

GOVERNANÇA DE TI E PADRONIZAÇÃO: O RISCO DOS SISTEMAS IRREGULARES NA POLÍCIA MILITAR DO PARANÁ

IT GOVERNANCE AND STANDARDIZATION: THE RISK OF IRREGULAR SYSTEMS IN THE MILITARY POLICE OF PARANÁ

Caio de Freitas Almeida¹

RESUMO: O presente artigo analisa os impactos e os riscos do desenvolvimento irregular e não supervisionado de sistemas, fenômeno conhecido como *Shadow IT*, no âmbito da Polícia Militar do Paraná (PMPR). A adoção de soluções tecnológicas à revelia do órgão central competente configura um grave problema institucional, pois pode ferir a lógica administrativa da impessoalidade, gerar passivos técnicos e expor a Corporação a vulnerabilidades cibernéticas e a potenciais violações da Lei Geral de Proteção de Dados (LGPD). Diante dessa problemática, o estudo tem por objetivo central analisar as fragilidades operacionais decorrentes dessa prática e propor um rol de ações aplicáveis de fiscalização, controle e conscientização doutrinária para mitigar o desenvolvimento irregular. Metodologicamente, a pesquisa classifica-se como aplicada e qualitativa, pautada em revisão bibliográfica e na análise documental da Portaria do Comando-Geral nº 131/2024 e da Diretriz nº 015/2024. As análises demonstram que a Corporação dispõe de mecanismos normativos e recursos tecnológicos institucionais destinados à padronização e governança do desenvolvimento de software, restando o desafio de transpor a barreira cultural para garantir a conformidade (*Compliance*). Conclui-se que o enfrentamento ao *Shadow IT* exige a adoção de medidas conjugadas entre a Diretoria de Tecnologia e Inovação (DTI) e as demais unidades da Corporação, tais como o fomento ao desenvolvimento descentralizado regulado, a capacitação de Gestores de TI locais e a inclusão da governança nos currículos de formação, assegurando a interoperabilidade e a continuidade ininterrupta dos serviços policiais.

Palavras-chave: Governança de TI. Segurança da Informação. *Shadow IT*. Polícia Militar do Paraná. Administração Pública.

¹Cargo público: 1º Tenente da Polícia Militar do Paraná. Graduado no Curso de Formação de Oficiais Policiais Militares pela Academia Policial Militar do Guatupê da Polícia Militar do Paraná (2019) – Bacharel em Segurança Pública e Cidadania (Unespar). Graduado em Engenharia Elétrica (Eletrônica/Telecomunicações) pela Universidade Tecnológica Federal do Paraná (2016). Pós-graduado em Gestão Pública pela Faculdade Focus (2024). Pós-graduado em Algoritmos e Estrutura de dados pela Faculdade Focus (2026). Pós-graduado em Desenvolvimento Full Stack, pela Faculdade Focus (2026).

ABSTRACT: This article analyzes the impacts and risks of irregular and unsupervised systems development, a phenomenon known as Shadow IT, within the Military Police of Paraná (PMPR). The adoption of technological solutions without the approval of the competent central organ constitutes a severe institutional problem, as it may violate the administrative logic of impersonality, generates technical liabilities, and exposes the Corporation to cyber vulnerabilities and potential violations of the General Data Protection Law (LGPD). Given this problem, the central objective of this study is to analyze the operational fragilities resulting from this practice and propose a set of applicable inspection, control, and doctrinal awareness actions to mitigate irregular development. Methodologically, the research is classified as applied and qualitative, based on a literature review and the documentary analysis of the General Command Ordinance No. 131/2024 and Guideline No. 015/2024. The analyses demonstrate that the Corporation possesses regulatory mechanisms and institutional technological resources destined for the standardization and governance of software development, leaving the challenge of overcoming the cultural barrier to ensure compliance. It is concluded that combating Shadow IT requires the adoption of joint measures between the Directorate of Technology and Innovation (DTI) and the other units of the Corporation, such as fostering regulated decentralized development, training local IT Managers, and including governance in training curricula, ensuring interoperability and the uninterrupted continuity of police services.

Keywords: IT Governance. Information Security. Shadow IT. Military Police of Paraná. Public Administration.

INTRODUÇÃO

2

A transformação digital no âmbito da Administração Pública tem se consolidado como um pilar estratégico para a garantia da eficiência, da probidade e da continuidade dos serviços prestados à sociedade. No contexto da segurança pública, a Polícia Militar do Paraná (PMPR) reconhece que a adoção de tecnologias da informação transcende o suporte administrativo, caracterizando-se como um elemento crítico de comando, controle e inteligência operacional. Para sustentar e padronizar essa modernização, a Corporação estruturou a sua Governança de Tecnologia da Informação (Governança de TI), conceito que define o alinhamento estratégico entre os recursos tecnológicos e os objetivos da instituição, centralizando as decisões estratégicas na Diretoria de Tecnologia e Inovação (DTI).

Buscando garantir a conformidade (*Compliance*), ou seja, o estrito cumprimento das normas, políticas e controles internos, o Comando-Geral e o Estado Maior da PMPR, juntamente com a DTI, estabeleceram normativas fundamentais, destacando-se a Portaria nº 131/2024 - CG e a Diretriz nº 015/2024 - PM/3. Tais documentos regulamentam os procedimentos relativos à Tecnologia da Informação e Comunicação (TIC) na Corporação, inclusive reforçando, por meio de comunicações oficiais, que qualquer Organização Policial

Militar (OPM) que tenha a intenção de desenvolver novos sistemas deve comunicar previamente a DTI e solicitar orientações técnicas antes de iniciar o projeto.

Apesar da consolidação desse arcabouço normativo e da infraestrutura tecnológica corporativa (que inclui linguagens padronizadas e controle de versionamento), a cultura organizacional frequentemente impõe desafios doutrinários. Depreende-se da necessidade de regulação interna e das pesquisas de Silic e Back (2014) que, motivados por demandas administrativas imediatas, usuários detentores de conhecimentos em desenvolvimento de software tendem a buscar ou criar soluções tecnológicas em ambientes isolados. Aplicando-se esse conceito ao contexto da PMPR, compreende-se que a eventual criação de sistemas não supervisionados configura o cenário que a academia denomina de Shadow IT (Tecnologia da Informação Invisível). A própria edição de normativas de controle por parte do Comando-Geral evidencia a preocupação institucional com esse fenômeno, o qual engloba sistemas, aplicativos ou processos desenvolvidos e utilizados sem o conhecimento, aprovação ou suporte do departamento oficial de tecnologia.

O desenvolvimento de aplicações à margem da supervisão da DTI configura um grave risco à segurança da informação e gera um passivo técnico para a PMPR. Sistemas criados como iniciativas isoladas fora do fluxo institucional não são necessariamente submetidos a práticas de *DevSecOps* (metodologia que integra o Desenvolvimento, a Segurança e as Operações em um ciclo contínuo), tampouco passam por *Code Review* (revisão de código realizada por pares para identificar vulnerabilidades e falhas lógicas antes da implantação). Ademais, a intrínseca rotina de movimentação do efetivo evidencia a fragilidade da continuidade do serviço nesses cenários. Quando o policial desenvolvedor é transferido para outra OPM ou passa para a reserva remunerada, há um alto risco de que o código-fonte perca manutenção regular, o que pode resultar na obsolescência prematura da ferramenta e no consequente desperdício de recursos e esforço humano despendidos.

Diante dessa problemática, o presente artigo tem por objetivo analisar os riscos institucionais, operacionais e de segurança da informação decorrentes do desenvolvimento de software não supervisionado nas OPMs da Polícia Militar do Paraná. Busca-se demonstrar que a inobservância das diretrizes da DTI não representa apenas uma irregularidade técnica, mas uma vulnerabilidade estratégica. Por fim, além de fornecer subsídios teóricos para a conscientização de Oficiais Comandantes, este estudo visa propor ações práticas de controle,

fiscalização e doutrinação por parte da DTI, a fim de mitigar o *Shadow IT* e garantir o cumprimento efetivo da governança tecnológica corporativa.

REFERENCIAL TEÓRICO

Governança de TI, Compliance e a Administração Pública

Para compreender a importância da padronização tecnológica, faz-se necessário, primeiramente, desmistificar o conceito de governança. Em seu sentido mais amplo, a governança corporativa pode ser definida como o sistema pelo qual as organizações são dirigidas, monitoradas e incentivadas, envolvendo o relacionamento entre gestores, conselhos e demais partes interessadas (IBGC, 2015). Trazendo este conceito para o universo tecnológico, Fernandes e Abreu (2014) destacam que a Governança de Tecnologia da Informação (Governança de TI) surge não como a gestão diária de infraestrutura e redes, mas como um mecanismo de direção estratégica e controle.

Em termos práticos, a Governança de TI assegura que os recursos tecnológicos e os sistemas desenvolvidos estejam estritamente alinhados à missão e aos objetivos operacionais da instituição. Segundo a clássica definição de Weill e Ross (2006), a Governança de TI consiste em definir claramente os direitos de decisão e as responsabilidades dentro da organização. Em outras palavras, trata-se de estabelecer, de forma oficial, quem possui a autoridade para decidir sobre a criação ou aquisição de novas tecnologias e quem responderá pelo sucesso, segurança e manutenção dessas soluções, evitando que ações isoladas ocorram sem o conhecimento do setor competente.

A necessidade de implementar a Governança de TI nas organizações pode ser compreendida sob a ótica da Teoria da Agência (JENSEN, MECKLING, 1976). No contexto corporativo, essa teoria explora os conflitos de interesse que surgem quando as decisões tomadas pelos executores (agentes) divergem dos objetivos estratégicos dos proprietários ou da alta direção (principal). Transpondo essa lente teórica para a administração pública e, mais especificamente, para o ambiente policial militar, observa-se que o "principal" é o Estado, representado pelo Comando-Geral, cujo objetivo primordial é a segurança institucional, a impessoalidade e a otimização dos recursos públicos. Em contrapartida, o "agente" pode ser figurado pelo policial desenvolvedor na ponta da linha (OPM), cujo interesse primário, embora bem-intencionado, foca na resolução imediata de um gargalo administrativo local.

Quando não há mecanismos rígidos de governança, a assimetria de informações prevalece, uma vez que o Comando desconhece quais sistemas estão em funcionamento em unidades sob sua responsabilidade e quais vulnerabilidades esses sistemas abrigam. Portanto, a Governança de TI atua justamente como o mecanismo de controle e alinhamento que mitiga esse conflito de agência, garantindo que o esforço tecnológico do policial na base atenda aos requisitos de segurança e continuidade exigidos pelo Comando.

No contexto da Administração Pública, e particularmente em uma instituição de Estado como a Polícia Militar do Paraná (PMPR), a aplicação da Governança de TI transcende a busca corporativa por resultados financeiros, configurando-se como um instrumento para assegurar o cumprimento dos preceitos constitucionais. O art. 37 da Constituição Federal de 1988 preconiza que a Administração Pública orienta-se, entre outros, pelos princípios da legalidade, impessoalidade, moralidade e eficiência. A ausência de um direcionamento padronizado na área de tecnologia pode fragilizar o atendimento a esses mandamentos.

Neste estudo, destaca-se a relação íntima entre a governança de software e o princípio da impessoalidade. É comum que esse princípio seja associado majoritariamente ao tratamento isonômico que o Estado deve dispensar a todos os cidadãos. Contudo, a renomada jurista Maria Sylvia Zanella Di Pietro (2022) ensina que a impessoalidade possui uma segunda vertente fundamental, voltada à própria Administração: os atos e realizações administrativo-governamentais são imputados ao ente estatal, e não à pessoa física do agente público que os executa.

5

Fazendo uma correlação dos ensinamentos de Di Pietro (2022) com o contexto tecnológico trabalhado neste artigo, compreende-se que uma aplicação criada por um policial militar, em horário de expediente e para suprir uma demanda da Corporação, é patrimônio intelectual e material do Estado. Quando esse desenvolvimento ocorre de forma isolada, sem documentação, sem linguagem padronizada e sem o uso dos repositórios oficiais da Diretoria de Tecnologia e Inovação (DTI), o sistema torna-se dependente exclusivamente do seu criador. Essa personalização da ferramenta pode comprometer a impessoalidade, pois atrela a continuidade de um serviço público à figura de um único militar. Da mesma forma, a eficiência institucional é mitigada devido ao risco de retrabalho e ao desperdício de recursos inerentes a projetos que não podem ser compartilhados ou sustentados pela Corporação de maneira uniforme.

Conforme lecionam Candeloro, Rizzo e Pinho (2012), o termo *Compliance* origina-se do verbo inglês *to comply*, o qual significa agir de acordo com uma regra, uma instrução interna ou um comando legal. No setor público, a conformidade está intimamente ligada ao dever de prestação de contas. Esse conceito é amplamente debatido na literatura administrativa sob o termo *accountability* (CAMPOS, 1990). Não basta apenas que a organização siga as normas vigentes. É estritamente necessário que ela possua mecanismos sistêmicos capazes de comprovar essa obediência em eventuais processos de auditoria.

Quando uma Organização Policial Militar desenvolve uma solução tecnológica à margem da governança oficial, ela inviabiliza a rastreabilidade das ações. A Diretoria de Tecnologia e Inovação perde a capacidade de auditar como os dados operacionais são manipulados e quem possui acesso a eles. Dessa forma, a centralização em repositórios corporativos funciona como uma ferramenta de proteção jurídica para o próprio gestor público. O uso do ambiente padronizado garante que todas as etapas de criação e modificação do software sejam registradas, tornando o processo de desenvolvimento totalmente transparente e rastreável perante os órgãos de controle interno e externo da Corporação.

Para materializar a Governança de TI e garantir a conformidade (*Compliance*), as organizações utilizam estruturas de trabalho pré-definidas e consolidadas no mercado global, chamadas de *frameworks*. Um *framework*, nesse contexto, funciona como um modelo de referência ou uma coleção de boas práticas já testadas internacionalmente, poupando a administração pública de criar metodologias de controle a partir do zero. Dentre os mais relevantes adotados no setor público, destacam-se:

I. COBIT (*Control Objectives for Information and Related Technologies*): É um modelo focado na governança e na alta gestão (ISACA, 2019). Ele auxilia diretores e detentores de cargos de gerência ou comando a garantirem que os investimentos em TI realmente tragam valor para a instituição e que os riscos operacionais (como vazamento de dados ou falhas de segurança) estejam mapeados e controlados. O COBIT orienta o que a organização precisa governar.

II. ITIL (*Information Technology Infrastructure Library*): Enquanto o COBIT foca na direção estratégica, o ITIL é um modelo voltado para a operação diária e para o gerenciamento de serviços (AXELOS, 2019). Ele fornece um guia prático de como a TI deve agir para garantir que os sistemas funcionem com qualidade, estabelecendo padrões para o suporte, resolução de incidentes e manutenção contínua das aplicações.

Dessa forma, a integração de diretrizes baseadas nesses modelos de referência pode contribuir significativamente para organizar a inovação tecnológica dentro da PMPR. O objetivo da adoção de tais parâmetros e boas práticas não seria suprimir a proatividade técnica nas OPMs, mas sim fornecer um alicerce sólido para garantir que toda solução desenvolvida esteja alinhada às normativas vigentes, protegendo o patrimônio do Estado e assegurando a continuidade ininterrupta do serviço policial militar.

O Fenômeno do *Shadow IT* e os Riscos à Segurança da Informação

A busca por eficiência e celeridade na resolução de problemas administrativos e operacionais frequentemente impulsiona os usuários a buscarem alternativas tecnológicas por conta própria. Quando essas iniciativas ocorrem à margem das políticas institucionais e sem o conhecimento do setor competente, configura-se o cenário que a literatura especializada denomina de *Shadow IT* (Tecnologia da Informação Invisível). Segundo Silic e Back (2014), o *Shadow IT* compreende sistemas, aplicativos, serviços em nuvem ou processos tecnológicos desenvolvidos, implantados e utilizados por departamentos ou indivíduos sem a aprovação, o suporte ou a supervisão do departamento oficial de Tecnologia da Informação da organização.

Estudos dedicados à governança corporativa, a exemplo da pesquisa de Silic e Back (2014), demonstram que o surgimento do *Shadow IT* não decorre, em regra, de má-fé. Transpondo essa premissa teórica para a realidade da PMPR, infere-se que o fenômeno tem origem no ímpeto de proatividade de policiais militares que, detentores de conhecimentos em programação, buscam suprir lacunas imediatas ou otimizar rotinas locais, a exemplo de controle de escalas, gestão de frota ou tramitação de documentos. Contudo, ao contornar as diretrizes da Diretoria de Tecnologia e Inovação (DTI), essas soluções criadas à revelia transformam-se em vulnerabilidades estratégicas.

O primeiro e mais crítico impacto dessa prática irregular recai sobre a Segurança da Informação. Soluções desenvolvidas fora do ambiente homologado pela instituição não são necessariamente submetidas às esteiras de *DevSecOps*, acrônimo em inglês para Desenvolvimento, Segurança e Operações. Essa prática consiste em uma cultura de engenharia de software voltada a integrar requisitos de segurança em todas as fases do desenvolvimento (GARTNER, 2021).

Consequentemente, sistemas isolados tendem a não passar por revisões de código estruturadas (*Code Review*) ou por testes de vulnerabilidade (*Penetration Tests*). Para Pressman

(2016), a revisão de código é um processo de controle de qualidade no qual pares examinam detalhadamente o trabalho do desenvolvedor para encontrar erros lógicos e falhas de padronização antes da entrega final do software. Por sua vez, o Instituto Nacional de Padrões e Tecnologia dos Estados Unidos (NIST, 2008) define o teste de intrusão como uma simulação controlada de ataques cibernéticos reais, possuindo o objetivo de identificar e explorar brechas de segurança em um sistema. A ausência da aplicação rotineira dessas duas práticas, conforme alerta Pressman (2016), reduz a capacidade de identificação preventiva de vulnerabilidades e falhas na implementação. A esse respeito, o Projeto Aberto de Segurança em Aplicações Web (OWASP, 2021) aponta, em sua lista das dez categorias de riscos mais críticos para aplicações web, que a exposição de credenciais diretamente no código-fonte e as falhas gerais de criptografia na proteção de dados sensíveis configuram vulnerabilidades recorrentes que podem facilitar o vazamento de informações operacionais.

Conforme adverte Fontes (2022) em suas análises sobre governança e gestão de riscos, o acúmulo dessas vulnerabilidades, inerente aos sistemas desenvolvidos fora do controle central, pode expor a Corporação a riscos severos de incidentes cibernéticos e vazamento de dados sensíveis. Considerando que a PMPR lida diariamente com bases de dados críticas, destacando-se principalmente informações sigilosas e operacionais da própria Corporação, bem como os dados pessoais de seu efetivo, o desenvolvimento não supervisionado pode confrontar as exigências da Lei Geral de Proteção de Dados Pessoais (LGPD – Lei nº 13.709/2018). Um caso de um incidente de segurança em um sistema não oficial, pode ampliar a exposição da instituição e dos agentes a consequências administrativas e jurídicas pela ausência de conformidade(*Compliance*) prévia.

A título de aprofundamento, o artigo 6º da Lei Geral de Proteção de Dados (BRASIL, 2018) estabelece princípios basilares para o tratamento de dados, dentre os quais destacam-se a segurança e a prevenção. O princípio da segurança impõe a utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas. Simultaneamente, o princípio da prevenção exige a adoção de medidas prévias para evitar a ocorrência de danos em virtude do tratamento de dados.

O desenvolvimento de software fora dos padrões estabelecidos atenta contra ambos os princípios. Ao hospedar bancos de dados em máquinas locais ou em provedores de nuvem não homologados pela Corporação, a OPM perde a capacidade de aplicar as políticas institucionais de criptografia, controle de *logs* de acesso e rotinas de *backup* corporativo. E ainda, numa hipótese

na qual haja vazamento, a Corporação enfrentará severas dificuldades para rastrear a origem do incidente e mitigar os danos.

Além das ameaças cibernéticas, o Shadow IT gera o que a literatura de engenharia de software denomina de dívida técnica. Conforme definem Kruchten, Nord e Ozkaya (2012), a dívida técnica representa o custo futuro e invisível do retrabalho, causado pela adoção de soluções tecnológicas rápidas, limitadas e não padronizadas no presente, em detrimento de uma abordagem estruturada. No contexto da PMPR, essa dívida compromete diretamente a continuidade do serviço. Conforme debatido anteriormente sob a ótica do princípio da impessoalidade, um sistema desenvolvido e hospedado localmente depende do conhecimento tácito do seu criador. Devido à intrínseca rotina de movimentação de efetivo na carreira militar, seja por transferência de local de trabalho, readequação de funções ou passagem para a reserva, há um alto risco de que a ferramenta perca sua manutenção regular.

Sem documentação técnica adequada e sem o uso de repositórios de versionamento de código padronizados e acessíveis à DTI, o sistema torna-se incompreensível para terceiros. Quando o policial desenvolvedor se ausenta, a OPM perde a capacidade de atualizar, corrigir erros ou evoluir a aplicação. Em situações ainda mais críticas, nas quais a unidade já desenvolveu forte dependência do sistema para o andamento de suas atividades rotineiras, a Diretoria de Tecnologia e Inovação acaba sendo acionada para intervir. Nestes casos, a DTI despende tempo, esforço e recursos valiosos apenas para realizar a engenharia reversa e tentar compreender a lógica de um sistema não padronizado, visando uma possível manutenção emergencial. O resultado prático é a obsolescência prematura da solução tecnológica e um evidente desperdício de recursos públicos.

Padrões de Desenvolvimento, DevSecOps e a Centralização do Código

Para mitigar os riscos inerentes ao *Shadow IT* e assegurar a continuidade dos serviços prestados pelas OPMs, a literatura e as melhores práticas de mercado apontam para a adoção rigorosa de padrões de desenvolvimento e para a centralização do código-fonte. Atualmente, a Diretoria de Tecnologia e Inovação (DTI) já dispõe de um padrão arquitetônico definido para a corporação, priorizando tecnologias como React para o desenvolvimento de interfaces de usuário (*frontend*), PHP com o *framework* Laravel para a lógica de negócio (*backend*) e PostgreSQL para o gerenciamento de banco de dados. A imposição dessa *stack* tecnológica institucional não visa engessar a criatividade do desenvolvedor, mas sim favorecer condições

de que a solução tecnológica seja escalável, auditável e passível de manutenção por qualquer outro profissional da área técnica da Instituição.

A padronização da *stack* tecnológica aliada a definições de interfaces, mecanismos de autenticação e requisitos de segurança transcende a mera organização de infraestrutura. Ela atua como o alicerce para a interoperabilidade sistêmica, conceito definido legalmente pela Lei que dispõe sobre princípios, regras e instrumentos para o Governo Digital (Lei nº 14.129/2021) como a capacidade de sistemas e organizações operarem entre si, de modo a garantir a troca de informações e de dados de forma segura e eficiente (BRASIL, 2021).

Conforme alertam Laudon e Laudon (2014) em suas análises sobre sistemas de informação, o desenvolvimento de soluções isoladas e sem padronização resulta na adoção de arquiteturas de dados heterogêneas, variando desde planilhas eletrônicas até bancos de dados locais não relacionais. Os referidos autores explicam que essa falta de integração arquitetônica cria as chamadas ilhas de informação ou silos de dados. Esse fenômeno organizacional impede que as informações coletadas por uma unidade sejam cruzadas ou consumidas por sistemas de outras unidades ou pelo Alto Comando. Ao adotar o uso do PostgreSQL e de arquiteturas padronizadas no backend (PHP e Laravel), a DTI favorece o uso de Interfaces de Programação de Aplicações (APIs) seguras. Consequentemente, viabiliza-se o cruzamento de dados de inteligência, o compartilhamento de estatísticas operacionais e a consolidação de painéis gerenciais (dashboards) precisos para a tomada de decisão estratégica da Corporação.

10

Outro pilar fundamental dessa padronização arquitetônica refere-se ao controle de acesso e identidade. Os sistemas desenvolvidos sob as diretrizes da DTI integram-se a um mecanismo de autenticação centralizada, conceito conhecido tecnicamente como Single Sign-On (SSO). Segundo Stallings (2015), o SSO é um processo de controle de acesso que permite ao usuário autenticar-se apenas uma vez no ambiente computacional e, a partir desse login inicial, obter acesso autorizado a múltiplos sistemas e aplicativos independentes sem a necessidade de novas verificações. Na prática, essa característica garante que o ingresso nas aplicações seja realizado exclusivamente com as credenciais institucionais do militar, utilizando o mesmo sistema de autenticação para todo o ecossistema oficial. Consequentemente, ao realizar o acesso inicial na intranet da PMPR, o usuário obtém ingresso seguro e fluido a todos os outros sistemas padronizados, sem a necessidade de múltiplos logins. Essa centralização pode reduzir significativamente o risco de vazamento de credenciais, evita a criação de bancos de

senhas isolados e vulneráveis nas OPMs e possibilita a rastreabilidade e a auditoria de quem acessou cada informação.

A principal ferramenta tecnológica para viabilizar a centralização da codificação, por sua vez, é o sistema de controle de versão. De acordo com Chacon e Straub (2014), sistemas modernos de versionamento, como o Git, aliados a plataformas de gerenciamento colaborativo, permitem o rastreamento detalhado de todas as alterações realizadas no código de um software ao longo do tempo. Na PMPR, essa gestão materializa-se por meio do uso da plataforma GitLab, hospedada em um domínio institucional e com acesso restrito mediante o uso das próprias credenciais corporativas do efetivo. Quando o código-fonte de um aplicativo criado em uma OPM é armazenado nesse repositório oficial, o conhecimento técnico deixa de residir exclusivamente na mente do seu criador e passa a integrar o patrimônio tecnológico da Corporação.

Além de reter o conhecimento, a centralização do código em repositórios institucionais é o pré-requisito técnico fundamental para a evolução rumo à cultura *DevSecOps*. Em um ambiente com código centralizado e governado, abre-se caminho para a implementação de esteiras automatizadas de CI/CD, sigla em inglês para Integração Contínua e Entrega Contínua. Na prática, trata-se de processos sistêmicos que testam e empacotam o código de forma automatizada a cada nova atualização submetida pelo programador. Essa estrutura permite realizar varreduras em busca de vulnerabilidades e validar o funcionamento da aplicação em um ambiente de homologação, ou seja, um cenário de testes seguro e apartado do sistema real, antes que o software entre efetivamente em ambiente de produção para uso oficial rotineiro.

11

Outro pilar de segurança e qualidade propiciado pelo versionamento centralizado no GitLab é a viabilidade da revisão de código por pares (*Code Review*). Em um fluxo de trabalho governado, o código escrito por um policial em sua respectiva unidade não precisa ser publicado diretamente. Ao ser submetido ao repositório da corporação, cria-se a possibilidade de que analistas da DTI, ou outros desenvolvedores, avaliem previamente a qualidade da programação, a conformidade com as regras de negócio e a ausência de brechas de segurança.

Na Polícia Militar do Paraná, a infraestrutura tecnológica básica para a recepção, versionamento e padronização de sistemas já se encontra estabelecida. Dessa forma, o desafio atual transcende a aquisição de novas ferramentas tecnológicas, residindo na consolidação de uma doutrina que compreenda o uso da arquitetura oficial da DTI não como uma mera opção

administrativa, mas como um mecanismo indispensável de controle, padronização e proteção institucional.

O Arcabouço Normativo Tecnológico da PMPR

A governança corporativa e a mitigação dos riscos tecnológicos na Polícia Militar do Paraná não se apoiam apenas em boas práticas de mercado, mas estão solidamente fundamentadas em um arcabouço normativo institucional recente e rigoroso. Reconhecendo a criticidade da Tecnologia da Informação e Comunicação (TIC) para a segurança e a eficiência das operações, a atual Diretoria de Tecnologia e Inovação (DTI), denominada à época da edição das normas como Diretoria de Desenvolvimento Tecnológico e Qualidade (DDTQ), elaborou um conjunto de regulamentações, devidamente publicadas e chanceladas pelo Comando-Geral e pelo Estado-Maior da PMPR, que centralizam e disciplinam o uso e o desenvolvimento de soluções tecnológicas na Corporação.

O pilar central dessa estruturação é a Portaria do Comando-Geral nº 131, de 2 de fevereiro de 2024. Para resguardar o patrimônio intelectual, a segurança da informação e garantir o efetivo controle sobre o ambiente tecnológico, a norma é categórica ao definir a propriedade dos sistemas e a proibição de iniciativas paralelas. Tais determinações encontram-se expressas em seus artigos 21 e 22 (PARANÁ, 2024):

Art. 21. A PMPR, por meio da DDTQ, é a detentora de todos os sistemas desenvolvidos e em contínua utilização na Corporação, podendo, a critério do Comandante-Geral, ser delegada essa atribuição.

Art. 22. São vedados o uso ou implantação de qualquer recurso de TIC, no âmbito da Corporação, sem a devida ciência, avaliação e aprovação da DDTQ.

Embora o termo "recurso de TIC" abranja de maneira ampla os equipamentos físicos, computadores e ativos de rede, é fundamental esclarecer que os softwares e sistemas desenvolvidos internamente são igualmente classificados como recursos tecnológicos. Dessa forma, essa vedação legal atinge a prática do desenvolvimento despadronizado e isolado nas Organizações Policiais Militares (OPMs).

Complementando a Portaria, a Diretriz nº 015/2024 materializa as regras técnicas e administrativas para o fluxo de sistemas, softwares e suporte. Em sua seção 3.7.5, que trata especificamente do desenvolvimento de software, a Diretriz formaliza a propriedade intelectual do Estado sobre as aplicações e classifica os sistemas criados no âmbito da PMPR em duas categorias distintas: o software institucional e o software irregular.

A definição normativa de "software irregular" traduz com exatidão o fenômeno do *Shadow IT* descrito pela literatura acadêmica. A Diretriz o define como todo programa que, mesmo desenvolvido, mantido e suportado pelos órgãos da PMPR, não atende aos requisitos da norma ou não possui o devido registro de homologação. Em uma demonstração clara da preocupação institucional ao risco gerado por essas práticas, a alínea "d" da referida seção é contundente ao determinar a interrupção dessas ferramentas (PARANÁ, 2024):

d) os softwares desenvolvidos sem a observância desta Diretriz serão classificados como irregulares e devem ser interrompidos imediatamente;

Para que um sistema saia da irregularidade e seja elevado à categoria de software institucional, a norma exige o cumprimento de requisitos estritos de homologação. Esses critérios incluem a obtenção de parecer favorável do diretor da DTI e a priorização do Chefe do Estado-Maior da Corporação. Reforçando o rigor do controle central, a Diretriz estabelece, na alínea "i" da mesma seção, o veto absoluto a qualquer atuação à revelia do órgão técnico (PARANÁ, 2024):

i) ficam vedadas quaisquer iniciativas ou continuidade de desenvolvimento, bem como a disponibilização de software ou recursos em servidores corporativos, sem a anuência e acompanhamento prévio e explícito da DDTQ.

Fica evidente, portanto, que a Polícia Militar do Paraná já possui o amparo regulamentar necessário para coibir o desenvolvimento isolado e as vulnerabilidades dele decorrentes. O desafio premente não é a criação de novas regras, mas sim a consolidação de uma cultura de conformidade. Faz-se necessário garantir que o efetivo e, sobretudo, os Oficiais Comandantes das OPMs compreendam e façam cumprir essas normativas, abandonando a aceitação tácita de sistemas irregulares locais em prol de uma governança tecnológica centralizada, impessoal e segura.

METODOLOGIA

Para o alcance dos objetivos propostos, o presente estudo caracteriza-se como uma pesquisa de natureza aplicada e com abordagem qualitativa. A escolha por essa tipologia justifica-se pela necessidade de compreender um fenômeno organizacional complexo, o *Shadow IT* nas Organizações Policiais Militares (OPMs), e de propor soluções práticas baseadas na centralização e na governança tecnológica para a Polícia Militar do Paraná (PMPR).

Do ponto de vista dos procedimentos técnicos, a investigação foi estruturada em duas frentes complementares. A primeira frente consistiu em uma revisão bibliográfica de caráter

exploratório e descritivo. Para tanto, foram consultadas obras de referência nacional e internacional, artigos científicos e diretrizes de institutos globais de tecnologia (como ISACA e Gartner). Essa etapa permitiu o embasamento de conceitos fundamentais como Governança de Tecnologia da Informação, conformidade (*Compliance*), riscos de segurança cibernética e cultura *DevSecOps*.

A segunda frente pautou-se na pesquisa documental, concentrando-se na análise minuciosa do arcabouço normativo interno da PMPR vigente. Foram objetos de estudo detalhado a Portaria do Comando-Geral nº 131, de 2 de fevereiro de 2024, e a Diretriz nº 015/2024 da 3ª Seção do Estado-Maior da PMPR. A análise desses documentos oficiais possibilitou a identificação das regras de propriedade de software, os critérios de homologação e a vedação explícita ao desenvolvimento de sistemas à revelia do órgão de tecnologia.

Por fim, o cruzamento dos dados obtidos na revisão bibliográfica com a análise documental permitiu a elaboração de uma correlação direta entre os riscos teóricos do desenvolvimento não supervisionado e a realidade operacional da Corporação. Essa triangulação de informações formou a base necessária para a formulação de proposições que visam conscientizar Oficiais Comandantes e fortalecer o cumprimento da governança tecnológica no ambiente policial militar.

ANÁLISE E PROPOSIÇÕES PRÁTICAS PARA A GOVERNANÇA TECNOLÓGICA

O Desafio Cultural e as Iniciativas de Conformidade

A análise do arcabouço normativo da PMPR demonstra que a Corporação possui as ferramentas jurídicas e tecnológicas necessárias para centralizar o desenvolvimento de software. No entanto, a emissão de orientações normativas pela DTI sugere que mitigar o Shadow IT representa um desafio essencialmente cultural e doutrinário. A norma internacional ISO/IEC 38500 e os teóricos Weill e Ross (2006) corroboram essa premissa ao definirem o comportamento humano e o estímulo a atitudes desejáveis como o foco central da governança tecnológica. Nesse contexto, infere-se que a urgência por soluções administrativas locais, aliada à proatividade da tropa, possa ofuscar a percepção dos riscos institucionais por parte do efetivo.

Ciente dessa assimetria entre a norma e a prática, a Diretoria de Tecnologia e Inovação (DTI) tem iniciado um movimento de conscientização ativa. Um exemplo claro dessa

mudança de postura é a veiculação de comunicados institucionais na intranet da Corporação, voltados diretamente aos gestores das unidades. O texto de uma dessas publicações recentes ilustra a tentativa de alinhar as expectativas e centralizar as demandas:

Aos excelentíssimos senhores diretores e ilustríssimos comandantes, Com base nas diretrizes da Portaria nº 131/2024 - CG e da Diretriz nº 015/2024 - DTI, reforçamos a importância do alinhamento tecnológico em nossa instituição. Caso sua unidade tenha a intenção de desenvolver novos sistemas, solicitamos que: Comunique previamente a Diretoria de Tecnologia e Inovação (DTI). Solicite orientações técnicas antes de iniciar o projeto.

Essa comunicação representa um passo importante. Contudo, a literatura de Governança de TI aponta que apenas a recomendação passiva pode ser insuficiente para mitigar o desenvolvimento irregular. Faz-se necessária a adoção de um conjunto de ações enérgicas de conscientização, incentivo e controle estruturado.

Proposições para a Conscientização e Doutrina do Efetivo

O sucesso da implantação da governança tecnológica depende intrinsecamente da mudança de cultura e do reconhecimento das boas práticas. É fundamental que as instâncias de comando compreendam que autorizar o desenvolvimento de um sistema isolado em sua unidade não constitui uma inovação administrativa, mas sim a assunção de um risco institucional severo.

15

Para concretizar essa mudança de mentalidade, propõem-se as seguintes ações:

Inclusão Curricular e Capacitação: Inserir a disciplina de Governança de TI e Segurança da Informação nos currículos dos cursos de formação, aperfeiçoamento e especialização de oficiais, bem como nos cursos de formação de praças. O objetivo é criar uma doutrina de segurança cibernética consolidada desde a base até o Alto Comando.

1. Política de Incentivo e Reconhecimento Profissional (Meritocracia): A cultura militar é fortemente pautada pelo reconhecimento. Sugere-se a criação de diretrizes que recompensem formalmente (por meio de referências elogiosas ou outros mecanismos formais de valorização) os policiais militares que desenvolverem soluções tecnológicas seguindo o rito de homologação da DTI. Transformar a conformidade em um critério de destaque profissional incentiva o abandono das práticas isoladas.

Responsabilização Administrativa: Esclarecer, por meio de instruções normativas complementares, que o endosso a softwares irregulares pode gerar responsabilidade solidária do

comandante da OPM em caso de incidentes cibernéticos, vazamento de dados corporativos ou paralisação de serviços essenciais.

Medidas Práticas de Fiscalização, Controle e Inovação Colaborativa

Além da conscientização, a Diretoria de Tecnologia e Inovação pode manter um protagonismo técnico e fiscalizatório, atuando de forma preventiva para neutralizar focos de *Shadow IT*, ao mesmo tempo em que fomenta a inovação de forma segura. Para tanto, sugere-se a implementação e a expansão das seguintes medidas práticas:

Fortalecimento do Modelo de Desenvolvimento Descentralizado Regulado: É imperativo reconhecer e expandir uma prática já em fase inicial de adoção pela DTI, na qual policiais lotados em OPMs diversas são autorizados a desenvolver soluções para suas unidades, desde que cumpram estritamente as regras do órgão central. Esse modelo deve ser institucionalizado em larga escala, garantindo que o programador local utilize a *stack* oficial (React, PHP/Laravel, PostgreSQL) e escreva o código diretamente no repositório corporativo (GitLab), submetendo seu trabalho à auditoria prévia.

I. Disponibilização de Ambientes de Homologação: Para facilitar a aderência às regras, a DTI poderia fornecer instâncias isoladas e seguras (ambientes de testes ou homologação) para que os desenvolvedores das OPMs possam prototipar e testar seus sistemas sem riscos à rede principal. Uma vez validada a utilidade e a segurança do código, o sistema seria migrado para o ambiente de produção oficial.

II. Empoderamento dos Gestores TI locais: A Diretriz nº 015/2024 prevê a atuação técnica e o controle de ativos nas unidades, função hoje consolidada institucionalmente sob a figura do Gestor TI. Propõe-se que esses militares recebam treinamento de nivelamento para atuarem não apenas no suporte local, mas como embaixadores da governança. Eles seriam os agentes de primeira linha encarregados de identificar e reportar a criação de bancos de dados ou servidores web não autorizados em sua respectiva área de responsabilidade.

III. Aprimoramento da Comunicação Institucional: Considerando que a mudança de cultura organizacional é um processo gradual, sugere-se a continuidade e o aprimoramento dos comunicados periódicos publicados na intranet da PMPR. A veiculação frequente de informativos, cartilhas de boas práticas de segurança e estudos de caso de sucesso sobre sistemas padronizados reforça a doutrina, mantendo a necessidade de governança sempre em evidência para os comandantes e para a tropa.

IV. Auditoria Ativa de Redes: Caso haja viabilidade e recursos técnicos disponíveis, sugere-se que a DTI estude a adoção de rotinas de monitoramento na infraestrutura da intranet corporativa. O emprego dessa prática, ou de outros métodos automatizados de mapeamento de aplicações, permitiria identificar tráfego atípico e serviços executados fora do *Data Center* oficial, viabilizando o bloqueio preventivo de portas lógicas utilizadas por soluções não homologadas.

Por meio dessas ações combinadas, a Polícia Militar do Paraná poderá transcender a teoria da Governança de TI, transformando suas diretrizes em práticas concretas que resguardem a segurança institucional e promovam uma inovação responsável e colaborativa.

CONCLUSÃO

A incessante busca por eficiência administrativa e operacional no âmbito da segurança pública não pode prescindir do rigor e do controle sobre os recursos tecnológicos. O presente estudo demonstrou que a prática do desenvolvimento não supervisionado de sistemas, caracterizada na literatura acadêmica como *Shadow IT* e normatizada internamente como "software irregular", representa um risco elevado para a Polícia Militar do Paraná (PMPR). Sistemas desenvolvidos de forma isolada nas Organizações Policiais Militares (OPMs) podem comprometer a lógica administrativa da impessoalidade e da eficiência, além de exporem a Corporação a vulnerabilidades de segurança cibernética e desrespeitarem a legislação referente a proteção de dados (LGPD).

Respondeu-se, ao longo da pesquisa, à indagação sobre como a implementação de diretrizes de Governança de TI pode mitigar tais riscos. A análise indica que a centralização do código-fonte em repositórios oficiais, associada à utilização de uma *stack* tecnológica padronizada e a práticas de *DevSecOps*, atua como condição facilitadora para a preservação do capital intelectual da Corporação. Essas ferramentas asseguram que o conhecimento tecnológico não se perca com a inevitável movimentação do efetivo, viabilizando a continuidade e resiliência dos serviços e proporcionando um ambiente auditável para manutenções e evoluções dos sistemas.

Constatou-se, mediante a análise da Portaria do Comando-Geral nº 131/2024 e da Diretriz nº 015/2024, que a Diretoria de Tecnologia e Inovação (DTI) já estabeleceu um sólido e moderno arcabouço normativo para disciplinar a Tecnologia da Informação. Destarte, conclui-se que o desafio contemporâneo da Instituição não reside na carência de amparo legal

ou na ausência de infraestrutura tecnológica, mas sim na imposição de uma profunda mudança na cultura organizacional, com foco irrestrito na conformidade (*Compliance*).

As ações propostas nesta pesquisa, voltadas à inclusão da governança nos currículos de formação, à valorização meritocrática do desenvolvedor padronizado, ao empoderamento do Gestor TI local e à criação de ambientes seguros para prototipação, oferecem um roteiro exequível para alinhar a proatividade da tropa à segurança corporativa. O modelo de "desenvolvimento descentralizado regulado", já iniciado pela DTI, ratifica que o alinhamento central não impede a inovação, mas a canaliza em benefício do Estado.

Cumprе salientar que o presente estudo apresenta limitações metodológicas decorrentes de seu caráter estritamente documental e bibliográfico. A ausência de uma pesquisa de campo empírica, voltada a mensurar quantitativamente o volume de softwares irregulares ativos ou a mapear de forma estatística a percepção individual dos comandantes das unidades locais, restringe as conclusões ao plano das inferências e das análises regulamentares. Ademais, dada a velocidade das transformações tecnológicas e das reestruturações administrativas, o modelo de governança proposto limita-se ao cenário normativo vigente na Corporação, podendo demandar futuras revisões estruturais diante do surgimento de novas plataformas ou demandas operacionais na segurança pública.

18

Conclui-se que o sucesso na mitigação do desenvolvimento irregular requer o envolvimento direto dos Oficiais Comandantes. Somente com a compreensão do Comando e com a fiscalização sistemática por parte da DTI, a PMPR consolidará a sua transformação digital de maneira segura, garantindo que a tecnologia cumpra o seu papel constitucional de servir de suporte seguro e impessoal para as atividades de preservação da ordem pública.

REFERÊNCIAS

ABNT. ABNT NBR ISO/IEC 38500: **Governança corporativa de tecnologia da informação**. Rio de Janeiro: ABNT, 2018.

AXELOS. **ITIL Foundation: ITIL 4 Edition**. London: TSO, 2019.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União**, Brasília, DF, 15 ago. 2018.

BRASIL. Lei nº 14.129, de 29 de março de 2021. Dispõe sobre princípios, regras e instrumentos para o Governo Digital. **Diário Oficial da União**, Brasília, DF, 30 mar. 2021.

CAMPOS, A. M. Accountability: quando poderemos traduzi-la para o português? **Revista de Administração Pública**, Rio de Janeiro, v. 24, n. 2, p. 30-50, 1990.

CANDELORO, A. P.; RIZZO, M. B. M.; PINHO, V. **Compliance 360º**: riscos, estratégias, conflitos e vaidades no mundo corporativo. São Paulo: Trevisan Editora, 2012.

CHACON, S.; STRAUB, B. **Pro Git**. 2. ed. New York: Apress, 2014.

DI PIETRO, M. S. Z. **Direito Administrativo**. 35. ed. Rio de Janeiro: Forense, 2022.

FERNANDES, A. A.; ABREU, V. F. **Implantando a Governança de TI**: da estratégia à gestão de processos. 4. ed. Rio de Janeiro: Brasport, 2014.

FONTES, E. **Segurança da Informação**: Gestão e Governança. Rio de Janeiro: Brasport, 2022.

GARTNER. **Gartner Glossary: DevSecOps**. Stamford: Gartner, 2021.

IBGC. Instituto Brasileiro de Governança Corporativa. **Código das Melhores Práticas de Governança Corporativa**. 5. ed. São Paulo: IBGC, 2015.

ISACA. **COBIT 2019 Framework: Introduction and Methodology**. Schaumburg: ISACA, 2019.

JENSEN, M. C.; MECKLING, W. H. Theory of the firm: Managerial behavior, agency costs and ownership structure. **Journal of Financial Economics**, v. 3, n. 4, p. 305-360, 1976.

KRUCHTEN, P.; NORD, R. L.; OZKAYA, I. **Technical Debt**: From Metaphor to Theory and Practice. **IEEE Software**, v. 29, n. 6, p. 18-21, 2012.

LAUDON, K. C.; LAUDON, J. P. **Sistemas de informação gerenciais**. 11. ed. São Paulo: Pearson Prentice Hall, 2014.

NIST. **Technical Guide to Information Security Testing and Assessment**. Special Publication 800-115. Gaithersburg: National Institute of Standards and Technology, 2008.

OWASP. **OWASP Top 10: 2021**. Open Web Application Security Project, 2021.

PARANÁ. Polícia Militar do Estado do Paraná. Comando Geral. **Portaria do Comando Geral nº 131**, de 2 de fevereiro de 2024. Disciplina procedimentos relativos à Tecnologia da Informação e Comunicação. Curitiba: PMPR, 2024.

PARANÁ. Polícia Militar do Estado do Paraná. Diretoria de Tecnologia e Inovação. **Diretriz nº 015/2024**. Tecnologia da Informação e Comunicação. Curitiba: PMPR, 2024.

PRESSMAN, R. S. **Engenharia de Software**: uma abordagem profissional. 8. ed. Porto Alegre: AMGH, 2016.

SILIC, M.; BACK, A. Shadow IT: A view from behind the curtain. **Computers & Security**, v. 45, p. 274-283, 2014.

STALLINGS, W. **Criptografia e segurança de redes**: princípios e práticas. 6. ed. São Paulo: Pearson Education do Brasil, 2015.

WEILL, P.; ROSS, J. W. **Governança de TI**: tecnologia da informação. São Paulo: M. Books, 2006.