Modelo de análise de efetividade de ações de conscientização cibernética com base em inteligência de ameaças

Júlio Valente C. Jr.[1], Augusto D. O. Silva[1], Luiz G. M. Florindo[1], Daniel C. Café[1]

[1]Faculdade de Tecnologia – Universidade de Brasília (UnB)
Campus Universitário Darcy Ribeiro – Brasília, DF – CEP 70910-900 – Brazil

julio.junior@aluno.unb.br, augustodamiaocybersec@gmail.com,
luiz.florindo@aluno.unb.br, dcafe@unb.br

Abstract. *Cybersecurity best practices emphasize the importance of awareness and institutional training to prevent attacks, as the human factor remains a primary vulnerability vector. Although institutions invest heavily in such actions, data regarding their effectiveness in preventing cyber events are scarce. This work describes ongoing research whose objective is to propose a model to objectively evaluate the effectiveness of cybersecurity awareness actions, through the cross-referencing of participation databases with cyber intelligence records.*

Resumo. *As melhores práticas de cibersegurança enfatizam a importância da conscientização e do treinamento institucional para prevenir ataques, já que o fator humano permanece como um dos principais vetores de vulnerabilidade. Embora haja intenso investimento institucional em tais ações, dados sobre sua efetividade na prevenção de eventos cibernéticos são escassos. Este trabalho descreve pesquisa em curso cujo objetivo é propor um modelo para avaliar objetivamente a efetividade de ações de conscientização em segurança cibernética, por meio do cruzamento de bases de dados de participação com registros de inteligência cibernética.*

1. Introdução

O **fator humano** é um vetor crítico de vulnerabilidade devido a comportamentos inseguros e engenharia social [Bada et al. 2019, Nakamura 2024]. Como resposta a esse cenário, instituições públicas e privadas têm intensificado investimentos em ações de conscientização e treinamentos em segurança cibernética, por meio de seus **programas de CSA** (*cybersecurity awareness*). Persiste, contudo, lacuna relevante quanto à capacidade das organizações de mensurar, de forma objetiva, a efetividade de tais ações. Normas e referenciais consolidados, como a ISO/IEC 27002 e as publicações do NIST, prescrevem a necessidade de monitoramento, medição e avaliação da efetividade desses controles. Contudo, na prática, grande parte das avaliações permanece restrita a métricas de alcance, como número de participantes ou taxa de conclusão de treinamentos, sem evidenciar o impacto das ações na redução real de incidentes de segurança, o que dificulta a tomada de decisão baseada em evidências e a justificativa de investimentos [Chaudhary et al. 2022, Richardson 2020].

O problema de pesquisa deste estudo consiste em medir a efetividade das ações de conscientização cibernética, hipotetizando que a correlação entre participação em tais

ações e registros de **inteligência de ameaças cibernéticas (IAC)** fornece indicadores robustos para análise de efetividade. A proposta se situa como ferramenta complementar às abordagens já tradicionais de análise de efetividade de programas de CSA, tais como métricas de alcance e simulações de engenharia social (testes de *phishing, smishing*, *vishing*, *baiting* etc.) [Alotaibi and Alfehaid 2018], com o diferencial de agregar dados de incidentes reais à análise de efetividade. Pressupõe-se que usuários expostos a ações de conscientização apresentem menor probabilidade de comprometimento de credenciais quando comparados a usuários não expostos [Nakamura 2024].

A relevância deste trabalho reside no fato de que a maior parte das organizações ainda carece de mecanismos objetivos para avaliar programas de CSA, apesar da crescente alocação de recursos nessa área [Alves et al. 2024]. Ao propor um modelo que articula dados comportamentais observáveis (participação em ações) e evidências de falhas de segurança (vazamentos de credenciais), a pesquisa busca, em complementação aos métodos tradicionais, oferecer uma abordagem orientada a impactos reais.

2. Referencial Teórico

O NIST SP 800-50r1 define consciência em cibersegurança como habilidade do usuário reconhecer e evitar comportamentos que possam comprometer a cibersegurança, bem como agir sábia e cuidadosamente para aumentar a cibersegurança [NIST 2024]. A relevância do fator humano na proteção cibernética de empresas e instituições é substantiva. Neste sentido, nota-se a ocorrência de incidentes cibernéticos facilitados pelo comportamento descuidado dos usuários, com base no desconhecimento de formas de prevenção a ataques. Por isso, recomendam-se políticas de cibersegurança que abordem a conscientização dos usuários em segurança cibernética [Alves et al. 2024].

De acordo com [Nakamura 2024], os ativos humanos, incluindo usuários, alta gestão, desenvolvedores, administradores, clientes ou parceiros, são cada vez mais utilizados como ponto inicial de ataques cibernéticos, permitindo o acesso e possibilitando as movimentações que levam a impactos relacionados à indisponibilidade, à perda de confidencialidade ou à perda de integridade.

As pesquisas sobre conscientização em cibersegurança no Brasil são escassas e há sugestão de mais estudos sobre o tema para diversas organizações públicas [Alves et al. 2024]. Nesse sentido, a análise da efetividade de programas de CSA emerge como ferramenta fundamental para avaliar e direcionar o planejamento estratégico de forma embasada. Contudo, [Chaudhary et al. 2022] apontam que não há padrões entendidos e acordados sobre programas de CSA. Similarmente, não há métricas para avaliação da efetividade de tais programas, o que dificulta sua avaliação e aumenta a probabilidade de fracasso de tais ações.

3. Metodologia

Este trabalho descreve pesquisa em curso, cujo objetivo é propor metodologia capaz de avaliar a efetividade de programas de CSA, tomando por base dados de participação nesses programas e informações de inteligência de ameaças cibernéticas (IAC).

3.1. Bases de Dados e Amostragem

A pesquisa está em curso em uma instituição da Administração Pública Federal. A amostra abrange todos os colaboradores ativos com credenciais monitoradas e a

participação em ações do programa de CSA não é obrigatória. Apesar de a participação não ser compulsória, a coleta de dados utiliza duas fontes primárias de informação: a. registros de participação no programa de CSA institucional (englobando dados completos de participação em ações do programa, com respectiva data de realização); b. registros em base de dados de IAC (dados de vazamento de credenciais de membros da instituição, obtidos por meio de monitoramento de *Dark Web*, mercados de credenciais e outras fontes de IAC, incluindo o vetor de ataque, a data de exposição/vazamento, a fonte e a quantidade de vezes que os dados de um usuário foram expostos).

Os dados são coletados com base em lastro normativo (Política de Segurança da Informação), que autoriza o monitoramento dos recursos institucionais de Tecnologia da Informação e Comunicação (TIC) utilizados pelos usuários e segue os fundamentos da Lei Geral de Proteção de Dados (LGPD) para fins de segurança institucional, com controle de acesso baseado em função, *Role-Based Access Control* (RBAC) [ABNT 2022]. Tais dados passam por etapa prévia de pseudoanonimização na coleta e cruzamento, por meio de *hashing* (SHA-512). Adicionalmente, os dados por unidade funcional com menos de 5 colaboradores são agregados em categoria "outros" para impedir identificação por dedução. Os pesquisadores envolvidos na pesquisa assinaram Termo de Confidencialidade e Sigilo, que assevera que os resultados devem ser apresentados apenas de forma global e impessoal, estruturados com a finalidade exclusiva de melhoria da efetividade e resiliência institucionais, sem fins disciplinares.

3.2. Análise de Dados e Etapas da Avaliação

A metodologia proposta compreende sequência de etapas exercitadas sobre os dados de entrada, pré-processados, conforme a Figura 1 a seguir. A análise temporal toma por base os **ciclos do programa de CSA**, que são replanejados e executados, com base no orçamento definido no final do ciclo anterior. Tais ciclos podem ser semestrais, anuais, ou obedecer a alguma outra frequência de ocorrência. Dessa forma, a análise temporal correlaciona as ações e incidentes do ciclo sob análise, seu predecessor e sucessor, conforme o caso. A análise de incidentes calcula a taxa de vazamento de credenciais entre grupos expostos e não expostos a ações de conscientização. A análise de reincidência, de caráter complementar, monitora padrões de recorrência de vazamento em ambos os grupos e verifica a adesão a treinamentos subsequentes (i.e., se, depois de serem atacados, usuários não capacitados passaram a participar de ações de conscientização). Por fim, a análise estratégica e organizacional permite aplicar os mesmos indicadores sobre unidades distintas, com o objetivo de avaliar se as unidades funcionais com menor aderência ao CSA têm maior probabilidade de incidência de vazamento de dados de seus colaboradores e se há discrepâncias entre as unidades funcionais capacitadas.

3.3. Indicadores de Efetividade

A aplicação da metodologia proposta resulta em indicadores, listados na Tabela 1, que possibilitam a mensuração do impacto das ações na redução de vulnerabilidades e incidentes cibernéticos.

Figura 1 – Visão diagramática da metodologia proposta

Tabela 1 – Indicadores propostos

Indicador	Descrição	Fórmula	Elementos da Fórmula
1. Incidência de vazamentos após capacitação recente	Percentual de falha de proteção em usuários que teoricamente já possuíam o conhecimento preventivo adquirido no ciclo anterior (C_{x-1}).	$IVACr(C_x) = \left(\frac{\lvert PV(C_x) \cap PC(C_{x-1})\rvert}{TPC(C_{x-1})}\right) x\ 100$	$IVACr(C_x)$: indicador de incidência de vazamentos no ciclo C_x após capacitação recente. $PV(C_x)$: conjunto de usuários com registros de incidentes no ciclo em análise (C_x). $PC(C_{x-1})$: conjunto de usuários que concluíram a capacitação no ciclo anterior (C_{x-1}). $TPC(C_{x-1})$: total de pessoas capacitadas no ciclo anterior (C_{x-1}).
2. Incidência de vazamentos após capacitação antiga (não recentes)	Taxa de incidência de falha de proteção em usuários que teoricamente já possuíam o conhecimento preventivo adquirido há mais de um ciclo de capacitação.	$IVACa(C_x) = \left(\frac{\lvert PV(C_x) \cap (\cup_{i=1}^{n} PC(C_i)) \setminus PC(C_{x-1})\rvert}{\lvert \cup_{i=1}^{n} PC(C_i) \setminus PC(C_{x-1})\rvert}\right) \times 100$	$IVACa(C_x)$: indicador de incidência de vazamentos no ciclo C_x após capacitação antiga. $PV(C_x)$: conjunto de pessoas com vazamentos no ciclo C_x. $\cup_{i=1}^{n} PC(C_i)$: A união de todos os capacitados dos ciclos primórdios até n ciclos atrás. $PC(C_{\{x-1\}})$: Conjunto de usuários capacitados no ciclo C_{x-1}.
3. Incidência de vazamentos pré-capacitação	Taxa de incidentes no grupo de usuários que ainda não foi exposto às ações de conscientização até o início do ciclo atual (C_x).	$IVAPC(C_x) = \left(\frac{\lvert PV(C_x) \setminus \cup_{i \in \{x-1,x-2,\ldots,1\}} PC(C_i)\rvert}{TP - \lvert \cup_{i \in \{x-1,x-2,\ldots,1\}} PC(C_i)\rvert}\right) x\ 100$	$IVAPC(C_x)$: indicador de incidência de vazamentos pré-capacitação no ciclo C_x. $PV(C_x)$: conjunto de pessoas com vazamentos no ciclo C_x. $\cup_{i \in \{x-1,x-2,\ldots,1\}} PC(C_i)$: conjunto de pessoas capacitadas em todos os ciclos anteriores. TP: total de pessoas da instituição.

Com base nos indicadores da Tabela 1, a **efetividade do programa** de CSA conduzido em um ciclo C_x é medida pela sua capacidade de reduzir a incidência de vazamentos no ciclo subsequente (C_{x+1}), comparando o grupo recém-capacitado com o grupo de controle (usuários ainda não expostos ao programa). Assim, a efetividade é sempre calculada em ciclo já passado, pois depende de informações do ciclo seguinte. Por sua vez, a **resiliência do programa** mede a retenção do conhecimento e a manutenção do comportamento

seguro por usuários que foram capacitados em ciclos remotos, ou seja, ciclos anteriores ao ciclo passado. Ambas as fórmulas são detalhadas na Tabela 2.

Tabela 2 – Cálculo de Efetividade e Resiliência

Indicador	Fórmula	Elementos da Fórmula	Interpretação
1. Efetividade do programa CSA no ciclo C_x	$Efetividade\ CSA(C_x) = \left(1 - \frac{IVACr(C_{x+1})}{IVAPC(C_{x+1})}\right) x\ 100$	$IVACr(C_{x+1})$: representa o percentual de usuários treinados em C_x que sofreram vazamentos no ciclo posterior (C_{x+1}). Mede a falha de proteção de quem acabou de ser capacitado. $IVAPC(C_{x+1})$: representa a taxa de incidentes no grupo de usuários que ainda não foi exposto a nenhuma ação de conscientização até o início de C_{x+1}. Funciona como grupo de controle.	- 100%: Ninguém do grupo capacitado sofreu vazamentos. - 0%: A taxa de vazamentos entre os capacitados é idêntica à taxa dos não capacitados. - Valor negativo: Indica que o grupo capacitado teve mais vazamentos que o grupo de controle (sugerindo que a capacitação foi ineficaz ou o grupo treinado é um alvo mais visado/específico).
2. Resiliência do programa CSA no ciclo C_x	$Resiliência\ CSA(C_x) = \left(1 - \frac{IVACa(C_x)}{IVAPC(C_x)}\right) x\ 100$	$IVACa(C_x)$: representa o percentual de falha em usuários que receberam treinamento no intervalo entre o primeiro ciclo C_1 e o ciclo retrasado C_{x-2}. $IVAPC(C_x)$: representa a taxa de incidentes no grupo de usuários que ainda não foi exposto a nenhuma ação de conscientização.	- Efetividade > Resiliência: Pode indicar que o treinamento tem forte impacto inicial, mas o efeito se perde com o tempo. - Resiliência ≈ Efetividade: Pode indicar que o conteúdo é bem retido e gera mudança cultural duradoura. - Resiliência ≈ 0: Pode indicar que, após algum tempo, o usuário capacitado volta a ter o mesmo perfil de risco de um usuário que nunca foi treinado. Isso pode acontecer também porque o panorama de ameaças mudou e o usuário não se atualizou.

4. Considerações Finais

O presente estudo discorre sobre pesquisa em curso, cujo objetivo é propor um modelo de análise da efetividade de programas de CSA, usando dados de participação e registros de IAC, com o objetivo de complementar as estratégias tradicionais (métricas de alcance e testes de engenharia social), com informações reais sobre incidentes. A aplicação em uma instituição da Administração Pública Federal está em curso, com o objetivo de avaliar se as novas métricas melhoram a compreensão, por parte dos gestores, do resultado dos ciclos de programas de CSA, em termos de efetividade e resiliência.

Apesar de sua relevância e adequação para inferir padrões e medir a efetividade das ações de conscientização, a pesquisa apresenta limitações em seu estado atual que indicam caminhos futuros, tais como: a ausência de informações sobre o conhecimento prévio dos usuários antes das campanhas; a não inclusão de fatores motivacionais ou comportamentais subjetivos; a dependência da completude, temporalidade e precisão das bases de IAC utilizadas. Assim, o andamento da pesquisa deve abarcar a análise estatística de significância dos resultados obtidos, bem como a integração de fatores subjetivos, tais como pesquisas de satisfação ou testes de conhecimento prévio, de forma a correlacionar o conhecimento base e fatores motivacionais com os indicadores de efetividade propostos. Adicionalmente, pode-se aplicar a metodologia em um escopo mais amplo de incidentes (além de vazamentos de credenciais), bem como utilizar os indicadores gerados para refinar o conteúdo das campanhas, estabelecendo um ciclo de melhoria contínua focado nos vetores de ataque mais prevalentes em cada unidade funcional.

Referências

Alotaibi, M., & Alfehaid, W. (2018). Information security awareness: A review of methods, challenges and solutions. Proceedings of the ICITST-WorldCIS-WCST-WCICSS-2018, Cambridge, UK, 10, 13.

Alves, D. A.; Melo Alves, C. A. ; Mendes, F. F.; Nunes, R. R. (2024). Conscientização em Segurança Cibernética: Estudo Baseado na Percepção de Trabalhadores de uma Organização Pública Federal Brasileira. RISTI – Revista Ibérica de Sistemas e Tecnologias de Informação, n. E65, p. 661-673, jan.2024.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27002: Segurança da informação, segurança cibernética e proteção à privacidade – Controles de segurança da informação. Rio de Janeiro, 2022.

Bada, M.; Sasse, A. M.; Nurse, J. R. C. (2019). Cyber Security Awareness Campaigns: Why do they fail to change behaviour? Cryptography and Security (cs.CR); Computers and Society (cs.CY); Human-Computer Interaction. https://doi.org/10.48550/arXiv.1901.02672.

Chaudhary, S.; Gkioulos, V.; Katsikas, S. (2022). Developing metrics to assess the effectiveness of cybersecurity awareness program, Journal of Cybersecurity, Volume 8, Issue 1, 2022, tyac006, https://doi.org/10.1093/cybsec/tyac006.

Nakamura, E. T. (2024). O Papel da Segurança Cibernética no Universo Digital: a importância do fator humano. In: KUBOTA, Luis Claudio (Org.). Digitalização e tecnologias da informação e comunicação: oportunidades e desafios para o Brasil. Rio de Janeiro: Ipea, 2024. p. 295-340, il. DOI: http://dx.doi.org/10.38116/9786556350660cap9.

Richardson R. (2020). CSI computer crime & security survey. Disponível em: <http://www.sis.pitt.edu/jjoshi/courses/IS2150/Fall11/CSIsurvey2008.pdf>. Acesso em: 15 nov. 2025.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (1998). Information Technology Security Training Requirements: a Role- and Performance-Based Model: NIST Special Publication 800-16. Gaithersburg, MD: U.S. Department of Commerce, 1998. Disponível em: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-16.pdf>. Acesso em: 15 nov. 2025.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (2020). Security and Privacy Controls for Information Systems and Organizations: NIST Special Publication 800-53, Revision 5. Gaithersburg, MD: U.S. Department of Commerce, 2020. Disponível em: < https://doi.org/10.6028/NIST.SP.800-53r5>. Acesso em: 15 nov. 2025.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (2024). Building a Cybersecurity and Privacy Learning Program: NIST Special Publication 800-50 Revision 1. Gaithersburg, MD: U.S. Department of Commerce, 2024. Disponível em: <https://doi.org/10.6028/NIST.SP.800-50r1>. Acesso em: 15 nov. 2025.