Ministério da Defesa
Exército Brasileiro
Escola de Saúde e Formação Complementar do Exército

1º Ten Al Bruno

1º Ten Al Maia

1º Ten Al Paiva

Análise de vulnerabilidades e ferramentas no âmbito da defesa cibernética no perímetro da Escola de Saúde e Formação Complementar do Exército

Salvador - BA
2023

1º Ten AI Bruno

1º Ten AI Maia

1º Ten AI Paiva

Análise de vulnerabilidades e ferramentas no âmbito da defesa cibernética no perímetro da Escola de Saúde e Formação Complementar do Exército

Trabalho de Conclusão de Curso apresentado à Banca Examinadora da Divisão de Ensino da Escola de Saúde e Formação Complementar do Exército, como requisito parcial para conclusão do Curso de Formação de Oficiais.

Orientador: TC QCO Informática **Arruda**

Salvador - BA
2023

Análise de vulnerabilidades e ferramentas no âmbito da defesa cibernética no perímetro da Escola de Saúde e Formação Complementar do Exército

Trabalho de Conclusão de Curso apresentado à Banca Examinadora da Divisão de Ensino da Escola de Saúde e Formação Complementar do Exército, como requisito parcial para conclusão do Curso de Formação de Oficiais.

Aprovado em: _____/_____/2023

_____
NOME-POSTO-PRESIDENTE

_____
NOME-POSTO-1ºMEMBRO

_____
NOME-POSTO-2ºMEMBRO

_____
NOME-POSTO-3ºMEMBRO

_____
TC **Arruda** – Orientador
ESCOLA DE SAÚDE E FORMAÇÃO COMPLEMENTAR DO EXÉRCITO

Agradecimentos

Primeiramente a Deus, por seu imensurável amor e justiça que nos momentos de nossas fraquezas e indecisões nos deu força além do natural para prosseguir.

Aos nossos parentes, pelos valores éticos e morais que nos foram ensinados, pelo carinho e compreensão incomparáveis e por nunca desistirem de nós.

Ao nosso orientador, TC Arruda, pois além de nos orientar e contribuir na realização deste trabalho, esteve empenhado em passar seus conhecimentos sobre o uso e importância da informática dentro da caserna.

Aos nossos instrutores do Curso de Formação de Oficiais, que demonstraram estar comprometidos com a qualidade e excelência do ensino.

Aos nossos amigos que nos motivaram em nossos momentos mais difíceis.

Aos nossos colegas de turma, pelo companheirismo e amizade.

A todos que participaram da pesquisa, pelo interesse, disponibilidade e colaboração.

RESUMO

Os *Malwares* são uma grande preocupação para todas as organizações militares, com o advento cada vez maior de processos digitalizados é de suma importância que se desenvolva uma política de mitigação. Esse objetivo pode ser atingido de várias maneiras. Isso passa pela conscientização dos usuários, gestão estratégica do alto comando da organização militar, passando até a área especializada da TI, setor responsável por direcionar a melhor maneira de fazê-lo. Há atualmente no mercado ferramentas capazes de identificar e tratar as ameaças impostas pelos *malwares* porém a necessidade de uma gestão eficiente é capaz de, por si só, mitigar parte dessas ameaças. No contexto da divisão de tecnologia da informação da Escola de Saúde e Formação Complementar do Exército (ESFCEX) destacou-se as principais vulnerabilidades encontradas no parque computacional. As vulnerabilidades destacadas no trabalho não são críticas, de forma que não representam risco imediato às informações e aos dispositivos presentes no perímetro interno. Porém a necessidade de correção ainda é pertinente e o atual trabalho apresenta ferramentas e técnicas capazes de corrigir tais problemas.

Palavras-chave: Malwares, processos digitalizados, vulnerabilidades, cibersegurança, infraestrutura de ti.

Abstract

Malwares are a major concern for all military organizations with the increasing advent of digitized processes it is of paramount importance to develop a mitigation policy. This objective can be achieved in several ways. This goes from user awareness, strategic management of the military organization's high command to the specialized area of IT, the sector responsible for directing the best way to do so. There are currently on the market tools capable of identifying and treating the threats posed by malware, but the need for efficient management is capable of mitigating part of these threats by itself. In the context of the ESFCEX information technology division, the main vulnerabilities found in the computational park were highlighted. The vulnerabilities highlighted in the work are not critical, so they do not pose an immediate risk to the information and devices present in the internal perimeter. However, the need for correction is still relevant and the current work presents tools and techniques capable of correcting such problems.

keywords: Malwares, digitized processes, vulnerabilities, cybersecurity, IT infrastructure.

Sumário

1. INTRODUÇÃO **8**
1.1 Objetivo Geral 10
1.2 Objetivos Específicos 10
1.3 Metodologia 10
2. DESENVOLVIMENTO **11**
2.1 Trabalhos Relacionados 11
2.2 Descrição do Dados 13
2.2 Tipos de Malware 14
2.3 Discussão 16
2.3.1 Pontos de Vulnerabilidades 16
2.3.1.1 Sistemas Operacionais Desatualizados 16
2.3.1.1.1 Puppet 18
2.3.1.1.2 Ansible 19
2.3.1.1.3 Puppet x Ansible 19
2.3.1.2 Computadores de uso público 20
2.3.1.3 Samba Server 20
2.3.1.4 Proteção de portas USB 21
2.3.2 Comparação entre a infraestrutura informática da ESFCEX e as outras organizações militares 22
3. CONSIDERAÇÕES FINAIS **24**
4. REFERÊNCIAS **25**
APÊNDICE A **31**
APÊNDICE B **33**
ANEXO A **34**
ANEXO B **36**

1. INTRODUÇÃO

A área de segurança cibernética evoluiu consideravelmente nas últimas décadas e continua evoluindo. Fato esse decorrente do crescimento no número de sistemas e da consequente dependência que esses vêm proporcionando no ecossistema de rede (STALLINGS, 2015). O risco associado a esses sistemas é proporcional ao número de aplicações construídas sobre eles, isso pode ser observado por meio do aumento no número de vazamentos de dados registrados (VEIRANO ADVOGADOS, 2021).

A segurança cibernética está diretamente ligada com o conceito de segurança da informação. O glossário de segurança da informação do Gabinete de Segurança Institucional o define como: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações (BRASIL, 2019).

A disponibilidade, a integridade e a confidencialidade, também conhecidas como os pilares da segurança da informação, são constantemente alvo de desenvolvedores de programas maliciosos que visam a obtenção de lucros. Esses desenvolvedores maliciosos se aproveitam da introdução da tecnologia e das redes de dados em quase todos os aspectos da sociedade para fazerem suas vítimas.

O meio militar não está imune à expansão da tecnologia, muito pelo contrário, tendo em vista ser um dos setores mais tecnológicos e que investe pesadamente em inovações e em pesquisa e desenvolvimento (SANDERS, JANG, HOLDERNESS, 2022).

A integração militar com a tecnologia, seja no âmbito material seja no cibernético, tornou as organizações militares alvos de ataques cibernéticos e, ao mesmo tempo, atacantes de outras organizações. Esse efeito originou o termo guerra cibernética.

A guerra cibernética refere-se ao uso de tecnologias de informação e comunicação (TIC) com aplicações militares e estratégicas. Neste tipo de guerra, os conflitos se desenvolvem principalmente no ciberespaço, que inclui redes de computadores, sistemas informáticos, dispositivos conectados à Internet e outras infraestruturas digitais. Os objetivos da guerra cibernética podem variar desde a espionagem e a coleta de informações até a sabotagem, a destruição ou a interrupção de infraestruturas críticas. Vide o conflito entre Rússia e Ucrânia em que o primeiro ataque foi cibernético (MCGEE-ABE, 2023).

Dessa forma, o ambiente cibernético de uma organização militar de um país cada dia mais se torna um alvo majoritário, seja para um governo seja para um cibercriminoso independente. Consequentemente, a proteção desse ambiente se torna uma questão de defesa nacional. Parte dessa proteção reside na identificação e proteção contra *malwares*.

Um *malware* pode ser definido como um programa que é inserido em um sistema, usualmente às escondidas, com a intenção de comprometer a confidencialidade, a integridade ou a disponibilidade dos dados, aplicações ou sistema operacional da vítima ou, possivelmente, apenas aborrecê-la ou perturbá-la (STALLINGS, 2015).

O entendimento acerca dos *malwares* é vital para a consolidação de uma defesa eficaz. E é nesse contexto que o governo brasileiro, em sua política nacional de defesa, visa o ambiente cibernético como um setor estratégico a ser protegido (BRASIL, 2022).

O Exército Brasileiro desempenha um papel central nessa política por meio do foco dado à segurança de suas informações, seja no nível mais alto da cadeia institucional, seja nas organizações mais abaixo nessa cadeia. Isso é importante uma vez que essas organizações podem ser exploradas a se tornar uma porta de entrada a indivíduos mal intencionados que visam comprometer o ambiente cibernético da força terrestre.

Inserida nesse contexto pode-se verificar a Escola de Saúde e Formação Complementar do Exército (ESFCEX). Para tal, a estrutura de defesa cibernética da escola deve estar condizente com os requisitos demandados pelos escalões mais altos. Dessa forma a situação do ambiente de informática deve ser periodicamente avaliada a fim de observar a adequação aos novos requisitos administrativos e técnicos.

É nessa problemática que o presente trabalho se insere, objetivando analisar a situação da ESFCEX no âmbito da informática a fim de averiguar a adequação aos objetivos de proteção da informação, sugerir pontos de melhoria e a situação das áreas de *software*, *hardware* e *peopleware* em busca de pontos sensíveis quanto à segurança. Dessa forma, visando agregar mais capacidades à segurança cibernética da organização ao criar um ambiente mais resiliente.

1.1 Objetivo Geral

Promover uma pesquisa exploratória capaz de elencar pontos de melhorias na prevenção contra *malwares* na infraestrutura de TIC da Escola de Saúde e Formação Complementar do Exército.

1.2 Objetivos Específicos

- Descrever o mecanismo de operação dos principais tipos de *malwares*;
- Identificar pontos de vulnerabilidade presentes na infraestrutura de TIC e no parque computacional da ESFCEX;
- Propor soluções aos pontos identificados como vulnerabilidades;

1.3 Metodologia

O desenvolvimento do trabalho em questão procedeu através da aplicação de uma metodologia exploratória. Ela teve como foco o ambiente de segurança cibernética implementado na Escola de Saúde e Formação Complementar do Exército (ESFCEX) e buscou encontrar possíveis vulnerabilidades no parque computacional.

Foi desenvolvido um questionário a fim de guiar uma entrevista com os chefes da seção de sistemas e de redes da Divisão de Tecnologia da Informação.

Esse questionário foi estruturado com o intuito de levantar informações e desenvolver uma visão geral da infraestrutura de TIC, desde o acesso físico ao *Datacenter*, a rede em que transitam os dados, os programas instalados nos computadores presentes na instituição e os seus usuários, ou seja, o *peopleware*.

De posse das respostas obtidas durante a entrevista buscou-se detalhar os pontos que foram visualizados como vulnerabilidades. Esses pontos foram explorados a fim de caracterizá-los ou não como pontos de melhoria, caso positivo, foi proposto possíveis ferramentas capazes de melhorar esse ponto.

Tais melhorias observadas visam a segurança cibernética da unidade, não limitada apenas aos *hardwares* ou *softwares*, mas também ao *peopleware* existente na organização.

A escolha de tais elementos, possíveis novos componentes da estrutura cibernética, foram escolhidos mediante pesquisa em sites especializados, livros ou através das consultas realizadas no Departamento de Tecnologia da Informação (DTI) da ESFCEX.

Foi desenvolvido um questionário tendo como público os profissionais de informática do exército brasileiro para possibilitar a comparação entre a situação da TI na ESFCEX e a situação geral das outras Organizações Militares em que atuam esses militares.

Essa comparação busca observar se a situação da ESFCEX está condizente com as outras organizações e destacar os pontos estão divergentes.

2. DESENVOLVIMENTO

A criticidade da segurança da informação é uma problemática inerente à computação, datando desde aquele que muitos consideram como sendo o primeiro vírus, o *Creeper* (KASPERSKY, 2019), até os dias atuais em que a segurança dos sistemas demanda defesas tipicamente militares.

A importância desse tema propicia grande variedade de trabalhos acadêmicos e publicações. A subseção a seguir cita trabalhos que embasam o desenvolvimento da pesquisa realizada. Nas seções seguintes são apresentadas as vulnerabilidades encontradas e as consequentes discussões acerca das soluções que podem ser empregadas para sanar essas ocorrências.

2.1 Trabalhos Relacionados

Sacramento (2018) propõe uma revisão da literatura tendo em vista a problemática da segurança de borda, tendo organizações militares da arma de comunicações como foco de estudo. Para tal, ele investiga a utilização do *firewall* de código aberto PFSense, suas conclusões observam a falta de conhecimento para a devida aplicação do *software* para o endurecimento das defesas das organizações, retratando a deficiência do *peopleware*.

Santos (2021) cita a aplicação e a interpretação que se tem da segurança cibernética no âmbito do Exército Brasileiro e nas forças armadas de outras nacionalidades. Para tal investiga-se os planos e a visão que o Exército Brasileiro tem da segurança cibernética, a importância dada à atual conjuntura da tecnologia e do combate na atualidade. Similarmente, Avelar (2018) explora a aplicação da segurança cibernética no Exército Brasileiro e na sociedade civil, o autor destaca a cooperação entre todos os ramos das Forças Armadas para se obter um ambiente de defesa cibernética mais eficiente.

A importância do estudo da segurança da informação é tal que Pereira (2019) investiga a possibilidade de se introduzir seu estudo durante a formação do oficial de carreira da arma de Comunicações do Exército Brasileiro.

A quantidade de ameaças existentes é bem explorada por Li, Rios e Trajković (2020), tendo em vista que conhecer cada uma dessas ameaças é imprescindível no momento de criar barreiras para proteger as informações de uma organização.

Uma vertente que vale ressaltar, visa classificar *malwares* por meio da análise de suas assinaturas, ou seja, analisar um arquivo e determinar se o seu conteúdo ou comportamento são maliciosos, para tal são empregadas técnicas de aprendizagem de máquina como em: Abusitta, Li e Fung (2021); Kalash et al. (2018); e Vasan (2020).

Outra vertente visa detectar *malwares*, a fim de proteger os dispositivos, tendo em vista a disseminação da computação, Wani (2020) e Aslan (2020) exploram as abordagens presentes na literatura a fim de proteger dispositivos vulneráveis.

A detecção dessas ameaças podem ser classificadas quanto à abordagem empregada. Saleh (2023) as observa em três tipos: estáticas, dinâmicas e híbridas. As estáticas não executam o *software*, já as dinâmicas o executa em um ambiente controlado, as híbridas se valem dos dois métodos.

Uma observação pertinente quanto à proteção de dispositivos e consequente infraestrutura pode ser visualizada em Telen, Abamonga e Chua (2020). Os autores observam que a vulnerabilidade da infraestrutura analisada é fruto de uma série de fatores, que vão desde capital humano deficiente, até a inadequação da infraestrutura empregada. Essa observação é crucial para entender a necessidade de se investir em *software*, *peopleware*, *hardware*.

Uma dessas áreas, o *peopleware*, é justamente alvo de análise de Hamoud e Aïmeur (2020). Em seu trabalho os autores investigam a tática de explorar a vulnerabilidade do lado do usuário, justamente o *peopleware*. A conclusão do *peopleware* ser uma grande vulnerabilidade do ecossistema de segurança também é discutido por Ghafir (2018).

Vishwanath et al (2011), buscam justamente entender os motivos pelos quais o usuários continuam a ser vítimas de *phishing*, culminando na racionalização de que as vítimas tendem a buscar atalhos mentais e fazer inferências rápidas e, dessa forma, deixam qualquer sistema de segurança vulnerável, não importando o capital humano ou monetário investido nesses ambientes.

Tanenbaum e Bos (2014) explicam a facilidade da disseminação de *malwares* por conta de dois fatores: 90% da população executar um mesmo sistema operacional (Windows); e o fato da *Microsoft* optar por facilidade de uso em detrimento à segurança.

Esse segundo ponto corrobora com Sasse (2022), que aponta para o fato da consciência de segurança inerente ao usuário é apenas o primeiro passo para a criação de um ambiente seguro. Esse ambiente deve ter a participação das organizações de forma a acompanhar de perto o crescimento da consciência dos colaboradores.

A criação desse ambiente passa pelos administradores da infraestrutura uma vez que devem manter as condições de segurança ambiente. Investigando a manutenção que é dada à atualização dos programas, Bormanieri (2017) observou a priorização, nas empresas de capital mais limitado, das operações em detrimento da atualização dos sistemas.

Isso se relaciona diretamente com as condições de segurança uma vez que está diretamente relacionada com a atualização dos sistemas que são utilizados na empresa.

2.2 Descrição do Dados

O presente trabalho buscou coletar dados através de questionários a fim de embasar as observações realizadas. Um questionário visou o departamento de TI da própria Escola de Saúde e Formação Complementar do Exército (ESFCEX), além de informações acerca do parque computacional, e o outro os profissionais de TI no âmbito do Exército.

O levantamento no âmbito da ESFCEX produziu observações da infraestrutura e informações dos sistemas operacionais das estações de trabalho. Esse levantamento utilizou a ferramenta *fusion inventory* para extrair o estado dos sistemas operacionais, porém alguns desses dados contém ruído proveniente decorrente do padrão de nomes no momento da configuração da máquina.

A pesquisa que objetivou levantar informações fora do espaço da ESFCEX buscou investigar algumas situações de outras organizações militares, paral tal foi confeccionado um questionário que foi disponibilizado aos profissionais de TI do Exército Brasileiro.

Um sumário dos dados obtidos estão disponíveis no Anexo A e B, as questões propostas estão disponíveis nos Apêndices A e B.

2.2 Tipos de Malware

Um *malware* nada mais é que um programa que é desenvolvido para prejudicar outro usuário, seja visando ganhos econômicos ou simplesmente prejudicar o sistema de outrem.

A existência desses programas é tamanha que a Akamai, empresa de soluções em tecnologia, alega processar 454 TB de dados de novos ataques cibernéticos todos os dias.

Muitos desses ataques são erradamente, tendo em vista a generalidade, imputados aos vírus, porém existe uma variedade maior de mecanismos por trás desses ataques.

Esses vírus, genericamente tratado como nome da classe de ameaças que no caso seria o *malware*, é um tipo de *software* que pode "infectar" outros programas ou até mesmo qualquer tipo de conteúdo executável, modificando-os. A modificação inclui injetar no código original uma rotina para fazer cópias do código do vírus, que então podem continuar a se propagar e infectar outro conteúdo (STALLINGS, 2015).

Um vírus que se liga a um programa executável pode fazer qualquer coisa que o programa tenha permissão de fazer. Ele executa secretamente quando o programa hospedeiro é executado. O vírus pode reproduzir-se anexando o seu código a outro programa, de maneira análoga à reprodução dos vírus biológicos. Assim como esses, podem ficar dormentes esperando um estímulo externo do programador criador. Dessa forma são capazes de infectar outros computadores através do compartilhamento de arquivos ou programas. A porta de entrada para esses programas é o próprio usuário que dá acesso ao seu sistema no momento que instala e executa programas não-licenciados infectados (TANENBAUM; BOS, 2014).

Outra variedade de *malware*, cujo comportamento se assemelha aos vírus são os *worms*. Os *worms* são programas autônomos que se auto-replicam e se propagam através de redes, sem necessidade de um arquivo hospedeiro, podendo trazer consigo outro *malware* como carga útil (LI; RIOS; TRAJKOVIĆ, 2020).

Ainda no âmbito de *software* malicioso que traz consigo uma carga mal intencionada, destacam-se os cavalos de Tróia. Esse tipo de *malware* é composto por programas que parecem ser legítimos, algumas vezes são versões pirateadas, mas trazem consigo código malicioso oculto. Dessa forma, roubam-se informações, fornecem acesso não autorizado aos atacantes ou abrem portas em seu sistema para livre acesso desses (LI; RIOS; TRAJKOVIĆ, 2020).

Grande parte desses *softwares* visam roubar dados que podem ser convertidos em valores reais, vide o tipo de ataque por *Ransomware*. Este tipo de *malware* cifra os arquivos no sistema da vítima e exige um resgate (quantias monetárias, frequentemente criptomoedas) para recuperá-los. Estes ataques podem causar perda de dados e interrupção nas operações, tendo em vista a disseminação lateral através da organização e a capacidade de atingir todas as estações de uma organização (KIMHY, KUPCHIK, 2022). Os *ransomwares* ganharam notoriedade após os famosos ataques do WannaCry em 2015. Esse ataque se espalhou por mais de 150 países (LIPTAK, 2017), levando a elevados danos financeiros (KIMHY, KUPCHIK, 2022).

Os *ransomwares* geralmente são instalados nos sistemas sem o conhecimento do usuário e assim como os *spywares,* que coletam informações confidenciais, como senhas, dados financeiros e hábitos de navegação, para enviá-los a terceiros mal intencionados (LI; RIOS; TRAJKOVIĆ, 2020).

Já os *keyloggers* registram todas as teclas que são pressionadas pelo usuário durante o uso de seu dispositivo e periodicamente as envia para alguma máquina, permitindo aos atacantes obter informações confidenciais, como senhas e dados pessoais após analisar o que foi coletado (TANENBAUM; BOS, 2014).

O *adware*, é um tipo de *malware,* que pode mostrar anúncios não desejados, coletar seus dados, impactar o desempenho do sistema, dificultar o uso do dispositivo ou pichar sua navegação uma vez que podem exibir imagens de cunho sexual (KASPERSKY, 2018).

Um grande vilão dos *malwares*, tendo em vista sua impregnação nos sistemas, os *rootkits* visam ocultar a presença de um outro *malware* por meio da alteração do sistema operacional e suas funções básicas a fim de permitir que os atacantes tenham acesso remoto e permaneçam infiltrados no sistema sem serem detectados. Os *rootkits* podem ser instalados por meio de vírus, *worms* e *spywares*. Uma vez instalado na máquina é dificilmente detectável, uma vez que o *hardware*, o sistema operacional, as bibliotecas e as aplicações deixam de ser confiáveis. O usuário final fica totalmente à mercê dos invasores. Os *rootkits* assim como outros *malwares* podem instalar uma “porta dos fundos” na máquina, possibilitando que a máquina seja controlada remotamente como uma espécie de zumbi. (LI; RIOS; TRAJKOVIĆ, 2020; TANENBAUM; BOS, 2014).

A coleção de zumbis, ou seja, várias máquinas controladas remotamente, é chamada de uma *botnet*. Essa rede (*botnet*) visa exercer atividades maliciosas, como ataques distribuídos de negação de serviço (DDoS, *Distributed Denial of Service*) ou roubo de dados (STALLINGS, 2015; TANENBAUM; BOS, 2014).

O ataque de negação de serviço (DDoS) acontece quando múltiplos dispositivos são utilizados em sincronia visando um acesso simultâneo a fim de requisitar os recursos de processamento e conectividade de uma só vez à máquina responsável por prover os conteúdos aos dispositivos requisitantes. Dessa forma o serviço se torna indisponível aos usuários que de fato necessitam do recurso (MITTAL; KUMAR; BEHAL, 2023).

2.3 Discussão

Por intermédio do instrumento de coleta de dados do Apêndice A, foram elencados no ambiente computacional da Escola de Saúde e Formação Complementar do Exército (ESFCEX), os pontos vulneráveis que podem ser explorados por meio de ataques cibernéticos. Além disso, essas potenciais “brechas” foram analisadas à luz dos trabalhos relacionados, sendo sugeridas ferramentas e boas práticas para mitigação de incidentes.

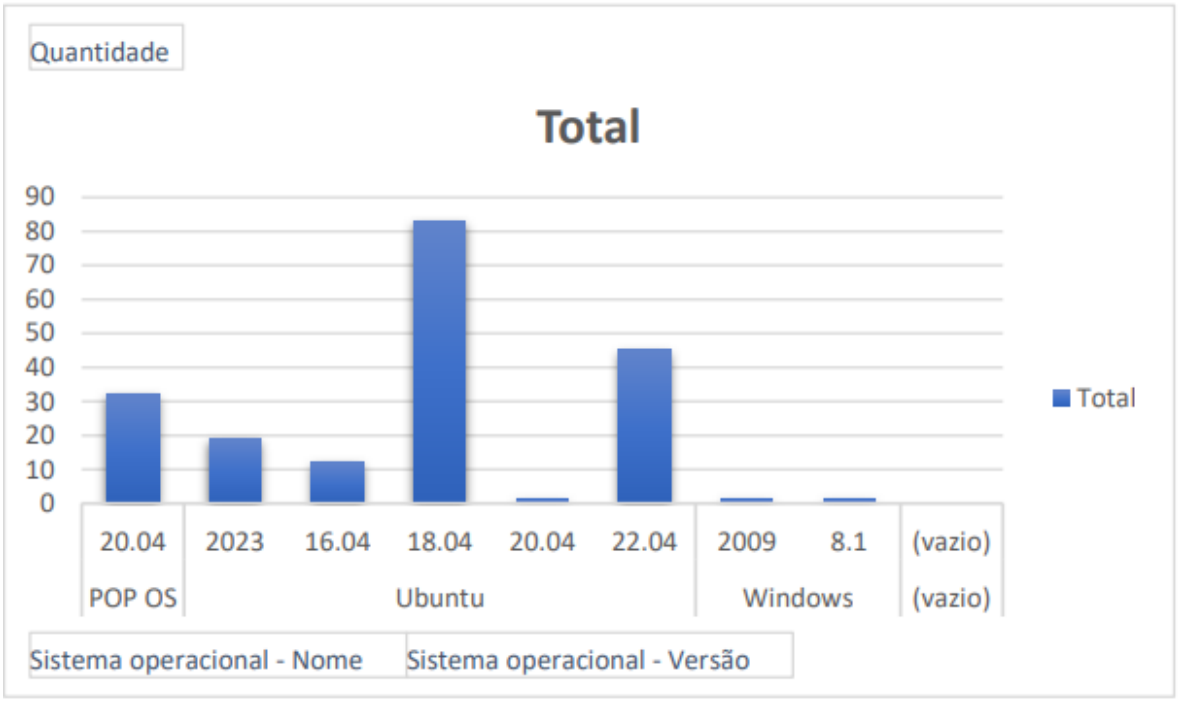
2.3.1 Pontos de Vulnerabilidades

Através das observações realizadas no parque computacional da ESFCEX foram elencados pontos vulneráveis que podem ser explorados por meio de ataques cibernéticos. Dessa forma, esses foram destacados como pontos de melhoria para a instituição e suas respectivas possíveis soluções.

2.3.1.1 Sistemas Operacionais Desatualizados

Foi observado a existência de dois tipos de sistemas operacionais no parque computacional, sendo distribuições Linux Ubuntu e Windows. Isso ocorre devido ao estímulo pelo uso de *software* livre em consonância com o Comando do Exército (BRASIL, 2013), no caso do uso de sistemas operacionais baseados em Linux. Porém em situações específicas, como o uso de ferramentas de edição de imagem e vídeo, o sistema operacional Windows se faz necessário. A Figura 1 apresenta a distribuição dos sistemas operacionais presentes no parque computacional.

Figura 1 - sistemas operacionais presentes no parque computacional da Escola de Saúde e Formação Complementar do Exército



Fonte: os autores.

A presença de um parque computacional com um considerável número de máquinas exibiu uma deficiência, a presença de versões desatualizadas dos sistemas operacionais. Isso impõe uma séria ameaça, uma vez que as atualizações provêm correções de falhas observadas nas versões anteriores (CASAGRANDE; BOAS; AQUINO, 2022).

Vale destacar que a atualização de *softwares* desatualizados não se aplica somente a sistemas operacionais, mas também para *softwares* de uso cotidiano, como navegadores, escritores de texto e etc.

A utilização de uma ferramenta para levantar o inventário de sistemas operacionais e *softwares* de uso geral se faz necessário, bem como a utilização de mecanismos para atualizá-los remotamente. Similarmente ao sugerido por Bormanieri (2018) que propôs a adoção de ferramentas que contemplem o gerenciamento de todos os sistemas operacionais utilizados no ambiente. As conclusões obtidas por Bormanieri (2018) são visíveis dentro do ambiente da Escola de Saúde e Formação Complementar do Exército (ESFCEX), uma vez que a atualização dos sistemas é colocada em segundo plano tendo em vista as operações diárias exigidas do Departamento de TI.

No contexto de gestão de atualizações de sistemas sugere-se duas ferramentas para análise: o Puppet e o Ansible.

2.3.1.1.1 Puppet

Puppet é uma ferramenta que visa o gerenciamento e a automatização da configuração de servidores e computadores clientes. A ideia central por trás do Puppet é ter a configuração centralizada, sendo essa configuração distribuída para diversos nós de uma rede.

Ao usar o Puppet, define-se o estado desejado dos sistemas na infraestrutura que se deseja gerenciar. Para tal escreve-se o código da infraestrutura na linguagem específica de domínio (DSL) do Puppet — código Puppet — que pode ser usado com uma ampla variedade de dispositivos e sistemas operacionais.

O código Puppet é declarativo, o que se traduz na descrição do estado desejado de seus sistemas, não nas etapas necessárias. O Puppet por sua vez automatiza o processo de colocar esses sistemas nesse estado. A ferramenta faz isso por meio de um servidor primário e de um agente. O servidor primário armazena o código definidor do estado desejado. Já o agente traduz seu código em comandos e, em seguida, o executa nos sistemas especificados. Isso é chamado de execução do Puppet. (PUPPET, documentação)

Quanto ao seu funcionamento, o Puppet geralmente é utilizado no modelo cliente/servidor. Normalmente, os clientes são chamados de nós (computadores de usuários, servidores físicos, dispositivos clientes, máquinas virtuais) e o servidor central de mestre. A execução do Puppet segue os seguintes passos:

- Coleção de fatos: os nós possuem um agente instalado que permanece em execução e se conecta ao servidor central periodicamente, geralmente de 30 em 30 minutos. O agente envia informações ao servidor central sobre as configurações do nó, como tempo de atividade, sistema operacional, endereço IP, versões dos pacotes, entre outras;
- Catalog Compilation: o “puppet mestre” usa a coleção de fatos fornecida pelo agente para compilar as informações sobre como cada nó deve ser configurado. Essas informações compiladas são chamadas de “catálogo”. O catálogo é um documento que informa o estado desejado para cada recurso de um nó. O *puppet* mestre envia o catálogo para o agente;

- Relatório: cada agente envia um relatório ao *puppet* mestre, indicando todas as alterações que foram efetivadas, havendo divergências ou não;

- Execução: o agente aplica o catálogo sobre os nós;

Existe a possibilidade de executar o puppet sem a presença de um agente nos nós. Nesse cenário, a aplicação do catálogo é agendada na *crontab* ou disparada via *Mcollective*. A codificação do ambiente na linguagem Puppet geralmente é armazenada em um controle de versão, como o GIT (Techente, 2019).

2.3.1.1.2 Ansible

O Ansible é um mecanismo de automação de TI *open source* para automação de processos como provisionamento, gerenciamento de configurações, implantação de aplicações, orquestração etc.

A ferramenta se conecta aos seus nós e envia a eles pequenos programas chamados módulos. Os módulos são usados para realizar tarefas de automação no Ansible. Esses programas são projetados para serem modelos de recursos do estado desejado do sistema.

Em seguida, o Ansible executa esses módulos e os remove ao finalizar. Essa aplicação é uma ferramenta sem agentes, ou seja, não requer instalação de *software* para gerenciar os nós. Ele acessa seu inventário e lê as informações sobre quais máquinas deseja gerenciar.

O Ansible tem um arquivo de inventário padrão, mas é possível criar um arquivo próprio e definir quais servidores se deseja gerenciar. Ele usa o protocolo SSH para se conectar aos servidores e executar as tarefas. Por padrão, o Ansible usa chaves SSH com o ssh-agent e seu nome de usuário atual para se conectar a máquinas remotas. (REDHAT, 2022).

2.3.1.1.3 Puppet x Ansible

Ambas as ferramentas são bastante poderosas para lidar com o problema do controle de versão dos sistemas operacionais desatualizados e dos próprios sistemas do parque computacional da ESFCEX. O Puppet sendo mais completo e complexo, tendo uma linguagem própria e que necessitaria maior tempo para aprender a manuseá-lo, já Ansible sendo mais simples e rápido de utilizar e colocar em produção.

2.3.1.2 Computadores de uso público

Computadores de uso público se destinam a permitir um controle mais livre de usuários que não são necessariamente membros da organização, tais como palestrantes e visitantes em geral. Porém é terminantemente desaconselhado que esses usuários momentâneos tenham acesso à máquinas com capacidades de administrador.

Uma máquina com acesso de administrador é capaz de desabilitar o *firewall*, modificar configurações de segurança e apagar dados. Tudo isso sem necessitar invadir o perímetro de segurança da organização uma vez que ele já está dentro desse perímetro. A divisão de tecnologia da informação fica sem controle de quais programas são instalados naquele computador, pois subentende-se que é um dos administradores do sistema que o está utilizando. O que não é necessariamente verdade. Esse fato cria uma vulnerabilidade no sistema de defesa da organização.

Como possível correção, sugere-se o rebaixamento dessas máquinas públicas a um nível de utilizador comum, com permissões limitadas, de forma que a DTI tenha mais controle quanto à instalação e uso dessa máquina.

A presença de máquinas com esse nível de permissão se correlaciona diretamente com o apontado por Telen, Abamonga e Chua (2020), uma vez que a vulnerabilidade do usuário com acesso de administrador pode ser foco de ataques.

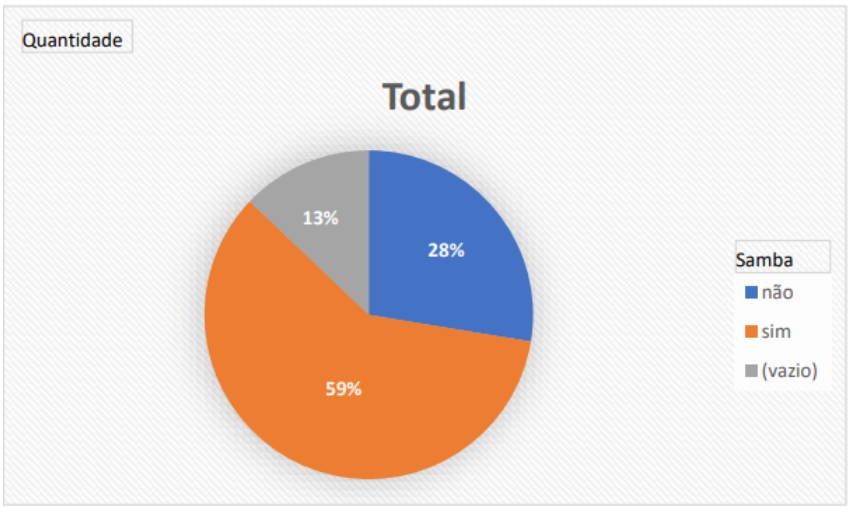
2.3.1.3 Samba Server

Alguns ambientes de rede utilizam sistemas baseados em Linux e em Windows que necessitam operar em conjunto. O Samba, segundo o material de referência da canonical, provê ferramentas para configurar o compartilhamento com clientes baseados em Windows, tais como:

- Server Message Block (SMB) para arquivos, pastas e volumes;
- Lightweight Directory Access Protocol (LDAP) e Microsoft Active Directory para compartilhar informações acerca dos computadores e usuários de rede;
- Autenticação e Acesso para determinar qual nível de acesso um determinado usuário possui;

A questão central do Samba ser aqui elencado como uma vulnerabilidade é oriunda do fato de ser um serviço com vulnerabilidades conhecidas, vide o CVE do samba, porém não está sendo utilizado. Por meio da Figura 2 é possível observar a grande quantidade de estações de trabalho com esse recurso ativado, ou seja, vulneráveis.

Figura 2 - divisão de computadores com o Samba Server ativado. (sim , Samba ainda ativo; não, desativado)



Fonte: os autores.

Essa característica é desestimulada entre os administradores de infraestrutura tendo em vista o risco que isso traz ao ambiente, principalmente por ser um risco desnecessário. A criticidade desse risco pode ser elucidado através do trabalho relacionado realizado por Liptak (2017), Kimhy e Kupchik (2022).

Entre esses mesmos administradores é difundido o conceito de prover apenas aquilo que está de fato sendo utilizado pelos usuário, ou seja, manter apenas o necessário.

A fim de contornar essa vulnerabilidade sugere-se a desativação desse recurso nas máquinas que não o utilizam.

2.3.1.4 Proteção de portas USB

A proteção contra ataques cibernéticos passa pela criação de um perímetro cibernético para manter a informação dentro da organização, porém medidas para controlar usuários de dentro da própria organização também são necessárias.

Esse controle é necessário pois os indivíduos que possuem acesso interno são aqueles que possuem autorização para ultrapassar o perímetro de segurança imposto pela organização, ou seja, esses colaboradores podem ser ameaças internas à informação e aos sistemas.

O controle das portas USB quanto à presença de *malwares* e quanto à cópia de arquivos é uma medida de proteção por vezes ignorada e que leva a cópias não autorizadas de documentos que por sua vez vazam através de um computador pessoal, tendo em vista que esse não dispõe do mesmo nível de proteção que a organização cujos dados foram copiados.

O mesmo se aplica ao uso de dispositivos USB removíveis infectados de forma que torna todo o arcabouço de defesa construído para proteger o ambiente de informática inútil, pois o próprio funcionário fez o trabalho de violar o perímetro para os invasores. Mamchenko e Sabanov (2020) se dedicaram a explorar uma taxonomia para os ataques baseados em USB, de forma que observaram a variedade de ataques existentes. Esse trabalho corrobora com a importância de se proteger essa porta de entrada.

Dessa maneira, sugere-se que arquivos e documentos sejam tramitados somente pela rede intranet do EB, sem ter qualquer contato com o mundo externo, além disso, seja utilizada uma das seguintes formas para se evitar um ataque : a primeira é desabilitar a execução automática para mídias e dispositivos no sistema e permitir que somente usuários administradores possam autorizar o uso. Outra estratégia, mais rigorosa, é bloquear as portas USBs de todos os computadores clientes.

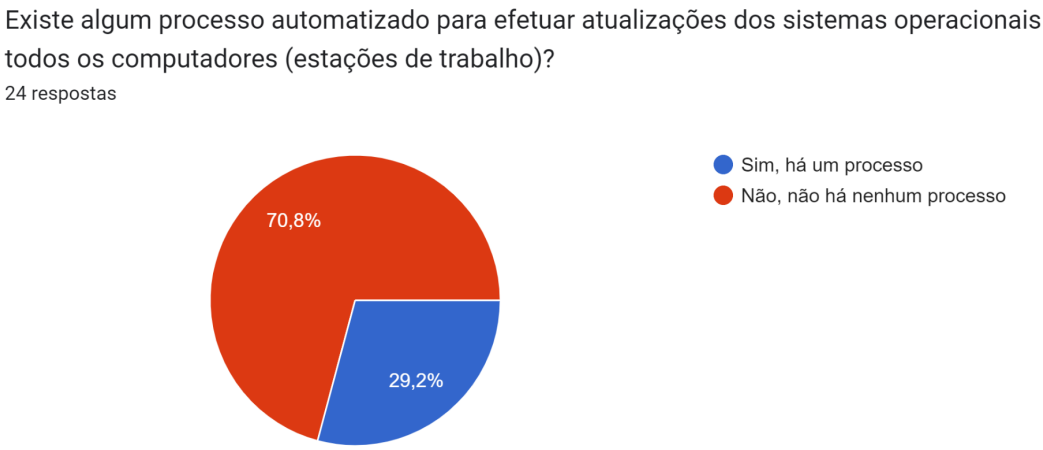
A grande maioria dos antivírus hoje em dia, possuem a função de escanear os dispositivos removíveis para verificar a existência de vírus, com isso, é importante mantê-lo atualizado contra novos *malwares* que surgirem.

2.3.2 Comparação entre a infraestrutura informática da ESFCEX e as outras organizações militares

O questionário disponibilizado aos profissionais de TI do Exército permitiu levantar informações acerca da situação de outras organizações, dessa forma foi possível comparar a atual situação da ESFCEX com a situação geral da força terrestre.

Um ponto observado durante a presente pesquisa, a inexistência de um processo automatizado para a atualização automática dos sistemas operacionais foi detectado em outras organizações. A Figura 3 corrobora com a afirmação de que as organizações, em geral, necessitam de um processo automatizado para atualizar os sistemas operacionais das estações dos respectivos parques computacionais.

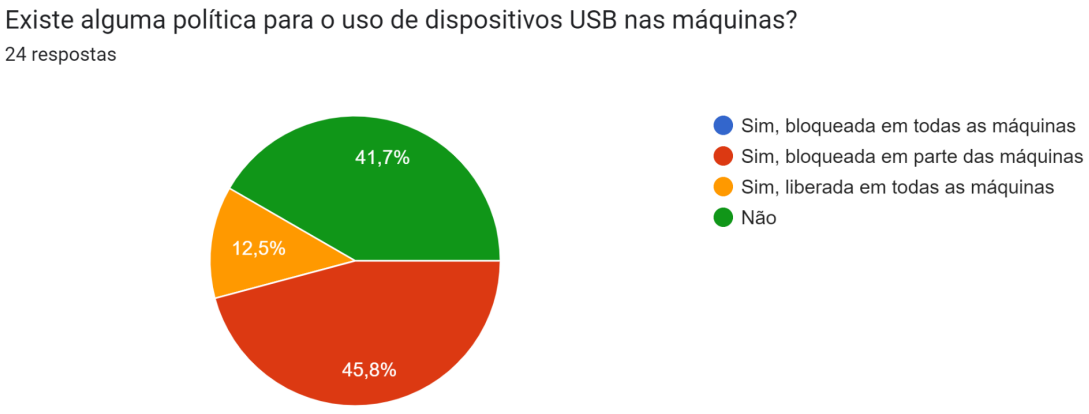
Figura 3 - divisão das respostas referentes à pergunta 12



Fonte: os autores.

As questões acerca da proteção das portas USB também foram confrontadas com a situação das outras organizações. A análise das respostas disponíveis na Figura 4 justificam a adoção de uma política padronizada.

Figura 4 - divisão das respostas referentes à pergunta 5

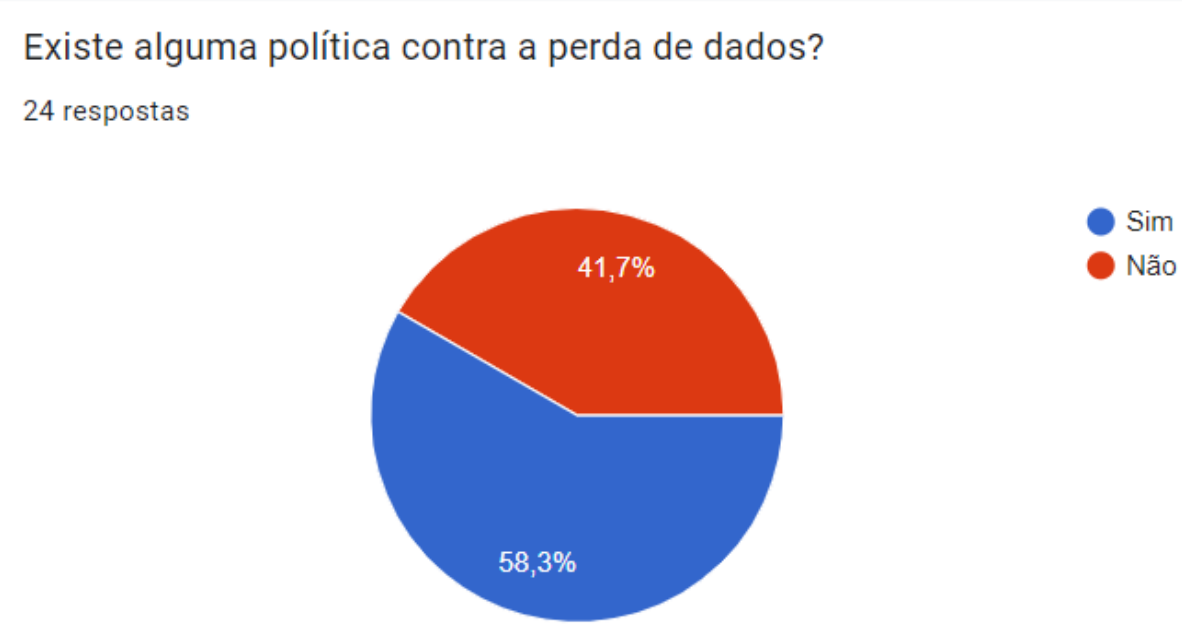


Fonte: os autores.

As formas de mitigação contra malware, tais como proteção às entradas USB, se mostram essenciais no mundo corporativo e a inexistência de qualquer política de proteção contra perda de dados não é recomendado, porém o questionário aplicado mostrou que parcela considerável das organizações não implementa nenhuma política visando a perda de dados.

Na Figura 5 é possível verificar o tamanho dessa parcela. Parcela essa que necessita endereçar essa questão por meio da adoção de uma política para prevenir a perda de dados.

Figura 9 - divisão das respostas referentes à pergunta 9



Fonte: os autores.

3. CONSIDERAÇÕES FINAIS

A área de segurança cibernética vem atraindo cada vez mais o holofote no âmbito da tecnologia da informação, isso ocorre pela importância que a informação tem em nosso cotidiano, seja pela quantidade que é gerada diariamente, seja pela incapacidade da sociedade atual viver sem essas informações as quais a define como globalizada.

As instituições governamentais não estão imunes a esse contexto e pior, se tornaram um baluarte para ataques cibernéticos, tendo em vista a quantidade de informações que processam e pelo valor monetário que essas possuem em nosso ecossistema globalizado.

A proteção dessas instituições passa por um setor de TI que deve estar constantemente preparado para agir. Porém, essa prontidão passa por constantes processos de adequação dos sistemas e equipamentos utilizados.

Inserido nesse contexto, o presente trabalho propôs uma pesquisa exploratória visando melhorias. Os pontos observados atestaram a existência de possíveis *softspots* na infraestrutura computacional da Escola de Saúde e Formação Complementar do Exército (ESFCEX) e *softwares* que podem agregar na defesa da informação, de forma que a tríade da segurança da informação (confiabilidade, integridade e autenticidade) seja preservada e sobretudo, mantida a reputação da instituição Exército Brasileiro.

O presente trabalho se limitou à detecção e análise dos pontos vulneráveis no perímetro da ESFCEX. A decisão de limitar o escopo da pesquisa foi devido ao fato deste trabalho ter um viés introdutório no que pode vir a ser uma pesquisa mais aprofundada no que tange a melhoria da infraestrutura de defesa da organização.

A presente pesquisa que visou a detecção de vulnerabilidades abre margem para trabalhos futuros tendo um escopo de maior abrangência. Contemplando a implementação e comparação entre as ferramentas sugeridas na seção 2.3.1.1 Sistemas Operacionais Desatualizados, no levantamento do nível de conhecimento dos usuários quanto ao uso da rede e consequente conhecimento da proteção da informação e por fim no aumento do nível de criteriosidade da pesquisa. Essa última visando capturar vulnerabilidades mais discretas presentes no âmbito da tecnologia da informação.

4. REFERÊNCIAS

ABUSITTA, A.; LI, M.; FUNG, B. Malware classification and composition analysis: A survey of recent developments. **Journal of Information Security and Applications**, v. 59, p. 102828, 2021.

ASLAN, Ö; SAMET, R. A comprehensive review on malware detection approaches. **IEEE access**, v. 8, p. 6249-6271, 2020.

AVELAR, J. **A guerra cibernética e seus desafios para o Brasil**, 2018.

BRASIL. Ministério da Defesa Nacional. **Estratégia nacional de defesa**. Brasília: Ministério da Defesa Nacional, 2022.

BRASIL. Gabinete de Segurança Institucional. Portaria nº 93, de 26 de setembro de 2019. Diário Oficial da República Federal do Brasil, Poder Executivo, Brasília, DF, de 1 de outubro de 2019. Edição 190, seção 1, página 3.

BRASIL. Ministério da Defesa. Secretaria Geral do Exército. Portaria nº 1.275 de 12 de dezembro de 2013. Diário Oficial da República Federativa do Brasil, Poder Executivo, Brasília, DF, 13 de dezembro de 2013. Seção 1.

BORMANIERI, J. A importância da gestão de patches e atualizações de softwares no ambiente corporativo. **Gestão da Segurança da Informação-Unisul Virtual**, 2018.

CASAGRANDE, L; BOAS, E; AQUINO, G. Systems, software, and applications updating for avoiding cyber attacks: A pentest demonstration. **XL Simpósio Brasileiro de Telecomunicações e Processamento de Sinais (SBrT2022)**, 2022.

GHAFIR, I, et al. Security threats to critical infrastructure: the human factor. **The Journal of Supercomputing**, v. 74, p. 4986-5002, 2018.

HAMOUD, A; AÏMEUR, E. Handling user-oriented cyber-attacks: STRIM, a user-based security training model. **Frontiers in Computer Science**, v. 2, p. 25, 2020.

KIMHY, E; KUPCHIK, S. Relatório de ameaças de ransomware da Akamai, 2022, **disponível em**: https://www.akamai.com/pt/resources/research-paper/akamai-ransomware-threat-report. Acesso em: 25/07/2023.

KASPERSKY, O que é um Adware?, 2018, Disponível em**:** https://www.kaspersky.com.br/resource-center/threats/adware. Acesso em: 20 de ago. de 2023.

KASPERSKY, A Brief History of Computer Viruses & What the Future Holds, 2019, Disponível em**:** https://www.kaspersky.com/resource-center/threats/a-brief-history-of-computer-viruses-and-what-the-future-holds. Acesso em: 03 de set. 2023.

KALASH M, ROCHAN M., Mohammed N., BRUCE N., WANG Y. and IQBAL F., **Malware Classification with Deep Convolutional Neural Networks**, 2018.

LI, Z; RIOS, A; TRAJKOVIĆ, L. Detecting internet worms, ransomware, and blackouts using recurrent neural networks. In: **2020 IEEE International Conference on Systems, Man, and Cybernetics (SMC)**. IEEE, 2020. p. 2165-2172.

LIPTAK, A. The WannaCry ransomware attack has spread to 150 countries. **The Verge**, v. 14, 2017.

MAMCHENKO, M.; SABANOV, A.. Exploring the taxonomy of USB-based attacks. In: **2019 Twelfth International Conference" Management of large-scale system development"(MLSD)**. IEEE, 2019. p. 1-4.

MCGEE-ABE, J. **One year on: 10 technologies used in the war in Ukraine**, 2023, disponível em: https://techinformed.com/one-year-on-10-technologies-used-in-the-war-in-ukraine/. Acesso em: 24/07/2023.

MITTAL, M; KUMAR, K; BEHAL, S. Deep learning approaches for detecting DDoS attacks: A systematic review. **Soft Computing**, v. 27, n. 18, p. 13039-13075, 2023.

PEREIRA, G. **Firewall GNU/LINUX e IPTABLES: um estudo de implementação de ensino no plano de disciplina da formação do oficial de carreira de comunicação**, 2019.

PUPPET, documentação oficial, 2023. Disponível em: https://www.puppet.com/ . Acesso em: 21 ago 2023.

REDHAT, Ansible x Puppet: o que você precisa saber, 2022, Disponível em: https://www.redhat.com/pt-br/topics/automation/ansible-vs-puppet. Acesso em: 21 ago 2023

REDHAT, Introdução ao Ansible, 2022, Disponível em: https://www.redhat.com/pt-br/topics/automation/learning-ansible-tutorial#:~:text=a%20Red%20Hat%3F-,Para%20que%20serve%20o%20Ansible%3F,aplica%C3%A7%C3%B5es%2C%20orquestra%C3%A7%C3%A3o%20e%20muitos%20outros. Acesso em: 21 ago 2023.

SASSE, M. et al. Rebooting IT Security Awareness–How Organisations Can Encourage and Sustain Secure Behaviors. In: **European Symposium on Research in Computer Security**. Cham: Springer International Publishing, 2022. p. 248-265.

SALEH, M. Malware Detection Approaches based on Operational Codes (OpCodes) of Executable Programs: A Review. **Indonesian Journal of Electrical Engineering and Informatics (IJEEI)**, v. 11, n. 2, p. 570-585, 2023.

SANDERS, G; JANG, W; HOLDERNESS, A. **Defense acquisition trends 2021**. Rowman & Littlefield, 2022.

SACRAMENTO, L. **Hardening em Linux: aperfeiçoamento da segurança do PFSense visando aumentar a segurança de borda nas organizações militares**, 2018.

SANTOS, M. **O emprego da proteção cibernética para ampliar a segurança nos postos de comando da Força Terrestre Componente**, 2021.

TELEN, M.; ABAMONGA, P.; CHUA, T. **Mitigating cyber threats to Philippine State universities and colleges: a comprehensive vulnerability assessment of University of Science and Technology of Southern Philippines-Cagayan de Oro Campus ict infrastructures**, 2023.

TANENBAUM, A.; BOS, H. **Modern Operating Systems** 4th Edition(2014).

TECHENTER, o que é Puppet ?, 2019, Disponível em: https://techenter.com.br/o-que-e-puppet/ . Acesso em 21 ago 2023.

VISHWANATH, A. et al. Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. **Decision Support Systems**, v. 51, n. 3, p. 576-586, 2011.

VASAN, D. et al. Image-Based malware classification using ensemble of CNN architectures (IMCEC). **Computers & Security**, v. 92, p. 101748, 2020.

VEIRANO ADVOGADOS, **Vazamentos de dados aumentaram 493% no Brasil, segundo pesquisa do MIT, 2021**, Disponível em: https://vocesa.abril.com.br/sociedade/vazamentos-de-dados-aumentaram-493-no-brasil-segundo-pesquisa-do-mit. Acesso em: 24 jul 2023.

STALLINGS, W. **Computer security: Principles and practice,** 2015.

WANI, A.; REVATHI, S. Ransomware protection in IoT using software defined networking. **Int. J. Electr. Comput. Eng**, v. 10, n. 3, p. 3166-3175, 2020.

APÊNDICE A

Questionário do estado do parque computacional da Escola de Saúde e Formação Complementar do Exército.

1 - A rede da instituição está segmentada?

2 - Já houve algum incidente de segurança no âmbito da escola? Caso sim, existe um histórico acerca de tal evento?

3 - A infraestrutura possui sistema de *firewall* para proteger a rede? Ele possui IPS integrado?

4 - Como está organizada a defesa dos servidores? Existe uma rede isolada para os servidores?

5 - Existe alguma organização de níveis de acesso aos usuários? Existe alguma política de acesso? Existe controle de contas dos usuários?

6 - Os usuários são orientados quanto ao uso aceitável da rede? Eles assinam um termo de uso permitido?

7 - Existe um servidor proxy? Caso sim, ele atua no nível do usuário?

8 - Os usuários são treinados e conscientizados no uso da rede?

9 - Existe alguma política contra a perda de dados?

10 - A divisão de TI implementa algum plano de continuidade dos serviços, caso algum evento adverso ocorra?

11 - A escola faz uso de algum antivírus corporativo? Há licença para todas as máquinas?

12 - Existe algum processo definido para efetuar atualizações dos sistemas operacionais de todos os computadores (servidores e estações de trabalho)?

13 - Existe algum controle de acesso físico ao *Datacenter* da instituição?

APÊNDICE B

Questionário do estado da infraestrutura de proteção cibernética das organizações militares (OM).

1 - A rede de sua OM está segmentada (rede de usuário, rede de servidores)?

2 - Já houve algum incidente de rede no âmbito de sua OM?

3 - A infraestrutura possui sistema de firewall para proteger a rede? Esse firewall possui IPS integrado?

4 - Existe alguma organização/divisão de níveis de acesso para os usuários?

5 - Existe alguma política para o uso de dispositivos USB nas máquinas?

6 - Existe controle de contas dos usuários?

7 - Os usuários assinam um termo de responsabilidade para utilização dos meios de TI?

8 - Existe um servidor proxy?

9 - Existe alguma política contra a perda de dados?

10 - A sessão de TI da sua OM implementa algum plano de continuidade dos serviços, caso algum evento adverso ocorra (disaster recover)?

11 - A sua OM faz uso de algum antivírus corporativo? Há licença para todas as máquinas?

12 - Existe algum processo automatizado para efetuar atualizações dos sistemas operacionais de todos os computadores (estações de trabalho)?

13 - Existe algum processo padronizado para a atualização dos servidores?

14 - Existe algum controle de acesso físico ao Datacenter da instituição?

15 - Qual o tipo de controle de acesso físico ao Datacenter (caso exista)?

ANEXO A

Sumarização dos resultados obtidos da situação do parque computacional da Escola de Saúde e Formação Complementar do Exército extraído por meio da ferramenta *fusion invetory.* Vale observar a existência de ruído nos dados.

Tabela 1 - Quantidade de estações com Samba Server ativado.

Samba Server ativo	Quantidade
não	45
sim	97
(vazio)	21
Total Geral	**163**

Fonte: os autores

Tabela 2 - Quantidade de estações com antivírus instalado.

Antivírus instalado	Quantidade
não	12
sim	130
(vazio)	21
Total Geral	**163**

Fonte: os autores

Tabela 3 - distribuição dos sistemas operacionais no parque computacional.

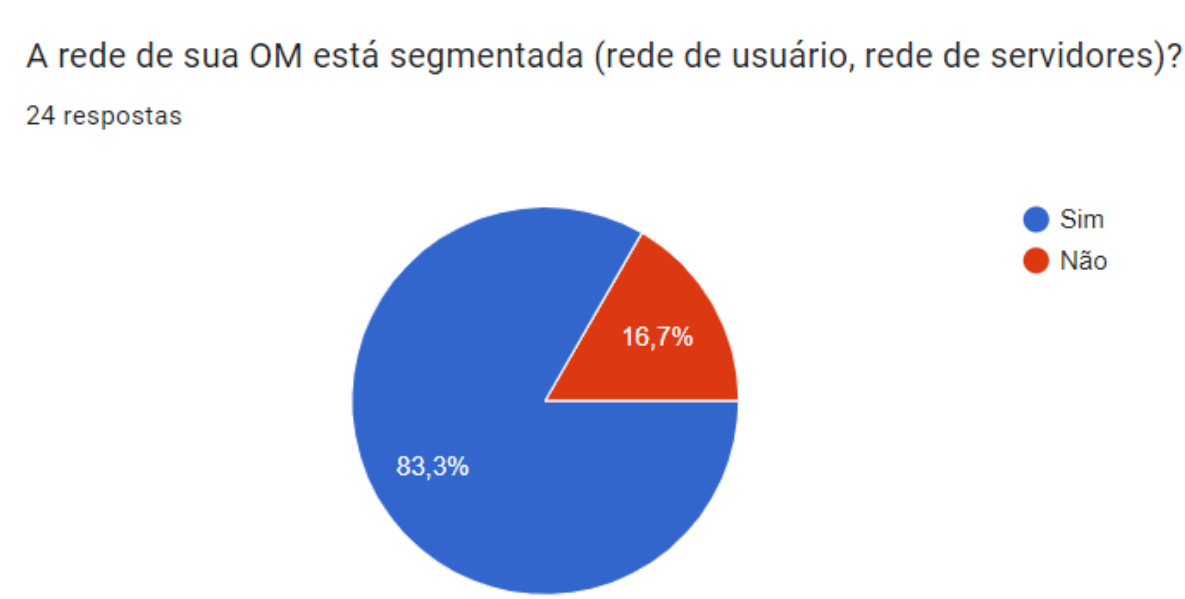
Sistemas Operacionais	Quantidade
POP OS	**32**
20.04	32
Ubuntu	**160**
2023	19
16.04	12
18.04	83
20.04	1
22.04	45
Windows	**2**
2009	1
8.1	1
(vazio)	
(vazio)	
Total Geral	**194**

Fonte: os autores

ANEXO B

Sumarização dos resultados obtidos por meio do questionário das condições da infraestrutura de segurança cibernética das Organizações Militares (OM), presente no Apêndice B.

Figura 1 - divisão das respostas referentes à pergunta 1

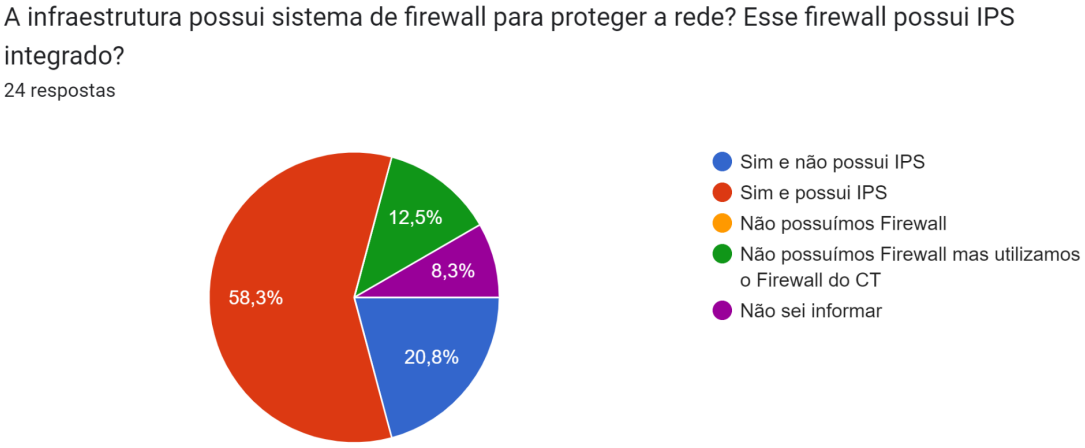


Fonte: os autores

Figura 2 - divisão das respostas referentes à pergunta 2

Fonte: os autores

Figura 3 - divisão das respostas referentes à pergunta 3

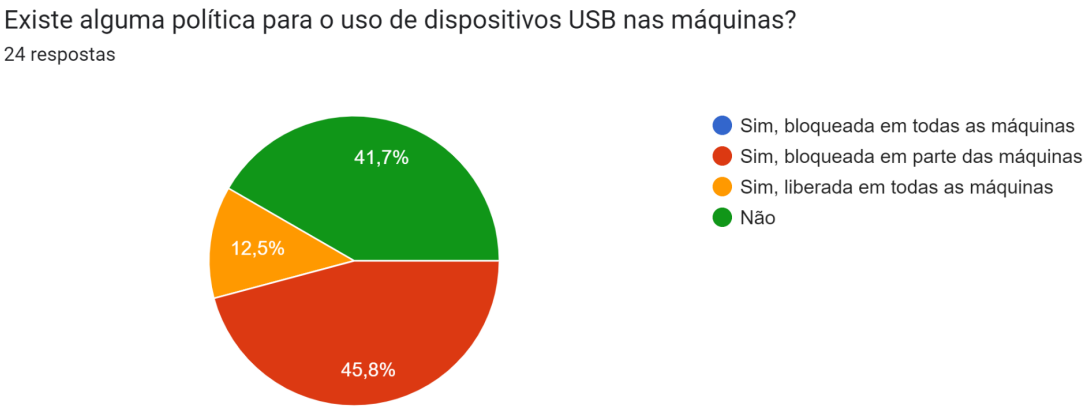


Fonte: os autores.

Figura 4 - divisão das respostas referentes à pergunta 4

Fonte: os autores.

Figura 5 - divisão das respostas referentes à pergunta 5



Fonte: os autores.

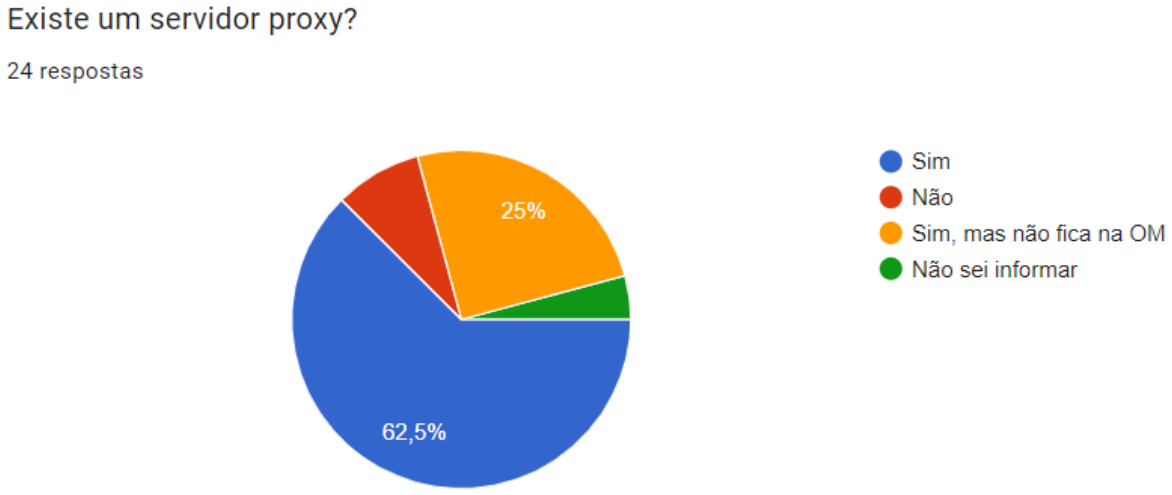
Figura 6 - divisão das respostas referentes à pergunta 6

Fonte: os autores.

Figura 7 - divisão das respostas referentes à pergunta 7

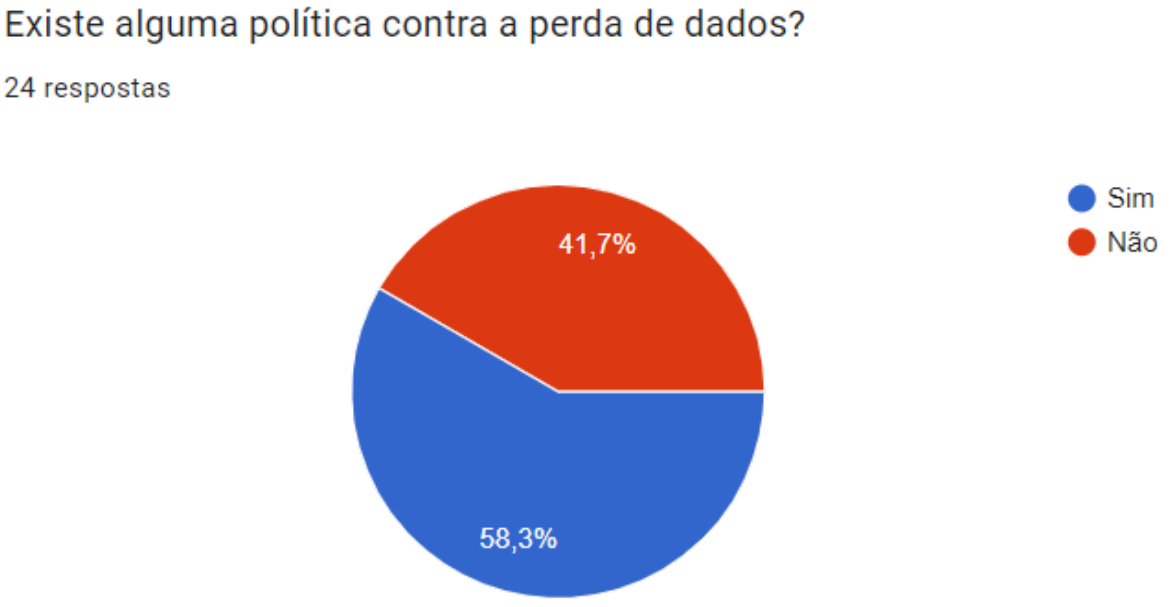
Fonte: os autores.

Figura 8 - divisão das respostas referentes à pergunta 8



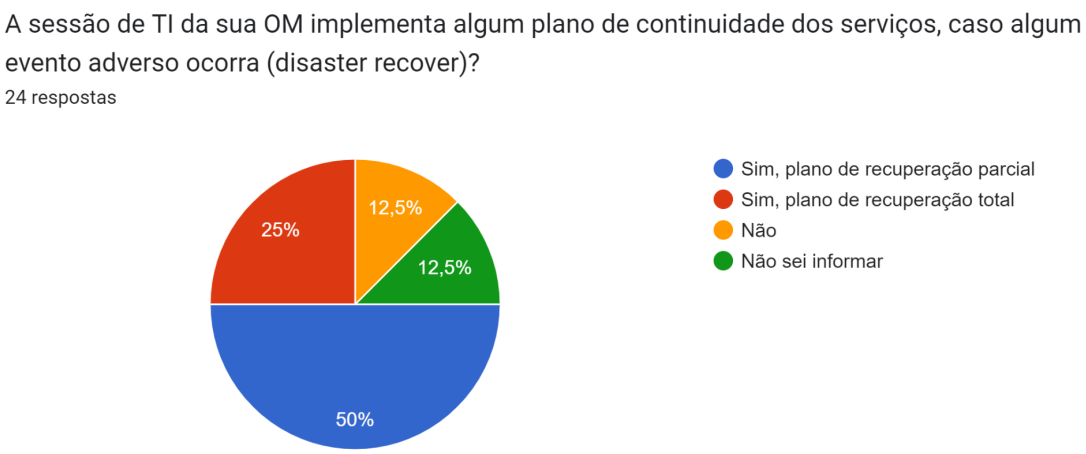
Fonte: os autores.

Figura 9 - divisão das respostas referentes à pergunta 9



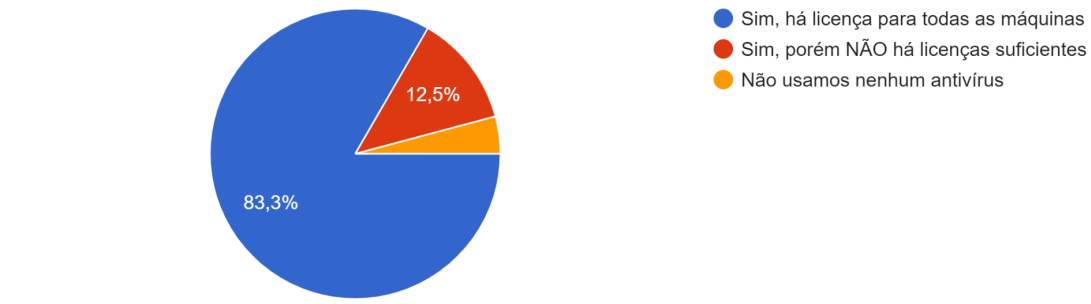
Fonte: os autores.

Figura 10 - divisão das respostas referentes à pergunta 10



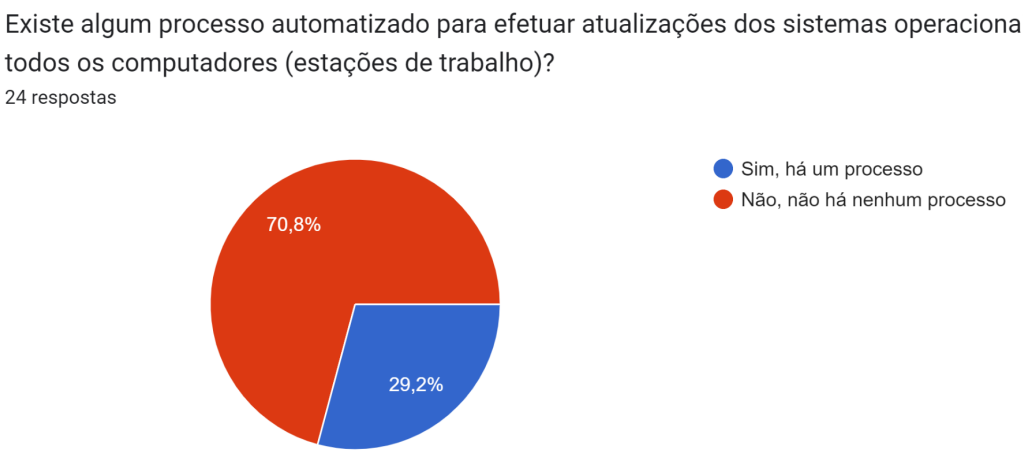
Fonte: os autores.

Figura 11 - divisão das respostas referentes à pergunta 11



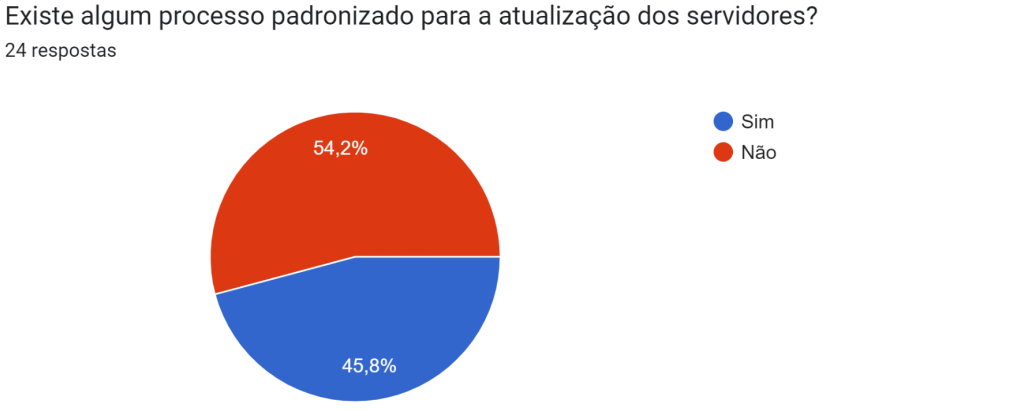
Fonte: os autores.

Figura 12 - divisão das respostas referentes à pergunta 12



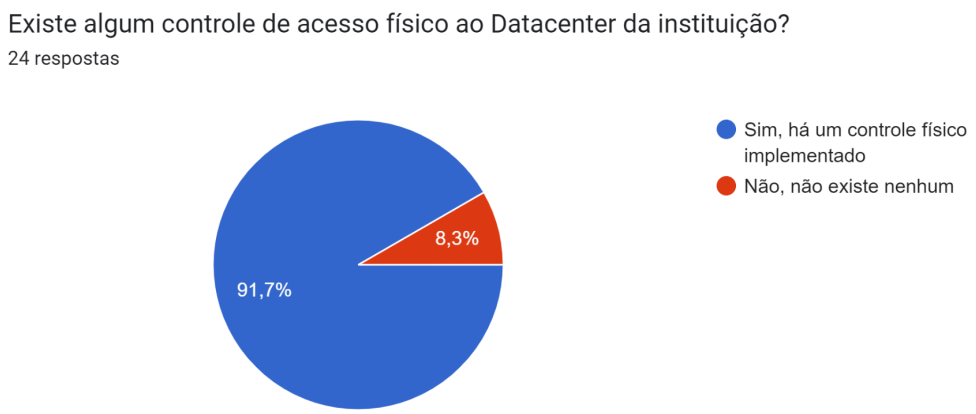
Fonte: os autores.

Figura 13 - divisão das respostas referentes à pergunta 13



Fonte: os autores.

Figura 14 - divisão das respostas referentes à pergunta 14



Fonte: os autores.

Tabela 1: sumário das respostas obtidas na pergunta 15

biometria	Liberação por perfis
porta com controle de acesso	Apenas militares autorizados podem adentrar ao datacenter.
A sala de servidores só tem acesso pessoas autorizadas e acompanhadas pelos militares da STI	tranca com acesso limitado
fechadura digital	Cartão de acesso e senha

Fonte: os autores.