CENTRO PAULA SOUZA
FACULDADE DE TECNOLOGIA DE ARARAQUARA
CURSO SUPERIOR DE TECNOLOGIA EM SEGURANÇA DA INFORMAÇÃO

Título do Artigo: TRANSFORMANDO VULNERABILIDADES EM OPORTUNIDADES: A REDEFINIÇÃO DA SEGURANÇA DA INFORMAÇÃO ATRAVÉS DE PROGRAMAS DE BUG BOUNTY.

Autores: Juliene Aparecida Theodoro Frigere
juliene.frigere@fatec.sp.gov.br

Michelle Caroline Pereira Francisco
michelle.francisco@fatec.sp.gov.br

Orientador: Fernando Tiosso
fernando.tiosso@fatec.sp.gov.br

Resumo

Este artigo analisa o papel dos programas de *Bug Bounty* como estratégia de fortalecimento da segurança da informação no cenário contemporâneo, marcado pela crescente sofisticação das ameaças cibernéticas. Ressalta-se a importância da identificação precoce de vulnerabilidades como meio de garantir a integridade, confidencialidade e disponibilidade dos sistemas. Para isso, são discutidos os conceitos fundamentais de segurança da informação, o surgimento e a evolução histórica do *Bug Bounty*, bem como sua distinção em relação ao pentest tradicional. Além disso, são apresentadas as principais plataformas especializadas que sustentam essa prática. A metodologia empregada compreendeu pesquisa bibliográfica complementada por um estudo de caso do programa de recompensas do Google Chrome e da Microsoft, que evidencia a relevância da colaboração entre empresas e a comunidade de pesquisadores de segurança. O estudo mostra que a adoção de programas de *Bug Bounty* amplia a capacidade de detecção de falhas, incentiva a cultura preventiva e contribui para a construção de sistemas mais resilientes. Assim, o estudo mostrou que essa prática se consolida como instrumento eficaz e complementar às estratégias tradicionais de defesa, promovendo inovação, engajamento e cooperação no enfrentamento das ameaças digitais.

Palavras-chave: *Bug Bounty*; Segurança da Informação; Ameaças Digitais.

CENTRO PAULA SOUZA
FACULDADE DE TECNOLOGIA DE ARARAQUARA
CURSO SUPERIOR DE TECNOLOGIA EM SEGURANÇA DA INFORMAÇÃO

Abstract

This article analyzes the role of Bug Bounty programs as a strategy for strengthening information security in the contemporary scenario, marked by the growing sophistication of cyber threats. It highlights the importance of early vulnerability identification as a means to ensure the integrity, confidentiality, and availability of systems. To this end, the fundamental concepts of information security, the emergence and historical evolution of Bug Bounty programs, as well as their distinction from traditional penetration testing, are discussed. In addition, the main specialized platforms that support this practice are presented. The methodology employed consisted of bibliographic research complemented by a case study of the Google Chrome and Microsoft reward programs, which demonstrates the relevance of collaboration between companies and the security research community. The study shows that the adoption of Bug Bounty programs expands the ability to detect flaws, encourages a preventive culture, and contributes to building more resilient systems. Thus, the study indicated that this practice is consolidated as an effective and complementary tool to traditional defense strategies, promoting innovation, engagement, and cooperation in addressing digital threats.

Keywords: *Bug Bounty; Information Security; Digital Threats.*

Dezembro/2025

1. INTRODUÇÃO

A segurança da informação deixou de ser um recurso operacional restrito à área de tecnologia para assumir posição estratégica na governança corporativa. Com a crescente digitalização de processos e a adoção massiva de serviços em nuvem, a preservação da confidencialidade, integridade e disponibilidade (CIA) dos ativos informacionais tornou-se essencial para a continuidade dos negócios e para a manutenção da confiança de clientes, parceiros e stakeholders.

A ampliação da superfície de ataque e a sofisticação de ameaças, como *ransomware* avançado, *spear phishing* e vulnerabilidades *zero-day,* evidenciam limitações de métodos tradicionais de defesa. Nesse contexto, ganham destaque o teste de penetração (pentest) e os programas de *Bug Bounty*, pois enquanto o pentest consiste em um exercício controlado e pontual de simulação de ataques, o *Bug Bounty* mobiliza uma comunidade distribuída de pesquisadores e hackers éticos, recompensados conforme a criticidade das vulnerabilidades identificadas (Akgul et al., 2023). Esse modelo, baseado em inteligência coletiva, amplia a capacidade de detecção de falhas pela diversidade técnica dos participantes.

Além disso, a adoção crescente de programas de *Bug Bounty* impulsionou a consolidação de princípios que estruturam a cooperação entre pesquisadores e organizações, como o *responsible disclosure,* prática que orienta o reporte ético e coordenado de vulnerabilidades, e as políticas de *safe harbor*, que oferecem garantias jurídicas a pesquisadores que atuam de boa-fé dentro do escopo autorizado. Esses mecanismos reforçam a confiança entre as partes e reduzem riscos associados à exploração indevida durante o ciclo de correção.

O amadurecimento dessa prática também depende de estruturas internas de governança e maturidade institucional, responsáveis por organizar o fluxo de recebimento, triagem e tratamento de vulnerabilidades. Em ecossistemas complexos, como navegadores baseados em projetos *open*

source, surge, ainda, o desafio da coordenação *upstream/downstream* que envolve alinhar correções entre o projeto principal (como o Chromium) e sistemas derivados, prevenindo efeitos sistêmicos na cadeia de suprimentos.

Esse paradigma colaborativo impulsionou o surgimento de plataformas como HackerOne, Bugcrowd e Synack, que intermediam a relação entre organizações e pesquisadores e profissionalizam a prática de *Bug Bounty*. Sua efetividade depende do equilíbrio entre incentivos financeiros, políticas claras de participação e processos estruturados de segurança.

Diante desse cenário, este estudo investiga a efetividade dos programas de *Bug Bounty* como mecanismo complementar às práticas tradicionais de segurança da informação, com ênfase em seus benefícios operacionais, nos desafios de implementação e nas implicações estratégicas para a consolidação de ambientes digitais resilientes. Assim, este artigo organiza-se da seguinte forma: a seção 2 apresenta o referencial teórico, a seção 3 descreve a metodologia, a seção 4 analisa o estudo de caso do Google Chrome e da Microsoft e, por fim, a seção 5 apresenta as considerações finais.

2. REFERENCIAL TEÓRICO

Com a finalidade de aprofundar o conhecimento sobre o tema proposto, faz-se necessário compreender o histórico dos programas de *Bug Bounty*, os principais tipos de hackers envolvidos e sua relação com essas iniciativas, bem como as diferenças entre os testes de penetração tradicionais e os modelos colaborativos. Além disso, tornam-se essenciais os conceitos de *responsible disclosure, safe harbor,* governança, maturidade institucional e coordenação na cadeia de suprimentos de software, visto que estruturam o funcionamento dos programas e influenciam sua efetividade. Essas bases permitem analisar a evolução do *Bug Bounty*, sua consolidação como prática de segurança da informação e o papel de plataformas especializadas que dão suporte a esse ecossistema.

2.1 Histórico do *Bug Bounty*

Tradicionalmente, as organizações dependiam de equipes internas de segurança e consultores externos para identificar vulnerabilidades por meio de testes de penetração. Em contraste, os programas de *Bug Bounty* incentivam especialistas independentes a analisar sistemas e reportar falhas mediante recompensas financeiras ou reconhecimento. A iniciativa pioneira ocorreu em 1995, com o Netscape Bugs Bounty Program, marco do surgimento dos *Vulnerability Reward Programs* (VRPs) e da incorporação da comunidade hacker como parceira legítima na proteção digital (Akgul et al., 2023; Lozano; Amir, 2018).

Nos anos 2000, projetos como o Mozilla Firefox consolidaram os Bug Bounties como estratégia complementar às auditorias tradicionais (Kuehn; Muller, 2014). A partir de 2010, o modelo foi institucionalizado com programas de grande escala, como o *Google Vulnerability Reward Program*, posteriormente expandido para o Chrome e referência em regras de escopo, responsabilidade e recompensa (Kuehn; Mueller, 2014; Lozano; Amir, 2018).

A profissionalização dessas práticas intensificou-se com o surgimento de plataformas especializadas, como HackerOne, Bugcrowd e Synack, criadas em 2012, que passaram a intermediar a relação entre organizações e pesquisadores e estabelecer padrões técnicos e jurídicos para participação (Albuquerque; Sousa Júnior; Costa, 2015). Na última década, os Bug Bounties expandiram-se para governos, setores corporativos e instituições acadêmicas, fortalecendo a cultura de segurança digital e a gestão contínua de riscos em diferentes regiões, incluindo a América Latina (Restrepo Gómez; Correa Ortiz, 2024).

2.2 Perfis de Hackers e Ética Hacker

A atuação dos bugs bounty hunters relaciona-se diretamente às categorias clássicas de hackers, classificadas por motivações e práticas éticas. Os *white hats* utilizam seus conhecimentos de forma autorizada e colaboram na identificação de vulnerabilidades seguindo princípios de *responsible disclosure* (Albuquerque; Souza Júnior; Costa, 2015; Lozano; Amir, 2018).

Os *black hats* exploram falhas de maneira maliciosa, enquanto os *gray hats* operam em zona intermediária, podendo reportar vulnerabilidades sem autorização ou explorá-las para benefício próprio (Kuehn; Mueller, 2014). Há também os hacktivistas, motivados por causas político-ideológicas, e os *script kiddies*, que utilizam ferramentas prontas sem domínio técnico.

Nesse ecossistema, os *bugs bounty hunters* representam uma vertente ética e profissionalizada, contribuindo para a resiliência organizacional e para a cultura global de segurança digital (Restrepo Gómez; Correa Ortiz, 2024).

2.3 Pentest e *Bug Bounty*: abordagens complementares

O teste de penetração (pentest) é uma prática consolidada de avaliação controlada da segurança de sistemas mediante simulação de ataques (Barbosa, 2025). Apesar de essencial para conformidade regulatória e auditoria técnica, apresenta limitações, tais como ocorrer em janelas específicas, não oferecer monitoramento contínuo e depender da expertise restrita de uma única equipe.

Programas de *Bug Bounty*, por sua vez, operam continuamente, mobilizando inteligência coletiva e diversidade metodológica de pesquisadores independentes (Albuquerque; Souza Júnior; Costa, 2015). Assim, pentest e *Bug Bounty* não se substituem, mas articulam-se em um ecossistema híbrido, no qual o pentest fornece análise formal e o *Bug Bounty* amplia a detecção de vulnerabilidades em escala.

2.4 Responsible Disclosure

A divulgação responsável (*responsible disclosure*) corresponde ao processo pelo qual vulnerabilidades são reportadas diretamente à organização antes da divulgação pública. Esse mecanismo, adotado em programas de *Bug Bounty*, reduz o risco de exploração maliciosa e estabelece fluxo seguro de comunicação entre pesquisadores e equipes internas (Lozano; Amir, 2018; Albuquerque; Souza Júnior; Costa, 2015). O modelo tornou-se um dos pilares operacionais dos programas contemporâneos, incluindo o Chrome VRP (Google, 2025).

2.5 Safe Harbor

As políticas de *Safe Harbor* estabelecem garantias jurídicas para pesquisadores que atuam de boa-fé e respeitam o escopo definido pelos programas. Ao delimitar práticas autorizadas e proteger pesquisadores de eventuais ações legais, essas diretrizes fortalecem a cooperação e aumentam a previsibilidade jurídica da participação (Google, 2025; CISA, 2021). O mecanismo é amplamente utilizado por grandes programas, como o Microsoft Security Response Center da Microsoft.

2.6 Governança e maturidade institucional

A efetividade dos programas de *Bug Bounty* depende de estruturas internas de governança responsáveis por padronizar processos de recebimento, triagem, priorização e correção de vulnerabilidades. Critérios de severidade, definições de escopo, políticas de recompensa e fluxos internos de resposta compõem esse arcabouço, cujo desempenho está associado ao grau de maturidade institucional (Restrepo Gómez; Correa Ortiz, 2024; Albuquerque; Sousa Júnior; Costa, 2015). Programas maduros evitam acúmulo de relatórios, garantem respostas tempestivas e contribuem diretamente para a resiliência cibernética (Lozano; Amir, 2018).

2.7 Cadeia de Suprimentos de Software (*Upstream* e *Downstream*)

A cadeia de suprimentos de software envolve projetos *upstream*, como o Chromium, e projetos *downstream*, que incorporam seus componentes. Vulnerabilidades identificadas em projetos centrais podem propagar-se para diversos sistemas derivados, exigindo coordenação eficiente entre mantenedores para evitar riscos sistêmicos (Chromium, 2025; CISA, 2021). No contexto de *Bug Bounty*, falhas encontradas na base *upstream* devem ser tratadas e disseminadas de forma consistente em toda a cadeia, reforçando a segurança do ecossistema como um todo (Google, 2025).

2.8 Plataformas de *Bug Bounty*

O amadurecimento dos programas de *Bug Bounty* impulsionou o surgimento de plataformas especializadas que estruturam a comunicação entre organizações e pesquisadores. HackerOne, Bugcrowd e Synack oferecem infraestrutura de submissão, triagem, validação e gestão de recompensas, consolidando a institucionalização do hacking ético (Lozano; Amir, 2018).

A HackerOne destaca-se por diretrizes robustas de *responsible disclosure*, enquanto a Bugcrowd pela flexibilidade de modelos de engajamento e a Synack por sua abordagem híbrida com validação prévia de pesquisadores. Em conjunto, essas plataformas ampliam a eficiência dos programas e fortalecem a resiliência organizacional por meio de cooperação estruturada.

3. METODOLOGIA

Para o desenvolvimento deste trabalho foram utilizadas duas estratégias metodológicas: revisão bibliográfica e estudo de caso. A pesquisa foi de caráter exploratório e descritivo, com abordagem qualitativa, pois busca compreender de forma aprofundada os programas de *Bug Bounty*.

Segundo Gil (2019), a revisão bibliográfica é a base que sustenta qualquer pesquisa, visto que ela compreende o procedimento racional e sistemático. O método de revisão bibliográfica foi conduzido para examinar as teorias psicológicas e os estudos empíricos relacionados ao tema de *Bug Bounty* em contextos de sistemas da informação. Essa revisão permitirá uma compreensão sólida das bases teóricas subjacentes ao tema.

Conjuntamente, foi realizado um estudo de caso específico sobre o programa de *Bug Bounty* do Google Chrome e da Microsoft, com o objetivo de examinar na prática como essas iniciativas funcionam, quais estratégias de recompensas são aplicadas e como as vulnerabilidades são gerenciadas, permitindo uma análise concreta que complemente a revisão bibliográfica. Segundo Yin (2015) o estudo de caso é uma estratégia de pesquisa que investiga conceitos dentro de um contexto da vida real, sendo útil para identificar se os conceitos foram bem definidos.

4. ANÁLISE E DISCUSSÃO DOS RESULTADOS

Os programas de *Bug Bounty* consistem em iniciativas que recompensam pesquisadores de segurança pela identificação e reporte de vulnerabilidades em sistemas, produtos ou aplicações. Diferentemente de auditorias ou testes de penetração realizados em intervalos específicos, esses programas operam de modo contínuo e aberto, permitindo que especialistas de diferentes contextos contribuam para o fortalecimento da segurança digital. Essa dinâmica amplia a capacidade organizacional de detectar falhas e mitigar riscos, alinhando-se à perspectiva estratégica da segurança da informação apresentada na introdução e às diretrizes metodológicas adotadas na pesquisa.

4.1 Etapas de Funcionamento de um Programa de *Bug Bounty*

De modo geral, os programas de *Bug Bounty* seguem uma sequência de etapas estruturadas que garantem a eficiência do processo e a confiabilidade dos resultados obtidos, conforme observa-se a seguir:

1. Descoberta da vulnerabilidade: o pesquisador de segurança identifica uma falha potencial em um sistema, aplicação ou serviço, observando comportamentos anômalos, erros de validação ou falhas de configuração.
2. Documentação e submissão: após confirmar a falha, o pesquisador prepara um relatório técnico detalhado, contendo evidências, descrições do impacto e, quando possível, sugestões de mitigação. Esse relatório é então enviado por meio da plataforma oficial do programa, como HackerOne, Bugcrowd ou o portal interno da própria empresa.
3. Triagem e validação: a equipe de segurança da organização analisa o relatório recebido, verifica a legitimidade da descoberta e avalia a gravidade da vulnerabilidade com base em critérios como impacto, facilidade de exploração e abrangência.
4. Correção e resposta: uma vez validada, a falha é encaminhada à equipe de desenvolvimento para correção. O pesquisador geralmente é informado sobre o andamento do processo e pode ser envolvido na verificação da solução.
5. Recompensa e divulgação: após a confirmação da correção, o pesquisador recebe uma recompensa financeira proporcional à severidade e ao impacto da vulnerabilidade reportada. Em muitos casos, a descoberta também é reconhecida publicamente em relatórios.

4.2 Programa de Recompensas do Google Chrome

Criado em 2010, o *Chrome Vulnerability Reward Program* (VRP) tornou-se referência global em *Bug Bounty* (Lozano; Amir, 2018; Google, 2025). O programa define escopo, regras de *responsible disclosure* e critérios de recompensa, fortalecendo mecanismos de governança e transparência. A estrutura prioriza vulnerabilidades críticas relacionadas ao isolamento de processos, especialmente *sandbox escapes*, que recebem valores elevados devido ao potencial de comprometimento sistêmico. Essa abordagem evidencia como a colaboração com a comunidade hacker ética se traduz em ganhos

diretos de segurança, alinhando incentivos financeiros à mitigação de riscos relevantes

Em 2025, o pesquisador “Micky” reportou ao Google a vulnerabilidade CVE-2025-4609, relacionada ao mecanismo de comunicação entre processos (IPC) do Chromium. A falha permitia a violação da *sandbox*, possibilitando execução de código fora das restrições impostas pelo navegador (NIST, 2025; Chromium, 2025; Google, 2025).

A resposta seguiu o fluxo padrão do VRP: análise, validação, desenvolvimento da correção e distribuição do patch nas versões estáveis. Devido à gravidade, o pesquisador recebeu a recompensa máxima prevista (Kovacs, 2025).

O caso evidencia desafios de segurança na cadeia de suprimentos, já que o Chromium serve como base para diversos navegadores e *frameworks*. O episódio reforça a importância do *responsible disclosure* e da coordenação entre mantenedores, evitando exploração maliciosa antes da correção (Siman Tov Bustan; Zadock, 2025).

4.3 Programa de Recompensas da Microsoft

O programa de *Bug Bounty* da Microsoft é conduzido pelo Microsoft Security Response Center (MSRC) e apresenta um dos ecossistemas mais amplos do setor (Microsoft, 2025). Criado em 2013, abrange produtos e serviços como Windows, Edge, Azure, .NET, Microsoft 365 e plataformas corporativas.

Assim como o Chrome VRP, o MSRC adota princípios de governança, *responsible disclosure* e critérios técnicos de validação. Seu diferencial está na amplitude da cobertura e na integração entre ambientes locais e de nuvem, além da política de *Safe Harbor*, que protege pesquisadores que atuam de boa-fé.

As recompensas variam conforme impacto e produto. Em 2025, a Microsoft anunciou cerca de US$ 17 milhões em pagamentos a pesquisadores, reforçando o papel estratégico desses programas (MSRC, 2025).

A vulnerabilidade *PrintNightmare* (CVE-2021-34527) afetou o componente *Windows Print Spooler*, permitindo execução remota de código e

elevação de privilégios (Microsoft, 2021; CISA, 2021). A publicação acidental de um *proof-of-concept* ampliou o impacto, resultando em exploração ativa antes da correção.

A Microsoft lançou atualizações emergenciais, mas o patch inicial não solucionou integralmente o problema, exigindo novas correções e recomendações como a desativação temporária do serviço (ZDNET, 2021; Securelist, 2021).

O caso se tornou referência sobre a importância da divulgação responsável e da coordenação entre pesquisadores e fornecedores, especialmente em falhas que afetam componentes centrais e podem gerar riscos sistêmicos na cadeia de suprimentos.

4.4 Comparação entre Programas de *Bug Bounty*: Google Chrome VRP e Microsoft

Os programas de *Bug Bounty* do Google Chrome e da Microsoft compartilham o objetivo de reforçar a segurança de seus produtos por meio da colaboração com pesquisadores externos, mas apresentam diferenças marcantes em termos de escopo, estrutura e gestão, refletindo também diferentes desafios e benefícios. A Tabela 1 sintetiza diferenças estruturais entre os programas de *Bug Bounty* do Google Chrome e da Microsoft.

Tabela 1: Comparativo dos Programas de Bug Bounty do Google Chrome e da Microsoft

Característica	Google Chrome Vulnerability Reward Program (VRP)	Microsoft Security Response Center (MSRC)
Escopo Primário	Focado e específico no ecossistema **Chromium** (navegador, OS, componentes).	Amplo e diversificado: **Windows,Azure, Edge, .NET, Microsoft 365** e produtos corporativos.
Natureza Operacional	Prioriza transparência, documentação técnica detalhada (*commits* e *issue trackers*) e **previsibilidade**.	Prioriza amplitude, **gestão de incidentes críticos em larga escala** e mitigação rápida de ameaças
Foco Estratégico	Segurança do produto e **engenharia de *sandboxing*** (prevenção de *sandbox escapes*).	**Defesa de infraestrutura corporativa** e mitigação de risco sistêmico (*e.g.*, falhas no *Print Spooler*).
Recompensas	Valores proporcionais à gravidade, com destaque para falhas críticas de *sandbox escape* (até US$ 250.000).	Valores proporcionais à gravidade, com recompensas variadas por programa (Azure, Windows, M365).

Fonte: Autores (2025)

4.5 Pontos Positivos dos Programas de *Bug Bounty*

Entre os méritos observados, destacam-se quatro dimensões principais: cobertura contínua e descentralizada, diversidade metodológica, custo-efetividade e fomento à ética hacker.

A cobertura contínua e descentralizada permite mobilizar pesquisadores distribuídos globalmente, fazendo com que os programas superem a natureza episódica dos pentests, promovendo uma vigilância quase ininterrupta

(Albuquerque; Sousa Júnior; Costa, 2015). Essa descentralização mitiga vieses de percepção característicos de equipes restritas e amplia a robustez da detecção em ecossistemas complexos.

A diversidade metodológica provém a heterogeneidade dos perfis de pesquisadores possibilitando identificar falhas que dificilmente emergiriam em auditorias convencionais (Akgul et al., 2023). O acúmulo de técnicas, experiências e perspectivas promove uma visão multifacetada da superfície de ataque.

O custo-efetividade possibilita adotar um modelo baseado em pagamento por resultado que otimizam a alocação de recursos financeiros e evitam dispêndios fixos característicos de contratos tradicionais de consultoria (Kuehn; Mueller, 2014).

Por fim, o fomento à ética hacker visa oferecer um espaço legítimo e recompensado para a prática, reduzindo o incentivo à exploração maliciosa e fortalecendo a consolidação de um ecossistema profissional de segurança colaborativa (Restrepo Gómez; Correa Ortiz, 2024).

4.6 Pontos Negativos e Desafios

Apesar de seu êxito, os programas apresentam desafios estruturais que limitam sua plena efetividade como a gestão do volume de relatórios e a dependência da maturidade institucional.

A gestão do volume de relatórios gera sobrecarga de submissões, muitas vezes redundantes ou irrelevantes, o que exige alto investimento interno em triagem e pode comprometer indicadores críticos, como o tempo médio de resposta (Lozano; Amir, 2018).

Já a dependência da maturidade institucional, embora eficaz em organizações altamente estruturadas, pode ser contraproducente em empresas sem processos ágeis de correção, gerando acúmulo de vulnerabilidades reportadas e desgaste da credibilidade (Restrepo Gómez; Correa Ortiz, 2024).

4.7 Discussões dos Resultados

A análise do programa de *Bug Bounty* do Google Chrome revela um modelo estruturado, maduro e eficiente, apoiado por mecanismos sólidos de governança, *responsible disclosure* e *safe harbor*. O fluxo integrado de submissão, triagem e correção demonstra que o programa evoluiu para além da simples identificação de falhas, tornando-se componente estratégico da segurança digital do navegador.

A comparação com a Microsoft evidencia que programas de *Bug Bounty*, embora compartilhem princípios essenciais, assumem configurações distintas conforme o ecossistema, arquitetura de software e maturidade institucional. Ambos reforçam que práticas colaborativas ampliam a capacidade de resposta frente às ameaças contemporâneas e fortalecem a resiliência organizacional.

A síntese demonstra que programas de *Bug Bounty* representam mecanismos complementares aos métodos tradicionais de defesa, oferecendo detecção contínua baseada em inteligência coletiva, diversidade metodológica e coordenação eficiente da cadeia de suprimentos.

5. CONSIDERAÇÕES FINAIS

Os objetivos deste artigo foram alcançados ao mostrar que os programas de *Bug Bounty* representam uma resposta moderna, colaborativa e estratégica aos desafios da segurança da informação. Desde a introdução, observou-se que o aumento das ameaças digitais exige respostas que vão além de métodos tradicionais, como os testes de intrusão.

No referencial teórico, evidenciou-se que esses programas se estruturaram a partir da evolução histórica da cultura hacker, do papel de plataformas especializadas e do engajamento de diferentes perfis de pesquisadores. Os estudos de caso analisados, o Google Chrome VRP e o incidente *PrintNightmare*, mostraram, na prática, como esses programas funcionam, seus benefícios e seus limites.

Essa compreensão é reforçada pela singularidade dos programas de *Bug Bounty*, evidenciados por Kuehn e Mueller como instituições emergentes capazes de reduzir a assimetria de informações entre empresas e pesquisadores, criando um mercado formalizado de vulnerabilidades. Para os autores, essas iniciativas transcendem a dimensão técnica e se inserem na lógica da governança digital, estabelecendo mecanismos regulares de troca baseados em confiança, transparência e reconhecimento.

Assim, os programas deixam de ser ferramentas pontuais de segurança para se consolidarem como inovações sociotécnicas com impacto duradouro sobre a economia da informação e as formas de cooperação entre atores da área. Constituem, portanto, instrumentos capazes de unir técnica, participação social e governança, transformando vulnerabilidades em oportunidades de proteção e aprendizado contínuo.

REFERÊNCIAS

AKGUL, B.; EGELE, M.; KIRDA, E. *Understanding the Ecosystem of Bug Bounty Programs*. **IEEE Transactions on Dependable and Secure Computing**, v. 20, n. 4, p. 1305–1320, 2023.

AKGUL, Omer; EGHTESAD, Taha; ELAZARI, Amit; GNAWALI, Omprakash; GROSSKLAGS, Jens; MAZUREK, Michelle L.; VOTIPKA, Daniel; LASZKA, Aron. *Bug Hunters' Perspectives on the Challenges and Benefits of the Bug Bounty Ecosystem*. In: **32nd USENIX Security Symposium (USENIX Security 2023)**, Anaheim, EUA. Anaheim: USENIX Association, 2023. p. 2275–2291. Disponível em: https://www.usenix.org/system/files/sec23fall-prepub-81-akgul.pdf. Acesso em: 31 ago. 2025.

ALALI, M. et al. *Improving risk assessment model of cyber security using fuzzy logic*. **Computers & Security**, v. 73, p. 1–13, 2018. Disponível em: https://doi.org/10.1016/j.cose.2017.09.004. Acesso em: 31 ago. 2025.

ALBUQUERQUE, Robson de Oliveira; SOUSA JÚNIOR, Rafael Timóteo de; COSTA, João Paulo C. Lustosa da. *Bug bounty programs as an effective method for information security management*. In: **INTERNATIONAL CONFERENCE ON FUTURE COMPUTER SYSTEMS AND COMMUNICATION (ICoFCS)**, 2015. [S. l.]: ICoFCS, 2015. p. 58–62. Disponível em: http://icofcs.org/2015/ICoFCS-2015-012.pdf. Acesso em: 26 abr. 2025.

ALBUQUERQUE, A.; SOUSA JÚNIOR, R.; COSTA, E. *Gestão colaborativa da segurança da informação: lições de programas de bug bounty*. **Revista Brasileira de Segurança da Informação**, v. 7, n. 2, p. 45–60, 2015.

BARBOSA, L. *Pentest: o que é, tipos e como funciona*. **InterOp | Tecnologia**, 2025. Disponível em: https://interop.com.br/2025/08/pentest-o-que-e-tipos-e-como-funciona/. Acesso em: 13 set. 2025.

CHROMIUM PROJECT. *Chromium Security and Vulnerability Reports*. Mountain View, 2025. Disponível em: https://chromium.googlesource.com/. Acesso em: 14 out. 2025.

CHROMIUM. *Rastreamento de problema: CVE-2025-4609*. Disponível em: https://issues.chromium.org/issues/412578726. Acesso em: 7 out. 2025.

CIMPANU, Catalin. *Risky Bulletin: Researcher scores $250,000 for Chrome bug*. **Risky Business News**, 11 ago. 2025. Disponível em: https://news.risky.biz/risky-bulletin-researcher-scores-250-000-for-chrome-bug/. Acesso em: 7 out. 2025.

CISA – CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY. *Alert (AA21-195A): PrintNightmare Critical Vulnerability (CVE-2021-34527)*. Washington, D.C., 2021. Disponível em: https://www.cisa.gov/. Acesso em: 14 out. 2025.

ENISA**.** EUROPEAN UNION AGENCY FOR CYBERSECURITY. *Vulnerability Disclosure Policies in the EU*. Athens, 2023. Disponível em: https://www.enisa.europa.eu. Acesso em: 21 out. 2025.

GIL, A. C. *Métodos e técnicas de pesquisa social*. 6. ed. São Paulo: Atlas, 2019.

GOOGLE. *Chrome Vulnerability Reward Program (VRP)*. Google, 2025. Disponível em: https://www.google.com/about/appsecurity/chrome-reward/. Acesso em: 14 out. 2025.

GOOGLE. *Google Chrome Vulnerability Reward Program (VRP) Rules and Hall of Fame*. Mountain View, 2025. Disponível em: https://bughunters.google.com/. Acesso em: 14 out. 2025.

GOOGLE. *Notas de lançamento do Chrome: atualização do canal estável para desktop*. Disponível em: https://chromereleases.googleblog.com/2025/05/stable-channel-update-for-desktop_14.html. Acesso em: 7 out. 2025.

KOVACS, Eduard. *Chrome sandbox escape earns researcher $250,000*. **SecurityWeek**, 11 ago. 2025. Disponível em: https://www.securityweek.com/chrome-sandbox-escape-earns-researcher-250000/. Acesso em: 7 out. 2025.

KOVACS, E. *Google Updates Chrome Vulnerability Reward Program With New Payout Rules*. **SecurityWeek**, 2025. Disponível em: https://www.securityweek.com/. Acesso em: 14 out. 2025.

KUEHN, Andreas; MUELLER, Milton. *Analyzing bug bounty programs: an institutional perspective on the economics of software vulnerabilities*. In: **TPRC – Research Conference on Communication, Information and Internet Policy**, 42., 2014.

KÜHN, Andreas; MUELLER, Milton. *Analyzing bug bounty programs: an institutional perspective on the economics of software vulnerabilities.* In: TPRC – Research Conference on Communication, Information and Internet Policy, 42., 2014. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2418812. Acesso em: 21 out. 2025

LOZANO, Carlos A.; AMIR, Shahmeer. *Bug bounty hunting essentials: quick-paced guide to help white-hat hackers get through bug bounty programs*.

Birmingham: Packt Publishing Ltd, 2018. 270 p. Disponível em: https://books.google.com.br/books?id=di59DwAAQBAJ. Acesso em: 19 mar. 2025.

MICROSOFT. *CVE-2021-34527 – Print Spooler Remote Code Execution Vulnerability*. **Microsoft Security Response Center**, 2021. Disponível em: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527. Acesso em: 14 out. 2025.

MICROSOFT. *Microsoft Bounty Programs | MSRC*. Redmond, 2025. Disponível em: https://www.microsoft.com/en-us/msrc/bounty. Acesso em: 10 out. 2025.

MICROSOFT. *Safe Harbor Policy*. 2025. Disponível em: https://www.microsoft.com/en-us/msrc/bounty-safe-harbor. Acesso em: 10 out. 2025.

MITRE. *CVE-2021-34527 Detail*. **MITRE CVE Database**, 2021. Disponível em: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34527. Acesso em: 14 out. 2025.

MSRC (MICROSOFT). *Microsoft Bug Bounty Year in Review: $17 Million in Rewards to 340 Researchers*. 2025. Disponível em: https://msrc.microsoft.com/blog/2025/08/. Acesso em: 10 out. 2025.

NIST – NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. *CVE-2025-4609: Descrição da vulnerabilidade*. Disponível em: https://nvd.nist.gov/vuln/detail/CVE-2025-4609. Acesso em: 7 out. 2025.

RESTREPO GÓMEZ, Jaime Andrés; CORREA ORTIZ, Luis Carlos. *Bug-bounty el futuro del pentesting?* **Ciencia e Ingeniería Neogranadina**, Bogotá, v. 1, p. 11–22, jun. 2024. Epub: 30 jun. 2024. Disponível em: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0124-81702024000100011. Acesso em: 26 abr. 2025.

SECURELIST (KASPERSKY). *PrintNightmare: Analysis of the Windows Print Spooler Vulnerability (CVE-2021-34527)*. Moscou, 2021. Disponível em: https://securelist.com/. Acesso em: 14 out. 2025.

SIMAN TOV BUSTAN, Moshe; ZADOK, Nir. *The aftermath of CVE-2025-4609: Critical sandbox escape leaves 1.5M developers vulnerable*. **OX Security**, 14 ago. 2025. Disponível em: https://www.ox.security/blog/the-aftermath-of-cve-2025-4609-critical-sandbox-escape-leaves-1-5m-developers-vulnerable/. Acesso em: 7 out. 2025.

VANTICO. *Pentest as a Service: do tradicional ao PtaaS*. 2025. Disponível em: https://vantico.com.br/transformacao-do-pentest-do-tradicional-ao-ptaas/. Acesso em: 30 set. 2025.

WIZ.IO. *CVE-2025-4609: Impacto, explorabilidade e etapas de mitigação*. Disponível em: https://www.wiz.io/vulnerability-database/cve/cve-2025-4609. Acesso em: 7 out. 2025.

YIN, R. K. *Estudo de caso: planejamento e métodos*. 5. ed. Porto Alegre: Bookman, 2015.

ZDNET. *PrintNightmare: Microsoft releases emergency Windows patch for Print Spooler bug*. **ZDNet**, 2021. Disponível em: https://www.zdnet.com/article/printnightmare-microsoft-releases-emergency-windows-patch-for-print-spooler-bug/. Acesso em: 14 out. 2025.