonte: Elaborado pelos Autores (2026).

2.4 Análise e Gerenciamento de Riscos

O gerenciamento de riscos em instituições de ensino evoluiu de uma preocupação meramente técnica para um componente estratégico essencial à sustentabilidade e à credibilidade institucional. Dada a crescente digitalização e a manipulação de grandes volumes de dados sensíveis, a análise sistemática de ameaças torna-se indispensável para garantir a continuidade das atividades pedagógicas e administrativas.

2.4.1 Conceito de Risco em Segurança da Informação

No âmbito da cibersegurança, o risco é definido como a probabilidade de uma ameaça explorar uma vulnerabilidade, resultando em impactos negativos sobre os sistemas e as pessoas. A gestão desse risco visa proteger os ativos digitais contra acessos não autorizados e garantir a preservação do tripé CID (Confidencialidade, Integridade e Disponibilidade). Conforme a perspectiva do NIST (National Institute of Standards and Technology), a maturidade organizacional nesse campo está associada ao grau de institucionalização das práticas de gestão de riscos, variando desde um estágio parcial até processos adaptativos e contínuos.

2.4.2 Identificação de Ameaças e Vulnerabilidades

As instituições de ensino tornaram-se alvos preferenciais de ataques devido à alta concentração de informações pessoais de menores e de seus responsáveis. Entre as principais ameaças identificadas, destacam-se o ransomware — com elevadas taxas de pagamento de resgate no setor educacional —, o phishing, ataques de comprometimento de e-mail corporativo (BEC) e o uso de softwares de acesso remoto maliciosos (RATs).

Simultaneamente, o ambiente escolar apresenta vulnerabilidades críticas, como a operação híbrida de sistemas legados e tecnologias recentes, o uso intensivo de redes descentralizadas e a utilização de dispositivos pessoais pelos usuários. A

carência de planejamento de infraestrutura e a ausência de políticas estruturadas de proteção de dados ampliam significativamente a exposição a riscos digitais nessas instituições.

2.4.3 Avaliação de Impacto e Probabilidade

A avaliação de riscos deve mensurar o potencial de danos, que no contexto educacional ultrapassam a esfera operacional. Sob a ótica econômica, os custos médios de uma violação de dados podem atingir cifras milionárias, comprometendo recursos que seriam destinados à educação. Além dos prejuízos financeiros e jurídicos decorrentes da Lei Geral de Proteção de Dados (LGPD), os incidentes geram perdas de imagem e de confiança, ativos considerados valiosos para qualquer escola. No diagnóstico de maturidade, muitas redes de ensino situam-se no nível "Informado por Risco", onde, embora as ameaças sejam reconhecidas pela administração, as medidas de mitigação ainda carecem de formalização plena como políticas organizacionais.

2.4.4 Métodos Básicos de Análise de Riscos

Para uma gestão eficaz, recomenda-se a adoção de abordagens estruturadas e diagnósticos sistemáticos. A utilização de frameworks reconhecidos internacionalmente, como o NIST CSF 2.0, permite organizar a defesa em seis dimensões: identificar, proteger, detectar, responder, recuperar e governança.

Entre os métodos fundamentais, destacam-se:

- Inventário e Gestão de Ativos: A realização de um levantamento rigoroso de hardware e software é o passo primário para identificar portas de entrada para ameaças.
- Gestão de Riscos na Cadeia de Suprimentos: Envolve a classificação e supervisão de fornecedores e integradores de tecnologia, evitando que falhas em agentes externos comprometam a rede interna.
- Planejamento Estratégico de TIC (PETI): O estabelecimento de diretrizes de governança e o monitoramento de Resultados-Chave (KRs) asseguram que a segurança esteja alinhada aos objetivos educacionais da instituição.
- Monitoramento Contínuo: A implementação de mecanismos de detecção em tempo real e planos de recuperação de desastres garantem a resiliência institucional frente a incidentes inevitáveis.

2.5 Medidas de Proteção e Boas Práticas

A implementação de medidas de proteção em redes escolares deve ser compreendida como um esforço multidimensional que integra tecnologia, processos e pessoas para criar um ambiente digital resiliente. Dada a crescente vulnerabilidade do setor educacional a ataques como o ransomware, a adoção de posturas defensivas estruturadas deixa de ser opcional para se tornar um requisito de continuidade das atividades pedagógicas. Conforme o Cybersecurity Framework 2.0 (NIST), a proteção eficaz depende da capacidade institucional de mitigar riscos previamente identificados por meio de controles técnicos e normativos.

2.5.1 Políticas de Segurança

A base de qualquer estratégia de defesa é a Política de Segurança da Informação (PSI), um documento que formaliza as diretrizes, normas e responsabilidades no uso dos ativos tecnológicos. No contexto escolar, a política deve definir o regramento geral de uso dos laboratórios e redes, estabelecendo, por exemplo, a proibição de instalação de softwares não autorizados e a desconexão obrigatória após o uso de sistemas. A eficácia dessa governança depende da sua integração plena à estratégia institucional, superando medidas puramente reativas para alcançar um nível de maturidade onde as práticas de segurança são formalmente institucionalizadas.

2.5.2 Firewall e Controle de Acesso

A proteção do perímetro e a segmentação interna são executadas por meio de ferramentas como firewalls (incluindo sistemas de detecção e prevenção de intrusão - IDS/IPS) e o controle rigoroso de acesso. A utilização de VLANs (Virtual Local Area Networks) destaca-se como uma prática técnica essencial, pois permite a segmentação lógica da rede física, isolando o tráfego de alunos, professores e setores administrativos. Essa arquitetura garante que, em caso de infecção por vírus em um dispositivo de laboratório, a ameaça não se propague para os servidores que contêm informações sensíveis. Complementarmente, sistemas de Gestão de Identidade e Acesso (IAM) asseguram que apenas usuários autenticados acessem recursos específicos, reduzindo a superfície de ataque para acessos não autorizados.

2.5.3 Backup e Recuperação de Dados

O backup é o recurso crítico para garantir a disponibilidade e a integridade das informações frente a incidentes graves ou falhas de hardware. As instituições de ensino devem estabelecer rotinas de backups automatizados e, preferencialmente, armazenar cópias em ambientes externos ou em nuvem para facilitar a restauração rápida de dados. A existência de um plano de recuperação de desastres é vital, detalhando as medidas a serem seguidas para restaurar a infraestrutura de TI e os sistemas críticos no menor tempo possível. Essa capacidade de restauração estruturada é a última linha de defesa contra o sequestro de dados e garante a resiliência institucional.

2.5.4 Conscientização e Treinamento de Usuários

O comportamento humano é frequentemente apontado como o elo mais frágil da segurança cibernética, sendo o principal vetor para ataques de phishing e engenharia social. Portanto, programas de treinamento e campanhas de conscientização são fundamentais para educar a comunidade escolar sobre o uso ético e seguro da tecnologia. Esse esforço deve abranger desde noções básicas de segurança na internet para alunos até orientações técnicas para professores e administrativos sobre a criação de senhas fortes e identificação de comunicações maliciosas. A educação digital é, assim, uma ferramenta de proteção dos direitos individuais e da privacidade de crianças e adolescentes, em conformidade com a LGPD.

2.5.5 Recomendações para Melhoria da Segurança em Escolas

Para elevar o nível de maturidade em cibersegurança, recomenda-se que as instituições escolares sigam um roteiro estruturado de melhoria contínua:

- Inventário de Ativos: Realizar um levantamento rigoroso de hardware e software para identificar vulnerabilidades em sistemas legados.
- Gestão de Vulnerabilidades: Implementar monitoramento contínuo, atualizações periódicas de firmware e realização de testes de intrusão (Pentests) para identificar portas de entrada para ameaças.
- Governança da Cadeia de Suprimentos: Estabelecer critérios formais para a classificação e supervisão de fornecedores de tecnologia, garantindo que agentes externos não comprometam a segurança interna.
- Conformidade Legal: Ajustar todos os processos de tratamento de dados pessoais às exigências da Lei Geral de Proteção de Dados, zelando pela transparência e pelo consentimento no uso das informações da comunidade escolar.

Essas ações permitem que a escola transite de uma postura "informada por risco" para um estágio de defesa proativa e resiliente, assegurando que a tecnologia cumpra seu papel como facilitadora da aprendizagem com a máxima segurança possível

CONFIGURAÇÃO E IMPLEMENTAÇÃO

Configuração Inicial do firewall, Implementação e amostra de evidências técnicas.

3 CONFIGURAÇÃO

Neste projeto foi utilizado o **UFW (Uncomplicated Firewall)**, ferramenta nativa do Debian que permite a implementação de políticas de segurança de forma simples e eficiente. Antes da aplicação das regras, foi realizada uma análise dos serviços necessários para o funcionamento do servidor, permitindo a definição das portas que deveriam permanecer acessíveis.

Com base nessa avaliação, adotou-se uma política de segurança fundamentada no princípio do menor privilégio, permitindo apenas os serviços essenciais para a hospedagem e administração. Também foram habilitados mecanismos de monitoramento e auditoria para registrar eventos relacionados à segurança e identificar possíveis tentativas de acesso não autorizado.

3.1 Comandos da Evidência: Configuração Inicial do Firewall e Proteção da Rede

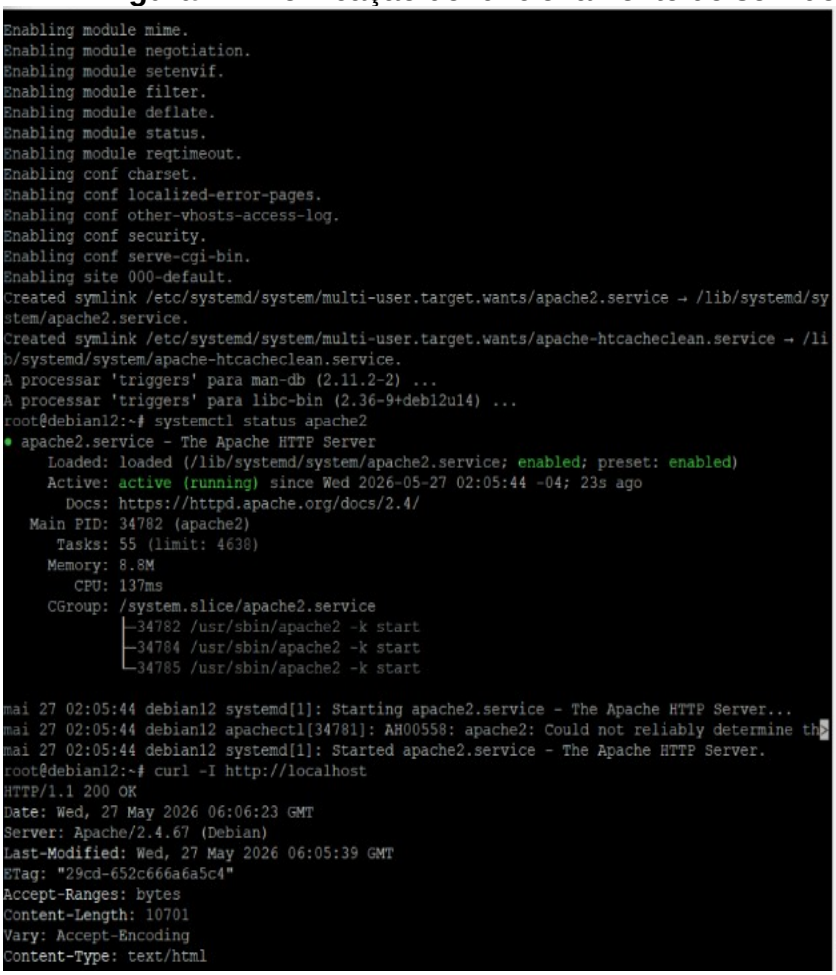
A disponibilização da cartilha requer um serviço para hospedar as páginas:

● apt install apache2 -y: Baixa e instala o Apache, um dos servidores web mais utilizados e estáveis do mercado.

● systemctl status apache2: Consulta o gerenciador de serviços do sistema para confirmar se o Apache iniciou corretamente e está ativo ("running").

● curl -I http://localhost: Ferramenta de linha de comando que simula um navegador. O parâmetro -I solicita apenas o cabeçalho da página local, verificando se o servidor responde com o código HTTP "200 OK" (sucesso).

Figura 2 – Verificação do funcionamento do servidor.



Fonte: Elaborado pelos autores (2026).

3. 1.1 Evidências Técnicas

A proteção das portas de entrada do servidor é controlada pelo Uncomplicated Firewall (UFW):

● ufw default deny incoming / allow outgoing: Define a política restritiva padrão. Tudo que tenta entrar no servidor é bloqueado, mas o servidor tem permissão para acessar a internet (para baixar atualizações, por exemplo).

● ufw allow 22/tcp, 80/tcp, 443/tcp: Abre exceções pontuais e exclusivas no firewall. A porta 22 garante o acesso remoto seguro via SSH para a administração, enquanto as portas 80 e 443 permitem que os usuários acessem a cartilha digital via **HTTP e HTTPS.**

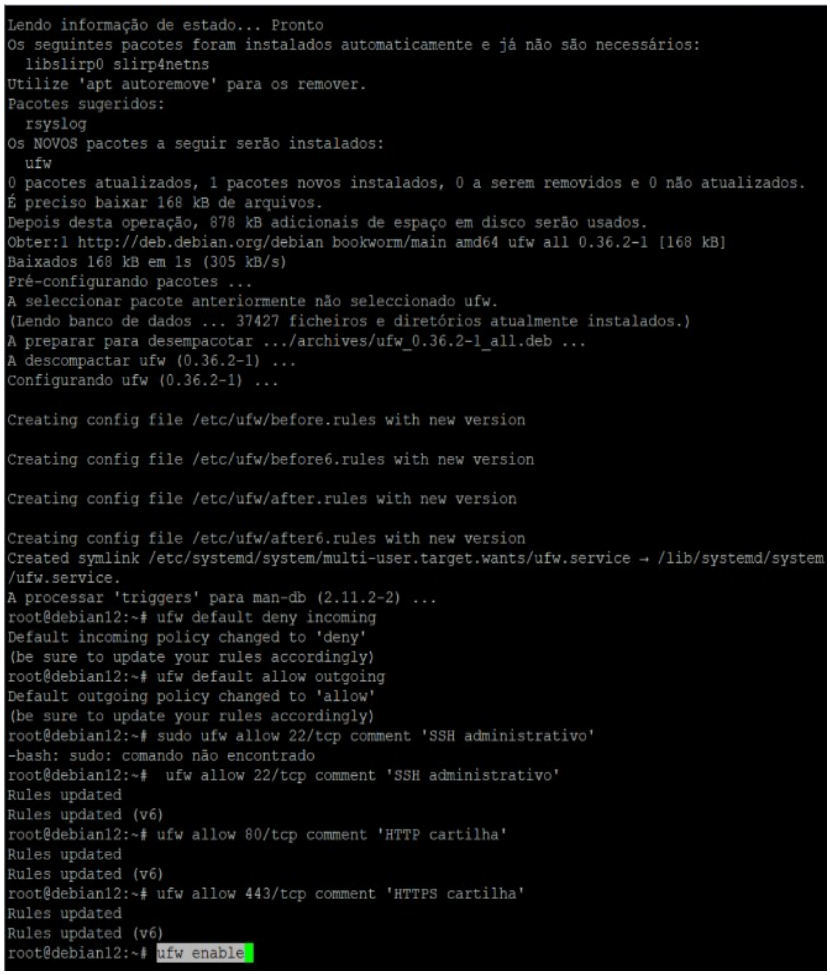
● ufw enable: Ativar o firewall com as regras configuradas.

● ufw status numbered: Exibe uma lista enumerada e organizada de todas as regras ativas, facilitando a auditoria.

Figura 3 – Configuração das políticas padrão do firewall UFW

Fonte: Elaborado pelos autores (2026).

Figura 4 – Configuração das regras de acesso do firewall UFW para os serviços SSH, HTTP e HTTPS.



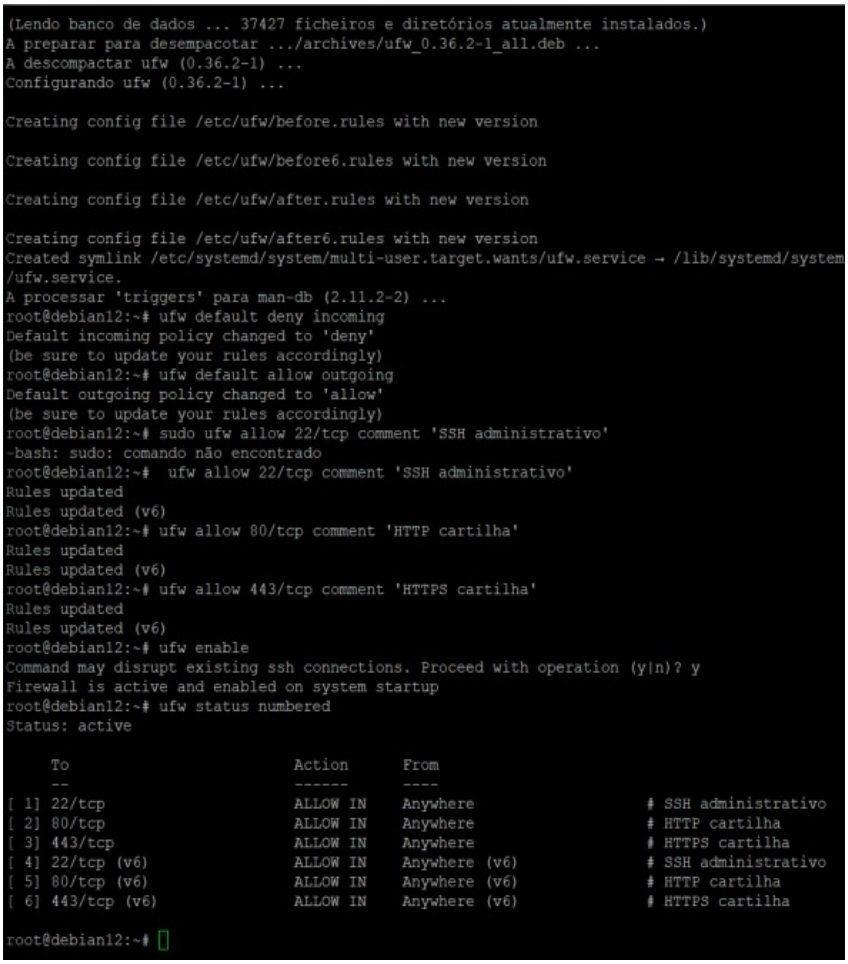
Fonte: Elaborado pelos autores (2026)

3.1.2 Comandos da Evidência: Estrutura e Permissões Seguras

Para evitar que invasores modifiquem os arquivos da cartilha, aplica-se o controle rigoroso de permissões Linux:

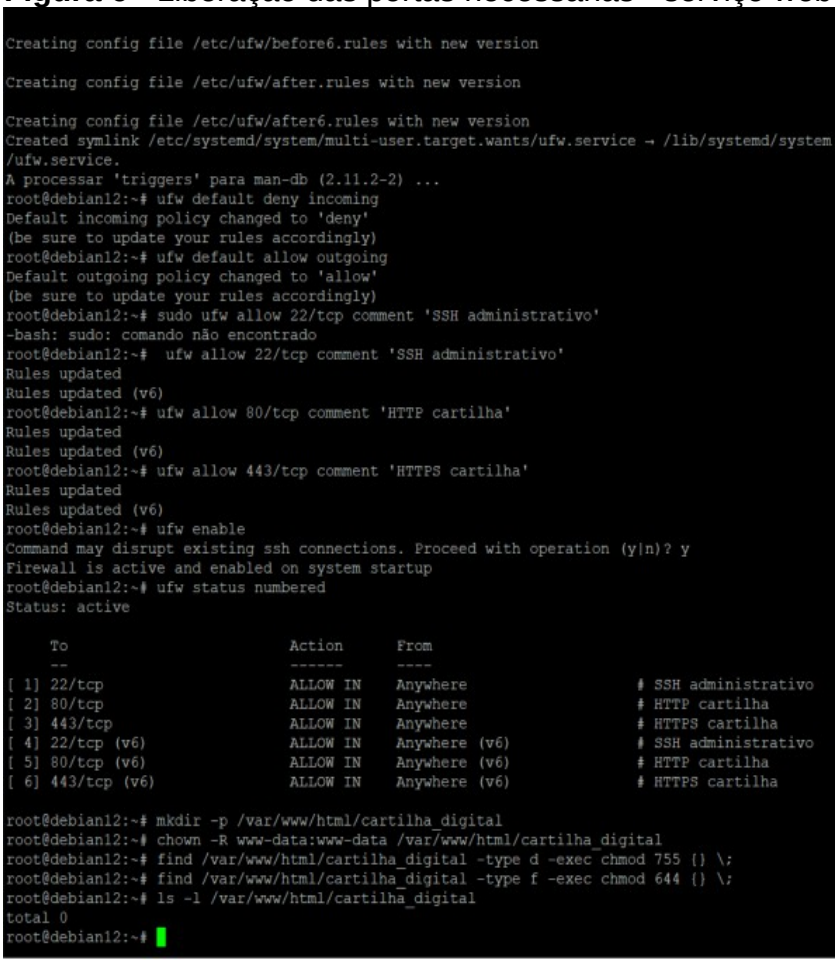
- mkdir -p /var/www/html/cartilha digital: Cria a estrutura de diretórios onde os arquivos do site serão armazenados.
- chown -R www-data:www-data: Transfere a propriedade de toda a pasta (de forma recursiva) para o usuário padrão do servidor web (www-data), isolando-a de outros usuários do sistema.
- find ... -type d -exec chmod 755 {} \;: Localiza todos os diretórios (-type d) da cartilha e aplica a permissão 755 (apenas o dono pode alterar; Os visitantes só podem ler e acessar a pasta).
- find ... -type f -exec chmod 644 {} \;: Localiza todos os arquivos (-type f) e aplica a permissão 644 (apenas o dono pode editar; os visitantes podem apenas ler o conteúdo).
- ls -l: Lista o conteúdo do diretório exibindo detalhadamente as permissões e os proprietários configurados.

Figura 5 - Liberação das portas necessárias - serviço web ativo.



Fonte: Elaborado pelos autores (2026)

Figura 6 - Liberação das portas necessárias - serviço web ativo.



Fonte: Elaborado pelos autores (2026)

3.1.3 Comandos da Evidência: Hardening SSH, Portas e Logs

A etapa final de auditoria comprova a eficácia das configurações de segurança:

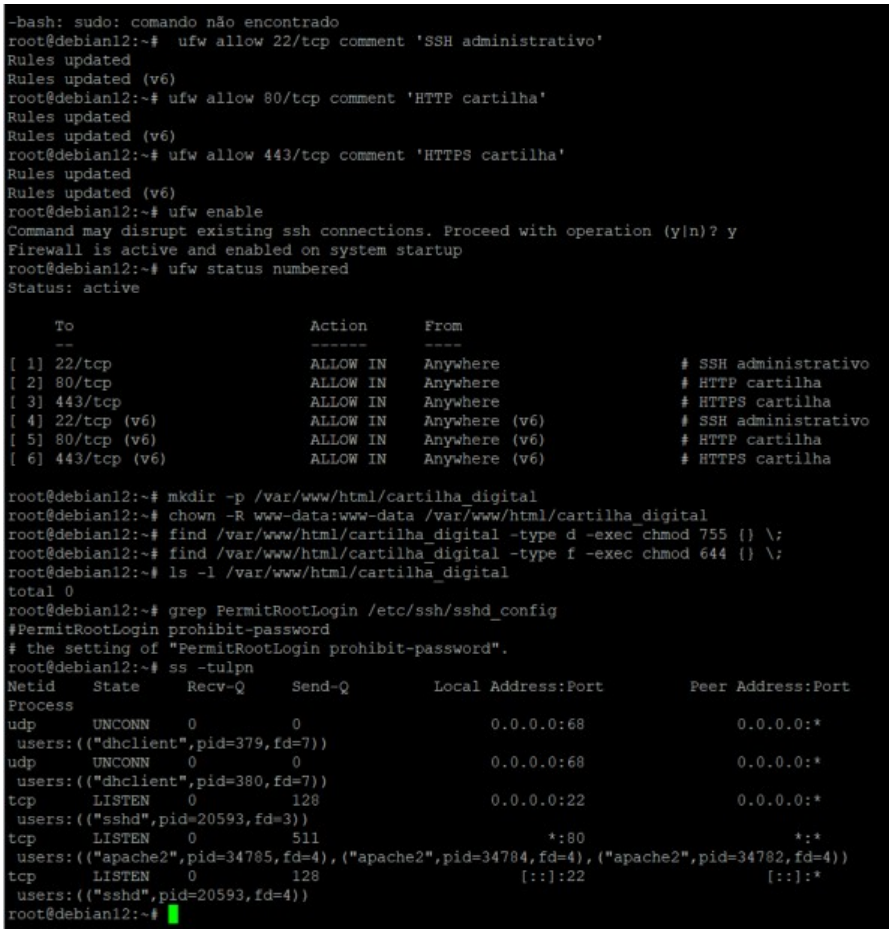
● grep PermitRootLogin /etc/ssh/sshd_config: Busca no arquivo de configuração do SSH a diretriz que bloqueia o acesso remoto direto com o usuário administrador (root). Essa é uma prática essencial para evitar ataques de força bruta.

● ss -tulpn: Mapeia e exibe todas as portas (TCP e UDP) que estão abertas e "escutando" no servidor, provando que apenas os serviços estritamente necessários estão rodando.

● journalctl -u apache2 --since today: Filtra os registros gerais (logs) do sistema para exibir apenas os eventos e mensagens de status gerados pelo servidor web no dia atual.

● tail -n 10 /var/log/apache2/access.log: Lê as 10 últimas linhas do arquivo de log de acessos, permitindo rastrear os endereços IP dos dispositivos que visitaram a cartilha digital e o horário da requisição.

Figura 7 - A verificação das portas ativas



Fonte: Elaborado pelos autores (2026)

3.2. OBJETIVO DO FIREWALL

O firewall é uma ferramenta de segurança responsável por controlar o tráfego de dados que entra e sai da rede. Seu principal objetivo é impedir acessos não autorizados, proteger informações sensíveis e reduzir os riscos de ataques cibernéticos.

No ambiente escolar, o firewall auxilia na proteção dos sistemas acadêmicos, servidores, computadores administrativos e demais recursos tecnológicos utilizados pela instituição.

3.2.1 Atualização Inicial do Sistema Debian

Antes da implementação das medidas de segurança, foi realizada a atualização completa do sistema operacional Debian. Essa etapa é fundamental para corrigir vulnerabilidades conhecidas e garantir que o servidor esteja utilizando versões atualizadas dos pacotes instalados. A atualização do sistema contribui para a estabilidade da plataforma e reduz significativamente os riscos de exploração por atacantes.

3.2.2 Levantamento dos Serviços Necessários

Após a atualização, foi realizada uma análise dos serviços que deveriam permanecer ativos no servidor. Esse procedimento permitiu identificar quais aplicações realmente necessitavam de acesso à rede.

A identificação correta dos serviços evita a exposição desnecessária de portas e reduz a superfície de ataque do ambiente computacional.

3.2.3 Configuração das Políticas de Segurança

Com base na análise realizada, foi adotada uma política de segurança fundamentada no princípio do menor privilégio. Dessa forma, apenas os serviços essenciais receberam autorização para funcionamento.

As principais configurações aplicadas foram:

- Bloqueio padrão de conexões de entrada;
- Permissão de conexões de saída;
- Liberação apenas das portas necessárias;
- Restrição de acessos não autorizados;
- Registro das atividades realizadas pelo firewall.

3.2.4 Liberação de Serviços Essenciais

Alguns serviços precisaram permanecer acessíveis para garantir o funcionamento adequado do ambiente.

Entre eles destacam-se:

SSH (Secure Shell)

Utilizado para administração remota segura do servidor, permitindo que administradores autorizados realizem configurações e manutenções sem acesso físico ao equipamento.

Serviços Web

Quando necessário, foram liberadas as portas destinadas aos serviços HTTP e HTTPS, responsáveis pelo acesso a aplicações e páginas web hospedadas no servidor.

3.2.5 Monitoramento e Registro de Eventos

Uma etapa importante da configuração foi a ativação dos logs do firewall. Esses registros armazenam informações sobre conexões permitidas, bloqueadas e tentativas de acesso suspeitas.O monitoramento contínuo desses eventos auxilia na identificação de comportamentos anormais e permite respostas rápidas diante de possíveis incidentes de segurança.

3.2.6 Benefícios da Configuração Implementada

A configuração inicial do firewall proporciona diversos benefícios para a infraestrutura de rede, entre eles:

- Redução da superfície de ataque;
- Controle de acesso aos recursos da rede;
- Proteção contra acessos indevidos;
- Monitoramento de atividades suspeitas;
- Maior segurança para servidores e usuários;

- Preservação da confidencialidade, integridade e disponibilidade das informações.

Dessa forma, a configuração inicial do firewall estabelece uma base sólida para as demais medidas de segurança que serão implementadas nas próximas etapas do projeto.

PROTEÇÃO E MONITORAMENTO

Verificação das Regras de Segurança Implementadas

4 PROTEÇÃO E MONITORAMENTO

A segurança de uma rede escolar não se encerra na sua configuração inicial; ela exige acompanhamento contínuo e a garantia de que as barreiras estabelecidas estão operando conforme o esperado. Esta seção detalha as práticas recomendadas para a administração segura do ambiente e os métodos para validar a eficácia das defesas implementadas.

A proteção da rede escolar envolve a implementação de mecanismos de segurança, como firewalls, antivírus, filtros de conteúdo e controle de acesso. Essas ferramentas auxiliam na prevenção de ameaças, bloqueando sites maliciosos, softwares prejudiciais e tentativas de invasão que possam comprometer os equipamentos e as informações da instituição.

4.1 Acesso remoto e Monitoramento Básico

A administração de servidores físicos ou virtuais raramente é feita de forma local (presencial). O acesso remoto é essencial, mas deve ser tratado com rigor para não se tornar uma porta de entrada para invasores.

Além da administração remota, é importante realizar o monitoramento contínuo dos serviços e dispositivos da rede. Essa prática permite identificar falhas, indisponibilidades e possíveis tentativas de acesso não autorizado, contribuindo para a manutenção da segurança e disponibilidade dos recursos tecnológicos da instituição.

4.1.2 Implementação de Acesso Remoto Seguro (SSH)

O protocolo SSH (Secure Shell) é o padrão ouro para a administração remota, garantindo que toda a comunicação e transferência de dados entre o administrador e o servidor seja criptografada.

Para habilitar o serviço em servidores baseados na distribuição Debian, utilize os seguintes comandos no terminal:

```
# Atualizar a lista de pacotes
sudo apt update

# Instalar o servidor SSH
sudo apt install openssh-server

# Verificar se o serviço está ativo
sudo systemctl status ssh
```

Após a instalação e ativação do serviço SSH, recomenda-se realizar testes de conexão a partir de outro dispositivo da rede para confirmar o correto funcionamento do acesso remoto. Essa verificação garante que o serviço esteja disponível apenas para usuários autorizados e configurado de forma segura.

4.1.3 Boas Práticas e Hardening do SSH

Para elevar o nível de segurança, é crucial editar o arquivo de configuração (/etc/ssh/sshd_config) e aplicar as seguintes diretrizes:

Desativar o login direto do usuário root: Mude a linha para PermitRootLogin no.

Administradores devem logar com contas comuns e escalar privilégios apenas quando necessário.

Alterar a porta padrão (Opcional, mas recomendado): Mudar da porta 22 para uma porta não padronizada (ex: 2222) ajuda a reduzir ataques automatizados de força bruta.

A aplicação dessas medidas reduz significativamente a superfície de ataque do servidor, dificultando tentativas automatizadas de invasão e aumentando a proteção do ambiente computacional. A utilização de autenticação por chaves criptográficas também pode ser considerada como uma camada adicional de segurança.

4.1.4 Conexão via Cliente (Exemplo com PuTTY)

Para acessar o servidor a partir de estações de trabalho Windows, recomenda-se o uso do cliente PuTTY.

1. Abra o PuTTY.
2. No campo Host Name (or IP address), insira o endereço IP do servidor (ex: 192.168.10.10).
3. No campo Port, insira 22 (ou a porta customizada, se alterada).
4. Certifique-se de que o Connection type está marcado como SSH.
5. Clique em Open. Ao abrir o terminal, insira suas credenciais de acesso seguro.

Após o estabelecimento da conexão, o administrador poderá executar tarefas de manutenção, atualização e monitoramento do sistema de forma segura, sem a necessidade de acesso físico ao equipamento.

4.2 Verificação das Regras de Segurança Implementadas

Uma vez que as políticas de firewall estão configuradas para proteger a rede escolar, é obrigatório verificar se elas estão sendo aplicadas corretamente pelo sistema operacional. Se o servidor estiver utilizando o UFW (Uncomplicated Firewall) para gerenciar as regras de rede, a verificação pode ser feita com o comando de status detalhado:

sudo ufw status verbose

Este comando listará todas as portas permitidas e bloqueadas, além do status geral (ativo/inativo) e a política padrão (ex: negar entrada, permitir saída). Caso a

administração seja feita diretamente via iptables, a listagem das regras de forma numérica e detalhada é feita com:

sudo iptables -L -n -v

Nesta saída, observe a contagem de pacotes (pkts) e bytes. Se as regras de bloqueio estiverem funcionando, você verá esses contadores aumentarem conforme o tráfego não autorizado é descartado.

A verificação periódica das regras configuradas é fundamental para garantir que as políticas de segurança continuem funcionando corretamente após atualizações do sistema ou alterações na infraestrutura da rede. Dessa forma, é possível assegurar que apenas os serviços autorizados permaneçam acessíveis.

4.3 Validação das Configurações de Segurança

A validação não apenas atesta que a rede está segura hoje, mas ajuda a prever e mitigar problemas futuros. O monitoramento de logs é a principal ferramenta do administrador para essa tarefa.

No ambiente Debian, os eventos relacionados à segurança e tentativas de login são

registrados no arquivo auth.log. O monitoramento contínuo em tempo real pode ser feito através do comando:

```
# Acompanhar tentativas de acesso e autenticação em tempo real
sudo tail -f /var/log/auth.log
```

A validação das configurações permite identificar comportamentos suspeitos e confirmar que os mecanismos de proteção estão operando conforme planejado. Esse processo auxilia na prevenção de incidentes e fortalece a segurança geral do ambiente computacional.

4.3.1 O que procurar na validação de logs

Falhas repetidas de autenticação: Linhas indicando "Failed password for..." repetidas vezes para o mesmo usuário ou a partir do mesmo IP indicam uma possível tentativa de ataque de força bruta. Sessões abertas fora do horário escolar: Logins bem-sucedidos ("Accepted password for..." ou "session opened ") em madrugadas e finais de semana podem indicar acessos indevidos ou credenciais vazadas, exigindo investigação imediata.

Além dos eventos de autenticação, recomenda-se observar mensagens relacionadas a falhas de serviços, alterações de configuração e atividades incomuns na rede. A análise contínua dos logs contribui para uma resposta mais rápida a incidentes e para a melhoria contínua da segurança da infraestrutura.

4.4 PROTEÇÃO E MONITORAMENTO: A SEGURANÇA COMO PROCESSO CONTÍNUO

A segurança de uma rede escolar não termina após a sua instalação, ela é um ciclo constante de vigilância e melhoria. Proteger o ambiente digital onde estudantes e professores interagem exige que a instituição garanta que as defesas técnicas estejam sempre ativas e operando corretamente.

4.4.1 Prevenção e Dever de Cuidado

De acordo com a LGPD (Art. 46), qualquer instituição que trate dados pessoais deve adotar medidas técnicas e administrativas para proteger essas informações contra acessos não autorizados ou situações ilícitas de perda e alteração. No contexto escolar, o ECA Digital (Lei nº 15.211/2025) reforça que produtos e serviços tecnológicos devem ser projetados com foco no melhor interesse da criança e do adolescente, garantindo níveis elevados de privacidade e segurança por padrão.

4.4.2 Acesso Remoto Seguro

A administração de servidores e da rede geralmente ocorre à distância. No entanto, o acesso remoto deve ser tratado com rigor técnico extremo. Sem protocolos de segurança e criptografia, essa facilidade pode se tornar uma vulnerabilidade para invasores. A legislação exige que os fornecedores e administradores adotem mecanismos de segurança reconhecidos para mitigar riscos de exposição indevida.

4.8.3 Monitoramento e Vigilância Ativa

O monitoramento contínuo dos dispositivos e serviços de rede é essencial para:

Identificar falhas: Garantir que os sistemas educacionais estejam sempre disponíveis.

Detectar intrusões: Perceber tentativas de acesso não autorizado antes que causem danos.

Proteção integral: Cumprir o princípio da prevenção da LGPD, agindo antes que um incidente ocorra.

Nota Técnica: Para a comunidade escolar, monitorar não significa vigilância indiscriminada. Segundo o ECA Digital, qualquer ferramenta de supervisão ou monitoramento deve respeitar a privacidade e o desenvolvimento progressivo do jovem, utilizando a tecnologia para prevenir riscos como o assédio e a exploração.

TESTES E VALIDAÇÃO

Testes Finais de Segurança e Verificação de Acesso

5 TESTE E VALIDAÇÃO HARDENING

O ciclo de testes, validação e auditoria no processo de hardening garante que as configurações de segurança aplicadas sejam eficazes, estejam em conformidade com padrões internacionais e não comprometam a operação do sistema. No ambiente Debian Linux, esse processo envolve testes controlados, auditorias automatizadas e monitoramento contínuo da integridade do sistema.

5.1 Ambiente de Testes e Homologação

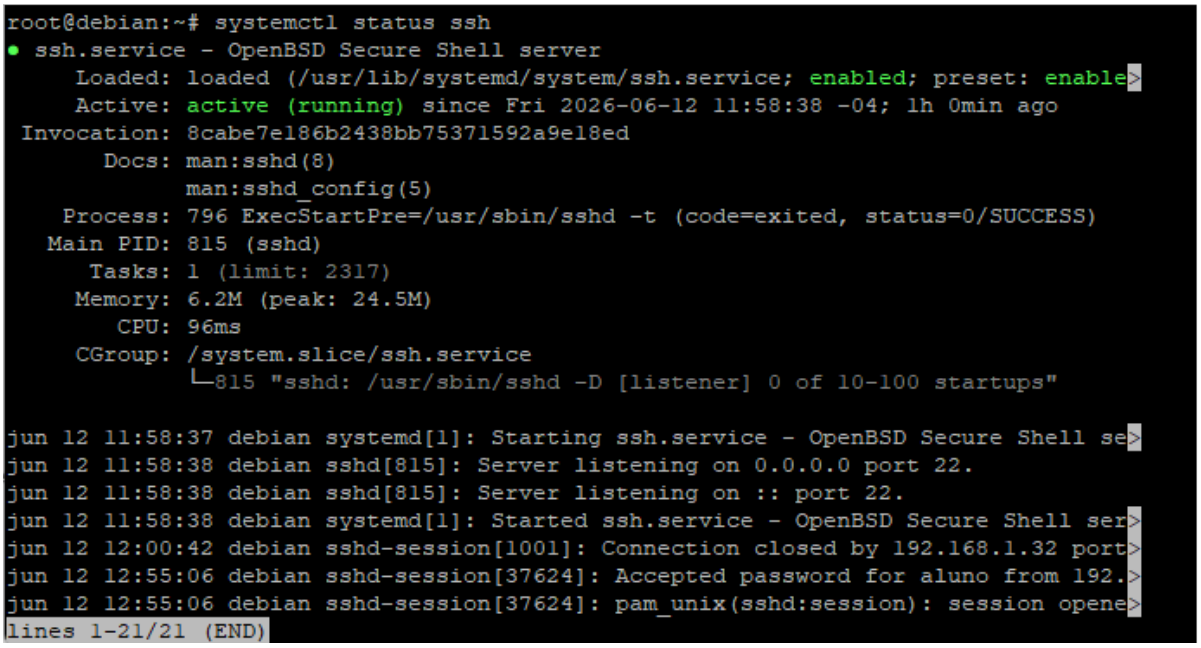
Uma diretriz fundamental do hardening é nunca aplicar alterações diretamente em servidores de produção. Dessa forma, foi utilizado um ambiente virtualizado para simulação e validação das configurações de segurança.

- **Isolamento e Virtualização:** Recomenda-se o uso de ferramentas como o VirtualBox para criar máquinas virtuais (VMs) isoladas da rede principal durante a fase de testes;
- **Snapshots:** No VirtualBox, utilize *snapshots* para criar pontos de restauração antes de aplicar atualizações ou mudanças críticas de configuração. Se um serviço essencial for interrompido, é possível retornar ao estado anterior rapidamente;

- **Validação de Patches:** Antes de implantar qualquer *patch*, *hotfix* ou atualização via apt, teste-os exaustivamente no ambiente de homologação para garantir que funcionem conforme o esperado no cenário específico da sua organização.

ex:

- ping 8.8.8.8
- systemctl status ssh
- apt update && apt upgrade



Os resultados demonstraram estabilidade do sistema após a aplicação dos patches de segurança.

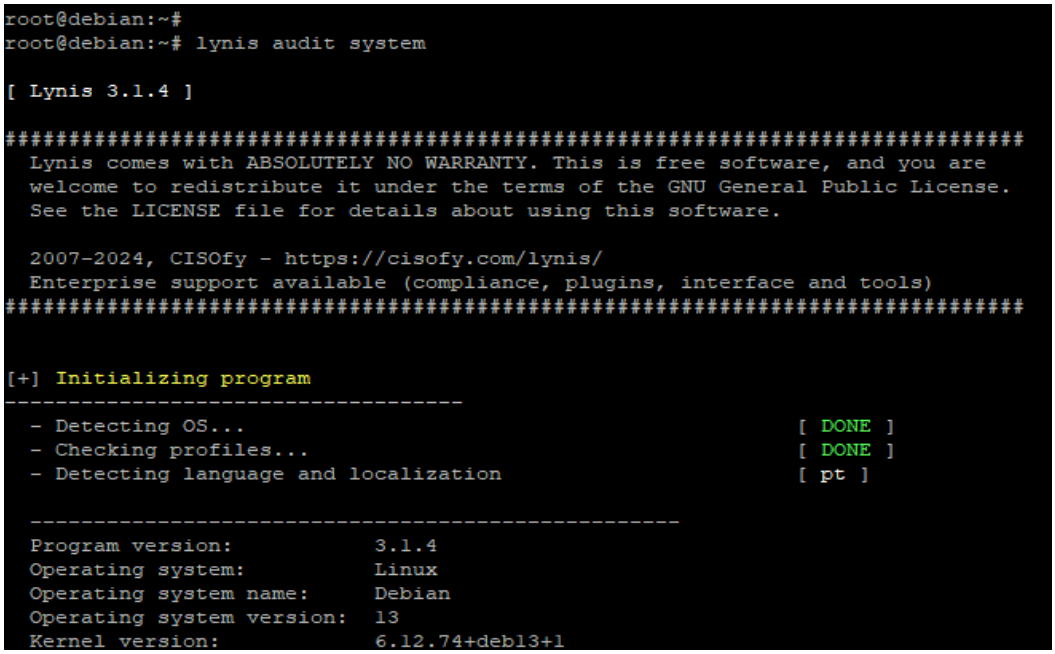
5.2 Ferramentas de Auditoria e Automação

A auditoria de segurança foi utilizada para identificar vulnerabilidades e verificar a conformidade do sistema em relação às boas práticas de hardening.

1. Auditoria com Lynis

Exemplo de execução:

lynis audit system

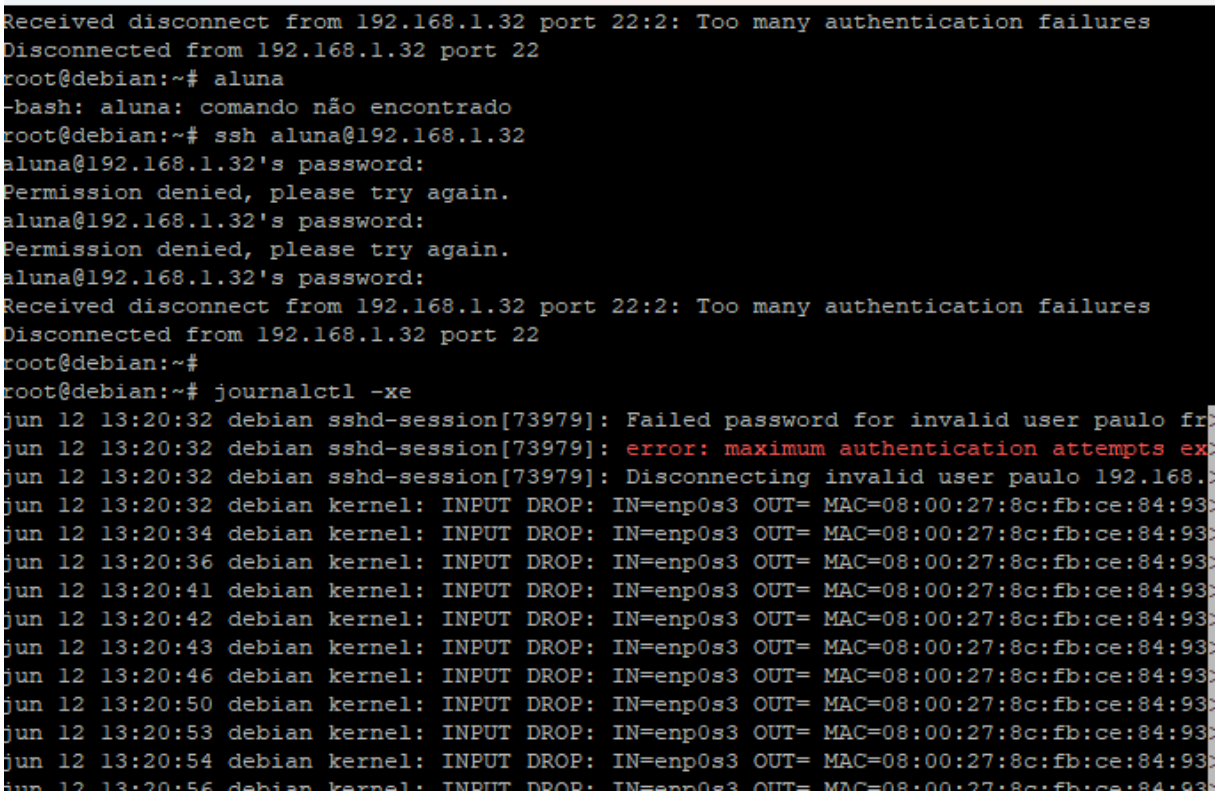


Durante os testes, o Lynis identificou serviços desnecessários ativos, permissões excessivas em diretórios e ausência de políticas avançadas de senha. Após as correções, o score de segurança do sistema apresentou melhoria significativa.

5.3 Monitoramento e Revisão Contínua

O hardening é um processo contínuo, exigindo revisões periódicas para adaptação a novas ameaças e vulnerabilidades.

- **Monitoramento de Integridade :** Foi implementado monitoramento de integridade de arquivos utilizando ferramentas de FIM (File Integrity Monitoring). Durante os testes, alterações simuladas em arquivos críticos do sistema foram detectadas automaticamente, gerando alertas de segurança.
- **Análise de Logs :** Os logs do sistema foram monitorados utilizando comandos como:
  - journalctl -xe



Nos testes realizados, tentativas de login inválidas via SSH foram registradas corretamente, permitindo identificar possíveis acessos não autorizados.

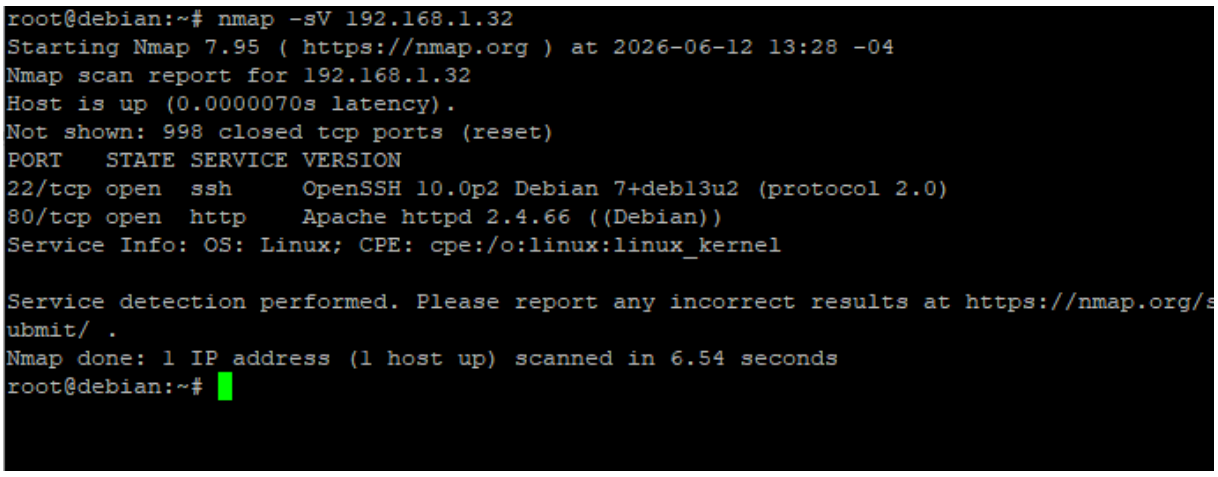
- **Frequência de Revisão :** Foi definido um ciclo trimestral de revisão das configurações de segurança, além de verificações adicionais após mudanças críticas no ambiente.
-

5.4 Técnicas de Testes Finais e Verificação

Para validar a eficiência das medidas de hardening, foram realizados testes ofensivos e defensivos.

- **Testes de Vulnerabilidade:** Foi utilizado o scanner Nmap para verificar portas abertas e serviços expostos.

Exemplo de teste:
nmap -sV 192.168.0.10



Após a aplicação das técnicas de hardening no sistema Debian, foi realizado um teste de varredura utilizando a ferramenta Nmap para identificar portas abertas e serviços ativos no servidor.

O parâmetro -sV permitiu identificar as versões dos serviços em execução no host analisado.

Como resultado da varredura, foram detectadas apenas duas portas abertas:

- Porta 22/TCP — Serviço SSH (OpenSSH);
- Porta 80/TCP — Serviço Web Apache HTTP Server.

O resultado demonstrou que o servidor estava com a superfície de ataque reduzida, mantendo apenas os serviços essenciais ativos após o processo de hardening. Além disso, a análise confirmou que 998 portas TCP estavam fechadas, indicando que serviços desnecessários foram desabilitados corretamente.

Resultado obtido durante o teste:

22/tcp open ssh OpenSSH 10.0p2 Debian

80/tcp open http Apache httpd 2.4.66 (Debian)

A validação também permitiu verificar:

1. funcionamento correto do servidor SSH para administração remota;
2. disponibilidade do serviço web Apache;
3. redução de riscos relacionados à exposição de serviços desnecessários;
4. conformidade com práticas de segurança recomendadas em ambientes Linux.

Esse teste é essencial no ciclo de hardening, pois ajuda a identificar portas expostas indevidamente e possíveis vulnerabilidades associadas aos serviços em execução.

- **Validação de firewall**: confirmar que as regras de filtragem estão funcionando corretamente.

```
root@debian:~# ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To                         Action      From
--                         ------      ----
22/tcp                     ALLOW IN    Anywhere
80/tcp                     ALLOW IN    Anywhere
22/tcp (v6)                ALLOW IN    Anywhere (v6)
80/tcp (v6)                ALLOW IN    Anywhere (v6)

root@debian:~#
```

Após a configuração das políticas de filtragem no sistema Debian Linux, foi realizada a validação das regras utilizando o comando:

ufw status verbose

Resultado obtido durante os testes:

Status: active

Logging: on (low)

Default: deny (incoming), allow (outgoing), disabled (routed)

```
To                         Action      From
--                         ------      ----
22/tcp                     ALLOW IN    Anywhere
80/tcp                     ALLOW IN    Anywhere
22/tcp (v6)                ALLOW IN    Anywhere (v6)
80/tcp (v6)                ALLOW IN    Anywhere (v6)
```

A análise demonstrou que o firewall estava ativo e configurado com a política padrão de bloqueio para conexões de entrada (deny incoming), permitindo apenas os serviços essenciais previamente autorizados.

Os testes confirmaram:

1. liberação da porta 22/TCP para acesso remoto SSH;
2. liberação da porta 80/TCP para hospedagem web Apache;
3. bloqueio automático de conexões não autorizadas;
4. funcionamento correto das regras IPv4 e IPv6;
5. redução da exposição desnecessária de serviços na rede.

Também foram realizados testes externos de conectividade para validar as regras implementadas:

- acesso SSH realizado com sucesso;
- acesso HTTP funcionando normalmente via navegador;
- portas não autorizadas apresentaram bloqueio de conexão.

Os resultados demonstraram que o firewall estava operando corretamente e contribuindo para o fortalecimento da segurança do servidor Debian após o processo de hardening.

- **Teste de backup e recuperação**: verificar se os backups podem ser restaurados com sucesso.

- **Monitoramento do sistema**: acompanhar o funcionamento após as alterações para garantir estabilidade e segurança.

Este ciclo rigoroso de validação é o que fornece a evidência técnica necessária para demonstrar conformidade com legislações como a LGPD, garantindo que os dados pessoais sejam protegidos por medidas técnicas robustas e testadas. Outro benefício importante é a melhoria da capacidade de resposta a incidentes. Ao identificar vulnerabilidades e desvios de configuração de forma antecipada, a organização reduz significativamente o tempo de detecção e mitigação de ameaças, minimizando impactos operacionais, financeiros e reputacionais. A combinação de monitoramento contínuo, verificação de integridade e análise de logs possibilita uma visão abrangente do ambiente computacional, permitindo a identificação de comportamentos anômalos e tentativas de acesso não autorizado antes que resultem em comprometimentos mais graves.

O ciclo de testes e auditorias também desempenha papel fundamental na continuidade dos negócios. Sistemas devidamente protegidos e constantemente avaliados apresentam maior disponibilidade, confiabilidade e resistência a falhas, garantindo que os serviços essenciais permaneçam operacionais mesmo diante de eventos adversos. Além disso, a validação periódica das configurações de segurança assegura que novas atualizações, aplicações e mudanças na infraestrutura não introduzem vulnerabilidades que possam comprometer a integridade dos dados ou a estabilidade dos serviços.

Em um cenário caracterizado pela rápida evolução das ameaças cibernéticas, o hardening deve ser encarado como um processo permanente de aperfeiçoamento. A adoção de práticas de melhoria contínua, associada ao uso de ferramentas de auditoria, automação e monitoramento, permite que a organização adapte seus controles de segurança às novas exigências tecnológicas e regulatórias. Dessa forma, o ciclo de testes, validação e auditoria não apenas protege os ativos de informação, mas também fortalece a governança de TI, aumenta a confiança de clientes e parceiros e contribui para a sustentabilidade e competitividade da organização em longo prazo.

6. CONSIDERAÇÕES FINAIS

REFERÊNCIAS

1. Empowering School IT Teams Through Cybersecurity ... - CoSN, https://www.cosn.org/wp-content/uploads/2026/06/Empowering-School-IT-Teams-Through-Cybersecurity-Professional-Development.pdf
2. K-12 Cybersecurity | U.S. Department of Education, https://www.ed.gov/teaching-and-administration/safe-learning-environments/school-safety-and-security/k-12-cybersecurity
3. State and Federal Cybersecurity Policy and Education in 2024 | CoSN, https://www.cosn.org/wp-content/uploads/2025/01/State-and-Federal-Cybersecurity-Policy-and-Education-in-2024-CoSN-v3.pdf
4. Protecting Our Future: Cybersecurity for K-12 | CISA, https://www.cisa.gov/topics/cybersecurity-best-practices/K12cybersecurity/protecting-our-future-cybersecurity-k12
5. PROPOSTA DE IMPLEMENTAÇÃO DE REDE SEM FIO EM UM AMBIENTE ESCOLAR. - UNIBRA, https://www.grupounibra.com/repositorio/REDES/2023/proposta-de-implementacao-de-rede-sem-fio-em-um-ambiente-escolar.pdf
6. Summary of Education Cybersecurity Policy Developments in 2023 - CoSN, https://www.cosn.org/wp-content/uploads/2024/01/CoSN-Cybersecurity-Policy-Developments-2023.pdf

7. AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES (ANATEL). https://www.gov.br/anatel
8. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD).
9. https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm
10. DEV.TO. Hardening Básico de Servidor Ubuntu/Debian: Acesso SSH e Firewall. João Pedro, 2025. Disponível em: https://dev.to/joaoprd/hardening-basico-de-servidor-ubuntudebian-acesso-ssh-e-firewall-5lm . Acesso em: 12 jun. 2026.
11. HELP SYS ADMIN. Hardening Linux: Checklist Essencial de Segurança (Guia 2026). 2026. Disponível em: https://helpsysadmin.com.br/blog/hardening-linux-checklist-seguranca/ . Acesso em: 12 jun. 2026.
12. HELP SYS ADMIN. Segurança Linux: 7 Passos para Proteger seu Servidor de Invasões. 2026. Disponível em: https://helpsysadmin.com.br/blog/como-proteger-servidor-linux-seguranca/ . Acesso em: 12 jun. 2026.
13. DANILO SANTOS. Ssh Hardening Server Linux: Protegendo o Acesso SSH com Segurança. danilosantos.info, 2025. Disponível em: https://danilosantos.info/pt-br/posts/ssh-hardening-server-linux/ . Acesso em: 12 jun. 2026.
14. LUKMIN-SH. Como monitorar arquivos de log em tempo real no Linux. Linux Terminal, 2022. Disponível em: https://pt.linux-terminal.com/?p=7723 . Acesso em: 12 jun. 2026.
15. ALURA. Estudando Logs no Linux e começando um mini-projeto de monitoramento. Fórum do Projeto, 2025. Disponível em: https://cursos.alura.com.br/forum/topico-projeto-estudando-logs-no-linux-e-comecando-um-mini-projeto-de-monitoramento-545132 . Acesso em: 12 jun. 2026.
16. OPENSSH. OpenSSH: Secure Shell. Disponível em: https://www.openssh.com/ . Acesso em: 12 jun. 2026..
17. NANOSHOTS. Dicas de Hardening e Proteção do Linux. 2016. Disponível em: https://www.nanoshots.com.br/2016/01/dicas-de-hardening-no-linux.html . Acesso em: 12 jun. 2026
18. Lei Geral de Proteção de Dados Pessoais (LGPD) BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília: Presidência da República, 2018.
19. Estatuto Digital da Criança e do Adolescente BRASIL. Lei nº 15.211, de 17 de setembro de 2025. Dispõe sobre a proteção de crianças e adolescentes em ambientes digitais (Estatuto Digital da Criança e do Adolescente). Brasília: Presidência da República, 2025.