JOÃO AUGUSTO ALEXANDRIA DE BARROS

SEGURANÇA CIBERNÉTICA NAS ESCOLAS E UNIVERSIDADES BRASILEIRAS:

avaliando a inserção da educação cibernética no sistema educacional brasileiro e seus efeitos na prevenção de incidentes cibernéticos

Ensaio Acadêmico apresentado ao Departamento de Estudos da Escola Superior de Guerra como requisito à obtenção do certificado do Curso Superior de Segurança e Defesa Cibernética.

RIO DE JANEIRO, RJ
2023

CSSDC2023 ESG

_____

JOÃO AUGUSTO ALEXANDRIA DE BARROS

AGRADECIMENTOS

Agradeço a Deus por sempre guiar meus passos e dedico este ensaio acadêmico com gratidão a todas as pessoas que têm sido a minha fonte de inspiração e apoio incondicional ao longo de minha vida.

Ao meu falecido pai, cujo amor, sabedoria e exemplo de perseverança continuam a me nortear, mesmo em sua ausência. Saiba que suas lições são eternas.

À minha mãe, que sempre acreditou em mim e me encorajou a seguir minha vocação. Seu carinho e apoio moldaram o que sou hoje.

À minha amada esposa, cujo amor, compreensão e paciência me fortalecem a cada desafio. Você é meu porto seguro.

À minha filha e ao meu filho, que trouxeram uma nova luz à minha vida e me inspiram a ser o melhor que posso ser. Que este trabalho seja um tributo ao futuro que continuaremos a construir juntos.

A todos vocês, minha família, dedico este ensaio com carinho e gratidão. Vocês são minha força motriz e meu maior tesouro. Obrigado por fazerem parte da minha vida.

Gostaria de expressar minha profunda gratidão por ter tido a oportunidade de ser estagiário e concluir o Curso Superior de Segurança e Defesa Cibernética na Escola Superior de Guerra. Esta jornada acadêmica e profissional foi enriquecedora em muitos aspectos, e não teria sido possível sem o apoio e a dedicação de vários atores.

Primeiramente, gostaria de agradecer ao Diretor do Curso, pelo comprometimento em fornecer um ambiente de aprendizado estimulante e atualizado. Sua liderança e orientação foram fundamentais para nosso sucesso acadêmico.

Quero estender meu agradecimento sincero aos professores e conferencistas que compartilharam seu conhecimento e experiência conosco ao longo do curso. Suas palestras inspiradoras foram inestimáveis na construção de nosso entendimento em segurança da informação e cibernética.

Além disso, sou grato à instituição, a Escola Superior de Guerra, por abrir as portas para esta oportunidade única. A dedicação de seus integrantes à excelência acadêmica e à formação de líderes na área de segurança cibernética é admirável.

Por fim, quero agradecer a todos os colegas de curso, cuja colaboração e camaradagem tornaram esta jornada ainda mais significativa.

Esta conquista não é apenas minha, mas também de todas as pessoas e instituições que acreditaram em meu potencial e me apoiaram ao longo do caminho. Estou ansioso para aplicar o conhecimento e as habilidades adquiridas neste curso para contribuir de forma positiva no campo da segurança cibernética e defesa.

Muito obrigado a todos por fazerem parte desta jornada.

RESUMO

Este ensaio acadêmico apresenta a análise de referenciais teóricos sobre conscientização e capacitação de segurança da informação e cibernética e sua implementação objetivando melhora na maturidade da sociedade que utilizam dispositivos em rede. O problema de pesquisa centraliza-se na investigação dos possíveis efeitos na taxa de incidentes cibernéticos maliciosos caso seja implementado um programa disciplinar de segurança da informação e cibernética nas instituições de ensino, em todos os níveis, do Brasil. Os tópicos discutidos ao longo do ensaio incluem a motivação por trás desse tema, a importância da conscientização e treinamento em segurança cibernética, a análise de programas de conscientização e treinamento, estratégias institucionais em segurança cibernética no ensino superior e o impacto da educação cibernética na redução da taxa de incidentes cibernéticos.

Palavras-chave: segurança cibernética; segurança da informação; ensino; educação – Brasil.

ABSTRACT

This academic paper presents an analysis of theoretical frameworks regarding awareness and training in information security and cybersecurity, aiming to enhance the maturity of society that utilizes networked devices. The central research problem focuses on investigating the potential effects on the rate of malicious cyber incidents if a mandatory information security and cybersecurity disciplinary program were to be implemented in educational institutions across Brazil. The topics discussed throughout the essay encompass the motivation behind this theme, the significance of awareness and training in cybersecurity, an evaluation of awareness and training programs, strategies in cybersecurity within higher education, and the impact of cyber education on reducing the rate of incidents.

Keywords: cybersecurity; information security; teaching; education – Brazil.

SUMÁRIO

1 INTRODUÇÃO

A segurança da informação e a segurança cibernética emergiram com questões importantes em um mundo cada vez mais interconectado. O advento da tecnologia em rede transformou profundamente a sociedade, moldando a forma como vivemos, trabalhamos e nos comunicamos. Nesse contexto, a educação desempenha um papel fundamental na preparação dos indivíduos para enfrentar os desafios e ameaças cibernéticas que permeiam nossa vida “virtual” cotidiana.

O tema central deste ensaio é a proposição de inclusão, no sistema educacional brasileiro, a temática de segurança da informação e segurança cibernética, bem como suas consequências e impactos. O trabalho foca na avaliação das possíveis implicações de uma intervenção específica no sistema educacional: a inclusão de um programa disciplinar de segurança cibernética. No cerne desta análise encontra-se: identificar e avaliar os prováveis impactos na taxa de incidentes cibernéticos que alcançam seus objetivos maliciosos, caso ocorra a inclusão do anteriormente citado programa. Esta questão de caráter multidisciplinar, requer uma abordagem adequada para compreender o potencial de evolução da educação em segurança da informação e segurança cibernética.

O objetivo deste ensaio é analisar trabalhos que tratem o estado atual da conscientização e capacitação em segurança cibernética e da informação, bem como explorar as consequências e impactos que podem surgir da implementação de um programa de segurança cibernética no ensino básico e superior. Ao fazê-lo, pretendemos sensibilizar formuladores de políticas públicas, educadores, profissionais de segurança e todos os interessados na construção de uma sociedade mais resiliente e ciente dos desafios cibernéticos.

A estrutura deste ensaio segue uma lógica coerente, com seções dedicadas à revisão da literatura existente, análise de dados, discussão de resultados e conclusões.

2 REFERENCIAL TEÓRICO

O referencial teórico deste ensaio acadêmico busca embasar a pesquisa sobre a implementação da segurança cibernética no sistema educacional e as prováveis consequências.

2.1. Conscientização e treinamento em segurança da informação e cibernética

O estudo de Jean-Pierre (2021) sobre conscientização e conhecimento em segurança cibernética da sociedade da Dominica destaca a importância da conscientização dos usuários como um elemento fundamental como ação de proteção contra ameaças cibernéticas. O autor ressalta que, mesmo familiarizados com um ambiente digital, muitos indivíduos ainda carecem de conhecimento sobre ameaças e práticas seguras online. O treinamento em segurança cibernética, conforme demonstrado no estudo, pode desempenhar um papel vital na capacitação das pessoas para proteger suas informações pessoais e ativos de rede.

Infere-se que a educação em segurança da informação e segurança cibernética desempenha papel relevante na preparação dos indivíduos para os desafios da segurança. A implementação não apenas informa sobre ameaças cibernéticas, mas também promove habilidades para identificar, prevenir, tratar e responder a incidentes de segurança. A educação cibernética capacita as pessoas a protegerem seus dados pessoais, evitarem ataques cibernéticos e contribuírem para um ambiente digital seguro.

De acordo com Sharmila R. (2023), o emprego de técnicas comuns e bem conhecidas, além de usar as redes de acordo com o código de ética cibernético, é aspecto construtor para uma postura segura por parte dos usuários.

Um aspecto que identifica o nível de maturidade em segurança da informação e segurança cibernética de grupos sociais é a sua consciência sobre os riscos. No caso de países de baixa maturidade, a insciência coletiva permite que adversários alcancem êxito em suas ações maliciosas, em particular utilizando, como vetor de ataque, a engenharia social. Disciplinas escolares de segurança cibernética, pautadas em códigos de ética e técnicas de segurança simples, seriam implementadas com baixa complexidade, particularmente no ensino fundamental, visto que, essas pautas, não demandam meios auxiliares significativos para seu ensino.

Conclui-se parcialmente que o nível de conscientização e capacitação de um determinado grupo é aspecto relevante para identificar a maturidade em segurança

cibernética. Além disso, autores identificam a conscientização e conhecimento em segurança da informação e segurança cibernética com uma boa prática que permite a implementação de uma cultura de segurança.

2.2. Programas de Conscientização e Treinamento em Segurança da informação e cibernética

O artigo de Hash e Wilson (2012) fornece diretrizes para o desenvolvimento de programas de conscientização e treinamento em segurança da informação e segurança cibernética. A abordagem proposta abrange desde a identificação de públicos-alvo até a avaliação contínua da eficácia do programa. Os autores destacam que a colaboração e a coordenação são fundamentais para o sucesso desses programas e enfatizam a importância de uma abordagem contínua e adaptável para enfrentar as ameaças cibernéticas em evolução constante.

O estudo de Mashiane, Dlamini e Mahlangu (2019) apresenta uma estratégia de implementação para campanhas de conscientização em segurança cibernética. Os autores destacam a necessidade de personalização das mensagens e abordagem de conscientização de acordo com os grupos-alvo. Além disso, enfatizam a importância da medição de sucesso por meio de métricas relevantes e da coordenação eficaz para promover uma cultura de segurança cibernética.

As ações visando a construção de uma evolução na maturidade cibernética coletiva é um ato contínuo. Apesar de resultados relativamente céleres quando da aplicação imersiva de treinamentos e capacitações, cabe ao promotor de políticas de conscientização e capacitação cibernética, selecionar o nível de entendimento de cada grupo, seja por uma classificação etária ou por nível de escolaridade, aplicando ações específicas e adequadas, baseadas em aspectos como maturidade, frequência de uso e curva de tendência de evolução no uso.

Paul Dolan *et al.* (2012) aborda questões relevantes para a segurança cibernética, principalmente no que diz respeito à compreensão do comportamento humano e à forma como as intervenções podem ser planejadas. Os pontos-chave destacados são a compreensão do comportamento humano, fatores motivacionais, arquitetura de escolha, comunicação clara e persuasiva, acompanhamento, normas sociais e personalização. O trabalho destaca questões psicológicas e comportamentais que têm aplicação prática na segurança cibernética, mostrando

como projetar programas e estratégias que influenciem positivamente o comportamento das pessoas em relação à segurança.

Infere-se parcialmente que estudos científicos indicam modos de implementar efetivamente ações de conscientização e capacitação. Esses mesmo trabalhos caracterizam a educação cibernética dos usuários, de todos os níveis e perfis, como essencial para a criação de uma cultura de segurança e redução das falhas humanas que permitem incidentes exitosos.

2.3. Estratégias Institucionais em Segurança Cibernética no Ensino

O artigo de Cheng e Wang (2022) explora estratégias institucionais para fortalecer a segurança cibernética em instituições de ensino superior. Os autores reconhecem os desafios específicos enfrentados por essas instituições, como a diversidade de usuários e de dispositivos conectados à rede. Eles destacam a importância de políticas claras, educação e treinamento em segurança da informação e cibernética, bem como a colaboração entre instituições e a indústria de segurança cibernética.

O estudo de Zwillling *et al.* (2022) realiza uma análise comparativa da conscientização, conhecimento e comportamento em segurança cibernética em diferentes grupos de participantes. Os resultados revelam diferenças significativas entre os grupos, enfatizando a necessidade de abordagens personalizadas para treinamento e conscientização em segurança cibernética.

Os trabalhos supracitados, com teorias e estudos, alicerçam a compreensão para desenvolver os processos de criação de capacidades em segurança cibernética, esclarecer a importância dos programas de treinamento, instituir medidas de conscientização, e tratar as especificidades da segurança cibernética no contexto do ensino. A análise desses conceitos e descobertas é aspecto relevante na avaliação de maturidade do sistema educacional brasileiro em segurança cibernética e proposição de iniciativas.

Apesar de sua declarada importância, a implementação da educação cibernética enfrenta desafios significativos. Um dos principais é a baixa maturidade e ausência de iniciativas de conscientização vocacionada aos responsáveis pela autorização das ações, alta gestão, além de parcos recursos dedicados. As instituições de ensino ainda não incorporaram a educação cibernética em seus currículos, deixando lacunas na preparação dos alunos de todos os níveis. Além disso,

a rápida evolução das tecnologias requer que os futuros programas de educação cibernética tenham a previsão de constante revisão e atualização.

As instituições de ensino e os governos deverão ser os principais protagonistas na promoção da educação cibernética. A educação básica e universitária deve integrar currículos de segurança cibernética desde os primeiros anos escolares, o que viria a subsidiar a transmissão de conhecimentos aos alunos. Além disso, os governos podem desenvolver políticas públicas e normatizações que incentivem a educação cibernética e apoie programas de treinamento e conscientização vocacionados aos corpos discentes das diversas instituições de ensino.

Conclui-se parcialmente que as ações de conscientização e capacitação são as componentes principais do escopo de um programa de educação cibernética para o sistema educacional. Essas terão maior impacto ou melhor aceitação dependente do grupo receptor daquele ensinamento, além da necessidade de uma personalização de acordo com as características culturais e nível de educação destes usuários.

2.4. Educação cibernética e seu Impacto na taxa de incidentes cibernéticos

O documento da Organização dos Estados Americanos (OEA), intitulado "Educação em Segurança: Planejamento do Futuro por Meio do Desenvolvimento da Força de Trabalho" aborda a importância da educação em segurança cibernética como parte do desenvolvimento da força de trabalho. O documento enfatiza a necessidade de preparar a força de trabalho com competências e conhecimentos em segurança cibernética, visando ao enfrentamento das ameaças cibernéticas. Sob esta ótica, defende-se a tese de que a educação em segurança cibernética exerce um papel pivotal na salvaguarda de organizações e indivíduos contra ataques cibernéticos, além de salientar a importância de elaborar currículos e programas educacionais que incorporem a segurança cibernética em todos os níveis de ensino, desde o ensino básico até o ensino superior, bem como no contexto do treinamento profissional. É relevante destacar que esta publicação da OEA, datada de 2020, ratifica a percepção de prevenção já identificada pelo Gabinete de Segurança Institucional da Presidência da República (GSI/PR).

Durante os anos de 2018 e 2019, o Grupo de Consulta de Segurança Cibernética do Centro Global de Capacidade de Segurança Cibernética (GCSCC) realizou atividades de coleta de informações em Brasília, envolvendo diversas partes interessadas, como representantes do setor público, privado e acadêmico, operadores de infraestrutura crítica, forças de segurança e outros atores relevantes. O objetivo dessas consultas foi avaliar a capacidade de segurança cibernética do país com base em cinco dimensões-chave: política e estratégia de segurança cibernética, cultura cibernética e sociedade, educação e treinamento em segurança cibernética, estruturas legais e regulatórias, e normas, organizações e tecnologias. A metodologia utilizada envolveu a aplicação do Modelo de Maturidade em Segurança Cibernética (CMM), proporcionando uma análise abrangente do cenário de segurança cibernética no Brasil e servindo como base para o desenvolvimento de relatórios de análise.

As consultas, que reuniram um amplo espectro de entidades, refletiram o compromisso brasileiro em avaliar e melhorar sua postura de segurança cibernética. Através do CMM e das cinco dimensões de avaliação, foi possível identificar áreas de força e fraqueza, bem como direcionar esforços para fortalecer a capacidade de segurança cibernética do país. O processo envolveu participantes de diversos setores, indicando uma abordagem multidisciplinar para abordar os desafios cibernéticos. Essa avaliação foi essencial para permitir que o Brasil esteja alinhado com as melhores práticas para ser capaz de enfrentar as ameaças cibernéticas em constante evolução. O relatório final foi emitido em 2020, indicando a dimensão de Cultura cibernética e sociedade como um dos aspectos que demandavam atenção especial por parte do governo brasileiro.

O Boletim Informativo mensal (BIM) do Gabinete de Segurança Institucional (GSI), cuja primeira edição foi emitida em janeiro de 2020, desempenhou um papel disruptivo na promoção da prevenção e na conscientização sobre questões relacionadas à segurança da informação e segurança cibernética no âmbito da Administração Pública Federal. Através de uma abordagem informativa e educacional, o boletim tem destacado as ameaças cibernéticas em constante evolução, informando os leitores sobre os riscos potenciais e as melhores práticas para se proteger contra essas ameaças. Além disso, o boletim fornece informações atualizadas sobre as medidas de segurança e boas práticas a serem seguidas, incentivando ativamente a prevenção e a adoção de medidas proativas.

Atualmente, o GSI/PR propõe, além do BIM, outras iniciativas de prevenção e conscientização, como as Orientações de Segurança da Informação e Cibernética (OSIC) e os Fascículos de segurança da informação e cibernética, instrumentos construtores em diversos níveis da conscientização e capacitação cibernética. Além de alertas e recomendações, voltados para os quadros técnicos, emitidos pelo CTIR Gov.

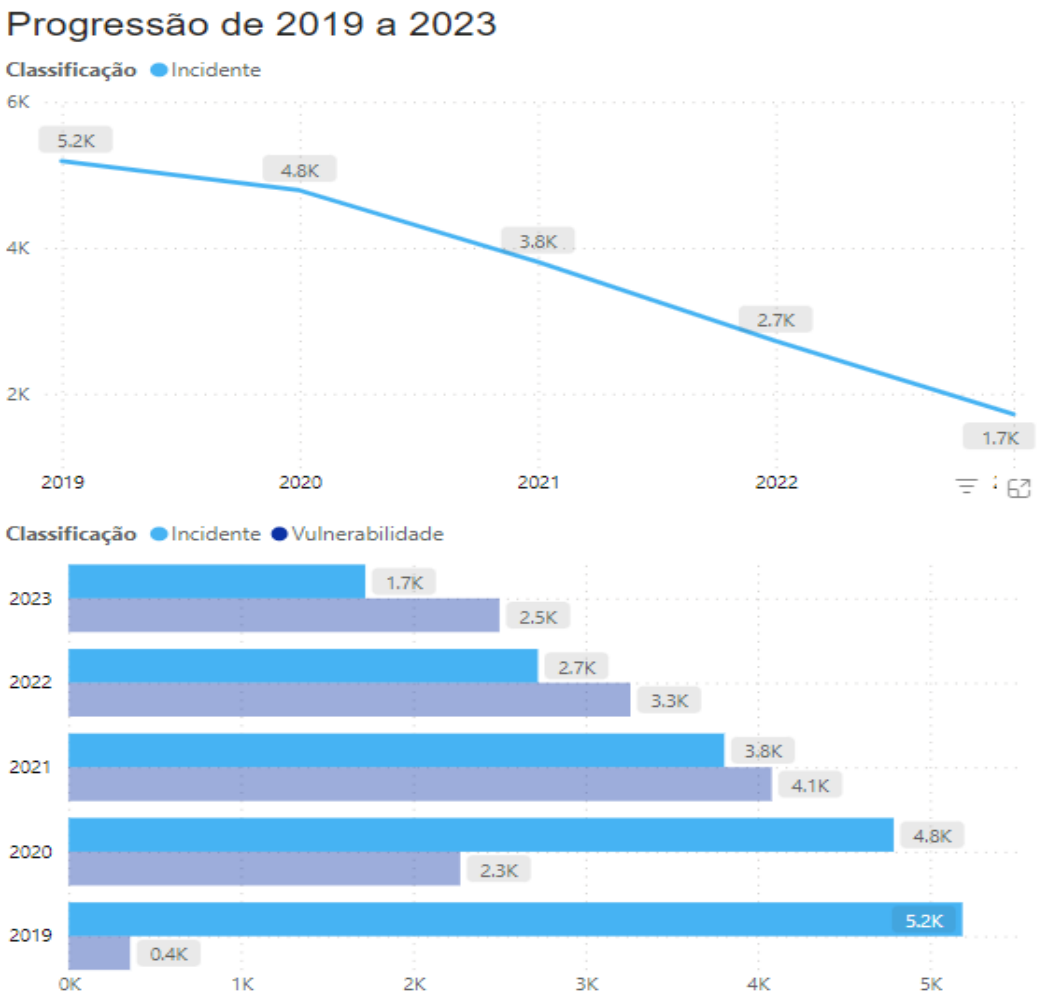
Ao compartilhar trabalhos, casos de estudo, boas práticas e exemplos de incidentes cibernéticos, o GSI/PR sensibilizou os usuários de seus produtos técnicos para os riscos e iniciou ações de promoção de uma cultura de segurança cibernética no âmbito do Governo Federal, contribuindo, assim, para a prevenção de incidentes.

As diversas iniciativas anteriormente apresentadas têm caráter educativo em diversos níveis. Considerando o universo da Administração Pública Federal Direta, Autárquica e Fundacional como receptores dos conhecimentos difundidos pelo GSI/PR, os usuários desse grupo específico seriam discentes dispostos a assimilar os conhecimentos repassados sobre segurança da informação e segurança cibernética pelo GSI/PR.

A evolução dos incidentes cibernéticos notificados ao Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov), entre 2019 e o corrente ano, está representada na *Figura 1*. Observa-se que os casos de incidentes decresceram no período em análise, cabe a ressalva de que em 2023 transcorreram apenas nove meses.

Conforme tratado anteriormente, fatos marcantes e iniciativas que estimularam a prevenção, por intermédio de capacitação e conscientização, são coincidentes com o período explicitado. Cabe a ressalva, que não há as estatísticas quanto ao investimento tecnológico, particularmente em ativos de segurança da informação e cibernética, todavia a especificação e utilização destes ativos também estão correlacionados com um melhor entendimento das equipes dos órgãos sobre a importância de preparação tecnológica de segurança e emprego de boas práticas, o que indica um incremento da educação cibernética e início da implementação de uma cultura de segurança.

Figura 1 - Gráfico – Progressão de 2019 a 2023



Fonte: Brasil, 2023.

A Tabela 1 apresenta duas ameaças comuns no ambiente virtual brasileiro: o Phishing e o Abuso de sítio Web. Com base nos dados do CTIR Gov, observa-se a tendência de redução dessas atividades maliciosas no período de 2019 a 2023, o que coincide com as ações educativas descritas anteriormente neste ensaio acadêmico. Isso sugere que existe uma correlação entre as medidas educativas e as variações nas taxas de ocorrência de incidentes. Cabe destacar, um aumento nas ações de phishing em 2023 em relação a 2022, apesar de inferior aos anos anteriores, pode vir a indicar uma mudança de tendência. Este ponto não invalida a análise, no entanto pode indicar a necessidade de atualização no programa proposto.

A seleção das duas ameaças, propostas na Tabela 1, permitem uma visão efetiva do impacto no usuário. O phishing e o abuso web são ações maliciosas dependentes de baixa maturidade do usuário para lograr êxito. Além disso, o uso do

e-mail ou exposição de dados em ambientes web são práticas comuns em uma grande gama de posições de trabalho e da vida pessoal dos integrantes da sociedade.

Tabela 1 - Quantidade de incidentes cibernéticos de phishing e abuso de sítio web entre 2019 e 2023 no âmbito da Administração Pública Federal direta, autárquica e fundacional.

Ameaça	2019	2020	2021	2022	2023
Phishing	226	807	285	134	180
Abuso de Sítio Web	4402	2525	1977	1272	958

Fonte: Brasil, 2023.

3 CONSIDERAÇÕES FINAIS

A educação em segurança da informação e da segurança cibernética é essencial devido a alta demanda no uso de equipamentos conectados. Ações que implementem a educação em segurança no uso dos meios digitais objetivando uma cultura de segurança apresenta fortes indícios que resultará no fortalecimento da resiliência de nossas infraestruturas e serviços digitais.

Entre os diversos aspectos que podem ser utilizados para verificar a maturidade em segurança cibernética está a conscientização e capacitação. Trabalhos acadêmicos apontam para propostas e estratégias de implementação efetiva de iniciativas de conscientização e capacitação. Esses mesmo trabalhos caracterizam a educação cibernética dos usuários, de todos os níveis e perfis, como essencial para a criação de uma cultura de segurança.

A partir dos referenciais teóricos verifica-se que as ações de conscientização e capacitação são as componentes principais do escopo de um programa de educação cibernética para o sistema educacional. Consequentemente, permite-se considerar que os impactos dessas ações serão coerentes com a aplicação de um programa de educação cibernética.

Os servidores públicos federais, integrantes da Administração Pública Federal Direta, Autárquica e Fundacional, estão presentes em todas as regiões do Brasil e apresentam os diversos níveis de escolaridade. Consequentemente, representam um espaço amostral viável para análise da sociedade brasileira.

A redução da taxa de êxito em incidentes cibernéticos na Administração Pública Federal Direta, Autárquica e Fundacional, consequentemente notificados ao CTIR Gov, indica na efetividade da conscientização e capacitação proposta pelo

GSI/PR, que pode ser entendido como a implementação efetiva da educação cibernética no ambiente de governo, extrapolando-se o entendimento pode-se inferir que a introdução de disciplinas específicas de segurança da informação e segurança cibernética favoreceriam a redução de incidentes e, além disso, promoveria a construção de uma cultura cibernética nacional.

Superar os desafios na consolidação da cultura de segurança no país, baseada na implementação da educação cibernética, requer esforço estatal e comprometimento coletivo de instituições de ensino, governos e demais setores. Promover a educação cibernética é investir, no médio e longo prazo, em um ambiente digital mais seguro e resiliente para toda sociedade brasileira.

Do exposto, o presente ensaio contribui cientificamente ao entendimento de que a inserção da disciplina de segurança da informação e segurança cibernética na base curricular do ensino básico permitirá a implementação de uma cultura de segurança com impactos positivos na redução dos incidentes cibernéticos com êxito.

REFERÊNCIAS

ANDRONACHE, Alina. Increasing security awareness through lenses of cybersecurity culture. **Journal of Information Systems & Operations Management**, v. 15, n. 1, 2021.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. **Estatísticas resultantes do trabalho de detecção, triagem, análise e resposta a incidentes cibernéticos**. Brasília, DF: GSI, 2023. Disponível em: https://www.gov.br/ctir/pt-br/assuntos/ctir-gov-em-numeros. Acesso em: 18 nov. 2023.

CHENG, Eric CK; WANG, Tianchong. Institutional strategies for cybersecurity in higher education institutions. **Information**, v. 13, n. 4, p. 192, 2022.

DOLAN, Paul *et al*. Influencing behaviour: the mindspace way. **Journal of economic psychology**, v. 33, n. 1, p. 264-277, 2012.

GRUPO DE CONSULTA DE SEGURANÇA CIBERNÉTICA DO CENTRO. **Revisão da Capacidade de Segurança Cibernética da República Federativa do Brasil**. [*S. l.*]: GCSCC, 2020.

HASH, J.; WILSON, M. **Building an information technology security awareness and training program**. Gaithersburg, MD: National Institute of

Standards and Technology, 2012. Disponível em: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf. Acesso em: 23 out. 2023.

JEAN-PIERRE, Jermaine Jewel. **User awareness and knowledge of cybersecurity and the impact of training in the commonwealth of Dominica**. 2021. Tese (Doutorado em Filosofia e Administração) - Walden University, [Minneapolis], 2021.

MASHIANE, Thulani; DLAMINI, Zama; MAHLANGU, Thabo. A rollout strategy for cybersecurity awareness campaigns. In: INTERNATIONAL CONFERENCE ON CYBER WARFARE AND SECURITY, 14, 2019, Stellenbosch, South Africa. **Proceedings** [...]. Stellenbosch: ICCWS, 2019.

ORGANIZAÇÃO DOS ESTADOS AMERICANOS. **Educação em segurança cibernética**: planejamento do futuro por meio do desenvolvimento da força de trabalho. OEA, 2020. Publicação n. 5.

SHARMILA, R.; SABITHA, J. Overview of cyber security and its safety measures. **Humanities And Social Science Studies**, v. 12, n. 20, 2023.

ZWILLING, Moti *et al*. Cyber security awareness, knowledge and behavior: a comparative study. **Journal of Computer Information Systems**, v. 62, n. 1, p. 82-97, 2022.