RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

A IMPORTÂNCIA DA PADRONIZAÇÃO DOS COMPUTADORES UTILIZADOS PELA POLÍCIA MILITAR DO PARANÁ SOB O OLHAR DA SEGURANÇA DA INFORMAÇÃO

THE IMPORTANCE OF STANDARDIZING THE COMPUTERS USED BY THE MILITARY POLICE OF PARANÁ FROM THE PERSPECTIVE OF INFORMATION SECURITY

LA IMPORTANCIA DE ESTANDARIZAR LAS COMPUTADORAS UTILIZADAS POR LA POLICÍA MILITAR DE PARANÁ DESDE LA PERSPECTIVA DE LA SEGURIDAD DE LA INFORMACIÓN

Fabrício Ferreira Pinheiro[1]

e616210
https://doi.org/10.47820/recima21.v6i1.6210

PUBLICADO: 1/2025

RESUMO

O presente artigo tem como finalidade apresentar e analisar a importância na padronização dos computadores em uso pela Polícia Militar do Paraná sob a ótica da “Segurança da Informação”, visando estimular e delimitar esta prática na corporação, tanto no processo da aquisição de novos equipamentos, quanto do recebimento destes dispositivos de outras formas de repasse como, por exemplo, através de doação de outros órgãos. Esta proposta tem como objetivo ainda, disseminar conceitos relacionados à Segurança da Informação na corporação, que se apresentam pouco discutidos entre os militares estaduais. Partindo desta discussão, a padronização de computadores se apresenta como um fator preponderante para se evitar exposições de dados relacionados à segurança pública, os quais, são de extrema importância para as atividades da Polícia Militar e dos cidadãos por ela atendidos. A metodologia utilizada se alicerçou em levantamentos da literatura, documentação, legislação e dados quantitativos, os quais validam a necessidade de discussão do tema em todas as atividades da corporação. Defronte, desta análise concluiu-se que é primordial colocar em discussão o tema e sugerir melhorias para que a atividade de padronização atenda próximo aos 100% dos computadores utilizados pela Polícia Militar do Paraná.

PALAVRAS-CHAVE: Computadores. Segurança da Informação. Padronização. Polícia Militar do Paraná.

ABSTRACT

The purpose of this article is to present and analyze the importance of standardizing the computers in use by the Military Police of Paraná from the perspective of "Information Security", aiming to stimulate and delimit this practice in the corporation, both in the process of acquiring new equipment and receiving these devices from other forms of transfer such as, for example, through donation of other organs. This proposal also aims to disseminate concepts related to Information Security in the corporation, which are little discussed among the state military. Based on this discussion, the standardization of computers presents itself as a preponderant factor to avoid exposure of data related to public security, which are extremely important for the activities of the Military Police and the citizens served by it. The methodology used was based on surveys of literature, documentation, legislation and quantitative data, which validate the need to discuss the topic in all activities of the corporation. From this analysis, it was concluded that it is essential to discuss the issue and suggest improvements so that the standardization activity meets close to 100% of the computers used by the Military Police of Paraná.

KEYWORDS: *Computers. Information Security. Standardization. Military Police of Paraná.*

RESUMEN

El objetivo de este artículo es presentar y analizar la importancia de estandarizar las computadoras en uso por la Policía Militar de Paraná desde la perspectiva de la "Seguridad de la Información", con el objetivo de estimular y delimitar esta práctica en la corporación, tanto en el proceso de adquisición de nuevos equipos como en la recepción de estos dispositivos de otras formas de transferencia como, por ejemplo, a través de la donación de otros órganos. Esta propuesta también tiene como objetivo difundir conceptos relacionados con la Seguridad de la Información en la corporación, los cuales son

[1] Graduando em Tecnologia da Informação pela UFPR. 1º Tenente da PMPR – Polícia Militar do Paraná.

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

poco discutidos entre los militares estatales. A partir de esta discusión, la estandarización de las computadoras se presenta como un factor preponderante para evitar la exposición de datos relacionados con la seguridad pública, los cuales son de suma importancia para las actividades de la Policía Militar y de los ciudadanos atendidos por ella. La metodología utilizada se basó en relevamientos de literatura, documentación, legislación y datos cuantitativos, que validan la necesidad de discutir el tema en todas las actividades de la corporación. A partir de este análisis, se concluyó que es fundamental discutir el tema y sugerir mejoras para que la actividad de estandarización satisfaga cerca del 100% de las computadoras utilizadas por la Policía Militar de Paraná.

PALABRAS CLAVE: *Computadoras, Seguridad de la Información. Normalización. Policía Militar de Paraná.*

INTRODUÇÃO

A Segurança da Informação é um tema que tem sido muito discutido e difundido em todos os ramos da vida das pessoas, seja ela no contexto profissional, familiar ou cultural, além de ser essencial para a proteção de dados e sistemas sob a responsabilidade das corporações públicas e privadas, sendo fundamentada por Cunha e Fenato (2013) em três pilares principais: confidencialidade, integridade e disponibilidade.

Dentro das Organizações Policiais Militares, a aplicação da Segurança da Informação adquire uma sensação ainda mais crítica, haja vista a "atribuição constitucional a realização do policiamento ostensivo para a prevenção criminal" (Oliveira Junior; Santos, 2022, p. 56) que lhes cabem.

Diante desta realidade, e das finalidades especificas das Corporações Militares Estaduais, não há como estas se mostrarem desconexas do tema, pois além de compreenderem o Sistema de Segurança Pública, dependem e tratam de forma objetiva de informações, que geram e tem acesso, necessitando "inovar e aprimorar os procedimentos de segurança que permitam uma atuação mais efetiva quanto à prevenção e repressão de ilícitos" (Paraná, 2019, p. 219).

Importante ressaltar que Polícia Militar do Paraná (PMPR), como órgão premente no âmbito da Segurança Pública Estadual, encontra-se atuante em todos os municípios do Estado do Paraná, executando sua atividade primordial de policiamento ostensivo, atendendo a população paranaense de forma preventiva e ostensiva, deve compreender este tema, relacionada à segurança da informação, com um olhar mais apurado.

A relevância deste assunto reflete na sua ligação direta com a segurança pública, com o advento das novas tecnologias, a proteção da informação tornou-se essencial, especialmente considerando que as empresas e o estado estão cada vez mais vulneráveis a ataques, portanto, assegurar a integridade, confidencialidade e disponibilidade dos sistemas da PMPR é fundamental para proteger, não somente informações sensíveis, mas também a própria população (Machado *et. al.*, 2024).

Neste sentido, um dos aspectos centrais para garantir a eficácia das políticas de segurança da informação e da segurança pública na PMPR, é a padronização dos ativos de TI, especialmente os computadores utilizados pelos militares estaduais, que são ferramentas indispensáveis no desempenho de suas atividades.

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

Estes ativos, que de acordo com normas técnicas publicadas sobre o tema, se caracterizam como ativos de suporte, ou seja, *hardware*, elementos físicos, equipamentos de processamento de dados, os quais, por conseguinte podem se tornar origens de vulnerabilidades e ameaças que visam comprometer outros ativos. (ABNT, 2019).

Além disso, há diversos outros desafios enfrentados pela PMPR na gestão desses ativos, dentre eles, cita-se restrições orçamentárias, diversidade de modelo, e a necessidade de garantir o acesso rápido e seguro às informações necessárias e por muitas vezes críticas. Tais obstáculos tornam este processo um tema de relevância no contexto da segurança da informação.

Todavia, o assunto Segurança de Informação e demais conceitos correlatos, que visam à proteção das informações, tanto dos cidadãos, como da atividade fim, entre outras finalidades básicas, não são tratados, de forma mais incisiva junto aos nossos principais usuários, os policiais militares, os quais precisam ter acesso, produzem e manipulam uma quantidade de informações diárias em um volume extremamente massivo, para executar as ações administrativas e operacionais.

Vale ressaltar que para tratar estas informações eles fazem uso de dispositivos tecnológicos, dentre estes, computadores e celulares. Com a utilização e manipulação direta destas informações pelos militares estaduais, através destes dispositivos, é de extrema relevância que em primeiro lugar a corporação compreenda a importância de proteger estes dados, não só mediante a utilização de meios tecnológicos de segurança disponíveis, mais principalmente através de seu comprometimento em resguardar estas informações.

Em um segundo momento, é relevante que os militares estaduais, compreendam também estas relações com o tratamento das informações, através de normas regulamentos e políticas, segundo Fontes (2015), é imperioso que, para instituir uma política de segurança da informação as corporações devem atuar em treinamento, conhecimento, entendimento e atribuições de responsabilidades dos usuários junto aos processos organizacionais.

Junto a isso, a corporação em parceria com a Companhia de Tecnologia e Informação do Paraná (Celepar), atua de forma ativa em um ponto crucial deste tema, segurança da informação, através da padronização dos computadores que fazem parte do patrimônio da PMPR e são utilizados pelos Policiais Militares, em todo o Estado, como um dispositivo de apoio a execução de suas atribuições.

Portanto, o presente artigo através de uma abordagem metodológica baseada em revisões de literatura especializada, fundamentação teórica e avaliação de informações levantadas junto à corporação e a Celepar tem por objetivo fornecer uma compreensão abrangente da importância da Segurança da Informação na PMPR, com ênfase na padronização dos computadores sob a responsabilidade e patrimônio da Polícia Militar do Paraná. Busca também, identificar os principais desafios relacionados a essa padronização e propor soluções que contribuam para o aprimoramento das políticas de segurança da informação e para a conscientização dos policiais militares sobre a importância da proteção dos ativos tecnológicos sob sua cautela.

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

Este levantamento de informações permite um exame aprofundado dos principais desafios enfrentados pela PMPR na padronização de seus ativos de TI, mais especificadamente dos computadores, assim como, a identificação de soluções práticas e eficazes que possam ser implementadas pela corporação.

Para tanto, o presente artigo foi dividido em três seções, a primeira sob o aspecto da Segurança da Informação, seus princípios básicos e como ela é abordada pela PMPR.

Em um segundo momento, será discutida a importância da padronização dos computadores utilizados pela Polícia Militar do Paraná, bem como, conceitos sobre o contexto de padronização de processos.

Após será realizada uma análise situacional, sobre a padronização dos computadores na PMPR, tanto quanto a *softwares*[1] básicos, como dos *softwares* de gestão, através de dados obtidos dos sistemas de gestão de ativos de TI da corporação.

Em se tratando da metodologia utilizada, foram utilizados componentes bibliográficos e análise quantitativa de dados pesquisados, junto à corporação.

1. SEGURANÇA DA INFORMAÇÃO E SEUS PRINCÍPIOS NA PMPR

Antes ao focar no objeto do referido artigo, é importante realizar uma reflexão sobre o conceito de segurança da informação, como sendo um conjunto de sugestões, normas, processos e demais procedimentos que tem por objetivo a proteção da informação, proporcionando que as organizações executem sua atividade e logrem êxito na sua missão (Fontes, 2006).

Além disso, a segurança da informação traz consigo demais princípios basilares do tema, que também são de primordial relevância quando abordamos o assunto, podendo citar de forma ativa e objetiva, os principais: confidencialidade, disponibilidade e integralidade conforme definido por Fontes:

> - Disponibilidade: a informação deve estar acessível para o funcionamento da organização e para o alcance de seus objetivos e missão.
> - Integridade: a informação deve estar correta, ser verdadeira e não estar corrompida.
> - Confidencialidade: a informação deve ser acessada e utilizada exclusivamente pelos que necessitam dela para a realização de suas atividades profissionais na organização; para tanto, deve existir uma autorização prévia (Fontes, 2017).

Ainda, no âmbito da segurança da informação, cabe ressaltar, o conjunto de normas da série ISO 27000, as quais, definem um eixo de pressupostos relativos, em virtude da importância da temática na vida de todos os cidadãos (Sansigolo, 2015).

[1] Software: Conjunto de programas, processos, regras e, eventualmente, documentação, relativos ao funcionamento de um conjunto de tratamento de informação, por oposição a *hardware*. Fonte: https://dicionario.priberam.org/ – 2024

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

Diante de todo este embasamento conceitual sobre Segurança da Informação, passa-se a entender as formas como esta ciência se correlaciona com a Segurança Pública e a Polícia Militar, e seus impactos nas atividades da PMPR e de seus principais agentes, os Policiais Militares.

Além disso, a Segurança da Informação é uma área estratégica para as organizações que lidam com dados sensíveis, e na PMPR, essa relevância é ampliada devido ao papel crítico da corporação, qual seja a preservação da ordem pública e consequentemente na proteção de informações sensíveis.

Da mesma forma, é observado pela PMPR (2024) que “toda informação, imagem gerada ou dado gerado, acessado, manuseado ou armazenado, no âmbito da PMPR, será classificado nos termos de seu valor, dos requisitos legais, da sensibilidade, criticidade e necessidade de compartilhamento".

Dessa forma, os três pilares fundamentais da Segurança da Informação, já citados devem nortear as boas políticas e práticas destinadas a assegurar que as informações, sistemas e ativos de Tecnologia da Informação (TI), da corporação permaneçam protegidos contra ameaças internas e externas. Para garantir esta proteção, a corporação estabelece mecanismos de controle proporcionais ao grau de confidencialidade e criticidade da informação, independentemente de seu formato ou meio de transmissão (PMPR, 2024).

O primeiro pilar, a confidencialidade, refere-se à garantia de que as informações estejam acessíveis apenas para pessoas autorizadas. Segundo Cunha e Fenato (2013, p. 12), "para garantir esse princípio, o acesso às informações deve ser feito somente pelas pessoas explicitamente autorizadas".

No contexto da PMPR, isso inclui o controle rigoroso sobre o acesso a registros operacionais, planos estratégicos e dados pessoais de cidadãos, neste sentido, “o fornecimento de informações constantes nos bancos de dados dos sistemas da Corporação deverá ser realizado mediante prévia autorização dos respectivos Comandantes, Diretores ou Chefes" (PMPR, 2024, p. 4).

Diante do exposto, se observa que a falta de medidas robustas para assegurar a confidencialidade pode resultar em exposição de informações sensíveis, comprometendo operações policiais e colocando em risco a segurança da população e dos próprios militares estaduais.

A integridade, segundo pilar fundamental, é o que garante que as informações não sejam modificadas ou destruídas de maneira não autorizada ou acidental. Na PMPR, a proteção da integridade dos dados é assegurada através de mecanismos específicos que garantem que somente pessoas autorizadas possam ter acesso e realizar modificações nas informações (PMPR, 2024).

No sentido, de minimizar erros ou manipulações em relatórios de ocorrências, os quais, podem prejudicar investigações criminais e comprometer a justiça, adicionalmente, é fundamental manter registros detalhados, incluindo "identificação do usuário que efetuou o acesso, data e hora de acesso ao sistema, origem do acesso, erros ou falhas de conexão". (PMPR, 2024, p. 25).

O terceiro pilar, a disponibilidade, assegura que as informações e os sistemas estejam acessíveis quando necessários, ou seja é a "qualidade da informação que pode ser conhecida e

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

utilizada por indivíduos, equipamentos ou sistemas autorizados" (Brasil, 2011). Permitindo que os dados e sistemas possam ser utilizados de forma eficiente por pessoas autorizadas quando precisarem (Cunha; Fenato, 2013).

Na PMPR, a disponibilidade dos sistemas é fundamental para a eficácia operacional, pois as atividades de segurança pública exigem processos modernos de gestão e adequado suporte tecnológico. Para tanto, é essencial manter uma infraestrutura robusta que garanta o acesso imediato às informações necessárias para as operações, permitindo uma resposta rápida e eficiente às demandas de segurança pública (Oliveira Junior; Santos, 2022).

Entende-se, em vista do exposto que a aplicação dos pilares da Segurança da Informação requer uma abordagem holística, pela Polícia Militar, principalmente pelos responsáveis direta e indiretamente pelo tratamento das informações, considerando tanto aspectos técnicos quanto comportamentais.

A implementação dos princípios, também enfrenta outros desafios específicos no contexto da PMPR, incluindo a variedade de ativos de sistemas, bem como, a necessidade de atuar em ambientes variados, que vão desde instalações administrativas, até a atividade do serviço operacional. Esses desafios exigem soluções criativas e adaptáveis, como o uso de dispositivos seguros e a priorização de investimentos em áreas de maior impacto para a segurança.

Em suma, a definição e a aplicação dos princípios da Segurança da Informação na PMPR não apenas garantem a proteção de dados sensíveis e a continuidade das operações, mas também reforçam a confiança da população na capacidade da corporação de cumprir seu papel. A efetividade dessa abordagem depende de um equilíbrio entre investimento em tecnologias, treinamento e a adoção de políticas organizacionais que priorizem a segurança em todos os níveis.

2. A IMPORTÂNCIA DA PADRONIZAÇÃO DE COMPUTADORES NA POLÍCIA MILITAR DO PARANÁ

A padronização é considerada uma das ferramentas gerenciais mais fundamentais no mundo empresarial moderno, sendo a base para o gerenciamento da rotina do trabalho diário e na qualidade total. No Brasil, entretanto, existem desafios significativos em relação à padronização, incluindo, falta de literatura adequada, carência de educação e treinamento para gestores, tendência a delegar a responsabilidade apenas aos técnicos, quando na verdade é uma função essencialmente gerencial (Campos, 2014).

Adrião e Gonçalves (2016), ainda acrescentam que quando a padronização é estabelecida como tática corporativa pela alta administração, sua implementação se torna mais efetiva e gera benefícios para a organização em escala global, incluindo a TI.

Neste sentido, a padronização dos ativos de TI, especialmente os computadores utilizados em uma organização, é uma estratégia fundamental para melhorar a segurança da informação. Essa prática não apenas garante a consistência e a eficiência no uso dos recursos tecnológicos, mas também contribui para a proteção dos dados e a mitigação de riscos associados à segurança da informação (Cunha; Fenato, 2013).

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

Segundo Dias *et al.,* (2023) e Adrião e Gonçalves (2016), os ativos de Tecnologia da Informação (TI) representam recursos estratégicos fundamentais que, quando adequadamente alinhados aos objetivos organizacionais, potencializam o valor do negócio e devem ir além do papel operacional, atuando como elementos consultivos e propositores de soluções inovadoras, sempre buscando agregar capacidades competitivas à organização.

No contexto da direção de TI da Polícia Militar do Paraná (PMPR), essa prática contribui diretamente para a redução de vulnerabilidades que podem ser exploradas por agentes maliciosos. Ainda, de acordo com PMPR (2024) a padronização tecnológica é fundamental para a segurança, pois todos os computadores da corporação devem estar configurados no padrão definido pela DDTQ, com mecanismos de proteção e *softwares* homologados devidamente instalados.

Por analogia, vislumbra-se que a padronização permite a implementação de políticas de segurança de maneira uniforme, facilitando a identificação e correção de potenciais pontos fracos na infraestrutura.

Outro benefício importante da padronização é a facilidade na atualização de sistemas e aplicativos, pois esta estratégia de padronização de elementos de tecnologia de informação, sejam eles de infraestrutura como *hardware* e *software* básico, estabelece processos de gestão que garantem maior eficiência em caráter geral para a organização (Adrião; Gonçalves, 2016).

Isso é particularmente relevante no combate a ameaças cibernéticas, que frequentemente exploram vulnerabilidades em *softwares* desatualizados. Na PMPR isso é reforçado pela exigência de que "os computadores possuem instalação padrão desenvolvida pela PMPR, composta por *softwares* e aplicativos necessários ao desempenho das funções de trabalho, além de *softwares* para proteção, monitoramento e auditoria do equipamento" (PMPR, 2024, p. 45).

Além disso, a padronização simplifica a gestão de ativos de TI, permitindo maior controle sobre o ambiente tecnológico. Com um inventário unificado, a equipe de TI da PMPR pode monitorar de maneira mais eficaz o desempenho e a segurança dos sistemas.

Destacam desta mesma forma, Schena e Junior (2022), que em questões de segurança, a integração tecnológica e a padronização facilitam o monitoramento e a proteção dos dados transmitidos, possibilitando respostas mais rápidas a incidentes e garantindo melhor conformidade com as políticas estabelecidas.

Portanto, a padronização desempenha um papel essencial na educação e conscientização dos usuários, no caso, os policiais militares que utilizam os equipamentos. Com sistemas uniformes, é mais fácil oferecer treinamentos padronizados sobre boas práticas de segurança e uso correto dos dispositivos. Isso não apenas melhora a segurança geral da corporação, mas também promove uma cultura organizacional voltada à proteção das informações.

3. ANÁLISE SITUACIONAL DA PADRONIZAÇÃO DE COMPUTADORES NA PMPR

a. *Softwares* básicos para padronização

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

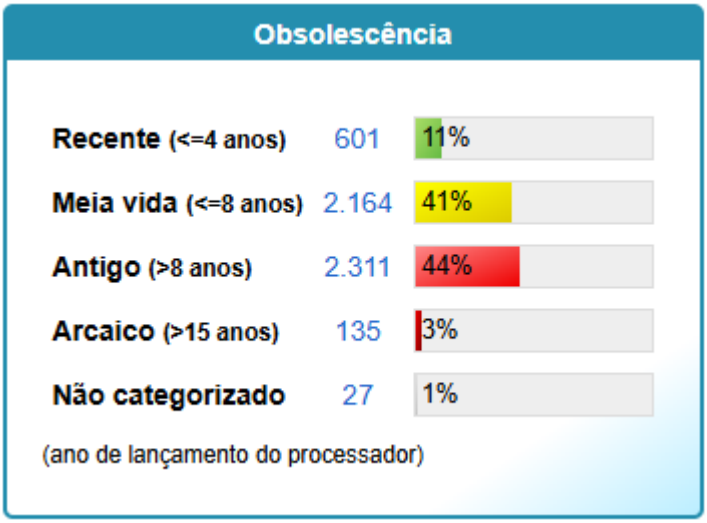
A PMPR possui uma rede constituída por diversas redes locais, sob sua responsabilidade, disponibilizadas para uso de suas Unidades e Subunidades. Esta infraestrutura é gerenciada pela Diretoria de Desenvolvimento Tecnológico e Qualidade (DDTQ), que atua como coordenadora de todos os sistemas informatizados utilizados na PMPR. Os equipamentos incluem desde estações de trabalho até sistemas embarcados, sendo que todos devem estar configurados no padrão PMPR. A gestão destes recursos tecnológicos visa garantir a correta aplicação e a confidencialidade, integridade e disponibilidade das informações, permitindo que a corporação atenda às demandas operacionais e administrativas em todo o estado. (PMPR, 2024).

Entretanto uma análise quantitativa revela a existência de uma heterogeneidade significativa dos computadores, principalmente em termos de *hardware*. Essa diversidade é corroborada pela própria corporação quando define a classificação dos seus computadores:

> e) fica definido que os computadores da Corporação e seus periféricos, como ativos de TIC, seguirão a seguinte classificação, observado a data de
> fabricação do item e o sistema institucional de gestão de materiais e serviços:
> – novo até 4 anos;
> – meia vida mais de 4 anos e até 8 anos;
> – antigo superior 8 anos;
> – obsoleto superior a 10 anos (PMPR, 2024, p. 10).

A partir desta definição dada pela corporação e pelos dados apresentados pelo sistema de gestão de ativos, é possível identificar a realidade quanto à obsolescência, avaliada de acordo com o ano do processador, dos computadores utilizados pela PMPR, fator básico quando se propõe um processo de padronização de ativos, conforme figura abaixo:

Figura 1: computadores quanto à obsolescência



Fonte: Sistema OCS Inventory, (com adaptações do autor, 2024)

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

Considerando que, conforme relatórios internos, fornecidos pela Celepar, através do sistema de gestão de ativos *OCS Inventory*[2]*,* a PMPR possui 5.237 computadores, em média monitorados, incluindo os dispositivos de mesa e notebooks.

A próxima etapa no processo de padronização dos computadores da PMPR está na análise do conjunto de *softwares* destinados ao pleno funcionamento destes ativos. Este processo também é realizado pela equipe de Suporte da Celepar, ou pelo Oficial de Tecnologia da Informação e seus auxiliares.

A função de Oficial de TI é definida pelo Regulamento Interno e dos Serviços Gerais da Polícia Militar do Paraná (RISG/PMPR), o qual traz também suas atribuições que segundo Paraná (2010) e PMPR (2024) são responsáveis por providenciar suporte em *hardware* e *software,* além de gerenciar os ativos de TIC, com o objetivo de oferecer suporte à DDTQ. (Paraná, 2010).

Para executar esta fase do processo de padronização de computadores a DDTQ/Celepar disponibiliza arquivos identificados como ISO, “Imagens” ou *ISO-image*[3]*.* para cada modelo de máquina existente no parque da PMPR. Estes arquivos são identificados desta forma, pois tem origem na Norma ISO 9660, a qual define o padrão de sistema de arquivos, que permite criar uma cópia idêntica do conteúdo armazenado em um disco, ou em uma mídia. (ISO, 1998)

Desta forma, a DDTQ/Celepar, definiram uma lista de *softwares* necessários para cada modelo de computador sob patrimônio da PMPR, os quais devem atender ao desempenho das atividades dos Policiais Militares, dentre a gama de serviços específicos de cada militar, visando atender de forma ampla todas as atribuições da corporação, tanto no âmbito administrativo como operacional.

Esta “imagem” disponibilizada tem como referência principal o Sistema Operacional (SO), considerado um *software* básico, que cada computador suporta em razão também do grau de obsolescência das máquinas este é um ponto minucioso, em virtude as atualizações de *hardware* e *software*, que se tornam cada vez mais constantes de dinâmicas. (Gomes Filho *et al.,* 2008).

A partir desta perspectiva, os Oficiais de TI e seus auxiliares designados, para a execução de suas atividades relacionadas à padronização dos computadores, algumas “imagens”, com o intuito de atender todo o parque de computadores de suas unidades, dependendo da marca, modelo e Sistema Operacional, conforme tabela abaixo:

Tabela 1: Imagens PMPR de acordo com o SO - 2024

Linux UBUNTU	Windows 10	Windows 11	**Total**
03	06	13	**22**

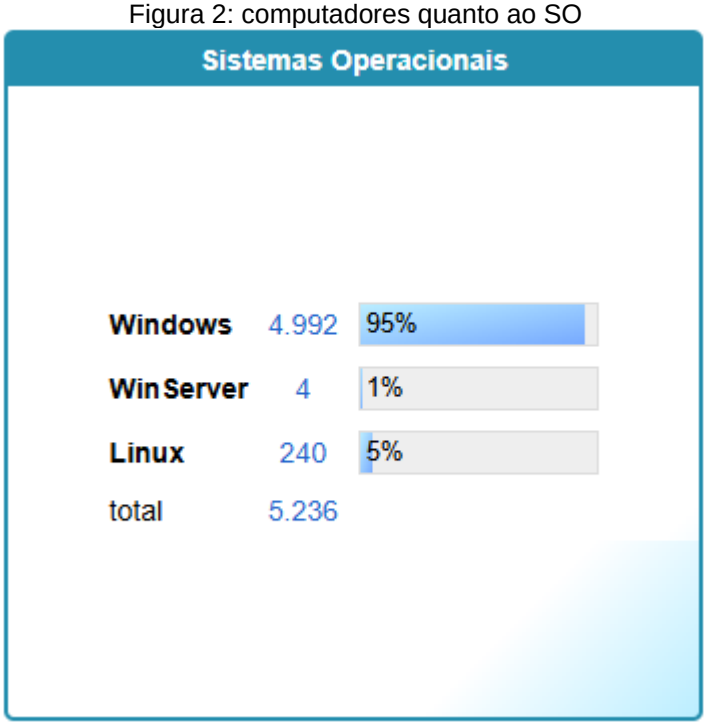
Fonte: Elaboração própria com base nos dados da Wiki Celepar (DDTQ/Celepar2024).

[2] OCS Inventory: Software livre para gestão de ativos de TI. Fonte: https://wiki.ocsinventory-ng.org – 2024
[3] ISO-Image: Arquivo que contém cópia fiel do conteúdo de uma mídia. Fonte: https://www.datastorage.com.br/post/o-que-e-imagem-iso – 2024

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

Diante desta quantidade de “imagens” disponíveis, e após consultar o sistema de *OCS Inventory,* delimitado pelo quesito sistema operacional, é possível identificar que grande parte do parque de máquinas em uso pela PMPR, é de dispositivos que tem como base SO Windows, independente de sua versão, conforme imagem abaixo:

Figura 2: computadores quanto ao SO



Fonte: Sistema OCS *Inventory*, (com adaptações do autor, 2024)

Ainda nesse sentido, para garantir que estas “imagens”, atendam os pilares da Segurança da Informação, ou seja, disponibilidade, integridade e confidencialidade, os arquivos ficam à disposição dos Oficiais de TI, dentro da rede da PMPR, e podem ser acessados através de autenticação do usuário. Sendo que a integridade do arquivo pode ser comprovada após seu *download* através do algoritmo de criptografia *hash256*[4] (Celepar, 2024).

Além do SO cada “imagem”, possui uma lista de *softwares*, *drivers*[5], personalização, regras do sistema, licenças, *scripts*[6] de configuração, arquivos locais necessários, *patchs*[7] de correção, homologados além de orientações quanto a configurações manuais a serem realizadas pelos Oficiais de TI. Toda esta gama de ações, faz parte do processo de padronização dos computadores que utilizaram estas “imagens” (Celepar, 2024).

[4] Hash256: Algoritmo seguro de 256 bits usado para proteção criptográfica. Fonte: https://support.google.com/ - 2024.
[5] Drivers: programa que possibilita a comunicação entre o SO e um *hardware*. Fonte: https://www.intel.com.br/ - 2024.
[6] Scripts: conjunto de instruções para que uma função seja executada em determinado aplicativo. Fonte: https://languages.oup.com/ - 2024
[7] Patchs: uma correção de software destinada a resolver problemas de funcionalidade, segurança ou atualização. Fonte: https://www.computerweekly.com/ - 2024

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

O catálogo de *software* que compõe estas "'imagens" segue a regulamentação de licenciamento de *software* definidas pela PMPR:

> a) todo software a ser instalado para uso na PMPR deve, obrigatoriamente, ter passado por processo de licenciamento de uso, aquisição regulamentar e obediência às normas patrimoniais do Estado do Paraná, bem como as normativas específicas da DDTQ: (PMPR, 2024, p. 47).

Tomando como parâmetro a "imagem" mais atual disponibilizada pela (DDTQ/Celepar), a qual, tem como base o SO Windows 11, a ser utilizado no computador marca Positivo, modelo D610, além do Sistema Operacional mais 45 *softwares* são agregados a ela, dentre os principais, relaciona-se aplicativos como (navegadores, leitor de arquivos PDF, antivírus, editor de imagens, pacote de escritório, *softwares* de impressão entre outros) (Celepar, 2024).

A variedade de computadores e *softwares* disponibilizados e utilizados pelos Policiais Militares evidencia a necessidade de uma abordagem estratégica para a padronização desses equipamentos, com o objetivo de aprimorar a compatibilidade, facilitar a manutenção e garantir a proteção das informações sensíveis da corporação.

b. *Softwares* de gestão de ativos

Outra fase preponderante no processo de padronização os computadores da PMPR está no conjunto de *softwares* destinados a gestão dos ativos de TI, os quais são primordiais, para o controle dos SO instalados, número de série dos equipamentos, avaliação das caraterísticas de *hardware* e *software.*

Neste sentido a corporação delimita que a padronização de computadores se dará futuramente em novas legislações internas conforme PMPR (2024, p. 53), "Os seguintes documentos serão definidos pela DDTQ em apartado: [...] d) padronização de computadores", a Celepar através de seu suporte técnico, entende que um computador é identificado como padronizado, quando possui minimamente quatro sistemas de gestão instalados e atualizados, quais sejam eles: *OCS Inventory*[8]*, Wsus*[9]*, Antivírus*[10] *e Mesh Central*[11]*.*

O sistema *OCS Inventory* é um *software* livre, disponibilizado pela DDTQ/Celepar que permite o inventário automatizado de ativos de TI. Auxiliando as atividades do Oficial de TI, coletando informações de *hardware* e *software* das máquinas da rede por meio do programa cliente.

Este inventário pode ser acessado através de uma interface web, oferecendo uma visão detalhada dos computadores, possibilita a implantação de outros *softwares* nos computadores com base em critérios definidos pela Corporação. (OCS Inventory, 2024)

Considerando os relatórios internos, fornecidos pela Celepar, através do sistema de gestão , *OCS Inventory* a PMPR possui 5.237 computadores, em média monitorados, incluindo os dispositivos

[8] OCS Inventory: Software livre para gestão de ativos de TI. Fonte: https://wiki.ocsinventory-ng.org – 2024
[9] Wsus: Gerenciamento centralizado do Sistema Operacional Windows. Fonte: https://learn.microsoft.com – 2024
[10] Antivírus: Software destinado a detecção e eliminação de vírus. Fonte: https://dicionario.priberam.org – 2024
[11] Mesh Central: Sistema de gerenciamento de acesso remoto WEB. Fonte: https://wiki.gga.celepar.pr.gov.br – 2024

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

de mesa e notebooks inventariados, 1.043 dispositivos não inventariados e mais 2.243 dispositivos identificados (DDTQ/Celepar, 2024), sendo que, estes dois últimos valores não se tratam especificadamente de computadores, temos, portanto de um universo de 8.523 dispositivos de rede, 61% sendo computadores monitorados aproximadamente.

A variação em relação aos computadores e dispositivos monitorados se dá em razão, do sistema *OCS Inventory*, realizar varreduras constantes na rede da PMPR, de acordo com parâmetros (dia, horário) definidos pela DDTQ/Celepar, e os computadores que possuem o cliente OCS ativo "responderem" ou não, estas solicitações ao servidor *OCS Inventory*, o qual, fornece estes dados de forma interativa aos responsáveis por esta gestão.

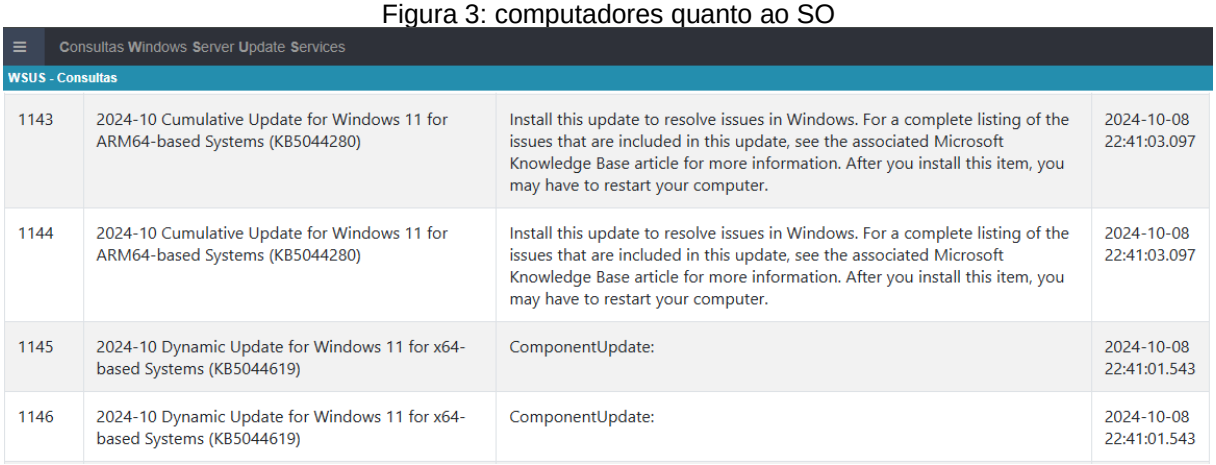
Já o Sistema WSUS permite que a (DDTQ/Celepar) implantem as atualizações mais recentes dos aplicativos da Microsoft licenciados. Através de um servidor centralizado os gestores podem gerenciar e distribuir essas atualizações, de acordo com regras definidas pela corporação. Desta forma a DDTQ/Celepar mantém um servidor ou vários servidores conectados na rede da Corporação conectados ao Microsoft Update para obter as informações sobre as atualizações disponíveis (Microsoft, 2024).

O uso específico deste *software* de gestão é utilizado somente nos computadores que possuem o SO Windows, sua importância se justifica conforme dados já expostos através da (Figura 2), que demonstra que 95% dos computadores inventariados utilizam este SO, como *software* básico.

Dados relativos ao ano de 2024, originados pelo sistema WSUS disponibilizados pelo servidor destinado a atualizações de máquinas da PMPR, forneceram 1.331 atualizações aprovadas e disponíveis para estes equipamentos compatíveis (Celepar, Paraná, 2024).

A imagem abaixo exemplifica como as atualizações autorizadas são listadas no Sistema WSUS para atualização dos SO Windows da PMPR:

Figura 3: computadores quanto ao SO



1143	2024-10 Cumulative Update for Windows 11 for ARM64-based Systems (KB5044280)	Install this update to resolve issues in Windows. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article for more information. After you install this item, you may have to restart your computer.	2024-10-08 22:41:03.097
1144	2024-10 Cumulative Update for Windows 11 for ARM64-based Systems (KB5044280)	Install this update to resolve issues in Windows. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article for more information. After you install this item, you may have to restart your computer.	2024-10-08 22:41:03.097
1145	2024-10 Dynamic Update for Windows 11 for x64-based Systems (KB5044619)	ComponentUpdate:	2024-10-08 22:41:01.543
1146	2024-10 Dynamic Update for Windows 11 for x64-based Systems (KB5044619)	ComponentUpdate:	2024-10-08 22:41:01.543

Fonte: Sistema WSUS, (com adaptações do autor, 2024)

O sistema Mesh Central tem como objetivo principal gerenciar o acesso remoto via WEB de dispositivos conectados a Internet, conforme a Celepar (2024) através deste sistema os gestores de TI, podem ter acesso remoto aso computadores da PMPR, conectados a rede específica, para

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

proceder alguma atividade necessária em algum dispositivo como: envio de arquivos, instalação de outros *softwares*, e principalmente prestar suporte em tempo real ao policial militar, em determinadas situações.

Por fim, o sistema de antivírus conforme PMPR (2024, p. 27) é obrigatório em todo dispositivo conectado à rede, bem como, devem permanecer sempre com licença ativa e atualizada, bem como, os responsáveis pela sua manutenção possuem autonomia para realizar medidas necessárias quando da identificação de ameaças.

Esta ferramenta é a mais comum utilizada para proteger computadores contra *malwares*[12] e outras ameaças, ele funciona basicamente analisando o equipamento e confronta os arquivos com uma base de ameaças conhecidas. Assim como emprega outras técnicas para identificar ameaças online, como vírus, *cavalos de Troia*[13] e *ransomware*[14], disponibilizando proteção avançada contra ciberameaças (Kaspersky, 2024).

Com base nestas informações, e dados obtidos no sistema *OCS Inventory,* é possível mensurar a quantidade de computadores que possuem os *softwares* básicos de gestão de ativos, ou seja, do total de 5.237 máquinas com patrimônio PMPR, quais possuem estas ferramentas, conforme ilustrado na tabela abaixo:

Tabela 2: quantidade aproximada de computadores com presença dos *softwares* básicos para gestão da padronização (%) - 2024

	OCS Inventory	Wsus	Antivírus	Mesh Central
Com	5.237	4.944	4951	5200
%	100	100	95,5	99,2

Fonte: Elaboração própria com base nos dados do OCS Inventory (DDTQ/Celepar, 2024).

Deste levantamento de dados, dos 61% de dispositivos que são identificados como computadores e estão monitorados e considerando a padronização relacionada à gestão dos ativos, 98,7% dos computadores da PMPR, que estão sobre a gestão destes sistemas se apresentam de acordo com as definições de controle de ativos de tecnologia da Corporação.

Considerando ainda, os dados já apresentados, há um universo de 12% de dispositivos, não inventariados e 26% de dispositivos identificados aproximadamente, neste último caso a maioria se tratando de impressoras, câmeras, roteadores etc., sendo está identificação realizada de forma manual pelos Oficiais de TI da Unidade (Celepar, 2024). Este cenário resulta em uma qualidade regular do inventário como se observa na imagem abaixo:

[12]Malwares: Software malicioso, desenvolvido para infectar um computador. Fonte: https://www.kaspersky.com.br/ – 2024
[13] Cavalo de Troia: Arquivo aparentemente normal, mas oculta um malware. Fonte: https://br.norton.com/ – 2024
[14] Ransomware: Tipo de malware, destinado a extorsão ou resgate . Fonte: https://www.kaspersky.com.br/ – 2024

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

Figura 4: Qualidade do Inventário PMPR

Fonte: Sistema OCS Inventory, (com adaptações do autor, 2024)

4. METODOLOGIA

Para construção deste estudo foram adotados dois tipos de abordagem, a primeira foi pesquisa bibliográfica sobre o tema, através de artigos científicos, publicações em revistas técnicas e normativas de órgãos reguladores, como as normas ISO e a legislações principalmente aquelas voltadas a Segurança da Informação, bem como, normas exaradas pela própria PMPR.

Conforme Moresi e Pinho (2021), a pesquisa bibliográfica busca por meio do mapeamento científico e abordagens diversas, como análise de citações, cocitações e co-ocorrência de palavras, fazer um levantamento do tema auxiliando o processo de pesquisa e sondagem de informações.

Com o objetivo de compreender como a padronização dos computadores utilizados pela corporação, pode contribuir com segurança da informação e em consequência com a eficiência das atividades dos Policiais Militares, também foi realizada uma interpretação quantitativa de dados obtidos através dos sistemas de gestão do parque de máquinas da PMPR, especificadamente relativos ao ano de 2024.

As fontes de dados utilizadas no estudo contribuíram muito, pois assim foi possível analisar os dados concretos e operáveis de forma objetiva, possibilitando ainda maiores propostas de intervenção (Costa *et al.,* 2022). Por intermédio destes relatórios técnicos da PMPR sobre as condições dos computadores da corporação foi possível garantir uma visão abrangente e embasada sobre o cenário atual.

A partir destes levantamentos foi viável atender os objetivos da pesquisa, revisando conceitos sobre Segurança da Informação e seus pilares básicos, bem como, refletir sobre a importância da padronização de processos, mais especificadamente relacionados aos ativos de TI de uma corporação.

As avaliações dos dados coletados em comparação com as melhores práticas recomendadas pela literatura em Segurança da Informação e padronização de TI corroboram com a hipótese. Haja vista, as informações indicarem uma relação positiva entre a padronização dos computadores, e as necessidades da corporação em disponibilizar equipamentos em condições para os militares

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

estaduais executarem suas atividades administrativas e operacionais, apontando caminhos viáveis para fortalecer a segurança dos dados tratados e consequentemente da corporação.

5. RESULTADOS E DISCUSSÃO DOS DADOS

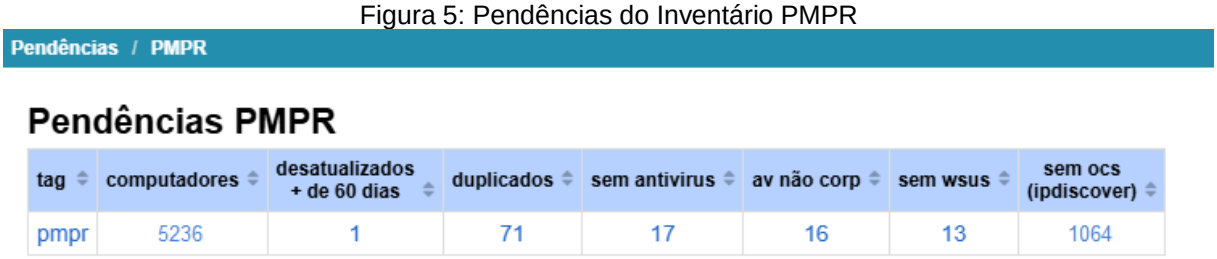
Do levantamento de dados coletados ficou claro que a falta de padronização nos computadores utilizados pela Polícia Militar do Paraná, compromete significativamente a eficiência das atividades administrativas e operacionais da corporação. Pois equipamentos fora do padrão e conectados na rede da PMPR, se tornam dispositivos vulneráveis a ameaças e ataques cibernéticos e por consequência podem ficar indisponíveis para utilização.

Entre os principais problemas identificados, está a obsolescência dos equipamentos o que provoca a necessidade ajustes nas “imagens” por incompatibilidade de *softwares* e sistemas operacionais, com o *hardware* das máquinas. Essas questões reforçam a necessidade de um ambiente tecnológico mais atualizado, capaz de garantir maior confiabilidade e proteção às informações sensíveis da corporação.

Outro ponto relevante destacado nos resultados foi à percepção de que existem mais de 10% de dispositivos não identificados na rede da Polícia Militar, ou seja, o sistema de gestão de ativos não foi capaz de identificá-los, ou o cliente de gestão não se encontra instalado no dispositivo, resultando em um equipamento fora do padrão, podendo ser um computador ou não, portanto a integridade destes dados fica prejudicada.

Abaixo é possível observar algumas pendências geradas pelo próprio sistema *OCS Inventory:*

Figura 5: Pendências do Inventário PMPR



Fonte: Sistema OCS Inventory, (com adaptações do autor, 2024)

Esta demanda de informações exige do Oficial de TI de cada unidade uma participação mais efetiva, quanto ao inventário de dispositivos das unidades, pois eles se encontram fisicamente nos locais e por este motivo podem realizar uma identificação mais fidedigna dos equipamentos e consequentemente manter o sistema de inventário atualizado.

Isso depende também da familiaridade e da experiência de cada um deles, pois em muitas oportunidades acabam por não possuir experiência com ativos de TI. Mas em contrapartida tanto a DDTQ como a Celepar disponibilizam suporte técnico especializado para atender as demandas deste Oficial de TI, bem como, podem orientar sobre estas necessidades.

Fica evidenciado também que ambientes de TI padronizados apontam benefícios, concretos para a corporação, como maior agilidade na resolução de problemas técnicos, maior controle sobre

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

os sistemas e uma significativa redução nas vulnerabilidades relacionadas ao uso de *softwares* não homologados.

O levantamento revela que a implementação da padronização é complexa, em virtude da variada gama de dispositivos, conectados a rede da PMPR, assim como, se identifica à necessidade de uma atualização do parque de máquinas e a capacitação dos Oficiais de TI para tal atividade. Entende-se, que para avançar com o processo de padronização, é necessário tomar ações mais efetivas que resultaram em ganhos a médio e longo prazo, como um suporte mais ágil, maior disponibilidade de computadores e melhoria na Segurança da Informação.

Entende-se que existem orientações claras por parte da legislação interna da corporação, quanto a este processo, mas fica evidenciado a necessidade de avançar com o uso de normas reconhecidas, como as da ISO/IEC 27005, que tem foco específico em segurança da informação além de pontuar com clareza orientações quanto a gestão de ativos de TI.

Assim, o estudo reforça que a padronização, não deve ser tratada apenas como uma questão técnica, e delimitada aos setores que atuam diretamente com tecnologia na corporação, mas sim, como um componente estratégico para a segurança da informação na Polícia Militar do Paraná.

6. CONSIDERAÇÕES

Com esta pesquisa buscou-se entender se a atividade de padronização dos computadores utilizados pela PMPR, sob a ótica da Segurança da Informação, tem relevância na proteção de dados sensíveis que a corporação trata, bem como, se este processo viabiliza uma melhoria na eficiência da gestão de ativos de TI.

O presente estudo demonstrou por meio de levantamento de informações bibliográficos e dados obtidos junto a sistemas de gestão de TI, que são utilizados pela corporação, qual a situação atual deste processo, e qual o grau de importância para a PMPR, em avançar com esta atividade de forma mais efetiva.

Dentre os principais resultados, destaca-se que 61% dos dispositivos inventariados pelos sistemas de gestão utilizados pela PMPR, são computadores que possuem padronização, tanto quanto a *softwares* básicos, quanto a *softwares* de gestão de ativos.

No tocante aos demais 39% de dispositivos conectados a rede da PMPR, observou-se que mais de 10% destes não se apresentam inventariados, portanto não se tem uma informação clara sobre eles. Podem sem computadores fora do padrão ou qualquer outro tipo de dispositivo, o que prejudica a análise dos resultados.

Estes fatos também podem ser confrontados, com a obsolescência dos equipamentos gestionados, pois conforme analisado mais de 45% dos computadores utilizados pela PMPR, estão classificados como “antigo” ou “arcaico”.

Por outro lado, estes dados relacionados com os princípios da Segurança da Informação, demonstram que a PMPR, precisa estimular este tema, além do efetivo que atua diretamente com TI na corporação. É necessário buscar formas de atingir, treinar e conscientizar os Policiais Militar, para

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

estarem atentos quando do uso dos computadores fornecidos pela instituição, entendendo que um computador padronizado faz parte de um processo maior relacionado a segurança digital de todos, inclusive da população atendida.

Entende-se que este estudo, traz contribuições práticas para a Corporação, principalmente no sentido de desenvolver ações relacionadas à aquisição de computadores novos, bem como, para a gestão de TI, a qual pode atuar de forma prática, entendendo as lacunas identificadas no controle de ativos, e avançar na elaboração de documentação específica e treinamento, com o intuito de auxiliar os demais responsáveis.

Claro que os estudos sobre o tema não se encerram, haja vista, que a evolução tecnológica é constante e os dispositivos vão se moldando e atualizando conforme a necessidade das corporações. Portanto há necessidade de novos estudos sobre o assunto, que podem colaborar com o desenvolvimento das atividades policiais militares e com a segurança pública como um todo.

REFERÊNCIAS

ABNT. Associação Brasileira de Normas Técnicas. **NBR ISO/IEC 27005:2019 – Tecnologia da informação:** Técnicas de segurança – Gerenciamento de riscos de segurança da informação. Rio de Janeiro: ABNT, 2019.

ADRIÃO, Milton; GONÇALVES, Sandro Aparecido. Padronização tecnológica, flexibilidade e alinhamento entre áreas de negócios e áreas de tecnologia-práticas de gestão de gerentes de relacionamento de Tecnologia da Informação. **Revista Organizações em Contexto**, v. 12, n. 24, 2016.

BRASIL. **Lei de Acesso a Informação** - **Lei 12.527/11**. Brasilia: Casa Civil, 2011. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 31 nov. 2024.

CAMPOS, Vicente Falconi. **Qualidade total-Padronização de empresas**. São Paulo: Falconi Editora, 2014.

CELEPAR - COMPANHIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO DO PARANÁ**. Wiki GGA**. Curitiba: Celepar, 2024a. Disponível em: https://wiki.gga.celepar.parana. Acesso em: 17 nov. 2024**.**

CELEPAR - COMPANHIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO DO PARANÁ. **Portal ARC - Arquitetura Corporativa do GGA.** Curitiba: Celepar, 2024b. Disponível em: https://arc.gga.celepar.parana/. Acesso em: 19 nov. 2024.

CELEPAR - COMPANHIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO DO PARANÁ. **Meshcentral - Plataforma de Gerenciamento de Dispositivos**. Curitiba: Celepar, 2024c. Disponível em: https://meshcentral.gga.celepar.pr.gov.br/. Acesso em: 20 nov. 2024.

COSTA, Maria Aparecida Alves da; SOARES, Stela Lopes; FLORÊNCIO, Thaís de Sousa. Abordagem quantitativa em pesquisas educacionais: Perspectivas no Programa de Pós-Graduação em Educação da Universidade Federal de Minas Gerais (2017-2019). **DOXA: Revista Brasileira de Psicologia e Educação**, p. e022019-e022019, 2022.

CUNHA, Dalvan; FENATO Marcos Alexandre. A Segurança da informação e a sua importância para a auditoria de sistemas. **Revista Científica Semana Acadêmica**, Fortaleza, ano MMXIII, n. 000029, 2013.

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

DIAS, Andrey Santana da Rocha; SANTOS, Ernani Marques dos; JUNIOR, Antônio Eduardo de Albuquerque. Execução do Plano Diretor de TI em Uma Organização Pública com Gestão de TI Descentralizada. **GESTÃO. Org: Revista Eletrônica de Gestão Organizacional**, v. 21, n. 1, 2023.

FONTES, Edison Luiz Gonçalves. **Políticas de Segurança da Informação**. Rio de Janeiro: RNP/ESR, 2015.

FONTES, Edison Luiz Gonçalves. **Segurança da Informação:** o usuário faz a diferença. São Paulo: Saraiva, 2006.

FONTES, Edison Luiz Gonçalves. **Segurança da informação**. São Paulo: Saraiva Educação SA, 2017.

GOMES FILHO, Antônio Costa et al. Importância do hardware e software em organizações ligadas ao governo eletrônico. **Revista Capital Científico-Eletrônica (RCCe)**, v. 6, n. 1, p. 127-144, 2008.

ISO - INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO 9660:1988 – Information processing:** Volume and file structure of CD-ROM for information interchange. Genebra: ISO, 1988.

KASPERSKY LAB. **Antivírus Kaspersky – Proteção contra ameaças online**. [S. l.]: KASPERSKY LAB, 2024. Disponível em: https://www.kaspersky.com.br/antivirus#. Acesso em: 21 nov. 2024.

MACHADO, Kalleb Ribeiro; CATA PRETA, Kaio Oliviera.; PUNGIRUM, João César Mendel. Segurança da informação para empresas no brasil, **Revista Multidisciplinar do Nordeste Mineiro**, v. 10, 2024.

MICROSOFT. **Windows Server Update Services (WSUS):** Introdução. [S. l.]: Microsoft, 2024. Disponível em: https://learn.microsoft.com/pt-br/windows-server/administration/windows-server-update-services/get-started/windows-server-update-services-wsus. Acesso em: 20 nov. 2024.

MORESI, Eduardo Amadeu Dutra; PINHO, Isabel. Proposta de abordagem para refinamento de pesquisa bibliográfica. **New Trends in Qualitative Research**, v. 9, p. 11-20, 2021.

OCS INVENTORY NG. **Wiki oficial do OCS Inventory NG.** [S. l.]: OCS INVENTORY NG, 2024. Disponível em: https://wiki.ocsinventory-ng.org. Acesso em: 18 nov. 2024.

OLIVEIRA JUNIOR Ilson; SANTOS, Franck Cione Coelho dos**.** Inteligência artificial e policiamento preditivo: possibilidades de inovação tecnológica para a Polícia Militar do Paraná no enfrentamento aos crimes violentos contra o patrimônio com emprego de explosivos. **Brazilian Journal of Technology**, v. 5, n. 1, p. 030–062, 31 mar. 2022.

PARANÁ. **Consulta WSUS - Atualizações e Gerenciamento de Sistemas**. Curitiba: Governo do Estado, 2019. Disponível em: https://consulta.wsus.parana/. Acesso em: 19 nov. 2024

PARANÁ. **Decreto Estadual n.º 7.339, de 8 de junho de 2010**. Regulamento de Serviços Gerais da Polícia Militar do Paraná. Curitiba: [s. n.], 2010.

PARANÁ. Lei nº 20.077, de 18 de dezembro de 2019. Dispõe sobre o Plano Plurianual do Paraná 2020-2023. **Diário Oficial do Estado do Paraná**, n 10.597, 3 jan. 2020. Disponível em: https://www.planejamento.pr.gov.br/sites/default/arquivos_restritos/files/documento/2020-10/lei_ppa_n_20077_ano_2020_2023_final2.pdf. Acesso em: 21 nov. 2024.

PMPR - POLÍCIA MILITAR DO PARANÁ. **Diretriz nº 015/2024-PM/3 – Tecnologia da Informação e comunicação**. Curitiba: PMPR, 2024.

PMPR - POLÍCIA MILITAR DO PARANÁ. **Portaria do Comando-Geral nº 131**. Curitiba: PMPR, 2024.

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

SANSIGOLO, Gabriel. **A importância da série ISO 27000**. [*S. l.: s. n.*]: 2015.

SCHENA, João Claudio; JÚNIOR, Eduil Nascimento. Desafios da Integração Tecnológica e Segurança nas Comunicações Policiais. **RECIMA21-Revista Científica Multidisciplinar,** v. 3, n. 5, p. e351526-e351526, 2022.