

HACKING ÉTICO COMO ESTRATÉGIA DE FORTALECIMENTO DA SEGURANÇA DIGITAL

ODS (16)

O avanço da digitalização nas esferas pessoal, empresarial e governamental tem ampliado os riscos relacionados à segurança da informação, o que demanda a adoção de novas abordagens preventivas. Em resposta a esses desafios, o hacking ético surge como uma estratégia fundamental para a proteção digital. Trata-se da aplicação de conhecimentos técnicos especializados na identificação e correção de vulnerabilidades em sistemas computacionais, sempre de forma autorizada e em conformidade com a legislação vigente. Este trabalho tem como propósito analisar as práticas de hacking ético adotadas por instituições públicas e privadas, destacando seus benefícios para a segurança digital e a construção de confiança junto aos usuários. Para atingir esse objetivo, a metodologia adotada neste estudo é de caráter qualitativo e exploratório, voltada principalmente para a análise de conteúdos teóricos que abordam a atuação dos hackers éticos, suas certificações e os limites éticos e legais que regem essa prática, bem como os benefícios decorrentes para organizações públicas e privadas. Observa-se um aumento significativo da oferta de cursos e treinamentos especializados em hacking ético, os quais têm como finalidade preparar profissionais qualificados para atuarem com responsabilidade e respeito aos parâmetros legais, reforçando a importância da formação contínua para o fortalecimento da segurança digital. Destaca-se ainda que empresas como Facebook, Google e Microsoft incentivam a prática do hacking ético por meio de programas de recompensa monetária, nos quais pesquisadores externos são remunerados ao reportar vulnerabilidades de maneira responsável, demonstrando a relevância dessas iniciativas para a construção de ambientes digitais mais seguros. Com base na análise, os resultados da revisão apontam que, quando realizado de forma responsável, o hacking ético desempenha um papel relevante na prevenção de ataques cibernéticos, no reforço à proteção de dados e na promoção de uma cultura voltada à segurança digital. Os artigos sobre hacking ético reforçam essa relevância ao destacar a prática como estratégia de fortalecimento da segurança digital, abordando aspectos técnicos, educacionais e legais, mas ainda apontando desafios como a ausência de métricas claras e de evidências sobre seus efeitos a longo prazo. Além disso, destaca-se o papel educativo do tema, já que a disseminação do conhecimento sobre práticas éticas na área de tecnologia da informação pode contribuir tanto para a formação de profissionais mais preparados quanto para a conscientização da sociedade em relação à importância da segurança digital. Considerando os resultados obtidos, conclui-se que o hacking ético representa uma ferramenta estratégica fundamental para a proteção dos ambientes digitais. Para seu fortalecimento, é essencial que as instituições promovam o desenvolvimento de setores internos dedicados ao hacking ético ou incentivem programas externos que envolvam usuários na identificação de vulnerabilidades, o que não só aprimora a segurança dos sistemas, como também contribui para a construção de uma imagem institucional positiva e de credibilidade. Ao fortalecer a transparência, a resiliência e a eficiência dos sistemas digitais, essas práticas se relacionam diretamente com os



objetivos do ODS 16, que busca promover instituições mais eficazes, responsáveis e seguras.

Palavras-chave: Hacking ético; Segurança digital; Responsabilidade institucional; Práticas éticas; Cibersegurança.