Ficha de identificação da obra elaborada pelo autor, através do Programa de Geração Automática do Sistema Integrado de Bibliotecas do IF Goiano - SIBi

Batista, Thiago Borges
T423 Análise de Segurança de Redes Insdustriais Ethernet: Um Estudo de Caso / Thiago Borges Batista. Catalão 2026.

14f. il.

Orientador: Prof. Dr. Eduardo Castilho Rosa.
Tcc (Bacharel) - Instituto Federal Goiano, curso de 0920203 - Bacharelado em Sistemas de Informação - Catalão - Noturno (Campus Catalão).
1. Rede. 2. Segurança. 3. Ethernet Industrial. I. Título.

TERMO DE CIÊNCIA E DE AUTORIZAÇÃO

PARA DISPONIBILIZAR PRODUÇÕES TÉCNICO-CIENTÍFICAS NO REPOSITÓRIO INSTITUCIONAL DO IF GOIANO

Com base no disposto na Lei Federal nº 9.610, de 19 de fevereiro de 1998, AUTORIZO o Instituto Federal de Educação, Ciência e Tecnologia Goiano a disponibilizar gratuitamente o documento em formato digital no Repositório Institucional do IF Goiano (RIIF Goiano), sem ressarcimento de direitos autorais, conforme permissão assinada abaixo, para fins de leitura, download e impressão, a título de divulgação da produção técnico-científica no IF Goiano.

IDENTIFICAÇÃO DA PRODUÇÃO TÉCNICO-CIENTÍFICA

Tese (doutorado)
Dissertação (mestrado)
Monografia (especialização)
TCC (graduação)
Artigo científico
Capítulo de livro
Livro
Trabalho apresentado em evento

Produto técnico e educacional - Tipo:

Nome completo do autor:

Matrícula:

Título do trabalho:

RESTRIÇÕES DE ACESSO AO DOCUMENTO

Documento confidencial: Não Sim, justifique:

Informe a data que poderá ser disponibilizado no RIIF Goiano: / /

O documento está sujeito a registro de patente? Sim Não

O documento pode vir a ser publicado como livro? Sim Não

DECLARAÇÃO DE DISTRIBUIÇÃO NÃO-EXCLUSIVA

O(a) referido(a) autor(a) declara:

• Que o documento é seu trabalho original, detém os direitos autorais da produção técnico-científica e não infringe os direitos de qualquer outra pessoa ou entidade;

• Que obteve autorização de quaisquer materiais inclusos no documento do qual não detém os direitos de autoria, para conceder ao Instituto Federal de Educação, Ciência e Tecnologia Goiano os direitos requeridos e que este material cujos direitos autorais são de terceiros, estão claramente identificados e reconhecidos no texto ou conteúdo do documento entregue;

• Que cumpriu quaisquer obrigações exigidas por contrato ou acordo, caso o documento entregue seja baseado em trabalho financiado ou apoiado por outra instituição que não o Instituto Federal de Educação, Ciência e Tecnologia Goiano.

Local / / Data

_____
Assinatura do autor e/ou detentor dos direitos autorais

Ciente e de acordo:

_____
Assinatura do(a) orientador(a)

SERVIÇO PÚBLICO FEDERAL
MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA GOIANO

Ata nº 4/2026 - CCBSI-CAT/GE-CAT/CMPCAT/IFGOIANO

ATA DE DEFESA DE TRABALHO DE CONCLUSÃO CURSO

Aos vinte e dois dias do mês de junho de 2026, às 19 horas, reuniu-se na Sala 212 do IF Goiano Campus Catalão a banca examinadora composta pelos docentes: Eduardo Castilho Rosa (orientador), Lacordaire Kemel Pimenta Cury (membro), e Jean Tomaz da Silva (membro), para examinar o Trabalho de Conclusão de Curso (TCC) intitulado "*Análise de Segurança de Redes Industriais Ethernet: Um Estudo de Caso*" do estudante Thiago Borges Batista, Matrícula nº 2021109202030032 do Curso de Bacharelado em Sistemas de Informação do IF Goiano – Campus Catalão. A palavra foi concedida ao estudante para a apresentação oral do TCC, onde houve posteriormente a arguição do candidato pelos membros da banca examinadora. Após tal etapa, a banca examinadora decidiu pela **APROVAÇÃO** do estudante, tendo este obtido média 7,76. Ao final da sessão pública de defesa foi lavrada a presente ata que segue assinada pelos membros da Banca Examinadora.

(Assinado Eletronicamente)

Dr. Eduardo Castilho Rosa

Orientador

(Assinado Eletronicamente)

Dr. Lacordaire Kemel Pimenta Cury

Membro

(Assinado Eletronicamente)

Ms. Jean Tomaz da Silva

Membro

Documento assinado eletronicamente por:

- **Eduardo Castilho Rosa**, **PROFESSOR ENS BASICO TECN TECNOLOGICO** , em 28/07/2026 22:45:54.
- **Jean Tomaz da Silva**, **PROFESSOR ENS BASICO TECN TECNOLOGICO** , em 28/07/2026 22:50:06.
- **Lacordaire Kemel Pimenta Cury**, **PROFESSOR ENS BASICO TECN TECNOLOGICO** , em 29/07/2026 10:40:25.

Este documento foi emitido pelo SUAP em 28/07/2026. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse https://suap.ifgoiano.edu.br/autenticar-documento/ e forneça os dados abaixo:

Código Verificador: 842299
Código de Autenticação: 4947656d1d

INSTITUTO FEDERAL GOIANO
Campus Catalão
Rua Salustiano Oliveira da Paz, 1621, Bairro Ipanema, CATALAO / GO, CEP 75.705-040
(64)99212-9907

Análise de Segurança de Redes Industriais Ethernet: Um Estudo de Caso

Thiago Borges Batista, Eduardo Castilho Rosa

Instituto Federal Goiano – Campus Catalão (IF Goiano)
CEP: 75701-655 – Catalão – GO – BR
Departamento de Sistemas de Informação

{thiago.batista@estudante.ifgoiano.edu.br,
eduardo.rosa@ifgoiano.edu.br}

Abstract. *This study aims to identify vulnerabilities and propose countermeasures to improve the security level of an industrial Ethernet network in a large company located in Catalão, Goiás. In this study the vulnerabilities were identified and mapped at both the physical and logical levels of the industrial network. To mitigate the security issues found, several corrective measures were implemented. The main actions included disabling unused switch ports to reduce the attack surface and strengthening network access control mechanisms. In addition, physical security measures were adopted, such as installing padlocks on the panels housing the network switches to restrict unauthorized physical access to the equipment.*

Resumo. *O objetivo desse trabalho é identificar vulnerabilidades e propor contramedidas para tornar segura uma rede Ethernet industrial de uma empresa de grande porte da cidade de Catalão – GO. Através de uma pesquisa de campo, foram mapeadas as vulnerabilidades da rede industrial, tanto no nível físico como no lógico. Como forma de mitigar os problemas de segurança encontrados, diversas medidas foram aplicadas. Dentre as principais estão os bloqueios de portas dos switches não utilizadas, para reduzir a superfície de ataque, e o reforço do controle de acesso à rede. Além disso, foram aplicados mecanismos de segurança física como o uso de cadeados nos painéis que abrigam os switches para restringir o acesso físico aos equipamentos.*

Palavras-chave: *Rede. Segurança. Ethernet Industrial.*

1. Introdução

As redes de comunicações *Ethernet* são fundamentais nos processos de automação e controle industrial, e a segurança é indispensável para que a integridade dos sistemas seja garantida, evitando acidentes e danos financeiros. Elas conectam e fazem a comunicação de dispositivos industriais, como controladores lógicos programáveis (CLP's), sensores, inversores de frequência e sistemas de supervisão.

Com a digitalização dos ambientes industriais, a superfície de ataque aumenta exponencialmente, como acesso não autorizado, ataques cibernéticos e falhas de integridade. Nesse contexto, a proteção dessas redes torna-se essencial para garantir a disponibilidade dos processos, a confiabilidade das informações trafegadas e a continuidade da produção, uma vez que qualquer vulnerabilidade pode comprometer o funcionamento de máquinas, sistemas de supervisão e etapas críticas da operação industrial.

Por isso, uma análise da segurança em redes industriais deve considerar não apenas o aspecto lógico da comunicação, mas também as condições físicas da infraestrutura. A pesquisa de campo, associada à observação direta do ambiente, e a inspeção da topologia física e lógica e ao uso de ferramentas de diagnóstico e monitoramento, como o *Wireshark* (WIRESHARK FOUNDATION, 2026) e o *Advanced Port Scanner (*FAMATECH, 2026) permite identificar vulnerabilidades reais, como tráfego sem criptografia, portas de *switches* não utilizadas, sistemas operacionais desatualizados e falhas no cabeamento e na proteção dos equipamentos.

Dessa forma, o presente trabalho tem como objetivo geral identificar problemas de segurança e propor melhorias em uma rede Ethernet de uma empresa de grande porte na cidade de Catalão. Para alcançar esse objetivo, foram definidos os seguintes objetivos específicos, como realizar inspeções no ambiente industrial; utilizar ferramenta de monitoramento e escaneamento de rede; implementar medidas de segurança no nível lógico; e implementar mecanismos de proteção física da infraestrutura.

Nesse sentido, o presente trabalho busca evidenciar a importância da segurança em redes *Ethernet* industriais e motivar a adoção de medidas preventivas e corretivas que reduzam a superfície de ataque e fortaleçam a infraestrutura. Ao analisar os riscos existentes e propor contramedidas, pretende-se contribuir para um ambiente industrial mais seguro, confiável e resiliente diante das ameaças cibernéticas e operacionais.

Este artigo está estruturado da seguinte forma: na Seção 2, apresenta-se a Fundamentação Teórica; na Seção 3 a empresa analisada é caracterizada. Na Seção 4, os materiais e métodos são apresentados, seguida pela Seção 5 onde os resultados são apresentados e discutidos. Por fim, a Seção 6 apresenta a conclusão do trabalho.

2. Fundamentação Teórica

Os sistemas de automação industrial estão cada vez mais incorporados no chão de fábrica e com isso estão usando os mesmos protocolos de comunicação dos computadores; diante disso, as redes de comunicações *Ethernet* industriais estão sujeitas a ataques e invasões.

Os crimes cibernéticos referem-se a ataques a redes de comunicações e computadores, com o objetivo específico de roubar informações e causar danos financeiros e materiais. Os crimes mais praticados são a espionagem industrial, violação de autorização, sabotagem e negação de serviços (BRANQUINHO et al., 2014).

Os atacantes são altamente qualificados, alguns engenheiros com conhecimentos em computação e automação industrial, capazes de criarem formas de ataques poderosas. Alguns são patrocinados por órgãos governamentais e empresas que querem prejudicar seus concorrentes. Esses indivíduos tomam vantagens das fraquezas tecnológicas de sistemas, praticando ataques de engenharia social contra indivíduos sem treinamento e conscientização (BRANQUINHO et al., 2014).

Existem várias formas de segurança de redes, como *software* antivírus e *antimalware*, segmentação de redes, controle de acesso, segurança de aplicações, análise do comportamento e sistema de prevenção contra invasão, que consiste em múltiplas camadas de defesa tanto na borda quanto na própria rede. Enquanto usuários autorizados têm acesso aos recursos da rede, indivíduos mal-intencionados são impedidos de realizar atividades exploratórias e representar ameaças.

A Norma NBR ISO/IEC 17799 (2001) faz a seguinte recomendação sobre perímetro de segurança:

> *A proteção física pode ser alcançada através da criação de diversas barreiras físicas em torno da propriedade física do negócio e de suas instalações de processamento da informação. [...]. Um perímetro de segurança é qualquer coisa que estabeleça uma barreira, por exemplo, uma parede, uma porta com controle de entrada baseado em cartão ou mesmo um balcão de controle de acesso com registro manual. A localização e a resistência de cada barreira dependem dos resultados da análise de risco.*

De acordo com Sêmola (2003), as barreiras de segurança são divididas em seis tipos diferentes. Cada uma delas tem uma parcela de participação no objetivo de reduzir os riscos e deve ser dimensionada de forma a proporcionar interação e integração entre elas.

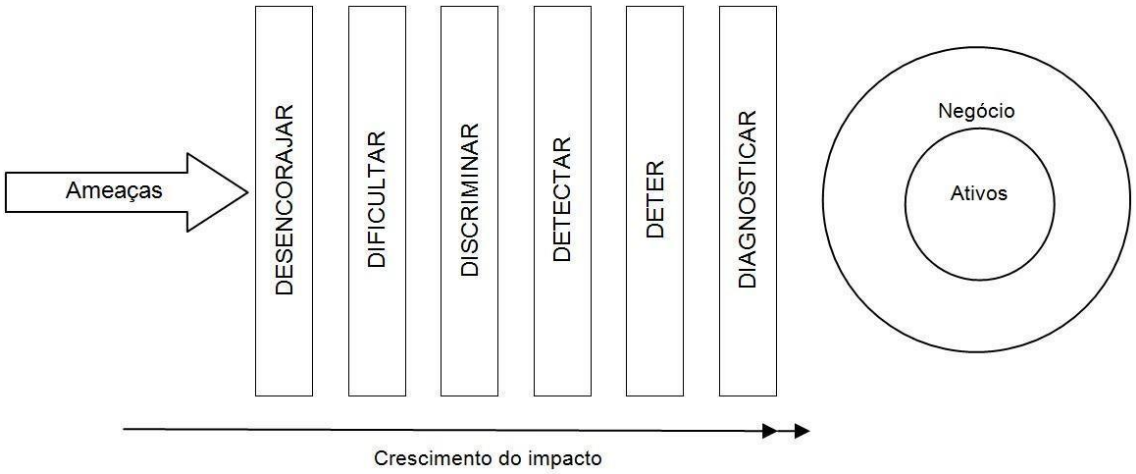


Figura 1 – Diagrama representativo das barreiras de segurança (Sêmola, 2003).

Este modelo conceitual implementa a teoria do perímetro, segmentando perímetros físicos ou lógicos e oferecendo níveis de resistência e proteção complementares e tendenciosamente crescentes, conforme pode ser observado na Figura 1.

A barreira **desencorajar** é a primeira das seis barreiras de segurança. Seu objetivo principal é desencorajar ameaças, que podem ser desmotivadas ou fazer o atacante perder o interesse em tentar violar a segurança. Isso pode ser alcançado através de mecanismos físicos, tecnológicos ou humanos. A presença de uma câmera de vídeo (mesmo que falsa), um aviso de alarmes existentes, campanhas de divulgação da política de segurança ou treinamento de funcionários sobre práticas de auditoria e monitoramento de acesso aos sistemas são eficazes nesta fase.

A barreira **dificultar** tem como objetivo adotar controles efetivos que dificultem o acesso indevido. No aspecto lógico, os controles podem incluir leitores de cartão magnético, senhas, *smartcards*, certificados digitais, criptografia, *firewall*, entre outros. Esses mecanismos aumentam a segurança, ao tornar mais difícil para os atacantes acessarem indevidamente os sistemas ou locais protegidos.

A barreira **discriminar**, aqui o importante é cercar-se de recursos que permitam identificar e gerir os acessos, definindo perfis e autorizando permissões. Os sistemas são largamente empregados para monitorar e estabelecer limites de acesso aos serviços de telefonia, perímetros físicos, aplicações de computador e banco de dados.

A barreira **detectar** é a quarta barreira de segurança e atua de forma complementar às barreiras anteriores. Esta barreira envolve o uso de dispositivos que sinalizam, alertam e auxiliam os gestores de segurança na detecção de situações de risco. Essas situações podem incluir tentativas de invasão, possíveis contaminações por vírus, descumprimento da política de segurança da empresa, ou a cópia e envio inadequado de informações sigilosas.

A barreira **deter** é a penúltima barreira de segurança. Seu objetivo é impedir que o atacante atinja os ativos que suportam o negócio. Medidas de detenção são implementadas, como ações administrativas punitivas e bloqueios de acessos físicos e lógicos a ambientes e sistemas. Essa barreira é crucial para prevenir danos aos ativos de negócios quando todas as outras barreiras falharam.

A barreira **diagnosticar** é a última barreira no diagrama, mas tem um papel especial na representação da continuidade do processo de gestão de segurança da informação. Ela deve ser conduzida por atividades de análise de riscos que considerem os aspectos tecnológicos, físicos e humanos, sempre orientados às características e necessidades específicas dos processos de negócio da empresa.

Além disso, existem empresas como a *Rockwell Automation* que em parceria com a Cisco e outras empresas, oferecerem produtos com protocolos de segurança incorporado no próprio dispositivo como *switch* industriais *Stratix*, *POINT Guard I/O*, e suporte técnico com orientações sobre projetos de melhores práticas de segurança, que aplicadas juntas com a diretrizes de segurança citadas acima, contribuíram para um ambiente mais seguro.

De acordo com Simone, José e Oliveira (2014), o ambiente industrial é bastante agressivo, diferente dos ambientes domésticos, a camada física deve ser projetada para garantir a integridade do sistema, a velocidade de transmissão e a redundância, com instalações de cabos (Cat6e), conectores RJ45 adequados, *switches* industriais, e a topologia da rede deve ser configurada em anel ou estrela.

Os protocolos de proteção *Ethernet* são utilizados para controlar, manter e gerenciar conexões protegidas em redes de comunicações, especialmente conexões redundantes. Existem vários protocolos de proteção, o *Spanning Tree Protocol* (STP) e o *Ethernet Automatic Protection Switching* (EAPS) são exemplos. O STP foi homologado pelo IEEE no padrão 802.1D. O EAPS foi homologado pelo ITU no padrão G.8031. Ambos os protocolos têm como objetivos garantir a disponibilidade e confiabilidade em redes *Ethernet*, fornecendo mecanismos para evitar falhas e garantir que o tráfego de dados possa fluir de maneira eficiente e segura (SILVA,2014).

Entretanto, a eficácia desses mecanismos de proteção é comprometida quando os sistemas operacionais que integram a rede possuem vulnerabilidades não corrigidas. Nesse contexto, o *Windows XP* foi bastante criticado devido à sua suscetibilidade a vírus, cavalos de Tróia, *worms* e estouro de *buffer* desde o seu lançamento em 2001 até o seu encerramento em 2014 (KASPERSKY, 2014). Na Figura 2, é possível visualizar a evolução anual dessas vulnerabilidades.

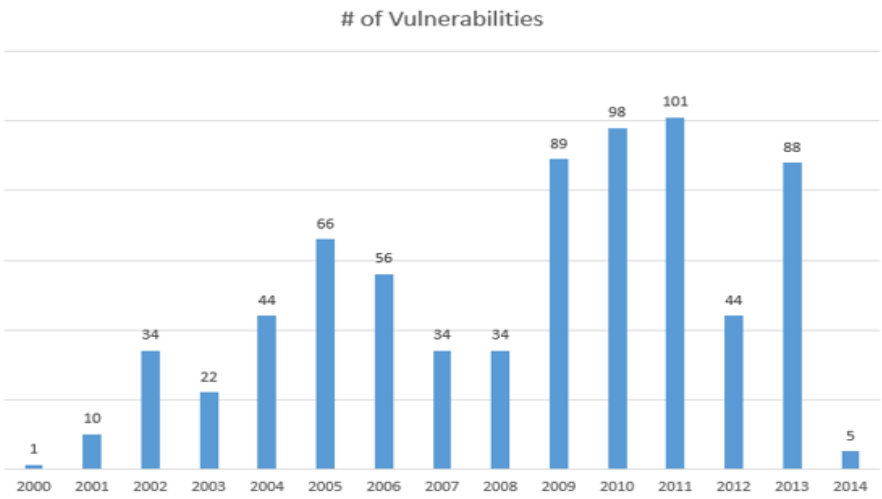


Figura 2 – Gráfico de vulnerabilidades do Windows XP (Kaspersky, 2014).

Observa-se um crescimento progressivo ao longo dos anos, com os maiores picos entre 2009 e 2011, período em que o sistema já se encontrava amplamente difundido. Esse comportamento indica que, com o passar do tempo, aumentou a exposição do sistema a falhas de segurança e à divulgação pública de novas vulnerabilidades. A queda encontrada após 2012 pode ser relacionada à redução do uso do sistema e ao encerramento do suporte oficial da *Microsoft*, que ocorreu em 8 de abril de 2014. A permanência de sistemas descontinuados, como o *Windows XP*, representa um risco crescente à segurança da informação, pois a ausência de atualizações oficiais deixa vulnerabilidades descobertas e novas falhas sem correção.

3. Caracterização da Empresa Analisada

Esse estudo foi realizado em uma empresa do setor industrial de Catalão. A empresa possui uma área de aproximadamente de 900 m^2, distribuídos em três andares. A planta é composta por vários equipamentos, controlados automaticamente por CLP (Controlador Lógico Programável), inversores de frequência, *soft starter*, *movimot*, *movifit* (inversores de frequência descentralizados), distribuidores passivos de I/O, além de vários transportadores, sendo alguns deles aéreos. A topologia de rede *Ethernet* da planta possui 31 *switches* conectando 339 periféricos. As matérias primas seguem um fluxo contínuo quando entram na planta, primeiramente elas recebem o tratamento no sistema PT (linha de pre - tratamento) e ED (linha de eletrodeposição), onde são mergulhadas em tanques, com as temperaturas controladas por sensores e válvulas automáticas que recebem e enviam informações via comunicação com CLP, assim como também os tempos de emersão e falhas nos processos.

Logo após os banhos, a matéria-prima entra na estufa com aquecedores a gás para realizar a secagem. Todo o controle de temperatura e tempo de permanência na estufa é monitorado por CLP's que se comunicam via rede *Ethernet* industrial, garantindo que os parâmetros do processo sejam cumpridos com precisão. Em seguida, a matéria-prima é enviada para a área de lixamento *e-coat* para correção de defeitos de sujeiras e grumos. Na sequência, entram na área de *sealer*, onde é aplicado o bate-pedras e *sealer*. Após isso, seguem para a cabine, que contém seis robôs responsáveis pela aplicação de fluido do produto final. Esses robôs recebem via rede *Ethernet* os dados de cada produto, como

modelo, cor, versão e *ID*, transmitidos por meio do protocolo *Ethernet/IP* através de uma *Message Instruction* (MSG) de um CLP para outro, assegurando que o robô aplique o fluido correto para cada tipo de produto. Após a aplicação, os produtos entram na estufa para secagem, cujo processo é igualmente supervisionado pelo sistema de automação conectado à rede.

Ao saírem da estufa, os produtos seguem para a linha de lixamento, onde defeitos como sujidade, crateras e escorrimentos são corrigidos. O rastreamento de cada produto ao longo dessa etapa é realizado por sensores e leitores conectados à rede industrial, permitindo que o sistema de supervisão registre e monitore o histórico de cada unidade em tempo real. Ao passarem por esse processo, seguem para a cabine de base e verniz, onde as aplicações são feitas de forma automática por robôs que, assim como na cabine de aplicação, dependem da rede *Ethernet* industrial para receber as informações necessárias à correta execução da pintura. Em seguida, os produtos passam por uma estufa para secagem e, ao saírem, entram na linha de polimento. Todo esse fluxo é continuamente monitorado pelo sistema de supervisão, que utiliza a rede industrial para coletar dados dos equipamentos, gerar alertas de falhas e garantir a rastreabilidade completa do processo.

4. Materiais e Métodos

Foi realizada uma pesquisa de campo com o objetivo de identificar as principais vulnerabilidades existentes na rede de comunicação *Ethernet* industrial da planta analisada. A metodologia baseou-se na observação direta da infraestrutura, na análise dos dispositivos de rede e na utilização de ferramentas específicas de diagnóstico e monitoramento.

Como suporte teórico, foram consultadas diversas referências bibliográficas relacionadas à segurança em redes industriais, abrangendo aspectos físicos, de *hardware* e de *software*. Para a análise do tráfego de dados, foi utilizada a ferramenta *Wireshark*), que permitiu a captura e inspeção dos pacotes transmitidos na rede. Além disso, foi empregado também a ferramenta *Advanced Port Scanner* para a realização de varreduras nos dispositivos de rede. A rede de comunicação apresenta uma topologia física em estrela, com 31 *switches* conectando 339 periféricos.

Como coleta de dados, no dia 09 de setembro de 2025 foi realizada a captura do tráfego de dados da rede, iniciado às 8 horas e 28 minutos e encerrado às 8 horas e 59 minutos, gerando um arquivo de 1.20 Gb. A captura foi realizada no *switch* do MOP (Painel de Operação Principal), porta 5, onde após acessar as configurações do mesmo pela interface *web*, foi habilitado a função *Mirror Configuration*, que possibilitou o desvio de todo o tráfego recebido do *switch* para essa porta em especifico.

5. Resultados e Discussões

5.1. Análise Lógica

Após uma análise do arquivo de captura do trafego de dados realizado com o *Wireshark*, podemos observar na Tabela 1 os principais parâmetros. Durante o intervalo de 1.829,685 segundos, foram capturados 10.228.743 pacotes, com taxa média de 5.590,4 pacotes por segundo e tamanho médio de 93 *bytes*, totalizando 946.367.778 *bytes* trafegados a uma

taxa média de 4.137 *kbits/s*. Esses valores são baixos em função da pequena quantidade de *bytes* que normalmente são enviados em uma rede industrial.

Tabela 1. Estatísticas da captura de tráfego de rede (Wireshark).

Medição	Capturado	Exibido
Pacotes capturados	10.228.743	10.228.743 (100,0%)
Intervalo de tempo (s)	1.829,685	1.829,685
Média de pacotes/s	5.590,4	5.590,4
Tamanho médio do pacote (B)	93	93
Bytes capturados	946.367.778	946.367.778 (100,0%)
Média de bytes/s	517 k	517 k
Média de bits/s	4.137 k	4.137 k

Fonte: Elaborado pelo autor.

Na Figura 3 abaixo é possível visualizar a vazão de tráfego medido pelo *Wireshark* em 10 segundos em uma rede *Ethernet* industrial, com taxa em torno de 41.000 *bit/s*. O tráfego permaneceu estável, com pequenas oscilações e alguns picos vindos de 46.000 *bit/s*, típico de comunicações periódicas entre CLP's, IHM's e inversores. Essa estabilidade indica operação adequada, sem congestionamento ou falhas relevantes; os picos podem refletir mensagens de diagnóstico, sincronização ou trocas simultâneas de dados.

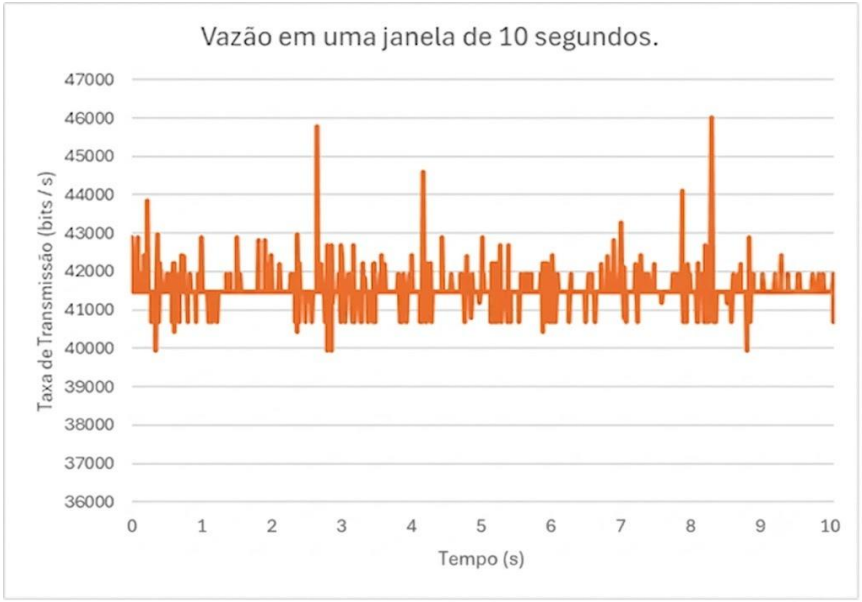


Figura 3 – Vazão de trafego da rede.

A Tabela 2 apresenta a distribuição dos pacotes capturados por faixa de tamanho. Os dados evidenciam que 96,24% dos pacotes estão concentrados na faixa de 80 a 159 *bytes*, com tamanho médio de 93 *bytes*, comportamento característico de redes industriais, nas

quais predominam mensagens curtas de controle e monitoramento, como comandos dos protocolos *Modbus* TCP e *Ethernet/IP*. Os demais intervalos apresentaram ocorrências insignificantes ou nulas, reforçando a homogeneidade do tráfego. Essa previsibilidade facilita a identificação de padrões de comunicação por agentes maliciosos, tornando ainda mais relevante a adoção de medidas de segurança na rede industrial.

Tabela 2. Distribuição dos pacotes capturados por faixa de tamanho (Wireshark).

Faixa (bytes)	Pacotes	Média (bytes)	Mín (bytes)	Máx (bytes)	Percentual
0 – 19	0	–	–	–	0,00%
20 – 39	0	–	–	–	0,00%
40 – 79	52.242	64	46	76	3,75%
80 – 159	1.342.260	93	82	157	96,24%
160 – 319	1	259	259	259	0,00%
320 – 639	207	354	331	450	0,01%
640 – 1279	0	–	–	–	0,00%
1280 – 2559	0	–	–	–	0,00%
2560 – 5119	0	–	–	–	0,00%
≥ 5120	0	–	–	–	0,00%
Total	1.394.710	92	46	450	100%

Fonte: Elaborado pelo autor.

A partir da análise dos pacotes capturados, constatou-se que o tráfego de dados não utiliza mecanismos de criptografia, como pode ser visto na Figura 4, o que representa um risco significativo à confidencialidade das informações. Vale ressaltar que a rede industrial da planta não possui acesso externo, o que minimiza os efeitos do tráfego não criptografado e diminui drasticamente a superfície de ataque. Essa análise, aliada a verificações visuais em campo, evidenciou a existência de portas ativas em *switches* que não estão em uso e não possuem qualquer tipo de bloqueio ou restrição de acesso.

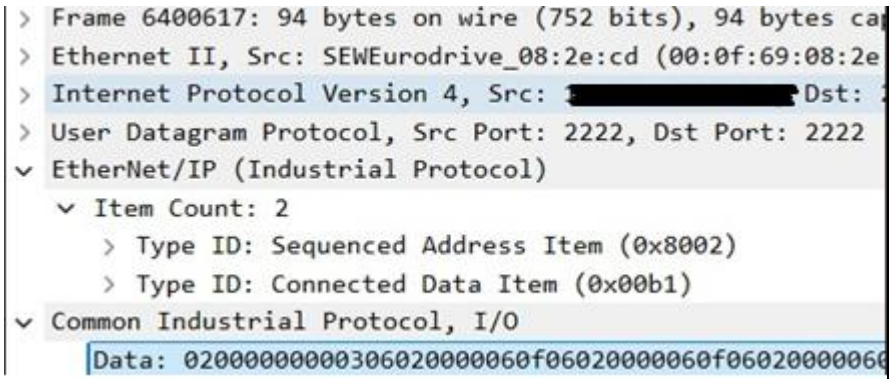


Figura 4 – Trafego de dados sem criptografia.

Após o escaneamento da rede com a ferramenta *Advanced Port Scanner*, foram encontrados 339 dispositivos ativos, e a identificação de portas abertas. A Figura 5 apresenta a distribuição percentual das portas abertas identificadas na varredura da rede. As portas com maior frequência de ocorrência foram a porta 300 (18,0%), a porta 23, *Telnet* (17,7%); a porta 502, *Modbus* TCP (17,7%); a porta 21, FTP (16,6%) e a porta 80 HTTP (15,2%).

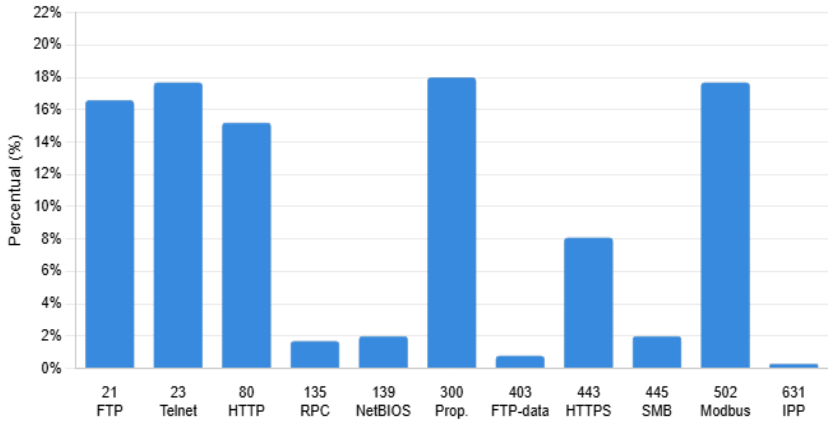


Figura 5 - Gráfico de barras mostrando a frequência percentual das portas abertas detectadas na rede, por número de porta.

Do ponto de vista da segurança, destacam-se as portas 21, 23 e 502, que correspondem, respectivamente, aos protocolos FTP, *Telnet* e *Modbus* TCP. Tais protocolos não implementam mecanismos nativos de criptografia, expondo as informações transmitidas a interceptações e ataques. Vale ressaltar que a rede industrial não está conectada com a rede corporativa e nem com a *Internet*. As contramedidas citadas acima incluem bloqueio das portas do *switch* não utilizadas, alteração do usuário e senha, e habilitação da função *MAC ID Management* que restringe quais endereços *MAC* estão autorizados a se comunicar em cada porta do switch, todas essas configurações são realizadas via interface *web* de configuração do *switch.* Além disso, a atualização dos *switches Stratix* 6000 por *switches 5700 Stratix* proporcionou um gerenciamento mais robusto (*Layer* 2 e *Layer* 3) da rede industrial, sendo possível o bloqueio via CLI das portas 21, 23.

5.2. Análise Física

A segurança da rede industrial abrange tanto o nível lógico quanto o físico. As próximas seções trazem o levantamento desses aspectos bem como as recomendações de segurança para a rede analisada.

Foram realizadas inspeções no ambiente industrial, onde identificou-se que a planta possui diversos terminais de operação, *Allen Bradley VersaView* 1700P, computador industrial que possibilita o acesso direto aos CLP’s e aos sistemas de supervisão. Observou-se que esses equipamentos operam com o sistema operacional *Windows XP*, o qual se encontra descontinuado e sem suporte oficial, não recebendo mais atualizações de segurança.

Em uma análise preliminar, as inspeções identificaram também outro ponto crítico relacionado à segurança física. Os painéis onde estão instalados os *switches* responsáveis pela comunicação *Ethernet* entre os periféricos da planta não possuem mecanismos de proteção física adequados, permitindo o acesso de pessoas não autorizadas aos equipamentos de rede.

Além disso, a análise da infraestrutura revelou problemas relacionados à instalação dos cabos de rede. Verificou-se que alguns enlaces de comunicação estão alocados junto a condutores elétricos de potência, além de falhas na montagem de conectores RJ45. Essas condições podem ocasionar interferências eletromagnéticas, diafonia e degradação do sinal de comunicação.

5.3. Recomendações

Antes das implementações das diretrizes de segurança, os painéis dos *switches* se encontravam sem nenhuma proteção. Para inibir o acesso não autorizado dos painéis dos *switches*, foram instalados cadeados de bloqueio e câmeras de monitoramento, como pode ser visto na Figura 6 abaixo.

a) Painel sem bloqueio. b) Painel com bloqueio. c) Câmera de monitoramento.

Figura 6 – Diretrizes de segurança aplicadas.

Os *Allen Bradley VersaView* 1700P que usavam o *Windows* XP, como sistema operacional foram substituídos por *desktops* com alta capacidade de processamento e sistema operacional *Windows* 11 Pro, como pode ser visto na Figura 7 e Figura 8, já que os *VersaView* estão descontinuados e possuem custo elevado de aquisição se comparado ao desktop.

a) Terminal VersaView Windows XP.

b) Desktop com Windows 11 Pro

Figura 7 – Identificação dos sistemas operacionais.

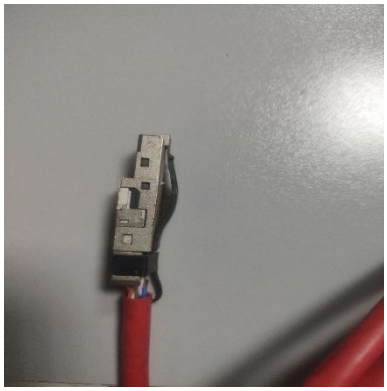
a) Captura de dados Wireshark identificando Windows XP.

Figura 8 – Analise do trafego capturado.

Outra medida de segurança implementada foi a separação dos cabos de rede dos condutores elétricos, que influencia diretamente na segurança da rede, devido à interferência eletromagnética que resulta em perdas de pacotes, lentidão e instabilidade da rede. Foram realizadas também as montagens correta dos conectores RJ45, como pode ser vista na Figura 9 abaixo.

a) Cabo de rede junto com condutor elétrico.

b) Cabo de rede colocado separado.

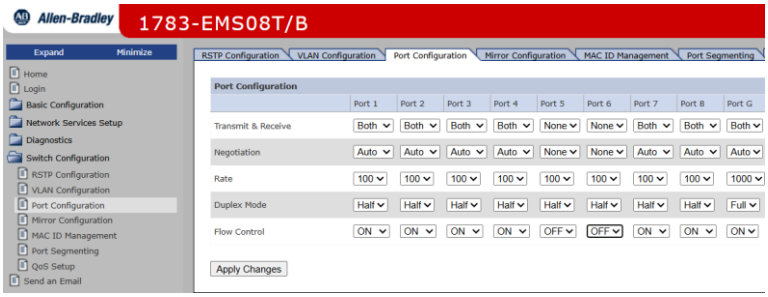


c) Conector RJ45 Cat6 montado errado.

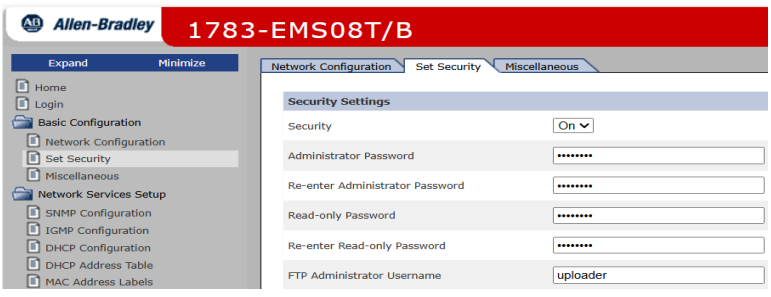
d) Conector RJ45 Cat6 montado certo.

Figura 9 – Relocação do cabeamento de rede e montagem dos conectores.

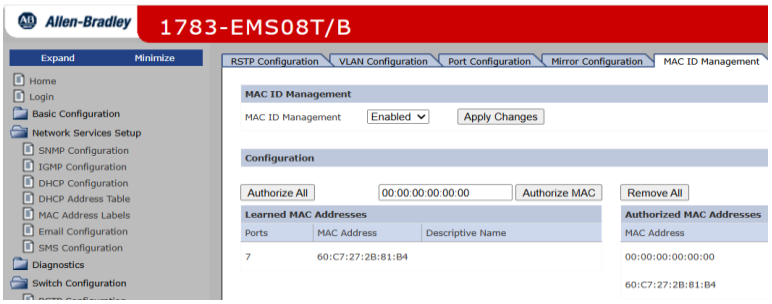
Alguns *switches* continham portas não utilizadas. Caso a barreira física fosse rompida, poderia haver o acesso às mesmas. Diante dessa condição, foi realizado o bloqueio lógico das portas inativas, alterada a senha e usuário de acesso do *switch*, e habilitada a função *MAC ID Management*. Dessa forma, mesmo que um dispositivo não autorizado seja conectado fisicamente à rede, ele não conseguirá estabelecer comunicação com os equipamentos industriais. Essas ações podem ser vistas na Figura 10 abaixo.



a) Bloqueio das portas não utilizadas.



b) Alteração de senha e usuário.



c) Ativação do controle de MAC.

Figura 10 – Status de configurações do switch.

Logicamente, recomenda-se o bloqueio de portas de *switches* não utilizadas. Fisicamente, a proteção é reforçada pelo uso de cadeados em painéis de equipamentos e pela instalação de câmeras de monitoramento, restringindo o acesso não autorizado em toda a planta.

Com base nas vulnerabilidades e problemas de segurança identificados, foi elaborado um plano de ações corretivas e preventivas. Para a vulnerabilidade relacionada à ausência de criptografia no tráfego de dados, propõe-se a implementação futura de dispositivos de *hardware* dedicados à criptografia da comunicação na rede industrial.

Em relação às portas de *switches* não utilizadas, recomenda-se a adoção do bloqueio lógico dessas portas, minimizando o risco de acessos indevidos à rede. Para mitigar os riscos associados ao uso de sistemas operacionais obsoletos, será realizada a substituição dos terminais industriais por *desktops* com versões de sistemas mais recentes e suportadas, garantindo maior nível de segurança e compatibilidade.

Quanto à segurança física da infraestrutura, propõe-se a instalação de sistemas de bloqueio físico nos painéis que abrigam os *switches* de rede, bem como a implementação de câmeras de monitoramento, com o objetivo de restringir o acesso apenas a pessoas autorizadas. Para corrigir os problemas relacionados à infraestrutura de cabeamento, será realizada a separação física dos cabos de rede dos condutores elétricos de potência, reduzindo as interferências eletromagnéticas. Adicionalmente, será refeita a montagem dos conectores RJ45, assegurando a conformidade com as boas práticas de cabeamento estruturado.

5. Conclusões

Os sistemas de automação industrial, ao utilizarem protocolos de comunicação de computadores, tornaram-se mais vulneráveis a ataques cibernéticos como espionagem, sabotagem e negação de serviços. Qualquer falha pode resultar em graves consequências, como a operação inadequada de máquinas e a paralisação total da rede.

Após uma análise em campo e identificadas as fraquezas de segurança da rede *Ethernet* industrial, foi possível implementar medidas de segurança eficazes, como acesso restrito e bloqueio físico ao acesso dos equipamentos. Tais medidas proporcionarão uma rede segura, inibindo e dificultando que ataques possam acontecer.

Investir em medidas de segurança robustas e seguir as melhores práticas é essencial para proteger os ativos industriais contra ameaças cibernéticas e manter a

eficiência operacional, promovendo uma rede segura e resiliente em conformidade com as normas ISO/IEC 17799 e práticas de segurança da *Rockwell Automation*. Como trabalhos futuros pretende-se implementar técnicas criptográficas em CLP's e em dispositivos finais para fortalecer o nível de segurança na rede industrial analisada.

Referências

ABNT. ISO/IEC 17799: Código de Prática para a Gestão da Segurança da Informação. Rio de Janeiro: ABNT, 2001.

BRANQUINHO, M. A. et al. Segurança de Automação Industrial e SCADA. [s.l.]: Elsevier Brasil, 2014.

CISCO. O que é segurança de rede? Disponível em: <https://www.cisco.com/c/pt_br/products/security/what-is-network-security.html>. Acesso em: 07 mar. 2024.

FAMATECH. *Advanced Port Scanner*. Versão 2.5.3869. Disponível em: https://www.advanced-port-scanner.com. Acesso em: 10 mar. 2026.

KASPERSKY. O fim da era Windows XP (2001-2014). Disponível em: <https://www.kaspersky.com.br/blog/o-fim-da-era-windows-xp-2001-2014/2701/>. Acesso em: 20 fev. 2026.

ROCKWELL AUTOMATION. Soluções de segurança em redes industriais. Disponível em: <https://literature.rockwellautomation.com/idc/groups/literature/documents/br/securbr001_-pt-p.pdf>. Acesso em: 12 abr. 2024.

SÊMOLA, M. Gestão da Segurança da Informação. Rio de Janeiro: Campus, 2003. 156 p.

SILVA, V. L. Protocolos de proteção Ethernet. 2014. Disponível em: <https://ric.cps.sp.gov.br/bitstream/123456789/1045/1/20142S_SILVAViniciusLuisda_CD1999.pdf>. Acesso em: 05 mar. 2024.

SIMONE, D.; JOSÉ, S.; OLIVEIRA, A. N. Rede Ethernet industrial como alternativa para chão de fábrica. Disponível em: <https://www.dca.ufrn.br/~affonso/FTP/DCA447/trabalho3/trabalho3_4.pdf>. Acesso em: 26 abr. 2026.

WIRESHARK FOUNDATION. *Wireshark*. Versão 4.2. Disponível em: https://www.wireshark.org. Acesso em: 10 mar. 2025.