XII SINGEP
Simpósio Internacional de Gestão, Projetos, Inovação e Sustentabilidade
International Symposium on Management, Project, Innovation and Sustainability
ISSN: 2317-8302
CYRUS Institute of Knowledge MAKE A DIFFERENCE
CIK 12th INTERNATIONAL CONFERENCE

CONSCIENTIZAÇÃO EM SEGURANÇA CIBERNÉTICA: PERCEPÇÃO DE TRABALHADORES DE TECNOLOGIA DA INFORMAÇÃO DE UMA ORGANIZAÇÃO PÚBLICA FEDERAL BRASILEIRA POR ÁREA DE ATUAÇÃO

CYBERSECURITY AWARENESS: PERCEPTION OF INFORMATION TECHNOLOGY WORKERS OF A BRAZILIAN FEDERAL PUBLIC ORGANIZATION BY AREA OF ACTIVITY

DANIELA ALMEIDA
UNIVERSIDADE DE BRASÍLIA - UNB

CARLOS ANDRÉ DE MELO ALVES
UNIVERSIDADE DE BRASÍLIA

Comunicação:
O XII SINGEP foi realizado em conjunto com a 12th Conferência Internacional do CIK (CYRUS Institute of Knowledge) e com o Casablanca Climate Leadership Forum (CCLF 2024), em formato híbrido, com sede presencial na ESCA Ecole de Management, no Marrocos.

CONSCIENTIZAÇÃO EM SEGURANÇA CIBERNÉTICA: PERCEPÇÃO DE TRABALHADORES DE TECNOLOGIA DA INFORMAÇÃO DE UMA ORGANIZAÇÃO PÚBLICA FEDERAL BRASILEIRA POR ÁREA DE ATUAÇÃO

Objetivo do estudo
O objetivo deste estudo é identificar a percepção de trabalhadores de Tecnologia da Informação (TI) em uma organização pública federal brasileira sobre conscientização em segurança cibernética, considerando suas áreas de atuação

Relevância/originalidade
A conscientização em segurança cibernética é relevante para prevenção contra ameaças cibernéticas na atualidade. Estudos sobre o tema são escassos, inclusive abordando a percepção de trabalhadores de TI de organizações públicas, estratificando esses trabalhadores por área de atuação.

Metodologia/abordagem
O estudo é descritivo, com abordagens qualitativa e quantitativa. Coletaram-se dados por pesquisa bibliográfica, consulta documental e aplicação de questionário a 109 respondentes de órgãos e unidades descentralizadas (UDs). Trataram-se dados com estatística descritiva, confrontando evidências dos questionários com documentos.

Principais resultados
Houve 81,82% dos trabalhadores nas UDs e 88,00% dos trabalhadores dos órgãos percebendo comunicação de ameaças cibernéticas. Para 73,08% dos trabalhadores dos órgãos e 77,72% dos trabalhadores nas UDs, inexistem treinamentos sobre segurança cibernética, apesar de evidências documentais contrárias.

Contribuições teóricas/metodológicas
O estudo contribui para entendimento sobre conscientização em segurança cibernética, principalmente em organizações públicas. O trabalho pode subsidiar reflexões sobre adoção de estratégias para conscientização em segurança cibernética nessas organizações considerando suas áreas de atuação.

Contribuições sociais/para a gestão
Este trabalho contribui para aperfeiçoamento de estratégias para conscientização em segurança cibernética na organização estudada, e para reflexões de acadêmicos, gestores públicos e órgãos de controle a respeito da percepção sobre conscientização em segurança cibernética de organizações públicas no Brasil.

Palavras-chave: segurança cibernética, conscientização em segurança cibernética, ameaças cibernéticas, organizações públicas

CYBERSECURITY AWARENESS: PERCEPTION OF INFORMATION TECHNOLOGY WORKERS OF A BRAZILIAN FEDERAL PUBLIC ORGANIZATION BY AREA OF ACTIVITY

Study purpose
The objective of this study is to identify the perception of Information Technology (IT) workers in a Brazilian federal public organization about cybersecurity awareness, considering their areas of activity.

Relevance / originality
Cybersecurity awareness is relevant for preventing cyber threats today. Studies on the topic are scarce, including addressing the perception of IT workers in public organizations, stratifying these workers by area of activity

Methodology / approach
The study is descriptive, with qualitative and quantitative approaches. Data were collected through bibliographical research, document consultation and questionnaire application to 109 respondents from agendies and decentralized units (UDs). Data were treated with descriptive statistics, comparing evidence from questionnaires with documents.

Main results
There were 81,82% of workers in the UDs and 88,00% of workers in the agencies noticing communication of cyber threats For 73,08% of agency workers and 77,72% of workers in UDs, there is no training on cybersecurity, despite contrary documentary evidences.

Theoretical / methodological contributions
The study contributes to the understanding of cybersecurity awareness, especially in public organizations. The work can support reflections on the adoption of strategies for cybersecurity awareness in these organizations considering their areas of activity.

Social / management contributions
This work contributes to improving strategies for cybersecurity awareness in the organization studied, and to reflections by academics, public managers and control bodies regarding the perception of cybersecurity awareness in public organizations in Brazil.

Keywords: cybersecurity, cybersecurity awareness, cyber threats, public organizations

CONSCIENTIZAÇÃO EM SEGURANÇA CIBERNÉTICA: PERCEPÇÃO DE TRABALHADORES DE TECNOLOGIA DA INFORMAÇÃO DE UMA ORGANIZAÇÃO PÚBLICA FEDERAL BRASILEIRA POR ÁREA DE ATUAÇÃO

1 Introdução

A conscientização em segurança cibernética é fator a ser considerado para prevenção contra ameaças cibernéticas pelas organizações na atualidade. Estudos sobre essa conscientização podem, inclusive, considerar as percepções de trabalhadores de tecnologia da informação (TI) de organizações públicas federais. Essas percepções podem, também, ser contrastadas por área de atuação desses trabalhadores, seja em unidades centrais ou em unidades descentralizadas das organizações públicas.

Ante ao exposto, o problema proposto neste estudo é o seguinte: qual a percepção de trabalhadores de TI de uma organização pública federal brasileira sobre conscientização em segurança cibernética, considerando suas áreas de atuação? Assim, o objetivo deste estudo é identificar a percepção de trabalhadores de TI em uma organização pública federal brasileira sobre conscientização em segurança cibernética, considerando suas áreas de atuação.

Este estudo busca contribuir para entendimento sobre conscientização em segurança cibernética, principalmente em organizações públicas. O trabalho pode subsidiar reflexões sobre adoção de estratégias para conscientização em segurança cibernética na organização de onde os dados foram coletados, considerando suas áreas de atuação. Também pode proporcionar reflexões de gestores, acadêmicos e demais partes interessadas a respeito da percepção sobre conscientização em segurança cibernética de organizações públicas no Brasil.

2 Referencial Teórico

O referencial teórico aborda a segurança cibernética, ameaças cibernéticas e conscientização em segurança cibernética. Também relaciona o tema às organizações públicas brasileiras. O conceito de segurança cibernética baseia-se no Glossário de Segurança da Informação (Brasil, 2019), que consiste em:

> (...) ações voltadas para a segurança de operações, de forma a garantir que os sistemas de informação sejam capazes de resistir a eventos no espaço cibernético capazes de comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados armazenados, processados ou transmitidos e dos serviços que esses sistemas ofereçam ou tornem acessíveis (Brasil, 2019, p. 20).

A definição de ‘conscientização em segurança cibernética’ adotada baseia-se no estudo de Ngoma (2019). Trata-se de um conjunto de estratégias de educação e sensibilização de usuários, visando a disseminar conhecimento sobre as ameaças cibernéticas, os respectivos impactos sobre a rotina laboral e ativos da organização, e desenvolvimento de comportamento online seguro.

Ameaças à segurança cibernéticas são definidas com base nos frameworks CIS V8 (CIS, 2021), ENISA (2021) e ABNT (2015). Entre aquelas reportadas por gestores de TI, destacam-se: *malware* (*software* malicioso infiltrado por meio de agente invasor, que pode ter diversos propósitos, tais como captura, criptografia, corrupção ou destruição de dados e informações da rede afetada (CIS, 2021)), *phishing* (técnicas de engenharia social que enganam usuários despreparados e inocula softwares maliciosos na rede do alvo (CIS, 2021)) e *ransomware* (sequestro e criptografia de dados e exigência de resgate para suposta devolução à vítima (ENISA, 2021)).

3 Metodologia

O estudo é descritivo, com abordagem qualitativa e quantitativa. A população abrange trabalhadores de uma organização pública federal, com sede em Brasília-DF – e em unidades

descentralizadas (UDs), situadas nas demais unidades da Federação. A amostra não probabilística possui 109 respondentes que voluntariamente participaram do estudo. Desses, 52 trabalhavam nos órgãos e 57 deles, nas UDs.

A coleta de dados empregou pesquisa bibliográfica prévia (Prodanov & Freitas, 2013) e pesquisa documental - com consulta a normas internas e documentos públicos da organização, e pesquisa de campo com aplicação de questionário (Babbie, 2020). O questionário contemplou perguntas objetivas de múltipla escolha e baseou-se no estudo de Ngoma (2019), adaptadas para particularidades da organização pública objeto deste estudo, também considerou normas e diretrizes do governo federal. Antes da aplicação do questionário, realizou-se pré-teste com seis trabalhadores da organização pública estudada, e foi obtida prévia autorização da organização pública para coleta dos dados.

O tratamento dos dados coletados empregou estatística descritiva (pelas operações de frequência mediana e moda) e organizados em planilha. A contagem de frequência e edição dos percentuais consideraram os retornos válidos para cada questão. As análises também foram complementadas pelo resultado da análise documental; os resultados foram pontuados com argumentos oriundos do referencial teórico.

4 Análise dos Resultados

A partir da análise das respostas obtidas com aplicação do questionário, observou-se que os trabalhadores atuantes nas UDs demonstraram percepção ligeiramente menor sobre comunicação a respeito de ameaças cibernéticas (81,82% contra 88,00% dos respondentes dos órgãos), bem como menor percepção sobre treinamentos promovidos pela organização estudada par fomentar o comportamento online seguro, conforme será descrito nos próximos parágrafos.

Sobre a ciência de política formal de segurança cibernética, verificou-se que 57,69% dos respondentes dos órgãos e 64,91% das unidades descentralizadas (UDs) não sabem ou desconhecem a existência de tal política. Esse resultado contrasta com as evidências documentais de divulgação e publicização dessa política.

Com relação aos canais empregados pela organização estudada para comunicar ameaça cibernéticas, apurou-se que 78,00% dos respondentes dos órgãos e 74,50% dos que atuam em UDs manifestaram percepção de que o e-mail é o canal de comunicação de ameaças à segurança cibernética. Por outro lado, 81,82% dos respondentes das UDs e 88,00% dos respondentes dos órgãos percebem que a organização comunica ameaças cibernéticas. Documentos institucionais contrastam com esses resultados, pois constituem-se de variados canais de comunicação.

Quanto à frequência com que a organização promove treinamentos sobre segurança cibernética, os resultados evidenciam que 73,08% dos trabalhadores dos órgãos e 77,72% dos trabalhadores UDs afirmam que a organização nunca ou raramente promove treinamentos sobre segurança cibernética – apesar de campanhas ostensivas de divulgação de treinamentos sobre o tema localizados nas fontes secundárias de informação.

No que diz respeito à percepção do responsável pela conscientização sobre segurança cibernética, foram obtidas 68,63% de respostas válidas para respondentes dos órgãos e 67,27% de respostas válidas para respondentes de UDs apontando a área de TI**.**

Quando foram indagados sobre estarem cientes da existência de comitê interno envolvido em questões de segurança cibernética na organização, 34,62% dos respondentes atuantes nos órgãos e 28,07% dos participantes lotados nas UDs declararam inconsciência da existência desse comitê. O resultado também contrasta com as iniciativas institucionais de divulgação do comitê e das atividades desenvolvidas, verificas por meio de consulta documental.

Sobre o conhecimento de iniciativa estratégica da organização para abordar a segurança cibernética, apurou-se que 42,10% dos respondentes das UDs e 38,46% dos atuantes nos órgãos

declaram ciência dessas iniciativas fontes documentais da organização estudada indicam comunicação das iniciativas estratégica aos trabalhadores.

5 Considerações Finais

O objetivo deste estudo é identificar a percepção de trabalhadores de TI em uma organização pública federal brasileira sobre conscientização em segurança cibernética, considerando suas áreas de atuação. Realizou-se uma pesquisa predominantemente quantitativa, com aplicação de questionários via formulário eletrônico online, além da consulta a documentos a respeito da referida organização.

Os resultados indicaram que apenas 81,82% os trabalhadores atuantes nas UDs e 88,00% dos trabalhadores dos órgãos demonstraram percepção sobre comunicação a respeito de ameaças cibernéticas. Adicionalmente, 73,08% dos trabalhadores dos órgãos e 77,72% dos trabalhadores UDs afirmam que a organização nunca ou raramente promove treinamentos sobre segurança cibernética, embora evidências documentais indiquem a existência desses treinamentos.

Ademais, 78,00% dos respondentes dos órgãos e 74,50% dos que atuam em UDs manifestam percepção de que o e-mail é o canal de comunicação pelos quais a organização comunica ameaças à segurança cibernética.

Em complemento, a área de TI é responsável pela conscientização em segurança cibernética para 68,63% de respondentes dos órgãos e 67,27% de respondentes de UDs, sendo verificado que 57,69% dos respondentes dos órgãos e 64,91% das UDs não sabem ou desconhecem a existência de tal política, resultado que contrasta com as evidências documentais de divulgação e publicização dessa política.

Sobre iniciativas estratégicas de segurança cibernética da organização as respostas predominantes entre trabalhadores dos órgãos e das unidades descentralizadas foi de ciência. Por outro lado, sobre a existência de comitê interno envolvido em questões de segurança cibernética na organização, 34,62% dos respondentes atuantes nos órgãos e 28,07% dos participantes lotados nas UDs declararam inconsciência da existência desse comitê.

Este estudo trata tema atual, de interesse de organizações públicas. A leitura das respostas, quando confrontadas com evidências documentais, é uma oportunidade aos gestores da organização estudada para refletir sobre a efetividade das ações de conscientização em segurança cibernética em prática, inclusive o alcance dessas iniciativas aos trabalhadores de TI das unidades descentralizadas. É adequado delimitar que os achados deste estudo baseiam-se nas entrevistas e nos documentos que foram coletados.

Como sugestões para estudos futuros, recomenda-se a replicação do estudo em outros períodos de análise e abrangendo outras organizações públicas. Dada a importância da segurança cibernética no setor público em geral, o estudo, também, pode ser estendido a organizações não apenas na esfera federal, mas também estadual, distrital e municipal. Por fim, o estudo pode, também, não ser restrito a profissionais de TI, mas também a profissionais atuantes em outras atividades das organizações públicas.

6 Referências

Associação Brasileira de Normas Técnicas (2015). ABNT NBR ISO/IEC 27032:2015. Tecnologia da Informação – Técnicas de segurança – Diretrizes para segurança cibernética. Rio de Janeiro: ABNT.

Babbie, E. R. (2020). The practice of social research. Cengage learning.

Center for Internet Security (2021). Critical Security Controls Version 8. Center for Internet Security. https://learn.cisecurity.org/CIS-Controls-v8-guide-pdf.

European Union Agency for Cybersecurity. (2021) ENISA Threat Landscape 2021: April 2020 to Mid-July 2021 October, 2021. Disponível em https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021.

International Telecommunication Union (2020). Global Cybersecurity Index 2020. ITU. Recuperado em 11 de agosto de 2024, de https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf.

Ngoma, M. L (2019). Cybersecurity Awareness in South African Public Sector Organisations. 2019. Dissertação de Mestrado. University of Johannesburg (South Africa). Recuperado em 11 de agosto de 2024, de https://search.proquest.com/openview/01424f13f773a0b79eaaa73104fc722c/1?pq-origsite=gscholar&cbl=18750&diss=y.

Presidência da República (2019). Gabinete de Segurança Institucional. Portaria GSI/PR nº 93/2019 - Glossário de Segurança da Informação. Recuperado em 11 de agosto de 2024, de https://www.gov.br/gsi/pt-br/assuntos/dsic/glossario-de-seguranca-da-informacao-1.