FACULDADE DE TECNOLOGIA DE AMERICANA "Ministro Ralph Biasi"
Curso Superior de Tecnologia em Segurança da Informação

Rafael Rodrigues Negri

Thiago Camillo

Segurança em Equipamentos CPE: Estudo de Efetividade do Ato nº 2436

Americana, SP

2025

FACULDADE DE TECNOLOGIA DE AMERICANA "Ministro Ralph Biasi"
Curso Superior de Tecnologia em Segurança da Informação

Rafael Rodrigues Negri

Thiago Camillo

Segurança em Equipamentos CPE: Estudo de Efetividade do Ato nº 2436

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação sob a orientação do Prof. Edson Roberto Gaseta.

Área de concentração: Segurança da Informação.

Americana, SP

2025

NEGRI, Rafael Rodrigues

Segurança em Equipamentos CPE: Estudo de Efetividade do Ato nº 2436. / Rafael Rodrigues Negri, Thiago Camillo – Americana, 2025.

57f.

Monografia (Curso Superior de Tecnologia em Segurança da Informação) - - Faculdade de Tecnologia de Americana Ministro Ralph Biasi – Centro Estadual de Educação Tecnológica Paula Souza

Orientador: Prof. Ms. Edson Roberto Gaseta

1. Análise de dados 2. Internet – rede de computadores 3. Qualidade. I. NEGRI, Rafael Rodrigues, II. CAMILLO, Thiago III. GASETA, Edson Roberto IV. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana Ministro Ralph Biasi

CDU: 681516
681.519Internet
658.56

Elaborada pelo autor por meio de sistema automático gerador de ficha catalográfica da Fatec de Americana Ministro Ralph Biasi.

Rafael Rodrigues Negri

Thiago Camillo

Segurança em Equipamentos CPE: Estudo de Efetividade do Ato nº 2436

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Curso Superior de Tecnologia em Segurança da Informação pelo Centro Paula Souza – FATEC Faculdade de Tecnologia de Americana Ministro Ralph Biasi.
Área de concentração: Segurança da Informação

Americana, 25 de junho de 2025.

Banca Examinadora:

Edson Roberto Gaseta
Mestre
Fatec Americana "Ministro Ralph Biasi"

João Emmanuel D' Alkmin Neves
Doutor
Fatec Americana "Ministro Ralph Biasi"

Henri Alves de Godoy
Doutor
Fatec Americana "Ministro Ralph Biasi"

RESUMO

O trabalho analisa a conformidade dos equipamentos CPE (*Customer Premises Equipment*) com os requisitos de segurança cibernética do Ato nº 2436 da Anatel, visando identificar vulnerabilidades e avaliar a eficácia das medidas de segurança implementadas. A pesquisa exploratória utiliza revisão bibliográfica, análise qualitativa e quantitativa para correlacionar conformidade e redução de riscos. Espera-se que o cumprimento do Ato melhore a segurança dos CPEs, reduzindo as chances de ataques cibernéticos e protegendo dados pessoais e corporativos. Os resultados podem orientar políticas públicas, beneficiando consumidores, fabricantes e provedores de serviços, promovendo um ambiente digital mais seguro e confiável, fortalecendo a confiança nas infraestruturas de rede.

Palavras-chave: Conformidade CPE, Segurança Cibernética, Ato 2436.

ABSTRACT

The work analyzes the compliance of CPE (*Customer Premises Equipment*) *equipment with the cyber security requirements of Anatel Act No. 2436, in order to identify vulnerabilities and evaluate the effectiveness of the security measures implemented. The exploratory research uses a literature review, qualitative and quantitative analysis to correlate compliance and risk reduction. Compliance with the Act is expected to improve the security of CPEs, reducing the chances of cyber attacks and protecting personal and corporate data. The results can guide public policies, benefiting consumers, manufacturers and service providers, promoting a safer and more reliable digital environment and strengthening trust in network infrastructures.*

Keywords: *CPE Compliance, Cyber Security, Act 2436*

LISTA DE ILUSTRAÇÕES

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

Anatel - Agência Nacional de Telecomunicações

AWS - *Amazon Web Services*

CPE - *Customer Premises Equipment*

HTTP- *Hypertext Transfer Protocol*

IBM - *International Business Machines Corporation*

LACNOG - *Latin American and Caribbean Network Operators Group*

LAN - *Local Area Network*

MAC - *Media Access Control*

M3AAWG - *Messaging, Malware and Mobile Anti-Abuse Working Group*

NMAP - *Network Mapper*

ONT - *Optical Network Terminal*

ONU - *Optical Network Unit*

SSH - *Secure Shell*

Telnet - *Teletype network*

xDSL - *generic Digital Subscriber Line*

SUMÁRIO

INTRODUÇÃO

A crescente digitalização dos ambientes corporativos e residenciais tem agregado muita conectividade nas demandas cotidianas, mas também aumentou a exposição a riscos cibernéticos. Os equipamentos CPE, como *modems*, roteadores e dispositivos de acesso sem fio, são pontos críticos de vulnerabilidade, frequentemente alvo de ataques cibernéticos que podem comprometer a privacidade e a segurança dos usuários finais.

O Ato nº 77 da Anatel é um grande precursor da cibersegurança no Brasil. A normativa de 05 de janeiro de 2021 estabelece requisitos de segurança cibernética para “equipamentos terminais que se conectam à Internet e para equipamentos de infraestrutura de redes de telecomunicações, em suas versões finais destinadas à comercialização” (Anatel, 2021, s.p.). Esta regulamentação visa mitigar vulnerabilidades e fortalecer a segurança de uma ampla gama de equipamentos, desde dispositivos de uso doméstico até sistemas complexos de redes.

O Ato nº 2436 emitido pela Anatel em 2023, estabelece requisitos mínimos de segurança cibernética para equipamentos CPE em específico, complementando o objetivo de aumentar a proteção contra ameaças e garantir a integridade das redes de comunicação.

Num cenário onde milhões de brasileiros dependem de dispositivos CPE para acessar a internet em suas casas e locais de trabalho, esses dispositivos, se não forem adequadamente protegidos, podem se tornar portas de entrada para cibercriminosos. Ataques cibernéticos podem resultar em roubo de dados pessoais, interrupção de serviços essenciais e até mesmo em prejuízos financeiros significativos.

No entanto, com a implementação dos requisitos de segurança cibernética do Ato nº 2436, espera-se que esses dispositivos sejam mais resistentes a ataques, protegendo os usuários finais. Este estudo investigará se as medidas prescritas pelo Ato estão sendo efetivamente adotadas pelos fabricantes e fornecedores, e se estão cumprindo seu propósito de aumentar a segurança dos equipamentos CPE.

Ao avaliar a conformidade de equipamentos CPE em relação à normativa n° 2436 da Anatel, o estudo contribuirá com uma visão objetiva das vulnerabilidades e

ataques cibernéticos, baseando-se em cenários práticos, gerando análises mais concretas sobre a proteção de dados.

Os resultados da pesquisa podem orientar políticas públicas e regulamentações futuras, promovendo um ambiente digital mais seguro e resiliente.

O estudo aumentará a conscientização sobre a importância da segurança cibernética, tanto para consumidores quanto para fabricantes.

A importância deste projeto está intrinsecamente ligada aos valores e prioridades das partes interessadas, que incluem consumidores, fabricantes de equipamentos, provedores de serviços de internet e reguladores. Ao analisar o impacto dos requisitos de segurança do Ato nº 2436, o estudo fornecerá *insights* valiosos sobre a eficácia das políticas atuais e as áreas que necessitam de melhorias.

A execução deste projeto é altamente viável, considerando a complexidade e o acesso às informações necessárias. Primeiramente, o tema envolve a análise dos requisitos de segurança cibernética estabelecidos pelo Ato nº 2436 da Anatel, um documento público e amplamente acessível. As informações sobre os equipamentos CPE e as práticas de segurança cibernética são abundantes em fontes acadêmicas, regulamentares e industriais.

Este trabalho tem como objetivo geral, analisar a conformidade dos equipamentos CPE aos requisitos de segurança cibernética estabelecidos pelo Ato nº 2436 da Anatel.

Como objetivos específicos identificar as principais vulnerabilidades de segurança cibernética em equipamentos CPE, e avaliar a eficácia das medidas de segurança implementadas pelos fabricantes.

As hipóteses são que a implementação dos requisitos de segurança cibernética estabelecidos pelo Ato nº 2436 melhoram significativamente a conformidade, e a segurança dos equipamentos CPE, reduzindo as vulnerabilidades e ataques cibernéticos nesses dispositivos.

O percurso metodológico deste trabalho é uma pesquisa exploratória, com revisão bibliográfica sobre a legislação vigente relacionada à segurança cibernética e as melhores práticas de segurança para equipamentos CPE. Os sujeitos serão os equipamentos CPE. Os indicadores serão a conformidade com os requisitos do Ato nº 2436 e o número de vulnerabilidades identificadas. Os dados levantados serão analisados de forma qualitativa e quantitativa, utilizando métodos analíticos para avaliar a relação entre a conformidade e a redução de incidentes.

O trabalho está organizado em cinco capítulos: o capítulo 1 será a fundamentação teórica, que abordará os conceitos de segurança cibernética, a legislação pertinente e as características dos equipamentos CPE; o capítulo 2 é o percurso metodológico, contendo o *checklist* utilizado durante os testes realizados; o capítulo 3 será o estudo de caso detalhando a abordagem da pesquisa; o capítulo 4 conterá os resultados da coleta e análise de dados; e por último o capítulo 5 conterá considerações finais os resultados, objetivos e hipótese formulada.

1 FUNDAMENTAÇÃO TEÓRICA

No embasamento desta pesquisa, optou-se por organizar este capítulo em cinco seções, apresentando os conceitos chave que referenciam o trabalho, sendo eles: Conformidade de Segurança Cibernética, Equipamentos CPE, Avaliação da Conformidade, Ato nº 2436 e Nº 77 da Anatel.

1.1 Conformidade de Segurança Cibernética

A conformidade de segurança cibernética é um aspecto essencial na proteção de informações e sistemas digitais, que existem em um ambiente virtual repleto de ameaças. Segundo a (Anatel, 2023) “[...] conformidade de produtos para telecomunicações garante ao consumidor o acesso a produtos testados de acordo com padrões de qualidade, segurança e requisitos funcionais”. Em um contexto em que as legislações, como o Ato nº 2436, impõem requisitos específicos aos provedores de serviços de internet, a conformidade se torna uma obrigação que transcende o mero cumprimento legal, servindo como uma estratégia de mitigação de riscos.

A implementação das diretrizes de segurança cibernética requer uma abordagem sistemática e contínua. Essa prática não apenas identifica vulnerabilidades, mas também permite que as organizações ajustem suas políticas de segurança em resposta a novas ameaças, garantindo um ambiente mais seguro.

Além disso, de acordo com o Gabinete de Segurança Institucional (Brasil, [s.d.]) uma das principais atribuições do Comitê Nacional de Cibersegurança é orientar as políticas de cibersegurança no país, propondo atualizações estratégicas a nível nacional e promover cooperação internacional na área. Chin (2024) ressalta a importância de promover uma cultura de segurança cibernética dentro das organizações.

Para que a conformidade de segurança cibernética seja efetiva, todos os colaboradores devem estar engajados e conscientes das suas responsabilidades. A conscientização e o treinamento contínuo dos funcionários são fundamentais para minimizar falhas humanas, que muitas vezes são a porta de entrada para ataques cibernéticos.

A conformidade também pode ser vista como uma vantagem competitiva. Segundo (EC-Council University, [s.d.]) as empresas que demonstram compromisso com a segurança cibernética gerenciam melhor a sua reputação perante o mercado já que são elementos que estão interligados e com isso, acabam conquistando a confiança dos consumidores. Em um cenário onde a segurança dos dados é uma preocupação crescente para os usuários, ser reconhecido por práticas de conformidade eficazes pode ser um diferencial significativo.

Por fim, a conformidade de segurança cibernética não é apenas uma questão de adequação a normas, mas sim uma abordagem estratégica que protege tanto as organizações quanto seus clientes. A adesão aos requisitos do Ato nº 2436, nesse sentido, representa um passo fundamental para garantir a segurança dos equipamentos CPE e, consequentemente, a integridade das redes no Brasil.

1.2 Equipamentos CPE

Os equipamentos *Customer Premises Equipment* (Equipamento de Instalações do Cliente) compreendem uma gama de dispositivos utilizados na *interface* entre a rede de um provedor de internet e a rede local do usuário. Esses dispositivos incluem *modems cable* (conexão de cabo coaxial) e xDSL (conexão telefônica com fio de cobre), ONUs, ONTs, roteadores ou *modems* destinados ao acesso fixo sem fio, via satélite e ponto de acesso sem fio, segundo (Anatel, 2023).

Infelizmente equipamentos CPE costumam partilhar uma série de vulnerabilidades comuns, como senhas padrão fracas que raramente são alteradas pelos usuários. Dessa forma, sua *interface web* de administração acaba se tornando uma superfície comum de ataque. Além da interface web, é muito visada também por atacantes cibernéticos, a varredura de portas em busca de serviços como conexão Telnet ou SSH.

O *firmware* dos CPEs também pode ser alvo de exploração para atacantes. De acordo com (Anatel, 2021, s.p.) o *firmware* é um “software acessível somente para leitura, programado em um hardware de propósito específico e armazenados de forma funcionalmente independente do armazenamento principal do equipamento”. Caso por exemplo, desenvolvido em uma arquitetura baseada em Linux – uma prática comum no mercado – os fabricantes podem acabar utilizando componentes de código

aberto que possuem vulnerabilidades conhecidas, impactando gravemente a resiliência do equipamento à ataques.

A segurança dos equipamentos CPE é uma preocupação crescente, especialmente em um ambiente digital repleto de ameaças. A (LACNOG e M3AAWG, 2019) específica algumas das vulnerabilidades para os CPE como *hard-coded, backdoors,* falta de mecanismos automáticos de atualização entre outros. Algumas dessas vulnerabilidades podem levar a incidentes que comprometem não apenas o usuário final, mas também a rede do provedor de serviços, criando um problema cascata de segurança.

Outro aspecto importante é o suporte e atualização contínua da segurança dos CPEs. De acordo com (LACNOG e M3AAWG, 2019), os fornecedores deveriam disponibilizar correções de segurança para os seus equipamentos por 03 anos após a data término da venda. A realização de auditorias periódicas e a análise de vulnerabilidades são práticas recomendadas que ajudam a manter os dispositivos seguros e em conformidade com as normas estabelecidas.

Em suma, os equipamentos CPE são essenciais para a conectividade e a comunicação em ambientes digitais, e sua segurança deve ser uma prioridade para provedores de serviços de Internet. A conformidade com legislações, como o Ato nº 2436, é crucial para garantir que esses dispositivos sejam seguros, reduzindo a vulnerabilidade a ataques e melhorando a confiança do usuário.

1.3 Avaliação de Conformidade

De acordo com (IBM, [s.d.]), "O monitoramento da conformidade é o ato de avaliar continuamente se uma organização está cumprindo os requisitos regulatórios, incluindo políticas internas e padrões específicos do setor". Este processo é essencial para garantir a qualidade e a segurança em diversos setores, incluindo o de tecnologia da informação.

No contexto da segurança cibernética, a avaliação de conformidade se torna ainda mais crítica. De acordo com (UniOpet, 2024), a crescente onda de invasões realizadas em empresas e governos tem demonstrado pontos de vulnerabilidade em infraestruturas causando consequências bilionárias. A realização de auditorias e testes de segurança se tornam, portanto, práticas altamente recomendadas, pois além dos prejuízos gerados pelo ataque diretamente, a (IBM, [s.d.]) ressalta que ignorar os

padrões de conformidade pode desencadear consequências graves para as empresas, não apenas em termos de sanções monetárias, mas também afetando a continuidade dos negócios e elevando consideravelmente o risco de incidentes de segurança.

Além disso, a cultura organizacional desempenha um papel significativo na eficácia da avaliação de conformidade. A (IBM, [s.d.]) destaca a natureza colaborativa deste processo, enfatizando que a responsabilidade pela conformidade se estende além de uma única equipe. Segundo a empresa, "É importante lembrar que a conformidade não é responsabilidade exclusiva da equipe de conformidade. O monitoramento eficaz da conformidade envolve vários departamentos e indivíduos em toda a organização" (IBM, [s.d.]). Esta abordagem holística sublinha a importância do engajamento coletivo na manutenção dos padrões de conformidade.

Em síntese, a avaliação de conformidade deve ser vista como uma atividade contínua, não apenas como um evento pontual. Nesse contexto, a (IBM, [s.d.]) enfatiza a importância de testes regulares como parte integrante do processo de monitoramento de conformidade. Segundo a empresa, essas avaliações periódicas são cruciais para identificar vulnerabilidades de forma eficaz e implementar medidas corretivas rapidamente, assegurando assim a robustez e eficiência contínua do programa de conformidade. A eficácia deste monitoramento depende de uma abordagem holística, envolvendo diversos departamentos. Este compromisso com a conformidade se traduz em uma postura proativa essencial para a sustentabilidade e segurança dos negócios no ambiente digital contemporâneo.

1.4 Ato n° 2436/2023

O Ato nº 2436 da Anatel visa fortalecer a segurança cibernética no âmbito dos serviços de internet no Brasil. A normativa estabelece "requisitos mínimos de segurança cibernética de aplicação mandatória" (Anatel, 2023, s.p.) para avaliar a conformidade dos equipamentos CPE, que são definidos como aqueles "de uso do público em geral empregados para conectar assinantes à rede do provedor de serviços de Internet" (Anatel, 2023, s.p.). Esta regulamentação abrange uma variedade de dispositivos comumente encontrados em residências e pequenas empresas, como *modems*, roteadores e outros equipamentos de conexão à internet. Ao implementar estes requisitos, a Anatel busca criar um ambiente digital mais seguro

para os usuários brasileiros, mitigando riscos associados a vulnerabilidades em equipamentos de uso cotidiano.

O Ato estabelece diretrizes abrangentes para a segurança cibernética de equipamentos CPE, visando mitigar as crescentes ameaças digitais. Conforme a (Anatel, 2023), esta normativa implementa múltiplas camadas de proteção, abordando desde a gestão robusta de senhas – com critérios rigorosos tanto para senhas de fábrica quanto para as definidas pelos usuários – até mecanismos avançados de defesa contra acessos não autorizados e criptografia de dados sensíveis. Essas medidas integradas visam não apenas proteger os usuários, mas também fomentar um ecossistema de internet mais seguro e confiável no país, incentivando a indústria a priorizar a segurança cibernética como componente essencial no desenvolvimento e suporte de produtos de telecomunicações.

A segurança da informação, na qual o Ato nº 2436 da Anatel é fundamentado, repousa sobre três pilares fundamentais: a confidencialidade, que restringe o acesso à informação a entidades autorizadas; a integridade, que garante a exatidão e a autenticidade dos dados, protegendo contra alterações indevidas; e a disponibilidade, que assegura o acesso aos sistemas da informação quando necessário. Esses pilares sustentam as exigências da normativa, visando proteger os equipamentos de telecomunicações contra ameaças, assegurando a confiabilidade dos dados e a continuidade dos serviços para usuários e redes.

Em resumo, o Ato nº 2436 é um marco importante na regulação da segurança cibernética no Brasil, estabelecendo requisitos que visam proteger tanto os provedores de serviços quanto os consumidores. A implementação efetiva dessa norma pode resultar em um ambiente digital mais seguro e confiável.

1.5 Ato n° 77/2021

O Ato nº 77 delineia um conjunto abrangente de diretrizes de segurança cibernética para uma série de dispositivos, incluindo os CPE. Apesar de não fornecer requisitos específicos para esses equipamentos, o ato lança os fundamentos que posteriormente foram usados pelo Ato 2436 para a regulamentação dos CPE. O Ato nº 77 aborda temas de grande relevância no cenário de segurança, tais como atualizações de *software, firmware*, gerenciamento remoto, processos de instalação e operação, acesso para configuração do equipamento, serviços de comunicação de

dados, capacidade de mitigar ataques, e até mesmo dados pessoais e dados pessoais sensíveis, observada a legislação vigente.

Além dos requisitos para fabricantes, o ato também delibera acerca das obrigatoriedades que devem ser observadas por fornecedores de equipamentos para telecomunicação, tais como “Disponibilizar um canal de comunicação que possibilite aos seus clientes, usuários finais e terceiros reportarem vulnerabilidades de segurança identificadas nos produtos.” (Anatel, 2021, s.p.), e divulgação coordenada de vulnerabilidades baseados em boas práticas e recomendações reconhecidas internacionalmente.

Em suma, o Ato nº 77 é um marco regulatório crucial para a segurança cibernética no Brasil, estabelecendo requisitos rigorosos para a proteção de equipamentos de telecomunicações. A implementação efetiva desta norma se faz essencial para garantir a segurança e a confiabilidade das redes de telecomunicações, protegendo usuários e infraestruturas críticas contra as crescentes ameaças digitais.

2 METODOLOGIA

Este capítulo visa detalhar a metodologia idealizada e utilizada para a avaliação da segurança cibernética dos equipamentos CPE, baseada única e exclusivamente nos requisitos estabelecidos no Ato nº 2436 da Anatel. Elaborou-se um ambiente de teste conforme explicitado na Seção 3 Estudo de caso, e realizou-se uma bateria que segue rigorosamente um *checklist* baseado em itens específicos do referido Ato. Além disso, os resultados dos testes são expostos em quadros conforme a sessão 4 Resultados.

2.1 Definições

Nesta seção encontram-se, segundo a Anatel em seu referido Ato 2436, algumas definições importantes que norteiam a pesquisa, sendo as mesmas, importantíssimas para diferirem os resultados de testes entre conformidade e não conformidade.

Dicionário de senhas:

- Mecanismos que impedem a definição de senhas que constam em dicionários de senhas comumente utilizadas ou associadas ao contexto do equipamento.

Senha fraca:

- Senhas que não atendam aos critérios mínimos de segurança: mínimo de 8 caracteres, contendo ao menos uma letra maiúscula, uma letra minúscula e um número.

2.2 Requisitos para as senhas providas de fábrica

Nesta seção encontram-se, segundo a Anatel, alguns requisitos importantes para as senhas de acesso à *interface* de configurações do equipamento e para acesso à rede sem fio definidas no processo fabril do equipamento.

Alguns dos itens indispensáveis no processo fabril dos equipamentos CPE são: a etiqueta no corpo do equipamento, onde consta a senha de fábrica, sendo que a mesma deve ser restaurada após um *reset*; e o registro no manual do usuário do equipamento, contendo a metodologia utilizada para a verificação de senhas fracas,

e critérios necessários para a definição de senhas conforme pode ser verificado nos quadros 1, 2, 3, 4, 10, 11, 12, 13, 20, 21 e 22.

Além de não poderem receber uma senha fraca conforme definido no item 2.1, os equipamentos precisam estar em conformidade com o Ato 77/2021 da Anatel, que dispões sobre:

a) **Senhas iniciais:** Credenciais e senhas iniciais de acesso às configurações do equipamento não devem ser iguais entre todos os dispositivos produzidos.
b) **Derivação de senhas:** Senhas iniciais não devem ser geradas a partir da derivação de informações facilmente obtidas por escaneamento de tráfego rede, como endereços MAC.
c) **Senhas em branco ou fracas:** O equipamento não deve permitir o uso de senhas em branco ou senhas consideradas fracas.

Caso os equipamentos saiam da fábrica com uma mesma senha em todos os dispositivos, é requirido aos fabricantes que durante a primeira utilização (ou após reset) do equipamento, ele force o usuário a alterar a senha de acesso à *interface* de configurações e para acesso à rede sem fio, evitando assim, senhas padronizadas em equipamentos plenamente operacionais.

Caso o mecanismo de alteração forçada de credenciais seja implementado, é necessário que ele exija a definição de novas senhas utilizando os conceitos de dicionário de senhas e senhas fracas, conforme descrito no item 2.1.

2.3 Requisitos para as senhas definidas pelo usuário

Nesta seção encontram-se, segundo a Anatel, alguns requisitos importantes para as senhas para acesso à *interface* de configurações do equipamento e para acesso à rede sem fio definidas pelo usuário. Os testes de senhas do usuário podem ser verificados nos Quadros 5, 6, 14, 15, 16, 23 e 24.

As senhas definidas pelo usuário devem ser gerenciadas pelos mecanismos implementados pelo fabricante conforme disposto no item 2.2, sendo impossibilitado ao usuário a configuração de senhas fracas ou em branco, utilizando os critérios e mecanismos previamente citados no item 2.1: senhas fracas; e dicionário de senhas.

2.4 Demais requisitos de segurança do equipamento

Nesta seção encontram-se, segundo a Anatel, demais requisitos importantes que visam garantir a conformidade com o Ato 2436 da Anatel, sendo eles:

a) Defesa contra força bruta: Deve existir mecanismos de defesa contra tentativas exaustivas de acesso não autorizado (ataques de força bruta).

b) Credenciais *hard-coded*: O equipamento não deve utilizar credenciais, senhas e chaves criptográficas definidas no código fonte (*hard-coded*) que não podem ser alteradas.

c) Proteção de senhas e credenciais: Utilização de métodos adequados de criptografia ou *hashing* para proteger senhas, chaves de acesso e credenciais armazenadas ou transmitidas.

d) *Timeout* de sessões inativas: Implementação de rotinas de encerramento automático de sessões inativas.

e) Serviços desabilitados por padrão: Serviços de comunicação de dados não usualmente utilizados devem ser desabilitados.

f) Desabilitação de funcionalidades: O equipamento deve atribuir ao usuário a possibilidade de desabilitar funcionalidades e serviços de comunicação não essenciais.

Além do citado acima, o ato 2436 da Anatel enriquece a abordagem, elucidando sobre a importância da robustez do mecanismo de recuperação de senha (caso implementado) contra tentativas de roubo de credenciais, os testes destes itens estão dispostos nos quadros 7, 8, 9, 17, 18, 19, 25, 26 e 27. Assim como para definição de senhas, o registro da metodologia de recuperação de senha adotada deve ser descrito no manual do usuário.

Ao seguir rigorosamente este *checklist*, elaborou-se a análise detalhada da segurança cibernética dos equipamentos CPE, garantindo que os requisitos mínimos estabelecidos pelo Ato nº 2436 da Anatel fossem devidamente verificados na avaliação de conformidade.

2.5 *Softwares* utilizados

Esta seção especifica detalhes técnicos referente à softwares para a realização de testes, e busca-se justificar o papel de cada um e sua contribuição para a análise.

2.5.1 Macro Recorder

O Macro Recorder (versão 5.9.0.0) é empregado para a automatização de tentativas de acesso, simulando ataques de força bruta com cadência controlada.

2.5.2 Wireshark

O Wireshark (versão 4.4.6) é utilizado para a captura e análise dos pacotes de dados trafegados na rede, possibilitando a verificação da estrutura dos pacotes e o diagnóstico de possíveis falhas de segurança.

2.5.3 Nmap

A ferramenta Nmap (versão 7.95) é aplicada para o mapeamento de portas abertas, o que permite avaliar a exposição indevida de interfaces administrativas ou protocolos não autorizados.

2.5.4 Burp Suite

O Burp Suite (versão 2025.2.4) é utilizado em testes de interceptação e manipulação de requisições HTTP, especialmente na análise das *interfaces web* de administração dos roteadores.

A combinação dessas ferramentas permite uma abordagem prática, com foco na verificação de aspectos funcionais e de segurança alinhados aos critérios de conformidade técnica definidos pela regulamentação vigente.

3 ESTUDO DE CASO

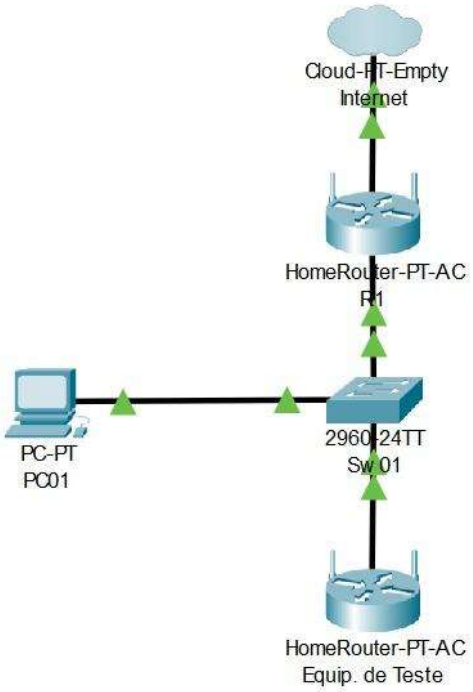
Este estudo de caso tem como objetivo avaliar a conformidade de dispositivos de rede em relação às diretrizes estabelecidas pelo Ato nº 2436 da Anatel, por meio de testes realizados em ambiente controlado com equipamentos domésticos acessíveis.

3.1 Cenário

- Um roteador fornecido pelo provedor de serviços de internet, que atua como *gateway* principal da rede.
- Um *switch* não gerenciável conectado à única porta LAN disponível no roteador do provedor local, que expande o número de portas de rede disponíveis.
- Um computador pessoal conectado via cabo ao *switch*, que aplica os testes de conformidade.
- Um segundo roteador (equipamento em avaliação), também conectado ao *switch*, em qual se conduzem os testes.

O cenário foi pensado em uma representação de uma casa comum no território brasileiro, onde a casa possui somente um provedor de internet, um roteador conectado a ele e um switch conectado ao roteador liberando assim mais portas LAN para a residência onde como dispositivo final tem o computador conforme demonstrado na Figura 1.

Figura 1 - Representação de cenário.



Fonte: Imagem criada pelos autores no Cisco Packet Tracer (2025).

3.1.1 Justificativa de cenário

A escolha deste ambiente se justifica por sua similaridade com configurações comuns em residências brasileiras. Além disso, o uso de um *switch* amplia a possibilidade de conexão para testes, sem interferir na operação do roteador do provedor. Este cenário permite avaliar o comportamento do equipamento em condições realistas de uso, conforme visam os parâmetros estabelecidos pela Anatel.

3.2 Equipamentos

Para a realização deste estudo de caso, foram selecionados três modelos de roteadores wireless da marca TP-Link, sendo eles: TL-WR740N, TL-WR941ND e TL-WP2543ND. A escolha desses dispositivos se motiva pela sua ampla utilização no mercado nacional, visando assim uma abordagem realista da residência do brasileiro.

4 RESULTADOS

4.1 Roteador TP-Link modelo: TL-WR740N(BR)

O TP-link TL-WR740N é um roteador wireless de 150Mbps que opera na frequência 2.4GHz ideal para uso doméstico.

Quadro 1 - Requisitos: Ato 2.436/2023, item 4.1 ao item 4.2[1]

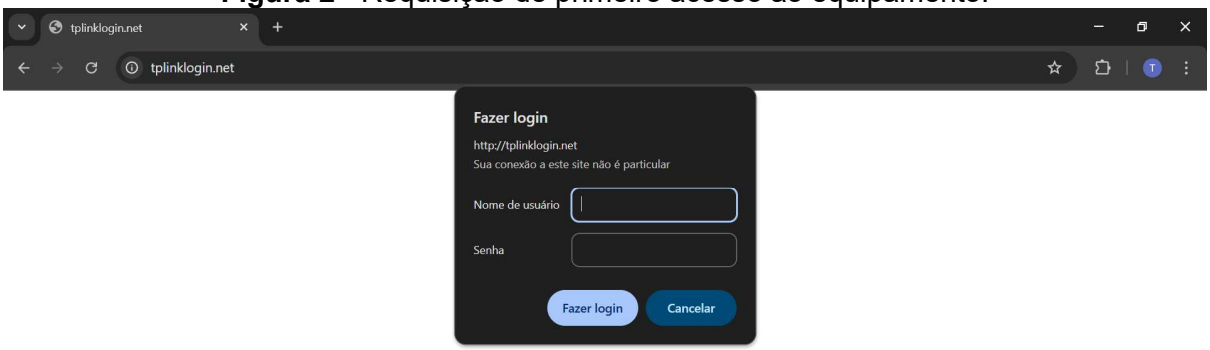
Requisitos do ato	**Resultados obtidos**
4.1. Os requisitos desta seção aplicam-se às senhas: – para acesso à interface de configurações do equipamento, e – para acesso à rede sem fio definidas no processo fabril do equipamento.	O acesso inicial do equipamento é: ● Usuário: admin ● Senha: admin O acesso inicial ao equipamento não atende aos requisitos contidos no item 3.1.3. Na Figura 2 é demonstrado o acesso inicial as configurações do equipamento utilizando as credenciais acima.
4.2. As senhas não podem ser fracas, conforme critérios contidos no item 3.1.3. 3.1.3. Senha fraca: Senha que não atende simultaneamente os seguintes critérios: a) Possuir, no mínimo, 8 caracteres; b) Conter, pelo menos, – uma letra maiúscula, – uma letra minúscula, – um número	

Fonte: Resultados obtidos pelos autores à luz do ato 2.436 da Anatel (2023).

[1] No Quadro 1 foi inserido na coluna esquerda uma transcrição direta do ato 2.436 da Anatel (2023), adicionalmente na coluna direita foram inseridos os resultados obtidos pelos autores.

A Figura 2 visa evidenciar o primeiro acesso realizado no equipamento no padrão de fábrica**.**

Figura 2 - Requisição de primeiro acesso ao equipamento.



Fonte: Autoria própria (2025)

Quadro 2 - Requisitos: Ato 2.436/2023, item 4.3 ao item 4.3b)[2]

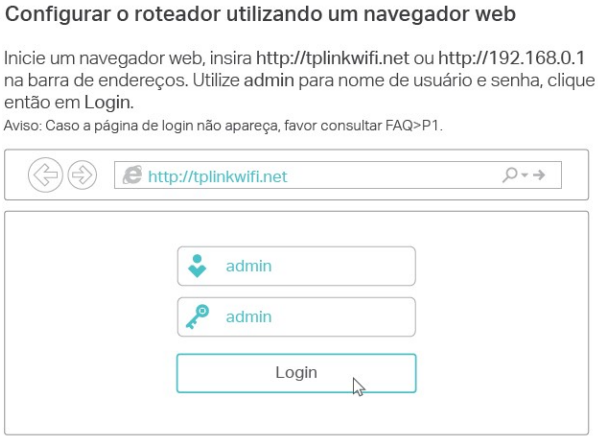
Requisitos do ato	**Resultados obtidos**
4.3. O equipamento deve apresentar conformidade aos seguintes itens dos "Requisitos de Segurança Cibernética para Equipamentos para Telecomunicações":	Não foi possível verificar em dois equipamentos iguais se as senhas iniciais de acesso as configurações eram idênticas, porém em seu manual disponibilizado no site da TP-Link chamado "*TL-WR740(BR)_V7_QIG_1478163261608w*", Na Figura 3 é descrito que para o acesso inicial do equipamento deve-se digitar "admin" nos espaços disponíveis para o usuário e senha.
a) Não utilizar credenciais e senhas iniciais para acesso às suas configurações que sejam iguais entre todos os dispositivos produzidos.	
b) Não utilizar senhas iniciais que sejam derivadas de informações de fácil obtenção por métodos de escaneamento de tráfego de dados em rede, tal como endereços MAC.	As senhas iniciais não são derivadas de informação de fácil obtenção como métodos de escaneamento de rede, endereços MAC etc.

Fonte: Resultados obtidos pelos autores à luz do ato 2.436 da Anatel (2023).

[2] No Quadro 2 foi inserido na coluna esquerda uma transcrição direta do ato 2.436 da Anatel (2023), adicionalmente na coluna direita foram inseridos os resultados obtidos pelos autores.

Na Figura 3 o manual do equipamento do equipamento demonstra com ilustrações e uma boa didática como é feito o primeiro acesso e com quais credenciais.

Figura 3 - Descrição de acesso contida no manual “TL-WR2543ND_V1_QIG_7106504086”.



Fonte: Autoria própria (2025)

Quadro 3 - Requisitos: Ato 2.436/2023, item 4.3 c)[3]

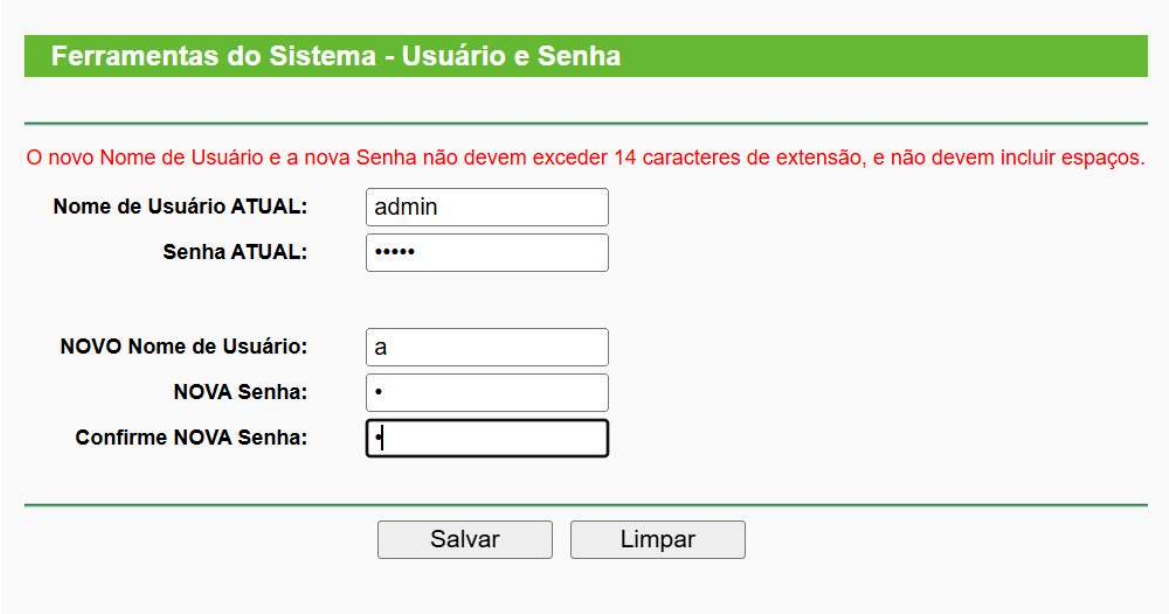
Requisitos do ato	Resultados obtidos
4.3 c) Não permitir o uso de senhas em branco ou senhas fracas.	Foi realizado um teste com o equipamento com as credenciais abaixo: ● Usuário: a ● Senha:1 Na Figura 4 é possível verificar que o equipamento permitiu a utilização destas credenciais. Com isso, o equipamento permite o uso de senhas fracas conforme critérios do item 3.1.3. Já na Figura 5 é possível verificar que o equipamento não permitiu o uso de senhas em branco.

Fonte: Resultados obtidos pelos autores à luz do ato 2.436 da Anatel (2023).

O teste realizado na Figura 4 demonstra quantos caracteres exatamente o software permitiria a alteração de nome do usuário e a senha.

[3] No Quadro 3 foi inserido na coluna esquerda uma transcrição direta do ato 2.436 da Anatel (2023), adicionalmente na coluna direita foram inseridos os resultados obtidos pelos autores.

Figura 4 - Descrição da criação de nova senhas.



Fonte: Autoria própria (2025)

Quadro 4 - Requisitos: Ato 2.436/2023, item 4.4 ao item 4.5[4]

Requisitos do ato	**Resultados obtidos**
4.4. Alternativamente ao atendimento dos requisitos especificados nos itens 4.2 e 4.3, o equipamento poderá forçar, na primeira utilização, a alteração da senha inicial de acesso à sua configuração e das senhas para acesso à rede sem fio, conforme "Requisitos de Segurança Cibernética para Equipamentos para Telecomunicações". 4.4.1. Neste caso, a interface de configuração do equipamento deverá exigir que, – no ato de sua primeira utilização/configuração, ou – após um reset para suas configurações iniciais de fábrica, o usuário defina novas senhas que atendam aos requisitos estabelecidos no item 5. A operação ou configuração do equipamento só poderá ser realizada após a definição de novas senhas.	O equipamento possui um usuário e senha padrão para acesso às suas configurações, não forçando o usuário a alterar a senha no acesso inicial.
4.5. As senhas devem constar em etiqueta no corpo do equipamento, e	Na etiqueta do equipamento consta o usuário e senha padrão de acesso.
4.5. devem ser restauradas sempre que for realizado o reset do equipamento para suas configurações iniciais de fábrica.	Após o *reset* de fábrica, o equipamento restaura a senha e o usuário aos padrões da etiqueta, A Figura 2 visa evidenciar o primeiro acesso realizado no equipamento no padrão de fábrica**.**

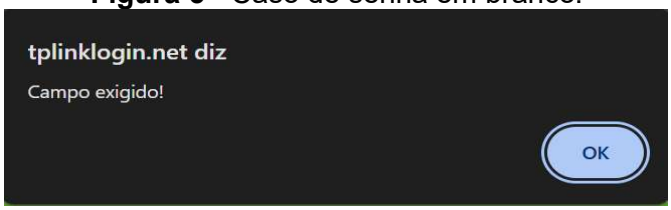
[4] No Quadro 4 foi inserido na coluna esquerda uma transcrição direta do ato 2.436 da Anatel (2023), adicionalmente na coluna direita foram inseridos os resultados obtidos pelos autores.

	Figura 2.

Fonte: Resultados obtidos pelos autores à luz do ato 2.436 da Anatel (2023).

No campo de alteração do nome do usuário e senha se acaso fosse deixado em branco o sistema identificaria e subiria um aviso para que algo fosse digitado conforme demonstrado na Figura 5.

Figura 5 - Caso de senha em branco.



Fonte: Autoria própria (2025)

Quadro 5 – Requisitos: Ato 2.436/2023, item 5.1 ao item 5.2[5]

Requisitos do ato	**Resultados obtidos**
5.1. Os requisitos desta seção aplicam-se às funcionalidades do equipamento relacionadas às senhas definidas pelo usuário: – para acesso à interface de configurações do equipamento, e – para acesso à rede sem fio.	A) O equipamento não permite o uso de senhas em branco conforme evidenciado na Figura 5, porém permite o uso de senhas fracas conforme critérios do item 3.1.3 e evidenciado na Figura 4. B) O equipamento permite senhas fracas conforme critérios do item 3.1.3 evidenciado na Figura 4. C) O manual do equipamento não possui a informação de quantidades mínimas ou máximas para redefinição de senha, ou as regras para sua formação.
5.2. O equipamento deve apresentar conformidade aos seguintes requisitos: a) Não permitir o uso de senhas em branco ou senhas fracas, conforme "Requisitos de Segurança Cibernética para Equipamentos para Telecomunicações". b) Garantir que não sejam definidas senhas fracas, conforme critérios contidos no item 3.1.3. c) O manual do produto, em meio físico ou digital, deve: – informar as quantidades mínima e máxima de caracteres permitidas para definição de senhas, – além da regra para sua formação.	

Fonte: Resultados obtidos pelos autores à luz do ato 2.436 da Anatel (2023).

[5] No Quadro 5 foi inserido na coluna esquerda uma transcrição direta do ato 2.436 da Anatel (2023), adicionalmente na coluna direita foram inseridos os resultados obtidos pelos autores.

Quadro 6 - Requisitos: Ato 2.436/2023, item 5.3 ao item 5.3.1[6]

Requisitos do ato	Resultados obtidos
5.3. O equipamento deve implementar verificações que coíbam a definição de senhas fracas ou comumente utilizadas. A verificação pode ser feita por meio de comparação com dicionários de senha*[1)], sendo permitida a adoção de outra metodologia. 5.3.1. A metodologia adotada deverá ser informada pelo requerente da homologação ao agente responsável pela avaliação da conformidade do produto.	Em teste de troca de senha utilizando um dicionário de senhas do GitHub localizada em "https://github.com/shawntns/top-100-worst-passwords". Todas as senhas foram permitidas no equipamento, sendo assim o ele permite senhas fracas conforme item 3.1.3 e comumente utilizadas conforme item 3.1.1.

Fonte: Resultados obtidos pelos autores à luz do ato 2.436 da Anatel (2023).

Quadro 7 - Requisitos: Ato 2.436/2023, item 6.1 a) ao item 6.1 b)[6]

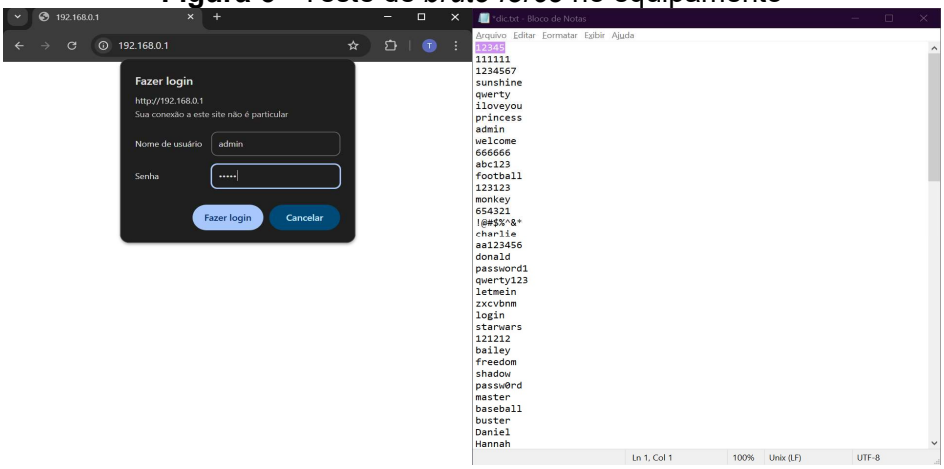
Requisitos do ato	Resultados obtidos
6.1. O equipamento deve apresentar conformidade aos seguintes itens dos "Requisitos de Segurança Cibernética para Equipamentos para Telecomunicações":	O teste de brute force foi feito utilizando o macro recorder, onde utilizando a wordlist localizada em: "https://github.com/shawntns/top-100-worst-passwords" aberta em um bloco de notas foi gravado o primeiro teste de acesso. Com isso foi programado dentro do software a velocidade e a quantidade de vezes em que realizaria o acesso novamente. Ao final do teste o equipamento não evidenciou nenhum tipo de defesa conforme disposto na Figura 6.
a) Possuir mecanismos de defesa contra tentativas exaustivas de acesso não autorizado (ataques de autenticação por força bruta).	
b) Não utilizar credenciais, senhas e chaves criptográficas definidas no próprio código fonte do software / firmware e que não podem ser alteradas (hard-coded).	Não verificado devido à falta de acesso ao código fonte do equipamento.

Fonte: Resultados obtidos pelos autores à luz do ato 2.436 da Anatel (2023).

[6] No Quadro 6 e Quadro 7 ***Quadro 7***foram inseridos na coluna esquerda uma transcrição direta do ato 2.436 da Anatel (2023), adicionalmente na coluna direita foram inseridos os resultados obtidos pelos autores.

A Figura 6 evidência a forma que foi realizada o brute force no equipamento utilizando o macro recorder.

Figura 6 - Teste de *brute force* no equipamento



Fonte: Autoria própria (2025)

Quadro 8 - Requisitos: Ato 2.436/2023, item 6.1 c) ao item 6.1 d)[7]

Requisitos do ato	**Resultados obtidos**
6.1 c) Proteger senhas, chaves de acesso e credenciais armazenadas ou transmitidas utilizando métodos adequados de criptografia ou hashing.	Utilizando o Wireshark, foi verificado dentro da completude de pacotes capturados se era possível localizar o usuário e senha. Dentro do filtro foi utilizado o comando contains que pode localizar algum conteúdo específico dentro dos pacotes de rede. A sintaxe do comando utilizado neste teste ficou: **tcp contains "admin".** Após o teste foi evidenciado que as credenciais transmitidas estão ocultas não sendo possível capturar o usuário e senha.
d) Implementar rotinas de encerramento de sessões inativas *(timeout)*.	Não encontrado na documentação qualquer menção a *timeout* do sistema do equipamento. Foi deixado o equipamento logado por 10 minutos e o *timeout* não ocorreu.

Fonte: Resultados obtidos pelos autores à luz do ato 2.436 da Anatel (2023).

[7] No Quadro 8 ***Quadro 7***foi inserido na coluna esquerda uma transcrição direta do ato 2.436 da Anatel (2023), adicionalmente na coluna direita foram inseridos os resultados obtidos pelos autores.

Quadro 9 - Requisitos: Ato 2.436/2023, item 6.1 e) ao item 6.1 f)[8]

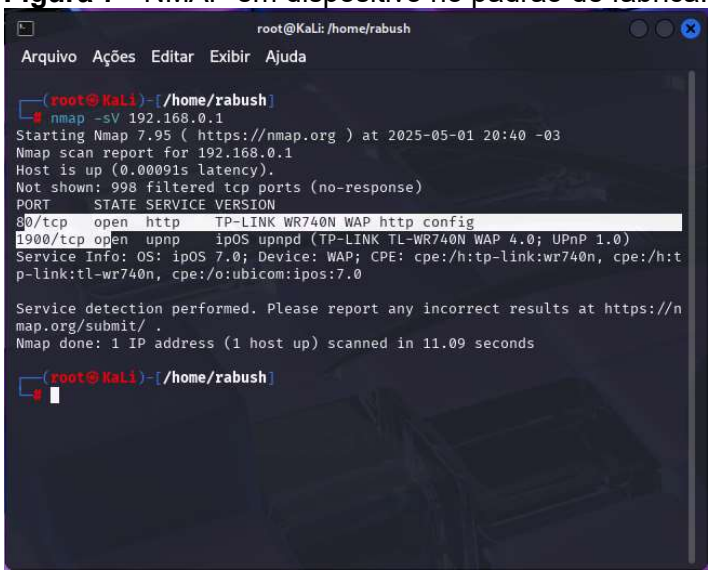
Requisitos do ato	**Resultados obtidos**
e) Ser fornecido com serviços de comunicação de dados (serviço associado a uma porta) não usualmente utilizados desabilitados, reduzindo sua superfície de ataque.	Utilizando o programa NMAP é possível verificar quantas portas abertas filtradas ou fechadas estão no equipamento. Para isso foi utilizando o comando nmap -sV 192.168.0.1 conforme na Figura 7onde: -nmap é a ferramenta de varredura de rede. -sV é uma opção para indicar ao NMAP para tentar identificar as versões dos serviços que estão rodando nas portas abertas do equipamento alvo. 192.168.0.1 é o IP do equipamento alvo. Após o teste é evidenciado que o equipamento possui somente 2 portas abertas.
f) Facultar ao usuário a possibilidade de desabilitar funcionalidades e serviços de comunicação não essenciais à operação ou ao gerenciamento do equipamento.	O equipamento não faculta ao usuário a possibilidade de desabilitar alguns serviços habilitados que não são essenciais à sua operação.

Fonte: Resultados obtidos pelos autores à luz do ato 2.436 da Anatel (2023).

[8] No Quadro ***8***9 ***Quadro 7***foi inserido na coluna esquerda uma transcrição direta do ato 2.436 da Anatel (2023), adicionalmente na coluna direita foram inseridos os resultados obtidos pelos autores.

Na Figura 7 é possível ver as portas abertas no equipamento por padrão de fábrica além dos programas e versão que estão funcionando nela.

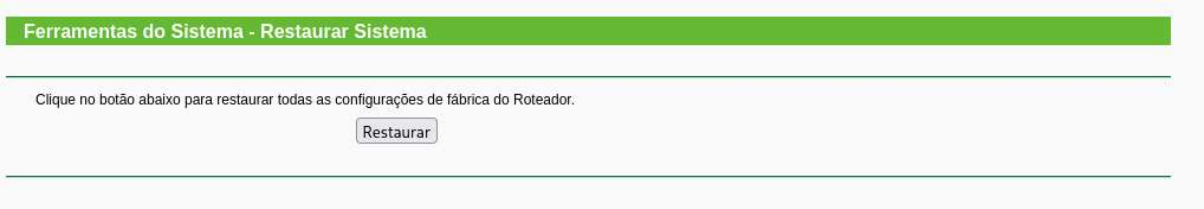
Figura 7 - NMAP em dispositivo no padrão de fábrica.



Fonte: Autoria própria (2025)

Dentro das configurações avançadas do equipamento possui uma aba somente para o reset de fábrica na web conforme evidenciado na Figura 8.

Figura 8 - Reset do equipamento via *web*.



Fonte: Autoria própria (2025)

4.2 Roteador TP-Link modelo: TL-WP2543ND

O TP-link TL-WP2543ND é um roteador wireless de 450Mbps que opera na frequência 2.4GHz e 5GHz ideal para uso doméstico.

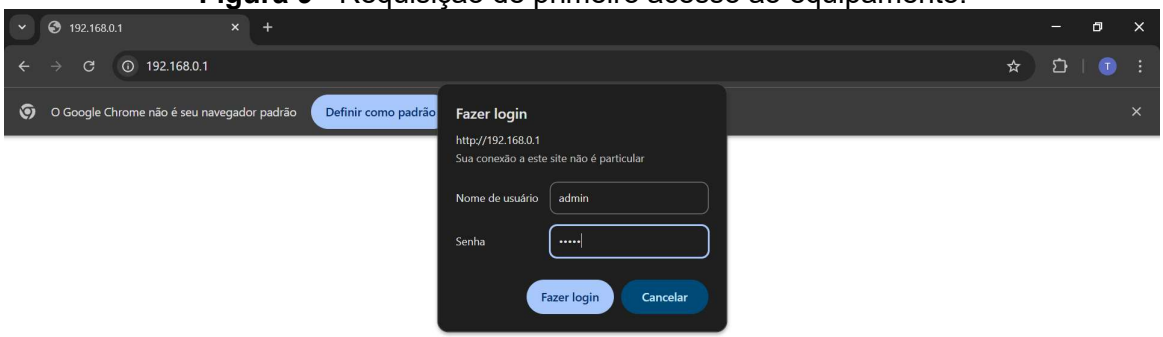
Quadro 10 - Requisitos: Ato 2.436/2023, item 4.1 ao item 4.2[9]

Requisitos do ato	**Resultados obtidos**
4.1. Os requisitos desta seção aplicam-se às senhas: – para acesso à interface de configurações do equipamento, e – para acesso à rede sem fio definidas no processo fabril do equipamento.	Nenhum teste aplicável.
4.2. As senhas não podem ser fracas, conforme critérios contidos no item 3.1.3. 3.1.3. Senha fraca: Senha que não atende simultaneamente os seguintes critérios: a) Possuir, no mínimo, 8 caracteres; b) Conter, pelo menos, – uma letra maiúscula, – uma letra minúscula, – um número	O acesso inicial do equipamento é: ● Usuário: admin ● Senha: admin O acesso inicial ao equipamento não atende aos requisitos contidos no item 3.1.3 Na Figura 9 é demonstrado o acesso inicial as configurações do equipamento utilizando as credenciais acima.

Fonte: Resultados obtidos pelos autores à luz do ato 2.436 da Anatel (2023).

A Figura 9 visa evidenciar o primeiro acesso realizado no equipamento no padrão de fábrica**.**

Figura 9 - Requisição de primeiro acesso ao equipamento.



Fonte: Autoria própria (2025)

[9] No Quadro ***10*** 10 foi inserido na coluna esquerda uma transcrição direta do ato 2.436 da Anatel (2023), adicionalmente na coluna direita foram inseridos os resultados obtidos pelos autores.

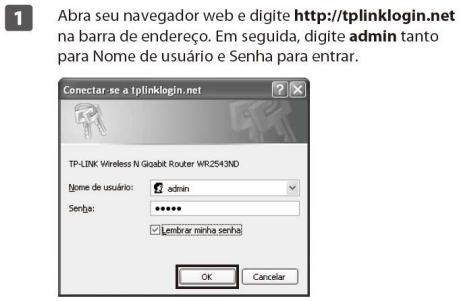
Quadro 11 - Requisitos: Ato 2.436/2023, item 4.3 a)[10]

Requisitos do ato	Resultados obtidos
4.3. O equipamento deve apresentar conformidade aos seguintes itens dos "Requisitos de Segurança Cibernética para Equipamentos para Telecomunicações": a) Não utilizar credenciais e senhas iniciais para acesso às suas configurações que sejam iguais entre todos os dispositivos produzidos.	Não foi possível verificar em dois equipamentos iguais se as senhas iniciais de acesso as configurações eram idênticas, porém em seu manual disponibilizado no site da TP-Link chamado “TL-WR2543ND_V1_QIG_7106504086” descreve as que para o acesso inicial do equipamento deve-se digitar “admin” nos espaços disponíveis para o usuário e senha, conforme a figura 10.

Fonte: Resultados obtidos pelos autores à luz do ato 2.436 da Anatel (2023).

Na Figura 10 o manual do equipamento do equipamento demonstra com ilustrações e uma boa didática como é feito o primeiro acesso e com quais credenciais.

Figura 10 - Descrição de acesso contida no manual “TL-WR2543ND_V1_QIG_7106504086”.



Fonte: Autoria própria (2025)

[10] No Quadro 11 foi inserido na coluna esquerda uma transcrição direta do ato 2.436 da Anatel (2023), adicionalmente na coluna direita foram inseridos os resultados obtidos pelos autores.

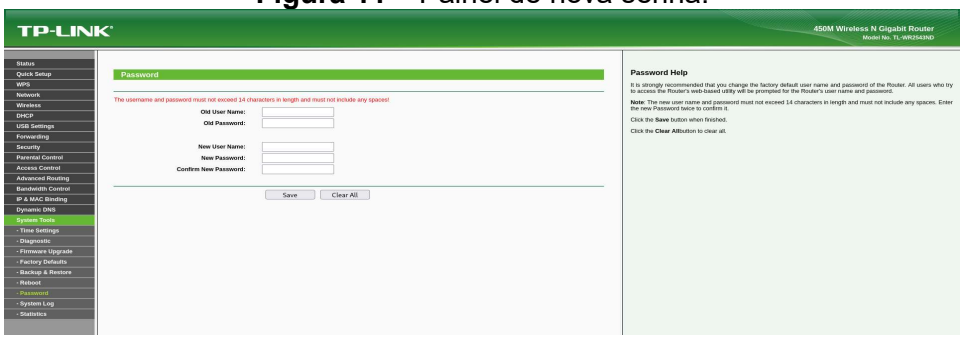
Quadro 12 - Requisitos: Ato 2.436/2023, item 4.3 b) ao item 4.3 c)[11]

Requisitos do ato	**Resultados obtidos**
4.3 b) Não utilizar senhas iniciais que sejam derivadas de informações de fácil obtenção por métodos de escaneamento de tráfego de dados em rede, tal como endereços MAC.	As senhas iniciais não são derivadas de informação de fácil obtenção como métodos de escaneamento de rede, endereços MAC etc.
c) Não permitir o uso de senhas em branco ou senhas fracas.	O equipamento permite o uso de senhas fracas conforme critérios contidos no item 3.1.3. Na Figura 11 é possível ver o painel de alteração de senhas com as informações de alteração.

Fonte: Resultados obtidos pelos autores à luz do ato 2.436 da Anatel (2023).

O teste realizado na Figura 11 demonstra quantos caracteres exatamente o software permitiria a alteração de nome do usuário e a senha.

Figura 11 – Painel de nova senha.



Fonte: Autoria própria (2025)

[11] No Quadro 12 foi inserido na coluna esquerda uma transcrição direta do ato 2.436 da Anatel (2023), adicionalmente na coluna direita foram inseridos os resultados obtidos pelos autores.

Quadro 13 - Requisitos: Ato 2.436/2023, item 4.4 ao item 4.5[12]

Requisitos do ato	**Resultados obtidos**
4.4. Alternativamente ao atendimento dos requisitos especificados nos itens 4.2 e 4.3, o equipamento poderá forçar, na primeira utilização, a alteração da senha inicial de acesso à sua configuração e das senhas para acesso à rede sem fio, conforme "Requisitos de Segurança Cibernética para Equipamentos para Telecomunicações". 4.4.1. Neste caso, a interface de configuração do equipamento deverá exigir que, – no ato de sua primeira utilização/configuração, ou – após um reset para suas configurações iniciais de fábrica, o usuário defina novas senhas que atendam aos requisitos estabelecidos no item 5. A operação ou configuração do equipamento só poderá ser realizada após a definição de novas senhas.	O equipamento possui um usuário e senha padrão para acesso às suas configurações, não forçando o usuário a alterar a senha no acesso inicial.
4.5. As senhas devem constar em etiqueta no corpo do equipamento, e	Na etiqueta do equipamento consta o usuário e senha padrão de acesso.
4.5. devem ser restauradas sempre que for realizado o reset do equipamento para suas configurações iniciais de fábrica.	Após o reset de fábrica, o equipamento restaura a senha e o usuário aos padrões da etiqueta conforme evidenciado na Figura 9.

Fonte: Resultados obtidos pelos autores à luz do ato 2.436 da Anatel (2023).

[12] No Quadro 13 foi inserido na coluna esquerda uma transcrição direta do ato 2.436 da Anatel (2023), adicionalmente na coluna direita foram inseridos os resultados obtidos pelos autores.

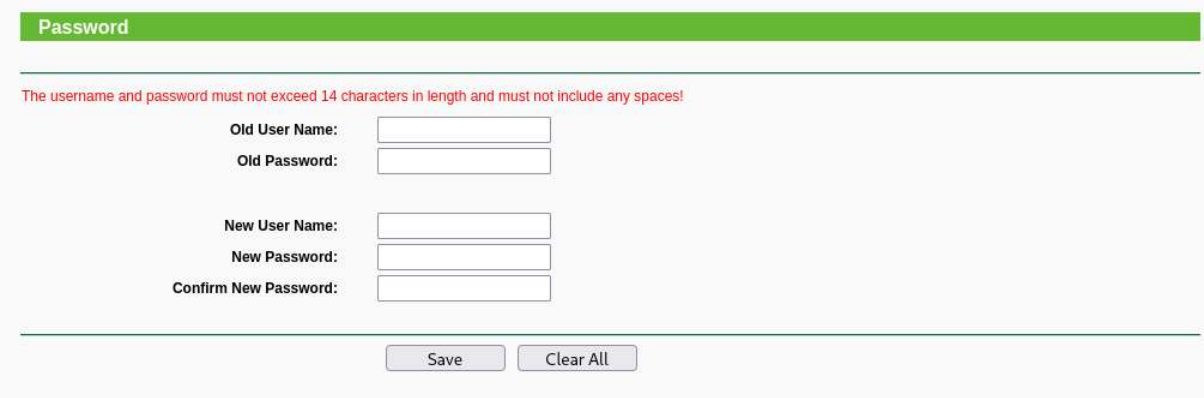
Quadro 14 - Requisitos: Ato 2.436/2023, item 5.1 ao item 5.2 b)[13]

Requisitos do ato	**Resultados obtidos**
5.1. Os requisitos desta seção aplicam-se às funcionalidades do equipamento relacionadas às senhas definidas pelo usuário: – para acesso à interface de configurações do equipamento, e – para acesso à rede sem fio.	Nenhum teste aplicável.
5.2. O equipamento deve apresentar conformidade aos seguintes requisitos: a) Não permitir o uso de senhas em branco ou senhas fracas, conforme "Requisitos de Segurança Cibernética para Equipamentos para Telecomunicações". b) Garantir que não sejam definidas senhas fracas, conforme critérios contidos no item 3.1.3.	A) O equipamento não permite o uso de senhas em branco conforme evidenciado na Figura 13, porém o equipamento permite senhas fracas conforme o teste realizado e exibido na Figura 12. B) O equipamento permite senhas fracas conforme critérios do item 3.1.3. É possível verificar os critérios de formação da senha na Figura 12.

Fonte: Resultados obtidos pelos autores à luz do ato 2.436 da Anatel (2023).

O teste realizado na Figura 12 demonstra quantos caracteres exatamente o software permitiria a alteração de nome do usuário e a senha.

Figura 12 - Troca de senhas no dispositivo.

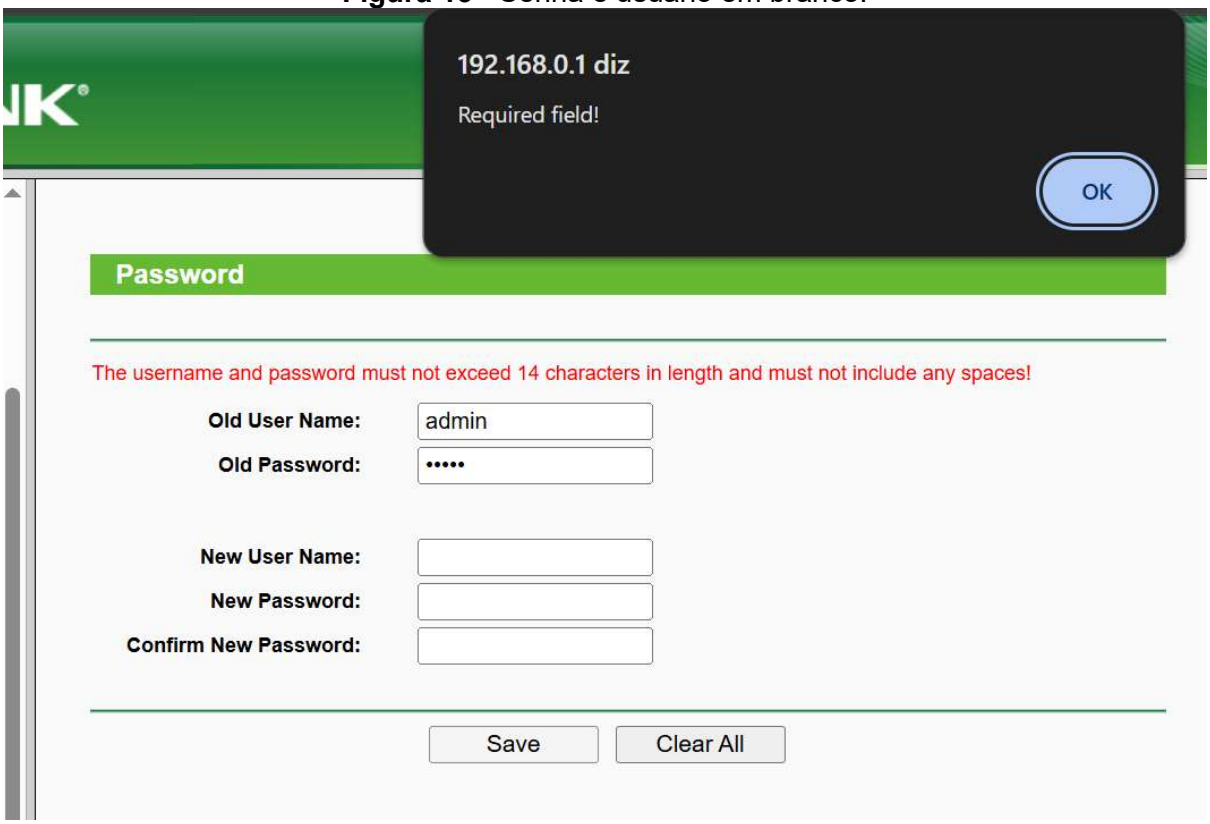


Fonte: Autoria própria (2025)

[13] No Quadro 14 foi inserido na coluna esquerda uma transcrição direta do ato 2.436 da Anatel (2023), adicionalmente na coluna direita foram inseridos os resultados obtidos pelos autores.

No campo de alteração do nome do usuário e senha se acaso fosse deixado em branco o sistema identificaria e subiria um aviso para que algo fosse digitado conforme demonstrado na Figura 13.

Figura 13 - Senha e usuário em branco.



Fonte: Autoria própria (2025)

Quadro 15 - Requisitos: Ato 2.436/2023, item 5.2 c)[14]

Requisitos do ato	Resultados obtidos
5.2 c) O manual do produto, em meio físico ou digital, deve: – informar as quantidades mínima e máxima de caracteres permitidas para definição de senhas, – além da regra para sua formação.	C) O manual do equipamento não possui a informação de quantidades mínimas ou máximas para redefinição de senha, ou as regras para sua formação.

Fonte: Resultados obtidos pelos autores à luz do ato 2.436 da Anatel (2023).

[14] No Quadro 15 foi inserido na coluna esquerda uma transcrição direta do ato 2.436 da Anatel (2023), adicionalmente na coluna direita foram inseridos os resultados obtidos pelos autores.

Quadro 16 - Requisitos: Ato 2.436/2023, item 5.3 ao item 5.3.1[15]

Requisitos do ato	Resultados obtidos
5.3. O equipamento deve implementar verificações que coíbam a definição de senhas fracas ou comumente utilizadas. A verificação pode ser feita por meio de comparação com dicionários de senha*1), sendo permitida a adoção de outra metodologia. 5.3.1. A metodologia adotada deverá ser informada pelo requerente da homologação ao agente responsável pela avaliação da conformidade do produto.	Em teste de troca de senha utilizando um dicionário de senhas do GitHub localizada em “https://github.com/shawntns/top-100-worst-passwords”. Todas as senhas foram permitidas no equipamento, com isso o mesmo permite senhas fracas e comumente utilizadas conforme item 3.1.1, e evidenciado pela Figura 14.

Quadro 17 - Requisitos: Ato 2.436/2023, item 6.1 ao item 6.1 c)[15]

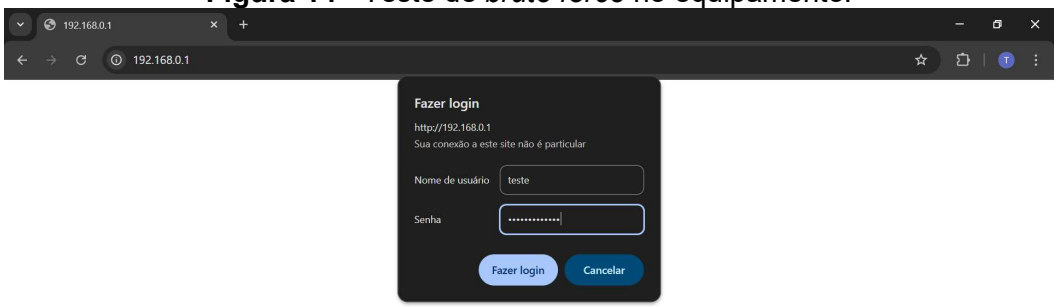
Requisitos do ato	Resultados obtidos
6.1. O equipamento deve apresentar conformidade aos seguintes itens dos "Requisitos de Segurança Cibernética para Equipamentos para Telecomunicações":	O teste de brute force foi feito utilizando o macro recorder, onde utilizando a wordlist localizada em: “https://github.com/shawntns/top-100-worst-passwords” aberta em um bloco de notas foi gravado o primeiro teste de acesso. Com isso foi programado dentro do software a velocidade e a quantidade de vezes em que realizaria o acesso novamente. Ao final do teste o equipamento não evidenciou nenhum tipo de defesa conforme disposto na Figura 14.
a) Possuir mecanismos de defesa contra tentativas exaustivas de acesso não autorizado (ataques de autenticação por força bruta).	

Fonte: Resultados obtidos pelos autores à luz do ato 2.436 da Anatel (2023).

[15] No Quadro 16 e no Quadro 17 ***Quadro 7***foram inseridos na coluna esquerda uma transcrição direta do ato 2.436 da Anatel (2023), adicionalmente na coluna direita foram inseridos os resultados obtidos pelos autores.

A Figura 14 evidencia a forma que foi realizada o brute force no equipamento utilizando o macro recorder.

Figura 14 - Teste de *brute force* no equipamento.



Fonte: Autoria própria (2025)

Quadro 18 - Requisitos: Ato 2.436/2023, item 6.1 b) ao item 6.1 c) [16]

Requisitos do ato	**Resultados obtidos**
6.1 b) Não utilizar credenciais, senhas e chaves criptográficas definidas no próprio código fonte do software / firmware e que não podem ser alteradas (hard-coded).	Não verificado devido à falta de acesso ao código fonte.
c) Proteger senhas, chaves de acesso e credenciais armazenadas ou transmitidas utilizando métodos adequados de criptografia ou hashing.	Utilizando o Wireshark, foi verificado dentro da completude de pacotes capturados se era possível localizar o usuário e senha. Dentro do filtro foi utilizado o comando **contains** que pode localizar algum conteúdo específico dentro dos pacotes de rede. A sintaxe do comando utilizado neste teste ficou: **tcp contains "admin".** Após o teste foi evidenciado que as credenciais transmitidas estão ocultas não sendo possível capturar o usuário e senha.

Fonte: Resultados obtidos pelos autores à luz do ato 2.436 da Anatel (2023).

[16] No Quadro 18 foi inserido na coluna esquerda uma transcrição direta do ato 2.436 da Anatel (2023), adicionalmente na coluna direita foram inseridos os resultados obtidos pelos autores.

Quadro 19 - Requisitos: Ato 2.436/2023, item 6.1 d) ao item 6.2.1[17]

Requisitos do ato	**Resultados obtidos**
6.1 d) Implementar rotinas de encerramento de sessões inativas (timeout).	Não encontrado na documentação qualquer menção a timeout do sistema do equipamento. Foi deixado o equipamento logado por 10 minutos e o timeout não ocorreu.
e) Ser fornecido com serviços de comunicação de dados (serviço associado a uma porta/port) não usualmente utilizados desabilitados, reduzindo sua superfície de ataque.	Utilizando o programa NMAP é possível verificar quantas portas abertas filtradas ou fechadas estão no equipamento. Para isso foi utilizando o comando nmap -sV 192.168.0.1 conforme a Figura 15, onde: -nmap é a ferramenta de varredura de rede. -sV é uma opção para indicar ao NMAP para tentar identificar as versões dos serviços que estão rodando nas portas abertas do equipamento alvo. 192.168.0.1 é o IP do equipamento alvo. Após o teste é evidenciado que o equipamento possui somente 4 portas abertas.
f) Facultar ao usuário a possibilidade de desabilitar funcionalidades e serviços de comunicação não essenciais à operação ou ao gerenciamento do equipamento.	O equipamento não faculta ao usuário a possibilidade de desabilitar alguns serviços habilitados que não são essenciais à sua operação.
6.2. O mecanismo de recuperação de senha, caso implementado no equipamento, deverá ser robusto contra tentativas de roubo de credenciais, conforme item dos "Requisitos de Segurança Cibernética para Equipamentos para Telecomunicações". **6.2.1.** O mecanismo adotado deverá ser informado pelo requerente da homologação ao agente responsável pela avaliação da conformidade do produto.	O mecanismo para recuperação de senha conforme o fabricante é o reset físico do equipamento restaurando assim o padrão de fábrica.

Fonte: Resultados obtidos pelos autores à luz do ato 2.436 da Anatel (2023).

[17] No Quadro 19 foi inserido na coluna esquerda uma transcrição direta do ato 2.436 da Anatel (2023), adicionalmente na coluna direita foram inseridos os resultados obtidos pelos autores.

Na Figura 15 é possível ver as portas abertas no equipamento por padrão de fábrica além dos programas e versão que estão funcionando nela.

Figura 15 - NMAP em dispositivo no padrão de fábrica.

Fonte: Autoria própria (2025)

4.3 Roteador TP-Link modelo: TL-WR941ND

O TP-link TL-WR941ND é um roteador wireless de 300Mbps que opera na frequência 2.4GHz ideal para uso doméstico.

Quadro 20 - Requisitos: Ato 2.436/2023, item 4.1 ao item 4.1 b)[18]

Requisitos do ato	**Resultados obtidos**
4.1. Os requisitos desta seção aplicam-se às senhas: – para acesso à interface de configurações do equipamento, e – para acesso à rede sem fio definidas no processo fabril do equipamento.	Nenhum teste aplicável.
4.2. As senhas não podem ser fracas, conforme critérios contidos no item 3.1.3. 3.1.3. Senha fraca: Senha que não atende simultaneamente os seguintes critérios: a) Possuir, no mínimo, 8 caracteres; b) Conter, pelo menos, – uma letra maiúscula, – uma letra minúscula, – um número	O acesso inicial do equipamento é: ● Usuário: admin ● Senha: admin O acesso inicial ao equipamento não atende aos requisitos contidos no item 3.1.3. Na Figura 16 é demonstrado a página de acesso inicial as configurações do equipamento onde é utilizado as credenciais acima.
4.3. O equipamento deve apresentar conformidade aos seguintes itens dos "Requisitos de Segurança Cibernética para Equipamentos para Telecomunicações":	Não foi possível verificar em dois equipamentos iguais se as senhas iniciais de acesso as configurações eram idênticas, porém em seu manual disponibilizado no site da TP-Link chamado “TL-WR941ND_V6_QIG”, é descrito que para o acesso inicial do equipamento deve-se digitar “admin” nos espaços disponíveis para o usuário e senha, ver Figura 17.
a) Não utilizar credenciais e senhas iniciais para acesso às suas configurações que sejam iguais entre todos os dispositivos produzidos.	
b) Não utilizar senhas iniciais que sejam derivadas de informações de fácil obtenção por métodos de escaneamento de tráfego de dados em rede, tal como endereços MAC.	As senhas iniciais não são derivadas de informação de fácil obtenção como métodos de escaneamento de rede, endereços MAC etc.

Fonte: Resultados obtidos pelos autores à luz do ato 2.436 da Anatel (2023).

[18] No Quadro 20 foi inserido na coluna esquerda uma transcrição direta do ato 2.436 da Anatel (2023), adicionalmente na coluna direita foram inseridos os resultados obtidos pelos autores.

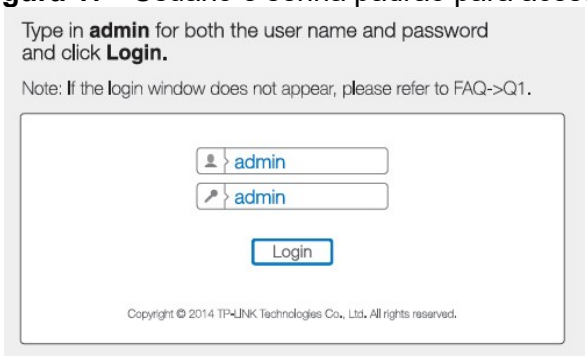
A Figura 16 visa evidenciar o primeiro acesso realizado no equipamento no padrão de fábrica**.**

Figura 16 - Requisição de primeiro acesso ao equipamento.

Fonte: Autoria própria (2025)

Na Figura 17 o manual do equipamento do equipamento demonstra com ilustrações e uma boa didática como é feito o primeiro acesso e com quais credenciais.

Figura 17 - Usuário e senha padrão para acesso



Fonte: Autoria própria (2025)

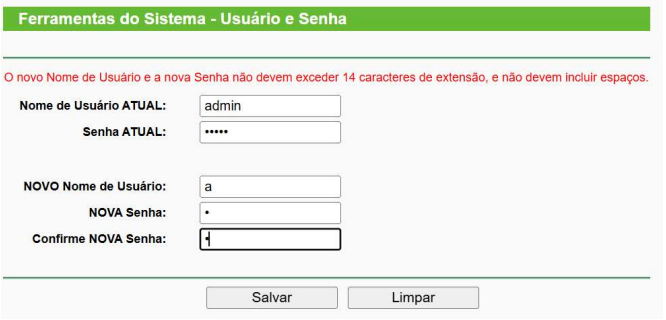
Quadro 21 - Requisitos: Ato 2.436/2023, item 4.1 c)[19]

Requisitos do ato	Resultados obtidos
4.3 c) Não permitir o uso de senhas em branco ou senhas fracas.	Foi realizado um teste com o equipamento com as credenciais abaixo: ● Usuário: a ● Senha:1 Na Figura 18 é possível verificar que o equipamento permitiu a utilização destas credenciais. Com isso, o equipamento permite o uso de senhas fracas conforme critérios do item 3.1.3. Já na Figura 19 é possível verificar que o equipamento não permitiu o uso de senhas em branco.

Fonte: Resultados obtidos pelos autores à luz do ato 2.436 da Anatel (2023).

O teste realizado na Figura 18 demonstra quantos caracteres exatamente o software permitiria a alteração de nome do usuário e a senha.

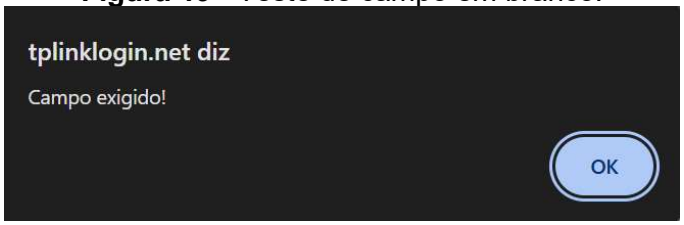
Figura 18 - Teste de novo usuário e senha.



Fonte: Autoria própria (2025)

No campo de alteração do nome do usuário e senha se acaso fosse deixado em branco o sistema identificaria e subiria um aviso para que algo fosse digitado conforme demonstrado na Figura 19.

Figura 19 - Teste de campo em branco.



Fonte: Autoria própria (2025)

[19] No Quadro 21 foi inserido na coluna esquerda uma transcrição direta do ato 2.436 da Anatel (2023), adicionalmente na coluna direita foram inseridos os resultados obtidos pelos autores.

Quadro 22 - Requisitos: Ato 2.436/2023, item 4.4 ao item 4.5[20]

Requisitos do ato	**Resultados obtidos**
4.4. Alternativamente ao atendimento dos requisitos especificados nos itens 4.2 e 4.3, o equipamento poderá forçar, na primeira utilização, a alteração da senha inicial de acesso à sua configuração e das senhas para acesso à rede sem fio, conforme "Requisitos de Segurança Cibernética para Equipamentos para Telecomunicações". 4.4.1. Neste caso, a interface de configuração do equipamento deverá exigir que, – no ato de sua primeira utilização/configuração, ou – após um reset para suas configurações iniciais de fábrica, o usuário defina novas senhas que atendam aos requisitos estabelecidos no item 5. A operação ou configuração do equipamento só poderá ser realizada após a definição de novas senhas.	O equipamento possui um usuário e senha padrão para acesso às suas configurações, não forçando o usuário a alterar a senha no acesso inicial.
4.5. As senhas devem constar em etiqueta no corpo do equipamento, e	Na etiqueta do equipamento consta o usuário e senha padrão de acesso.
4.5. devem ser restauradas sempre que for realizado o reset do equipamento para suas configurações iniciais de fábrica.	Após o *reset* de fábrica, o equipamento restaura a senha e o usuário aos padrões da etiqueta, onde novamente é feito o primeiro acesso conforme a Figura 16

Fonte: Resultados obtidos pelos autores à luz do ato 2.436 da Anatel (2023).

Quadro 23 - Requisitos: Ato 2.436/2023, item 5.1[20]

Requisitos do ato	**Resultados obtidos**
5.1. Os requisitos desta seção aplicam-se às funcionalidades do equipamento relacionadas às senhas definidas pelo usuário: – para acesso à interface de configurações do equipamento, e – para acesso à rede sem fio.	Nenhum teste aplicável.

Fonte: Resultados obtidos pelos autores à luz do ato 2.436 da Anatel (2023).

[20] No Quadro 22 e Quadro 23 foi inserido na coluna esquerda uma transcrição direta do ato 2.436 da Anatel (2023), adicionalmente na coluna direita foram inseridos os resultados obtidos pelos autores.

Quadro 24 - Requisitos: Ato 2.436/2023, item 5.2 ao item 5.3.1[21]

Requisitos do ato	**Resultados obtidos**
5.2. O equipamento deve apresentar conformidade aos seguintes requisitos: a) Não permitir o uso de senhas em branco ou senhas fracas, conforme "Requisitos de Segurança Cibernética para Equipamentos para Telecomunicações". b) Garantir que não sejam definidas senhas fracas, conforme critérios contidos no item 3.1.3. c) O manual do produto, em meio físico ou digital, deve: – informar as quantidades mínima e máxima de caracteres permitidas para definição de senhas, – além da regra para sua formação.	A) O equipamento não permite o uso de senhas em branco conforme evidenciado na Figura 19, porém permite o uso de senhas fracas conforme critérios do item 3.1.3 e evidenciado na Figura 18 B) O equipamento permite senhas fracas conforme critérios contidos no item 3.1.3 evidenciado na Figura 18. C) Nenhum dos manuais do equipamento possui a informação de quantidades mínimas ou máximas para redefinição de senha ou as regras para sua formação.
5.3. O equipamento deve implementar verificações que coíbam a definição de senhas fracas ou comumente utilizadas. A verificação pode ser feita por meio de comparação com dicionários de senha*1), sendo permitida a adoção de outra metodologia. 5.3.1. A metodologia adotada deverá ser informada pelo requerente da homologação ao agente responsável pela avaliação da conformidade do produto.	Foi feita uma verificação com um dicionário de senhas do GitHub localizada em "https://github.com/shawntns/top-100-worst-passwords". Todas as senhas passaram no equipamento, sendo assim o equipamento permite senhas fracas e comumente utilizadas conforme item 3.1.1 e evidenciado pela Figura 20.

Fonte: Resultados obtidos pelos autores à luz do ato 2.436 da Anatel (2023).

[21] No Quadro 24 foi inserido na coluna esquerda uma transcrição direta do ato 2.436 da Anatel (2023), adicionalmente na coluna direita foram inseridos os resultados obtidos pelos autores.

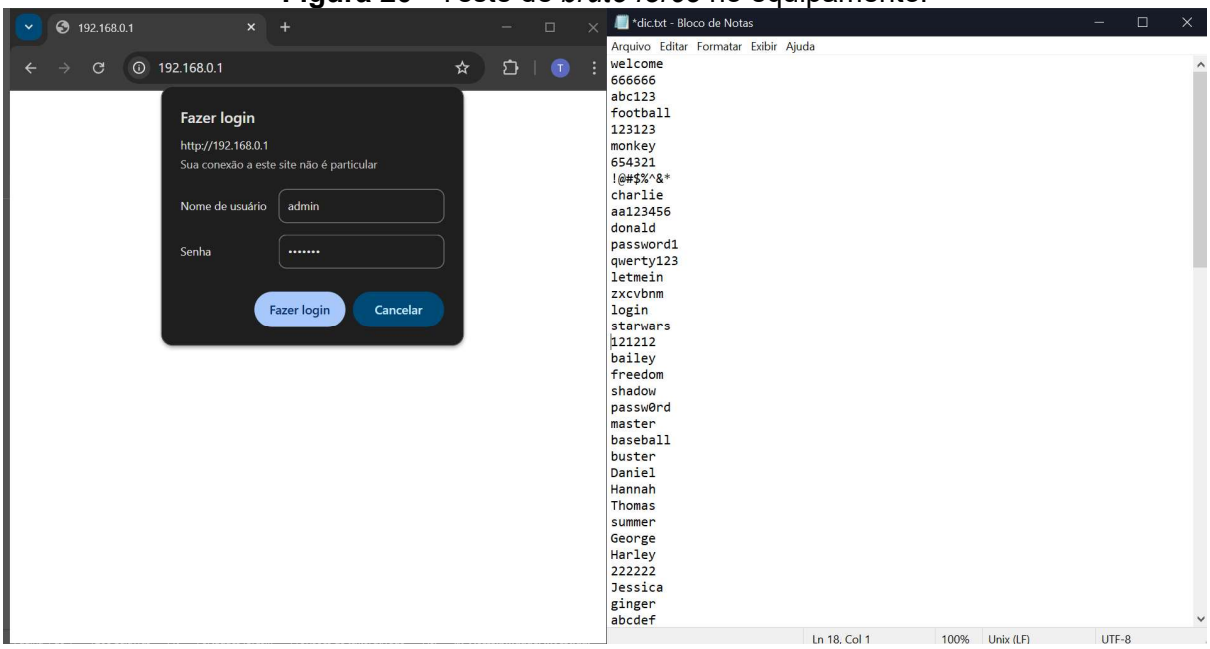
Quadro 25 - Requisitos: Ato 2.436/2023, item 6.1 ao item 6.1 b)[22]

Requisitos do ato	**Resultados obtidos**
6.1. a) Possuir mecanismos de defesa contra tentativas exaustivas de acesso não autorizado (ataques de autenticação por força bruta).	O teste de brute force foi feito utilizando o macro recorder, onde utilizando a wordlist localizada em: "https://github.com/shawntns/top-100-worst-passwords" aberta em um bloco de notas foi gravado o primeiro teste de acesso. Com isso foi programado dentro do software a velocidade e a quantidade de vezes em que realizaria o acesso novamente. Ao final do teste o equipamento não evidenciou nenhum tipo de defesa conforme disposto na Figura 20.
b) Não utilizar credenciais, senhas e chaves criptográficas definidas no próprio código fonte do software / firmware e que não podem ser alteradas (hard-coded).	Não verificado devido à falta de acesso ao código fonte.

Fonte: Resultados obtidos pelos autores à luz do ato 2.436 da Anatel (2023).

A Figura *20 evidência a forma que foi realizada o brute force no equipamento utilizando o macro recorder.*

Figura 20 - Teste de *brute force* no equipamento.



Fonte: Autoria própria (2025)

[22] No Quadro 25 foi inserido na coluna esquerda uma transcrição direta do ato 2.436 da Anatel (2023), adicionalmente na coluna direita foram inseridos os resultados obtidos pelos autores.

Quadro 26 - Requisitos: Ato 2.436/2023, item 6.1 c) ao item 6.1 f)[23]

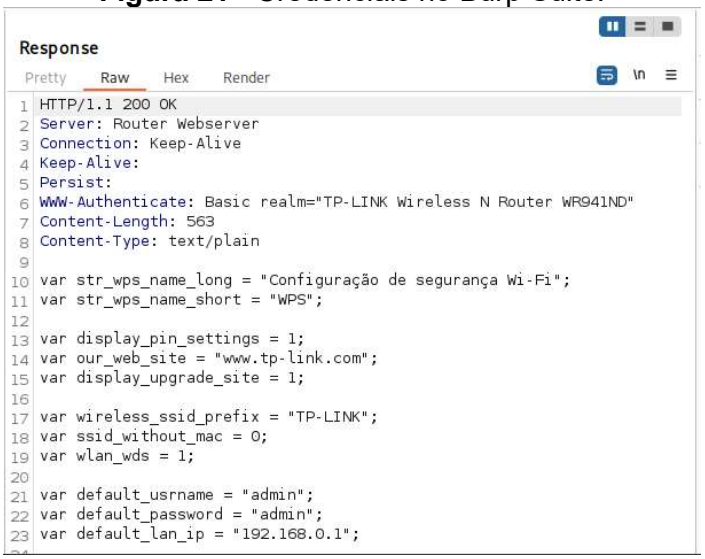
Requisitos do ato	Resultados obtidos
c) Proteger senhas, chaves de acesso e credenciais armazenadas ou transmitidas utilizando métodos adequados de criptografia ou hashing.	Utilizando o Wireshark, foi verificado dentro da completude de pacotes capturados se era possível localizar o usuário e senha. Dentro do filtro foi utilizado o comando contains que pode localizar algum conteúdo específico dentro dos pacotes de rede. A sintaxe do comando utilizado neste teste ficou: **tcp contains "admin".** Após o teste foi evidenciado que as credenciais transmitidas estão ocultas não sendo possível capturar o usuário e senha. Porém no Burp Suite, foi possível verificar que o equipamento em cada requisição de acesso envia também o usuário e senha padrão conforme evidenciado na Figura 21.
d) Implementar rotinas de encerramento de sessões inativas (timeout).	Não encontrado na documentação qualquer menção a timeout do sistema do equipamento. Foi deixado o equipamento logado por 10 minutos e o timeout não ocorreu.
e) Ser fornecido com serviços de comunicação de dados (serviço associado a uma porta/port) não usualmente utilizados desabilitados, reduzindo sua superfície de ataque.	Utilizando o programa NMAP é possível verificar quantas portas abertas filtradas ou fechadas estão no equipamento. Para isso foi utilizando o comando nmap -sV 192.168.0.1 conforme a Figura 22 onde: -nmap é a ferramenta de varredura de rede. -sV é uma opção para indicar ao NMAP para tentar identificar as versões dos serviços que estão rodando nas portas abertas do equipamento alvo. 192.168.0.1 é o IP do equipamento alvo. Após o teste é evidenciado que o equipamento possui somente 3 portas abertas.
f) Facultar ao usuário a possibilidade de desabilitar funcionalidades e serviços de comunicação não essenciais à operação ou ao gerenciamento do equipamento.	O equipamento não faculta ao usuário a possibilidade de desabilitar alguns serviços habilitados que não são essenciais à sua operação.

Fonte: Resultados obtidos pelos autores à luz do ato 2.436 da Anatel (2023).

[23] No Quadro 26 foi inserido na coluna esquerda uma transcrição direta do ato 2.436 da Anatel (2023), adicionalmente na coluna direita foram inseridos os resultados obtidos pelos autores.

Foi verificado dentro do programa burp suíte que as credenciais padrões de fábrica (usuário: admin e senha: admin) eram enviadas todas as vezes junto com a requisição de login conforme evidenciado na Figura 21.

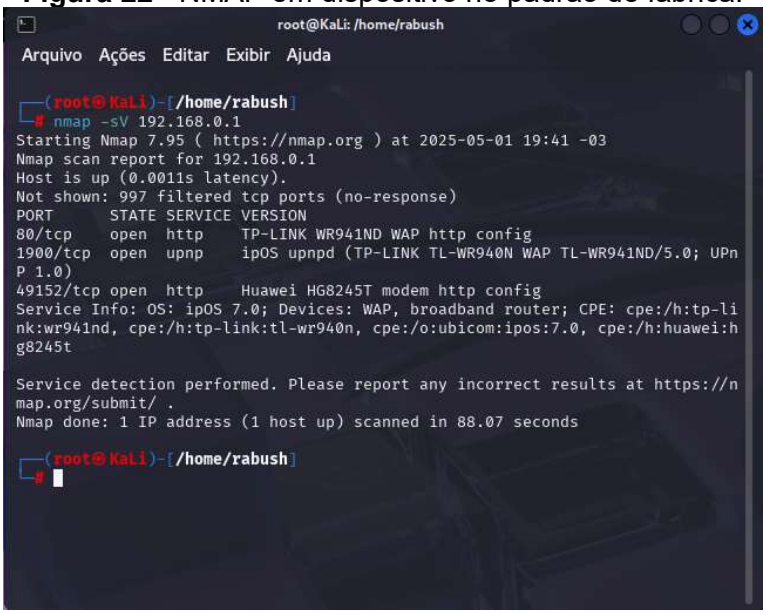
Figura 21 - Credenciais no Burp Suite.



Fonte: Autoria própria (2025)

Na Figura 22 é possível ver as portas abertas no equipamento por padrão de fábrica além dos programas e versão que estão funcionando nela.

Figura 22 - NMAP em dispositivo no padrão de fábrica.



Fonte: Autoria própria (2025)

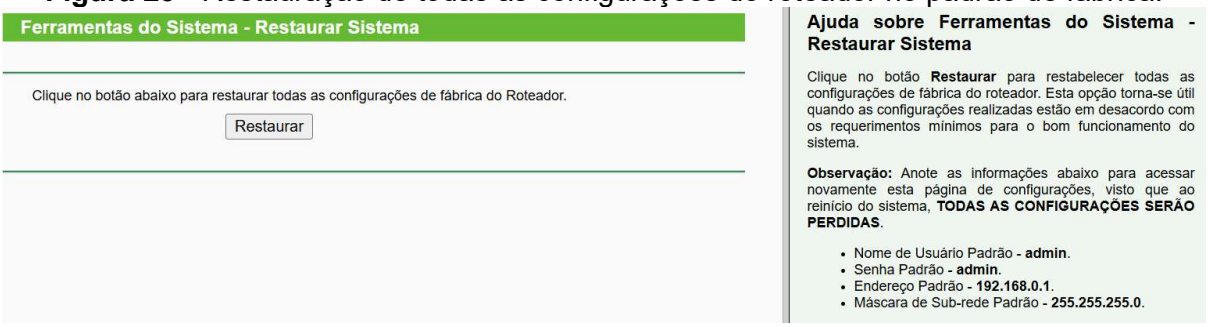
Quadro 27 - Requisitos: Ato 2.436/2023, item 6.2 ao item 6.2.1[24]

Requisitos do ato	**Resultados obtidos**
6.2. O mecanismo de recuperação de senha, caso implementado no equipamento, deverá ser robusto contra tentativas de roubo de credenciais, conforme item dos "Requisitos de Segurança Cibernética para Equipamentos para Telecomunicações". **6.2.1.** O mecanismo adotado deverá ser informado pelo requerente da homologação ao agente responsável pela avaliação da conformidade do produto.	O mecanismo para recuperação de senha é o reset físico do equipamento e o reset web, restaurando assim o padrão de fábrica conforme evidenciado na Figura 23.

Fonte: Resultados obtidos pelos autores à luz do ato 2.436 da Anatel (2023).

Dentro das configurações avançadas do equipamento possui uma aba somente para o reset de fábrica na web conforme evidenciado na Figura 23.

Figura 23 - Restauração de todas as configurações do roteador no padrão de fábrica.



Fonte: Autoria própria (2025)

[24] No Quadro 27 foi inserido na coluna esquerda uma transcrição direta do ato 2.436 da Anatel (2023), adicionalmente na coluna direita foram inseridos os resultados obtidos pelos autores.

5 CONSIDERAÇÕES FINAIS

Esta pesquisa exploratória permitiu a identificação e análise de falhas de segurança em três modelos distintos de equipamentos, totalizando 28 itens falhos. Cada modelo apresentou um número elevado de vulnerabilidades: 9 falhas no modelo TL-WR740N(BR), 9 no modelo TL-WP2543ND e 10 no modelo TL-WR941ND, o que evidencia um padrão vulnerabilidades críticas da segurança da informação. Esse cenário levanta sérias preocupações sobre a situação prática em que se encontram empresas e domicílios, e evidencia a necessidade de que fornecedores de internet se adequem com urgência às diretrizes do Ato 2436 da Anatel.

As vulnerabilidades identificadas não se restringem a falhas técnicas pontuais, mas refletem falhas estruturais no ciclo de desenvolvimento seguro, indicando a ausência de processos de segurança que contemplam desde o projeto até a entrega dos equipamentos ao consumidor final. Tais falhas colocam em risco não apenas a integridade dos sistemas, mas também a confidencialidade e disponibilidade das informações tratadas por esses dispositivos, com agravantes adicionais em ambientes corporativos ou críticos.

Considera-se atingido o objetivo geral de analisar a conformidade dos equipamentos CPE selecionados, à luz do Ato 2436. Sob a lupa do objetivo específico proposto de identificou-se uma série de vulnerabilidades de segurança cibernética nos equipamentos CPE, dentre as quais se destacam: a não resiliência à ataques de força bruta; a inexistência de dicionários de senha fraca; e o fato do equipamento não forçar a alteração de credenciais no primeiro uso.

Atesta-se a hipótese de que a conformidade com o Ato 2436 melhora significativamente a segurança do equipamento, reduzindo vulnerabilidades a ataques e tentativas simples de violação do equipamento, tal qual foi proposto no cenário de testes.

Além disso, a presente pesquisa busca viabilizar a apoiar novas investigações em diversas frentes, como novas baterias de testes na existência de alterações nas resoluções da Anatel, o surgimento de novas legislações e novos modelos de gestão da segurança da informação.

REFERÊNCIAS

AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES. **Ato nº 77, de 05 de janeiro de 2021**. Disponível em: https://informacoes.anatel.gov.br/legislacao/atos-de-certificacao-de-produtos/2021/1505-ato-77. Acesso em: 20 mar. 2025 às 13h05min.

AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES. **Ato nº 2436, de 7 de março de 2023.** Disponível em: https://informacoes.anatel.gov.br/legislacao/resolucoes/1850-ato-2436. Acesso em: 14 nov. 2024 às 22h35min.

AMAZON WEB SERVICES. **O que é segurança cibernética?** – AWS. 2024. Disponível em: https://aws.amazon.com/pt/what-is/cybersecurity/Acesso em: 13 nov. 2024 às 22h15min.

BRASIL. Gabinete de Segurança Institucional. **Comitê Nacional de Cibersegurança (CNCiber).[s.d.].** Disponível em: https://www.gov.br/gsi/pt-br/colegiados-do-gsi/comite-nacional-de-ciberseguranca-cnciber. Acesso em: 13 nov. 2024 às 22h30min.

BRASIL. Serviços e Informações. **Homologar produtos de telecomunicações - ANATEL.[s.d]**. Disponível em: https://www.gov.br/pt-br/servicos/homologar-produtos-de-telecomunicacoes-anatel. Acesso em: 27 jun. 2025 às 22h00min.

CENTRO UNIVERSITÁRIO UNIOPET. **Escassez de especialistas em segurança da informação impulsiona novas carreiras no setor.** G1, Paraná, 31 out. 2024. Disponível em: https://g1.globo.com/pr/parana/especial-publicitario/uniopet/opet-inovacao-em-rede/noticia/2024/10/31/escassez-de-especialistas-em-seguranca-da-informacao-impulsiona-novas-carreiras-no-setor.ghtml. Acesso em: 13 nov. 2024 às .

CHIN, Kyle. **Developing a culture of cybersecurity within your organization**. UpGuard, 18 nov. 2024. Disponível em: https://www.upguard.com/blog/developing-a-culture-of-cybersecurity. Acesso em: 15 nov. 2024 às 23h15min.

EC-COUNCIL UNIVERSITY. **Why cybersecurity is important for brand reputation**. [s.d.]. Disponível em: https://www.eccu.edu/blog/cybersecurity-brand-reputation/. Acesso em: 15 nov. 2024 às 22h55min.

IBM. **O que é monitoramento de conformidade?**. [s.d.]. Disponível em: https://www.ibm.com/br-pt/topics/compliance-monitoring. Acesso em: 13 nov. 2024 às 23h25min.

LACNOG; M3AAWG. **Melhores Práticas Operacionais Atuais sobre Requisitos Mínimos de Segurança para Aquisição de Equipamentos para Conexão de Assinante (CPE) LAC-BCOP-1.** mai. 2019. Disponível em: https://www.m3aawg.org/sites/default/files/lac-bcop-1-m3aawg-v1-portuguese-final.pdf. Acesso em: 15 nov. 2024 às 22h40min.

SHAWNTNS. **Top 100 worst passwords**. 2019. [repositório GitHub]. Disponível em: https://github.com/shawntns/top-100-worst-passwords. Acesso em: 05 maio 2025. 22h45min.

TP-LINK TECHNOLOGIES CO., LTD. **User guide: TL-WR2543ND 450Mbps Dual-Band Wireless N Gigabit Router**. Disponível em: https://static.tp-link.com/resources/document/TL-WR2543ND_V1_User_Guide.pdf. Acesso em: 05 maio 2025 às 22h50min.

TP-LINK TECHNOLOGIES CO., LTD. **User guide: 150Mbps Wireless N Router TL-WR740N.** Disponível em: https://static.tp-link.com/TL-WR740N(EU)_V7_UG_1474248366966c.pdf. Acesso em: 05 maio 2025 às 22h55min.

TP-LINK TECHNOLOGIES CO., LTD. **User guide: TL-WR940N TL-WR941ND 450Mbps Wireless N Router**. Disponível em: https://static.tp-link.com/res/down/doc/TL-WR941ND_V6_UG.pdf. Acesso em: 05 maio 2025 às 23h00min.