Segurança da informação como estratégia de gestão: avaliação de treinamentos personalizados para prevenção de phishing

Information security as a management strategy: assessment of personalized training for phishing prevention

Seguridad de la información como estrategia de gestión: evaluación de entrenamientos personalizados para la prevención del phishing

Como citar:

Silva, Ana Clara M. & D'Alkmin Neves, João Emmanuel (2026). Segurança da informação como estratégia de gestão: avaliação de treinamentos personalizados para prevenção de phishing. Revista Gestão & Tecnologia, vol. 26, nº 2, p: 216-241

Ana Clara Matthiesen Silva, Profa. Faculdade de Tecnologia de Americana Ministro Ralph Biasi
https://orcid.org/0009-0005-2738-2197

João Emmanuel D'Alkmin Neves, Doutor em Tecnologia pela Universidade Estadual de Campinas, docente do Ensino Superior na FATEC Americana e Editor da Revista Tecnológica da Fatec Americana.
https://orcid.org/0000-0002-9472-9753

"Os autores declaram não haver qualquer conflito de interesse de natureza pessoal ou corporativa, em relação ao tema, processo e resultado da pesquisa"

Editor Científico: José Edson Lara
Organização Comitê Científico
Double Blind Review pelo SEER/OJ
Recebido em 19/07/2025
Aprovado em 09/06/2026

Resumo

Objetivo: Investigar a eficácia de diferentes estratégias de treinamento adaptativo na redução da vulnerabilidade humana frente a ataques de *phishing* em ambientes organizacionais, por meio de simulação computacional baseada em agentes.

Metodologia: O estudo utiliza modelagem baseada em Sistemas Multiagentes (SMA) para simular o comportamento de usuários, atacantes e treinadores em um ecossistema organizacional. Foram testadas quatro estratégias de treinamento, baseadas em diferentes métricas internas, além de um cenário de controle, totalizando 125 execuções na plataforma NetLogo, com análise quantitativa das métricas de desempenho.

Originalidade: A pesquisa responde a uma lacuna na literatura sobre segurança organizacional ao avaliar comparativamente estratégias de capacitação baseadas em critérios gerenciais, aplicando SMA como ferramenta preditiva e exploratória no apoio à tomada de decisão em cibersegurança.

*Principais resultados***:** Todas as estratégias superaram o cenário de controle. A estratégia Aleatória demonstrou maior estabilidade e eficácia na contenção de ataques, seguida pela abordagem baseada em Risco, ambas com ampla cobertura entre os grupos simulados

Contribuições metodológicas: O estudo contribui para o avanço do uso de SMA em problemas de segurança da informação, evidenciando seu potencial para simular interações complexas entre comportamento humano e decisões estratégicas em organizações.

Contribuições para a gestão: Apresenta implicações práticas para gestores, ao oferecer evidências sobre a eficácia de estratégias de conscientização e apoiar a alocação inteligente de recursos em políticas de segurança mais eficazes.

Palavras-chave: Segurança da Informação, phishing, Sistemas Multiagentes, Treinamento Corporativo, Gestão de Riscos

Abstract

Objective: To investigate the effectiveness of different adaptive training strategies in reducing human vulnerability to phishing attacks in organizational environments, through agent-based computational simulation.

Methodology: The study employs modeling based on Multi-Agent Systems (SMA) to simulate the behavior of users, attackers, and trainers within an organizational ecosystem. Four training strategies were tested, each based on different internal metrics, in addition to a control scenario, totaling 125 executions on NetLogo platform, with quantitative analysis of performance metrics.

Originality: The research addresses a gap in the literature on organizational security by comparatively evaluating training strategies based on managerial criteria, applying MAS as a predictive and exploratory tool to support cybersecurity decision-making.

Main results: All strategies outperformed the control scenario. The Random strategy showed greater stability and effectiveness in mitigating attacks, followed by the Risk-based approach, both achieving broad coverage across simulated groups.

Methodological contributions: The study advances the application of SMA to information security problems, demonstrating its potential to simulate complex interactions between human behavior and strategic decisions in organizations.

Management contributions: It presents practical implications for managers by providing evidence on the effectiveness of awareness strategies and supporting the intelligent allocation of resources to more effective security policies.

Keywords: Information Security, phishing, Multi-Agent Systems, Corporate Training, Risk Management

Resumen

Objetivo: Investigar la eficacia de diferentes estrategias de capacitación adaptativa en la reducción de la vulnerabilidad humana frente a ataques de phishing en entornos organizacionales, mediante simulación computacional basada en agentes.

Metodología: El estudio emplea modelado basado en Sistemas Multiagente (SMA) para simular el comportamiento de usuarios, atacantes y entrenadores dentro de un ecosistema organizacional. Se probaron cuatro estrategias de entrenamiento basadas en diferentes métricas internas, además de un escenario de control, totalizando 125 ejecuciones en la plataforma NetLogo, con análisis cuantitativo de métricas de desempeño.

Originalidad: La investigación responde a una laguna en la literatura sobre seguridad organizacional al evaluar comparativamente estrategias de capacitación basadas en criterios gerenciales, aplicando SMA como herramienta predictiva y exploratoria en el apoyo a la toma de decisiones sobre ciberseguridad.

Resultados principales: Todas las estrategias superaron el escenario de control. La estrategia Aleatoria mostró mayor estabilidad y eficacia en la contención de ataques, seguida por el enfoque basado en Riesgo, ambas con amplia cobertura entre los grupos simulados.

Contribuciones metodológicas: El estudio contribuye al avance del uso de SMA en problemas de seguridad de la información, demostrando su potencial para simular interacciones complejas entre el comportamiento humano y decisiones estratégicas en organizaciones.

Contribuciones para la gestión: Presenta implicaciones prácticas para los gestores, al ofrecer evidencias sobre la eficacia de las estrategias de concientización y apoyar la asignación inteligente de recursos en políticas de seguridad más eficaces.

Palabras claves: Seguridad de la Información, phishing, Sistemas Multiagente, Capacitación Corporativa, Gestión de Riesgos

1. Introdução

A transformação digital tem reconfigurado profundamente a dinâmica organizacional, exigindo que empresas adotem tecnologias em nuvem e criem ecossistemas altamente conectados, nos quais a integração entre sistemas, pessoas e processos se torna fundamental para a continuidade e competitividade dos negócios. No entanto, essa crescente dependência de tecnologias digitais também ampliou a superfície de exposição a riscos cibernéticos, entre os quais se destaca o *phishing*, que é uma ameaça que compromete a segurança organizacional ao explorar o elo mais vulnerável da cadeia: o fator humano (Vilela; Ueda & Gava, 2023).

No campo da Administração, a Gestão de Riscos e a Governança da Informação são pilares essenciais para garantir a eficiência operacional, a integridade dos dados e a continuidade dos negócios (Chiavenato, 2021; Maximiano, 2022). Nesse contexto, a Segurança da Informação deixa de ser uma preocupação exclusivamente técnica e passa a ocupar espaço estratégico na agenda corporativa, exigindo o envolvimento de gestores e líderes na formulação de políticas, na alocação de recursos e na promoção de uma cultura organizacional orientada à segurança (Laudon & Laudon, 2020).

O phishing, em sua essência, representa uma forma de engenharia social que manipula as limitações cognitivas humanas para obter acesso não autorizado a sistemas, credenciais e informações sensíveis. Essa tática tem evoluído rapidamente, acompanhando o avanço tecnológico e adaptando-se às deficiências comportamentais dos usuários, o que torna sua prevenção um desafio organizacional relevante (Tonezer *et al.*, 2024). Mesmo diante da ampla adoção de programas de conscientização, os incidentes continuam a crescer, indicando que estratégias convencionais de treinamento não têm sido suficientemente eficazes (Chiew; Yong & Tan, 2018).

Diante desse cenário, torna-se fundamental investigar abordagens mais eficazes de mitigação de riscos que aliem tecnologia, comportamento organizacional e estratégias adaptativas de capacitação. A hipótese central deste estudo é que treinamentos personalizados e dinâmicos, adaptados ao contexto e perfil dos usuários, podem aumentar significativamente a resiliência organizacional contra ataques de *phishing*.

Este trabalho propõe a análise e a simulação de estratégias de treinamento utilizando Sistemas Multiagentes (SMA), com o objetivo de compreender o comportamento dos usuários diante de ataques e identificar quais métodos de capacitação apresentam maior eficácia na redução da vulnerabilidade humana. Ao observar o impacto de diferentes critérios de priorização na tomada de decisão e no desempenho organizacional, espera-se contribuir para a construção de políticas de segurança mais eficazes, com base em evidências comportamentais.

A relevância deste estudo está ancorada na necessidade das organizações modernas de alinhar suas práticas de segurança à estratégia empresarial, fortalecendo a proteção de seus ativos informacionais e garantindo sua sustentabilidade no mercado. Assim, este trabalho busca integrar as abordagens da Administração com os princípios da Segurança da Informação, promovendo uma visão sistêmica, proativa e centrada no fator humano, como forma de enfrentar os desafios contemporâneos impostos pelas ameaças cibernéticas.

2. Referencial teórico

Esta seção abordará os Fundamentos da Engenharia Social e *Phishing*, com ênfase em suas implicações para a gestão de riscos organizacionais; os Modelos de Treinamento em Segurança da Informação, analisando-os como instrumentos estratégicos de gestão de pessoas e cultura organizacional; e, por fim, a aplicação de SMA como suporte à tomada de decisão gerencial em contextos de segurança da informação.

2.1 Engenharia social, *phishing* e as implicações para a gestão de risco organizacional

A engenharia social é um conjunto de técnicas utilizadas para manipular indivíduos com o objetivo de obter informações confidenciais, acesso a sistemas ou realizar ações que favoreçam atacantes mal-intencionados. Diferente de ataques puramente técnicos, a engenharia

social explora vulnerabilidades humanas, como a confiança, a curiosidade e o medo, o que a torna uma das principais ameaças à Segurança da Informação (Hadnagy, 2018).

O conceito de engenharia social não é recente, com relatos históricos indicando que técnicas de manipulação psicológica foram utilizadas desde os primórdios da comunicação interpessoal. No contexto digital, a engenharia social ganhou relevância na década de 1980, quando surgiram os primeiros ataques baseados na confiança. Com o avanço da conectividade global e a popularização da Internet, a engenharia social se consolidou como uma ameaça predominante em ambientes corporativos e pessoais, refletindo a crescente dependência de plataformas digitais para comunicação e transações (Tonezer et al., 2024).

Ao longo do tempo, diferentes formas de ataques baseados em engenharia social foram desenvolvidas, sendo o *phishing* uma das mais comuns. O *phishing* consiste em tentativas fraudulentas de obtenção de informações sensíveis, como credenciais de acesso e dados bancários, por meio da simulação de entidades confiáveis. Originalmente disseminado via e-mail, o *phishing* expandiu-se para diversas plataformas, incluindo redes sociais, mensagens instantâneas e telefonemas, refletindo a evolução contínua das técnicas empregadas pelos atacantes (Chiew; Yong & Tan, 2018).

Esses ataques podem ser classificados de acordo com a abordagem adotada pelos criminosos e o público-alvo. Entre as técnicas mais frequentemente empregadas, destaca-se o *phishing* tradicional, que consiste no envio de e-mails fraudulentos que imitam comunicações legítimas de instituições como bancos, empresas ou organizações governamentais. Esses e-mails contêm, normalmente, endereços falsos que direcionam as vítimas para páginas da *web* maliciosas, onde são induzidas a fornecer credenciais de acesso e informações pessoais (Khonji; Iraqi & Jones, 2013).

Uma variação do phishing tradicional é o *spear phishing*, que se caracteriza por ser um ataque altamente direcionado. Nesse caso, os atacantes realizam pesquisas detalhadas sobre as vítimas, explorando redes sociais e bancos de dados vazados para obter informações específicas, o que torna o ataque convincente. O objetivo é criar mensagens personalizadas que induzam o alvo ao erro de forma mais eficaz do que no *phishing* tradicional (Fornasier; Knebel & Silva, 2020).

Dentro das estratégias mais sofisticadas, o *whaling* se destaca como uma forma de *spear phishing* voltada para indivíduos de altos cargos, como executivos, diretores ou autoridades governamentais. O foco desse ataque é obter informações privilegiadas ou autorizações que possibilitem transações financeiras fraudulentas ou o acesso a dados sensíveis (Resnick & Bastos-Filho, 2024).

Além dessas abordagens, existem variações que envolvem a utilização de canais diferentes para enganar as vítimas. O *vishing*, ou *voice phishing*, é uma técnica que envolve chamadas telefônicas fraudulentas, nas quais os atacantes se passam por representantes de instituições legítimas, com o objetivo de obter informações sensíveis da vítima. De maneira similar, o *smishing* utiliza mensagens de texto (SMS) contendo links maliciosos ou instruções enganosas, com a finalidade de induzir as vítimas a executar ações prejudiciais (Vilela; Ueda & Gava, 2023).

Outra técnica comum é o *clone phishing*, que ocorre quando os atacantes replicam e-mails legítimos já recebidos pela vítima, modificando os links ou anexos para versões maliciosas. Como o e-mail aparenta familiar à vítima, há uma maior probabilidade de que ela confie no conteúdo e interaja com ele, expondo-se a riscos (Tonezer et al., 2024).

Por fim, o *pharming* é uma técnica avançada de *phishing* que visa redirecionar os usuários para sites fraudulentos, mesmo quando o endereço correto é digitado no navegador. Esse tipo de ataque pode ser realizado por meio da manipulação do sistema de nomes de domínio (DNS) ou pela infecção de dispositivos com malware que altera configurações de rede, conduzindo a vítima a páginas da *web* falsas sem seu conhecimento (Chiew; Yong & Tan, 2018).

Essas técnicas, cada uma com suas características e complexidades, demonstram a diversidade e sofisticação dos ataques de *phishing*, que evoluem constantemente em resposta às medidas de segurança adotadas para combatê-los (Khonji; Iraqi & Jones, 2013).

A eficácia desses ataques está intimamente relacionada à exploração de vulnerabilidades cognitivas e emocionais dos usuários. Com o tempo, as estratégias de manipulação psicológica utilizadas pelos criminosos evoluíram, tornando-se cada vez mais sofisticadas e difíceis de detectar. Esses ataques se aproveitam de diversas abordagens psicológicas, visando criar

condições que induzam a vítima a tomar decisões precipitadas, sem a devida análise crítica (Hadnagy, 2018).

Uma das estratégias mais comuns envolve a indução de um senso de urgência, com mensagens que pressionam a vítima a agir rapidamente, geralmente sem considerar a veracidade da solicitação. Exemplos típicos incluem alegações de problemas em contas bancárias, notificações sobre prazos curtos para atualização de informações ou ameaças de bloqueio de serviços, que buscam gerar um estado de pânico e apressar a tomada de decisão (Resnick & Bastos-Filho, 2024).

Outra técnica amplamente utilizada é a manipulação da autoridade e da confiança. Criminosos se passam por representantes de instituições respeitáveis, como bancos, órgãos governamentais ou superiores hierárquicos, a fim de aumentar a credibilidade das mensagens fraudulentas. Esse uso da autoridade tem como objetivo convencer os usuários a fornecerem informações sensíveis ou a executarem ações específicas sem questionamento (Vilela; Ueda & Gava, 2023).

Além disso, com o avanço das redes sociais e a crescente disponibilidade de dados através de vazamentos e perfis públicos, os ataques de *phishing* passaram a incorporar uma abordagem mais personalizada. Ao utilizar informações detalhadas sobre as vítimas, os criminosos tornam suas mensagens fraudulentas mais convincentes e difíceis de detectar, aproveitando-se do conhecimento prévio sobre o comportamento e preferências dos indivíduos (Fornasier & Knebel; Silva, 2020).

A evolução das tecnologias também contribuiu para a sofisticação dos ataques, com a introdução de *chatbots* e Inteligência Artificial. Esses sistemas são capazes de simular interações humanas em tempo real, respondendo a perguntas de maneira convincente, o que eleva ainda mais a eficácia dos ataques de *phishing* ao criar uma sensação de familiaridade e autenticidade (Tonezer et al., 2024).

Embora muitos ataques de *phishing* utilizem o medo e a urgência para manipular as vítimas, alguns exploram emoções positivas como estratégia. Campanhas fraudulentas que oferecem brindes, descontos exclusivos ou oportunidades de investimento atraentes são

exemplos de como os criminosos utilizam promessas de recompensa para seduzir vítimas desavisadas, levando-as a tomar decisões sem a devida cautela (Khonji; Iraqi & Jones, 2013).

Essas estratégias de manipulação psicológica demonstram a complexidade crescente dos ataques de *phishing*, que se adaptam constantemente ao comportamento dos usuários e à evolução das tecnologias, tornando cada vez mais difícil a sua detecção e prevenção (Chiew; Yong & Tan, 2018).

Tais ameaças não apenas afetam a dimensão técnica da organização, mas impactam diretamente suas estratégias gerenciais, exigindo que a gestão da segurança da informação seja integrada ao planejamento estratégico e às práticas de governança corporativa. A construção de uma cultura organizacional voltada à segurança é, portanto, uma responsabilidade transversal que envolve todos os níveis hierárquicos, desde a alta direção até os colaboradores operacionais (Bateman & Snell, 2017 e Robbins & Coulter, 2020).

Tais ameaças não apenas afetam a dimensão técnica da organização, mas impactam diretamente suas estratégias gerenciais, exigindo que a gestão da segurança da informação seja integrada ao planejamento estratégico e às práticas de governança corporativa. A construção de uma cultura organizacional voltada à segurança é, portanto, uma responsabilidade transversal que envolve todos os níveis hierárquicos, desde a alta direção até os colaboradores operacionais (Bateman & Snell, 2017; Robbins & Coulter, 2020).

2.2 Treinamentos de segurança como estratégia de gestão de pessoas e cultura

A Segurança da Informação permanece como um dos pilares fundamentais para a proteção de ativos organizacionais em um cenário digital marcado por ameaças cibernéticas cada vez mais sofisticadas e frequentes. Os métodos tradicionais de conscientização, amplamente empregados por empresas e instituições, caracterizam-se por campanhas periódicas, palestras expositivas e distribuição de materiais informativos estáticos, como cartilhas impressas e *e-mails* educativos. Embora tais abordagens ofereçam uma introdução inicial aos conceitos básicos de segurança, apresentam deficiências significativas quanto à sua efetividade e sustentabilidade ao longo do tempo (Moura & D'Alkmin Neves, 2021).

Dentre as principais limitações, destacam-se a baixa retenção do conteúdo transmitido, a reduzida participação ativa dos colaboradores e a carência de métricas precisas para mensuração do impacto das ações. Ademais, esses treinamentos tendem a ignorar as particularidades dos distintos perfis de usuários dentro das organizações, resultando em iniciativas descontextualizadas, com pouco impacto na mudança comportamental dos indivíduos. Do ponto de vista gerencial, essa lacuna compromete não apenas a eficácia técnica das ações, mas também o alinhamento entre os treinamentos e os objetivos estratégicos organizacionais, o que pode gerar desperdício de recursos, baixa adesão dos colaboradores e perda de vantagem competitiva em setores que exigem conformidade normativa e alta resiliência digital (Robbins & Coulter, 2020).

A falta de atualização dos conteúdos, bem como a superficialidade na abordagem de ameaças emergentes, também compromete a eficácia desses modelos (Aduku; Lawal & Baballe, 2024).

Esse panorama evidencia a urgência em revisar práticas convencionais de capacitação em Segurança da Informação, buscando metodologias mais dinâmicas, interativas e personalizadas, capazes de promover maior engajamento dos usuários e consolidar uma cultura organizacional orientada à segurança (Moura & D'Alkmin Neves, 2021).

Nesse cenário, o avanço das tecnologias educacionais e da Inteligência Artificial tem viabilizado a adoção de metodologias inovadoras, entre as quais o treinamento adaptativo e o aprendizado baseado em simulação como abordagens promissoras e efetivas para a capacitação de usuários (Souza *et al*., 2024).

A integração dessas abordagens ao planejamento de Recursos Humanos permite que a Segurança da Informação deixe de ser tratada como um setor isolado e passe a integrar a gestão por competências, atuando como diferencial competitivo e critério de performance gerencial.

O treinamento adaptativo se apoia em algoritmos inteligentes capazes de ajustar, em tempo real, o conteúdo e o nível de complexidade das atividades de ensino, com base no desempenho e no perfil do aprendiz. Essa abordagem permite identificar lacunas de conhecimento de forma individualizada, fornecendo *feedbacks* contínuos e direcionados. Como

resultado, há um aumento do engajamento e da efetividade do aprendizado, promovendo o desenvolvimento de competências críticas de maneira mais eficiente (Tan *et al*., 2020).

Por sua vez, o aprendizado baseado em simulação proporciona um ambiente controlado onde os usuários podem interagir com cenários realistas de incidentes cibernéticos, como ataques de *phishing*, disseminação de *ransomware* ou tentativas de engenharia social. A simulação permite que os participantes pratiquem decisões sob pressão e observem as consequências de suas ações sem comprometer a infraestrutura real da organização (Kavak *et al*., 2021). Essa abordagem experiencial contribui para a consolidação de conhecimentos práticos e para o fortalecimento da consciência situacional dos usuários, tornando-os mais preparados para enfrentar ameaças reais.

Ambas as metodologias superam as limitações dos modelos tradicionais ao promover aprendizado ativo, personalizado e contextualizado. No entanto, sua implementação exige investimentos em infraestrutura tecnológica, bem como apoio institucional para integração com políticas de segurança já existentes.

Nesse sentido, a diversidade de perfis entre os usuários de sistemas corporativos representa um dos principais desafios na elaboração de treinamentos eficazes em Segurança da Informação. A adoção de modelos personalizados de capacitação surge, assim, como uma estratégia fundamental para garantir que os conteúdos sejam significativos do ponto de vista do contexto e das responsabilidades de cada colaborador (Aduku; Lawal & Baballe, 2024).

A personalização dos treinamentos pode ser realizada com base em múltiplos critérios, tais como o setor de atuação do colaborador, sua função na organização, histórico de incidentes, nível de familiaridade com tecnologias e resultados anteriores em avaliações de segurança. Por meio dessas informações, é possível desenvolver trilhas de aprendizagem individualizadas, com foco nos riscos mais relevantes para cada grupo, otimizando o tempo de treinamento e os recursos disponíveis (Tan *et al*., 2020).

Além disso, ferramentas baseadas em Inteligência Artificial e em análise comportamental permitem o monitoramento contínuo das interações dos usuários com sistemas digitais, identificando padrões de risco e ajustando os conteúdos dos treinamentos de forma proativa (Souza *et al*., 2024). Essa abordagem responsiva permite alinhar os treinamentos às

ameaças mais recentes e específicas do ambiente organizacional, promovendo uma formação mais ágil e eficaz.

A personalização não apenas potencializa os resultados pedagógicos das ações de conscientização, mas também amplia a percepção de relevância dos treinamentos por parte dos usuários, promovendo maior adesão às práticas recomendadas de segurança (Kavak *et al*., 2021).

Além disso, a adoção de treinamentos alinhados à estratégia organizacional e à gestão de competências contribui para a formação de um capital humano resiliente, que atua de forma proativa frente a riscos e ameaças. A gestão de pessoas passa a desempenhar papel essencial na criação de ambientes de aprendizagem contínua, engajamento e responsabilidade, aspectos fundamentais para o fortalecimento da segurança organizacional (Fleury & Fleury, 2000).

2.3 Sistemas multiagentes como suporte à tomada de decisão gerencial em segurança da informação

Os SMA representam uma abordagem computacional inspirada em sistemas distribuídos e inteligentes, nos quais múltiplos agentes autônomos interagem em um ambiente comum, cooperando e/ou competindo para alcançar objetivos individuais ou coletivos. Esses agentes são entidades computacionais dotadas de capacidade de percepção, decisão e ação, operando de forma autônoma, adaptativa e, muitas vezes, comunicativa (Wooldridge, 2009).

A natureza descentralizada dos SMA os torna particularmente apropriados para domínios complexos e dinâmicos, como a Segurança da Informação. Neste contexto, os SMA podem ser empregados para monitorar ambientes computacionais, detectar padrões anômalos, coordenar respostas a incidentes e implementar estratégias dinâmicas de defesa. O uso de múltiplos agentes permite a divisão de tarefas, a redundância de operações críticas e a ampliação da resiliência contra falhas e ataques (Neves, 2024).

As aplicações de SMA abrangem desde a simulação de fenômenos sociais e econômicos até sistemas embarcados e industriais, com destaque recente para a incorporação de técnicas de aprendizado por reforço em múltiplos agentes. Tal integração tem proporcionado avanços significativos na adaptação e cooperação entre agentes em ambientes hostis ou parcialmente

observáveis, o que se alinha diretamente com os desafios enfrentados na proteção de infraestruturas digitais (Albrecht; Christianos & Schäfer, 2024).

Nesse contexto, uma das vertentes mais promissoras do uso de SMA na Segurança da Informação reside na modelagem e simulação de comportamentos humanos. Ao utilizar agentes para representar usuários com diferentes perfis e intenções (legítimos ou maliciosos), é possível construir cenários realistas que auxiliem na análise de riscos, detecção de vulnerabilidades e avaliação de políticas de segurança (Neves *et al*., 2023).

Modelos baseados em agentes permitem a incorporação de características individuais e coletivas, como preferências, padrões de navegação, hábitos de consumo e níveis de conformidade com normas de segurança. Tais simulações oferecem suporte à compreensão de comportamentos emergentes em ambientes complexos, como redes corporativas ou infraestruturas críticas (Neves, 2021). Além disso, possibilitam a execução de experimentos que seriam impraticáveis ou inseguros no mundo real.

A modelagem de comportamentos humanos em sistemas computacionais também pode ser enriquecida por técnicas de mineração de dados, que extraem padrões e correlações a partir de grandes volumes de informação, alimentando os agentes com regras e probabilidades mais próximas da realidade (Neves, 2024). Esse processo confere maior verossimilhança aos modelos e amplia a sua utilidade para a formulação de políticas preventivas e corretivas em segurança cibernética.

Nesse mesmo escopo, a aplicação de agentes inteligentes na Segurança da Informação está diretamente relacionada à sua capacidade de perceber ameaças, aprender com interações passadas e reagir de forma autônoma e coordenada. Em SMA voltados à defesa, agentes podem assumir papéis como monitoramento de tráfego de rede, detecção de intrusões, análise de logs, gerenciamento de vulnerabilidades e resposta automatizada a incidentes (He *et al*., 2022).

Os autores Albrecht, Christianos e Schäfer (2024) destacam a importância da robustez e da resiliência desses sistemas frente a ataques maliciosos, sobretudo em arquiteturas distribuídas. Estratégias de controle seguro, baseadas em redundância, consenso e monitoramento distribuído, são fundamentais para garantir a continuidade dos serviços e a integridade dos dados, mesmo diante de comprometimentos parciais da rede.

Adicionalmente, o uso de aprendizado por reforço multiagente tem proporcionado avanços substanciais na definição de políticas defensivas adaptativas. Ao interagirem com o ambiente e com outros agentes, os sistemas podem aprender táticas de defesa eficientes, inclusive em situações de adversidade e incerteza, como ocorre em ataques de dia zero ou em campanhas persistentes avançadas (Wooldridge, 2009).

Um exemplo de aplicação inovadora de SMA para ser adaptado ao contexto de segurança cibernética é a simulação de ataques de *phishing*, onde são utilizadas técnicas complexas para testar a vulnerabilidade de sistemas. Essas abordagens destacam a versatilidade dos SMA na integração de fontes heterogêneas de informação e na tomada de decisões em tempo real (Neves *et al*., 2023).

Do ponto de vista da Administração, os SMA podem ser utilizados como ferramentas de apoio à decisão, oferecendo simulações baseadas em dados que auxiliam gestores na formulação de políticas mais assertivas. A análise preditiva de comportamento organizacional, viabilizada por tais sistemas, representa uma importante inovação no campo da inteligência estratégica e da análise de riscos corporativos (Davenport & Harris, 2017).

Ao mesmo tempo, os SMA oferecem aos gestores dados para avaliação preditiva e monitoramento de tendências comportamentais, permitindo o redesenho de políticas de segurança de forma alinhada à gestão estratégica organizacional. Tal alinhamento é essencial para que as políticas deixem de ser reativas e se tornem instrumentos proativos de resiliência institucional (Bateman & Snell, 2017).

3. Metodologia

A metodologia deste estudo foi desenvolvida para criar um modelo robusto de simulação baseado em SMA, com o objetivo de avaliar estratégias de treinamento e conscientização no combate a ataques de *phishing.* Inicialmente, foi realizada uma pesquisa bibliográfica exploratória, abrangendo artigos nas áreas de Engenharia Social, Segurança da Informação e simulações SMA, coletados em bases como Google Acadêmico e IEEE Xplore, que fundamentaram teoricamente o desenvolvimento do modelo.

Além disso, a abordagem metodológica reflete princípios da Administração Estratégica ao propor a simulação como ferramenta de apoio à tomada de decisão, permitindo observar o impacto de diferentes alocações de recursos em treinamentos e a gestão eficiente do risco humano.

Para sua implementação, utilizou-se a ferramenta NetLogo, reconhecida por sua flexibilidade e interface intuitiva, permitindo representar comportamentos emergentes a partir das interações dinâmicas entre três tipos principais de agentes: usuários, atacantes e treinadores, os quais simulam um sistema organizacional realista de defesa contra *phishing.*

A seguir, são detalhadas as características, comportamentos e lógicas implementadas para cada espécie de agente, bem como o fluxo geral da simulação.

3.1 Usuários

Os usuários representam os elementos mais numerosos e diversos da simulação, correspondendo a indivíduos de um sistema organizacional que estão suscetíveis a ataques de *phishing*. Estes agentes são organizados em grupos, refletindo diferentes equipes ou departamentos dentro de uma organização. Cada grupo possui características independentes, influenciando diretamente o comportamento coletivo e individual dos demais agentes na simulação.

A variabilidade entre os usuários é introduzida por meio de diferentes níveis de suscetibilidade inicial e influência, definidos a partir de um valor atribuído dentro dos intervalos estipulados para cada grupo. Essa abordagem permite explorar a heterogeneidade típica de sistemas reais.

Sob a ótica da gestão organizacional, essa variabilidade reflete a heterogeneidade presente em equipes reais, marcada por diferentes perfis comportamentais, níveis de conhecimento e graus de exposição ao risco. Esse cenário demanda estratégias de capacitação mais personalizadas e alinhadas às necessidades específicas de cada grupo, reforçando a importância da gestão estratégica de pessoas e do desenvolvimento contínuo. As principais variáveis atribuídas aos usuários são:

Suscetibilidade Inicial: probabilidade de o usuário cair em um ataque antes de receber qualquer treinamento, refletindo fatores individuais como atenção, perfil comportamental e conhecimento prévio.

Conscientização: nível de conhecimento e vigilância em relação a ataques de *phishing*. Inicia em zero e aumenta com treinamentos ou interações com o grupo.

Informação: valor representativo dos dados sensíveis sob sua responsabilidade, indicando a criticidade do conjunto de informações que poderia ser comprometido e o impacto potencial de um ataque bem-sucedido.

Suscetibilidade Real: valor dinâmico que representa a probabilidade atual de o usuário ser vítima de *phishing*, considerando sua Suscetibilidade Inicial, Conscientização e o estado do ambiente.

Estado de Alerta: variável booleana que, ativada quando um usuário atinge um determinado nível de consciência e identifica uma tentativa de *phishing*, reduz temporariamente a Suscetibilidade Real própria e dos demais usuários do grupo.

O modelo explora, assim, tanto a heterogeneidade individual quanto a dinâmica de grupo: usuários com diferentes perfis reagem a treinamentos e alertas, e interações coletivas promovem um aprendizado progressivo, refletindo colaboração, comunicação e cultura organizacional, aspectos centrais da gestão de pessoas e do comportamento organizacional.

3.2 Atacantes

Os atacantes representam agentes maliciosos cujo objetivo é realizar ataques de *phishing* contra os usuários e acumular informações críticas. Cada ataque é direcionado a um grupo específico, simulando campanhas coordenadas, abordagem baseada em táticas de *spear-phishing*, que visam maximizar o impacto ao atingir múltiplos alvos simultaneamente.

No contexto da gestão da informação, o acúmulo de dados sensíveis pelos atacantes representa uma falha de governança informacional, cujos impactos afetam diretamente a continuidade e a reputação da organização.

A cada tentativa de ataque, o atacante seleciona um grupo-alvo e avalia individualmente os usuários pertencentes a esse grupo. Quando um ataque é bem-sucedido, o atacante obtém

uma fração do valor de Informação do usuário atingido, aumentando assim sua variável de Informações Adquiridas. Esse acúmulo gradual representa o impacto cumulativo de ataques anteriores, criando um efeito de escalada: quanto mais informações o atacante acumula, mais eficaz ele tende a se tornar em ataques futuros. Esse mecanismo simula as consequências reais de falhas de segurança em ambientes organizacionais, onde vazamentos com informações críticas têm potencial de fortalecer ataques futuros. Esse efeito de escalada permite, na ótica gerencial, observar como decisões não preventivas podem acarretar custos operacionais crescentes, alinhando-se a modelos de análise de risco corporativo.

A Probabilidade de Sucesso de um ataque é definida por uma função construída especificamente para este modelo, com base em parâmetros operacionais e comportamentais do sistema. Trata-se de uma estimativa heurística que representa a chance de um atacante obter sucesso ao tentar comprometer um usuário. A função combina dois fatores centrais:

A Suscetibilidade Real (SR) do alvo, que reflete sua vulnerabilidade atual;

O volume de Informações Adquiridas (Info) do atacante, que representa sua capacidade ofensiva acumulada.

A fórmula utilizada para esse cálculo é:

$$P_{sucesso} = \left(\frac{SR}{100}\right) \times \left(1 + \frac{Info}{100}\right)$$

Esse cálculo retorna um valor entre 0 e 1, representando a chance de o ataque ser bem-sucedido. A função modela o equilíbrio entre o nível de defesa do usuário e a força ofensiva do atacante, permitindo analisar a evolução dos riscos ao longo do tempo e a eficácia das contramedidas implementadas, os treinamentos.

3.3 Treinadores

Os treinadores são os agentes que desempenham o comportamento central na análise da simulação. Como agentes responsáveis por implementar estratégias de treinamento em grupo para reduzir a suscetibilidade dos usuários aos ataques de *phishing*. A sua atuação simula o papel de gestores de segurança ou líderes de treinamento corporativo que devem tomar decisões baseadas em indicadores de desempenho e alocação estratégica de recursos.

Eles são os únicos agentes com acesso às variáveis globais do modelo, o que lhes permite analisar métricas e escolher o grupo-alvo para treinamento, de acordo com a estratégia selecionada pelo observador. A simulação propõe 4 estratégias de treinamento a serem analisadas:

A **Estratégia de Volume** funciona de forma que grupos que detém maior incidência de ataques são escolhidos para receber o treinamento. Essa escolha é feita com a contagem de ataques recebidos por cada grupo, elegendo os que foram focalizados em ataques.

A **Estratégia de Risco** foca nos grupos com a maior Média de Suscetibilidade, e, portanto, perfis mais vulneráveis a ataques de *phishing*. Essa lógica utiliza da variável que calcula a SR Média de cada grupo, selecionando entre os grupos mais suscetíveis

A **Estratégia por Perdas** seleciona o grupo com maior volume acumulado de dados vazados até o momento da simulação. Essa estratégia baseia-se na listagem de informações cedidas por grupo, permitindo os treinadores priorizar grupos que causaram maior dano à segurança.

A **Estratégia Aleatória** seleciona o grupo a ser treinado de forma randômica, sem influência das métrica. Essa abordagem propõe uma distribuição neutra de treinamentos entre os grupos, permite analisar os efeitos de uma alocação equitativa e imparcial de treinamentos.

Cada estratégia reflete um estilo distinto de gestão, podendo ser associada a decisões reativas, proativas ou distribuídas, conceitos amplamente discutidos em gestão estratégica e gestão de pessoas.

À medida que a simulação avança, o impacto dos treinamentos aumenta progressivamente, refletindo o acúmulo de aprendizado e experiência no sistema. Esse efeito é comparável ao desenvolvimento contínuo de competências organizacionais e à consolidação de uma cultura de segurança, elementos fundamentais para a sustentabilidade da gestão. Essa dinâmica é implementada de forma que cada novo treinamento se torne mais eficaz em elevar os níveis de conscientização dos usuários ao longo do tempo.

A metodologia para análise dos resultados foi realizada por meio da execução sistemática do modelo em diferentes cenários. Foram conduzidas 25 execuções independentes para cada uma das quatro estratégias de treinamento propostas, totalizando 100 simulações completas.

Cada execução teve duração de 100 ciclos (*ticks*), com ambiente composto por 15 grupos organizacionais, cada um contendo 20 usuários, além de 10 atacantes e 5 treinadores. Além disso, foi incluído um cenário de controle, simulações sob as mesmas condições, porém sem a atuação de treinadores, permitindo avaliar o comportamento do sistema na ausência de estratégias de conscientização. Durante as execuções os dados gerados pelos agentes foram exportados em arquivos CSV estruturados, contendo os valores das variáveis a cada ciclo, viabilizando a posterior análise quantitativa dos resultados.

Essa abordagem permite avaliar, sob a ótica gerencial, como diferentes políticas de capacitação influenciam os resultados organizacionais ao longo do tempo, fornecendo subsídios quantitativos para a tomada de decisão baseada em evidências.

4. Apresentação e discussão dos resultados

A seguir, são apresentados os resultados obtidos a partir das simulações, com foco na comparação entre as quatro estratégias de treinamento propostas (Volume, Perdas, Risco e Aleatória) e um cenário de controle sem treinadores. A análise considerou métricas-chave relacionadas à dinâmica dos usuários e atacantes, como a evolução da SR média, o volume de informações vazadas e a taxa de sucesso dos ataques. Os dados foram agregados em médias por *tick*, com seus respectivos intervalos de confiança, permitindo observar a evolução temporal das variáveis e avaliar a consistência dos resultados coletados. Os gráficos apresentados mostram a média dos resultados das execuções por estratégia, e a faixa de intervalo de confiança calculada em 95%, assumindo média com distribuição aproximadamente normal.

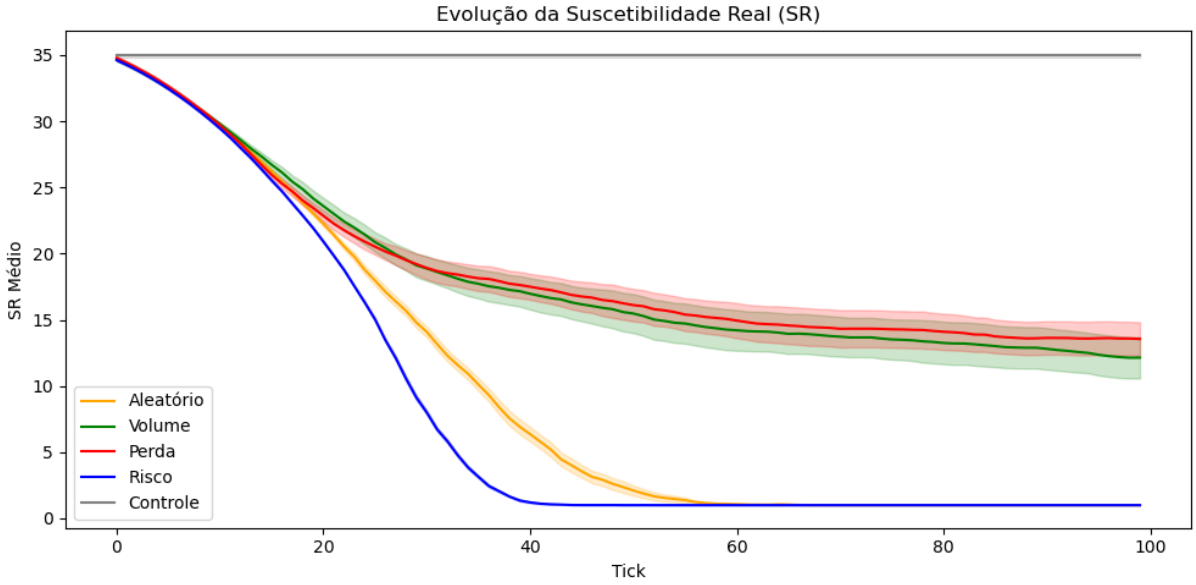

Figura 1: Evolução da Suscetibilidade Real Média dos usuários

Como pode ser observado na Figura 01, em todas as estratégias os treinadores foram capazes de diminuir consideravelmente a suscetibilidade a ataques. Esse resultado reforça a importância de políticas organizacionais de treinamento contínuo e customizado como parte integrante da gestão de riscos operacionais e humanos. As estratégias de Risco e Aleatória se destacam por levarem essa métrica a um nível mínimo de forma consistente, esses resultados podem ser atribuídos ao foco específico sobre essa variável e à equidade na seleção dos grupos para o treinamento ao longo do período de execução. Quanto às outras estratégias, Volume e Perda, o desempenho inferior se deve à tendenciosidade criada a partir de agentes externos independentes que, neste modelo, operam com uma certa imprevisibilidade. Essa natureza do ambiente deprime a eficácia dessas estratégias que esperam padrões de ataque, gerando atenção desigual entre os grupos, resultando em lacunas passíveis de exploração. Tais lacunas evidenciam como falhas na alocação estratégica de recursos humanos e treinamentos podem ampliar os riscos organizacionais, comprometendo a eficácia da gestão de segurança.

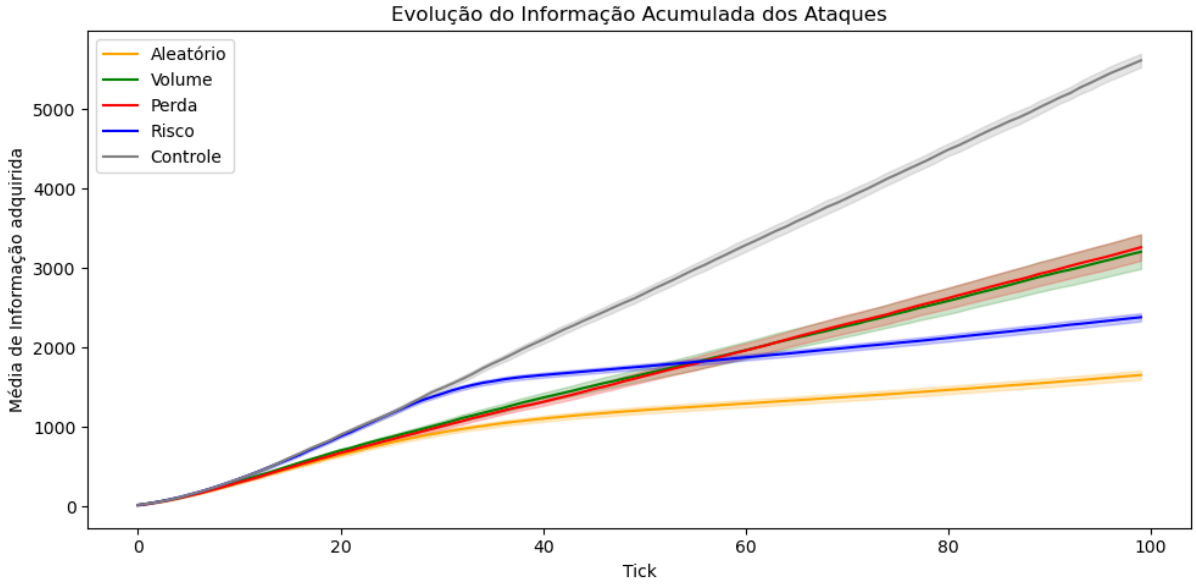

Figura 2: Evolução de informação acumulada dos atacantes

O comportamento observado na Figura 02, assim como observado na métrica de SR, as Estratégias Aleatória e de Risco apresentaram os melhores desempenhos, sendo a primeira superior em termos de estabilidade e contenção do avanço dos atacantes. Esse resultado destaca a relevância da equidade e abrangência na política de capacitação, alinhando-se aos princípios de gestão participativa e distribuição eficiente de recursos. Por outro lado, a Estratégia Risco apresentou um pico inicial mais acentuado de informações vazadas nos primeiros ciclos, antes de sua curva começar a declinar. Esse comportamento está relacionado à lógica da simulação, na qual os grupos com menor valor de informação tendem a ter maior suscetibilidade inicial. Assim, enquanto os treinadores priorizam esses grupos vulneráveis, os atacantes exploram os grupos que detêm maiores volumes de informação, os quais demoram mais a se tornar prioridade no treinamento, permitindo um acúmulo inicial mais expressivo. Essa dinâmica pode ser interpretada como uma consequência da priorização tática de curto prazo, um dilema clássico enfrentado na administração entre decisões imediatas e planejamento estratégico.

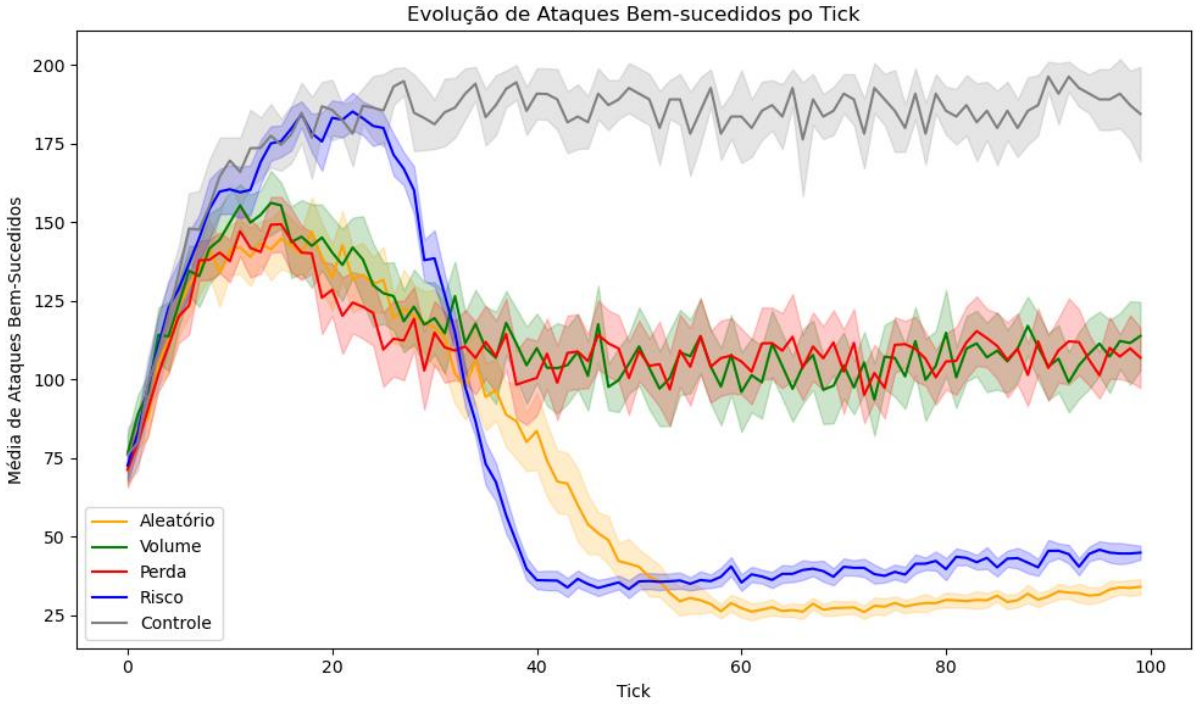

Figura 3: Evolução de ataques bem-sucedidos por tick

O comportamento observado na Figura 03 apresenta uma variabilidade significativamente maior que as demais analisadas, uma vez que depende diretamente do grupo-alvo selecionado em cada ataque, uma escolha aleatória que pode afetar consideravelmente os resultados entre as execuções. É importante destacar que, em todos os ciclos da simulação, ocorrem exatamente 200 ataques simultâneos, resultantes da atuação de 10 atacantes. Além disso, como escolha de modelagem próxima à realidade, foi definido que a probabilidade de sucesso de um ataque nunca pode ser nula, mesmo em condições em que a suscetibilidade é mínima, refletindo o risco residual presente mesmo em sistemas bem protegidos.

Portanto, A Figura 03 evidencia novamente o padrão observado anteriormente: a estratégia de Risco apresenta um pico inicial acentuado, seguido por uma queda na eficácia dos ataques, comportamento diretamente ligado ao fato de que os grupos mais suscetíveis inicialmente detêm menos informações críticas, permitindo que os atacantes ganhem força rapidamente antes que os grupos mais valiosos se tornem prioridade no treinamento.

Os resultados sugerem que abordagens proativas e distribuídas na gestão de treinamentos tendem a ser mais eficazes na mitigação de riscos cibernéticos, ao passo que abordagens

reativas (como Volume ou Perda) podem falhar em ambientes com alta variabilidade. Mesmo com essa fragilidade inicial, foi capaz de reduzir o sucesso ofensivo para cerca de 21,44% no intervalo final da execução. A estratégia Aleatória foi a que melhor conteve os ataques aos últimos ciclos de simulação, mantendo uma média de apenas 30 ataques bem-sucedidos por *tick,* o que equivale a aproximadamente 15% de efetividade ofensiva, ou seja, 84,96% dos ataques foram frustrados. Tais achados têm implicações diretas para gestores que precisam decidir entre estratégias de capacitação com foco em risco individual, impacto financeiro ou abrangência organizacional.

Por outro lado, as estratégias de Volume e Perda apresentaram desempenhos medianos, permitindo que mais da metade dos ataques tivessem sucesso. Ainda assim, ambas foram superiores ao cenário de controle, no qual, com o acúmulo contínuo de informações pelos atacantes, a taxa de sucesso manteve-se próxima de 90%, evidenciando o impacto da ausência de treinamentos.

5. Conclusão

Este estudo abordou de forma integrada os desafios contemporâneos da Segurança da Informação e da Gestão Organizacional, simulando estratégias de treinamento frente a ataques de engenharia social em ambientes corporativos. A partir da modelagem baseada em SMA, foi possível representar de maneira dinâmica a complexidade de um ecossistema organizacional realista, onde indivíduos com diferentes perfis comportamentais e graus de conhecimento interagem sob constante risco cibernético.

Os resultados obtidos indicam que, contrariamente à expectativa inicial, a estratégia Aleatória de treinamento foi a que apresentou melhor desempenho médio na contenção de ataques de *phishing.* Essa abordagem, ao distribuir os treinamentos de forma equitativa entre os grupos, evitou a formação de lacunas vulneráveis frequentemente exploradas por atacantes. Já a estratégia baseada em risco mostrou bons resultados ao priorizar usuários mais suscetíveis, embora sua eficácia dependa de ajustes táticos, especialmente no que diz respeito ao momento e à priorização de grupos com maior valor informacional.

Do ponto de vista da Gestão, essas descobertas reforçam a importância da tomada de decisão baseada em dados, da alocação inteligente de recursos de treinamento e da compreensão do comportamento organizacional como variável estratégica. Abordagens de conscientização mais simples, quando aplicadas de maneira uniforme e planejada, podem ser tão ou mais eficazes do que estratégias complexas que dependem de previsões de comportamento adversário. Isso se alinha com princípios da Administração contemporânea, como a gestão adaptativa, o desenvolvimento contínuo de pessoas, e a promoção de culturas organizacionais resilientes.

Além disso, o modelo proposto oferece uma ferramenta de apoio à tomada de decisão gerencial na área de cibersegurança, permitindo testar, em ambiente simulado e controlado, os efeitos de diferentes abordagens. Em termos aplicados, trata-se de uma contribuição relevante para o campo da gestão de riscos e da governança da informação, especialmente em tempos em que o fator humano permanece como principal vetor de vulnerabilidade.

As limitações do modelo, como a ausência de inteligência adaptativa nos atacantes e a representação simplificada dos perfis de usuários, não diminuem seu valor, ao contrário, apontam caminhos promissores para aprofundamentos futuros. A incorporação de variáveis de desempenho organizacional, perfis comportamentais baseados em modelos de gestão de competências, e ataques mais sofisticados tornaria o sistema ainda mais representativo do mundo corporativo real.

Dessa forma, este estudo contribui para o avanço do conhecimento técnico e gerencial, demonstrando que a integração entre Segurança da Informação e Administração Estratégica é não apenas possível, mas necessária. Em um cenário onde as ameaças evoluem mais rapidamente do que os sistemas de proteção, a capacidade de simular, analisar e intervir preventivamente torna-se uma vantagem competitiva decisiva. Promover a consciência digital entre colaboradores, com base em estratégias bem planejadas e embasadas em modelos organizacionais, não é mais uma vantagem, é uma necessidade da gestão moderna.

Referências

Albrecht, S. V., Christianos, F., & Schäfer, L. (2024). *Multi-agent reinforcement learning: Foundations and modern approaches*. MIT Press. https://www.marl-book.com

Bateman, T. S., & Snell, S. A. (2017). *Administração: Princípios e aplicações* (11ª ed.). Cengage Learning.

Chiew, T. K., Yong, K. S. C., & Tan, C. L. (2018). A survey of phishing attacks: Their types, vectors and technical approaches. *Expert Systems with Applications*, 106, 1–20. https://doi.org/10.1016/j.eswa.2018.03.057

Davenport, T. H., & Harris, J. G. (2017). *Competing on Analytics, Updated, with a New Introduction: The New Science of Winning*. Harvard Business Review Press.

Fleury, A. C. C., & Fleury, M. T. L. (2000). *Estratégias empresariais e formação de competências*. Atlas.

Fornasier, M. O., Knebel, N. M. P., & Silva, F. V. (2024). Phishing e Engenharia Social: entre a criminalização e a utilização de meios sociais de proteção. *Meritum: Revista de Derecho de la Universidad FUMEC*, 15(1), 123-140. https://doi.org/10.46560/meritum.v15i1.7771

Hadnagy, C. (2018). *Social engineering: The science of human hacking* (2nd ed.). John Wiley & Sons.

He, W., Xu, W., Ge, X., Han, Q., Du, W., & Qian, F. (2022). Secure control of multiagent systems against malicious attacks: a brief survey. *IEEE Transactions on Industrial Informatics*, 18(6), 3595-3608. https://doi.org/10.1109/TII.2021.3126644

Kavar, H., Padilla, J. J., Vernon-Bido, D., Diallo, S. Y., Gore, R., & Shetty, S. (2021). Simulation for cybersecurity: state of the art and future directions. *Journal of Cybersecurity*, 7(1). https://doi.org/10.1093/cybsec/tyab005

Khonji, M., Iraqi, Y., & Jones, A. (2013). Phishing Detection: A Literature Survey. *IEEE Communications Surveys & Tutorials*, 15(4), 2091-2121. https://doi.org/10.1109/SURV.2013.032213.00009

Laudon, K. C., & Laudon, J. P. (2020). Sistemas de informação gerenciais (14ª ed.). Pearson.

Livingston, S. A., Sarafadeen, L. L., & Muhammad, A. B. (2024). Human-Centric Cybersecurity: Behavioral Insights and Strategic Approaches for Enhanced Awareness. *Global Journal of Research in Engineering & Computer Sciences*, 4(6), 107–113. gjrpublication. https://doi.org/10.5281/zenodo.14497164

Maximiano, A. C. A. (2022). *Teoria Geral da Administração* (9ª ed.). Atlas.

Moura, T. M., & D' Alkmin Neves, J. E. (2021). Análise de segurança em dispositivos internet das coisas. *Revista Interface Tecnológica*, 18(2), 15-27. https://doi.org/10.31510/infa.v18i2.1174

Neves, J. E. D. (2024). *Mineração de dados aplicada a simulação de cenários complexos em sistemas multiagentes* [Tese de doutorado, Universidade Estadual de Campinas]. Repositório Institucional da UNICAMP. https://www.repositorio.unicamp.br/acervo/detalhe/1395946

Neves, J. E. D. A. (2021). Modelo Baseado em Agentes para Simulação de Consumo de Energia Elétrica em Função do Comportamento Humano. *Revista Eletrônica Anima Terra*, 12, 89-103. https://fatecmogidascruzes.com.br/pdf/animaTerra/edicao12/artigo7.pdf

Neves, J. E. D., Pedro, P. S. M., de Freitas Gomes Hernandez, M., & Junior, L. A. F. (2023). Simulation of the implementation of domestic solar systems using multi-agent systems from web scraping. In Y. Iano, O. Saotome, G. L. Kemper Vásquez, C. Cotrim Pezzuto, R. Arthur, & G. Gomes de Oliveira (Eds.), *Proceedings of the 7th Brazilian Technology Symposium (BTSym'21)* (Vol. 207, pp. 85–97). Springer. https://doi.org/10.1007/978-3-031-04435-9_8

Resnick, N. E., & Bastos-Filho, C. J. A. (2024). Aplicação de Aprendizado de Máquinas para Detecção de URLs Phishing. *Revista de Engenharia e Pesquisa Aplicada*, 9(1), 41-49. https://doi.org/10.25286/repa.v9i1.2773

Robbins, S. P., & Coulter, M. (2020). *Administração* (14ª ed.). Pearson.

Souza, A. L. O., Bastos, C. V., Santos, P. M. S., Soares, N. M., & Neves, J. E. D. (2024). Cibersegurança na Agricultura de Precisão: Exploração à Aplicação de Medidas Preventivas. *Advances in Global Innovation & Technology*, 2, 61-73. https://doi.org/10.29327/2384439.2.2-5

Tan, Z., Beuran, R., Hasegawa, S., Jiang, W., Zhao, M., & Tan, Y. (2020). Adaptive security awareness training using linked open data datasets. *Educ Inf Technol*, 25, 5235–5259. https://doi.org/10.1007/s10639-020-10155-x

Tonezer, L. N., Silva, A. C. M., Almeida, A. H., & Neves, J. E. D. (2024). Simulações Multiagentes e Phishing: Explorando a Segurança em Ambientes de Nuvem. *Revista Tecnológica da Fatec de Americana*, 11(02). https://fatec.edu.br/revista/index.php/RTecFatecAM/article/view/393

Vilela, E., Ueda, E. T., & Gava, V. L. (2023). Phishing e engenharia social: Conceitos, modalidades, técnicas de detecção e prevenção de fraudes; uma revisão sistemática da literatura. *In Anais do 19º Congresso Internacional sobre Gestão de Sistemas de Informação e Tecnologia – CONTECSI*. FEA. https://ipt.br/2023/01/27/phishing-e-engenharia-social-conceitos-modalidades-tecnicas-de-deteccao-e-prevencao-de-fraudes-uma-revisao-sistematica-da-literatura/

Wooldridge, M. (2009). *An introduction to multiagent systems* (2nd ed.). Wiley.