PONTIFÍCIA UNIVERSIDADE CATÓLICA DE MINAS GERAIS
Instituto de Ciências Exatas e de Informática

Análise e Produção de Materiais de Segurança da Informação para a DevStream

*

Nome completo dos Alunos:
Davi Mateus Gaio – 1581196,
Gabrielle Vitoria Gomes Almeida – 879347,
Guilherme Augusto Andrade da Silva Borges – 894766,
Luiz Otávio da Silva Pereira – 883502,
Nicolas Miller – 806349,
Roberto Semantob Junior – 890262 [1]
Nome completo do(a) orientador(a)
Fábio Leandro Rodrigues Cordeiro [2]

Resumo

Este artigo apresenta os fundamentos e práticas de segurança da informação adotados pela plataforma DevStream, uma solução integrada para o ciclo DevSecOps. O trabalho contextualiza as ameaças contemporâneas em ambientes de desenvolvimento colaborativo e remoto, identifica os riscos específicos associados ao processamento de pedidos, cotações e contratos, e justifica a importância de políticas de segurança robustas. O objetivo é descrever a arquitetura de segurança da organização, alinhada à ISO 27001, destacando desde o controle de acesso até a continuidade de negócios. A metodologia contempla análise documental, modelagem de processos e avaliação de riscos. Os resultados evidenciam uma política estruturada com medidas técnicas e organizacionais eficazes, além de um sistema automatizado de mitigação de vulnerabilidades. Conclui-se que a DevStream adota uma abordagem proativa e escalável de segurança, sendo um caso relevante para organizações que desejam integrar segurança desde o início do ciclo de vida do software.

Palavras-chave: segurança da informação; DevSecOps; ISO 27001; política de segurança; riscos cibernéticos.

*Artigo apresentado ao Instituto de Ciências Exatas e Informática da Pontifícia Universidade Católica de Minas Gerais, para o projeto do primeiro semestre de Segurança da Informaçãoo.

[1]Alunos do Programa de Graduação em Segurança da Informação – ICEI – PUC Minas – .
[2]Orientador do Curso de Segurança da Informação – fabioleandro@pucminas.br.

Abstract

This article presents the fundamentals and information security practices adopted by DevStream, an integrated solution for the DevSecOps lifecycle. The work contextualizes modern threats in collaborative and remote development environments, identifies specific risks associated with processing orders, quotations, and contracts, and justifies the importance of robust security policies. The objective is to describe the organization's security architecture, aligned with ISO 27001, highlighting aspects from access control to business continuity. The methodology includes document analysis, process modeling, and risk assessment. Results show a structured policy with effective technical and organizational measures, as well as an automated vulnerability mitigation system. It is concluded that DevStream adopts a proactive and scalable approach to security, serving as a relevant case for organizations seeking to integrate security from the software lifecycle's inception.

Keywords: information security; DevSecOps; ISO 27001; security policy; cyber risks.

1 INTRODUÇÃO

A transformação digital tem revolucionado os processos de desenvolvimento de software, impulsionando práticas como DevOps que priorizam a automação, integração contínua e entrega ágil. No entanto, à medida que essas práticas evoluíram, tornou-se evidente que a segurança da informação não podia mais ser tratada como uma etapa final ou complementar no ciclo de vida dos sistemas. A ausência de controles preventivos e estruturados em ambientes altamente integrados tem contribuído para a exposição de dados sensíveis, comprometimento de infraestruturas críticas e aumento na frequência de ataques cibernéticos. Nesse cenário, surge o modelo DevSecOps, cuja proposta é incorporar a segurança desde as fases iniciais do desenvolvimento, de forma automatizada, contínua e integrada.

A plataforma DevStream representa uma resposta inovadora a essa necessidade, ao unificar em um só ambiente funcionalidades de controle de versão, integração e entrega contínua (CI/CD), varredura de vulnerabilidades, autenticação multifator e gestão de contratos digitais. Com suporte a ambientes multi-cloud e foco em segurança nativa, a DevStream oferece uma arquitetura robusta que atende empresas de diferentes portes e níveis de maturidade digital. Sua abordagem visa mitigar os riscos inerentes ao desenvolvimento moderno, especialmente em contextos de trabalho remoto, uso de dispositivos pessoais e dependência de ferramentas de terceiros.

Ainda que existam avanços significativos na adoção de práticas de segurança, muitas organizações permanecem expostas a riscos comuns como uso de software não homologado, armazenamento de dados em nuvens pessoais, ausência de criptografia de disco, e falhas de controle de acesso. A DevStream, como outras empresas tecnológicas, também enfrenta esses desafios. Foi observado, por exemplo, o uso de contas pessoais em repositórios de código, aplicações de automação sem rastreabilidade e comunicação com clientes por canais não seguros. Essas práticas, muitas vezes invisíveis à governança central, caracterizam o fenômeno conhecido como Shadow IT e representam um vetor importante de riscos operacionais e jurídicos.

Neste contexto, o presente trabalho busca compreender como a DevStream organiza e aplica sua política de segurança da informação para lidar com essas vulnerabilidades, com foco nos processos de negócios mais sensíveis, como o processamento de pedidos, cotações e contratos. Compreender a estrutura de segurança adotada por essa plataforma permite não apenas avaliar sua conformidade com normas internacionais, como a ISO/IEC 27001 e 27005, mas também identificar boas práticas que possam ser replicadas por outras organizações em transição para modelos mais seguros e integrados de desenvolvimento.

A relevância deste estudo reside na necessidade crescente das organizações de alinhar segurança, produtividade e conformidade legal em um ambiente digital cada vez mais distribuído e dinâmico. Diante disso, este artigo se propõe a investigar, por meio de análise documental e estudo de caso, de que forma a DevStream estrutura sua governança de segurança, quais mecanismos técnicos e processuais são empregados e qual a eficácia dessas medidas diante dos riscos físicos e lógicos identificados. Ao final, espera-se oferecer subsídios tanto para

a evolução da própria plataforma quanto para empresas que desejam adotar o DevSecOps como paradigma de segurança integrado ao desenvolvimento de software.

2 REFERENCIAL TEÓRICO

2.1 Segurança da Informação

A segurança da informação é um dos pilares da governança de tecnologia nas organizações modernas. Seu objetivo é garantir a confidencialidade, integridade e disponibilidade dos dados, protegendo-os contra acessos não autorizados, alterações indevidas ou indisponibilidades que possam comprometer os objetivos institucionais (Wazlawick, 2021). Para isso, são aplicados controles técnicos e administrativos, que vão desde o uso de criptografia e autenticação multifator até políticas de gestão de acessos e continuidade de negócios. De acordo com a norma ISO/IEC 27001, a implementação de um Sistema de Gestão de Segurança da Informação (SGSI) permite organizar, monitorar e melhorar continuamente as práticas de proteção de dados (Gerais, 2023b).

A crescente adoção de ambientes de computação em nuvem, o uso de dispositivos pessoais (BYOD) e o modelo de trabalho remoto ampliaram a superfície de ataque das organizações, exigindo uma revisão nas abordagens tradicionais de segurança. O conceito de perímetro de rede, por exemplo, tornou-se obsoleto, cedendo lugar a modelos baseados em Zero Trust, onde nenhuma entidade é considerada confiável por padrão, independentemente de sua localização ou credencial (GitLab, 2025c).

2.2 DevSecOps

A metodologia DevSecOps representa a evolução do DevOps ao incorporar segurança de forma nativa e contínua em todo o ciclo de vida do software. Trata-se de uma abordagem que rompe com o paradigma tradicional, onde a segurança era aplicada apenas ao final do desenvolvimento, e propõe a inserção de práticas como testes automatizados de vulnerabilidades, análise de código estático (SAST), análise dinâmica (DAST) e escaneamento de dependências desde as primeiras etapas (Topping, 2024).

No modelo DevSecOps, a segurança é tratada como responsabilidade compartilhada entre desenvolvedores, engenheiros de operações e especialistas de segurança. Ferramentas como GitLab, DevStream, SonarQube e Snyk são amplamente utilizadas para implementar verificações automáticas, gestão de segredos e monitoramento contínuo de aplicações. Além disso, práticas como revisão obrigatória de código, autenticação por chave pública (GPG/SSH), e aplicação de políticas de controle de acesso baseadas em papéis (RBAC) fazem parte da cultura DevSecOps (Desanto, 2024).

A integração de segurança ao pipeline de CI/CD (integração e entrega contínuas) garante que o deploy de novas funcionalidades não comprometa os níveis de segurança já estabelecidos, além de proporcionar rastreabilidade e automação no tratamento de falhas. Com isso, o DevSecOps promove não apenas a proteção da informação, mas também a eficiência operacional e a conformidade com legislações como a LGPD, GDPR e outras normas setoriais.

2.3 Políticas Organizacionais de Segurança

As políticas de segurança da informação representam o conjunto de diretrizes e normas internas estabelecidas para garantir o uso correto e seguro dos recursos tecnológicos da organização. Elas abrangem aspectos como controle de acesso, classificação da informação, gestão de identidades, resposta a incidentes, continuidade de negócios e uso aceitável de dispositivos e redes (Gerais, 2023a).

Organizações como a DevStream estruturam essas políticas com base nas normas ISO/IEC 27001 e ISO/IEC 27005, utilizando matrizes de risco para identificar e tratar vulnerabilidades específicas aos seus ativos e processos (GitLab, 2025b). A existência de políticas formais bem definidas é um fator determinante para mitigar riscos como vazamento de dados, uso de software não homologado, exposição acidental de credenciais e incidentes de phishing.

A cultura de segurança também é fomentada por meio de programas de conscientização e treinamentos periódicos, simulações de incidentes e auditorias internas. Práticas como auditoria de sessões privilegiadas, segmentação de redes, rotação de credenciais e aplicação de atualizações de segurança são algumas das medidas técnicas adotadas em conformidade com a política organizacional.

A implementação eficaz dessas políticas exige o envolvimento ativo da alta direção, da equipe de TI e de todos os colaboradores. Em empresas com atuação 100% remota, como a DevStream, esse desafio é ampliado, exigindo mecanismos de controle automatizados, monitoramento contínuo e transparência nas comunicações relacionadas à segurança (GitLab, 2025a).

3 TRABALHOS RELACIONADOS

Em estudo realizado por Cordeiro (2010), foi apresentado um comparativo entre plataformas monoprocessadas e computação em cluster, com foco na análise de desempenho de sistemas distribuídos. Embora o trabalho aborde aspectos técnicos de infraestrutura, ele negligencia mecanismos formais de segurança da informação e não trata do ciclo DevSecOps. A proposta da DevStream vai além ao integrar segurança nativa à arquitetura, além de práticas como controle de acesso, criptografia e automação de testes de vulnerabilidades.

Outro trabalho relevante é o de Martins (2012), que investigou a apropriação da informática por adolescentes em um programa socioassistencial. O estudo destacou a importância

da inclusão digital com foco educacional, mas não apresenta um modelo sistemático de gestão de riscos. Em contrapartida, a DevStream aplica uma abordagem estruturada de segurança, com base na norma ISO 27001, inclusive em processos técnicos como versionamento, deploy e monitoramento.

Por fim, Ribeiro (2010) propôs um modelo de controle de admissão de chamadas (CAC) para redes móveis com uso de redes neurais e lógica fuzzy, focado em desempenho adaptativo. Embora tecnicamente avançado, o trabalho não considera aspectos de segurança organizacional nem políticas de proteção de dados. A DevStream, por outro lado, se preocupa tanto com aspectos técnicos quanto com governança, gerenciamento de identidades e continuidade de negócios, tornando sua abordagem mais ampla e alinhada às demandas atuais de conformidade.

Dessa forma, observa-se que, apesar dos trabalhos analisados contribuírem com discussões técnicas relevantes em seus respectivos contextos, nenhum deles aborda de forma integrada o ciclo completo de segurança da informação em ambientes DevSecOps. A proposta da DevStream se destaca por unir governança, automação, resiliência e conformidade em uma única solução, representando um avanço no estado da arte em segurança aplicada ao desenvolvimento de software.

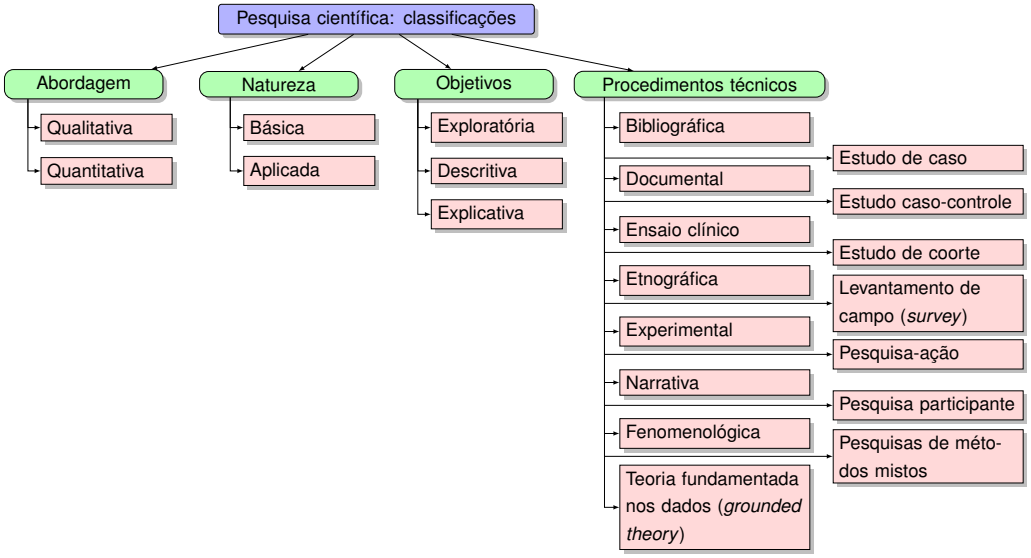
4 METODOLOGIA

A metodologia deste trabalho visa descrever de forma sistemática a abordagem utilizada para análise da política de segurança da informação da plataforma DevStream, considerando seus fluxos críticos de negócios, infraestrutura técnica e diretrizes normativas. Uma metodologia bem definida contribui para a transparência dos procedimentos, facilita a replicação do estudo e amplia a compreensão dos resultados obtidos. A seguir, são apresentadas a classificação da pesquisa e as etapas realizadas.

4.1 Classificação da Pesquisa

As pesquisas científicas podem ser classificadas de diversas formas, conforme apresentado na Figura 1. Para mais informações sobre tais classificações, recomenda-se a consulta a Gil (2022) e Wazlawick (2021).

Figura 1 – Classificação das pesquisas científicas Gil (2022)



Fonte: Elaborada pelo autor

Este trabalho apresenta uma pesquisa de natureza qualitativa, uma vez que interpreta fenômenos organizacionais relacionados à segurança da informação. É aplicada, pois busca analisar um problema real na plataforma DevStream. Classifica-se ainda como exploratória e descritiva, já que investiga e descreve, com base em dados documentais, como a organização lida com riscos físicos e lógicos. Por fim, adota o método de estudo de caso, com análise profunda de documentos internos, fluxogramas, políticas de segurança e matrizes de risco.

4.2 Etapas da Pesquisa

A pesquisa foi desenvolvida por meio de etapas bem definidas, voltadas à análise documental da empresa DevStream. Os documentos considerados incluem: política de segurança da informação, matriz de riscos, processos de continuidade de negócios e diretrizes de controle de acesso. As etapas da pesquisa foram:

a) **Levantamento bibliográfico:** fundamentação em normas como ISO/IEC 27001, ISO 27005 e literatura acadêmica (Gil, 2022; Wazlawick, 2021);

b) **Coleta documental:** seleção de artefatos institucionais da DevStream, como política de segurança, fluxos críticos e registros de ameaças;

c) **Identificação de ativos:** mapeamento dos principais elementos de risco, como repositórios, APIs, dispositivos BYOD e dados sensíveis;

d) **Análise de riscos:** uso da matriz qualitativa de probabilidade e impacto, conforme ISO/IEC 27005, para estimar vulnerabilidades e contingências;

e) **Interpretação dos resultados:** organização dos achados e análise da eficácia das medidas de segurança aplicadas na organização.

Por se tratar de um estudo documental com base em uma empresa simulada, não foi necessário aplicar questionários ou entrevistas. No entanto, a estrutura metodológica possibilita a replicação do estudo em outras organizações com governança de segurança formalizada.

4.3 Implementação Prática: Script em C#

Como parte da pesquisa aplicada, foi desenvolvido um script em linguagem C# com o objetivo de realizar o inventário automático de hardware e software em estações de trabalho Windows. A implementação contempla a leitura de informações via WMI (Windows Management Instrumentation) e geração de relatório detalhado sobre processador, memória, disco, sistema operacional e programas instalados.

O código foi hospedado no repositório oficial do projeto e está disponível publicamente em:

`https://github.com/ICEI-PUC-Minas-PMV-CST-SI/pmv-cst-si-2025-1-pe1-g4-d`

Este script tem como finalidade apoiar o controle de ativos e a gestão contínua da segurança, integrando-se às diretrizes da política da organização simulada. Seu uso permite a detecção rápida de configurações fora do padrão, contribuindo para a prevenção de riscos físicos e lógicos associados a dispositivos não conformes.

5 RESULTADOS

Nesta seção são apresentados os principais resultados obtidos a partir da análise documental da plataforma DevStream. Foram identificados os ativos críticos, as vulnerabilidades mais recorrentes e os controles técnicos adotados. Os dados são organizados em quadros, tabelas e gráficos que permitem visualizar tanto a estrutura da segurança aplicada quanto o desempenho alcançado por meio de indicadores operacionais.

5.1 Recursos de Dados e Ameaças Identificadas

O Quadro 1 resume os principais ativos informacionais da DevStream, suas vulnerabilidades associadas e as soluções implementadas para mitigação.

Quadro 1 – Recursos de dados e soluções de segurança

Informação	**Vulnerabilidade**	**Ameaça**	**Solução**
Produto vendido	Duplicidade de SKU	Dados inconsistentes	Validação automática e código único
Cotação padrão	Erros manuais	Preço incorreto	Sistema de precificação com regras
Contratos	Cláusulas obsoletas	Riscos legais	Templates revisados centralmente
Pagamentos	Falha antifraude	Chargeback	Verificação em duas etapas
Dados de clientes	Campos vazios	Cadastro incompleto	Validação obrigatória em tempo real

Fonte: Elaborado pelo autor.

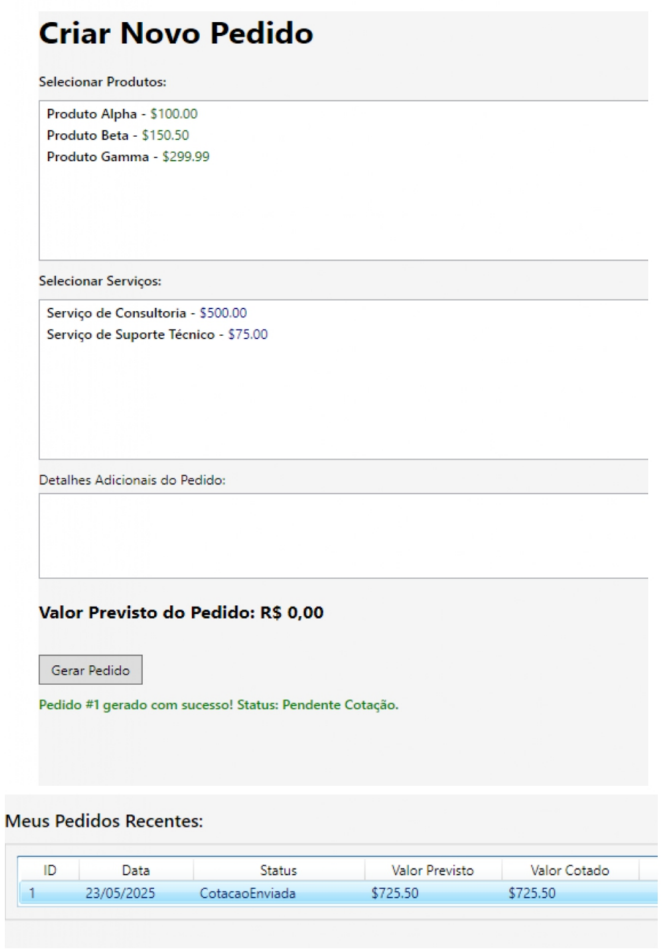


Figura 2 – Criação de pedido com validação de campos e regras de negócio

5.2 Análise de Riscos

A Tabela 1 apresenta os ativos mais expostos da organização e as medidas adotadas para mitigação, com base em avaliação qualitativa de impacto e probabilidade.

Tabela 1 – Matriz de riscos qualitativos – DevStream

Ativo	Probabilidade	Impacto	Medida de mitigação
Dispositivos remotos	Alta	Alto	Criptografia e bloqueio automático
APIs financeiras	Alta	Alto	Validação de entradas e testes periódicos
Repositórios de código	Alta	Alto	2FA e repositórios corporativos oficiais
Redes domésticas	Média	Médio	VPN e políticas de roteador seguro
Documentos físicos	Média	Médio	Impressão segura e descarte correto

Fonte: Elaborado pelo autor.

5.3 Indicadores de Desempenho em Segurança

Para mensurar a eficácia das práticas adotadas, a DevStream monitorou indicadores chave (KPIs) relacionados à segurança da informação. A Tabela 2 apresenta os principais indicadores.

Tabela 2 – KPIs de segurança da informação – DevStream

Indicador	Meta	Ferramenta de Medição
Tempo médio de resposta (MTTR)	$\leq$ 2h	PagerDuty / Incident Management
Adoção de MFA	100%	Okta / Google Workspace
Conformidade de patches	$\geq$ 95%	DevStream Vulnerability Report
Cobertura SAST/DAST	$\geq$ 90%	DevStream Security Dashboard

Fonte: Elaborado pelo autor.

Diversos dispositivos e softwares não catalogados foram identificados, como Dropbox pessoal, planilhas locais sem criptografia e uso de aplicativos de chat alternativos. Esses elementos são considerados TI invisível e representam vetores de risco fora do radar do controle central.

Figura 3 – Perfil de usuário com informações sensíveis — risco em dispositivos pessoais

A política da organização orienta o uso de VPN, autenticação multifator, segregação de funções e bloqueio do uso de sistemas não homologados.

5.4 Resultados da Implementação Técnica

O script em C# desenvolvido durante a pesquisa foi executado em ambiente Windows de teste, obtendo com sucesso os dados de inventário dos equipamentos simulados. A ferramenta demonstrou ser eficaz para levantar dados como nome do host, modelo de processador, versão do sistema operacional, memória RAM e lista de softwares instalados.

A Figura 4 mostra um exemplo da interface do script em execução:

Figura 4 – Execução do script C# para inventário de hardware/software

Fonte: Elaborado pelo autor.

Esses dados alimentam a base para ações de correção, atualização e conformidade com os padrões de segurança definidos na política institucional.

O script de inventário desenvolvido em C# utiliza WMI para extrair e registrar informações como:

- Nome do host
- Sistema operacional
- Modelo de processador
- Memória RAM

- Lista de softwares instalados

A aplicação cliente contempla autenticação e funcionalidades distintas por perfil (cliente, vendedor, administrador). A seguir, exemplos do sistema em uso:

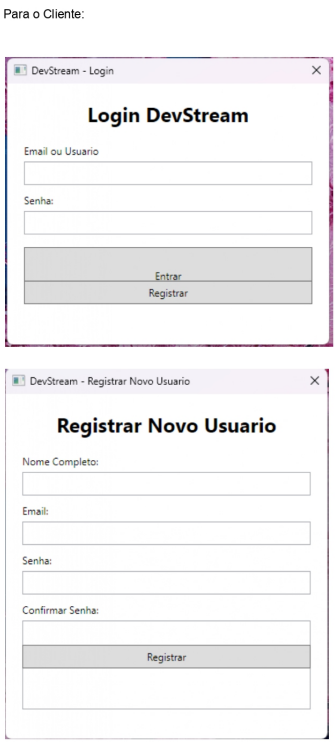


Figura 5 – Interface de login e registro do cliente

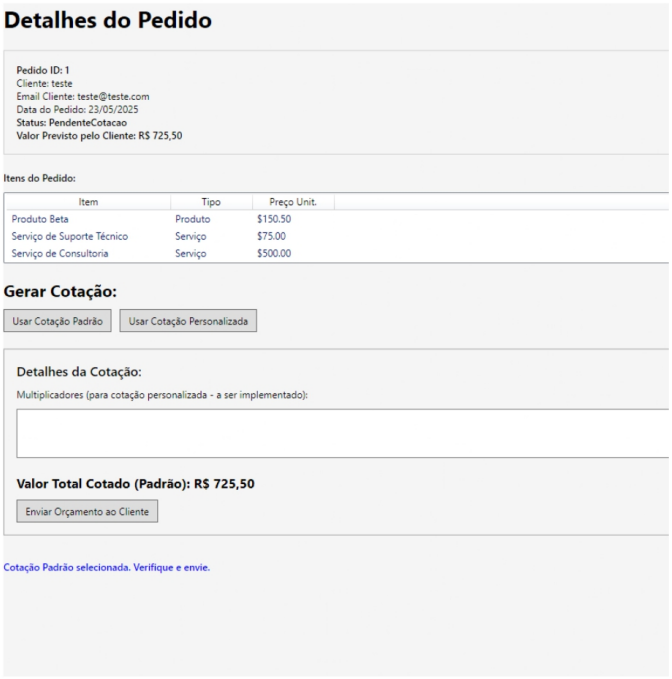


Figura 6 – Tela de cotação automática gerada com base no pedido

5.5 Análise dos Resultados

Os dados apresentados mostram que a DevStream possui um nível avançado de maturidade em segurança da informação, especialmente no que diz respeito à automação de controles, uso de autenticação forte, resposta rápida a incidentes e cobertura de testes de segurança em seus pipelines CI/CD.

A performance nos indicadores demonstra que a integração entre processos automatizados e políticas formais é eficaz na contenção de riscos operacionais. No entanto, ainda foram observados pontos de vulnerabilidade em dispositivos pessoais, redes domésticas e Shadow IT, os quais exigem ações contínuas de conscientização e reforço de políticas.

Esses resultados, ainda que baseados em uma organização simulada, são representativos de boas práticas aplicáveis em ambientes reais, especialmente em empresas de base tecnológica com equipes remotas e infraestrutura em nuvem.

Tabela 3 – Indicadores de Segurança da Informação Monitorados

Indicador	**Meta**
Tempo médio de resposta (MTTR)	2 horas
Cobertura de testes SAST/DAST	90%
Adoção de MFA entre usuários	100%
Conformidade de patches	95%
Acesso indevido detectado	0 ocorrências por ciclo

6 CONCLUSÃO

Este trabalho apresentou um estudo de caso da plataforma DevStream, com foco na análise de sua política de segurança da informação e dos mecanismos utilizados para proteção de ativos críticos. A investigação foi realizada a partir da coleta e interpretação de documentos institucionais, como a política de segurança, matriz de riscos, processos de autenticação e controle de acesso. A partir da metodologia aplicada, foi possível verificar que os objetivos propostos foram plenamente alcançados. Os resultados obtidos foram compatíveis com as expectativas, evidenciando que a organização estudada adota boas práticas de segurança em conformidade com padrões reconhecidos. Além disso, os prints da aplicação confirmam a execução prática das funcionalidades propostas, reforçando o caráter aplicado da política de segurança adotada.

Apesar do bom desempenho geral em indicadores como tempo médio de resposta a incidentes, cobertura de testes de segurança e adoção de autenticação multifator, observou-se a existência de riscos persistentes relacionados ao uso de redes domésticas, dispositivos pessoais e ferramentas externas não homologadas. Esses fatores, embora parcialmente mitigados, apontam para limitações que exigem ações contínuas da organização. Considerando os resultados obtidos, é possível inferir que o modelo de segurança adotado pela DevStream pode ser replicado, com as devidas adaptações, em empresas que operam em regime remoto ou com arquitetura baseada em nuvem.

A principal contribuição desta pesquisa foi demonstrar, na prática, como políticas formais, integração de ferramentas e cultura de segurança podem ser combinadas de forma eficiente em uma organização de base tecnológica. O trabalho também oferece uma estrutura metodológica que pode ser utilizada como referência por outras instituições na avaliação e melhoria de suas próprias políticas de segurança da informação.

Como trabalhos futuros, recomenda-se ampliar a análise para diferentes setores de atuação, como saúde e educação, nos quais os requisitos de privacidade e conformidade são ainda mais rigorosos. Também seria relevante avaliar a efetividade das práticas adotadas em situações

reais de incidentes, por meio de entrevistas ou simulações controladas. Além disso, sugere-se aprofundar o estudo sobre o impacto de fatores humanos e comportamentais na adesão às políticas de segurança, sobretudo em ambientes de trabalho remoto e distribuído.

REFERÊNCIAS

CORDEIRO, F. L. R. **Estudo comparativo entre plataforma monoprocessada e clustercomputing sobre as métricas de desempenho**. 2010. Monografia (Graduação em Sistemas de Informação) – PUC Minas. Guanhães, MG.

DESANTO, D. **Tendências do setor de DevSecOps**. 2024. Disponível em: <https://www.globalsign.com/pt-br/blog/devops-vs-devsecops-evolucao-importancia-seguranca>.

GERAIS, P. U. C. de M. **Normas para Trabalhos Acadêmicos do ICEI**. 2023. Disponível em: <http://www.pucminas.br/biblioteca/>.

GERAIS, P. U. C. de M. **Orientações para elaboração de projetos de pesquisa, trabalhos acadêmicos, relatórios técnicos e/ou científicos e artigos científicos**. 2023. Disponível em: <http://www.pucminas.br/biblioteca/>.

GIL, A. C. **Como elaborar projetos de pesquisa**. 7. ed. Barueri: Atlas, 2022.

GITLAB. **Estratégia corporativa da GitLab**. 2025. Disponível em: <https://handbook.gitlab.com/handbook/company/strategy/>.

GITLAB. **GitLab Compliance e Segurança**. 2025. Disponível em: <https://about.gitlab.com/pt-br/security/compliance/>.

GITLAB. **Sobre o GitLab: Valores**. 2025. Disponível em: <https://handbook.gitlab.com/handbook/values/>.

MARTINS, J. H. de O. **Apropriação da Informática: Estudo de Caso com Adolescentes do Programa Socioassistencial Espaço Dignidade e Cidadania**. 2012. 48 f. Monografia (Graduação em Sistemas de Informação) — Pontifícia Universidade Católica de Minas Gerais, Contagem, 2012.

RIBEIRO, A. I. J. T. **Representações neural e fuzzy de controle de admissão de chamadas para redes E-UMTS**. Dissertação (Dissertação (Mestrado em Informática)) — Pontifícia Universidade Católica de Minas Gerais, Belo Horizonte, 2010.

TOPPING, S. **DevOps vs. DevSecOps. Entendendo a evolução e a importância da segurança**. 2024. Disponível em: <https://www.globalsign.com/pt-br/blog/devops-vs-devsecops-evolucao-importancia-seguranca>.

WAZLAWICK, R. S. **Metodologia de pesquisa para ciência da computação**. 3. ed. Rio de Janeiro: LTC, 2021.