A IMPORTÂNCIA DO PROFISSIONAL DE CIBERSEGURANÇA E DO PENTESTING

THE IMPORTANCE OF THE CYBERSECURITY PROFESSIONAL AND PENTESTING

Luiz Felipe Borges Ribeiro[1]
Ana Carolina Nicolosi da Rocha Gracioso[2]

Resumo

Este trabalho analisa a importância da segurança da informação no ambiente corporativo, destacando o teste de intrusão (*pentest*) como uma ferramenta estratégica fundamental para a mitigação de riscos cibernéticos. A pesquisa fundamenta-se em revisão bibliográfica e na análise de um estudo de caso experimental baseado na metodologia de Piconi (2016), demonstrando como a execução de testes controlados protege ativos digitais e auxilia na conformidade com normas internacionais, como ISO/IEC 27001 e o NIST Cybersecurity Framework. O estudo aborda dados de mercado, contrastando a postura de empresas proativas *versus* reativas, e discute os desafios impostos pela escassez de profissionais qualificados. Conclui-se que a atuação do especialista em cibersegurança, aliada à prática contínua de *pentests*, é essencial para reduzir a superfície de ataque, minimizar prejuízos financeiros e fortalecer a resiliência operacional das organizações frente a ameaças crescentes.

Palavras-chave: Segurança da Informação. *Pentest*. Vulnerabilidades. Gestão de Riscos. Conformidade.

Abstract

This paper analyzes the importance of information security in the corporate environment, highlighting penetration testing (pentest) as a fundamental strategic tool for mitigating cyber risks. The research is based on a literature review and the analysis of an experimental case study based on Piconi's (2016) methodology, demonstrating how controlled testing protects digital assets and assists in compliance with international standards such as ISO/IEC 27001 and the NIST Cybersecurity Framework. The study addresses market data, contrasting the posture of proactive versus reactive companies, and discusses the challenges posed by the shortage of qualified professionals. It is concluded that the cybersecurity specialist's role, combined with continuous pentesting, is essential to reduce the attack surface, minimize financial losses, and strengthen organizational resilience against growing threats.

***Keywords**: Information Security. Pentest. Vulnerabilities. Risk Management. Compliance.*

[1] Acadêmico do curso de Análise e Desenvolvimento de Sistemas da FATEC Presidente Prudente. E-mail: luiz.ribeiro38@fatec.sp.gov.br.
[2] Docente da FATEC Presidente Prudente. E-mail: ana.gracioso@fatec.sp.gov.br.

1 INTRODUÇÃO

A sociedade contemporânea vivencia uma era em que a informação se tornou um dos ativos mais valiosos para indivíduos, organizações e governos. A transformação digital, impulsionada pela popularização da internet e pela adoção massiva de tecnologias da informação, trouxe consigo não apenas benefícios operacionais e estratégicos, mas também uma série de novos riscos.

Dentre esses riscos, destacam-se os relacionados à segurança da informação. O aumento exponencial de ataques cibernéticos tem exposto vulnerabilidades críticas em sistemas corporativos, resultando em prejuízos financeiros, danos à reputação e comprometimento de dados sensíveis. O custo médio global de uma violação de dados foi de US$ 4,45 milhões em 2023, e empresas que investem em práticas preventivas, como testes de intrusão, conseguiram reduzir esse impacto em até 45% (IBM, 2023).

Nesse cenário, a prática do teste de intrusão, ou *pentest*, emerge como uma ferramenta indispensável para a identificação de falhas antes que elas sejam exploradas por agentes maliciosos. O *pentest* simula ataques controlados, com o objetivo de descobrir vulnerabilidades em redes, sistemas e aplicações, permitindo que a organização tome medidas corretivas proativas.

Dessa forma, o objetivo geral deste estudo é analisar a importância do profissional de cibersegurança e da prática do *pentest* como estratégia essencial de mitigação de riscos nas organizações.

Especificamente, busca-se: descrever as principais ameaças e vulnerabilidades que comprometem a segurança da informação; destacar o papel e as competências do profissional de cibersegurança; apresentar como o *pentest* contribui para a prevenção de ataques e para a governança de TI; e discutir os impactos reais dos ataques, contrastando posturas proativas e reativas adotadas pelas empresas.

A justificativa deste estudo fundamenta-se na crescente dependência tecnológica das organizações e na escalada de incidentes cibernéticos que afetam tanto o setor público quanto o privado. Do ponto de vista acadêmico e científico, o trabalho amplia o debate sobre práticas preventivas e modelos de gestão de risco em segurança da informação. Sob a ótica prática, evidencia a necessidade de investimento em profissionais especializados e no uso sistemático de metodologias de teste de intrusão, favorecendo a resiliência operacional e a conformidade regulatória das empresas.

2 FUNDAMENTOS DA SEGURANÇA DA INFORMAÇÃO

A compreensão dos fundamentos da segurança da informação é essencial para o desenvolvimento de estratégias eficazes de proteção dos ativos digitais de uma organização. Esta seção aborda os conceitos básicos, princípios e diretrizes normativas que orientam a implementação de medidas de segurança, proporcionando uma visão estruturada sobre os principais pilares que sustentam a gestão da segurança da informação nas empresas.

2.1 Conceitos e Princípios

Segurança da informação é definida como o conjunto de práticas e controles destinados a proteger os ativos informacionais de uma organização contra acessos não autorizados, alterações indevidas, destruição ou interrupção. De acordo com a norma ISO/IEC 27001 (2022), a segurança da informação visa assegurar a confidencialidade, integridade e disponibilidade das informações — princípios que formam a conhecida tríade CID.

- Confidencialidade refere-se à garantia de que a informação seja acessada somente por pessoas autorizadas.
- Integridade assegura que a informação seja mantida exata e completa durante todo o seu ciclo de vida.
- Disponibilidade refere-se à acessibilidade das informações e sistemas sempre que necessário, por usuários autorizados.

Esses três pilares são interdependentes e essenciais para a proteção dos dados corporativos. O comprometimento de qualquer um deles pode causar sérios prejuízos a uma organização, tanto do ponto de vista financeiro quanto reputacional.

Além da tríade CID, autores como AMORIM (2020) acrescentam outros princípios relevantes, como autenticidade, responsabilidade, não repúdio e conformidade, os quais têm ganhado destaque em função da evolução das ameaças digitais e das exigências regulatórias.

2.2 Normas e Diretrizes

A adoção de normas e boas práticas é fundamental para o desenvolvimento de um Sistema de Gestão de Segurança da Informação (SGSI) eficaz. As principais normas que regulam e orientam a gestão da segurança são:

- A ISO/IEC 27001 estabelece os requisitos para um SGSI, incluindo políticas, processos e controles técnicos (ISO/IEC, 2022).
- A ISO/IEC 27002 fornece um código de práticas para controles de segurança da informação (ISO/IEC, 2022).
- NIST Cybersecurity Framework (CSF): desenvolvido pelo Instituto Nacional de Padrões e Tecnologia dos Estados Unidos, estrutura-se em cinco funções principais identificar, proteger, detectar, responder e recuperar e é amplamente utilizado por empresas de diferentes portes (NIST, 2018).

Essas normas promovem uma abordagem sistemática e baseada em riscos, permitindo que a organização identifique, avalie e trate suas vulnerabilidades de forma planejada e alinhada aos objetivos de negócio.

Além das normas técnicas, há também legislações específicas, como a Lei Geral de Proteção de Dados (LGPD) no Brasil, o Regulamento Geral sobre a Proteção de Dados (GDPR) na União Europeia e outras normas setoriais como a HIPAA (*Health Insurance Portability and Accountability Act*) nos Estados Unidos, voltada ao setor de saúde, e o PCI DSS (*Payment Card Industry Data Security Standard*), exigido de empresas que processam pagamentos eletrônicos. O descumprimento dessas normas pode acarretar sanções severas, reforçando a necessidade de práticas estruturadas de segurança da informação (ENISA, 2020).

A conformidade regulatória, portanto, não é apenas uma exigência legal, mas um componente essencial da estratégia de segurança da informação, sendo o *pentest* uma ferramenta que contribui diretamente para sua implementação e comprovação.

A integração da cibersegurança à governança corporativa tem crescido. Observa-se um aumento expressivo na inclusão de especialistas em segurança da informação nos conselhos administrativos, reforçando o papel estratégico do tema nas decisões organizacionais.

3 AMEAÇAS, VULNERABILIDADES E RISCO CIBERNÉTICO

Após a definição dos fundamentos da segurança da informação, torna-se imprescindível analisar as principais ameaças, vulnerabilidades e os riscos cibernéticos que afetam o ambiente corporativo. Esta seção tem como objetivo apresentar os diferentes tipos de ameaças existentes, as fragilidades mais exploradas por agentes maliciosos e a forma como esses riscos se materializam, impactando diretamente a continuidade dos negócios.

3.1 Ameaças mais comuns

As ameaças cibernéticas representam potenciais causas de incidentes de segurança da informação. Com a expansão da transformação digital, o número e a sofisticação dessas ameaças cresceram significativamente. Entre as mais comuns no ambiente corporativo, destacam-se:

- *Ransomware*: *software* malicioso que criptografa arquivos e exige pagamento para devolução do acesso.
- *Phishing*: fraude eletrônica que visa enganar usuários e coletar dados sensíveis.
- Ataques *DDoS (Distributed Denial of Service)*: sobrecarregam servidores com tráfego, tornando serviços indisponíveis.
- Exploração de vulnerabilidades conhecidas: ataques que se aproveitam de falhas em sistemas e *softwares* desatualizados.
- Engenharia social: manipulação psicológica de usuários para obtenção de acesso não autorizado, evidenciando a fragilidade do fator humano.

Segundo o relatório da Verizon, “74% dos incidentes de violação envolveram o elemento humano, incluindo ataques de engenharia social, erros ou uso indevido” (VERIZON, 2023).

3.2 Vulnerabilidades humanas e técnicas

Vulnerabilidade é uma fraqueza que pode ser explorada por uma ameaça para causar um impacto negativo à organização. Essas fragilidades podem ser técnicas ou humanas.

- Vulnerabilidades técnicas envolvem falhas de configuração, sistemas desatualizados, ausência de criptografia, uso de senhas fracas e falta de segmentação de rede.
- Vulnerabilidades humanas incluem comportamentos imprudentes, como clicar em links suspeitos, compartilhar senhas ou ignorar atualizações de segurança. A engenharia social explora justamente essas falhas comportamentais.

A maioria das vulnerabilidades humanas está relacionada à ausência de conscientização, falhas de treinamento e comportamentos inseguros por parte dos usuários. Diante disso, estratégias como campanhas educativas, simulações de phishing e capacitações contínuas são indicadas para mitigar esses riscos (ENGEBRETSON, 2013).

Um exemplo marcante ocorreu no caso Yahoo, em que investigações indicaram que práticas fracas de segurança — como o uso do algoritmo MD5 para armazenamento de senhas e a ausência de autenticação multifator — contribuíram para a escala dos danos. Isso demonstra que mesmo grandes corporações estão sujeitas a falhas humanas e técnicas quando não há uma cultura de segurança consolidada (REUTERS, 2016).

3.3 Conceito de risco cibernético

O risco cibernético pode ser definido como a possibilidade de que uma ameaça explore uma vulnerabilidade, causando impactos negativos aos ativos de informação. A ISO/IEC 27005 propõe que o risco seja mensurado pela combinação entre a probabilidade de ocorrência e a gravidade do impacto.

Risco Cibernético = Probabilidade × Impacto

Por exemplo, uma vulnerabilidade crítica não corrigida em um servidor *web*, quando exposta à internet, possui alta probabilidade de exploração, e o impacto pode envolver indisponibilidade do serviço e vazamento de dados. Essa combinação resulta em um risco elevado.

A gestão eficaz do risco cibernético exige identificação, análise, avaliação e tratamento dos riscos com base em prioridades. Entre as principais formas de tratamento, destacam-se ações preventivas que permitem antecipar falhas e responder proativamente. Essas estratégias fortalecem a resiliência organizacional frente a um cenário de ameaças cada vez mais sofisticado.

4 IMPACTOS REAIS DOS ATAQUES

Após compreender os principais conceitos de ameaças e riscos cibernéticos, é possível analisar como essas fragilidades se manifestam em situações reais. Empresas como Microsoft e Nubank ilustram como falhas específicas de segurança resultam em diferentes impactos operacionais e financeiros. Nesta seção, apresentam-se três estudos de caso que evidenciam os danos provocados por falhas na segurança da informação.

4.1 Estudo de Caso: Microsoft (2024)

Em janeiro de 2024, a Microsoft confirmou que teve partes do código-fonte de seus produtos comprometidas por um grupo conhecido como Midnight Blizzard. O ataque teve como vetor inicial o comprometimento de credenciais de uma conta corporativa de teste, sem autenticação multifator (MICROSOFT, 2024).

Impactos:

- Acesso não autorizado a e-mails de executivos e arquivos internos.
- Repercussão global com investigações regulatórias nos EUA e Europa.
- Revisão urgente de políticas de autenticação e resposta a incidentes.

A empresa foi considerada proativa por divulgar rapidamente o incidente, colaborar com autoridades e aplicar medidas de contenção e transparência, reforçando sua postura de *security by design*.

4.2 Estudo de Caso: 23andMe (2023)

Em 2023, a empresa de testes genéticos 23andMe foi alvo de um ataque massivo de *credential stuffing*, no qual hackers utilizaram combinações de usuário e senha vazadas em outras plataformas para acessar contas da base de clientes. A ausência de autenticação multifator obrigatória e a reutilização de senhas por parte dos usuários facilitaram o comprometimento das credenciais.

Impactos:

- Aproximadamente 14 mil contas foram acessadas indevidamente, o que permitiu ao atacante obter dados de mais de 6 milhões de pessoas conectadas por correspondência genética.
- As informações vazadas incluíam nomes, sexo, localização, ancestralidade genética e vínculos familiares.
- O incidente gerou repercussão internacional e levou à abertura de processos judiciais, investigações regulatórias e multas por parte de autoridades no Reino Unido e no Canadá.

A resposta da empresa foi predominantemente reativa. Medidas como o bloqueio de contas, redefinição de senhas e a implementação tardia de autenticação multifator só foram adotadas após a divulgação do incidente. O caso exemplifica os riscos de uma abordagem não preventiva à segurança da informação, especialmente quando se trata de dados extremamente sensíveis.

4.3 Estudo de Caso: Rede de Hospitais do Sul do Brasil (2025)

Segundo o portal Security Leaders (2025), a Unimed de Brusque, localizada no sul do Brasil, confirmou em fevereiro de 2025 um ataque de ransomware que afetou os sistemas internos e comprometeu agendamentos de exames e atendimentos.

Impactos:

- Suspensão de exames e adiamento de cirurgias eletivas.
- Necessidade de transferir pacientes para outras unidades.
- Perdas operacionais e risco à vida humana.

A resposta ao ataque revelou uma postura reativa. A ausência de testes de intrusão prévios, falta de backups atualizados e treinamento insuficiente da equipe contribuíram para a gravidade do incidente.

Esses estudos evidenciam a diferença entre empresas proativas, como Microsoft e Nubank, que mitigaram os impactos de forma eficaz, e instituições reativas, como a rede hospitalar, que enfrentaram grandes prejuízos pela ausência de uma cultura preventiva de segurança da informação.

4.4 Comparativo: Empresas Proativas vs Reativas

Com base em pesquisas recentes, é possível traçar um contraste nítido entre empresas que adotam estratégias proativas de segurança desde sua fundação e aquelas que só investem após incidentes significativos.

As empresas proativas, geralmente pertencentes aos setores financeiro, saúde, tecnologia e infraestrutura crítica, incorporam a cibersegurança desde o design de seus produtos e processos (*security by design*). Empresas como Google, Microsoft e Amazon adotam estratégias de segurança baseadas em ciclos contínuos de análise de vulnerabilidades. O Google, por exemplo, mantém a equipe Project Zero, criada para encontrar falhas críticas em softwares amplamente utilizados antes que sejam exploradas por atacantes (GOOGLE, 2025).

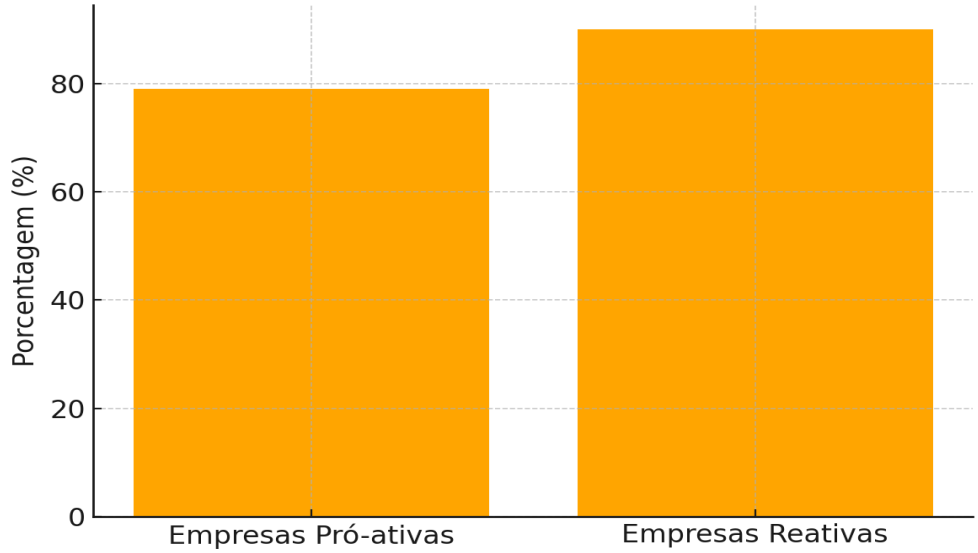
Essas empresas colhem benefícios como redução de riscos, ganho de reputação, maior confiança de clientes e economia de recursos a longo prazo. A Figura 1 apresenta a taxa de empresas que sofreram ataques cibernéticos, contrastando os perfis proativo e reativo, enquanto a Figura 2 ilustra o custo médio pós-incidente para cada perfil.

Estima-se que apenas 79% dessas empresas tenha sofrido algum tipo de ataque cibernético nos últimos dois anos, índice inferior aos 90% observados entre empresas reativas.

Por outro lado, as empresas reativas — comuns em setores como varejo, e-commerce e serviços médicos — tendem a investir em cibersegurança apenas após sofrerem violação de dados. Um exemplo marcante é o caso da Equifax, que em 2017 sofreu um vazamento de dados de quase 150 milhões de consumidores e, como consequência, comprometeu-se a pagar pelo menos US$ 575 milhões em um acordo com autoridades regulatórias dos Estados Unidos (EQUIFAX, 2019). Estimativas independentes indicam que o custo total do incidente pode ter ultrapassado US$ 1,6 bilhão, somando multas, indenizações e medidas de resposta.

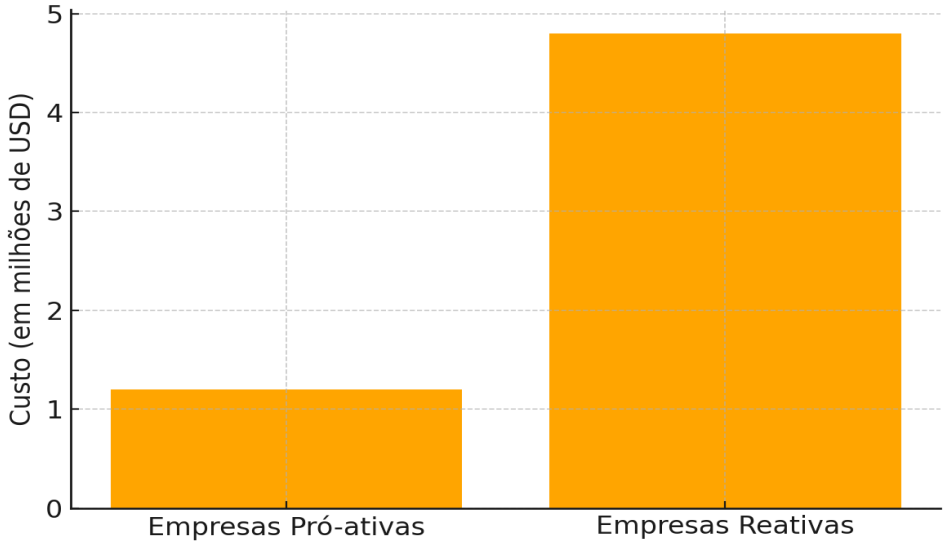
Um estudo da Security Leaders (2024) revelou que 79% das empresas no Brasil só aprovam orçamento para segurança após incidentes. Essa postura, além de financeiramente arriscada, compromete a resiliência organizacional frente a ameaças futuras.

Figura 1 – Taxa de empresas que sofreram ataques cibernéticos (%)



Fonte: Elaborado pelo autor com base em dados de IBM (2023), Verizon (2023) e Security Leaders (2024).

Figura 2 – Custo médio pós-incidente por perfil de empresa (em milhões de USD)



Fonte: Estimativa elaborada pelo autor com base nos casos da Equifax, e nas informações de IBM (2023), Cybersecurity Dive (2024) e Security Leaders (2024).

Essas visualizações reforçam que empresas proativas tendem a mitigar melhor os impactos financeiros e operacionais de ataques, tornando o investimento antecipado em práticas como o *pentest* uma medida mais eficaz e econômica.

Em síntese, empresas proativas integram o *pentest* à sua estratégia de governança e gestão de riscos, enquanto as reativas tendem a usá-lo como medida emergencial, o que compromete sua eficácia e previsibilidade.

5 PENTEST COMO FERRAMENTA DE PREVENÇÃO

Considerando o cenário de ameaças apresentado anteriormente, destaca-se a necessidade de adotar medidas preventivas que possibilitem a identificação e correção de vulnerabilidades antes que sejam exploradas. Nesse contexto, o *pentest* surge como uma das ferramentas mais relevantes para diagnosticar falhas e fortalecer a segurança dos sistemas. A seguir, serão detalados os conceitos, tipos e metodologias envolvidas na execução de testes de intrusão.

5.1 Definição e Tipos de Pentest

O teste de intrusão, conhecido como *pentest* (do inglês "*penetration test*"), é uma técnica proativa de avaliação da segurança de sistemas de informação. Consiste em simular ataques reais sob condições controladas com o objetivo de identificar e explorar vulnerabilidades antes que agentes mal-intencionados o façam.

De acordo com Bertóglio e Zorzo (2017), o *pentest* não visa apenas encontrar falhas, mas também avaliar o impacto e a viabilidade de sua exploração. Essa abordagem permite à organização corrigir proativamente seus pontos fracos.

Os principais tipos de p*entest* são:

- *Pentest* de Caixa Preta: o testador não possui nenhuma informação prévia sobre o ambiente-alvo. Simula o ponto de vista de um atacante externo.
- *Pentest* de Caixa Branca: o testador tem pleno acesso a informações internas, como código-fonte, arquitetura e credenciais. Simula uma auditoria interna.
- *Pentest* de Caixa Cinza: o testador possui acesso parcial a informações. Representa o cenário de um usuário interno mal-intencionado ou atacante com algum grau de conhecimento.

5.2 Fases da Execução

A condução de um *pentest* eficaz segue uma sequência de fases bem estabelecidas, como destacado por (PICONI, 2016):

1. Planejamento e Reconhecimento: definição do escopo, autorização formal e coleta de informações sobre os alvos.
2. Enumeração e Mapeamento: identificação de portas abertas, serviços ativos e possíveis vetores de ataque.
3. Análise de Vulnerabilidades: uso de ferramentas (como Nessus, Nmap, OpenVAS) para encontrar falhas conhecidas.
4. Exploração: tentativa de explorar as vulnerabilidades detectadas para obter acesso não autorizado.
5. Pós-exploração: verificação do nível de acesso obtido, possibilidade de movimentação lateral e coleta de provas de conceito.

6. Relatório: documentação detalhada dos achados, riscos associados e recomendações de correção.

Além das ferramentas mencionadas, outras amplamente utilizadas no contexto de *pentest* incluem:

- **Burp Suite**: especializada na análise de segurança de aplicações *web*, com foco em testes de injeção, XSS e controle de sessão.
- **OWASP ZAP (Zed Attack Proxy)**: scanner de segurança para aplicações *web* mantido pela comunidade OWASP, com funcionalidades de detecção automática e manual de falhas.

Essas ferramentas complementam as abordagens tradicionais e são especialmente úteis em testes focados na camada de aplicação. A escolha das ferramentas depende do escopo definido e da complexidade dos sistemas a serem avaliados. Cada fase deve ser executada com ética, responsabilidade e em conformidade com acordos contratuais para evitar implicações legais.

Em termos de mercado de trabalho, estima-se que havia cerca de 3,5 milhões de vagas não preenchidas em cibersegurança no mundo em 2023, e a previsão de crescimento é de aproximadamente 33% até 2033 (COURSERA, 2025). Isso indica que o investimento em *pentest* também exige planejamento de recursos humanos, capacitação técnica e parcerias estratégicas para superar a escassez de talentos.

5.3 Benefícios Estratégicos

Nesse contexto, organizações proativas têm adotado medidas estruturadas de capacitação interna, como academias corporativas de cibersegurança, programas de mentoria técnica, e parcerias com instituições educacionais como SENAI, FATEC e plataformas de cursos como Cisco Networking Academy e Coursera. Essas ações contribuem para formar profissionais alinhados às necessidades específicas da organização, além de promover uma cultura de aprendizagem contínua em segurança da informação.

Por fim, o *pentest* contribui diretamente para abordagens de *"security by design"*, alinhando segurança ao desenvolvimento de produtos e serviços desde o início. Empresas como Microsoft, Amazon e Google são referências nesse modelo, que reduz retrabalho, incidentes e custos com correções tardias.

6 ESTUDO DE CASO — SÍNTESE METODOLÓGICA

Após a abordagem teórica sobre o *pentest* e suas metodologias, apresenta-se uma síntese metodológica de um estudo de caso em ambiente de laboratório, com o objetivo de evidenciar, de forma descritiva, como as etapas de um *pentest* podem ser aplicadas para identificar e mitigar vulnerabilidades de maneira ética e controlada. O estudo é baseado na pesquisa desenvolvida por Piconi (2016), que aplicou um teste de intrusão em ambiente simulado com múltiplos sistemas operacionais.

6.1 Metodologia Utilizada

Esta seção apresenta uma análise do estudo de caso experimental realizado por Piconi (2016). O ambiente descrito por pelo autor foi estruturado com quatro máquinas virtuais — Windows XP, Windows 7, Ubuntu 8.10 e Kali Linux (máquina atacante) — configuradas propositalmente com falhas conhecidas, a fim de simular um cenário corporativo vulnerável.

As ferramentas empregadas incluíram: **Nmap** (varredura de portas e serviços), **Nessus** (detecção de vulnerabilidades), **Metasploit Framework** (exploração e execução de *payloads*), além de **Netcat** e **Hydra** (testes de autenticação).

O procedimento seguiu seis fases clássicas da metodologia de *pentest*:

1. Planejamento e definição de escopo;
2. Reconhecimento ativo e passivo;
3. *Scanning* e enumeração;
4. Identificação e exploração de vulnerabilidades;
5. Escalonamento de privilégios e manutenção de acesso;
6. Elaboração de relatório técnico e executivo.

Essa estrutura sistematizada permitiu reproduzir, de maneira controlada, um fluxo completo de análise e exploração de vulnerabilidades, representando fielmente as etapas de um teste de intrusão corporativo.

6.2 Resultados Obtidos

O estudo de caso confirma a eficácia do *pentest* como instrumento de diagnóstico e prevenção. A simulação revelou vulnerabilidades críticas que poderiam ser exploradas em um ataque real, reforçando a importância de testagens periódicas como parte integrante da estratégia de segurança da informação nas empresas.

No cenário Windows XP, foi identificada a vulnerabilidade MS08-067 (SMB), que permitiu a execução remota de código e elevação de privilégios. No **Windows 7**, verificaram-se falhas em serviços de rede, enquanto no **Ubuntu** foi detectada uma versão vulnerável do vsftpd (*Very Secure FTP Daemon*) contendo *backdoor* com acesso privilegiado remoto.

As explorações realizadas possibilitaram a obtenção de *shell* remoto, a captura de credenciais administrativas e a implantação de persistência no ambiente.

Entre as medidas corretivas recomendadas destacam-se:

- aplicação de *patches* de segurança e *hardening* dos serviços;
- implementação de autenticação multifator e políticas de senha forte;
- segmentação da rede com *VLANs* e *ACLs*;
- monitoramento contínuo com soluções *SIEM* e análise comportamental.

7 CONSIDERAÇÕES FINAIS

A segurança da informação representa atualmente um dos maiores desafios enfrentados pelas organizações no contexto da transformação digital. A crescente incidência de ataques cibernéticos e o impacto potencial sobre os ativos corporativos exigem ações preventivas, contínuas e alinhadas às melhores práticas internacionais.

Apresentou-se uma análise detalhada sobre a importância da segurança da informação nas empresas, com ênfase na prática do *pentest* como ferramenta de diagnóstico e prevenção. Foram abordados os conceitos fundamentais da segurança, as principais ameaças e vulnerabilidades, o conceito de risco cibernético, bem como exemplos reais de ataques que demonstram as consequências de falhas nos controles de proteção.

A prática do *pentest* revelou-se eficaz e indispensável para:

- Identificar vulnerabilidades técnicas e comportamentais antes que sejam exploradas.
- Avaliar a maturidade e a resiliência da infraestrutura de TI.
- Apoiar a conformidade com normas como ISO/IEC 27001, LGPD, PCI DSS e HIPAA.

- Sensibilizar equipes internas sobre a importância da cibersegurança.

Além disso, observou-se que empresas que integram o *pentest* à sua cultura organizacional — de forma proativa e planejada — tendem a apresentar maior resiliência, menor índice de incidentes e redução significativa de custos operacionais e reputacionais. Dados de mercado mostram que essas organizações colhem benefícios como aumento da confiança dos consumidores, vantagem competitiva e eficiência regulatória.

A crescente escassez de profissionais especializados e a complexidade dos ecossistemas digitais tornam ainda mais relevante a institucionalização do *pentest* como componente da governança de segurança da informação. A prática deve estar alinhada aos objetivos estratégicos da organização, promovendo não apenas proteção, mas também inovação segura e sustentabilidade de longo prazo.

7.1 Aspectos Éticos e Dilemas do Pentest

A prática do *pentest* (teste de intrusão), embora essencial, levanta importantes questões éticas que não devem ser negligenciadas. Conforme argumenta (Dunn Cavelty, 2014), a segurança deve equilibrar as necessidades de proteção com os direitos à privacidade e à transparência. Testes de intrusão, mesmo autorizados, devem respeitar limites legais, escopos bem definidos e a confidencialidade das informações manipuladas.

Exemplos práticos reforçam esses dilemas. Em ambientes de infraestrutura crítica, como hospitais ou sistemas industriais SCADA, a simulação de ataques pode comprometer a operação real, exigindo planejamento rigoroso para não interromper serviços essenciais. Há também dilemas sobre testes realizados sem o conhecimento prévio de todos os envolvidos, o que pode gerar conflito entre realismo e ética.

Certificações reconhecidas internacionalmente, como a *Offensive Security Certified Professional* (OSCP) e a *Certified Ethical Hacker* (CEH), estabelecem códigos de ética que reforçam a conduta profissional esperada:

- Realizar testes apenas com autorização formal e explícita.
- Garantir integridade dos dados durante os testes.
- Documentar todas as ações e comunicar riscos de forma clara.

O profissional ético de segurança deve manter integridade, respeitar os contratos estabelecidos, garantir o consentimento explícito e evitar ações que possam impactar

negativamente os sistemas testados. Assim, o *pentest* se consolida não apenas como uma prática técnica, mas como um exercício de responsabilidade profissional e de governança organizacional, que exige sensibilidade para os contextos legais, humanos e sociais em que se aplica.

7.2 Limitações do estudo e perspectivas futuras

Como limitação, este trabalho baseia-se em revisão bibliográfica e em casos públicos, sem experimentação em ambientes corporativos reais, o que restringe a mensuração quantitativa de benefícios e custos.

Para pesquisas futuras, recomenda-se a realização de estudos de campo que apliquem *pentest* em organizações de diferentes portes e setores, com o objetivo de mensurar impacto e retorno sobre o investimento (ROI). Sugere-se, ainda, a investigação do uso de inteligência artificial e automação em testes de intrusão e monitoramento, bem como análises setoriais — nos segmentos de saúde, finanças e governo — considerando requisitos regulatórios específicos. Entretanto, é importante ressaltar que experimentos em ambientes simulados, como o analisado, oferecem uma aproximação valiosa dos riscos, permitindo estimar prejuizos e justificar inventimentos preventivos.

REFERÊNCIAS

AMORIM, J. R. Fundamentos de segurança da informação. 2. ed. São Paulo: Novatec, 2020.

BERTÓGLIO, D. D.; ZORZO, A. F. Overview and open issues on penetration test. Journal of the Brazilian Computer Society, v. 23, n. 2, 2017. Disponível em: https://doi.org/10.1186/s13173-017-0051-1. Acesso em: 20 mai. 2025.

COURSERA. Your Cybersecurity Career Guide for 2025: Pay, Jobs + More. 2025. Disponível em: https://www.coursera.org/articles/cybersecurity-career-guide. Acesso em: 24 mai. 2025.

CYBERSECURITY DIVE. Where organizations invest after a data breach. 2024. Disponível em: https://www.cybersecuritydive.com/news/data-breach-recovery-investments/. Acesso em: 24 mai. 2025.

DUNN CAVELTY, M. Breaking the cyber-security dilemma: Aligning security needs and removing vulnerabilities. Science and Engineering Ethics, v. 20, p. 701–715, 2014.

ENISA – EUROPEAN UNION AGENCY FOR CYBERSECURITY. Threat Landscape for the Energy Sector. Heraklion: ENISA, 2020. Disponível em: https://www.enisa.europa.eu/publications/threat-landscape-for-the-energy-sector. Acesso em: 24 mai. 2025.

ENGEBRETSON, P. The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy. 2. ed. Waltham: Elsevier, 2013.

FEDERAL TRADE COMMISSION – FTC. Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach. 22 jul. 2019. Disponível em: https://www.ftc.gov/news-events/news/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related-2017-data-breach. Acesso em: 4 mai. 2025.

GOOGLE. Project Zero. Disponível em: https://googleprojectzero.blogspot.com/. Acesso em: 24 mai. 2025.

IBM. Cost of a Data Breach Report 2023. Ponemon Institute. Disponível em: https://www.ibm.com/reports/data-breach. Acesso em: 15 mai. 2025.

ISO/IEC 27001. Information technology — Security techniques — Information security management systems — Requirements. International Organization for Standardization, 2022.

ISO/IEC 27002**.** Information technology — Security techniques — Code of practice for information security controls. International Organization for Standardization, 2022.

ISO/IEC 27005. Information security risk management. International Organization for Standardization, 2018.

MASTERCARD. Investimento em cibersegurança ainda não é prioridade para empresas, aponta Datafolha. Newsroom Mastercard Brasil, 2024. Disponível em: https://www.mastercard.com/news/latin-america/pt-br/noticias/comunicados-de-imprensa/pr-pt/mais-que-cartao/ciberseguranca/investimento-em-ciberseguranca-ainda-nao-e-prioridade-para-empresas-aponta-datafolha/. Acesso em: 24 mai. 2025.

MICROSOFT. Microsoft Actions Following Attack by Nation State Actor Midnight Blizzard. Microsoft Security Response Center (MSRC), 19 jan. 2024. Disponível em: https://www.microsoft.com/en-us/msrc/blog/2024/01/microsoft-actions-following-attack-by-nation-state-actor-midnight-blizzard. Acesso em: 12 abr. 2025.

MISHRA, S. et al. Impact of human vulnerabilities on cybersecurity. Computer Systems Science and Engineering, v. 39, n. 2, p. 503–517, 2021.

NIST. Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. National Institute of Standards and Technology, 2018.

PICONI, R. C. A importância do pentest para os negócios de uma empresa. Trabalho de Conclusão de Curso (Tecnologia em Segurança da Informação) – Faculdade de Tecnologia de Americana, Americana, 2016.

REUTERS. Yahoo security problems a story of too little, too late. 2016. Disponível em: https://www.reuters.com/article/technology/yahoo-security-problems-a-story-of-too-little-too-late-idUSKBN1480AM. Acesso em: 03 mai. 2025.

SECURITY LEADERS. Pesquisa revela que 79% das empresas só investem em cibersegurança após invasão. 2024. Disponível em: https://securityleaders.com.br/pesquisa-revela-que-79-das-empresas-so-investem-em-ciberseguranca-apos-invasao/. Acesso em: 24 mai. 2025.

SECURITY MANAGEMENT. 23andMe Data Breach Compromises Millions of Genetic Profiles. ASIS International, 04 dez. 2023. Disponível em: https://www.asisonline.org/security-management-magazine/latest-news/today-in-security/2023/december/23andme-data-breach/. Acesso em: 04 maio. 2025.

TI INSIDE. A importância da cibersegurança proativa para o sucesso dos negócios. 25 mar. 2024. Disponível em: https://tiinside.com.br/25/03/2024/a-importancia-da-ciberseguranca-proativa-para-o-sucesso-dos-negocios/. Acesso em: 24 mai. 2025.

UNITED STATES. Federal Trade Commission. Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach. 2019. Disponível em: https://www.ftc.gov/news-events/news/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related-2017-data-breach. Acesso em: 20 abr. 2025.

VERIZON. Data Breach Investigations Report 2023. Disponível em: https://www.verizon.com/business/resources/reports/2023-data-breach-investigations-report-dbir.pdf Acesso em: 18 mai. 2025