CAPÍTULO 2

PRIVACIDADE E SEGURANÇA NA ERA DA IOT EM RESIDÊNCIAS: POSSIBILIDADES E DESAFIOS

PRIVACY AND SECURITY IN THE ERA OF IOT IN HOMES: POSSIBILITIES AND CHALLENGES

Orientador(a): Maria Cristina Aranda, Fatec Americana, mcris.aranda@fatec.sp.gov.br
Gabriel Julião, FATEC Americana, gabriel.juliao01@fatec.sp.gov.br
Isabella Manoel da Silva, FATEC Americana, isabella.silva25@fatec.sp.gov.br

DOI: 10.46898/rfb.65d4a7e4-b121-40ca-835b-48adf09ea300

RESUMO

O uso da Internet das Coisas (IoT) na segurança residencial tem se tornado cada vez mais relevante com a crescente presença de dispositivos inteligentes em lares modernos. Essa evolução traz consigo uma série de benefícios, como maior conveniência, monitoramento remoto e automação de tarefas cotidianas. No entanto, também surgem preocupações significativas relacionadas à segurança cibernética e à privacidade dos dados dos usuários. Este estudo se propõe a examinar em profundidade os desafios inerentes à implementação da IoT para aprimorar a segurança residencial. Um dos principais aspectos abordados é a integração eficiente de dispositivos IoT, visando garantir a interoperabilidade e a comunicação segura entre eles. Além disso, investiga-se as melhores práticas e soluções recomendadas para mitigar os riscos associados a possíveis vulnerabilidades e ataques cibernéticos. Um dos pontos cruciais é a proteção contra ameaças cibernéticas, incluindo a implementação de medidas de segurança robustas, como *firewalls*, criptografia de dados e autenticação de dispositivos.

Palavras-chave: Internet das Coisas, IoT, Casa inteligente, Segurança da Informação.

ABSTRACT

The use of the Internet of Things (IoT) in home security has become increasingly relevant with the growing presence of smart devices in modern homes. This evolution brings with it a series of benefits, such as greater convenience, remote monitoring and automation of daily tasks. However, significant concerns related to cybersecurity and user data privacy also arise.This study aims to examine in depth the challenges inherent in implementing IoT to improve home security. One of the main aspects addressed is the efficient integration of IoT devices to ensure interoperability and secure communication between them. It also investigated, best practices and recommended solutions to mitigate the risks associated with possible vulnerabilities and cyber attacks.One of the crucial points is protection against cyber threats, including the implementation of robust security measures such as firewalls, data encryption and device authentication.

Keywords: Internet of Things, IoT, Smart Home, Information Security.

1. INTRODUÇÃO

A Internet das Coisas, ou IoT, é uma tecnologia que se refere à interconexão de objetos físicos através da Internet. Esses objetos, que podem ser desde eletrodomésticos até veículos, são equipados com sensores, *software* e conectividade para coletar e compartilhar dados, permitindo que interajam e sejam controlados de forma remota. A IoT tem ganhado espaço em vários campos da sociedade, trazendo benefícios como automação, monitoramento e análise de dados em tempo real.

A implantação dos dispositivos IoT tem alterado a maneira como as pessoas vivem e interagem com o ambiente ao seu redor. A utilização dos dispositivos em ambientes residenciais permite ao usuário um processo automatizado de suas rotinas, ou seja, os dispositi-

vos podem ser controlados de forma remota. Esse processo de automação trouxe o conceito de *smart home* (casa inteligente). O conceito de *smart home* se divide em dois componentes: a integração entre a casa com um ambiente inteligente e inter-relações entre o ambiente e usuário (Ghaffarianhoseini *et al*., 2016).

Com o desenvolvimento tecnológico também cresce a preocupação com a segurança cibernética, pois à medida que novos dispositivos são implementados na sociedade, novas vulnerabilidades são criadas. Neste contexto, surge a seguinte questão: como lidar com as novas tecnologias alocadas em ambientes residenciais?

O objetivo deste trabalho será proporcionar uma visão abrangente sobre a interação complexa entre a IoT e a segurança da informação em residências, explorando seus elementos fundamentais, oportunidades e desafios, bem como fornecer orientações práticas para proteger os usuários e suas casas nesse cenário dinâmico.

Para lidar com os desafios da segurança virtual, em especial por usuários residenciais de IoT, será apresentada uma visão abrangente das medidas de segurança disponíveis. Nessa proposta foram exploradas soluções técnicas, de como realizar análise das características técnicas de um dispositivo de vigilância, em particular uma câmera IP, que é capaz de se conectar com dispositivos móveis através de rede *wifi* e realizar interações inteligentes conforme for configurada. Além de boas condutas práticas, como a importância da conscientização do usuário e da adoção de senhas seguras.

A abordagem visa proporcionar um panorama completo da intersecção entre IoT e segurança da informação, transmitindo o conhecimento prático e teórico para explorar as possibilidades da IoT, ao mesmo tempo em que protegem lares de maneira eficaz e segura.

2. REFERENCIAL TEÓRICO

Segundo Greengard (2015), a IoT é a interconexão de objetos físicos do cotidiano com a Internet, abrangendo desde utensílios domésticos comuns, como lâmpadas, até dispositivos médicos, acessórios e aparelhos inteligentes. Embora a Internet tenha revolucionado a rapidez das trocas de informações e dados, é inegável que ela se tornou um centro para atividades maliciosas, como o roubo de informações, espionagem, ataques cibernéticos entre outras ameaças.

Devido ao aumento das ameaças e vulnerabilidades associadas à Internet das Coisas (IoT), é crucial adotar medidas de segurança robustas para garantir a proteção das informações transmitidas entre esses dispositivos interconectados.

A segurança da informação, como definido por Hintzbergen J., Hintzbergen K., Smulders A. e Baars H, (2010), envolve a proteção contra uma gama de ameaças, com a finalidade de reduzir os riscos. Isso envolve garantir a confidencialidade, integridade e disponibilidade das informações, bem como outras propriedades como autenticidade, responsabilidade, não repúdio e confiabilidade. Integrar medidas de segurança eficazes com essa definição abrangente de segurança da informação é fundamental para mitigar os riscos e garantir a confiança e a disponibilidade dos sistemas IoT.

2.1. Internet of Things

A Internet das Coisas, também conhecida como Internet of Things (IoT), refere-se ao cenário em que diversos dispositivos e objetos do nosso cotidiano estão interconectados por meio da Internet. Essa interconexão cria um ambiente onde esses dispositivos automatizados podem comunicar, coletar e compartilhar informações, oferecendo a eles maior capacidade computacional e autonomia nos processos (Lima, 2023).

A IoT possibilita aos usuários o controle remoto de seus dispositivos, permitindo que estejam virtualmente presentes em qualquer lugar, mesmo estando fisicamente em outro. Um exemplo notável desse fato são as casas inteligentes, também conhecidas como *smart homes*. Nesses ambientes, uma variedade de dispositivos, como termostatos, lâmpadas, câmeras de segurança e eletrodomésticos, são conectados à Internet e controlados por meio de aplicativos em dispositivos móveis ou computadores (Magrani, 2018).

Além disso, a IoT tem aplicações em diversos setores, como saúde, indústria, agricultura e transporte. Na área da saúde, por exemplo, dispositivos médicos conectados e implantados podem monitorar pacientes remotamente e transmitir dados para profissionais de saúde em tempo real. Na indústria, sensores e dispositivos IoT são usados para otimizar processos de produção e manutenção de máquinas. Na agricultura, sensores permitem o monitoramento de cultivos e rebanhos, facilitando o aumento da eficiência (Sinclair, 2018).

A crescente expansão da IoT traz benefícios significativos, como maior conveniência, eficiência e controle para as pessoas e empresas. No entanto, também levanta preocupações sobre segurança e privacidade, à medida que mais dispositivos estão interconectados e coletam informações pessoais. Portanto, o desenvolvimento responsável e a implementação segura da IoT são aspectos fundamentais a serem considerados à medida que essa tecnologia continua a evoluir (Lima, 2023).

2.1.1. História da IoT

Em 1990, o engenheiro John Romkey deixou sua marca na história ao conceber um dos primeiros dispositivos precursores da IoT. Sua visão visionária levou à criação de uma torradeira que podia ser controlada remotamente pela Internet. Inicialmente, o processo exigia intervenção manual, porém, em 1991, Romkey deu um passo adiante ao implementar um pequeno guindaste robótico, que, conectado à Internet, automatizou completamente o funcionamento do aparelho (Mancini, 2018).

Ainda em 1991, Mark Weiser delineou um conceito fundamental para a IoT em seu artigo "The Computer for the 21st Century". Weiser vislumbrou um futuro onde dispositivos estariam interconectados de maneira tão transparente que se tornariam quase invisíveis para os usuários, simplificando assim as tarefas cotidianas (Singer, 2012).

O termo Internet das Coisas foi citado oficialmente em 1999 por Kevin Ashton, durante uma palestra proferida para a Procter & Gamble. Ashton propôs a ideia de conectar objetos físicos à Internet, antecipando um mundo onde a inteligência estaria integrada em todos os aspectos do ambiente físico (Singer, 2012).

Após esse marco, a tecnologia de identificação por radiofrequência (RFID – Radio Frequency Identification) ganhou relevância, especialmente em aplicações voltadas para cadeias de suprimentos. Embora a abordagem de conectividade de dispositivos por meio do RFID seja diferente da IoT contemporânea, que se baseia principalmente no Protocolo de Internet (IP), a visão pioneira de Ashton desempenhou um papel crucial na história da IoT e no desenvolvimento tecnológico de forma geral (Fia, 2021).

Através de uma série de avanços tecnológicos e desenvolvimentos ao longo dos anos, a IoT se tornou realidade, com bilhões de dispositivos conectados e em uso em todo o mundo. Seu impacto transformador não se limita apenas ao ambiente empresarial, mas também se estende à sociedade em geral, alterando fundamentalmente a forma de interação com o mundo.

2.1.2 Vantagens proporcionadas pela Internet das Coisas (IoT)

A IoT tem se revelado uma ferramenta inestimável para fabricantes de produtos e usuários, desempenhando um papel fundamental na otimização de processos e na melhoria da experiência do consumidor.

Para os fabricantes, a IoT oferece uma fonte rica de dados que permite uma compreensão mais profunda das necessidades e desejos dos usuários. Ao coletar informações

em tempo real sobre o uso e o desempenho de seus produtos, as empresas podem ajustar e personalizar seus produtos e serviços de acordo com as demandas do mercado. Essa análise de dados também ajuda na tomada de decisões estratégicas, como aprimorar a eficiência de produção, reduzir custos operacionais e antecipar tendências do consumidor (Mocrii, 2018).

Por outro lado, para os usuários, a IoT tem simplificado a vida de diversas maneiras. Um exemplo disso é o controle remoto de dispositivos, que possibilita o controle em qualquer lugar do mundo, proporcionando maior comodidade e economia de tempo. Além disso, a IoT desempenha um papel fundamental na área da saúde, permitindo a monitorização contínua da condição física e da saúde em tempo real através de relógio e outros dispositivos de monitoramento, o que possibilita a detecção precoce de problemas de saúde e a promoção de um estilo de vida mais saudável (Evans, 2011).

Na atualidade, a IoT desempenha um papel crucial tanto na indústria quanto no cotidiano dos consumidores. Sua presença influencia significativamente a compreensão das empresas em relação às demandas dos usuários, proporcionando conveniência e bem-estar. A coleta e análise de dados gerados pela IoT estão transformando a fabricação, entrega e utilização de produtos, promovendo uma sociedade mais interligada e eficiente.

2.1.3 Desafios no uso da IoT.

Ao explorar a IoT, é evidente que ela proporciona benefícios significativos tanto para as empresas que as adotam quanto para os usuários. No entanto, é crucial reconhecer que essa tecnologia também apresenta desafios significativos. Alguns dos principais desafios incluem questões de segurança, privacidade, vulnerabilidade e a dependência da conectividade (Castro, 2022).

A segurança é uma preocupação central na IoT. A interconexão de dispositivos expõe redes e dados a ameaças cibernéticas. Vulnerabilidades em dispositivos IoT podem ser exploradas por *hackers*, comprometendo a integridade e a privacidade dos dados. A garantia de segurança é fundamental para a confiança na tecnologia (Godoi; Araújo, 2018; Leite, 2019).

A coleta constante de dados pela IoT pode levantar preocupações sobre a privacidade. Os usuários muitas vezes não têm controle total sobre como seus dados são usados e compartilhados. A regulamentação e as políticas de privacidade são necessárias para proteger os interesses dos consumidores (Hurel; Lobato, 2018).

Dispositivos IoT podem ser vulneráveis a ataques, especialmente se não forem adequadamente atualizados e protegidos. Isso pode levar à exposição de informações pessoais e à manipulação de dispositivos, criando riscos substanciais (Damasceno, 2022).

A IoT com conexão através de IP, depende de uma conexão constante com a Internet para funcionar efetivamente. Em momentos de falha na conexão, os dispositivos podem não operar como esperado. Isso pode causar interrupções indesejadas na vida cotidiana dos usuários, como a perda de controle sobre sistemas de automação residencial (Apeti, 2023).

2.2. Iot na Industria 4.0 e 5.0

De acordo com o *site* Lyra M2M (2023), a Indústria 4.0 marcou uma fase crucial na evolução industrial, introduzindo a conectividade avançada, automação e análise de dados em larga escala. A IoT desempenhou um papel fundamental nesse contexto, permitindo a interconexão de dispositivos, máquinas e sistemas para otimizar processos, melhorando a eficiência operacional e impulsionando a produtividade.

Essa era industrial possibilitou que as empresas pudessem operar de forma mais inteligente, identificando padrões, prevenindo falhas e tomando decisões com base em dados concretos, tudo em tempo real.

Com a evolução para a Indústria 5.0, a IoT não apenas continuou a desempenhar seu papel na conectividade e análise de dados, mas também se expandiu para promover a colaboração entre humanos e máquinas de uma maneira mais harmoniosa e eficiente.

Na Indústria 5.0, a IoT é utilizada para criar ambientes de trabalho mais adaptáveis, onde humanos e robôs colaboram em tarefas que se complementam. Isso significa que a IoT não só otimizou processos, mas também permitiu a capacitação dos trabalhadores, fazendo com que se concentrem em tarefas mais complexas e criativas, enquanto as máquinas lidam com as tarefas repetitivas e físicas.

Além disso, a IoT na Indústria 5.0 também está focada em personalização e experiência do cliente. Com dados coletados em tempo real sobre as preferências dos clientes e as demandas do mercado, as empresas podem adaptar sua produção de forma ágil e eficiente, oferecendo produtos e serviços altamente personalizados e sob demanda.

2.2.1 Uso da IoT em Ambientes Residenciais

A tecnologia IoT desempenha um papel crucial no ambiente residencial, além de promover uma automação de tarefas, também aprimora a qualidade dos serviços e fortalece a segurança do ambiente (Messeas, 2022).

O termo casa inteligente, frequentemente conhecido como *smart home*, é utilizado para descrever residências que adotam a tecnologia para automatizar e gerenciar várias funções. Isso vai desde o controle de dispositivos como aspiradores robôs, câmeras de segurança e fechaduras, até a regulagem de temperatura e iluminação. As casas inteligentes representam um ambiente altamente conectado e integrado, onde a comodidade é levada a um novo patamar (Messeas, 2022).

2.2.2 Os primeiros passos da IoT Residencial

De acordo com o do site positivo ([s.d.]), na década de 1960, o engenheiro Jim Sutherland da Westinghouse inventou a Echo IV, o primeiro operador eletrônico computadorizado para residências. Lançada em 1966, essa máquina complexa tinha a capacidade de armazenar receitas, imprimir lista de compras e, principalmente, controlar eletrodomésticos da cozinha, além de regular a temperatura da casa.

Na década de 1980, as tecnologias de automação residencial se tornaram mais acessíveis, tornando itens como portões eletrônicos, sistemas de segurança e sensores de presença populares. Foi nesse período que, mais precisamente em 1984 que surgiu o termo casa inteligente.

Como já mencionado, em 1990 Simon Hackett e John Romkey criaram a primeira torradeira de pão controlada pela Internet, que deu início a era da IoT.

No início dos anos 2000, a Microsoft apresentou uma visão inovadora para o futuro das casas inteligentes, incorporando conceitos precisos de dispositivos inteligentes, como sistemas de segurança interconectados e serviços de automação. Essas ideias anteciparam um ambiente residencial altamente conectado e automatizado.

O avanço substancial nessa trajetória foi impulsionado pela proliferação dos *smartphones*, que se tornaram os principais aliados no processo de automação residencial. Eles não apenas ampliaram as possibilidades, mas também atingiram uma escala global, tornando a automação residencial acessível e conveniente para um público amplo. Com a capacidade de controlar dispositivos e sistemas diretamente de seus *smartphones*, os proprietários de residências conquistaram um controle mais prático e abrangente sobre suas

casas inteligentes. Essa tendência continua até os dias atuais. Na Figura 1 pode-se observar a evolução da automação residencial ao longo de cinco décadas.

3. CFTV IP

O avanço da tecnologia tem revolucionado a forma de garantir a segurança em ambientes, sejam eles residenciais, comerciais ou industriais. Entre as inovações mais significativas nesse campo, o sistema de Circuito Fechado de TV (CFTV) baseado em IP tem se destacado como uma solução poderosa e versátil.

Segundo Marcelo Peres (2004-2006) CFTV IP utiliza a infraestrutura de redes de dados para transmitir e gravar imagens de vídeo em tempo real. Isso significa que as câmeras de vigilância são conectadas a uma rede de computadores, permitindo o monitoramento remoto e o acesso às imagens de qualquer lugar com conexão à Internet.

3.1. Algumas considerações essenciais sobre a segurança no sistema de CFTV IP

A utilização do CFTV é direcionada à segurança, contudo, ele apresenta suas próprias fragilidades, tais como ataques de força bruta e interceptação de senha entre cliente e servidor. Para mitigá-las, é crucial empregar criptografia de dados, controle de acesso, atualizações de segurança, armazenamento seguro de informações e capacitação dos usuários. A criptografia de dados garante a integridade da informação, através da codificação da informação, ou seja,não pode ser acessada, logo não pode ser alterada por usuários não autorizados. O controle de acesso limita quem pode acessar informações. Atualizações de segurança corrigem vulnerabilidades conhecidas. O armazenamento seguro e a capacitação dos usuários complementam essas medidas, fortalecendo a proteção contra ameaças cibernéticas, e nesse paragrafo citou Silva(2018):

Criptografia de Dados: Uma das maiores preocupações ao transmitir imagens de vídeo pela Internet é garantir que esses dados não sejam interceptados ou acessados por pessoas não autorizadas. Portanto, é fundamental implementar medidas de criptografia robustas para proteger a integridade e a confidencialidade das transmissões de vídeo.

Controle de Acesso: O acesso ao sistema de CFTV IP deve ser estritamente controlado. Isso significa atribuir credenciais de acesso exclusivas a cada usuário autorizado e garantir que apenas pessoas autorizadas possam visualizar e gerenciar as imagens das câmeras. Além disso, é essencial implementar políticas de senhas fortes e atualizadas regularmente para evitar violações de segurança.

Atualizações de segurança**:** Assim como qualquer outro sistema baseado em tecnologia, o *software* utilizado no sistema de CFTV IP deve ser mantido atualizado para garantir que quaisquer vulnerabilidades de segurança conhecidas sejam corrigidas. Isso inclui tanto o *software* das câmeras de vigilância quanto o *software* dos dispositivos de armazenamento e monitoramento.

Armazenamento Seguro de Dados: As imagens de vídeo capturadas pelo sistema de CFTV IP contêm informações sensíveis e devem ser armazenadas de forma segura para evitar acesso não autorizado ou adulteração. Isso pode incluir a criptografia dos dados armazenados, o uso de sistemas de armazenamento redundante com *pen drive* e a implementação de políticas de retenção de dados adequadas.

Treinamento de Usuários: Por fim, é crucial fornecer treinamento adequado aos usuários do sistema de CFTV IP para garantir que eles compreendam as melhores práticas de segurança e saibam como utilizar o sistema de forma segura e eficaz. Isso pode incluir treinamento e conscientização dos ataques já existentes como o *phishing* e *trojan*.

3. Metodologia do desenvolvimento prático

No trabalho, é empregada a abordagem de pesquisa exploratória para realizar o levantamento de informações sobre os dispositivos IoT, com o objetivo de compreender suas vulnerabilidades e limitações. Ademais, para a realização deste trabalho utiliza-se metodologias de pesquisa associadas a metodologia descritiva em conjunto com a pesquisa exploratória que segundo Severino (2013, p.107):

> […] busca apenas levantar informações sobre um determinado objeto, delimitando assim um campo de trabalho, mapeando as condições de manifestação desse objeto. Na verdade, ela é uma preparação para a pesquisa explicativa.

Baseando-se em dados colhidos em um compilado de fontes teóricas tais como livros especializados, monografias, e outros artigos acadêmicos que tratam da temática. Inicialmente, realiza-se uma abrangente análise dos dados colhidos, focada na obtenção de informações relevantes relacionadas à IoT.

Durante o estudo foram identificadas as principais aplicações de dispositivos IoT em ambientes residenciais. Reconhecendo possíveis riscos e ameaças nestes. Isso inclui uma investigação aprofundada das vulnerabilidades que podem comprometer a segurança e a privacidade dos dispositivos, assim como a avaliação das possíveis consequências de tais riscos. Ao adquirir um entendimento sólido das demandas identificadas nos dispositivos são desenvolvidas recomendações.

Após uma análise detalhada, procedeu-se à instalação e configuração de uma câmera IP em um ambiente de teste. Com base nas informações obtidas durante a pesquisa exploratória, foram conduzidos testes para identificar vulnerabilidades e destacar as possíveis consequências dessas falhas de segurança.

4.1 Desenvolvimento

Primeiramente, realizou-se a seleção dos equipamentos necessários para o projeto, que incluem: uma câmera IP, DVR (gravador de vídeo digital), *smartphone* e um Ponto de acesso.

A escolha dos equipamentos foi fundamentada nos critérios de preço e qualidade, priorizando marcas consolidadas em mercado e com amplo suporte para seus produtos. Essas marcas são utilizadas tanto em ambientes domésticos quanto em ambientes organizacionais, garantindo confiabilidade e desempenho. Abaixo está a lista dos equipamentos utilizados nesse projeto com suas respectivas descrições:

4.1.1 Câmera: Hikvision - DS-2CD2032-I - Câmera IP IR Bullet 3MP DWDR

Figura 1 – Câmera IP

Fonte: Amazon[1]

A câmera Hikvision DS-2CD2032-I é uma câmera IP Bullet de alta resolução com 3 *megapixels* e tecnologia IR (infravermelho) para visão noturna. Ela foi escolhida com base nos critérios de preço e qualidade para atender às necessidades de segurança do projeto. A resolução de 3 *megapixels* acompanha os padrões de qualidade para captura de imagens e monitoramento, também possui a função DWDR (Wide Dynamic Range Digital), que garante a captura de imagens com alta qualidade mesmo em ambientes com iluminação desafiadora, como locais com alto contraste de luz e sombra. Além disso ela possui recursos avançados como detecção de movimento, análise de vídeo e suporte a protocolos de rede.

A média de preço da câmera Hikvision DS-2CD2032-I, no ano desta pesquisa está entre US$ 20,79 dólares.

1 Disponível em: https://www.amazon.com/Hikvision-DS-2CD2032-I-Bullet-Security-Network/dp/B00G7GMEOG. Acesso em: 02 abr. 2024.

4.1.2 DVR: Intelbras Multi HD- MHDX 1104

Figura 2 - DVR

Fonte: Intelbras[2]

O gravador digital de vídeo (DVR) Multi HD MHDX 1104, fabricado pela Intelbras, empresa brasileira de segurança eletrônica e telecomunicações, é compatível com cinco tecnologias de transmissão de vídeo: HDCVI, AHD, HDTVI, Analógica e IP. As tecnologias HDCVI, AHD e HDTVI permitem a transmissão de vídeos em alta definição através de cabos coaxiais, suportando resoluções de até 4k. Em contraste, a tecnologia analógica transmite vídeos em resoluções mais baixas, como 480p ou 720p. Por sua vez, o IP possibilita a transmissão de vídeos em resoluções que ultrapassam 4k e oferece recursos adicionais, como *backup* em nuvem, gerenciamento de logs e configurações específicas, como sistema de intrusão.

O valor médio deste equipamento, no ano desta pesquisa encontra-se entre US$126,27 dólares.

4.1.3 Smartphone: Samsung A32

Para o projeto foi utilizado o *smartphone* Samsung Galaxy A32 que possui um processador MediaTek Helio G80, 4GB de memória RAM e possui 128 GB de armazenamento interno. Seu preço médio é de US$253,83 dólares, para a configuração desses dispositivos, qualquer aparelho *Android* atenderia os requisitos para a instalação do aplicativo de monitoramento.

2 Disponível em: https://www.intelbras.com/pt-br/gravador-digital-de-video-4-canais-mhdx-1104. Acesso em: 02 abr. 2024.

4.1.4 Ponto de Acesso: SAGEMCOM ST3486

Figura 3 - SAGEMCOM ST3486

Fonte: Claro[3]

O Sagemcom ST3486 é um *modem* que possui funções de *modem* e roteamento em um único equipamento, ele oferece velocidade de até 300Mbps na banda de 2,4GHz, possui portas Ethernet para conexão por cabo RJ45E e contem configurações de *firewall* e criptografia WPA/WPA2.

O equipamento é instalado pelo provedor de Internet, logo os valores são integrados com os custos de instalação, ou seja, cada provedor possui sua média de valores. No ambiente de teste foi utilizado o equipamento fornecido pela Claro, mas qualquer ponto de acesso é compatível para realizar a configuração dos equipamentos de monitoramento.

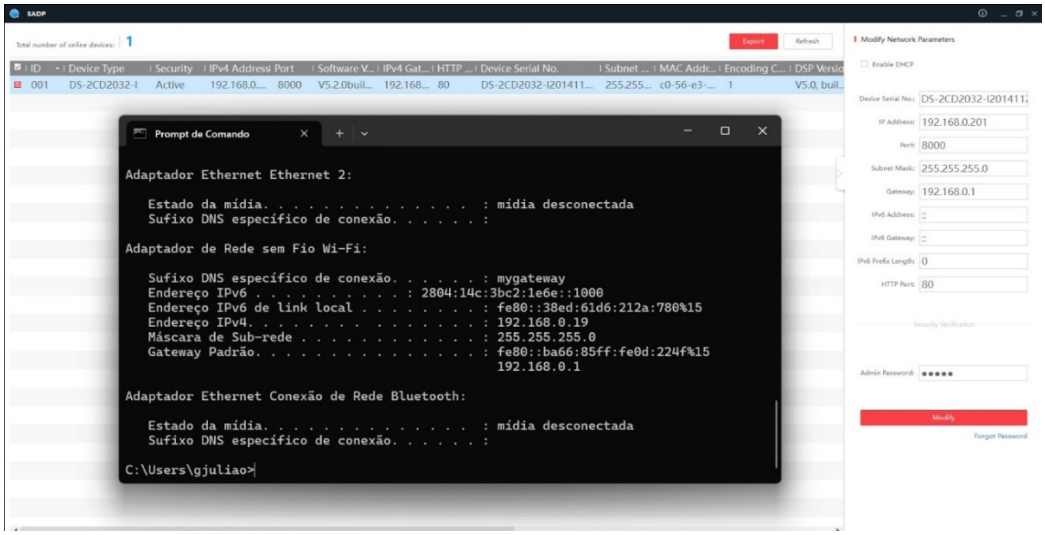
Após finalizar a seleção dos equipamentos, procedeu-se com a configuração dos mesmos.

Inicialmente, realizou-se a conexão dos dispositivos a um ponto de acesso à Internet. Devido à discrepância de marcas entre a câmera e o DVR, além de estarem em redes distintas, foi necessário estabelecer um endereço IP estático, para que não ocorra o risco do equipamento assumir outro IP dentro da rede, pois quando DVR e câmera IP estiverem

3 Disponível em: https://configuraraparelhos.claro.com.br/sagemcom/f-st-3486/especificacoes.Acesso em: 04 abr. 2024

vinculados, as informações serão transmitidas através da rede com destinos já definidos nas configurações, caso contrário, se um dos dois dispositivos ou ambos assumirem IP's diferente, o direcionamento de informações ficariam obsoletos, ocasionando na não troca de informações entre os dois.

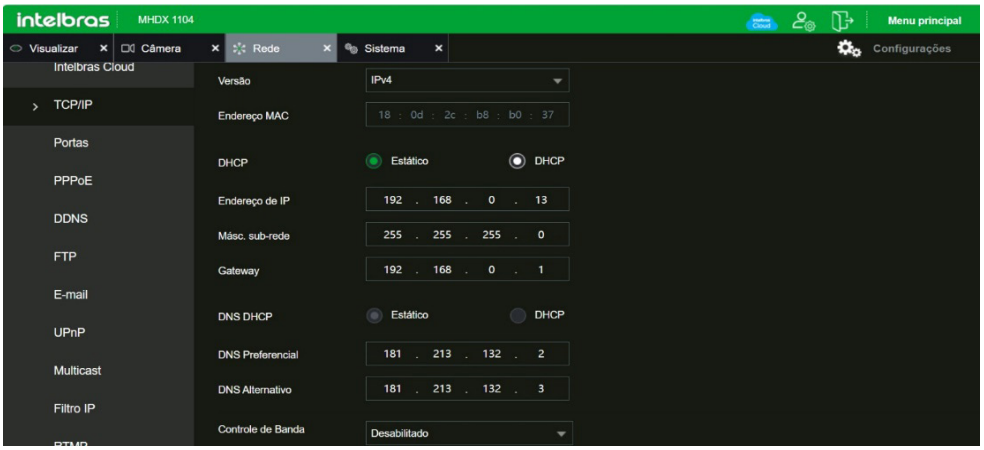
Figura 4 - Alteração de IP



Fonte: Próprio autor

Após alteração de IP da câmera, conforme visto na figura 4, foi acessado a configuração do DVR via porta HTTP, alterando o endereçamento do mesmo que se encontrava em DHCP para um IP estático.

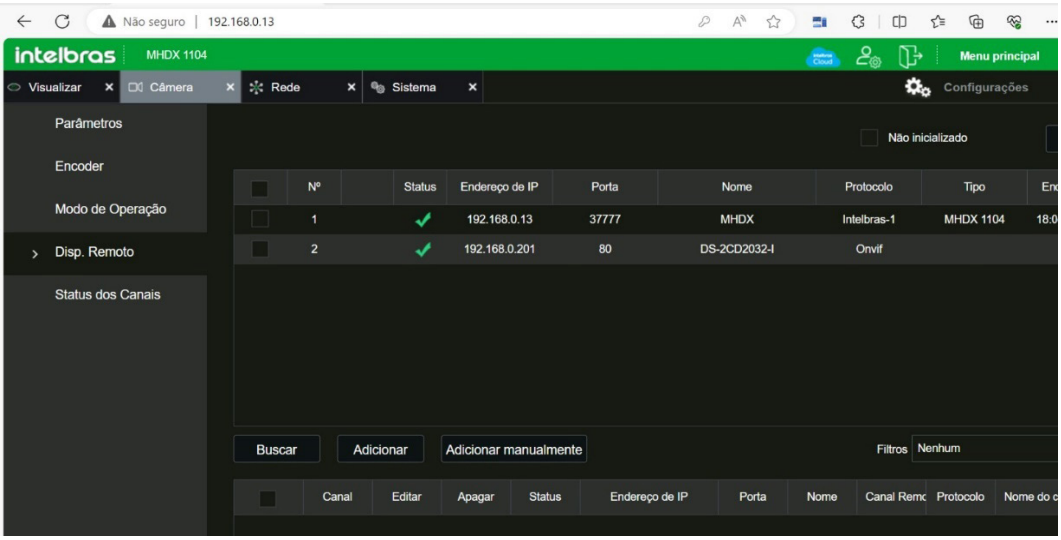
Figura 5 - Endereçamento IP DVR



Fonte: Próprio autor

Os dois dispositivos com endereços fixos e na mesma Subrede, conforme figura 5, automaticamente se identificam para possíveis conceções. Isso trouxe informações de forma clara e objetiva dos equipamentos, conforme figura 6.

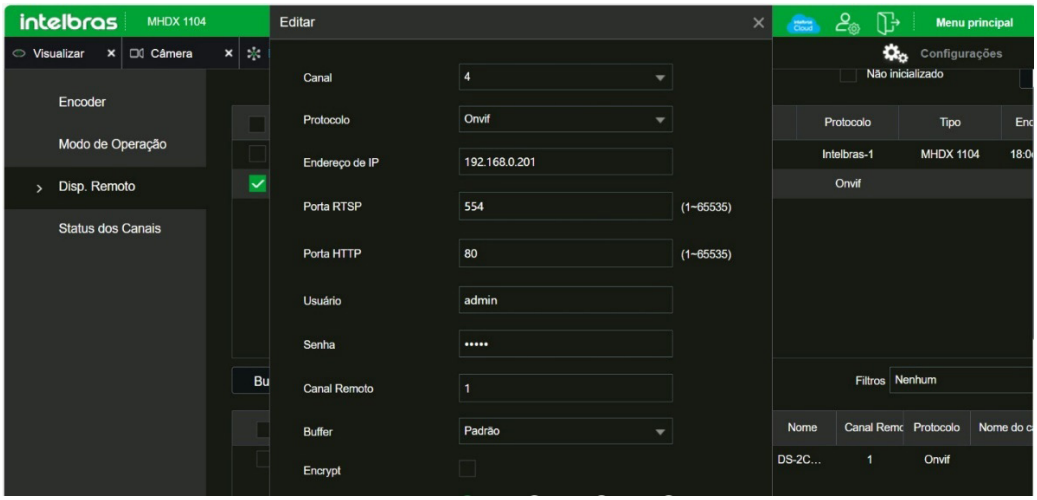
Figura 6 - Informações dos equipamentos



Fonte: Próprio autor

Foi iniciada a adição da câmera IP ao aparelho DVR, selecionando a mesma e clicando no botão "adicionar", sendo necessário preencher usuário e senha cadastrados na ativação dos dispositivos, figura 7.

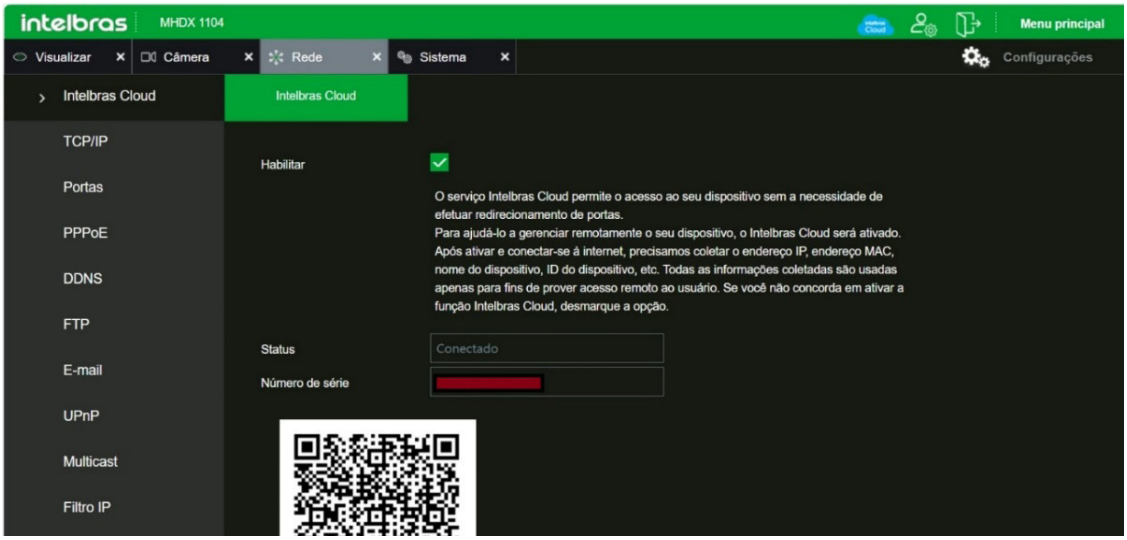
Figura 7 - Adicionando câmera ao DVR



Fonte: Próprio autor

Finalizada a configuração dos equipamentos conforme visto nas figuras 4,5,6 e 7 foi dado início à vinculação do dispositivo através do *smartphone*. A vinculação foi feita utilizando a aplicação ISIC lite conforme orientado pelo fabricante do DVR, figura 8.

Figura 8 - Vinculação ao aplicativo



Fonte: Próprio autor

Figura 9 - Configuração do Aplicativo

Fonte: Próprio autor

Utilizando o aplicativo ISIC Lite, figura 9, aplicativo que permite ao usuário realizar o monitoramento através do aparelho celular, foi possível efetuar o monitoramento contínuo do ambiente em tempo real, além de realizar capturas, gravações de vídeo e imagem, inclusive com a funcionalidade de áudio. Além disso, a aplicação possui em sua configuração um sistema de envio de notificação em casos de intrusão dentro do perímetro previamente programado e definido em configurações.

Com o ambiente pronto, foi realizado os testes de segurança, incluindo teste de negação de serviço e ataque de força bruta. Para tal foram utilizadas as aplicações *SADP* e *Wireshark.*

Ambas as aplicações utilizadas são buscadores de rede, capturando informações sobre os dispositivos que trafegam em nosso ambiente de teste.

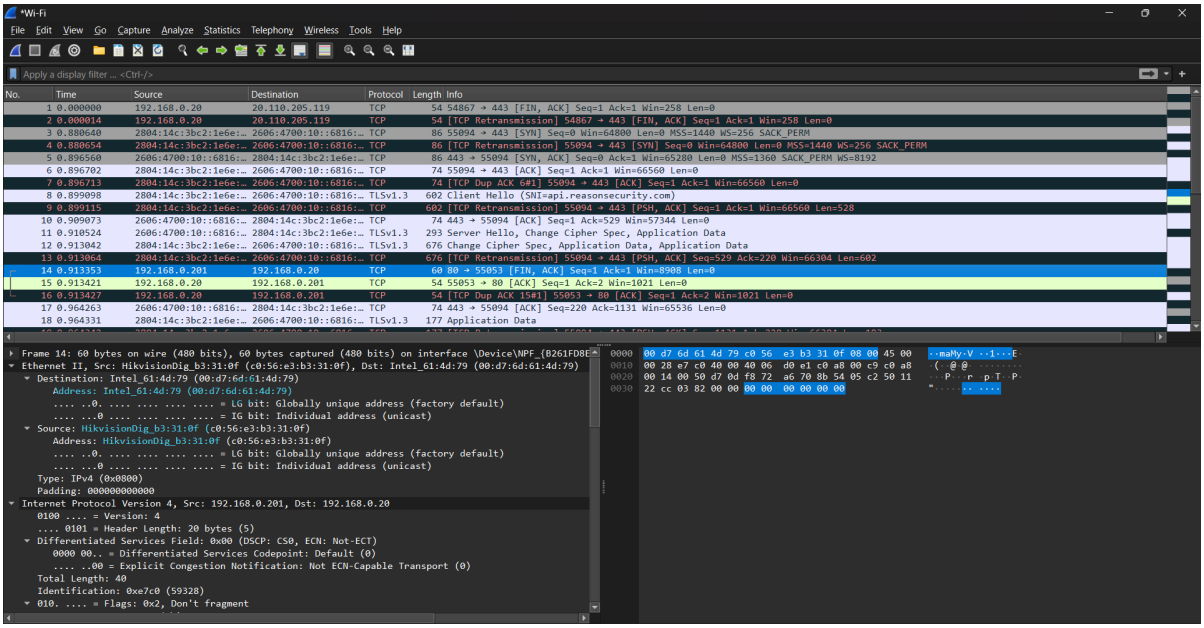
Segundo Ahlgre, F.T (2020). SADP é um software de ativação dos dispositivos de segurança, manutenção e monitoramento dos mesmos que estão conectados a rede. Trazendo informações sobre os dispositivos *Hikvision* em sua rede local, conforme visto na figura 16.

De acordo com, Cordeiro.F, Santos.G e Oliveira.H (2023), o *wireshark* possui várias aplicações e foi utilizada nesse estudo de caso como umas das principais ferramentas para o monitoramento e análise do tráfego de rede gerado pelos testes realizados (figura 10), permitindo a captura de pacotes de rede, análise de protocolos, e identificação de padrões de tráfego.

Para a realização do teste prático, baseou-se o cenário em uma rede doméstica onde amigos, vizinhos e provedores têm acesso ao local e à rede de internet.

Inicialmente, realizou-se a conexão à rede Wi-Fi e deu-se início ao primeiro ataque, o Brute Force. Utilizando o SO *kali Linux* e a aplicação Wireshark, foi feita a coleta do tráfego para localizar o endereçamento lógico dos dispositivos conectados à rede, conforme visto na figura 10.

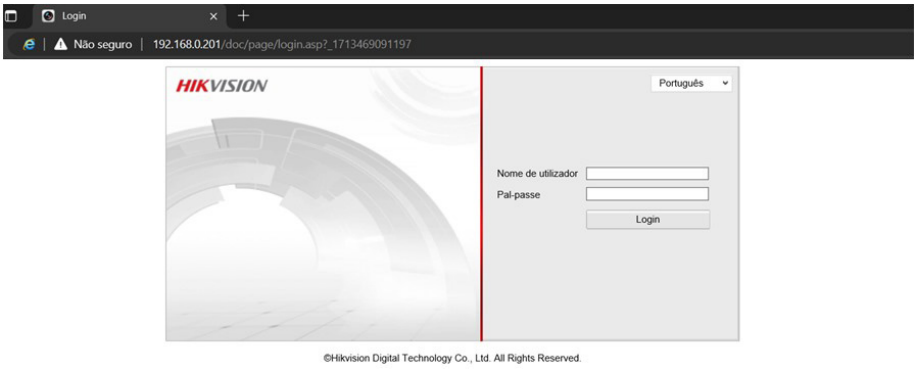
Figura 10: Wireshark



Fonte: Próprio Autor

Após identificar o IP da câmera, acessou-se o navegador para verificar o acesso ao software do equipamento, onde foi constatada a necessidade de credenciais para autenticação (figura11).

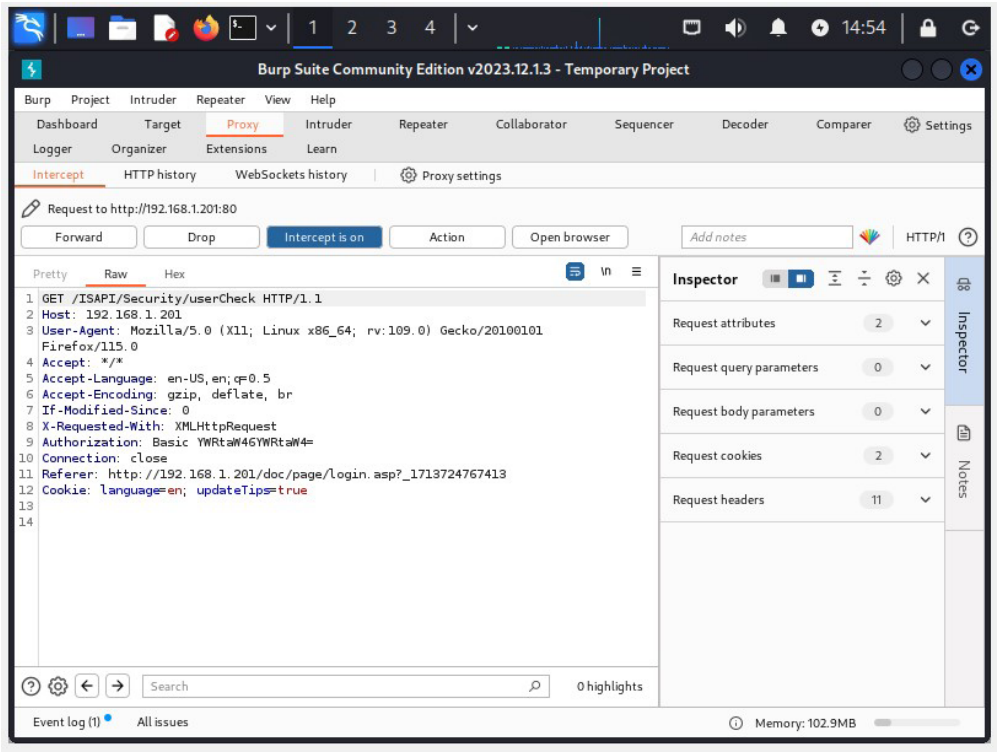
Figura 11: Software câmera



Fonte: Próprio autor

A realização de várias tentativas diretamente no software poderia ocasionar bloqueio de acesso, sendo assim foi utilizado o *Burp Suite* para ver o conteúdo do *request*, e com os dados analisados foi realizado a tentativa de acesso a interface com a ferramenta *Hydra*(figura 12).

Figura 12: Burp Suite

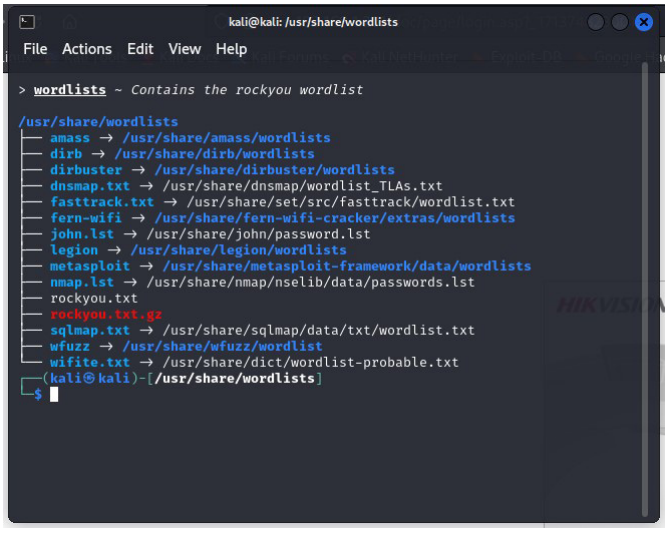


Fonte: Próprio Autor

Por padrão essa câmera de segurança já vem com usuário de login definido e não permite alteração, sendo ele 'admin', logo foi necessário apenas o brute force na senha.

Para iniciar o *Brute Force* na senha, foi utilizado o arquivo *Rockyou.txt* que se encontra nas aplicações de *wordlist* disponíveis no *Kali Linux* (figura 13).

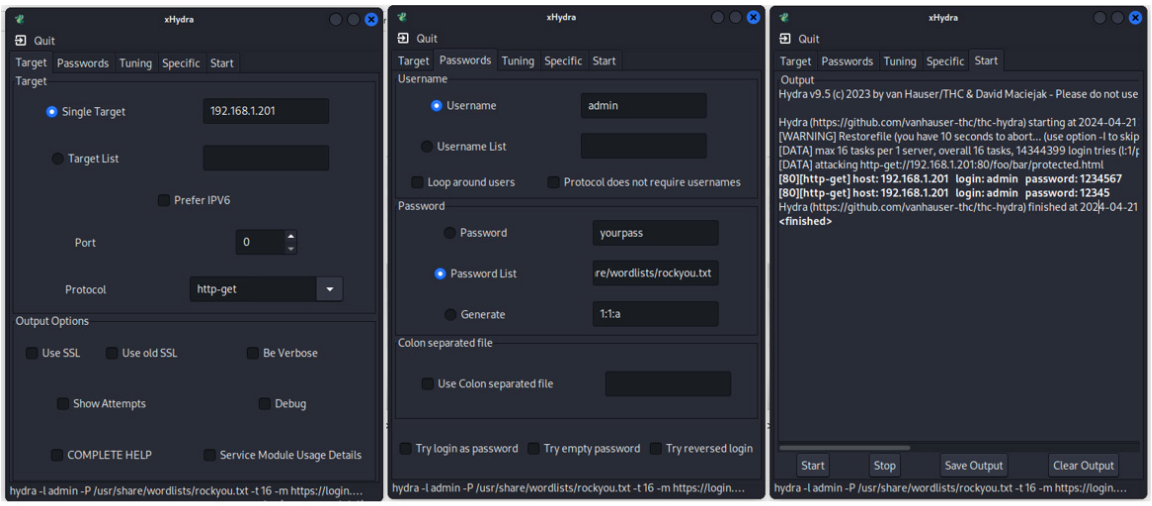
Figura 13: Arquivo Rockyou.txt



Fonte: Próprio Autor

Com o arquivo rockyou.txt e o *request*, foi utilizado a interface gráfica do Hydra para iniciar o ataque de *Brute Force* (figura 14).

Figura 14: Ataque Hydra



Fonte: Próprio Autor

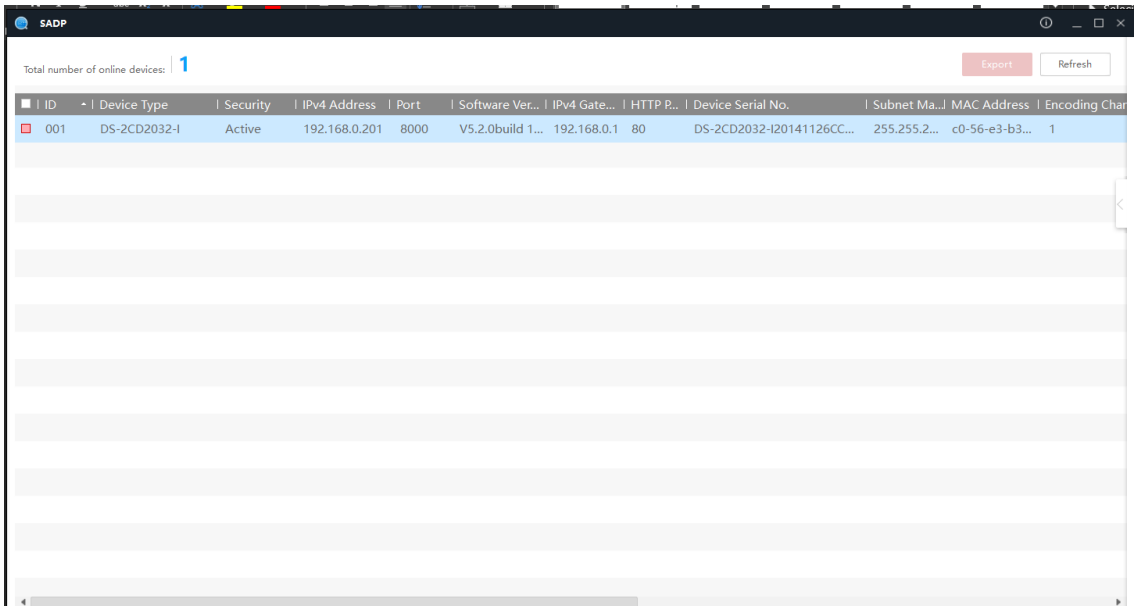
Em seguida, o Hydra validou duas possíveis senhas para a câmera IP, conforme visto na figura14, e com isso foi possível obter acesso as imagens coletadas pelo equipamento em tempo real, conforme visto na figura 15.

Figura 15: Ataque bem-sucedido.

Fonte: Próprio Autor

Para o segundo ataque, DDoS com a finalidade de utilizar outras ferramentas realizamos o mapeamento do IP através do SADP, conforme figura 16.

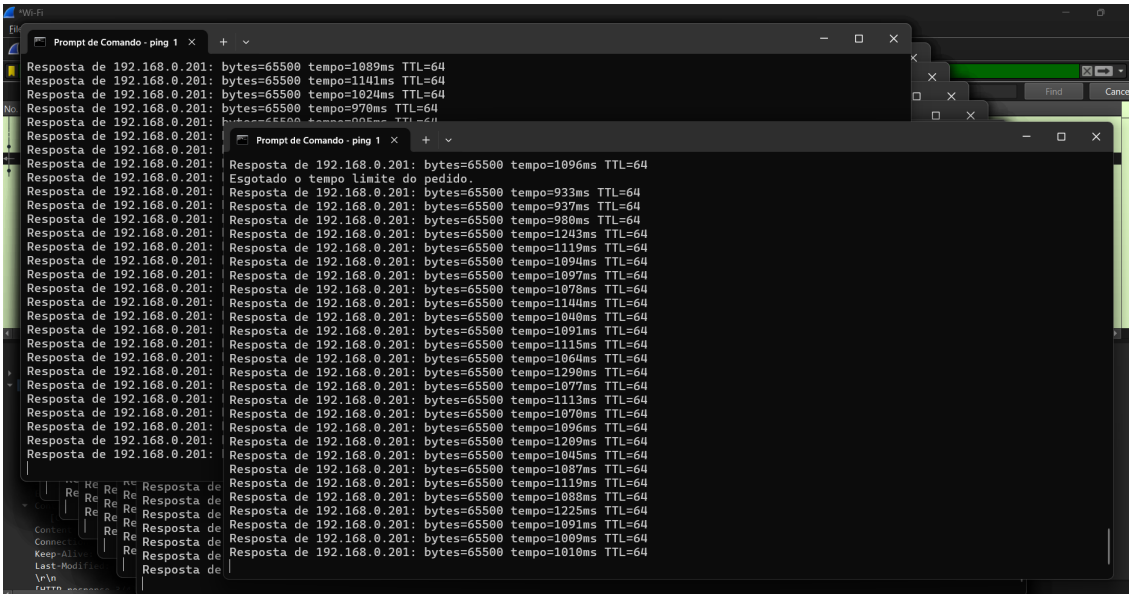
Figura 16: Sniffing SADP



Fonte: Próprio Autor

Com o IP identificado utilizamos o CMD para realizar um ataque DDoS com o intuito de sobrecarregar o dispositivo com o volume excessivo de trafego, tornando os pacotes enviados e recebidos pelo dispositivo inacessíveis, ocasionando assim indisponibilidade do equipamento (figura 17).

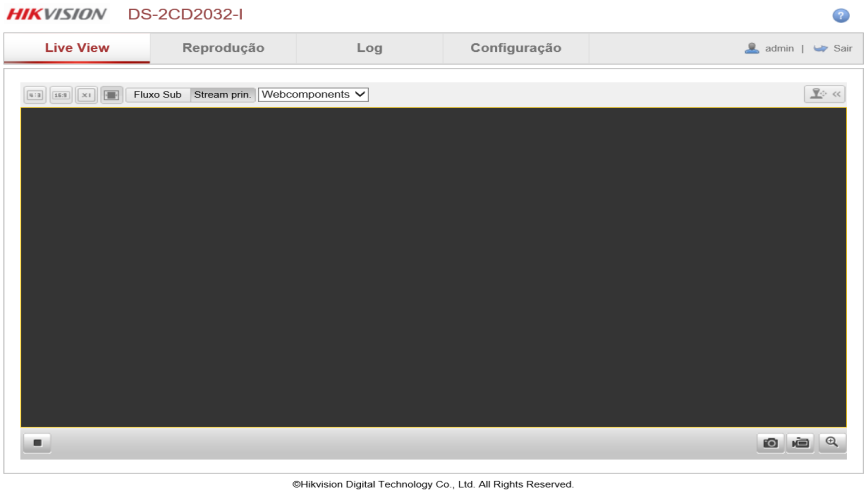
Figura 17: Ataque DDoS



Fonte: Próprio Autor

Após inúmeros envios de pacotes o equipamento sofreu sobrecarga e ficou indisponível, conforme exibido na figura 18.

Figura 18: DDoS bem-sucedido.



Fonte: Próprio Autor

Com base nos resultados, foram identificadas vulnerabilidades físicas e vulnerabilidades logicas:

Vulnerabilidades físicas: Fácil acessibilidade da entrada RJ45 pela qual o aparelho se conecta à rede, podendo resultar em danos ao dispositivo, como a quebra ou remoção do conector, resultando na indisponibilidade de serviço e acesso a gravações e monitoramento em tempo real. Além disso, a câmera possui em sua parte traseira um botão de reset que pode ser manipulado facilmente causando perda de configuração do equipamento.

Vulnerabilidade Logica: Aparelhos conectados à rede IP estão visíveis para todos os usuários da mesma rede, o que, em conjunto com *softwares* específicos, pode ser explorado por terceiros para comprometer a disponibilidade e integridade das informações, conforme demostrado nesse estudo de caso. Um usuário mal-intencionado que tenha acesso ao IP pode também acessar a gerência do sistema e realizar ataques lógicos, como alteração de endereço, imagens e qualidade, gravações e áudios.

Após a conclusão do experimento, foram identificadas medidas de mitigação para cada uma das vulnerabilidades encontradas, para a vulnerabilidade física foi encontrado o uso do protetor para câmeras *Bullet* onde o mesmo esconde o conector e o botão Reset do equipamento. visando fortalecer a segurança do sistema e prevenir potenciais ataques.

Figura 20: Protetor para câmera.

Fonte: Mercado Livre[4]

E para as vulnerabilidades logicas foi selecionada seguintes medidas de proteção:

A utilização de controles de rede via modem para bloquear portas especificas de acesso para quaisquer IP's que trafeguem em sua rede local;

Configurar a câmera em uma VPN na tentativa de ocultar o IP da câmera;

Utilizar um outro link de internet para configurar os dispositivos e ocultar a rede Wi-Fi, garantindo mais segurança.

Após uma análise minuciosa, o estudo busca oferecer uma contribuição significativa para a segurança da informação em dispositivos IoT residenciais. O objetivo é proporcionar uma compreensão mais profunda e promover melhorias na segurança nesse campo emergente.

5. CONCLUSÃO

Foi concluído, através deste estudo teórico e prático, utilizando conhecimentos adquiridos durante o curso e materiais acadêmicos para nossa pesquisa, os desafios e as oportunidades associadas à implementação da Internet das Coisas (IoT) na segurança residencial, especificamente aparelhos de monitoramento conectados à rede. Ao analisar profundamente questões como a integração eficiente de dispositivos IoT e a proteção contra ameaças cibernéticas, foi identificado estratégias e soluções para mitigar os riscos de segurança a que esses dispositivos estão sujeitos em um ambiente residencial.

Em sua maioria, os dispositivos IoT são de fácil acesso e manejo, tanto pelos usuários mais experientes em tecnologia quanto pelos mais leigos, o que os torna extremamente vulneráveis e suscetíveis à ação de invasores ou pessoas mal-intencionadas. É evidente que, apesar dos dispositivos de segurança estudados em questão utilizarem maneiras para

4 Disponível em: Protetor Para Câmera Bullet Proteção Para Câmera Canhão | MercadoLivre. Acesso em: 22 abr. 2024.

impedir o acesso não autorizado, ainda existem maneiras de contornar essas barreiras, sejam pelas vulnerabilidades físicas ou lógicas exploradas no trabalho desenvolvido.

O objetivo do estudo de caso foi apresentar uma realidade na qual milhares de dispositivos, como aquele exemplificado, estão conectados a redes domésticas, vulneráveis a ataques. Isso aumenta o risco de vazamento de dados e imagens pela internet, ficando à disposição de indivíduos mal-intencionados para serem explorados conforme sua vontade. Embora haja diversas estratégias para mitigar esses riscos, é essencial que os usuários compreendam o dispositivo presente em suas residências e estejam cientes de seu potencial, especialmente em situações graves, como um vazamento de informações, mesmo em dispositivos aparentemente simples, como câmeras de segurança.

Referências

Ahlgre, F.T **CAMERA SECURITY CASE: Hikvision and Label X camera.**2020. Tutku University pf Applied sciences. Disponivel em: <https://www.theseus.fi/bitstream/handle/10024/353692/Frans_Ahlgren_IoT_newest.pdf?sequence=2&isAllowed=y > Acesso em: 30 abr. 2024

Positivo, **A história da automação residencial: cinco décadas de evolução.** POSITIVO,2020. Disponível em: <https://blog.positivocasainteligente.com.br/historia-automacao-residencial/> Acesso em: 25 abr. 2023.

APETI, **Internet das coisas: vantagens e desvantagens dessa revolução.** APETI, 2023. Disponível em: <https://apeti.org.br/blog/internet-das-coisas-vantagens-e-desvantagensdessarevolucao#:~:text=Principais%20desvantagens,se%20torna%20uma%20quest%C3%A3o%20crucial. > Acesso em: 31 out 2023.

CASTRO, B. S., Melo, G. M. P., Mesquita, Y. F. **Testes de segurança e privacidade em um dispositivo de monitoramento remoto:** identificando vulnerabilidades. 2022 Bacharelado em Sistemas da Informação, Instituto Federal de Educação, Ciência e Tecnologia de Goiás, Campus Goiânia. Goiânia, GO. 2022.

Cordeiro,F., Santos,G. e Oliveira,H. **Monitoramento de ataque loic utilizando o wireshark.**2023. Congresso de Segurança da Informação das Fatecs.2023.

DAMASCENO, G. **Desafios na aplicação de tecnologias IOT em residências:** uma análise sobre os atributos da segurança da informação. 2022. Trabalho de conclusão de curso (artigo científico). Instituto Federal de Educação, Ciência e Tecnologia do Piauí. Campus Floriano. Floriano.2022

EVANS, D. **A Internet das coisas como a próxima evolução da Internet está mudando** tudo. 2011. Disponível em: <https://www.cisco.com/c/dam/global/pt_br/assets/executives/pdf/internet_of_things_iot_ibsg_0411final.pdf> . Acesso em: 02 nov. 2023.

FIA. **History of IoT 2021.** Disponível em: https://www.fia.uk.com/news/history-of-iot.html. Acesso em 06 mar. 2024.

GHAFFARIANHOSEINI, A. et al. **The essence of smart homes:** application of intelligent technologies towards smarter urban future. 2016.Disponível em:<https://www.researchgate.net/publication/316996187_The_essence_of_smart_homes_Application_of_intelligent_technologies_towards_smarter_urban_future>. Acesso em 22 mar.2024

GREENGARD, S. **The Internet of Things.**Londres, Inglaterra:The MIT Press, 2015.

GODOI, M; ARAÚJO, L. **A Internet das coisas: evolução, impactos e benefícios.**2018. Artigo. Faculdade de Tecnologia de Catanduva (FATEC). Catanduva. 2018. Disponível em: <ttps://revista.fatectq.edu.br/interfacetecnologica/article/view/538/363>. Acesso em: 31 out. 2023.

Hintzbergen J.; Hintzbergen K.; Smulders A.; Baars H. **Foundations of Information Security: based on ISO 27001 and 27002**, 3ª edição revisada. Série "Best Practices". Copyright: © Van Haren Publishing, 2010,2015

HUREL, L. M.; LOBATO, L. C. **Segurança e privacidade para a Internet das Coisas.** Instituto Igarapé, Rio de Janeiro, p. 1–22, 2018. Disponível em: <https://www.researchgate.net/profile/LouiseMarieHurel/publication/329972976_Seguranca_e_Privacidade_para_a_Internet_das_Coisas/links/5c269915a6fdccfc706f3001/Seguranca-e-Privacidade-para-a-Internet-das-Coisas.pdf.> Acesso em: 31 out. 2023.

LEITE, L. **Internet das coisas (IoT): vulnerabilidades de segurança e desafios.** 2019. Monografia (curso superior de tecnologia em segurança da informação) – Faculdade de Tecnologia de Americana – Centro estadual de educação tecnológica Paula Souza. Americana. 2019. Disponível em: <https://ric.cps.sp.gov.br/handle/123456789/3978>. Acesso 11 nov. 202>. Acesso em: 18 de mar. 2024.

LIMA, G. **Uma visão geral sobre segurança em soluções IOT para ambientes residenciais.** 2023. Trabalho de Conclusão de Curso (Graduação em Tecnologia em Telemática). Instituto Federal da Paraíba. Paraíba, 2023.

Lyra M2M. **A relação da IoT com a Indústria 4.0 e a indústria 5.0: o guia definitivo.**2023. Disponível em: https://blog.lyram2m.com.br/iot-na-industria-5/. Acesso em: 28 abr. 2024.

MAGRANI, Eduardo. **A Internet das Coisas.** Rio de Janeiro: FGV EDITORA, 2018. Disponível em: <https://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/23898/A%20internet%20das%20coisas.pdf.> Acesso em: 11 nov. 2023.

MANCINI, M. **A história da Internet das coisas ou Internet of things (IoT).** Disponível em: https://www.linkedin.com/pulse/hist%C3%B3ria-da-internet-das-coisas-ou-things-iot-m%C3%B4nica-mancini/?originalSubdomain=pt > Acesso em: 06 mar. 2024.

MESSEAS, G. **Estudo sobre a segurança de dispositivos domésticos conectados à Internet das Coisas.** 2022. Trabalho de Conclusão de curso (Bacharelato em Ciência da Computação) - Universidade Estadual de Londrina. Londrina. 2022.

MOCRII, D; CHEN, Y; MUSILEK, P. **IoT-based smart homes: a review of system architecture, software, communications, privacy and security. Internet Of Things,** [S.l.], v. 1-2, p. 81-98, 2018. Disponível em: <https://www.sciencedirect.com/science/article/abs/pii/S2542660518300477>. Acesso em: 30 out. 2023.

PERES, M. Guia do CFTV: **Curso básico**. Copyright GuiadoCFTV 2004-2006. Disponível em: <https://d1wqtxts1xzle7.cloudfront.net/37625519/cftv_basico-libre.pdf?1431548151=&response-content-disposition=inline%3B+filename%3DCftv_basico.pdf&Expires=1712988308&Signature=HKPeuXC7XGcKV~vNOiFg-mj7H0nunuoWzhDuVKKL3zXboEJUy~CaYmJCpG501HtOZoaNJb0SGuIdE-pUZGBwQIEiN-KFDIhJ4kj6CNFiBHh4-p4dwCw-mxKHhQXsgnX-XnYUGejlSCho0OGl9vNOaY-T3S8MovHTOrKv7Bd372rhKLZr1XAlZgHRIEwa06wHYlzHQgtv2T bdX-V9WzkJ-CaXzKXNEPTx6eWKPGggWrVHN02Sl-ANQ8H-tsappWaWyNj~Z 5o7iiTg-c6KHlO9gt5CyMAuJYpKh7KRrz4n6yjEdnfvqc5~8AgomsDkuBCN8mvIUti~AJJbA8W-CO5c3TlVfQ__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA>. Acesso em 25 de mar. 2024.

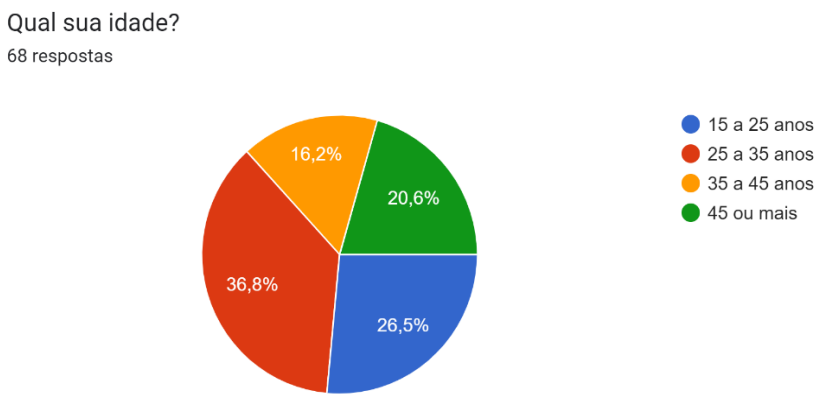
Silva, A. Segurança para câmeras IP.2018. **Trabalho de Conclusão de Curso - Universidade Federal de Uberlândia.** UFU. Uberlândia, 2018.

SINCLAIR, B; IoT: **como usar a Internet das coisas para alavancar seus negócios**; tradução Afonso Celso da Cunha Serra. -- 1. ed. -- São Paulo: Autêntica Business, 2018.

SINGER, T. **Tudo conectado: conceitos e representações da Internet das coisas**. **SIMSOCIAL** – II Simpósio em tecnologias digitais e sociabilidade – 11 e 12 de setembro 2012.

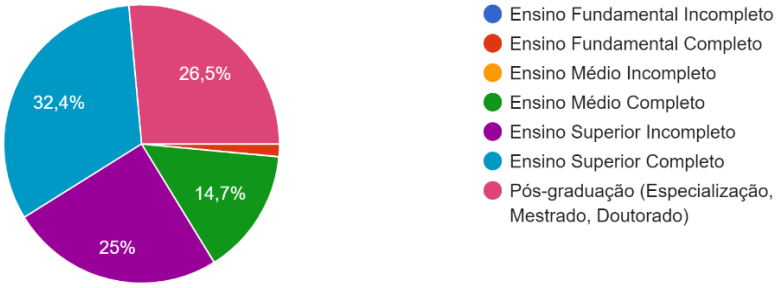
SEVERINO, A. J. **Metodologia do trabalho científico**. 24 ed. São Paulo: Cortez Editora, 2013. 304 p

Apêndice A – Questionário social sobre o conhecimento tecnológico



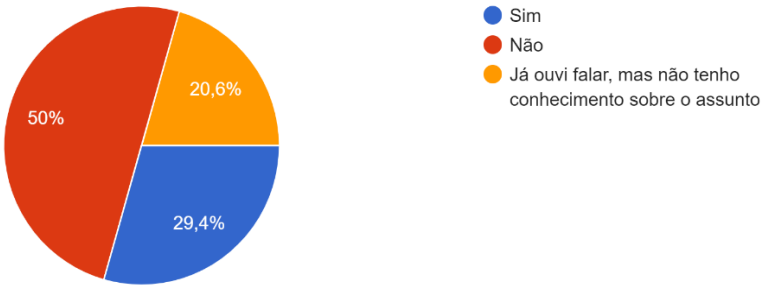
Qual é o seu nível de escolaridade?

68 respostas



Você sabe oque é IoT?

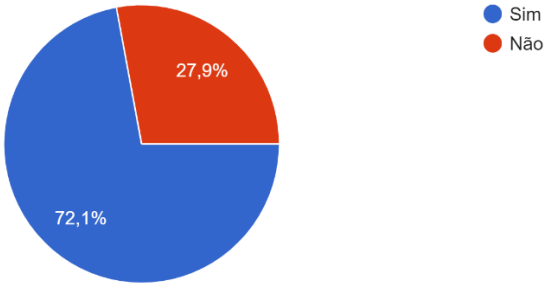
68 respostas



Apêndice B – O uso do IT

Você utiliza algum dispositivo IoT?

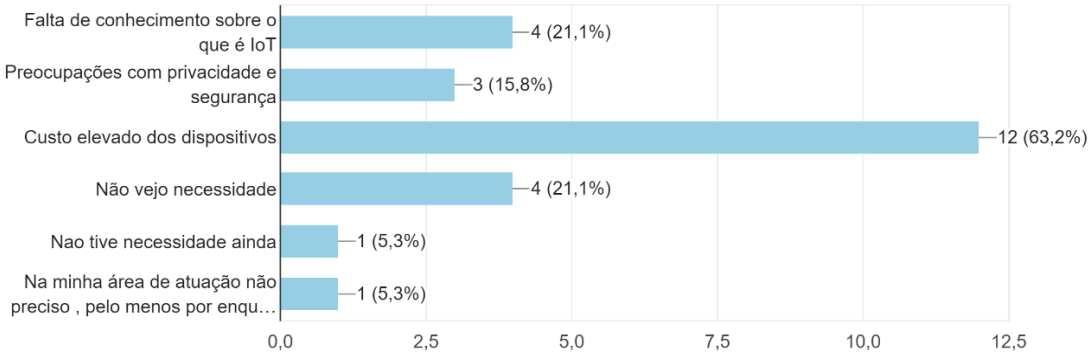
68 respostas



Apêndice C – Das pessoas que não utilizam

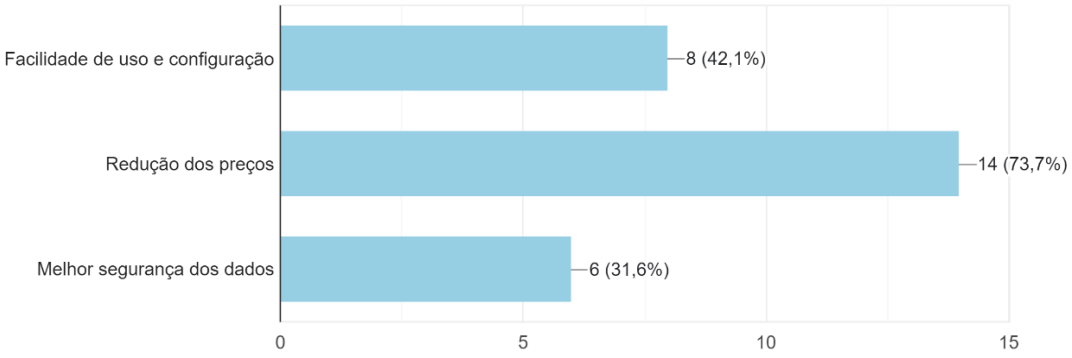
Qual é a principal razão para você não utilizar dispositivos IoT?

19 respostas



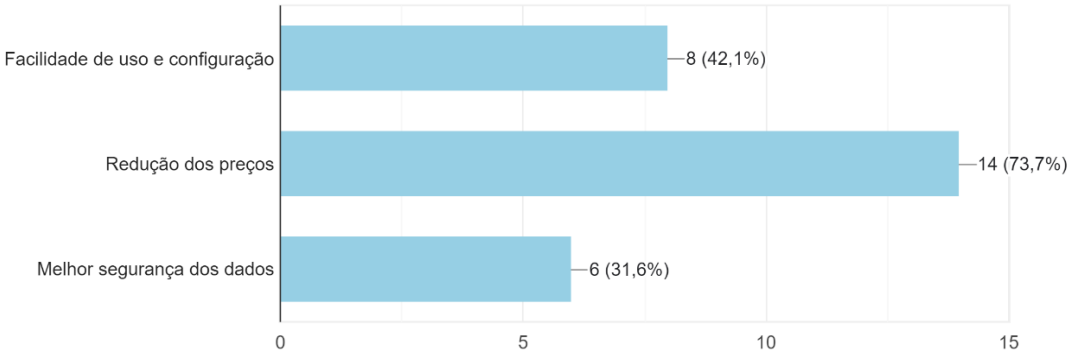
O que poderia motivar você a começar a usar dispositivos IoT?

19 respostas



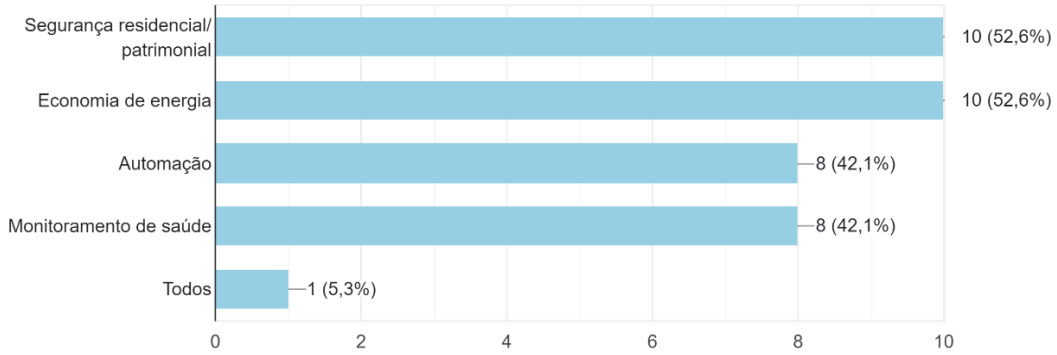
O que poderia motivar você a começar a usar dispositivos IoT?

19 respostas



Quais áreas da sua vida você acha que poderiam ser mais beneficiadas com a IoT?

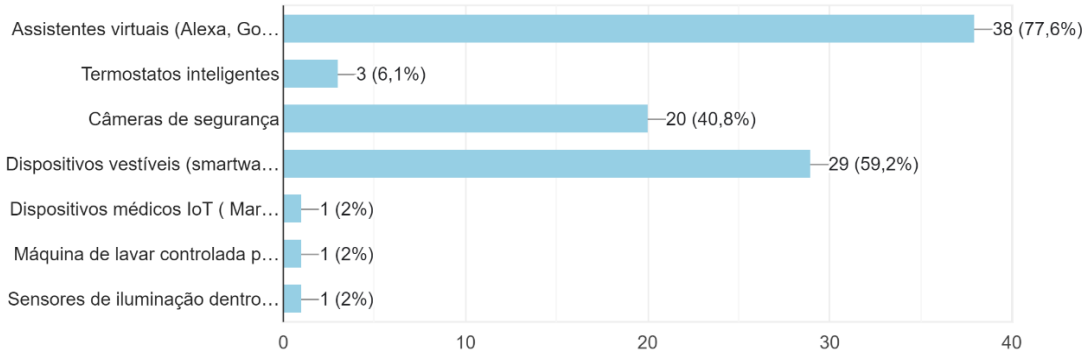
19 respostas



Apêndice D – Das pessoas que utilizam

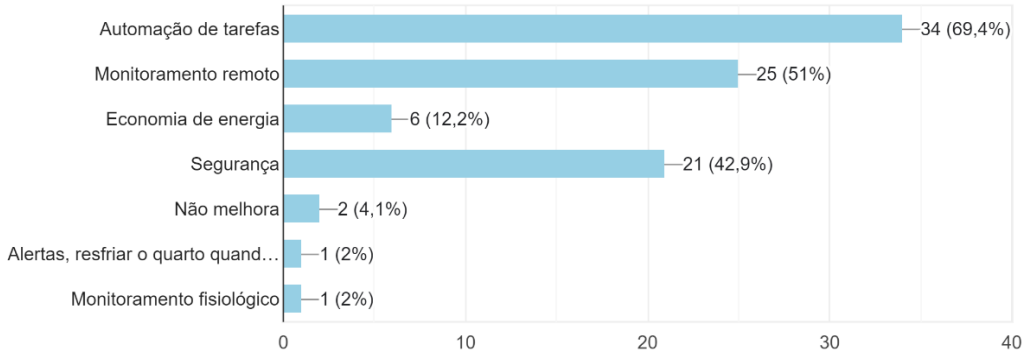
Quais dispositivos IoT você utiliza?

49 respostas



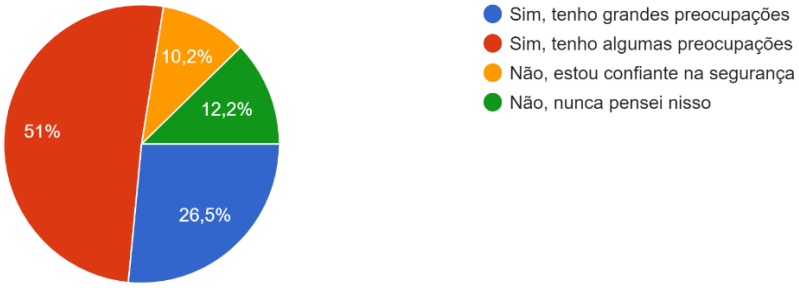
Como a IoT tem melhorado sua vida diária ou processos de trabalho?

49 respostas



Você tem preocupações com a segurança e privacidade dos dados coletados por dispositivos IoT?

49 respostas



Você tem conhecimento de alguma medida de segurança para os dados coletados por dispositivos IoT? Se sim, cite alguns que tenha conhecimento.

18 respostas